Пороговые функции и пороговые схемы

В.В. Подольский

Булевы функции

- Булева функция: $f : \{0,1\}^n \to \{0,1\}$
- $\{f_n\}_{n=1}^{\infty}$, $f_n : \{0,1\}^n \to \{0,1\}$
- $x = (x_1, \ldots, x_n) \in \{0,1\}^n$

Примеры:

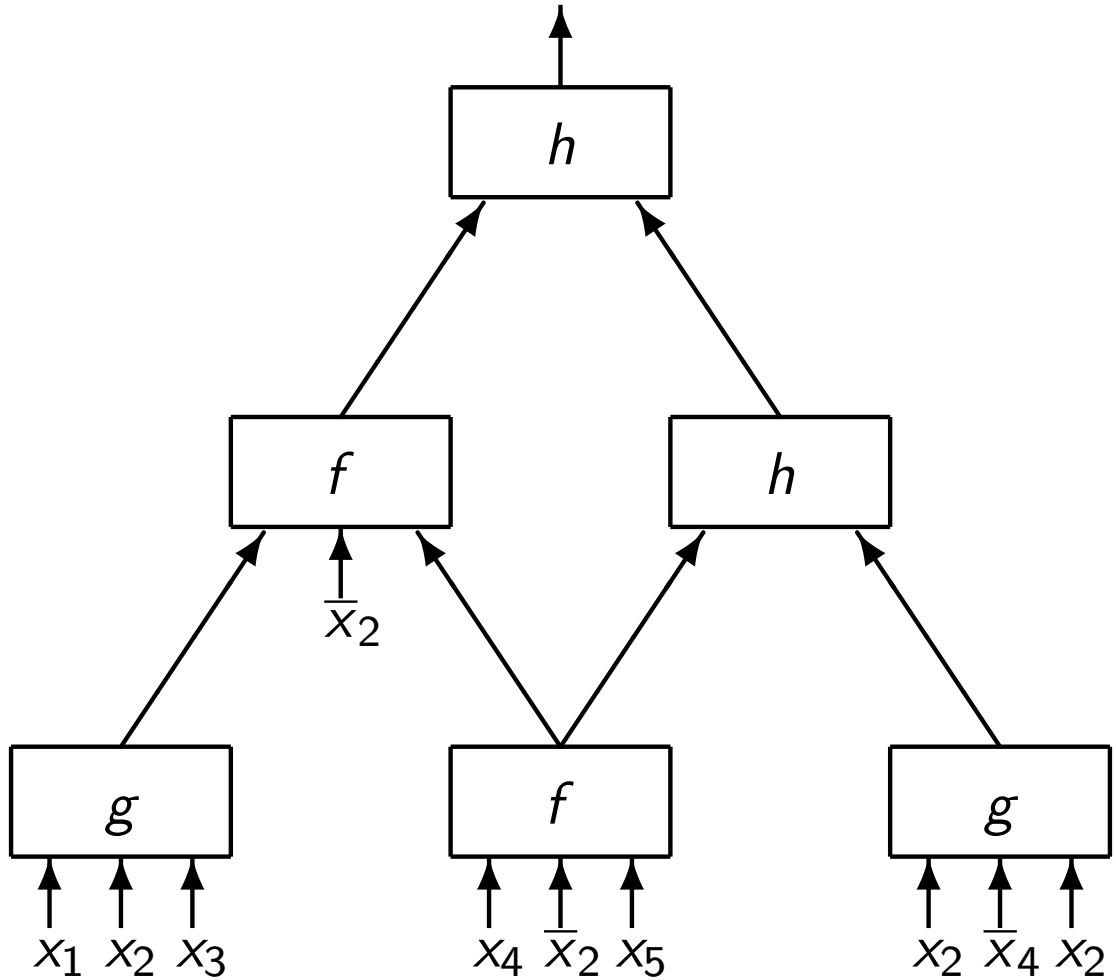
$$\mathrm{AND}(x) = \bigwedge_{i=1}^{n} x_i, \quad \mathrm{OR}(x) = \bigvee_{i=1}^{n} x_i$$

$$\mathrm{XOR} = \bigoplus_{i=1}^{n} x_i$$

$$\mathrm{MOD}_m(x) = 1 \Leftrightarrow \sum_{i=1}^{n} x_i \equiv 1 \pmod{m}$$

$$\mathrm{MAJ}(x) = 1 \Leftrightarrow \sum_{i=1}^{n} x_i > \frac{n}{2}$$

Булевы схемы



Размер схемы — число элементов в ней.

Класс AC^0

Определение

Класс AC^0 состоит из булевых функций, реализуемых схемами полиномиального размера и постоянной глубины, состоящими из AND, OR неограниченной входной степени и отрицаний.

Теорема (Фёрст, Сакс, Сипсер, 1983)

$\mathrm{XOR} \notin AC^0$.

Более того, $\mathrm{MOD}_m \notin AC^0$.

Класс ACC^0

Определение

Класс ACC^0 состоит из булевых функций, реализуемых схемами полиномиального размера и постоянной глубины, состоящими из AND, OR, MOD_m для всех m неограниченной входной степени и NOT.

Класс $\mathrm{ACC}^0[m]$ состоит из булевых функций, реализуемых схемами полиномиального размера и постоянной глубины, состоящими из AND, OR, MOD_m неограниченной входной степени и отрицаний.

