

Кутырёва Елена Вячеславовна
Логачёв Олег Алексеевич

О связи основных параметров деревьев решений по четностям со
спектральными свойствами булевых функций

Для произвольного двоичного дерева T с корнем обозначим через $lvs(T)$ множество листьев дерева T , $d(u)$ — длина пути в дереве T от корня до листа u (число внутренних вершин дерева T на этом пути).

Размером $size(T) = \#lvs(T)$ дерева T будем называть количество его листьев.

Глубиной $depth(T)$ дерева T называют максимальную длину пути от корня до листа в этом дереве:

$$depth(T) = \max_{u \in T} d(u).$$

Уровнем $lev(T)$ дерева T называют минимальную длину пути от корня до листа в этом дереве:

$$lev(T) = \min_{u \in T} d(u).$$

Вычислительная модель, называемая дерево решений по четностям (parity decision tree), является обобщением модели дерево решений (decision tree).

Деревом решений по четностям T булевой функции $f \in \mathcal{F}_n$ называют двоичное дерево с корнем, у которого все внутренние вершины помечены линейными формами $\bigoplus_{i \in S} x_i$, $S \subseteq [n]$, и имеют два исходящих ребра, помеченных 0 и 1. На входном наборе $\mathbf{b} = (b_1, \dots, b_n) \in \{0, 1\}^n$ вычисление в каждой внутренней вершине (начиная с корня) производится следующим образом: в вершине, помеченной $\bigoplus_{i \in S} x_i$, если $\bigoplus_{i \in S} b_i = 1$, переход осуществляется по ребру, помеченному 1, в противном случае — по ребру, помеченному 0. Таким образом, входной набор $\mathbf{b}$ определяет некоторый путь по дереву T и заканчивается в листе, помеченном выходным значением, совпадающим со значением функции $f(\mathbf{b})$ (то есть дерево T определяет процесс вычисления значений функции f).

Деревом решений T булевой функции $f \in \mathcal{F}_n$ называется вычислительная модель, отличающаяся от дерева решений по четностям тем, что все внутренние вершины дерева T помечены переменными $x_i, i \in [n]$.

Необходимо отметить, что дерево решений, как и дерево решений по четностям для функции $f : \{0, 1\}^n \rightarrow \{0, 1\}$ может быть построено различными способами.

Через $PDT(f)$ будем обозначать множество всех деревьев решений по четностям для булевой функции f , а через $DT(f)$ — множество всех деревьев решений для булевой функции f .

Любое дерево решений (дерево решений по четностям) функции из $\mathcal{F}_n$ можно преобразовать в «полное» двоичное дерево размера 2^n . Но такие деревья решений «скрывают» (не отражают) ряд параметров и свойств булевой функции.

Дерево решений T булевой функции f назовём информативным, если для него выполнено следующее условие: для любого пути от корня данного дерева к листу длины r его подпуть длины $r - 1$ не вычисляет (не определяет) значение функции f .

Дерево решений по четностям T булевой функции f назовём информативным, если для него выполнено следующее условие: для любого пути длины r от корня данного дерева к листу соответствующая ему система линейных уравнений имеет ранг r .

Определим функцию $\text{Sort}_3 : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2$ следующим образом:
 $\text{Sort}_3(x_1, x_2, x_3) = 1$ тогда и только тогда, когда $x_1 \leq x_2 \leq x_3$ или $x_1 \geq x_2 \geq x_3$.

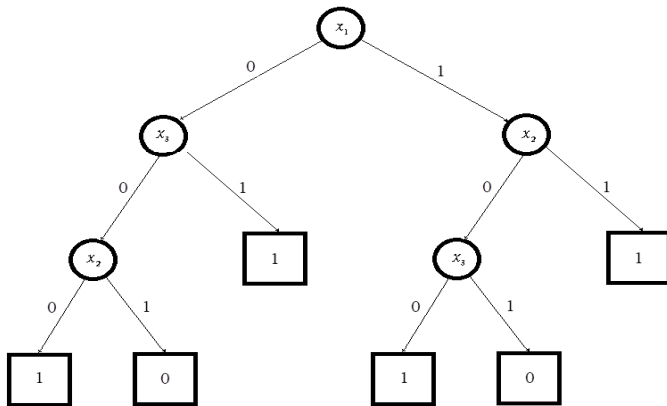


Рис.: Пример дерева решений функции Sort_3 .

