Властивості класу складності $\mathcal{NP}$

Андрій Фесенко

Використання зведення

$HALT \leq HALT^{\varepsilon}$
$HALT \leq A_{TM}$

Використання зведення

$HALT \leq_m HALT^{\varepsilon}$

$HALT \leq_m A_{TM}$

R є замкненим відносно зведення $\leq_m$, а $HALT \notin R$, $HALT \in RE$

Використання зведення

$HALT \leq_m HALT^{\varepsilon}$
$HALT \leq_m A_{TM}$
R є замкненим відносно зведення $\leq_m$, а $HALT \notin R$, $HALT \in RE$

Властивості класу складності відносно зведення:

- замкненість;
- існування важких задач;
- існування повних задач.

RE-повні задачі

Твердження

Нехай $L_1 \in RE$. Тоді, $L_1 \leq_m HALT$.

RE-повні задачі

Твердження

Нехай $L_1 \in RE$. Тоді, $L_1 \leq_m HALT$.

Доведення.

$L_1 \in RE \Rightarrow \exists$ ДМТ $M_1 : L(M_1) = L_1$. ($x \in L_1 \Leftrightarrow M_1(x) = 1$)

□

RE-повні задачі

Твердження

Нехай $L_1 \in RE$. Тоді, $L_1 \leq_m HALT$.

Доведення.

$L_1 \in RE \Rightarrow \exists$ ДМТ $M_1 : L(M_1) = L_1$. ($x \in L_1 \Leftrightarrow M_1(x) = 1$)

$$\text{ДМТ } \tilde{M}_1(x) = \begin{cases} M_1(x), & M_1(x) \neq 0 \\ \perp, & M_1(x) = 0 \end{cases}$$

□

RE-повні задачі

Твердження

Нехай $L_1 \in RE$. Тоді, $L_1 \leq_m HALT$.

Доведення.

$L_1 \in RE \Rightarrow \exists$ ДМТ $M_1 : L(M_1) = L_1$. ($x \in L_1 \Leftrightarrow M_1(x) = 1$)

$$\text{ДМТ } \tilde{M}_1(x) = \begin{cases} M_1(x), & M_1(x) \neq 0 \\ \perp, & M_1(x) = 0 \end{cases}$$

$\forall x \in \{0,1\}^*$ функція зведення $f(x) = (\tilde{M}_1, x)$

□

RE-повні задачі

Твердження

Нехай $L_1 \in RE$. Тоді, $L_1 \leq_m HALT$.

Доведення.

$L_1 \in RE \Rightarrow \exists$ ДМТ $M_1 : L(M_1) = L_1$. ($x \in L_1 \Leftrightarrow M_1(x) = 1$)

$$\text{ДМТ } \tilde{M}_1(x) = \begin{cases} M_1(x), & M_1(x) \neq 0 \\ \perp, & M_1(x) = 0 \end{cases}$$

$\forall x \in \{0,1\}^*$ функція зведення $f(x) = (\tilde{M}_1, x)$

$x \in L_1 \Leftrightarrow M_1(x) = 1 \Leftrightarrow \tilde{M}_1(x) \neq \perp \Leftrightarrow f(x) = (\tilde{M}_1, x) \in HALT$

□

RE-повні задачі

Твердження

Нехай $L_1 \in RE$. Тоді, $L_1 \leq_m HALT$.

Доведення.

$L_1 \in RE \Rightarrow \exists$ ДМТ $M_1 : L(M_1) = L_1$. ($x \in L_1 \Leftrightarrow M_1(x) = 1$)

$$\text{ДМТ } \tilde{M}_1(x) = \begin{cases} M_1(x), & M_1(x) \neq 0 \\ \perp, & M_1(x) = 0 \end{cases}$$

$\forall x \in \{0,1\}^*$ функція зведення $f(x) = (\tilde{M}_1, x)$
$x \in L_1 \Leftrightarrow M_1(x) = 1 \Leftrightarrow \tilde{M}_1(x) \neq \perp \Leftrightarrow f(x) = (\tilde{M}_1, x) \in HALT$

□

Наслідок

HALT є *RE*-повною задачею відносно зведення $\leq_m$

R-повні задачі

Твердження

Нехай $L_1 \in R$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in R : L_2 \leq_m L_1$.