Теорема (Разборов, Смоленский, 1987)

Если p и q – различные простые числа, то $MOD_p \notin \mathrm{ACC}^0[q]$

Теорема (Разборов, 1987)

$\mathrm{MAJ} \notin \mathrm{ACC}^0[p]$ *для простого p*

Класс TC^0

Определение

Класс TC^0 состоит из булевых функций, реализуемых схемами полиномиального размера и постоянной глубины, состоящими из AND, OR, MAJ неограниченной входной степени и NOT.

Лемма

Для всякого m верно $\mathrm{MOD}_m \in \mathsf{TC}^0$. Следовательно $\mathsf{ACC}^0 \subseteq \mathsf{TC}^0$

Определение

Пусть $\mathcal{C}_1$ и $\mathcal{C}_2$ классы булевых схем. Тогда через $\mathcal{C}_1 \circ \mathcal{C}_2$ мы обозначаем класс схем полиномиального размера состоящих из схемы из $\mathcal{C}_1$, в которую вместо входных переменных подставили схемы из $\mathcal{C}_2$.

Мы обозначаем также $\mathcal{C}^{(i)} = \underbrace{\mathcal{C} \circ \ldots \circ \mathcal{C}}_{i}$

Пороговые элементы

Определение

Линейный пороговый элемент $f : \{0,1\}^n \to \{0,1\}$ задается целыми числами $w_1, \ldots, w_n, t$ и $f(x) = 1$ тогда и только тогда, когда

$$w_1 x_1 + w_2 x_2 + \ldots + w_n x_n \geqslant t.$$

- Обозначим через THR класс всех пороговых функций.
- Обозначим через MAJ класс всех обобщенных функций голосования, таких что все w_i и t полиномиальны по n.

Пороговые схемы

Лемма

$$\mathsf{TC}^0 = \bigcup_{i=1}^{\infty} \mathsf{MAJ}^{(i)}$$

Теорема (Goldmann, Håstad, Razborov'92)

Для всех i

$$\mathsf{MAJ}^{(i)} \subseteq \mathsf{THR}^{(i)} \subseteq \mathsf{MAJ}^{(i+1)}.$$

Следовательно, $\mathsf{TC}^0 = \bigcup_{i=1}^{\infty} \mathsf{THR}^{(i)}$

Иерархия пороговых схем

$$\mathsf{MAJ} \subseteq \mathsf{THR} \subseteq \mathsf{MAJ}^{(2)} \subseteq \mathsf{THR}^{(2)} \subseteq \mathsf{MAJ}^{(3)} \subseteq \mathsf{THR}^{(3)} \subseteq \ldots$$

Определение

Положим

$$\mathrm{IP}(x, y) = \bigoplus_{i=1}^{n} x_i \wedge y_i,$$

где $x, y \in \{0,1\}^n$.

Теорема (Hajnal et al.'93)

$\mathrm{IP}(x, y) \notin \mathrm{MAJ} \circ \mathrm{MAJ}$.

Открытый вопрос

Предъявить функцию, не лежащую в $\mathrm{THR} \circ \mathrm{THR}$.

Между $\mathsf{MAJ} \circ \mathsf{MAJ}$ и $\mathsf{THR} \circ \mathsf{THR}$

$\mathsf{THR} \circ \mathsf{THR}$

| Chattopadhyay, Mande '18

$\mathsf{THR} \circ \mathsf{MAJ}$

| Goldmann et al.'92

$\mathsf{MAJ} \circ \mathsf{MAJ}$

Теорема (Goldmann, Håstad, Razborov'92)

$\mathsf{MAJ} \circ \mathsf{THR} = \mathsf{MAJ} \circ \mathsf{MAJ}$.

Теорема (Forster et al.'01)

$\mathrm{IP} \not\in \mathsf{THR} \circ \mathsf{MAJ}$.

Полиномиальные пороговые элементы

Полиномиальным пороговым элементом называется целочисленный многочлен p от n переменных.

Полиномиальный пороговый элемент вычисляет $f\colon \{0,1\}^n \to \{0,1\}\colon p(x) \geqslant 0 \Leftrightarrow f(x) = 1$.

Степень порогового элемента — просто степень многочлена
Вес порогового элемента — сумма абсолютных значений его коэффициентов

Пороговая степень f — минимальная степень порогового элемента для f
Обозначаем пороговую степень f через $\deg(f)$.

Пороговый вес f — минимальный вес порогового элемента для f

Обозначим через $W(f, d)$ минимальный вес порогового элемента для f степени не выше d.

Оценки порогового веса

Теорема (Muroga'71, Håstad'94)

$W(f,1) = n^{\Theta(n)}$

Теорема (P.'09)

$W(f,d) = n^{\Theta_d(n^d)}$

$$W \stackrel{def}{=} \max_d \max_{f:\ \deg(f)\leqslant d} W(f,d)$$

Лучшая ранее известная оценка на W:

$$W \geqslant 2^{\Omega(2^{n/8})}$$

Оценки порогового веса

Теорема (Muroga'71, Håstad'94)

$W(f,1) = n^{\Theta(n)}$

Теорема (P.'09)

$W(f,d) = n^{\Theta_d(n^d)}$

$$W \stackrel{def}{=} \max_d \max_{f:\ \deg(f)\leqslant d} W(f,d)$$

Лучшая ранее известная оценка на W:

$$W \geqslant 2^{\Omega(2^{n/8})}$$

Теорема

$$W \geqslant 2^{\Omega(2^{2n/5})}$$

Небольшое число пороговых элементов

Известные результаты:

Экспоненциальная нижняя оценка для схем с $n^{o(1)}$ элементами MAJ (Beigel'94)

Экспоненциальная нижняя оценка для схем с одним элементом THR (Aspnes et al.'94)

Сверхполиномиальная нижняя для схем с $O(\log^2 n)$ элементами THR (Chattopadhyay, Hansen'05)

Теорема

Для всякого $\epsilon > 0$ всякая схема глубины h, вычисляющая XOR и содержащая $t \leqslant \left(\frac{1}{4} - \epsilon\right) \log n$ пороговых элементов имеет размер

$$S \geqslant 2^{\frac{1}{14}\left(\frac{n}{g(t)}\right)^{\frac{1}{h+1}}}$$

для достаточно больших n, где $g(t) = (t+1)^2 2^{4t}$.

