Схемы для функции голосования и других пороговых функций

А. Козачинский[1] В. Подольский[2]

[1]University of Warwick, Coventry, UK

[2]Steklov Mathematical Institute, Moscow, Russia

Научно-исследовательский семинар по математической логике, 17 марта 2021

Введение

Рассматриваются схемы из функциональных элементов над различными базисами булевых функций (например, $\{\wedge_2, \vee_2, \neg\}$ или $\{\wedge_2, \vee_2\}$).

Размер схемы – количество элементов в ней.

Глубина схемы – максимальное d, для которого в схеме найдется d последовательно подключенных друг к другу элементов.

Известный факт

Схемами в базисе $\{\wedge_2, \vee_2, \neg\}$ можно вычислить все булевы функции.
Схемами в базисе $\{\wedge_2, \vee_2\}$ можно вычислить все монотонные булевы функции, и только их.

Глобальная проблема схемной сложности

Доказать, что некоторая явная булева функция не может быть вычислена схемой полиномиального размера в базисе $\{\wedge_2, \vee_2, \neg\}$.

- последовательность $\{f_n\}_{n\in\mathbb{N}}$, где $f_n\colon \{0,1\}^n \to \{0,1\}$;
- явная: язык $\{x \in \{0,1\}^* \mid f_{|x|}(x) = 1\}$ принадлежит классу сложности C (например, NP, PSPACE);
- что от нас хотят: не существует последовательности схем $\{D_n\}_{n\in\mathbb{N}}$ в базисе $\{\wedge_2, \vee_2, \neg\}$ такой, что (a) D_n вычисляет f_n при любом n и (b) размер D_n есть $n^{O(1)}$ при $n \to \infty$.
- если получится это доказать $\Longrightarrow$ P $\neq$ C.

Мотивирующий вопрос

Вопрос: Пусть мы вычислили **монотонную** булеву функцию f схемой полиномиального размера в базисе $\{\wedge_2, \vee_2, \neg\}$. Можно ли f вычислить схемой полиномиального размера в базисе $\{\wedge_2, \vee_2\}$?

- Разборов (1985): монотонная функция из NP такая, для которой в базисе $\{\wedge_2, \vee_2\}$ нет схемы полиномиального размера;
- если бы в базисе $\{\wedge_2, \vee_2, \neg\} \implies$ P$\neq$ NP.
- Ответ на Вопрос положительный $\implies$ P$\neq$ NP.
- Разборов (1985): на самом деле ответ на Вопрос отрицательный.

Основной результат

Функция $f\colon \{0,1\}^n \to \{0,1\}$ называется самодвойственной, если $f(x_1,\ldots,x_n) = \neg f(\neg x_1,\ldots,\neg x_n)$ при всех $x_1 \ldots x_n \in \{0,1\}$. Пример: $\mathrm{MAJ}_3(x,y,z) = xy \vee xz \vee yz$.

Известный факт

Схемами в базисе $\{\mathrm{MAJ}_3, \neg\}$ можно вычислить все самодвойственные булевы функции, и только их.

Theorem (К., Подольский 2020)

Пусть самодвойственную булеву функцию f от n переменных можно вычислить схемой размера s и глубины d в базисе $\{\wedge_2, \vee_2, \neg\}$. Тогда f можно вычислить схемой в базисе $\{\mathrm{MAJ}_3, \neg\}$ размера $n^{O(1)} \cdot s$ и глубины $d + O(\log n)$.

Для самодвойственных функций: нет схемы полиномиального размера в базисе $\{\mathrm{MAJ}_3, \neg\}$ $\Longrightarrow$ нет схемы полиномиального размера в базисе $\{\wedge_2, \vee_2, \neg\}$.

Монотонно-самодвойственный вариант

Известный факт

Схемами в базисе $\{\mathrm{MAJ}_3\}$ можно вычислить все монотонные самодвойственные булевы функции, и только их.

