Сложность пропозициональных доказательств

Эдуард Алексеевич Гирш

http://logic.pdmi.ras.ru/~hirsch

ПОМИ РАН

21 октября 2010 г.

Cutting Plane: нижняя оценка

- Монотонная интерполяция.

- Экспоненциальная нижняя оценка на интерполянт.

Cutting Plane: нижняя оценка

- Монотонная интерполяция.

Теорема (Пудлак)

Пусть в $A(\vec{x},\vec{y}) \supset B(\vec{x},\vec{z})$ все вхождения x_i в A и в B положительны. Тогда из док-ва в Res (или CP) получается монотонный интерполянт — булева (или арифметическая) $C(\vec{x})$ полиномиального размера.

- Экспоненциальная нижняя оценка на интерполянт.

Cutting Plane: нижняя оценка

- Монотонная интерполяция.

Теорема (Пудлак)

Пусть в $A(\vec{x},\vec{y}) \supset B(\vec{x},\vec{z})$ все вхождения x_i в A и в B положительны. Тогда из док-ва в Res (или CP) получается монотонный интерполянт — булева (или арифметическая) $C(\vec{x})$ полиномиального размера.

- Экспоненциальная нижняя оценка на интерполянт.

Теорема (Разборов; Алон-Боппана; Пудлак)

Для булевых (или арифметических) схем,
разделяющих n–клики и $(n-1)$–раскрашиваемые графы,
$|C| = 2^{\Omega(\sqrt{n})}$ при $n = \lfloor \frac{1}{8}(m/\log m)^{2/3} \rfloor$.

Нижние оценки, основанные на ширине

Схема доказательства:

- Линейная нижняя оценка на какой-то параметр (ширину).
- Лемма: в коротком док-ве π можно понизить ширину до $\sim \ln |\pi|$.

Нижние оценки, основанные на ширине

Схема доказательства:

- Линейная нижняя оценка на какой-то параметр (ширину).
- Лемма: в коротком док-ве π можно понизить ширину до $\sim \ln |\pi|$.

Резолюция:

- Ширина дизъюнкции $W(l_1 \vee \ldots \vee l_k)$ — количество переменных.

Нижние оценки, основанные на ширине

Схема доказательства:

- Линейная нижняя оценка на какой-то параметр (ширину).
- Лемма: в коротком док-ве π можно понизить ширину до $\sim \ln|\pi|$.

Резолюция:

- Ширина дизъюнкции $W(l_1 \vee \ldots \vee l_k)$ — количество переменных.
- Ширина формулы/вывода — ширина самой широкой дизъюнкции.
- $G \vdash_w H$: есть вывод ширины $\leq w$.
- $W_\vdash(F)$ — минимально возможная ширина док-ва.
- $S_\vdash(F)$ — минимально возможное кол-во дизъюнкций док-ва.

Нижние оценки, основанные на ширине

Схема доказательства:

- Линейная нижняя оценка на какой-то параметр (ширину).
- Лемма: в коротком док-ве π можно понизить ширину до $\sim \ln |\pi|$.

Резолюция:

- Ширина дизъюнкции $W(l_1 \vee \ldots \vee l_k)$ — количество переменных.
- Ширина формулы/вывода — ширина самой широкой дизъюнкции.
- $G \vdash_w H$: есть вывод ширины $\leq w$.
- $W_\vdash(F)$ — минимально возможная ширина док-ва.
- $S_\vdash(F)$ — минимально возможное кол-во дизъюнкций док-ва.
- **Лемма (для формулы F от n переменных)**

  $W_\vdash(F) \leq W(F) + O(\sqrt{n \ln S_\vdash(F)})$

Нижние оценки, основанные на ширине

Схема доказательства:

- Линейная нижняя оценка на какой-то параметр (ширину).
- Лемма: в коротком док-ве π можно понизить ширину до $\sim \ln|\pi|$.

Резолюция:

- Ширина дизъюнкции $W(l_1 \vee \ldots \vee l_k)$ — количество переменных.
- Ширина формулы/вывода — ширина самой широкой дизъюнкции.
- $G \vdash_w H$: есть вывод ширины $\leq w$.
- $W_{\vdash}(F)$ — минимально возможная ширина док-ва.
- $S_{\vdash}(F)$ — минимально возможное кол-во дизъюнкций док-ва.
- **Лемма (для формулы F от n переменных)**

  $$W_{\vdash}(F) \leq W(F) + O(\sqrt{n \ln S_{\vdash}(F)})$$

  Лемма (к лемме)

- 1. $F|_{x=0} \vdash_w C \implies F \vdash_{w+1} C \vee x$.