Точные пороговые элементы

Определение

Точная пороговая функция $f : \{0,1\}^n \to \{0,1\}$ задается целыми числами $w_1, \ldots, w_n, t$ и $f(x) = 1$ тогда и только тогда, когда

$$w_1 x_1 + w_2 x_2 + \ldots + w_n x_n = t$$

- Обозначим через ETHR класс всех точных пороговых функций
- Обозначим через EMAJ класс всех пороговых функций с ограниченными полиномом w_i и t

Иерархия точных пороговых схем

Теорема

Для всех i верно

$$\mathsf{EMAJ}^{(i)} \subseteq \mathsf{ETHR}^{(i)} \subseteq \mathsf{EMAJ}^{(i+1)}$$

То есть,

$$\mathsf{EMAJ} \subseteq \mathsf{ETHR} \subseteq \mathsf{EMAJ}^{(2)} \subseteq \mathsf{ETHR}^{(2)} \subseteq \mathsf{EMAJ}^{(3)} \subseteq \mathsf{ETHR}^{(3)} \subseteq \ldots$$

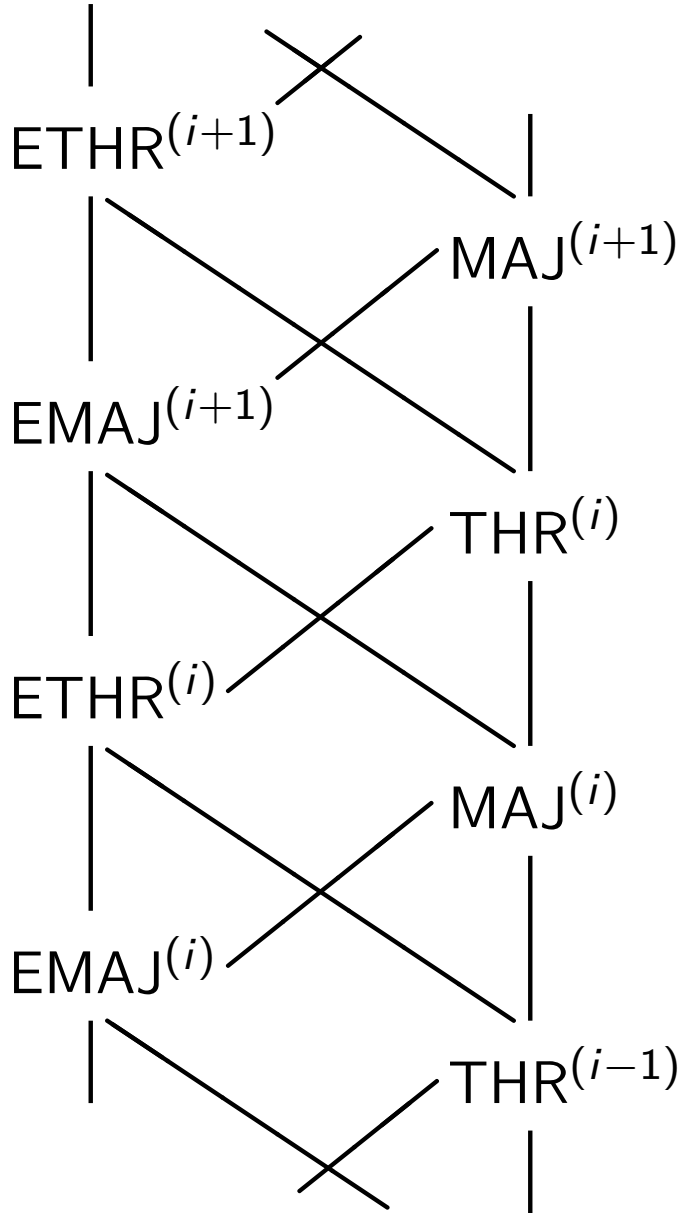
Объединенная иерархия

Для всех $i \geqslant 1$

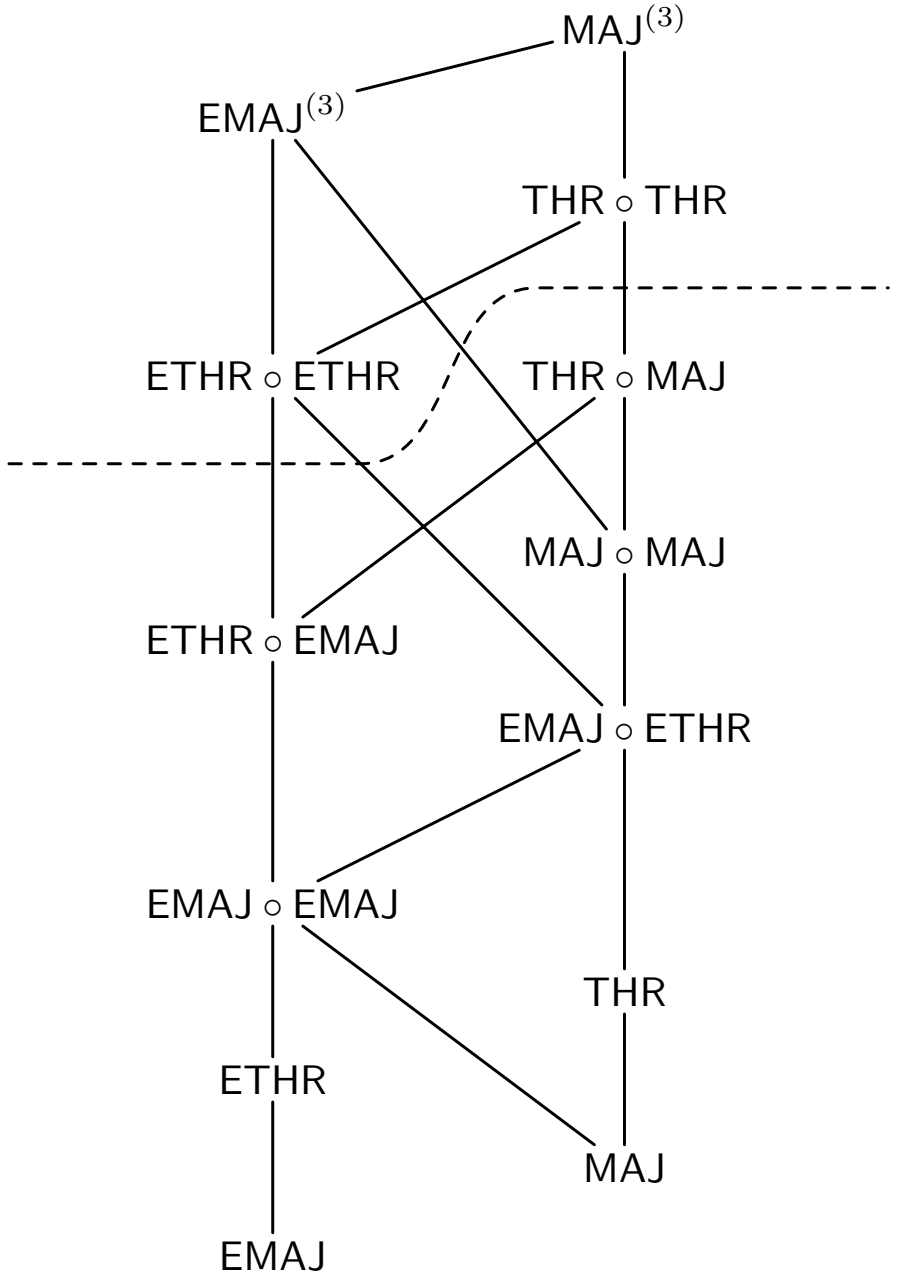
$$\mathsf{MAJ}^{(i)} \subseteq \mathsf{EMAJ}^{(i+1)} \subseteq \mathsf{MAJ}^{(i+1)}$$

$$\mathsf{THR}^{(i)} \subseteq \mathsf{ETHR}^{(i+1)} \subseteq \mathsf{THR}^{(i+1)}$$

Объединенная иерархия



Разделения классов: общая картина



Разделения классов

Теорема

1. $\mathrm{THR} \circ \mathrm{MAJ} \neq \mathrm{ETHR} \circ \mathrm{ETHR}$,
2. $\mathrm{MAJ} \circ \mathrm{MAJ} \neq \mathrm{ETHR} \circ \mathrm{ETHR}$,
3. $\mathrm{THR} \circ \mathrm{MAJ} \neq \widehat{\mathrm{ELT}}_3$,
