理論計算機科学特論 (2026 年前学期)

計算複雑性の基礎

第 7 回

Ladner の定理：$\mathrm{NP} - \mathrm{P} = \mathrm{NPC} \Rightarrow \mathrm{P} = \mathrm{NP}$

岡本 吉央　(電気通信大学)

okamotoy@uec.ac.jp

2026 年 5 月 26 日

最終更新：2026 年 5 月 26 日　11:41

スケジュール (前半)

1. 計算理論の復習 (4/7)
2. 時間計算量：P, NP, coNP (4/14)
3. 帰着と完全性：NP 完全 (4/21)
4. 領域計算量：L, NL, PSPACE (4/28)

* 休み (祝日) (5/5)

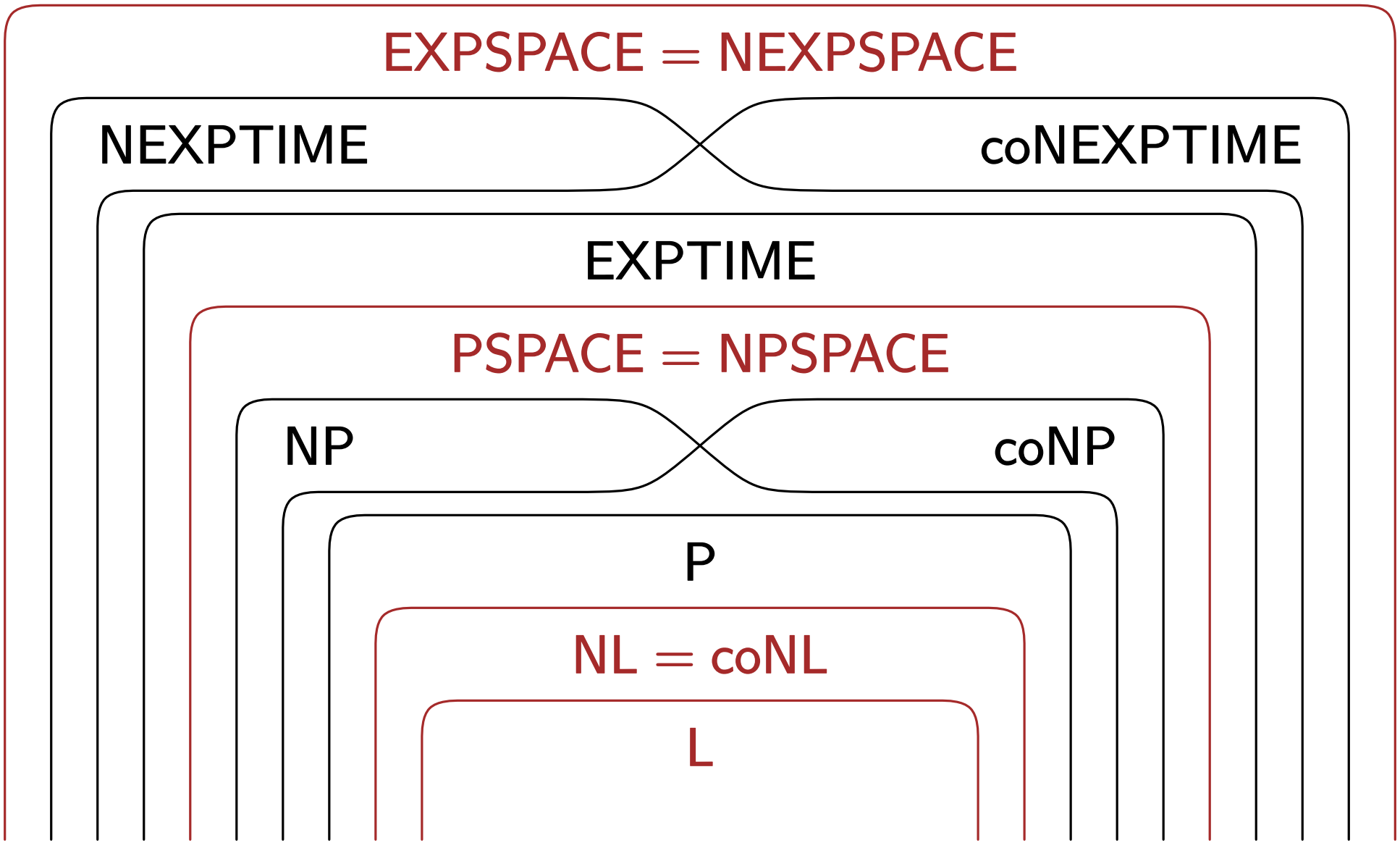
5. 時間と領域の関係：$P \subseteq PSPACE \subseteq EXPTIME$ (5/12)
6. 階層定理：$P \neq EXPTIME$ (5/19)
7. **Ladner の定理：** $NP - P = NPC \Rightarrow P = NP$ (5/26)