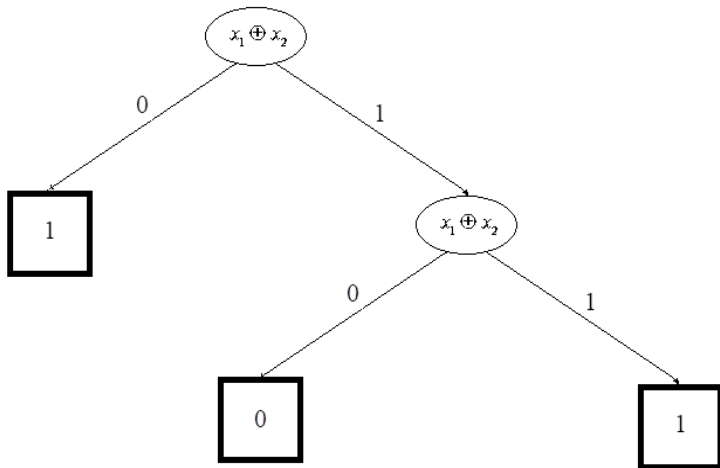


Рис.: Пример дерева решений по чётностям функции **Sort₃**.

Обобщенной глубиной (соответственно, глубиной) $depth^*(f)$ (соответственно, $depth(f)$) булевой функции $f \in \mathcal{F}_n$ будем называть минимальную глубину дерева по всем деревьям из множества $PDT(f)$ (соответственно, $DT(f)$),

$$depth^*(f) = \min_{T \in PDT(f)} depth(T), depth(f) = \min_{T \in DT(f)} depth(T).$$

Обобщенным уровнем (соответственно, уровнем) $lev^*(f)$ (соответственно, $lev(f)$) булевой функции $f \in \mathcal{F}_n$ будем называть минимальный уровень дерева по всем деревьям из множества $PDT(f)$ (соответственно, $DT(f)$),

$$lev^*(f) = \min_{T \in PDT(f)} lev(T), lev(f) = \min_{T \in DT(f)} lev(T).$$

Обобщенным размером (соответственно, размером) $size^*(f)$ (соответственно, $size(f)$) булевой функции $f \in \mathcal{F}_n$ будем называть минимальный размер дерева по всем деревьям из множества $PDT(f)$ (соответственно, $DT(f)$),

$$size^*(f) = \min_{T \in PDT(f)} size(T), size(f) = \min_{T \in DT(f)} size(T).$$

Замечание

В приведённых выше определениях поиск минимума осуществляется по всем деревьям решений по чётностям (или просто деревьям решений), вычисляющим булеву функцию f , однако, в силу того, что минимум достигается на информативном дереве, и поиск следует ограничивать только множеством информативных деревьев для данной булевой функции.

Предложение

Верны соотношения

$$\mathit{depth}^*(f) \leq \mathit{depth}(f), \mathit{lev}^*(f) \leq \mathit{lev}(f), \mathit{size}^*(f) \leq \mathit{size}(f).$$

Предложение

Для любого дерева решений по четностям T булевой функции справедливо неравенство $\mathit{lev}(T) \leq \mathit{depth}(T)$.

Все утверждения ниже сформулированы для информативных деревьев и информативных деревьев по чётностям, если не указано иное.

Представляет определённый интерес описание классов булевых функций, обладающих экстремальными значениями параметров уровня и глубины. В частности, рассмотрим вопрос о необходимых и достаточных условиях максимальности значений этих параметров.

Будем обозначать функцию чётности от n переменных как

$$XOR_n(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n.$$

Предложение

Булева функция $f \in \mathcal{F}_n$, $f \neq \text{const}$, удовлетворяет условию

$$\text{depth}(f) = \text{lev}(f) = n$$

тогда и только тогда, когда $f = XOR_n \oplus c$, где $c \in \mathbb{F}_2$.

Пусть $T \in DT(f)$ состоит из s путей $P_1, \dots, P_s$. Множество векторов из V_n , соответствующих вычислительному пути P в дереве T , является аффинным подпространством пространства V_n , обозначим его через C_P . Функция f является константой на C_P . Обозначим её значение на C_P через $f(P)$. Так как каждый вектор из V_n соответствует единственному пути в дереве T , аффинные подпространства $\{C_P : P \in T\}$ образуют разбиение пространства V_n .

