Машины Тьюринга с оракулами

30.04.2013

Определение 1. Оракул для языка A — устройство, моментально распознающее принадлежность слова языку A.

Машина Тьюринга с оракулом M^A имеет возможность проконсультироваться у оракула для языка A:

- M^A пишет слово w на специальной *ленте оракула* и за один шаг узнает, верно ли, что $w \in A$.

$\mathbf{P}^A$ — класс языков, разрешимых за полиномиальное время на детерминированной машине Тьюринга с оракулом для языка A.

$\mathbf{NP}^A$ — класс языков, разрешимых за полиномиальное время на недетерминированной машине Тьюринга с оракулом для языка A.

Пример 2.

- $\mathrm{NP} \subseteq \mathrm{P}^{\mathrm{SAT}}$
- $\mathrm{coNP} \subseteq \mathrm{P}^{\mathrm{SAT}}$

Пример 3.

- Две формулы ϕ и ψ с переменными $x_1, \ldots, x_\ell$ *эквивалентны*, если их значения одинаковы при любом означивании переменных.
- Формула *минимальна*, если ей не эквивалентна никакая формула меньшего размера.
- NONMIN-FORMULA $= \{\langle\phi\rangle \mid \phi$ — не является минимальной булевой формулой$\}$
- NONMIN-FORMULA $\in$ NP? — неизвестно
- NONMIN-FORMULA $\in \mathrm{NP}^{\mathrm{SAT}}$

Машина Тьюринга с оракулом

Теорема 4.

- *Существует оракул A, такой что $P^A \neq NP^A$*
- *Существует оракул B, такой что $P^B = NP^B$*

Доказательство.

- Построим оракул A таким образом, чтобы для распознавания некоторого языка L_A из NP^A требовался полный перебор.
  - Покажем, что никакая полиномиальная машина с оракулом не распознает L_A.
- $L_A \notin \mathrm{P}^A$
- $\mathrm{P}^A \neq \mathrm{NP}^A$
- Для произвольного языка X введем обозначение:

$$L_X = \{w \mid \exists x \in X(|x| = |w|)\}.$$

- $L_X \in \mathrm{NP}^X$
- Построим A, такой что $L_A \notin \mathrm{P}^A$.
- $M_1, M_2, \ldots$ — список всех полиномиальных машин Тьюринга с оракулом.
- Допустим, что машина M_i работает в течение времени n^i.
- Строим A по шагам:
  - На шаге i построим часть A, отвечающую за то, что M_i^A не распознает L_A.
  - На каждом шаге некоторое конечное число строк объявляется принадлежащим A и некоторое конечное число строк — не принадлежащим A.

Шаг i:

- Выбрать n, превышающее длину любой строки, «статус» которой относительно A уже определен, такое что $2^n > n^i$.
- Запустить M_i на 1^n.
- M_i обращается к оракулу с вопросом про y:
  - Если статус y определен, отвечаем в соответствии с этим статусом.
  - Иначе, отвечаем «нет» — $y \notin A$.
- У M_i недостаточно времени, чтобы спросить про все строки длины n.
  - Если M_i принимает 1^n, считаем, что все строки длины n не входят в A.
  - Иначе, включаем в A строку длины n, о которой M не спрашивала.

□