R-повні задачі

Твердження

Нехай $L_1 \in R$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in R : L_2 \leq_m L_1$.

Доведення.

L_1 — нетривіальна мова $\Rightarrow \exists x_0, x_1 \in \{0,1\}^*$: $x_0 \notin L_1$ і $x_1 \in L_1$

□

R-повні задачі

Твердження

Нехай $L_1 \in R$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in R : L_2 \leq_m L_1$.

Доведення.

L_1 — нетривіальна мова $\Rightarrow \exists x_0, x_1 \in \{0,1\}^*$: $x_0 \notin L_1$ і $x_1 \in L_1$

$L_2 \in R \Rightarrow \exists$ ДМТ $M_2 : L(M_2) = L_2$

$x \in L_2 \Leftrightarrow M_2(x) = 1$, $x \notin L_2 \Leftrightarrow M_2(x) = 0$

□

R-повні задачі

Твердження

Нехай $L_1 \in R$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in R : L_2 \leq_m L_1$.

Доведення.

L_1 — нетривіальна мова $\Rightarrow \exists x_0, x_1 \in \{0,1\}^*$: $x_0 \notin L_1$ і $x_1 \in L_1$

$L_2 \in R \Rightarrow \exists$ ДМТ $M_2 : L(M_2) = L_2$
$x \in L_2 \Leftrightarrow M_2(x) = 1$, $x \notin L_2 \Leftrightarrow M_2(x) = 0$

ДМТ $\tilde{M}_2(x) = \begin{cases} x_0, & M_2(x) = 0 \\ x_1, & M_2(x) = 1 \end{cases}$, функція зведення $f(x) = \tilde{M}_2(x)$

□

R-повні задачі

Твердження

Нехай $L_1 \in R$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in R : L_2 \leq_m L_1$.

Доведення.

L_1 — нетривіальна мова $\Rightarrow \exists x_0, x_1 \in \{0,1\}^*$: $x_0 \notin L_1$ і $x_1 \in L_1$

$L_2 \in R \Rightarrow \exists$ ДМТ $M_2 : L(M_2) = L_2$
$x \in L_2 \Leftrightarrow M_2(x) = 1$, $x \notin L_2 \Leftrightarrow M_2(x) = 0$

ДМТ $\tilde{M}_2(x) = \begin{cases} x_0, & M_2(x) = 0 \\ x_1, & M_2(x) = 1 \end{cases}$, функція зведення $f(x) = \tilde{M}_2(x)$

$x \in L_2 \Leftrightarrow M_2(x) = 1 \Leftrightarrow \tilde{M}_2(x) = f(x) = x_1 \in L_1$

□

R-повні задачі

Твердження

Нехай $L_1 \in R$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in R : L_2 \leq_m L_1$.

Доведення.

L_1 — нетривіальна мова $\Rightarrow \exists x_0, x_1 \in \{0,1\}^*$: $x_0 \notin L_1$ і $x_1 \in L_1$

$L_2 \in R \Rightarrow \exists$ ДМТ $M_2 : L(M_2) = L_2$

$x \in L_2 \Leftrightarrow M_2(x) = 1$, $x \notin L_2 \Leftrightarrow M_2(x) = 0$

ДМТ $\tilde{M}_2(x) = \begin{cases} x_0, & M_2(x) = 0 \\ x_1, & M_2(x) = 1 \end{cases}$, функція зведення $f(x) = \tilde{M}_2(x)$

$x \in L_2 \Leftrightarrow M_2(x) = 1 \Leftrightarrow \tilde{M}_2(x) = f(x) = x_1 \in L_1$

□

Наслідок

Будь-яка нетривіальна мова з класу R є R-повною відносно $\leq_m$

P-повні задачі

Наслідок

Зведення повинно використовувати менше ресурсів ніж необхідно для розв'язку задач

P-повні задачі

Наслідок

Зведення повинно використовувати менше ресурсів ніж необхідно для розв'язку задач

Твердження

Нехай $L_1 \in P$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in P : L_2 \leq_m L_1$.