Замечание

Для $f \in \mathcal{F}_n$ выполняется

$$f = \sum_{P \in T} f(P) \cdot \mathbf{1}_{C_P},$$

где $\mathbf{1}_{C_P}$ — индикаторная функция, $\mathbf{1}_{C_P}(x) = \begin{cases} 1, & \text{если } x \in C_P, \\ 0, & \text{если } x \notin C_P. \end{cases}$

Рассмотрим в дереве $T \in PDT$ размера s путь P_i длины r , $i \in [s]$, внутренние вершины которого помечены линейными формами

$$\bigoplus_{k \in S_1^{(i)}} x_k, \dots, \bigoplus_{k \in S_r^{(i)}} x_k,$$

$$P_i = \{ \bigoplus_{k \in S_1^{(i)}} x_k = \alpha_1^{(i)}, \dots, \bigoplus_{k \in S_r^{(i)}} x_k = \alpha_r^{(i)} \}.$$

Для мультиаффинной функции

$$g = \left(\bigoplus_{k \in S_1^{(i)}} x_k \oplus \alpha_1^{(i)} \oplus 1 \right) \wedge \dots \wedge \left(\bigoplus_{k \in S_r^{(i)}} x_k \oplus \alpha_r^{(i)} \oplus 1 \right) \text{ через } N_g$$

обозначим множество наборов значений переменных из пространства V_n , для которых значение g равно 1.

Множество N_g является аффинным подпространством в V_n , описываемым задаваемой путём P_i системой линейных уравнений

$$\left\{ \bigoplus_{k \in S_1^{(i)}} x_k = \alpha_1^{(i)}, \dots, \bigoplus_{k \in S_r^{(i)}} x_k = \alpha_r^{(i)} \right\}. \quad (1)$$

Размерность аффинного подпространства равна разности числа переменных и ранга системы (1).

Если

$$f = g_1 \vee g_2 \vee \dots \vee g_m,$$

то для носителя функции f верно $\text{supp}(f) = \bigcup_{j=1}^m N_{g_j}$. Поэтому с каждым представлением булевой функции f в виде дизъюнкции мультиаффинных функций связано покрытие носителя f аффинными подпространствами, соответствующими этим мультиаффинным функциям.

Дизъюнкцию мультиаффинных функций $f = g_1 \vee g_2 \vee \dots \vee g_m$ будем называть точной, если покрытие $\text{supp}(f)$ аффинными подпространствами, соответствующими мультиаффинным функциям $g_j, j = 1, \dots, m$, является разбиением $\text{supp}(f)$ (т.е. аффинные подпространства $N_{g_j}, j = 1, \dots, m$, попарно не пересекаются, $N_{g_i} \cap N_{g_j} = \emptyset, i \neq j$).

Предложение

Любому дереву по четностям $T \in PDT(f), f \in \mathcal{F}_n$ соответствует точная дизъюнкция мультиаффинных функций f .

Пусть $\mathbf{g}_1, \mathbf{g}_2$ — мультиаффинные функции и существует аффинная функция $\bigoplus_{k \in S} x_k \oplus \alpha$ такая, что $\mathbf{g}_1 = \left(\bigoplus_{k \in S} x_k \oplus \alpha \right) \wedge \mathbf{g}'_1$,
 $\mathbf{g}_2 = \left(\bigoplus_{k \in S} x_k \oplus \alpha \oplus \mathbf{1} \right) \wedge \mathbf{g}'_2$. В этом случае будем говорить, что $\mathbf{g}_1$ и $\mathbf{g}_2$ имеют общую аннигилирующую аффинную функцию.

Предложение

Пусть $\mathbf{g}_1, \mathbf{g}_2$ — мультиаффинные функции. Тогда $N_{\mathbf{g}_1} \cap N_{\mathbf{g}_2} = \emptyset$ (или, что эквивалентно, $\mathbf{g}_1 \wedge \mathbf{g}_2 = \mathbf{0}$) тогда и только тогда, когда $\mathbf{g}_1$ и $\mathbf{g}_2$ имеют общую аннигилирующую аффинную функцию.

Теорема

Дизъюнкция мультиаффинных функций является точной тогда и только тогда, когда любая пара ее мультиаффинных функций имеет общую аннигилирующую аффинную функцию.