スケジュール (後半)

8. Savitch の定理：PSPACE = NPSPACE (6/2)
9. Immerman-Szlepcsényi の定理：NL = coNL (6/9)
10. 多項式階層：$P = NP \Rightarrow P = PH$ (6/16)
11. 交代性計算：AP = PSPACE (6/23)
12. 確率的計算：$P \subseteq BPP \subseteq PP$, $NP \subseteq PP$ (6/30)
13. 対話証明系 (1)：$NP \subseteq MA \subseteq AM$ (7/7)
14. 対話証明系 (2)：$IP \subseteq PSPACE$ (7/14)
15. 対話証明系 (3)：$PSPACE \subseteq IP$ (7/21)

* 休み (授業のない日) (7/28)

復習：時間計算量と領域計算量



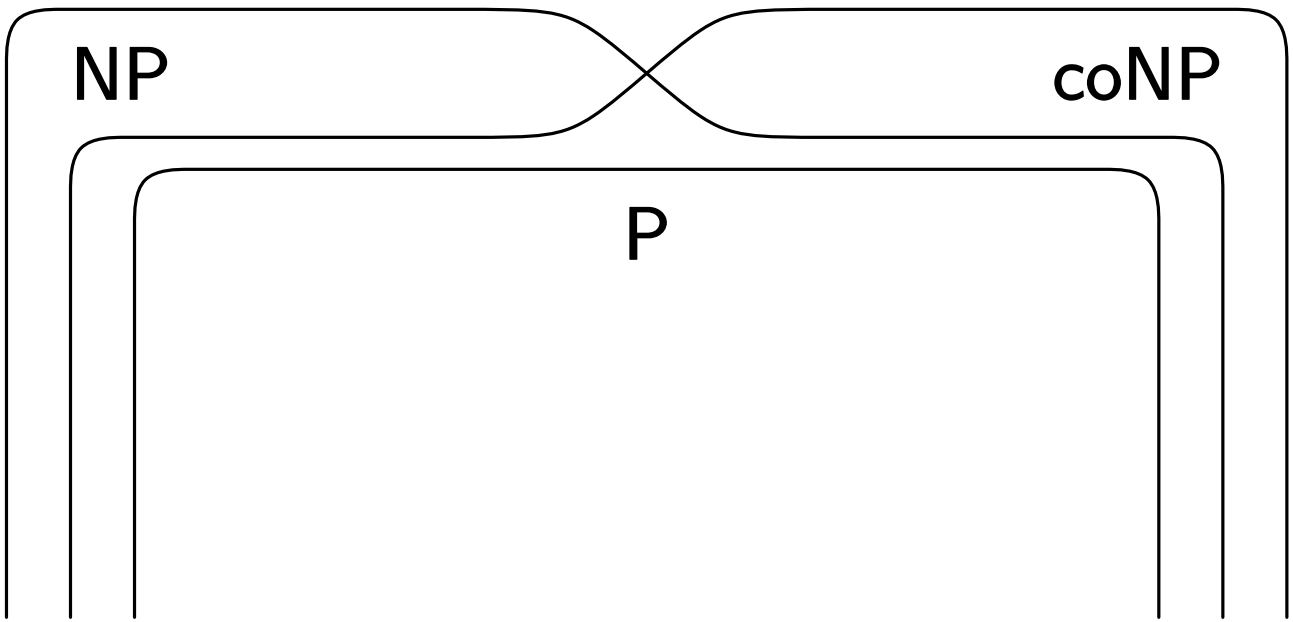
黒は時間複雑性クラス，茶は領域複雑性クラス

復習：P vs NP 問題

未解決問題

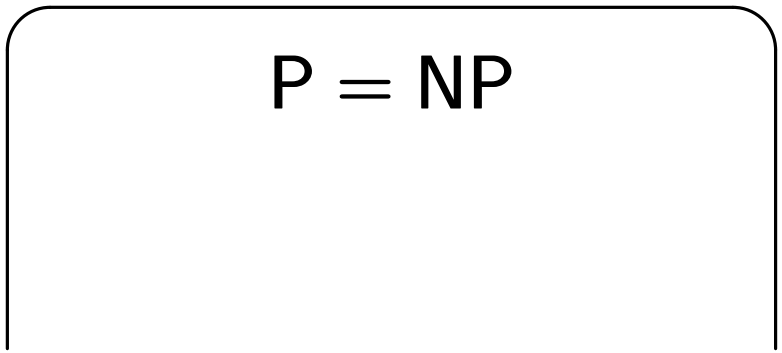
- $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$
- $\mathrm{P} \stackrel{?}{=} \mathrm{coNP}$
- $\mathrm{P} \stackrel{?}{=} \mathrm{NP} \cap \mathrm{coNP}$

