Вычислительно трудные задачи и дерандомизация
Лекция 2: Нижние оценки для схем ограниченной глубины

Дмитрий Ицыксон

ПОМИ РАН

22 февраля 2009

Постановка задачи

- Рассматриваем схемы из $\bigvee, \bigwedge$ (с неограниченной входящей степенью) и $\neg$.
- Глубина схемы — это длина максимального пути от входа схемы к выходу схемы
- Основная модель вычислений: схемы, глубина которых ограничена константой.
- $\mathit{Parity}(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n = \sum_{i=1}^{n} x_i \bmod 2$.
- Теорема. Функция *Parity* не вычисляется полиномиального размера схемой константной глубины.

Преобразование схемы

- Преобразовать граф схемы в дерево: размер схемы увеличится в полиномиальное число раз, глубина не поменяется.
- Пронести все отрицания к переменным, пользуясь правилами де Моргана: $\neg \bigvee x_i = \bigwedge \neg x_i$ и $\neg \bigwedge x_i = \bigvee \neg x_i$.
- Если гейт $\bigvee$ является входом для гейта $\bigvee$, то их можно объединить в один гейт. Аналогично для $\bigwedge$.
- Разбить гейты на уровни так, чтобы на каждом уровне были бы только гейты одного типа, и $\bigvee$ и $\bigwedge$ уровни чередовались бы.

