Сложность пропозициональных доказательств

Эдуард Алексеевич Гирш

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

ПОМИ РАН

25 ноября 2010 г.

Семантическая полуалгебраическая система

Система $\mathbf{Th}(k)$:

- Строки — мультилинейные неравенства степени k.
- Аксиомы — перевод исходной формулы.
- Правило — $\dfrac{f(\vec{z}) \geq 0}{g(\vec{z}) \geq 0}$, если $\forall \vec{z} \in \{0,1\}^n \ (f \geq 0 \implies g \geq 0)$.

Семантическая полуалгебраическая система

Система $\mathbf{Th}(k)$:

- Строки — мультилинейные неравенства степени k.
- Аксиомы — перевод исходной формулы.
- Правило — $\dfrac{f(\vec{z}) \geq 0}{g(\vec{z}) \geq 0}$, если $\forall \vec{z} \in \{0,1\}^n \ (f \geq 0 \implies g \geq 0)$.

Доказательство нижней оценки для treelike $\mathbf{Th}(k)$:
док-во $\mapsto$ decision tree $\mapsto$ коммуникационный протокол.

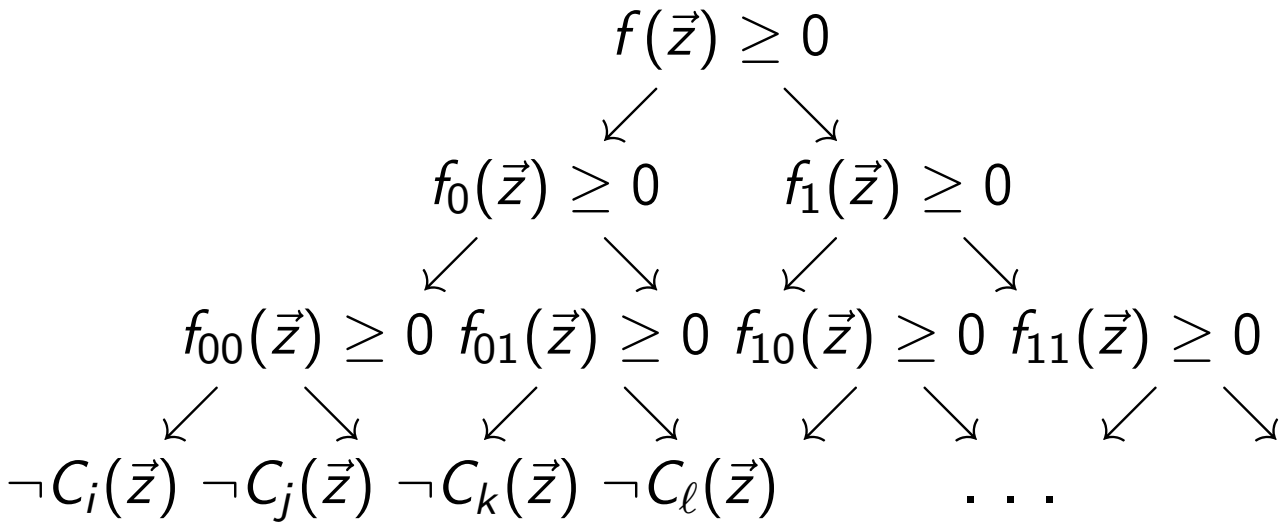
Семантическая полуалгебраическая система

Система $\mathbf{Th}(k)$:

- Строки — мультилинейные неравенства степени k.
- Аксиомы — перевод исходной формулы.
- Правило — $\dfrac{f(\vec{z}) \geq 0}{g(\vec{z}) \geq 0}$, если $\forall \vec{z} \in \{0,1\}^n \ (f \geq 0 \implies g \geq 0)$.

Доказательство нижней оценки для treelike $\mathbf{Th}(k)$:
док-во $\mapsto$ decision tree $\mapsto$ коммуникационный протокол.