性質：$\mathrm{P} = \mathrm{NP} \Leftrightarrow \mathrm{P} = \mathrm{coNP}$

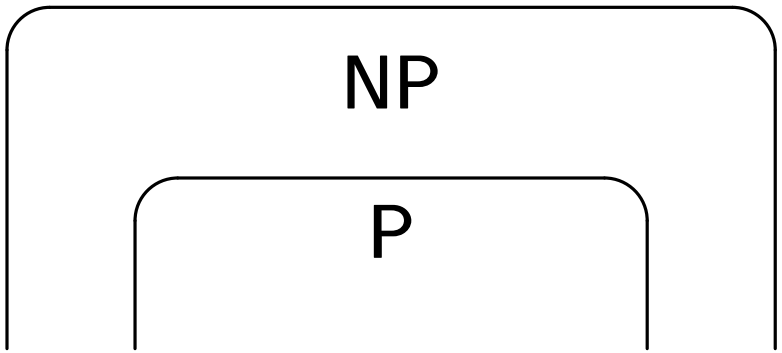


P = NP か P ≠ NP か

P = NP ならば

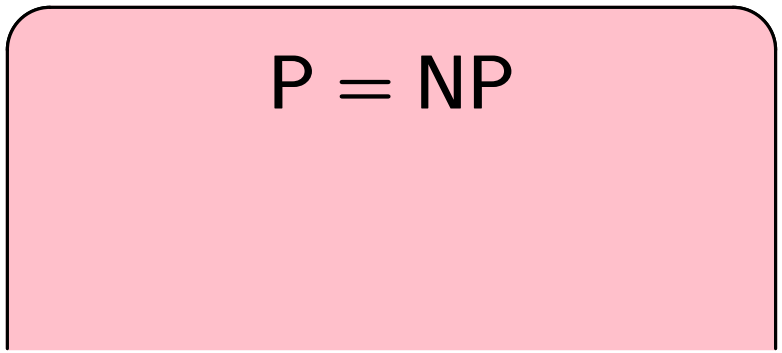


P ≠ NP ならば



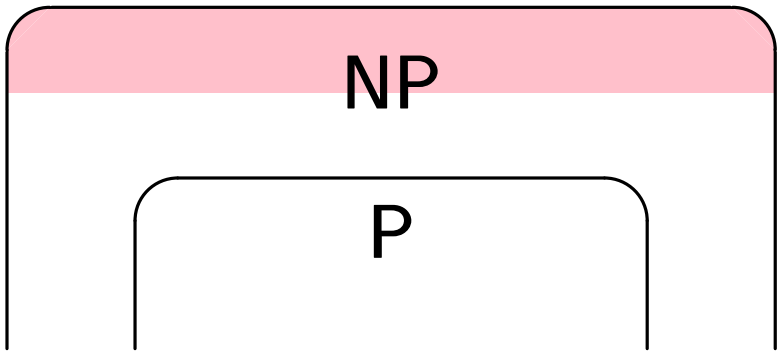
P = NP か P ≠ NP か

P = NP ならば



