Полиномиальная иерархия.

Классы Σ_2^P и Π_2^P

INDSET $= \{(G,k) \mid$ G сод. нез. мн. размера $\geq k\}$

EXACT INDSET $= \{(G,k) \mid$ наибольшее незав. мн. имеет размер $k\}$

$\downarrow$

кажется для этой задачи нет короткого сертификата

MIN DNF $= \{ \llcorner\varphi\lrcorner :$ φ — ДНФ формула неэквивалентная никакой меньшей формуле$\} =$

$$= \{ \llcorner\varphi\lrcorner \mid \forall \psi, |\psi| < \varphi \Rightarrow \exists\, s, \text{ что } \varphi(s) \neq \psi(s) \}.$$

Обе задачи живут в PSPACE, но скорее всего не PSPACE-полные.

Определение: Класс Σ_2^P — это множество языков L, для которых $\exists$ полином. машина Тьюринга M и полином q такие, что

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)}\ \forall v \in \{0,1\}^{q(|x|)}\ M(x,u,v) = 1.$$

Замечание $NP, coNP \subseteq \Sigma_2^P$.

Пример. EXACT INDSET

$\exists S\ \forall S'$: S — незав. мн. и $|S| = k$ и

S' — не явл. незав. мн. размера $\geq k+1$.

Определение $\Pi_2^P = \{\overline{L} \mid L \in \Sigma_2^P\}$

$\Updownarrow$

$\forall x:\quad x \in L \iff \forall y \in \{0,1\}^{q(|x|)}\ \exists w \in \{0,1\}^{q(|x|)}\ M(x,y,w) = 1$.

Пример EXACT INDSET $\in \Pi_2^P$.

MIN-DNF $\in \Pi_2^P$.

Полиномиальная иерархия

Определение $L \in \Sigma_i^P$ если $\exists_{poly}$ МТ M и полином poly q:

$x \in L \iff \exists u_1 \in \{0,1\}^{q(|x|)}\ \forall u_2 \in \{0,1\}^{q(|x|)} \ldots Q_i u_i \in \{0,1\}^{q(|x|)}\ M(x,u_1,\ldots u_i) = 1$

Аналогично Π_i^P.

Полином иерархия $PH = \bigcup_i \Sigma_i^P$.

Замечание $\Sigma_1^P = NP$, $\Pi_1^P = coNP$, $\Pi_i^P = co\Sigma_i^P$

$\Sigma_i^P \subseteq \Pi_{i+1}^P \Rightarrow PH = \bigcup_i \Pi_i^P$

Св-ва полином иерархии

Мы верим: $P \neq NP$, $NP \neq coNP$.

Обобщение данной веры $\Sigma_i^P \neq \Sigma_{i+1}^P$

Теорема (i) $\forall i$ $\Sigma_i^P = \Pi_i^P \Rightarrow PH = \Sigma_i^P$

(ii) $P = NP \Rightarrow PH = P$.

Упражнение

Полные задачи для класса PH

Опр Σ_i^P-полная задача

~~Altertating~~ Alternating Turing Machines.

$\forall$ состояние кроме C_{accept} и C_{halt} помечено символом $\exists$ или $\forall$. В остальном ~~похоже~~ как НМТ.

<u>Определение</u> M — $T(n)$ ATM если $\forall x \in \{0,1\}^* \; \forall$ последов. переходов ATM остановится в течении $T(|x|)$ шагов.

Граф конфигураций для ATM и определение принадлежности языку.

<u>Опр</u> $ATime(T(n))$ — языки распознаваемые $O(T(n))$ time ATM.

<u>Опр.</u> $\forall i$ $\Sigma_i Time\, T(n)$ — ~~языки~~ распознающиеся с помощью $T(n)$-time ATM M и ~~перв~~ C_{start} помечено $\exists$ и на любом пути метка меняется не более $i-1$ раза.

<u>Утв.</u> $$\Sigma_i^P = \bigcup \Sigma_i Time(n^c)$$

Упражнение.

Утв Если L - PH-полная задача, то $\exists\, i$

$\Sigma_i^P = PH$.

Замечание $PH \subseteq PSPACE$.

$PH \neq PSPACE$ иначе иерархия схлопывается.

Пример $\Sigma_i SAT = \exists u_1 \forall u_2 \ldots Q_i u_i\ \varphi(u_1, \ldots u_i) = 1$

$\swarrow$

Σ_i^P-полная задача. u_i - вектор.

Time-space tradeoffs for SAT.

На данный момент мы не умеем показывать, что для решения SAT необходимо больше линейного времени или больше $\log$ памяти. Покажем, что нет алгоритма использующего линейное время и $\log$ памяти.