Decision tree для $C_1 \wedge C_2 \wedge \ldots$ от переменных $\vec{z}$:



Древесное док-во $\mapsto$ decision tree

- Дано док-во π — дерево P,
  соблюдающее логические следствия и с противоречием в корне.
- Найдём поддерево T размера $|\pi|/3\,..\,2|\pi|/3$ с корнем $g(\vec{z}) \geq 0$.
- Это будет корень decision tree.

Древесное док-во $\mapsto$ decision tree

- Дано док-во π — дерево P,
  соблюдающее логические следствия и с противоречием в корне.
- Найдём поддерево T размера $|\pi|/3\,..\,2|\pi|/3$ с корнем $g(\vec{z}) \geq 0$.
- Это будет корень decision tree.
- Если $g(\vec{z}) < 0$, ложная дизъюнкция — в T,
  построим decision subtree для T рекурсивно.
- А если $g(\vec{z}) \geq 0$, то не в T,
  заменим T на $0 \geq 0$ и построим decision subtree для P рекурсивно.

Древесное док-во $\mapsto$ decision tree

- Дано док-во π — дерево P,
  соблюдающее логические следствия и с противоречием в корне.
- Найдём поддерево T размера $|\pi|/3\,..\,2|\pi|/3$ с корнем $g(\vec{z}) \geq 0$.
- Это будет корень decision tree.
- Если $g(\vec{z}) < 0$, ложная дизъюнкция — в T,
  построим decision subtree для T рекурсивно.
- А если $g(\vec{z}) \geq 0$, то не в T,
  заменим T на $0 \geq 0$ и построим decision subtree для P рекурсивно.
- Итого размер тот же, неравенства те же, глубина $O(\log |\pi|)$.

Коммуникационная сложность

- Общаются $A_1, \ldots, A_k$. Общий вход F и ещё входы $z_1, \ldots, z_k$.

Коммуникационная сложность

- Общаются $A_1, \ldots, A_k$. Общий вход F и ещё входы $z_1, \ldots, z_k$.
- Number-in-hand model: A_i знает z_i.
- Number-on-forehead model: A_i знает всё, кроме z_i.

Коммуникационная сложность

- Общаются $A_1, \ldots, A_k$. Общий вход F и ещё входы $z_1, \ldots, z_k$.
- Number-in-hand model: A_i знает z_i.
- Number-on-forehead model: A_i знает всё, кроме z_i.
- Надо вычислить $f(F, z_1, \ldots, z_k)$.
  Сложность — общее кол-во переданных битов.

Коммуникационная сложность

- Общаются $A_1, \ldots, A_k$. Общий вход F и ещё входы $z_1, \ldots, z_k$.
- Number-in-hand model: A_i знает z_i.
- Number-on-forehead model: A_i знает всё, кроме z_i.
- Надо вычислить $f(F, z_1, \ldots, z_k)$.
  Сложность — общее кол-во переданных битов.
- Можно детерминированно, можно вероятностно.

Коммуникационная сложность

- Общаются $A_1, \ldots, A_k$. Общий вход F и ещё входы $z_1, \ldots, z_k$.
- Number-in-hand model: A_i знает z_i.
- Number-on-forehead model: A_i знает всё, кроме z_i.
- Надо вычислить $f(F, z_1, \ldots, z_k)$.
  Сложность — общее кол-во переданных битов.
- Можно детерминированно, можно вероятностно.
- Наша задача: дана КНФ F, набор значений z разбит на части.
  Надо выдать номер невыполненной дизъюнкции.

Коммуникационная сложность

- Общаются $A_1, \ldots, A_k$. Общий вход F и ещё входы $z_1, \ldots, z_k$.
- Number-in-hand model: A_i знает z_i.
- Number-on-forehead model: A_i знает всё, кроме z_i.
- Надо вычислить $f(F, z_1, \ldots, z_k)$.
  Сложность — общее кол-во переданных битов.
- Можно детерминированно, можно вероятностно.
- Наша задача: дана КНФ F, набор значений z разбит на части.
  Надо выдать номер невыполненной дизъюнкции.
- F — цейтинская, но x_i заменены на $\bigwedge_{j=1}^{k} z_{ij}$.