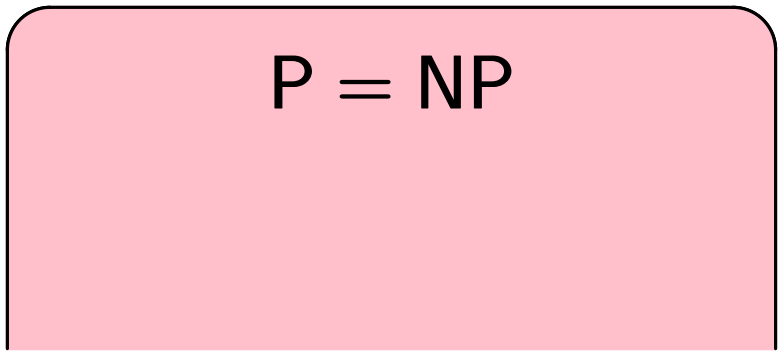
P ≠ NP ならば

NP 完全



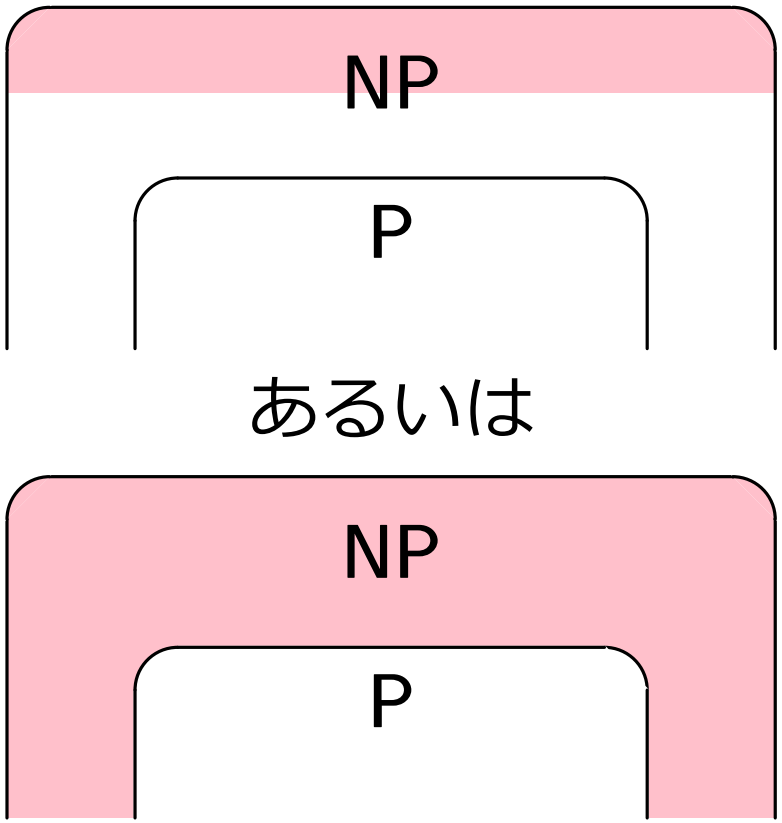
P = NP か P ≠ NP か

P = NP ならば



P ≠ NP ならば

NP 完全



注：P ≠ NP かつ $P \in$ P $\Rightarrow$ P は NP 完全ではない

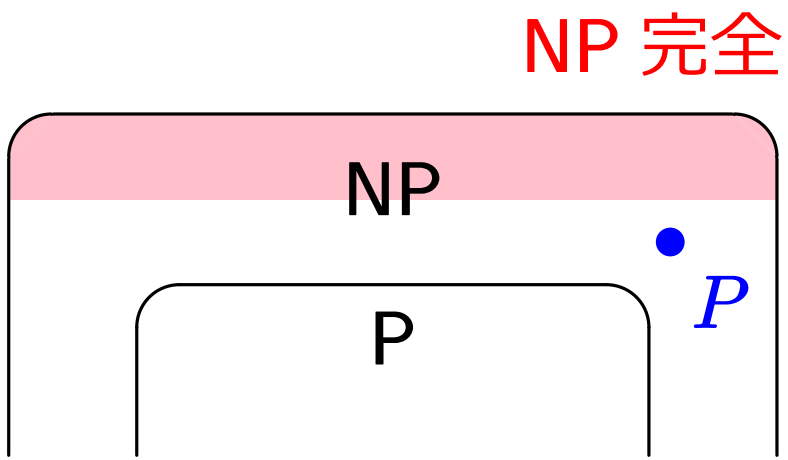
Ladner の定理

性質：Ladner の定理 (Ladner '75)