4. $\mathrm{MAJ} \circ \mathrm{MAJ} \not\subseteq \mathrm{EMAJ} \circ \mathrm{ETHR}$.

Пороговые функции с произвольным множеством входов

Булева функция $f : \{a, b\}^n \to \{-1, +1\}$

Полиномиальным пороговым элементом, вычисляющим f называется многочлен $p \in \mathbb{R}[x_1, \ldots, x_n]$, такой что для всех $x \in \{a, b\}^n$ верно

$$f(x) = \operatorname{sign} p(x).$$

Меры сложности:

Степень p — просто степень многочлена

Длина p — число мономов в нем

Классы PTF

Для данных $l(n)$ и $d(n)$ обозначим через

$$\mathrm{PTF}_{a,b}(l(n), d(n))$$

класс булевых функций над $\{a, b\}^n$, вычислимый полиномиальными пороговыми элементами длины $l(n)$ и степени $d(n)$

$\mathrm{PTF}_{a,b}(l(n), \infty)$ — нет ограничения на степень

$\mathrm{PTF}_{a,b}(d(n)) = \mathrm{PTF}_{a,b}(\mathrm{poly}(n), d(n))$

Классы PTF

Для данных $l(n)$ и $d(n)$ обозначим через

$$\mathrm{PTF}_{a,b}(l(n), d(n))$$

класс булевых функций над $\{a, b\}^n$, вычислимый полиномиальными пороговыми элементами длины $l(n)$ и степени $d(n)$

$\mathrm{PTF}_{a,b}(l(n), \infty)$ — нет ограничения на степень

$\mathrm{PTF}_{a,b}(d(n)) = \mathrm{PTF}_{a,b}(\mathrm{poly}(n), d(n))$

Мы обсудим область определения $\{1, 2\}^n$. Результаты переносятся на все области $\{a, b\}^n$, существенно отличающиеся от $\{0, 1\}$ и $\{-1, +1\}$.