P-повні задачі

Наслідок

Зведення повинно використовувати менше ресурсів ніж необхідно для розв'язку задач

Твердження

Нехай $L_1 \in P$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in P : L_2 \leq_m L_1$.

Твердження

Нехай $L_1 \in P$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in P : L_2 \leq_p L_1$.

P-повні задачі

Наслідок

Зведення повинно використовувати менше ресурсів ніж необхідно для розв'язку задач

Твердження

Нехай $L_1 \in P$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in P : L_2 \leq_m L_1$.

Твердження

Нехай $L_1 \in P$ є нетривіальною мовою.

Тоді, для довільної мови $L_2 \in P : L_2 \leq_p L_1$.

Але клас P є замкненим відносно $\leq_p$

NP-повні задачі

Клас *NP* — поліноміальне зведення (за Карпом)

NP-повні задачі

Клас *NP* — поліноміальне зведення (за Карпом)

Клас *NP* є також замкненим відносно $\leq_p$

NP-повні задачі

Клас *NP* — поліноміальне зведення (за Карпом)

Клас *NP* є також замкненим відносно $\leq_p$

Означення

Клас складності *NPC* — множина всіх *NP*-повних задач відносно поліноміального зведення

NP-повні задачі

Клас *NP* — поліноміальне зведення (за Карпом)

Клас *NP* є також замкненим відносно $\leq_p$

Означення

Клас складності *NPC* — множина всіх *NP*-повних задач відносно поліноміального зведення

Твердження

Нехай L_1 є *NP*-важкою мовою. Якщо $L_1 \in P$, то $P = NP$.

NP-повні задачі

Клас *NP* — поліноміальне зведення (за Карпом)

Клас *NP* є також замкненим відносно $\leq_p$

Означення

Клас складності *NPC* — множина всіх *NP*-повних задач відносно поліноміального зведення

Твердження

Нехай L_1 є *NP*-важкою мовою. Якщо $L_1 \in P$, то $P = NP$.

Доведення.

$P \subseteq NP$

$\forall L_2 \in NP\ L_2 \leq_p L_1$ і $L_1 \in P \Rightarrow L_2 \in P \Rightarrow NP \subseteq P$

□

NP-повні задачі

Чи існують *NP*-повні задачі?

NP-повні задачі

Чи існують *NP*-повні задачі?

Так!

$TMSAT = \{(\alpha, x, 1^n, 1^t) \mid \exists u \in \{0,1\}^n :$ АНДМТ $M_\alpha(x, u) =$ 1 не більше ніж за t тактів$\}$

NP-повні задачі

Чи існують *NP*-повні задачі?

Так!

$TMSAT = \{(\alpha, x, 1^n, 1^t) \mid \exists u \in \{0,1\}^n :$ АНДМТ $M_\alpha(x,u) =$ 1 не більше ніж за t тактів$\}$

Доведення.

$TMSAT \in NP$, використовуючи універсальну АНДМТ

$\forall L_1 \in NP : \exists$ поліноми $p, q : \mathbb{N} \to \mathbb{N}$ і АНДМТ M_1 такі, що

$\forall x \in \{0,1\}^* \; \exists u \in \{0,1\}^{q(|x|)} \; M_1(x,u) = 1$ за час, не більше ніж $p(|x|)$.

функція зведення — $f(x) = (\lfloor M_1 \rfloor, x, 1^{q(|x|)}, 1^{p(|x|)})$ $\square$

NP-повні задачі

Чи існують *NP*-повні задачі?