Theorem (К., Подольский 2020)

Пусть монотонную самодвойственную булеву функцию f от n переменных можно вычислить схемой размера s и глубины d в базисе $\{\wedge_2, \vee_2\}$. Тогда f можно вычислить схемой в базисе $\{\mathrm{MAJ}_3\}$ размера $n^{O(1)} \cdot s$ и глубины $d + O(\log n)$.

Эффективный вариант

Theorem (К., Подольский 2020)

Существует полиномиальный алгоритм со следующим свойством. Получив на вход схему от n переменных в базисе $\{\wedge_2, \vee_2, \neg\}$ размера s и глубины d, вычисляющую самодвойственную функцию, алгоритм выдает схему в базисе $\{\mathrm{MAJ}_3, \neg\}$ размера $n^{O(1)} \cdot s$ и глубины $d + O(\log n)$, вычисляющую ту же функцию.

Theorem (К., Подольский 2020)

Существует полиномиальный алгоритм со следующим свойством. Получив на вход схему от n переменных в базисе $\{\wedge_2, \vee_2\}$ размера s и глубины d, вычисляющую монотонную самодвойственную функцию, алгоритм выдает схему в базисе $\{\mathrm{MAJ}_3\}$ размера $n^{O(1)} \cdot s$ и глубины $d + O(\log n)$, вычисляющую ту же функцию.

Основное применение

При нечетном n через MAJ_n обозначим функцию голосования от n переменных.

Theorem (К., Подольский 2020)

При нечетном n существует схема в базисе $\{\mathrm{MAJ}_3\}$ глубины $O(\log n)$, вычисляющая MAJ_n. Более того, существует полиномиальный алгоритм, выдающий такую схему по n в унарной записи.

- Вэлиент 1984: доказано существование.
- Кохэн и др. 2013: существование + алгоритм, но схема совпадает с MAJ_n только для входов с долей единиц, отличающейся от $1/2$ хотя бы на $\exp\{-\sqrt{\ln(n)}\}$.
- Кохэн и др. 2013: ПСГ $\Longrightarrow$ существование + алгоритм.
- Кохэн и др. 2013: применения для протоколов конфиденциального вычисления.

Как получить применение

Theorem (Айтай, Комлос, Семереди 1983)

Существует полиномиальный алгоритм, который по нечетному n в унарной записи выдает схему в базисе $\{\wedge_2, \vee_2\}$ глубины $O(\log n)$ для MAJ_n.

Theorem (К., Подольский 2020)

Существует полиномиальный алгоритм со следующим свойством. Получив на вход схему от n переменных в базисе $\{\wedge_2, \vee_2\}$ размера s и глубины d, вычисляющую монотонную самодвойственную функцию, алгоритм выдает схему в базисе $\{\mathrm{MAJ}_3\}$ размера $n^{O(1)} \cdot s$ и глубины $d + O(\log n)$, вычисляющую ту же функцию.

Использование для нижних оценок?

Открытый вопрос: доказать, что любая формула для функции MAJ_n в базисе $\{\wedge, \vee\}$ имеет размер $\Omega(n^{2.001})$. Формула – это схема, где каждый элемент подключен максимум к одному другому элементу.

Theorem (K., Подольский 2020)

Пусть монотонную самодвойственную булеву функцию f от n переменных можно вычислить схемой размера s в базисе $\{\wedge_2, \vee_2\}$. Тогда f можно вычислить схемой в базисе $\{\mathrm{MAJ}_3\}$ размера $n^{\log_2(3)} \cdot s$.

Достаточно доказать, что любая формула для функции MAJ_n в базисе $\{\mathrm{MAJ}_3\}$ имеет размер $\Omega(n^{2.001+\log_2(3)})$.

Известно, что MAJ_n в базисе $\{\mathrm{MAJ}_3\}$ можно вычислить формулой размера $O(n^{2.71+\log_2(3)})$.