Результаты

Лемма

$\mathrm{PTF}_{1,2}(2, \infty) = \mathrm{THR}$ *и* $\mathrm{PTF}_{1,2}(2, \mathit{poly}(n)) = \mathrm{MAJ}$.

Теорема

$$\mathrm{PTF}_{1,2}(\mathit{poly}(n)) = \mathrm{THR} \circ \mathrm{MAJ}$$

Заметим, что

$$\mathrm{PTF}_{0,1}(\mathrm{poly}(n)) = \mathrm{THR} \circ \mathrm{AND}$$

и

$$\mathrm{PTF}_{-1,1}(\mathrm{poly}(n)) = \mathrm{THR} \circ \mathrm{XOR}.$$

Как следствие, пороговые элементы над $\{1, 2\}$ строго сильнее

Побочный результат

Лемма

Всякая схема в $\mathrm{THR} \circ \mathrm{MAJ}$ *полиномиального размера эквивалентна схеме полиномиального размера того же вида, в которой все элементы на нижнем уровне монотонны*

То же самое верно для класса $\mathrm{MAJ} \circ \mathrm{MAJ}$

Нижние оценки

Пусть $x, y \in \{0,1\}^n$.
Функция скалярного произведения

$$IP(x,y) = \bigoplus_i x_i \wedge y_i.$$

Нижние оценки

Пусть $x, y \in \{0,1\}^n$.
Функция скалярного произведения

$$IP(x,y) = \bigoplus_i x_i \wedge y_i.$$

Теорема (повтор)

$$\mathrm{PTF}_{1,2}(poly(n)) = \mathrm{THR} \circ \mathrm{MAJ}$$

Следствие

$\mathrm{IP} \notin \mathrm{PTF}_{1,2}(poly(n))$, $\mathrm{AND} \circ \mathrm{OR} \circ \mathrm{AND}_2 \notin \mathrm{PTF}_{1,2}(poly(n))$.

То же самое верно для $\mathrm{PTF}_{1,2}(\infty)$

Ограниченная степень vs. неограниченная степень

- Верно ли $\mathrm{PTF}_{1,2}(\mathrm{poly}(n)) = \mathrm{PTF}_{1,2}(\infty)$?

Ограниченная степень vs. неограниченная степень

- Верно ли $\mathrm{PTF}_{1,2}(\mathrm{poly}(n)) = \mathrm{PTF}_{1,2}(\infty)$?
- Это открытый вопрос

Ограниченная степень vs. неограниченная степень

- Верно ли $\mathrm{PTF}_{1,2}(\mathrm{poly}(n)) = \mathrm{PTF}_{1,2}(\infty)$?
- Это открытый вопрос

Теорема

Если $\mathrm{THR} \circ \mathrm{THR} \not\subseteq \mathrm{THR} \circ \mathrm{MAJ} \circ \mathrm{AND}_2$ *то* $\mathrm{PTF}_{1,2}(\infty) \not\subseteq \mathrm{PTF}_{1,2}(\mathit{poly}(n))$.

Соотношения между областями определений

Лемма

Для всех a, b, таких что $a, b \neq 0$ и $|a| \neq |b|$, верно $\mathrm{PTF}_{a,b}(poly(n)) = \mathrm{PTF}_{1,2}(poly(n))$.

Лемма

Для всех a, b, таких что $a, b \neq 0$ и $|a| \neq |b|$, и для всех k верно $\mathrm{PTF}_{a,b}(\infty) = \mathrm{PTF}_{a^k,b^k}(\infty)$.

Как следствие,

$$\mathrm{PTF}_{1,2}(\infty) = \mathrm{PTF}_{1,-2}(\infty).$$

Макс-плюс пороговые функции

$$\max_{i=1,\ldots,l_1}(L_i(x)) \geqslant \max_{j=1,\ldots,l_2}(M_j(x)).$$

Назовем выражения такого вида *макс-плюс полиномиальной пороговой функцией*. Длиной назовем $l_1 + l_2$. Степенью назовем максимальную сумму абсолютных значений коэффициентов в линейных формах

По существу, макс-плюс полиномиальная пороговая функция — это просто неравенства в макс-плюс алгебре

Положим $\mathrm{mpPTF}(l(n), d(n))$ равным множеству булевых функций, вычислимых макс-плюс полиномиальными пороговыми функциями длины $l(n)$ и степени $d(n)$.

Макс-плюс PTF и AC0 ∘ THR

Лемма
$\mathsf{AND} \circ \mathsf{THR}, \mathsf{OR} \circ \mathsf{THR} \subseteq \mathsf{mpPTF}(\infty)$.

Лемма
$\mathsf{mpPTF}(\infty) \subseteq \mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}, \mathsf{OR} \circ \mathsf{AND} \circ \mathsf{THR}$.

Макс-плюс PTF и обычные PTF

Лемма

$\mathsf{mpPTF}(\mathit{poly}(n), \mathit{poly}(n)) \subseteq \mathsf{PTF}_{1,2}(\mathit{poly}(n), \mathit{poly}(n))$.