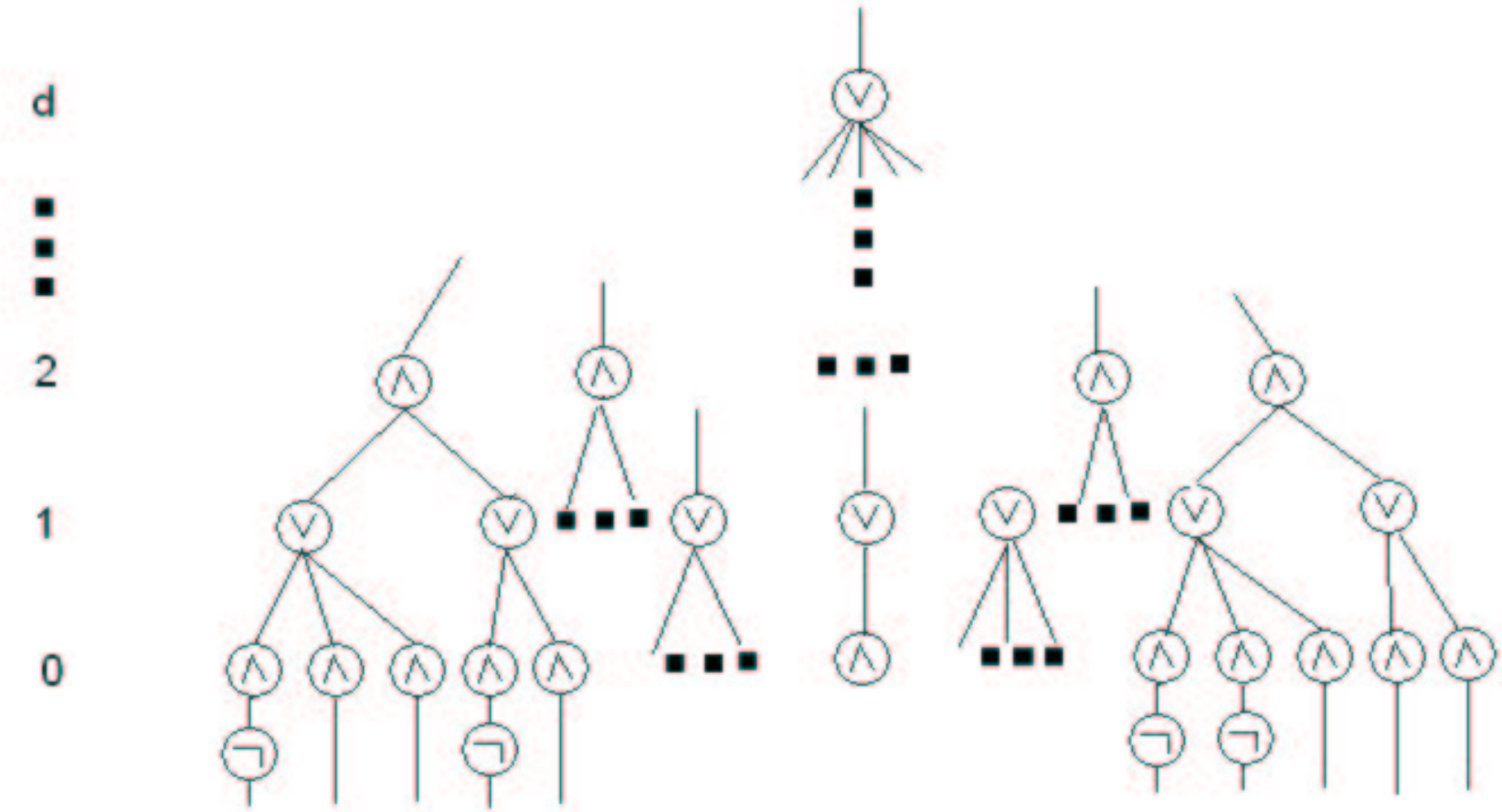
Разбиение схемы на уровни

- 0-й уровень: Входные переменные и их отрицания
- 1-й уровень: Все $\bigvee$ от нулевого уровня. Фиктивные $\bigvee$ для того, чтобы поднять входы повыше.
- 2-й уровень: $\bigwedge$ от первого уровня.

...

Добавим между нулевым и первым уровнем фиктивные $\bigwedge$ для всех переменных, используемых на первом уровне.

Схема



Напоминание

- Литерал — это переменная или ее отрицание
- Дизъюнкт — это дизъюнкция нескольких литералов $\bigvee l_i$.
- Конъюнкт — это конъюнкция нескольких литералов $\bigwedge l_i$.
- Формула в k-ДНФ: $\bigvee_j C_j$, где C_j — это конъюнкт из k литералов.
- Формула в k-КНФ $\bigwedge_j D_j$, где D_j — это дизъюнкт из k литералов.

Ключевая лемма

Лемма. (Switching lemma) Пусть функция f выразима как k-ДНФ формула, пусть подстановка ρ назначает случайное значение случайно выбранным $t > \frac{n}{2}$ переменным. Тогда для каждого $s \geq 2$ выполняется

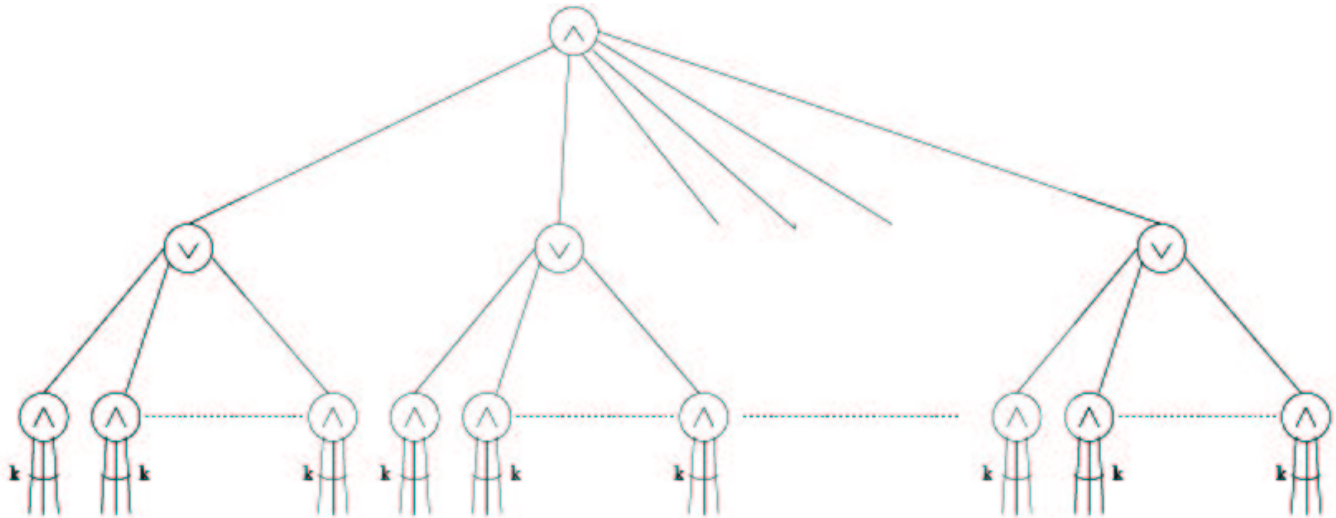
$$\Pr_{\rho}[f|_{\rho} \text{ не выразима в виде } s\text{-КНФ}] \leq \left(100k\frac{(n-t)}{n}\right)^{s}$$