Decision tree $\mapsto$ детерминированный протокол

- Вычисляем $R(x_1, \ldots, x_n)$, имея
  - дерево глубины d,
  - неравенства степени k,
  - n и коэффициенты $\leq N$.
- Строим $(k+1)$-NOF протокол сложности $O(d \cdot \log N)$.

Decision tree $\mapsto$ детерминированный протокол

- Вычисляем $R(x_1, \ldots, x_n)$, имея
  - дерево глубины d,
  - неравенства степени k,
  - n и коэффициенты $\leq N$.
- Строим $(k+1)$-NOF протокол сложности $O(d \cdot \log N)$.

- Каждый моном целиком виден хотя бы одному участнику.
- Протокол: каждый сообщает сумму "своих" мономов, проверяет неравенство и движется дальше по дереву.

Decision tree $\mapsto$ вероятностный протокол

- Вычислим с ошибкой $1/n$ и сложностью $O(d(\log\log N)^2)$.

Decision tree $\mapsto$ вероятностный протокол

- Вычислим с ошибкой $1/n$ и сложностью $O(d(\log\log N)^2)$.
- $(k+1)$-NIH протокол для проверки $y_1 + \ldots + y_{k+1} \geq 0$ с ошибкой $O(1/n^c)$ и сложностью $O(k \cdot \log^2 n)$, где n — число битов в y_i:

Decision tree $\mapsto$ вероятностный протокол

- Вычислим с ошибкой $1/n$ и сложностью $O(d(\log\log N)^2)$.
- $(k+1)$-NIH протокол для проверки $y_1 + \ldots + y_{k+1} \geq 0$ с ошибкой $O(1/n^c)$ и сложностью $O(k \cdot \log^2 n)$, где n — число битов в y_i:
  - $y_i = h_i + \ell_i$, где $h_i \leq y_i/2^{\lfloor n/2 \rfloor}$ (старшие $\lceil n/2 \rceil$ битов),
  - Если $\sum h_i > 0$ или $\sum h_i < -k$, то всё ясно.
  - Поэтому "главный" выбирает $p \in \mathbb{P} \cap [n^{c+2} \ln n \,..\, 2n^{c+2} \ln n]$, собирает $h_i \mod p$, вычисляет сумму $\mod p$.

Decision tree $\mapsto$ вероятностный протокол

- Вычислим с ошибкой $1/n$ и сложностью $O(d(\log\log N)^2)$.
- $(k+1)$-NIH протокол для проверки $y_1 + \ldots + y_{k+1} \geq 0$
  с ошибкой $O(1/n^c)$ и сложностью $O(k \cdot \log^2 n)$,
  где n — число битов в y_i:
  - $y_i = h_i + \ell_i$, где $h_i \leq y_i/2^{\lfloor n/2 \rfloor}$ (старшие $\lceil n/2 \rceil$ битов),
  - Если $\sum h_i > 0$ или $\sum h_i < -k$, то всё ясно.
  - Поэтому "главный" выбирает $p \in \mathbb{P} \cap [n^{c+2} \ln n \,..\, 2n^{c+2} \ln n]$,
    собирает $h_i \mod p$, вычисляет сумму $\mod p$.
  - Если получилось $j \in \{-k, \ldots, 0\}$,
    то запускаем для $\ell_1 + \ldots + \ell_{k+1} + j \cdot 2^{\lfloor n/2 \rfloor} \geq 0$.

Decision tree $\mapsto$ вероятностный протокол

- Вычислим с ошибкой $1/n$ и сложностью $O(d(\log\log N)^2)$.
- $(k+1)$-NIH протокол для проверки $y_1 + \ldots + y_{k+1} \geq 0$
  с ошибкой $O(1/n^c)$ и сложностью $O(k \cdot \log^2 n)$,
  где n — число битов в y_i:
  - $y_i = h_i + \ell_i$, где $h_i \leq y_i/2^{\lfloor n/2 \rfloor}$ (старшие $\lceil n/2 \rceil$ битов),
  - Если $\sum h_i > 0$ или $\sum h_i < -k$, то всё ясно.
  - Поэтому "главный" выбирает $p \in \mathbb{P} \cap [n^{c+2} \ln n \,..\, 2n^{c+2} \ln n]$,
    собирает $h_i \mod p$, вычисляет сумму $\mod p$.
  - Если получилось $j \in \{-k, \ldots, 0\}$,
    то запускаем для $\ell_1 + \ldots + \ell_{k+1} + j \cdot 2^{\lfloor n/2 \rfloor} \geq 0$.
  - Иначе запускаем для $h_1 + \ldots + h_{k+1} \geq 0$.