Следствие

Всякий макс-плюс PTF, вычисляющий IP_2*, имеет длину не меньше* $2^{\frac{n}{2}}$*. Всякий макс-плюс PTF, вычисляющий* $\mathrm{AND} \circ \mathrm{OR} \circ \mathrm{AND}_2$*, имеет длину* $2^{\Omega(n^{1/3})}$.

Макс-плюс PTF и обычные PTF

Лемма

$\mathrm{mpPTF}(poly(n), poly(n)) \subseteq \mathrm{PTF}_{1,2}(poly(n), poly(n))$.

Следствие

Всякий макс-плюс PTF, вычисляющий IP_2*, имеет длину не меньше* $2^{\frac{n}{2}}$*. Всякий макс-плюс PTF, вычисляющий* $\mathrm{AND} \circ \mathrm{OR} \circ \mathrm{AND}_2$*, имеет длину* $2^{\Omega(n^{1/3})}$.

Как следствие, $\mathrm{mpPTF}(\infty)$ является промежуточным классом в иерархии схем $\mathrm{AC0} \circ \mathrm{THR}$, для которого нам известны сильные нижние оценки

Макс-плюс PTF и обычные PTF

Лемма

$\mathrm{mpPTF}(poly(n), poly(n)) \subseteq \mathrm{PTF}_{1,2}(poly(n), poly(n))$.

Следствие

Всякий макс-плюс PTF, вычисляющий IP_2*, имеет длину не меньше* $2^{\frac{n}{2}}$*. Всякий макс-плюс PTF, вычисляющий* $\mathrm{AND} \circ \mathrm{OR} \circ \mathrm{AND}_2$*, имеет длину* $2^{\Omega(n^{1/3})}$.

Как следствие, $\mathrm{mpPTF}(\infty)$ является промежуточным классом в иерархии схем $\mathrm{AC0} \circ \mathrm{THR}$, для которого нам известны сильные нижние оценки

При этом класс является достаточно сильным
$\mathrm{OMB}(x) = 1$ тогда и только тогда, когда самая правая 1 в x находится на нечетной позиции

Лемма

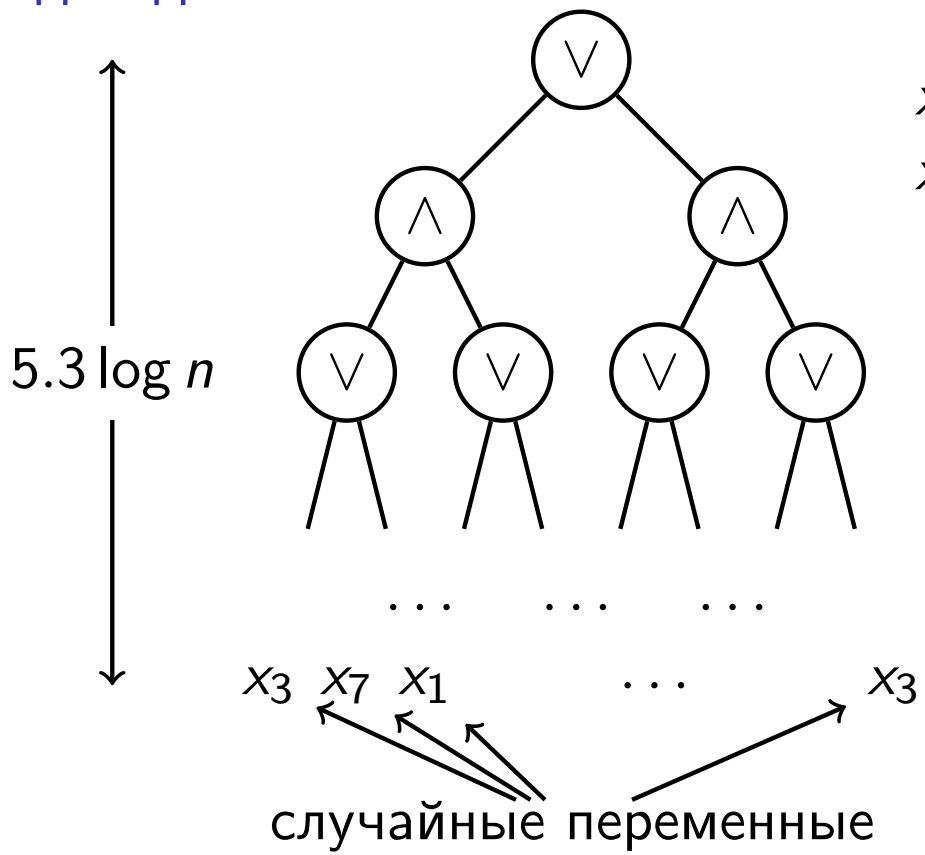
$\mathrm{PARITY} \in \mathrm{mpPTF}(poly(n))$, $\mathrm{OMB} \circ \mathrm{THR} \subseteq \mathrm{mpPTF}(\infty)$.

Конструкция Вэлианта

Теорема (Valiant'84)

Функцию голосованию можно вычислить монотонной формулой глубины $5.3 \log n$

Идея доказательства.