Так!

$TMSAT = \{(\alpha, x, 1^n, 1^t) \mid \exists u \in \{0,1\}^n :$ АНДМТ $M_\alpha(x, u) =$ 1 не більше ніж за t тактів$\}$

Доведення.

$TMSAT \in NP$, використовуючи універсальну АНДМТ

$\forall L_1 \in NP : \exists$ поліноми $p, q : \mathbb{N} \to \mathbb{N}$ і АНДМТ M_1 такі, що

$\forall x \in \{0,1\}^* \; \exists u \in \{0,1\}^{q(|x|)}$ $M_1(x, u) = 1$ за час, не більше ніж $p(|x|)$.

функція зведення — $f(x) = (\lfloor M_1 \rfloor, x, 1^{q(|x|)}, 1^{p(|x|)})$ $\square$

Твердження

Нехай $L_1 \in NPC$, $L_2 \in NP$ і $L_1 \leq_p L_2$. Тоді $L_2 \in NPC$.

Теорема Кука

Теорема Кука(-Левіна), 1971р., 1973р.

SAT є *NP*-повною задачею.

Теорема Кука

Теорема Кука(-Левіна), 1971р., 1973р.

SAT є *NP*-повною задачею.

Доведення.

$\forall L_1 \in NP : \exists$ поліноми $p, q\colon \mathbb{N} \to \mathbb{N}$ і АНДМТ M_1 такі, що $\forall x \in \{0,1\}^* \; \exists u \in \{0,1\}^{q(|x|)} \; M_1(x,u) = 1$ за час, не більше ніж $p(|x|)$.

$T_{i,j,k}$ — комірка i містить символ j на такті k

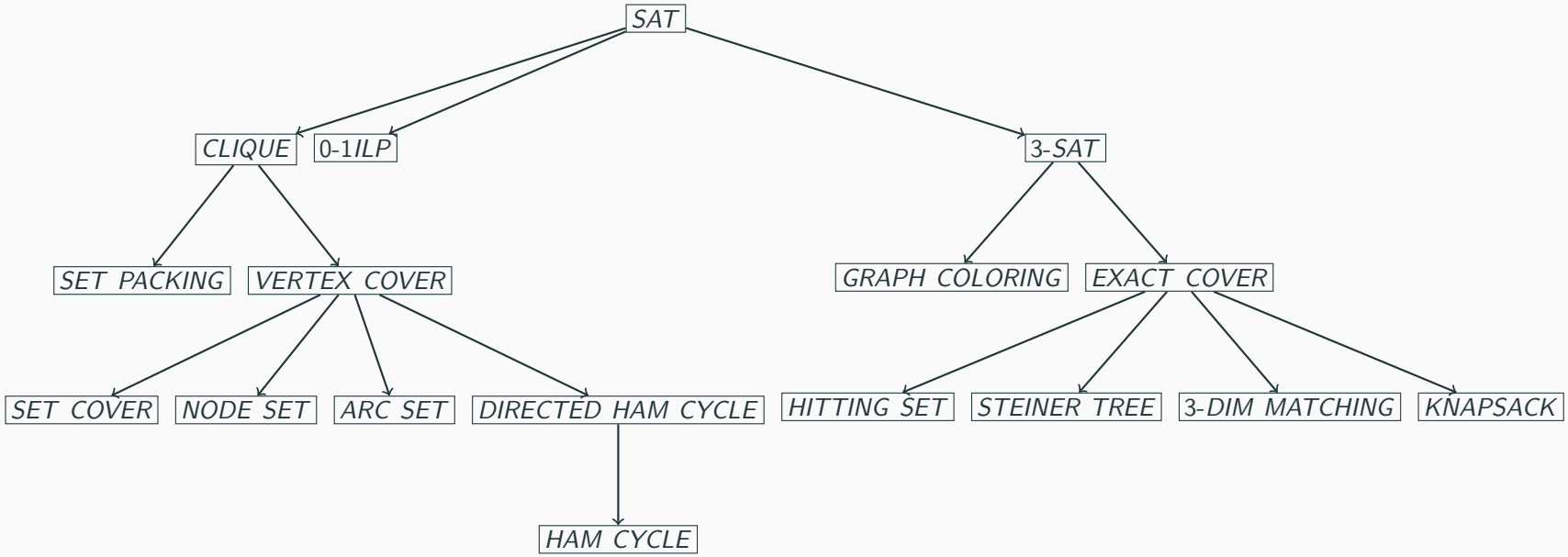
$H_{i,k}$ — зчитувальний пристрій на комірці i на такті k