Другие пороговые функции

$$\mathrm{THR}_t^n : \{0,1\}^n \to \{0,1\}, \qquad \mathrm{THR}_t^n(x) = 1 \iff x_1 + \ldots + x_n \geq t.$$

Для фиксированного $k \geq 2$ интересуют вычисление $\mathrm{THR}_{m+1}^{km+1}$ схемами в базисе $\{\mathrm{THR}_2^{k+1}\}$. При $k = 2$ получаем MAJ_{2m+1} и MAJ_3.

Theorem (К., Подольский 2020)

Для любого k существует полиномиальный алгоритм, выдающий по m в унарной записи схему размера $m^{O(1)}$ и глубины $O(\log^2 m)$ в базисе $\{\mathrm{THR}_2^{k+1}\}$ для функции $\mathrm{THR}_{m+1}^{km+1}$.

- Кохэн и др. 2013: глубина $O(\log m)$, но зато совпадает с $\mathrm{THR}_{m+1}^{km+1}$ только на входах, в которых доля единиц отличается от $1/k$ хотя бы на $1/\sqrt{m}$.
- Кохэн и др. 2013: при $k = 3$ применения для протоколов конфиденциального вычисления.

Техника

Раньше:

- Хорошая схема в более выразительном базисе (Айтай, Комлос, Семереди).
- Теорема о переходе от схем в более выразительном базисе к схемам в менее выразительном базисе.

Теперь нужна коммуникационная сложность.

- Хороший протокол для некоторой коммуникационной задачи.
- Теорема о переходе от протокола к схеме.

Коммуникационная задача в частном случае

Есть k множеств $X_1, X_2, \ldots, X_k \subseteq \{1, 2, \ldots, km+1\}$, каждое размера m. За один шаг можно для некоторого i (по вашему выбору) спросить любой вопрос про X_i с ответом ДА/НЕТ. Надо найти какой-нибудь элемент из

$$\{1, 2, \ldots, km+1\} \setminus (X_1 \cup X_2 \cup \ldots \cup X_k).$$

Theorem

Коммуникационную задачу можно решить за $O(\log^2 m)$ вопросов.

Theorem

Если коммуникационную задачу можно решить за d вопросов, то функцию $\mathrm{THR}_{m+1}^{km+1}$ можно вычислить схемой глубины $O(d)$ в базисе $\{\mathrm{THR}_2^{k+1}\}$.

При $k = 2$ существование решения за d вопросов равносильно существованию схемы глубины d в базисе $\{\wedge_2, \vee_2\}$, вычисляющей MAJ_{2m+1} (Карчмер, Вигдерсон 1990).

Открытый вопрос: при каком-нибудь $k \geq 3$ решить коммуникационную задачу быстрее, чем за $O(\log^2 m)$ вопросов.

Открытый вопрос: при каком-нибудь $k \geq 3$ решить быстрее более простую коммуникационную задачу, в которой можно выдать также любой элемент $X_1 \cap X_2 \cap \ldots \cap X_k$. Мы научились бы вычислять $\mathrm{THR}_{m+1}^{km+1}$ с меньшей глубиной в базисе $\{\mathrm{THR}_2^{k+1}, \neg\}$ (причем $\neg$ применяется только к переменным).

Обобщение

Через Q_k обозначим множество всех булевых функций, у которых любые k нулевых входов имеют общую нулевую координату. Например, $\mathrm{THR}_{m+1}^{km+1} \in Q_k$.

Функция f принадлежит $Q_k \iff$ есть схема в базисе THR_2^{k+1}, обращающаяся в нуль на всех нулевых входах f.

Коммуникационная задача для $f \in Q_k$: есть k нулевых входов f, за один шаг про какой-нибудь из этих k входов можно спросить любой вопрос с ответом ДА/НЕТ. Найти какую-нибудь общую нулевую координату для этих k входов.

Theorem (К., Подольский 2020)

Для любого k и любой $f \in Q_K$ следующие две величины отличаются не более чем $O_k(1)$ раз: (a) минимальное количество вопросов, требуемое для решения коммуникационной задачи для f; (b) минимальная глубина схемы в базисе $\{\mathrm{THR}_2^{k+1}, \neg\}$, обращающаяся в ноль на нулях f.

Спасибо за внимание!