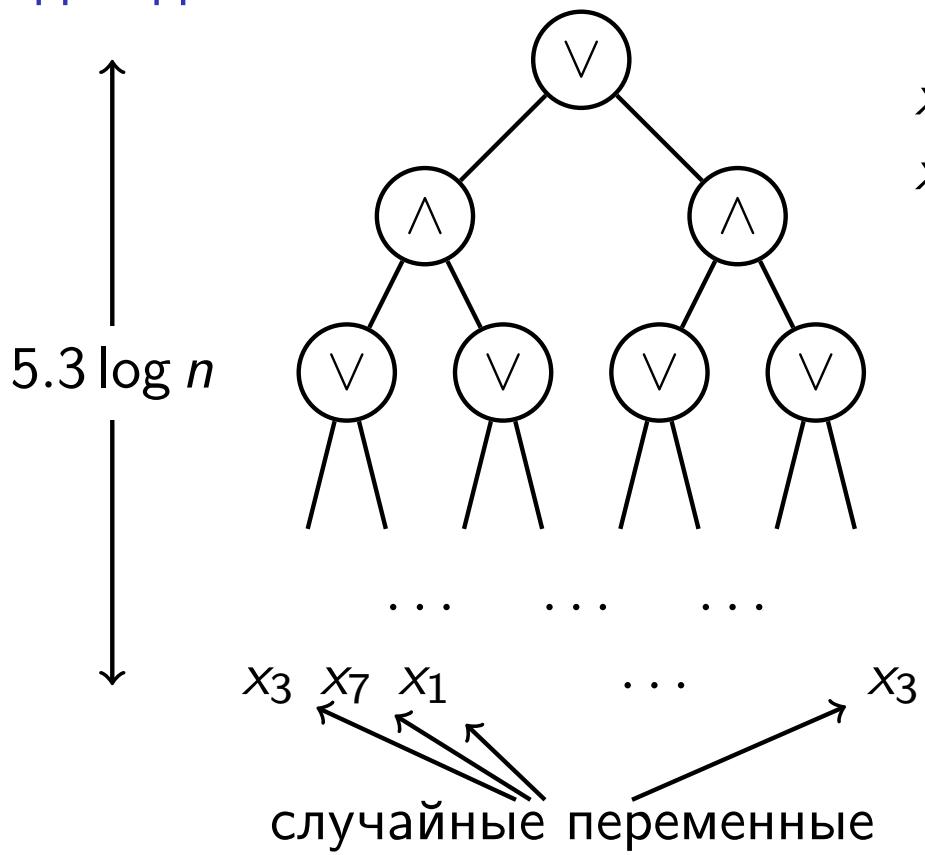
$$x \wedge y = 1 \iff x + y > 1$$
$$x \vee y = 1 \iff x + y > 0$$

Конструкция Вэлианта

Теорема (Valiant'84)

Функцию голосованию можно вычислить монотонной формулой глубины $5.3 \log n$

Идея доказательства.

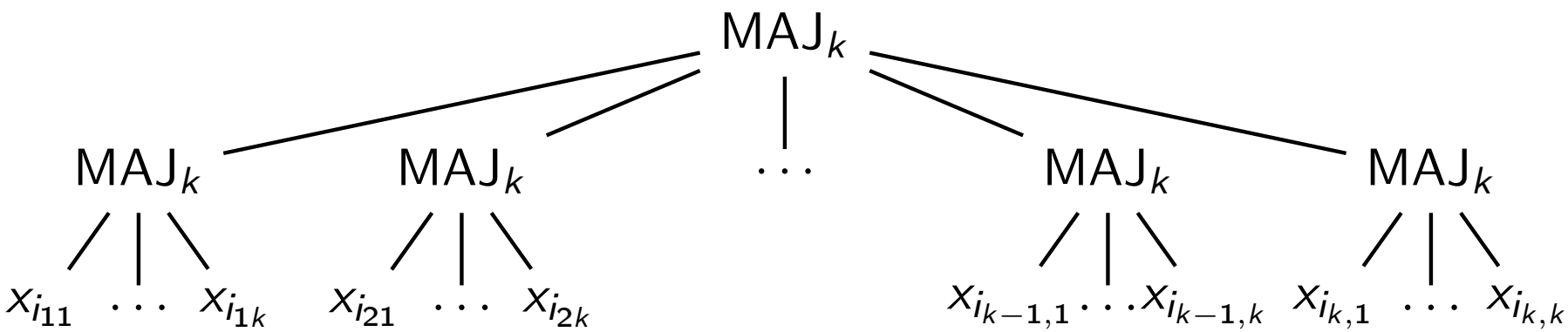


$$x \wedge y = 1 \iff x + y > 1$$
$$x \vee y = 1 \iff x + y > 0$$

Есть версия этой конструкции с элементами MAJ_3

Версия с небольшой глубиной

Вопрос. Мы хотим вычислить MAJ_n схемой постоянной глубины, состоящей из MAJ_k. Для каких k это возможно?



Результаты

Вопрос. Мы хотим вычислить MAJ_n схемой постоянной глубины, состоящей из MAJ_k. Для каких k это возможно?

Теорема

$k = O(n^{2/3})$ *для схем глубины 3*

Теорема

$k = \widetilde{\Omega}(n^{2/3+1/57}) = \widetilde{\Omega}(n^{13/19})$ *для схем глубины 2*

Теорема

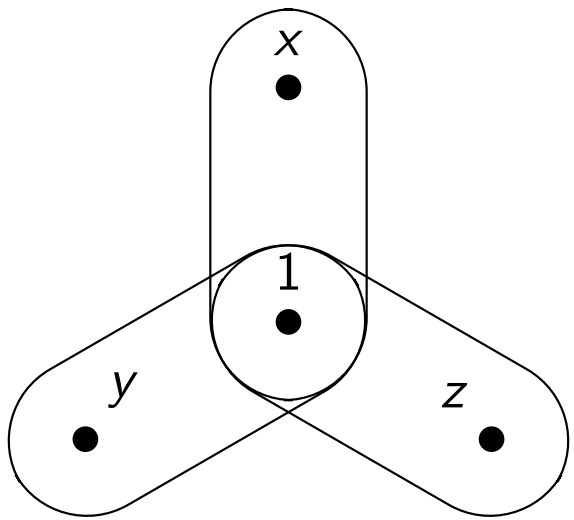
$k = \widetilde{\Omega}\left(n^{26/(13d+12)}\right)$ *для схем глубины* d

Гиперграфовые программы

Гиперграф $H = (V, E)$

Вершины помечены литералами и булевыми константами.