$Q_{q,k}$ — АНДМТ в стані q на такті k

□

NP-повні задачі

Річард Карп ‘Reducibility among combinatorial problems’ 1972р.



Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи, 1982р. — 300+ задач

Самозведення *NP*-повних задач

Задача суперечності булевої формули (*SAT*)

З'ясувати чи має модель задана булева формула $\varphi(x_1, \ldots, x_k)$.

Задача суперечності булевої формули (*CNFSAT*)

З'ясувати чи має модель задана у КНФ булева формула $\varphi(x_1, \ldots, x_k)$.

Задача суперечності булевої формули (n-*SAT*)

З'ясувати чи має модель задана у КНФ булева формула $\varphi(x_1, \ldots, x_k)$, кожен диз'юнкт якої містить не більше ніж n літер.

Самозведення *NP*-повних задач

Твердження

$SAT =_p 3\text{-}SAT$.

Доведення.

$u_1 \vee \bar{u}_2 \vee \bar{u}_3 \vee u_4 \Rightarrow (u_1 \vee \bar{u}_2 \vee z) \wedge (\bar{u}_3 \vee u_4 \vee \bar{z})$ $\square$

Самозведення *NP*-повних задач

Твердження

$SAT =_p 3\text{-}SAT$.

Доведення.

$u_1 \vee \bar{u}_2 \vee \bar{u}_3 \vee u_4 \Rightarrow (u_1 \vee \bar{u}_2 \vee z) \wedge (\bar{u}_3 \vee u_4 \vee \bar{z})$ $\square$

Наслідок.

$SAT =_p n\text{-}SAT$ для довільного значення $n \in \mathbb{N}$, $n \geq 3$

Самозведення *NP*-повних задач

Твердження

$SAT =_p 3\text{-}SAT$.

Доведення.

$u_1 \vee \bar{u}_2 \vee \bar{u}_3 \vee u_4 \Rightarrow (u_1 \vee \bar{u}_2 \vee z) \wedge (\bar{u}_3 \vee u_4 \vee \bar{z})$ $\square$

Наслідок.

$SAT =_p n\text{-}SAT$ для довільного значення $n \in \mathbb{N}$, $n \geq 3$

Твердження

$2\text{-}SAT \in P$ (метод резолюцій Рабіна)

Самозведення *NP*-повних задач

Задача пошуку моделі булевої формули (*SAT SEARCH*)

Знайти модель заданої булевої формули $\varphi(x_1, \ldots, x_k)$.

Самозведення *NP*-повних задач

Задача пошуку моделі булевої формули (*SAT SEARCH*)

Знайти модель заданої булевої формули $\varphi(x_1, \ldots, x_k)$.

Твердження

$SAT =_p SAT\ SEARCH$

Самозведення *NP*-повних задач

Задача пошуку моделі булевої формули (*SAT SEARCH*)

Знайти модель заданої булевої формули $\varphi(x_1, \ldots, x_k)$.

Твердження

$SAT =_p SAT\ SEARCH$

Доведення.

Перевірити чи має модель $\tilde{\varphi}(1, \ldots, x_k)$ та $\tilde{\varphi}(0, \ldots, x_k)$ і тд. $\square$

Самозведення *NP*-повних задач

Задача пошуку моделі булевої формули (*SAT SEARCH*)

Знайти модель заданої булевої формули $\varphi(x_1, \ldots, x_k)$.