Пусть $f \in \mathcal{F}_n$, $1 \leq i_1 < \dots < i_m \leq n$, $0 \leq m \leq n$, и $a_1, \dots, a_m \in \{0, 1\}$. Тогда подфункцией $f_{i_1, \dots, i_m}^{a_1, \dots, a_m} \in \mathcal{F}_{n-m}$ функции f будем называть функцию вида:
 $f_{i_1, \dots, i_m}^{a_1, \dots, a_m}(\tilde{x}) = f(\dots, x_{i_1-1}, a_1, x_{i_1+1}, \dots, x_{i_m-1}, a_m, x_{i_m+1}, \dots)$, где $\tilde{x} = (x_1, \dots, x_{i_1-1}, x_{i_1+1}, \dots, x_{i_m-1}, x_{i_m+1}, \dots, x_n)$.

Булева функция $f \in \mathcal{F}_n$ называется корреляционно-иммунной порядка m , $0 < m < n$, тогда и только тогда, когда для любых наборов $1 \leq i_1 < \dots < i_m \leq n$, $a_1, \dots, a_m$, $a_i \in \mathbb{F}_2$, $i = 1, \dots, m$, выполняется равенство $\text{wt}(f_{i_1, \dots, i_m}^{a_1, \dots, a_m}) = \text{wt}(f)/2^m$. Если функция корреляционно-иммунна порядка m , то она корреляционно-иммунна порядка k для любого $0 < k < m$.

Предложение

Пусть $f \in \mathcal{F}_n$ — корреляционно-иммунная функция порядка m , $2^m < \text{wt}(f) < 2^n$, и T — произвольное информативное дерево решений из $DT(f)$. Тогда выполнено неравенство $\text{lev}(T) > m$.

Следствие

Если $f \in \mathcal{F}_n$ — корреляционно-иммунная функция порядка m , $0 < m < n - 1$ и $2^m < \text{wt}(f) < 2^n$, то для любого дерева решений T из $DT(f)$ выполнено неравенство $\text{size}(T) > 2^m$.

Следствие

Пусть $f \in \mathcal{F}_n$ — корреляционно-иммунная функция порядка m , $0 < m < n - 1$ и $2^m < wt(f) < 2^n$. Тогда справедливо неравенство

$$depth(f) - lev(f) < n - m.$$

Следствие

Пусть $f \in \mathcal{F}_n$ — корреляционно-иммунная функция порядка m . Тогда ширина любой её дизъюнктивной нормальной формы $DNF(f)$ удовлетворяет неравенству $width(DNF(f)) > m$.

Пусть $f \in \mathcal{F}_n$. Функция $g \in \mathcal{F}_n$ называется аннигилятором булевой функции f , если выполняется тождество $f(x)g(x) \equiv 0$. Множество всех аннигиляторов функции f будем обозначать через

$$Ann(f) = \{g \in \mathcal{F}_n | fg \equiv 0\}.$$

Порядком алгебраической иммунности булевой функции $f \in \mathcal{F}_n$ называют неотрицательное целое число

$$AI(f) = \min\{deg_2(g) | g \in \mathcal{F}_n, g \neq 0, f(x)g(x) \equiv 0 \vee (1 \oplus f(x))g(x) \equiv 0\}.$$

Предложение

Пусть $f \in \mathcal{F}_n$ и $lev^*(f) < n/2$. Тогда справедливо неравенство $AI(f) \leq lev^*(f)$.

Предложение

Пусть $K \vee f = f, f \in \mathcal{F}_n$, и $rank(K) = r$. Тогда справедливы соотношения

$$lev(f) \leq r,$$

$$AI(f) \leq r.$$

Пусть $\mathcal{PF}_n = \mathbb{R}^{\{0,1\}^n}$ — множество псевдобулевых функций $f : \{0,1\}^n \rightarrow \mathbb{R}$ от n переменных.

В пространстве $\mathcal{PF}_n$ для произвольной пары псевдобулевых функций f и g определено скалярное произведение

$$\langle f, g \rangle = 2^{-n} \sum_{x \in \{0,1\}^n} f(x)g(x),$$

а для любой псевдобулевой функции f определена L_2 норма

$$\|f\|_2 = \sqrt{2^{-n} \sum_{x \in \{0,1\}^n} f(x)^2} = \sqrt{\langle f, f \rangle}.$$

Множество псевдобулевых функций

$$\chi(n) = \{\chi_u(x) = (-1)^{u \cdot x} | u, x \in \{0,1\}^n\},$$

составляет ортонормированный базис пространства $\mathcal{PF}_n$.