Decision tree $\mapsto$ вероятностный протокол

- Вычислим с ошибкой $1/n$ и сложностью $O(d(\log\log N)^2)$.
- $(k+1)$-NIH протокол для проверки $y_1 + \ldots + y_{k+1} \geq 0$
  с ошибкой $O(1/n^c)$ и сложностью $O(k \cdot \log^2 n)$,
  где n — число битов в y_i:
  - $y_i = h_i + \ell_i$, где $h_i \leq y_i/2^{\lfloor n/2 \rfloor}$ (старшие $\lceil n/2 \rceil$ битов),
  - Если $\sum h_i > 0$ или $\sum h_i < -k$, то всё ясно.
  - Поэтому "главный" выбирает $p \in \mathbb{P} \cap [n^{c+2} \ln n \,..\, 2n^{c+2} \ln n]$,
    собирает $h_i \mod p$, вычисляет сумму $\mod p$.
  - Если получилось $j \in \{-k, \ldots, 0\}$,
    то запускаем для $\ell_1 + \ldots + \ell_{k+1} + j \cdot 2^{\lfloor n/2 \rfloor} \geq 0$.
  - Иначе запускаем для $h_1 + \ldots + h_{k+1} \geq 0$.
  - Ошибка, если p оказалось среди делителей чисел $\{\sum h_i + t\}_{t=0}^{k}$.

Decision tree $\mapsto$ вероятностный протокол

- Вычислим с ошибкой $1/n$ и сложностью $O(d(\log\log N)^2)$.
- $(k+1)$-NIH протокол для проверки $y_1 + \ldots + y_{k+1} \geq 0$
  с ошибкой $O(1/n^c)$ и сложностью $O(k \cdot \log^2 n)$,
  где n — число битов в y_i:
  - $y_i = h_i + \ell_i$, где $h_i \leq y_i/2^{\lfloor n/2 \rfloor}$ (старшие $\lceil n/2 \rceil$ битов),
  - Если $\sum h_i > 0$ или $\sum h_i < -k$, то всё ясно.
  - Поэтому "главный" выбирает $p \in \mathbb{P} \cap [n^{c+2} \ln n \,..\, 2n^{c+2} \ln n]$,
    собирает $h_i \mod p$, вычисляет сумму $\mod p$.
  - Если получилось $j \in \{-k, \ldots, 0\}$,
    то запускаем для $\ell_1 + \ldots + \ell_{k+1} + j \cdot 2^{\lfloor n/2 \rfloor} \geq 0$.
  - Иначе запускаем для $h_1 + \ldots + h_{k+1} \geq 0$.
  - Ошибка, если p оказалось среди делителей чисел $\{\sum h_i + t\}_{t=0}^{k}$.
- Вместо того, чтобы сообщать сумму мономов,
  воспользуемся вероятностным протоколом
  (свободный член учитывает первый участник).

Нижняя оценка на длины док-в в $\mathbf{Th}(k)$

Теорема

Нижняя оценка $(\log n)^{3+\epsilon}$ на $(k+1)$-NOF сложность задачи OddCharge (по суммам в вершинах и набору значений, распределённому среди участников, определить вершину с ошибкой) влечёт суперполиномиальную нижнюю оценку на длины доказательств формул для тех же графов в treelike $\mathbf{Th}(k)$.

Планы

- Список вопросов к экзамену — на сайте клуба.
- Последняя лекция и консультация — 16 декабря.
- Экзамен рекомендуется сдать **до конца декабря**.

Планы

- Список вопросов к экзамену — на сайте клуба.
- Последняя лекция и консультация — 16 декабря.
- Экзамен рекомендуется сдать **до конца декабря**.
- . . . но можно и после 15 января.