Твердження

$SAT =_p SAT\ SEARCH$

Доведення.

Перевірити чи має модель $\tilde{\varphi}(1, \ldots, x_k)$ та $\tilde{\varphi}(0, \ldots, x_k)$ і тд. □

SAT вирішувачі

P vs NP

$P = NP = NPC$

$P \neq NP$

Клас складності *NPI*

Означення

$NPI = \{L \in NP | L \notin NPC, L \notin P\}$, $NPI = NP \backslash (P \cup NPC)$

Клас складності *NPI*

Означення

$NPI = \{L \in NP | L \notin NPC, L \notin P\}$, $NPI = NP \backslash (P \cup NPC)$

Теорема Ладнера

Якщо $P \neq NP$, то існує мова $L_1 \in NP$ така, що $L_1 \in NP \setminus P$ і $L_1 \notin NPC$.

Клас складності *NPI*

Означення

$NPI = \{L \in NP | L \notin NPC, L \notin P\}$, $NPI = NP \backslash (P \cup NPC)$

Теорема Ладнера

Якщо $P \neq NP$, то існує мова $L_1 \in NP$ така, що $L_1 \in NP \setminus P$ і $L_1 \notin NPC$.

Доведення.

Збільшення довжини φ у КНФ $\square$

Клас складності *NPI*

Означення

$NPI = \{L \in NP | L \notin NPC, L \notin P\}$, $NPI = NP \backslash (P \cup NPC)$

Теорема Ладнера

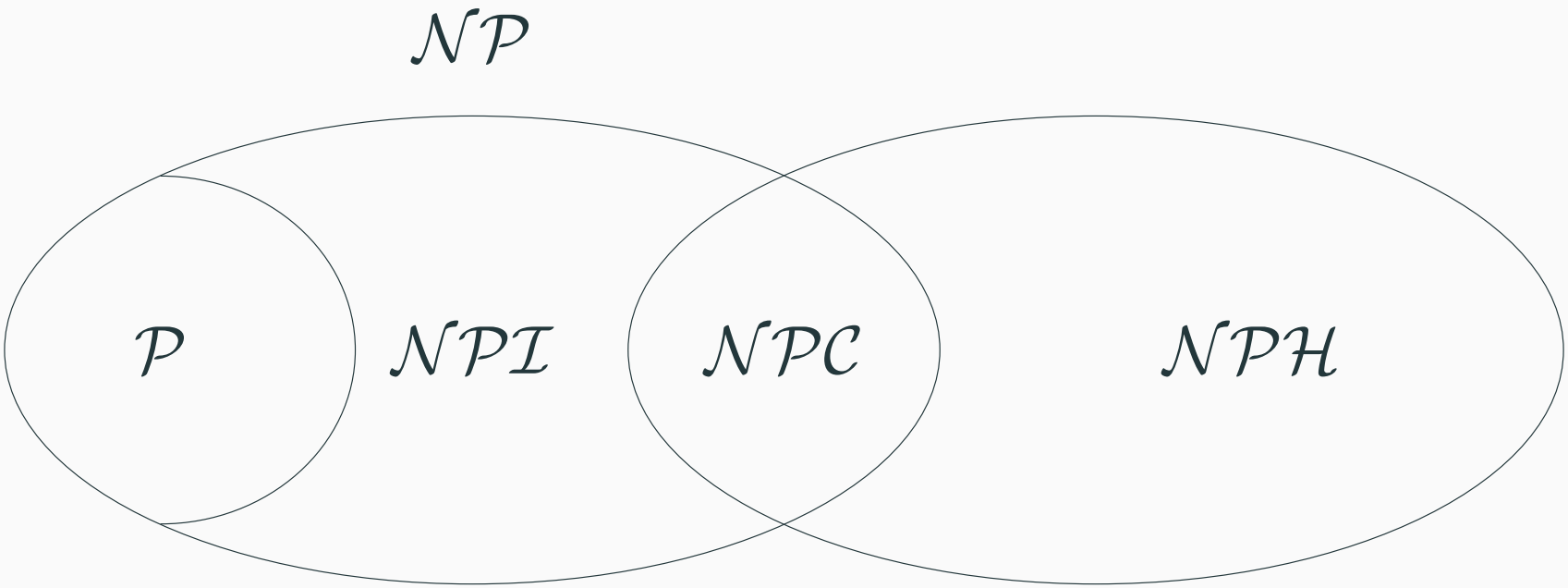
Якщо $P \neq NP$, то існує мова $L_1 \in NP$ така, що $L_1 \in NP \setminus P$ і $L_1 \notin NPC$.