  2. $W_{\vdash}(F|_{x=0}) \leq w{-}1,\ W_{\vdash}(F|_{x=1}) \leq w \implies$

  $$\implies W_{\vdash}(F) \leq \max\{w, W(\{C \in F | \neg x \in C\})\}.$$

Нижние оценки, основанные на ширине

Схема доказательства:

- Линейная нижняя оценка на какой-то параметр (ширину).
- Лемма: в коротком док-ве π можно понизить ширину до $\sim \ln|\pi|$.

Резолюция:

- Ширина дизъюнкции $W(l_1 \vee \ldots \vee l_k)$ — количество переменных.
- Ширина формулы/вывода — ширина самой широкой дизъюнкции.
- $G \vdash_w H$: есть вывод ширины $\leq w$.
- $W_\vdash(F)$ — минимально возможная ширина док-ва.
- $S_\vdash(F)$ — минимально возможное кол-во дизъюнкций док-ва.
- **Лемма (для формулы F от n переменных)**

  $W_\vdash(F) \leq W(F) + O(\sqrt{n \ln S_\vdash(F)})$

Лемма (к лемме)

- 1. $F|_{x=1} \vdash_w C \implies F \vdash_{w+1} C \vee \neg x$.

  2. $W_\vdash(F|_{x=1}) \leq w-1,\ W_\vdash(F|_{x=0}) \leq w \implies$

  $\implies W_\vdash(F) \leq \max\{w, W(\{C \in F| \ x \in C\})\}$.

Цейтинские формулы

- $G = (V, E)$ — граф.
- Переменная $x_e \in \{0, 1\}$ для каждого $e \in E$.
- Условие $\bigoplus\limits_{e \ni v} x_e = 1$.

- $|V| \not\vdots\, 2$.

Цейтинские формулы

- $G = (V, E)$ — граф.
- Переменная $x_e \in \{0, 1\}$ для каждого $e \in E$.
- Условие $\bigoplus\limits_{e \ni v} x_e = c_v$.
- Константа $c_v \in \{0, 1\}$ для каждой $v \in V$.
- $\bigoplus\limits_{v \in V} c_v = 1$.

Цейтинские формулы

- $G = (V, E)$ — граф.
- Переменная $x_e \in \{0, 1\}$ для каждого $e \in E$.
- Условие $\bigoplus_{e \ni v} x_e = c_v$.
- Константа $c_v \in \{0, 1\}$ для каждой $v \in V$.
- $\bigoplus_{v \in V} c_v = 1$.

Определение

Расширительная способность
$$e(G) = \min\left\{|\mathrm{cut}(V', V \setminus V')| \;\middle|\; V' \subseteq V,\ \tfrac{1}{3}|V| \le |V'| \le \tfrac{2}{3}|V|\right\}.$$
G — расширитель, если $e(G) = \Omega(|V|)$.

Факт

Существуют связные регулярные расширители степени 3.

- В выводе есть дизъюнкция C, следующая в точности из уравнений

$$\bigwedge_{v \in U} \left(\bigoplus_{e \ni v} x_e = c_v \right), \tag{1}$$

где $|U| \in \left[\frac{1}{3}|V| .. \frac{2}{3}|V|\right]$.

- В выводе есть дизъюнкция C, следующая в точности из уравнений
$$\bigwedge_{v \in U} \left(\bigoplus_{e \ni v} x_e = c_v \right), \tag{1}$$
где $|U| \in \left[\frac{1}{3}|V| \,..\, \frac{2}{3}|V|\right]$.
- Каждая переменная из сечения $(U, V \setminus U)$ меняет истинность (1) для какого-то набора…

- В выводе есть дизъюнкция C, следующая в точности из уравнений
$$\bigwedge_{v \in U} \left(\bigoplus_{e \ni v} x_e = c_v \right), \tag{1}$$
где $|U| \in \left[\frac{1}{3}|V| \,..\, \frac{2}{3}|V|\right]$.
- Каждая переменная из сечения $(U, V \setminus U)$ меняет истинность (1) для какого-то набора...
- ...и должна входить в C.