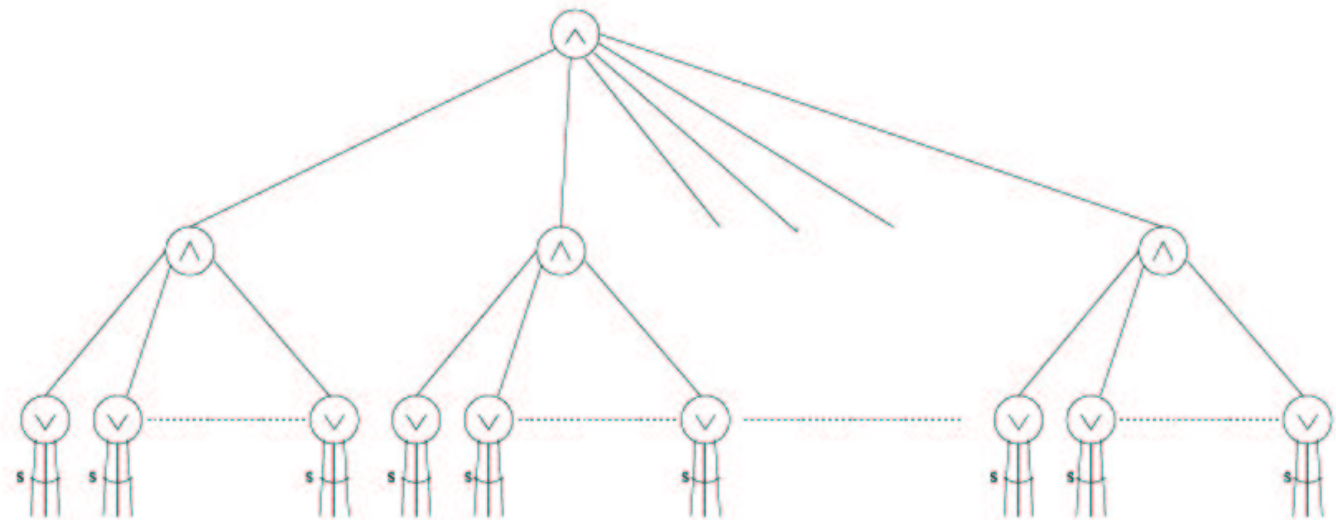
Следствие. КНФ и ДНФ можно поменять местами.

Почему из леммы все следует?

- n входов, n^b гейтов, глубина d.
- $n_i = n^{1/2^i}$, $k_i = b2^{i+2}$
- Перед i-м шагом: глубина $d - i + 1$, переменных n_{i-1}, гейты первого уровня в k_i-ДНФ (или k_i-КНФ).
- i-й шаг: случайно подставить $n_i - n_{i+1}$ входов.
- Функция в гейте первого уровня не в k_{i+1}-КНФ (или k_{i+1}-ДНФ) с вероятностью $\leq \left(100k_i \frac{n_{i+1}}{n_i}\right)^{k_{i+1}} = \left(\frac{100k_i}{n^{1/2^{i+1}}}\right)^{k_{i+1}} < \left(\frac{1}{n^{1/2^{i+2}}}\right)^{b2^{i+3}} = \frac{1}{n^{2b}} < \frac{1}{10n^b}$.
- С вероятностью $1 - \frac{1}{10}$ все гейты первого уровня можно “развернуть” (и уменьшить глубину на 1).
- После d шагов: константа, n_d переменных. Это точно не *Parity*.