Доведення.

Збільшення довжини φ у КНФ $\square$

NPI — Факторизація цілих чисел, ізоморфізм графів, дискретний логарифм

Діаграма класів складності



Теореми про ієрархію

Теорема (про часову ієрархію)

Нехай $f, g : \mathbb{N} \to \mathbb{N}$ — конструктивні за часом функції такі, що $f(n) \log f(n) = o(g(n))$. Тоді $DTIME(f(n)) \subset DTIME(g(n))$.

Теореми про ієрархію

Теорема (про часову ієрархію)

Нехай $f, g : \mathbb{N} \to \mathbb{N}$ — конструктивні за часом функції такі, що $f(n) \log f(n) = o(g(n))$. Тоді $DTIME(f(n)) \subset DTIME(g(n))$.

Доведення.

Доведемо, що $DTIME(n) \subset DTIME(n^{1,5})$

Нехай ДМТ D для довільного вхідного слова $x \in \{0,1\}^*$ моделює $|x|^{1,4}$ тактів роботи ДМТ M_x на вхідному слові x.

$$D(x) = \begin{cases} 1 - M_x(x), & M_x(x) \neq \perp \\ 0, & M_x(x) = \perp \end{cases} \Rightarrow L(D) \in DTIME(n^{1,5})$$

Нехай $L(D) \in DTIME(n) \Rightarrow \exists$ ДМТ M, $L(M) = L(D)$.

УДМТ U моделює роботу ДМТ M за час $c'c|x| \log |x|$

$\Rightarrow \exists n_0 \ \forall n > n_0 \ n^{1.4} > c'cn \log n$

$\exists x = \lfloor M \rfloor$ таке, що $|x| > n_0 \Rightarrow D(x) = 1 - M(x) \neq M(x)$ $\square$

Теореми про ієрархію

Теорема (про часову ієрархію)

Нехай $f, g : \mathbb{N} \to \mathbb{N}$ — конструктивні за часом функції такі, що $f(n) \log f(n) = o(g(n))$. Тоді $DTIME(f(n)) \subset DTIME(g(n))$.

Доведення.

Доведемо, що $DTIME(n) \subset DTIME(n^{1,5})$

Нехай ДМТ D для довільного вхідного слова $x \in \{0,1\}^*$ моделює $|x|^{1,4}$ тактів роботи ДМТ M_x на вхідному слові x.

$$D(x) = \begin{cases} 1 - M_x(x), & M_x(x) \neq \perp \\ 0, & M_x(x) = \perp \end{cases} \Rightarrow L(D) \in DTIME(n^{1,5})$$

Нехай $L(D) \in DTIME(n) \Rightarrow \exists$ ДМТ M, $L(M) = L(D)$.

УДМТ U моделює роботу ДМТ M за час $c'c|x| \log |x|$

$\Rightarrow \exists n_0 \; \forall n > n_0 \; n^{1.4} > c'cn \log n$

$\exists x = \lfloor M \rfloor$ таке, що $|x| > n_0 \Rightarrow D(x) = 1 - M(x) \neq M(x)$ $\square$

$f(n+1) = o(g(n)) \Rightarrow NTIME(f(n)) \subset NTIME(g(n))$

Непряме порівняння *PvsNP*

Якщо $NP \neq coNP$, то $P \neq NP$.