P $\neq$ NP $\Rightarrow$

次をすべて満たす判定問題 P が存在する

- $P \in$ NP
- $P \notin$ P
- P は NP 完全ではない



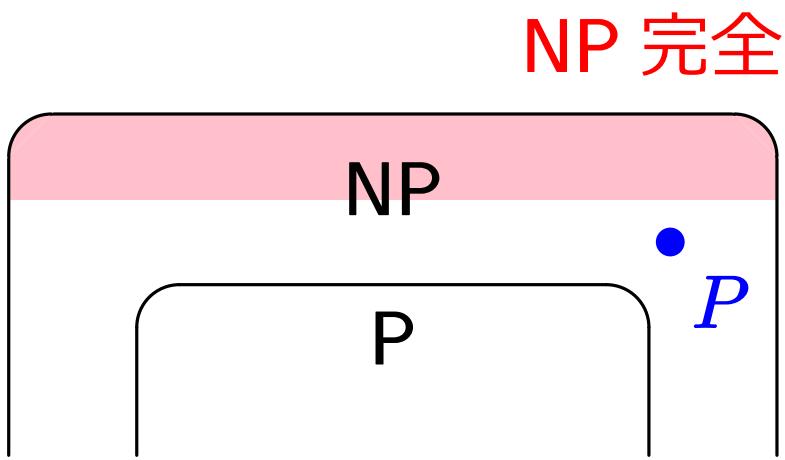
NP 中間問題

定義：NP 中間問題

判定問題 P が **NP 中間** (NP-intermediate) であるとは
$P \in \mathrm{NP} - \mathrm{P}$ であり，P が NP 完全ではないこと

Ladner の定理 は次と同値

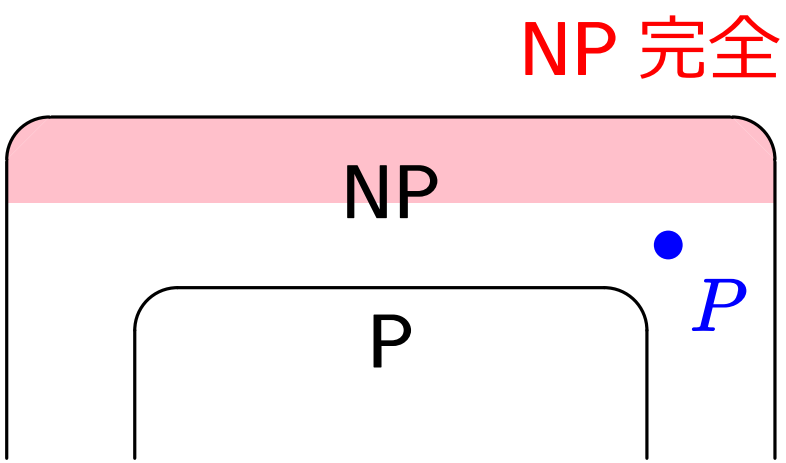
- $\mathrm{P} \neq \mathrm{NP} \Rightarrow$ NP 中間問題が存在する