Представлением Фурье для функции $f : \{0, 1\}^n \rightarrow \mathbb{R}$ относительно базиса $\chi(n)$ называют соотношение вида

$$f(x) = \sum_{u \in \{0,1\}^n} \hat{f}(u) \chi_u(x),$$

где

$$\hat{f}(u) = 2^{-n} \sum_{x \in \{0,1\}^n} f(x) \chi_u(x). \quad (2)$$

Величину (2) называют коэффициентом Фурье функции f , соответствующим вектору u , а совокупность величин $\{\hat{f}(u), u \in \{0, 1\}^n\}$ — спектром Фурье этой функции.

Для булевой функции $f : \{0, 1\}^n \rightarrow \{0, 1\}$ определим для любого $u \in \{0, 1\}^n$ величину

$$F_f(u) = 2^n \hat{f}(u).$$

Пусть $T \in PDT(f)$ состоит из m путей $P_1, \dots, P_m$. Множество векторов из V_n , соответствующих вычислительному пути $P \in \{P_1, \dots, P_m\}$ длины r ,

$$P = \left\{ \bigoplus_{k \in S_1} x_k = \alpha_1, \dots, \bigoplus_{k \in S_r} x_k = \alpha_r \right\},$$

является аффинным подпространством $H_P = L_P \oplus u_P$ пространства V_n , где L_P — соответствующее линейное подпространство размерности $n - r$, а u_P — некоторый вектор из V_n .

Функция-индикатор аффинного подпространства H_P имеет вид

$$\prod_{j=1}^r \left(\bigoplus_{k \in S_j} x_k \oplus \alpha_j \oplus 1 \right) = Ind_{H_P}(x).$$

Замечание

Пусть $f \in \mathcal{F}_n$, $T \in PDT(f)$, и $P \in T$,
 $P = \{ \bigoplus_{k \in S_1} x_k = \alpha_1, \dots, \bigoplus_{k \in S_r} x_k = \alpha_r \}.$

Тогда множество H_P состоит из 2^{n-r} векторов вида $(*_{{a_r}^{(j)}}^{i_r} ***_{{a_2}^{(j)}}^{i_2} *_{{a_1}^{(j)}}^{i_1} *)$,
 $j = \overline{1, 2^{n-r}}$. Переменные с индексами из $[n] \setminus \{i_1, \dots, i_r\}$ при этом
принимают все возможные 2^{n-r} значений. Значения $\{i_1, \dots, i_r\}$
можно выбирать произвольным образом.

Лемма

Пусть P — вычислительный путь длины r из $T \in PDT(f)$, $f \in \mathcal{F}_n$, и $g(x) = Ind_{H_P}(x)$. Тогда $F_g(w) = 0$, если $w \notin L_P^\perp$,
 $F_g(w) = 2^{n-r} \cdot (-1)^{w \cdot u_P}$, если $w \in L_P^\perp$.

Предложение

Пусть $T \in PDT(f)$, $size(T) = s$, пути $P_{j_1}, \dots, P_{j_m}$, $j_i \in [s]$, заканчиваются листьями с пометкой 1, остальные пути заканчиваются листьями с пометкой 0, r_i — длина P_{j_i} , $i \in [m]$, $f \in \mathcal{F}_n$. Тогда $F_f(w) = \sum_{i=1}^m Ind_{w \in L_{P_{j_i}}^\perp} \cdot 2^{n-r_{j_i}} \cdot (-1)^{w \cdot u_{P_{j_i}}}$.

Следствие

Пусть $f = \{f^{(n)}\}_{n=1}^{\infty}$ — семейство отображений, $f^{(n)} : \{0, 1\}^n \longrightarrow \{0, 1\}$, и $p(n)$ — некоторый полином с неотрицательными коэффициентами, такие, что $\text{size}^*(f^{(n)}) < p(n)$. Тогда величина $F_{f^{(n)}}(w) = 2^n \widehat{f^{(n)}}(w)$ вычисляется для любого $w \in \{0, 1\}^n$ с полиномиальной трудоёмкостью.

Замечание

Указанное следствие не предлагает алгоритма вычисления соответствующих коэффициентов Фурье. Речь идет лишь о существовании алгоритма с указанной трудоёмкостью.

Спасибо за внимание