$H(\vec{x}) = 1$ тогда и только тогда, когда существует множество непересекающихся гиперребер, покрывающее все вершины, метки которых равны 0 на $\vec{x} \in \{0,1\}^n$.
Размер H равен $|V| + |E|$.



Гиперграфовые программы

Гиперграф $H = (V, E)$

Вершины помечены литералами и булевыми константами.

$H(\vec{x}) = 1$ тогда и только тогда, когда существует множество непересекающихся гиперребер, покрывающее все вершины, метки которых равны 0 на $\vec{x} \in \{0,1\}^n$.
Размер H равен $|V| + |E|$.

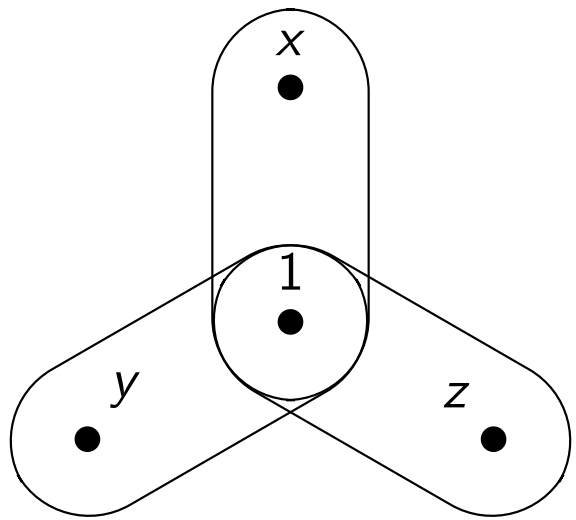


Рис.: $\mathrm{MAJ}(x, y, z)$

Гиперграфовые программы, разновидности

Два вида ограничений: максимальная степень и структура

Обозначим гиперграфовые программы степени d через HGP_d.

Древесные гиперграфовые программы: на вершинах гиперграфа задано дерево, все гиперребра — поддеревья. Обозначаем через HGP^{tree}

Линейные гиперграфовые программы HGP: на вершинах гиперграфа задан путь, все гиперребра — подпути. Обозначаем через HGP^{path}.

Гиперграфовые программы, сложность

Теорема

Следующие равенства верны как в монотонном, так и в общем случае:

1. $\mathsf{HGP} = \mathsf{HGP}_3 = \mathrm{NP}/\mathit{poly}$;
2. $\mathsf{HGP}_2 = \mathsf{coNL}/\mathit{poly}$;
3. $\mathsf{HGP}^{\mathit{path}} = \mathsf{NL}/\mathit{poly}$;
4. $\mathsf{HGP}^{\mathit{tree}} = \mathsf{SAC}^1$;
5. $\mathsf{HGP}_2^{\mathit{tree}} = \mathsf{HGP}_2^{\mathit{path}} = \mathsf{AC}^0_{3,\mathrm{AND}}$.

Следствия

Приложения к задачам в теории баз данных с онтологическим доступом

	глубина 1	глубина $d > 1$	произвольная глубина
линейные запросы	$\leqslant \mathsf{AC}^0_4$	NL/poly	NL/poly
древесные запросы	$\leqslant \mathsf{AC}^0_4$	SAC^1	$\mathrm{NP}/\mathrm{poly}^*$
произвольные запросы	NL/poly	$\mathrm{NP}/\mathrm{poly}$	$\mathrm{NP}/\mathrm{poly}^*$

Таблица: Классы функций, которые можно закодировать в запросах к базам данных с онтологическим доступом

$*$ — было известно ранее

Заключение 1/2

- Получены дважды экспоненциальные нижние оценки на веса полиномиальных пороговых элементов заданной степени, вычисляющих заданные булевы функции.
- Доказана экспоненциальная нижняя оценка сложности вычисления функции четности схемами постоянной глубины, содержащими логарифмическое число пороговых элементов.
- Построена иерархия точных пороговых схем и доказано, что она тесно переплетается с иерархией пороговых схем. Доказаны разделения некоторых классов в нижних уровнях этих иерархий.
- Исследованы вопросы реализации булевых функций многочленами над переменными, принимающими значения $\{a, b\}$ для произвольной пары чисел a и b. Установлены связи этой модели с пороговыми схемами.

Заключение 2/2

- Исследованы монотонные булевы схемы постоянной глубины d, состоящие из функций MAJ_k и вычисляющие функцию MAJ_n. Доказаны верхние и нижние оценки на минимальное значение k, для которого такие схемы глубины d существуют.
- В связи с приложениями к исследованиям размера преобразований запросов к базам данных с онтологическим доступом исследована сложность булевых функций в модели гиперграфовых программ. Для различных классов таких программ установлена их выразительная способность в терминах известных сложностных классов.
- В доклад не вошли результаты о макс-плюс полукольце и многочленах над ним