~~Теорема~~ Определение: $TISP(T(n), S(n))$ — язык решающийся с пом. ДТМ за время $O(T(n))$ и $O(S(n))$ памяти.

Теорема о иерархии по времени для NDTM машин

Теорема $NTime[N] \not\subseteq TISP(n^{1,2}, n^{0,2})$

док-во

Лемма $TISP(n^{12}, n^2) \subseteq \Sigma_2 Time(n^8)$

док-во: Рассмотрим граф конфигураций. Из c_{start} есть путь в c_{accept} длины не более n^{12} $\Rightarrow \exists$ ~~$c_1, \ldots c_{n^6}$~~ конфигурации $c_1, c_2, \ldots c_{n^6}$, такие что из c_i в c_{i+1} можно попасть за n^6 шагов и $c_1 = c_{start}$, $c_{n^6} = c_{accept}$.

$c_1, \ldots c_6$ - занимает n^8 места.

$\exists C_1, \ldots C_{n^6}\ \forall i \in \overline{1, n^6}\ M(C_i, C_{i+1})$

можно из C_i добраться за n^6 шагов в C_{i+1}

это можно просимулировать за n^8 $\Rightarrow$

$\cancel{NTime}\ TISP[n^{12}, n^2] \subseteq \Sigma_2 Time(n^8)$

Лемма Если $NTime[n] \subseteq DTime(n^{1.2})$, то

$\Sigma_2 Time(n^8) \subseteq NTime(n^{9.6})$

Док-во Рассмотрим $\Sigma_2 Time(n^8) \ni L$

$x \in L \iff \exists u \in \{0,1\}^{c|x|^8}\ \forall w \in \{0,1\}^{d|x|^8}\ M(x,u,w)=1.$

$M(\underbrace{x,u}_{\text{вход}},\ w) = 0 \leftarrow$ язык из $NTime[n]$.

подсказка

$\exists D \in DTime[n^{1.2}]$, что $D(x,u)=1$ iff

$\exists w\ M(x,u,w)=0.$

$x \in L \iff \exists u\ D(x,u) = 1$

от x работает за время $(n^8)^{1.2} = n^{9.6}$

$\Rightarrow L \in NTime(n^{9.6})$.

$NTime[n] \subseteq TISP(n^{1.2}, n^{0.2}) \Rightarrow NTime[n^{10}] \subseteq TISP(n^{12}, n^2)$

$\Rightarrow NTime[n^{10}] \subseteq \Sigma_2 Time[n^8] \subseteq NTime[n^{9.6}]$

противоречие.

$SAT \in TISP(n^{1.1}, n^{0.1}) \Rightarrow NTime[n] \subseteq TISP(n^{1.1} polylog, n^{0.1} polylog)$ (Ч)

Определение полиномиальной иерархии через оракульные машины

Теорема $\Sigma_i^P = NP^{\Sigma_{i-1}\text{SAT}}$

Док-во мы покажем только

$$\Sigma_2^P = NP^{SAT}.$$

(i) $\Sigma_2^P \subseteq NP^{SAT}$

$L \in \Sigma_2^P \Rightarrow x \in L \Leftrightarrow \exists u_1 \in \{0,1\}^{q(|x|)}\ \forall u_2 \in \{0,1\}^{q(|x|)}\ M(x, u_1, u_2) = 1$

Для фиксированного x, u_1 утв. выше это отрицание NP-утв. $\Rightarrow$ его истинность можно проверить с помощью оракула с доступом ~~к~~ SAT.

Т.е. ~~сразу~~ недетерминированно угадаем u_1 с пом. оракула узнаем ответ $\forall u_2\ (M(x, u_1, u_2))$.

(ii) $NP^{SAT} \subseteq \Sigma_2^P$.

$L \in NP^{SAT} \Rightarrow \exists c_1 \ldots c_m \in \{0,1\}$ и ответы оракула $a_1 \ldots a_k \in \{0,1\}$. Пусть оракульные запросы $\varphi_1, \ldots \varphi_k$. тогда:

Если $a_i = 1 \Rightarrow \exists u_i$, что $\varphi_i(u_i) = 1$

Если $a_i = 0 \Rightarrow \forall v_i\ \varphi_i(v_i) = 0$.

$x \in L \Leftrightarrow \exists c_1 \ldots c_m\ a_1 \ldots a_k\ u_1 \ldots u_k\ \forall v_1 \ldots v_k$ s.t.

N принимает x используя выборы c_i и ответы a_i и $\exists \varphi_i(u_i) = 1$ для $a_i = 1$ и $\varphi_i(v_i) = 0\ \forall v_i$ для $a_i = 0$.