Картинки





Минтермы и макстермы

- f — булева функция
- Минтерм — это минимальный по включению набор литералов, что если назначить им значение 1, то значение f автоматически будет 1.
- Макстерм — это минимальный по включению набор литералов, что если назначить им значение 1, то значение f автоматически будет 0.
- Конъюнкт в ДНФ содержит минтерм.
- Отрицание дизъюнкта в КНФ содержит макстерм.
- Если f не выражается в виде s-КНФ, то f содержит макстерм размера хотя бы $s + 1$.

Идея доказательства switching леммы

- ρ — плохая подстановка, если $f|_\rho$ не выразимо в s-КНФ.
- Число подстановок размера t: $C_n^t 2^t$.
- Число подстановок размера $t+s$: $C_n^{t+s} 2^{t+s}$.
- При $t > \frac{3}{4}n$:

$$\frac{C_n^{t+s}}{C_n^t} = \frac{t!(n-t)!}{(t+s)!(n-t-s)!} = \frac{(n-t)\dots(n-t-s+1)}{(t+s)\dots(t+1)} < \left(\frac{n-t}{t}\right)^s << 2^{-s}$$

- Идея: сопоставить каждой плохой подстановке t переменных подстановку $t+s$ переменных.

Доказательство

- f выразима в k-ДНФ, ρ — плохая подстановка.
- Зафиксируем порядок переменных.
- $t_1, t_2, \ldots,$ — это все минтермы f (в алфавитном порядке).
- Пусть π — это макстерм $f|_\rho$ размера $p > s$.
- Пусть t_{l_1} — первый минтерм, который опровергнут $\rho\pi$, но не опровергнут ρ.
- π_1 — часть π, которая соответствует переменным t_{l_1}.
- σ_1 — подстановка переменным π_1, которая согласуется с t_{l_1}.

Доказательство

- f выразима в k-ДНФ, ρ — плохая подстановка.
- Зафиксируем порядок переменных.
- $t_1, t_2, \ldots,$ — это все минтермы f (в алфавитном порядке).
- Пусть π — это макстерм $f|_\rho$ размера $p > s$.
- Пусть t_{l_i} — первый минтерм, который опровергнут $\rho\pi$, но не опровергнут $\rho\pi_1 \ldots \pi_{i-1}$
- π_i — часть $\pi \setminus \{\pi_1 \cup \cdots \cup \pi_{i-1}\}$, которая соответствует переменным t_{l_i}.
- σ_i — подстановка переменным π_i, которая согласуется с t_{l_i}.
- Закончить, когда $\pi_1\pi_2 \ldots \pi_m = \pi$.

Доказательство (продолжение)

- Пытаемся по $\rho\sigma_1 \dots \sigma_m$ восстановить ρ.
- t_{l_1} — это первый минтерм f, который согласуется с подстановкой $\rho\sigma_1 \dots \sigma_m$.
- z и c — две строчки с дополнительной информацией.
- t_{l_1} содержит $l \leq k$ литералов. Первые l битов строчки c говорят, какие литералы назначены подстановкой σ_1 (π_1).
- В строке z записано, какие биты отличаются в σ_1 и π_1.
- Восстанавливаем π_1.
- t_{l_2} — это первый минтерм f, который согласуется с подстановкой $\rho\pi_1\sigma_2 \dots \sigma_m$. И т.д.
- $z \in \{0,1\}^p$, c — это строка из $\leq kp$ бит, в которой p единиц (дополним нулями до строки из kp бит).

Подсчет

- Число различных c не превосходит $C_{kp}^{p} < \frac{(kp)^p}{p!} < \frac{(kp)^p}{(p/e)^p} = (ke)^p$.
- Число различных z не превосходит 2^p.
- Доля плохих подстановок:

$$\frac{C_n^{t+p} 2^{t+p} 2^p (ke)^p}{C_n^t 2^t} \leq (4ek\frac{n-t}{t})^p$$

$$\leq (8ek\frac{n-t}{n})^p \leq (100k\frac{n-t}{n})^p$$