Непряме порівняння *PvsNP*

Якщо $NP \neq coNP$, то $P \neq NP$.

Доведення.

$P = NP \Rightarrow coNP = coP = P = NP$ □

Непряме порівняння *PvsNP*

Якщо $NP \neq coNP$, то $P \neq NP$.

Доведення.

$P = NP \Rightarrow coNP = coP = P = NP$ □

Якщо $EXP \neq NEXP$, то $P \neq NP$.

Непряме порівняння *PvsNP*

Якщо $NP \neq coNP$, то $P \neq NP$.

Доведення.

$P = NP \Rightarrow coNP = coP = P = NP$ □

Якщо $EXP \neq NEXP$, то $P \neq NP$.

Доведення.

Нехай $P = NP$ і $L_1 \in NTIME(2^{n^c})$

$L_{1+pad} = \left\{ \left(x, 1^{2^{|x|^c}} \right) \mid x \in L_1 \right\} \Rightarrow L_{1+pad} \in NP$

Перевіряємо формат слова $y = z||1^{2^{|z|^c}}$ і запускаємо НДМТ M_1 на слові z

Час роботи є поліноміальним відносно $|y|$. □

Непряме порівняння *PvsNP*

Якщо $NP \neq coNP$, то $P \neq NP$.

Доведення.

$P = NP \Rightarrow coNP = coP = P = NP$ □

Якщо $EXP \neq NEXP$, то $P \neq NP$.

Доведення.

Нехай $P = NP$ і $L_1 \in NTIME(2^{n^c})$

$L_{1+pad} = \left\{ \left(x, 1^{2^{|x|^c}} \right) \mid x \in L_1 \right\} \Rightarrow L_{1+pad} \in NP$

Перевіряємо формат слова $y = z||1^{2^{|z|^c}}$ і запускаємо НДМТ M_1 на слові z

Час роботи є поліноміальним відносно $|y|$. □

метод доповнення (padding)

Теорема Бейкера-Джіла-Соловея

$\forall O \subseteq \{0,1\}^*$ P^O (NP^O) – всі мови ДМТ (НДМТ) з оракулом O

Твердження

1. $\overline{SAT} \in P^{SAT}$;
2. $O \in P$, $P^O = P$;
3. $EXPCOM = \{(M, x, 1^n) \mid M(x) = 1$ за $\leq 2^n$ тактів $\}$
   $P^{EXPCOM} = NP^{EXPCOM} = EXP$

Доведення.

1. інша відповідь;
2. моделювання роботи оракула;
3. $EXP \subseteq P^{EXPCOM}$ запит до оракула $(M, x, 1^{n^c})$
   $P^{EXPCOM} \subseteq NP^{EXPCOM}$
   $NP^{EXPCOM} \subseteq EXP$ моделювання НДМТ з усіма відповідями оракула

□

Теорема Бейкера-Джіла-Соловея

Теорема Бейкера-Джіла-Соловея

$\exists A, B$ — оракули такі, що $P^A = NP^A$ і $P^B \neq NP^B$.

Доведення.

$A = EXPCOM$

$\forall B \subseteq \{0,1\}^*$ унарна мова — $U_B = \{1^n, \exists x \in B, |x| = n\}$

$\forall B \subseteq \{0,1\}^*$ $U_B \in NP^B$

Побудуємо таку мову B, щоб $U_B \notin P^B$:

кожна ДМТ M_i^B має двійкове представлення i

покроково додаємо слова в мову B індукцією за i, щоб M_i^B не могла розв'язати U_B за час $\frac{2^n}{10}$

обираємо довжину більшу за всі довжини запитів

про вже визначені слова відповідаємо чесно

про нові слова відповідаємо 'ні'

перебрати всі слова з довжиною n за час $\frac{2^n}{10}$ неможливо $\square$