Монотонная интерполяция для задачи BPHP

Пётр Смирнов, Академический Университет

Научный руководитель: Д. О. Соколов

21 июля 2017 года

Пропозициональные доказательства

- *Система доказательств* для языка L — полиномиальный алгоритм *V(x, w)* такой, что:
  - $V(x, w) = 1 \Rightarrow x \in L$ *(корректность)*
  - $\forall x \in L\ \exists w: V(x, w) = 1$ *(полнота)*
- Система доказательств *полиномиально ограничена*, если для любого x из *L* существует «*короткое*» доказательство, то есть

  $$\forall x \in L\ \exists w: V(x, w) = 1, |w| < p(|x|)$$

  для некоторого фиксированного многочлена p

[Cook, Reckhow, 1979]

Системы доказательств для UNSAT

- Таблица истинности
- Дерево решений
- Резолюционная
- …

Правило резолюции:

$$\frac{x \vee a_1 \vee \ldots \vee a_n, \quad \neg x \vee b_1 \vee \ldots \vee b_m}{a_1 \vee \ldots \vee a_n \vee b_1 \vee \ldots \vee b_m}$$

Мотивация изучения

- «Лог» алгоритма, решающего SAT — доказательство невыполнимости формулы
- Алгоритмы расщепления (DPLL) эквивалентны древовидным резолюционным доказательствам
- Существование полиномиальной системы доказательств для UNSAT равносильно вопросу NP = coNP
- Программа Кука: для всё более сильных систем доказательств доказывать нижние оценки

Semantic Cutting Planes

- $\varphi(x_1, x_2, \ldots, x_n) = C_1 \wedge C_2 \wedge \ldots \wedge C_m$
- Опровержение в SCP — L_1, L_2, …, L_l — линейные неравенства с вещественными коэффициентами:
  - L_i равносильно $C_i = 1$ для $i = 1…m$
  - L_l: *“0 > 1”*
  - Каждое L_i для $i > m$ семантически следует из каких-то двух предыдущих L_j и L_k $(j, k < i)$,
    то есть для всех x из $L_j(x) \wedge L_k(x)$ следует $L_i(x)$

Монотонные вещественные схемы

- В каждой вершине вычисляется своя монотонная функция $f(x, y)$: $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$
- Лемма Юкны [Jukna, 2012]
  - Дана монотонная булева функция *f*, множество $U \subseteq f^{-1}(1)$, $V \subseteq f^{-1}(0)$
  - Тогда лемма даёт оценку снизу на размер любой монотонной вещественной схемы, правильно вычисляющей *f* на *U* и *V*

CSP-SAT

- $\varphi(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m)$ — невыполнимая формула в КНФ
- Отношение Search_φ:
  - *(x, y, i)* лежит в отношении, если подстановка *(x, y)* опровергает дизъюнкт с номером *i*
- Задача CSP-SAT $_{\text{Search}_\varphi}$
- Можно построить множества *U* и *V* принимаемых и отвергаемых входов для CSP-SAT, обладающих свойством:
  - Если опровержение в Semantic Cutting Planes имеет размер *s*, то существует вещественная монотонная схема для *U* и *V* полиномиального от *s* размера [Hrubes, Pudlak, 2016]
- [Fleming, Pankratov, Pitassi, Robere, 2017] — использовали для доказательства нижней оценки на случайные КНФ

Weak Bit Pigeon Hole Principle

- Таблица $M \times n$, в каждой клетке 0 или 1. Если $M > 2^n$, то существуют две одинаковые строчки
- Запишем в виде (невыполнимой) КНФ утверждение о том, что все строчки различны — Mn переменных, $2^n M(M-1)/2$ дизъюнктов
- [Hrubes, Pudlak, 2017] — получили нижнюю оценку $2^{\Omega(2^{n/8})}$ на размер опровержения в Semantic Cutting Planes

Доказательство нижней оценки

- **Теорема.** Размер любого опровержения в Semantic Cutting Planes формулы $BPHP$ не меньше $2^{\Omega(2^{n/8})}$
- План доказательства:
  - Сводим оценку размера опровержения в SCP к оценке размера вещественной монотонной схемы, разделяющей два множества задачи SCP-SAT
  - Вводим меру для подмножеств, рассматриваемых в лемме Юкны
  - Применяем одну из модификаций этой леммы для мультимножеств с заданной мерой

Планы

- Эквивалентность преобразований, описанных в двух статьях
- Оценки для квадратичных цейтинских формул

Спасибо за внимание