本日の内容

目標

- Ladner の定理を証明する
- NP 中間問題の候補を紹介する



本日の内容

1. **Ladner の定理の証明：概要**
2. Ladner の定理の証明：詳細
3. NP 中間問題の候補

再掲：Ladner の定理

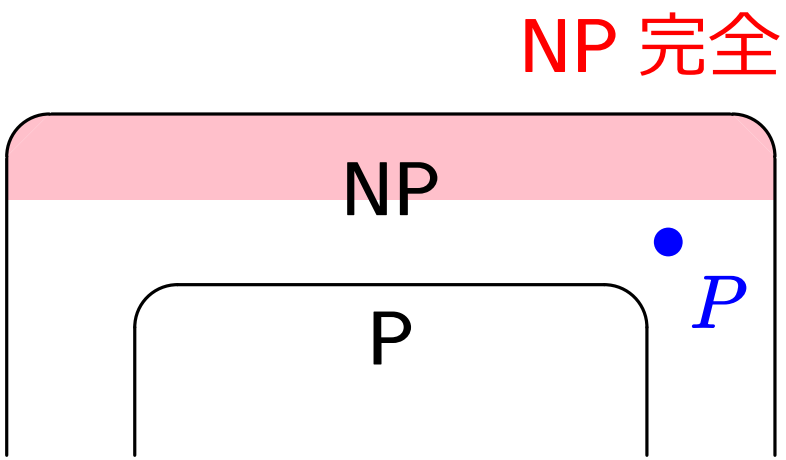
性質：Ladner の定理 (Ladner '75)

P $\neq$ NP $\Rightarrow$

次をすべて満たす判定問題 P が存在する

- $P \in$ NP
- $P \notin$ P
- P は NP 完全ではない

紹介する証明は
Downey, Fortnow ('03) の論文に
書いてあるが，もともとは
Impagliazzo が考案したらしい



以下，証明では常に「P $\neq$ NP」を仮定する

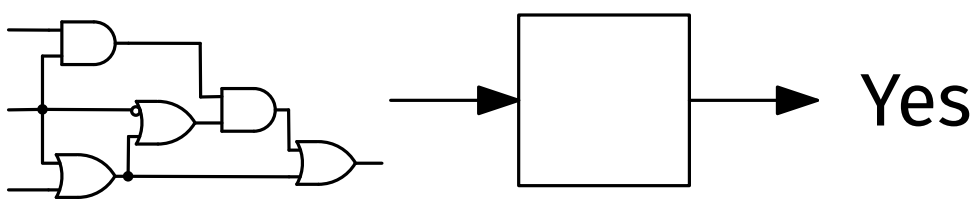
復習：論理回路の充足可能性問題

次の NP 完全問題を考える

論理回路の充足可能性問題 (CIRCUIT-SAT)

入力： 論理回路 C
出力： C が充足割当を持つ $\Rightarrow$ Yes
C が充足割当を持たない $\Rightarrow$ No

充足可能性問題 $=$ Satisfiability Problem



定義：充足割当 (satisfying assignment)

論理回路 $C(x)$ に対する割当 α が **充足割当** であるとは
$C(\alpha) = 1$ であること

水増し充足可能性問題

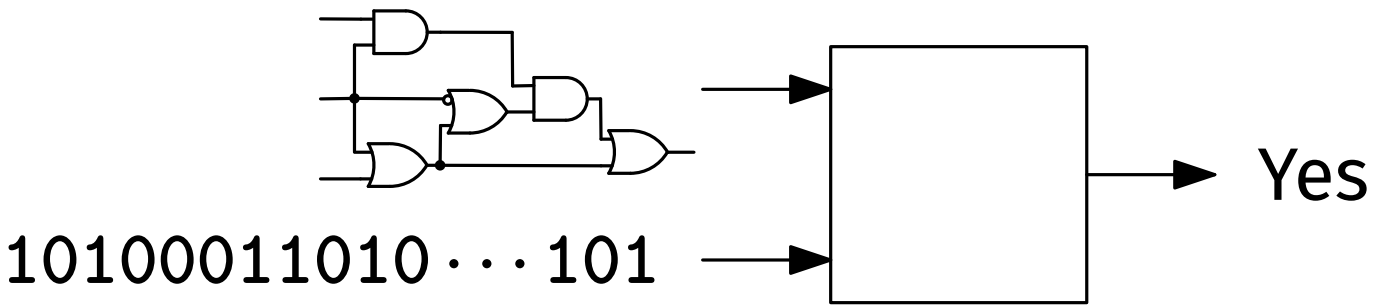
関数 $h\colon \mathbb{N} \to \mathbb{N}$

(あとで定める；$h(n)$ は n の多項式時間で計算可能)

問題：水増し SAT

入力： 論理回路 C (符号長 $n = |C|$)
長さ $n^{h(n)}$ のビット列 b

出力： C が充足可能である $\Rightarrow$ Yes
C が充足可能でない $\Rightarrow$ No

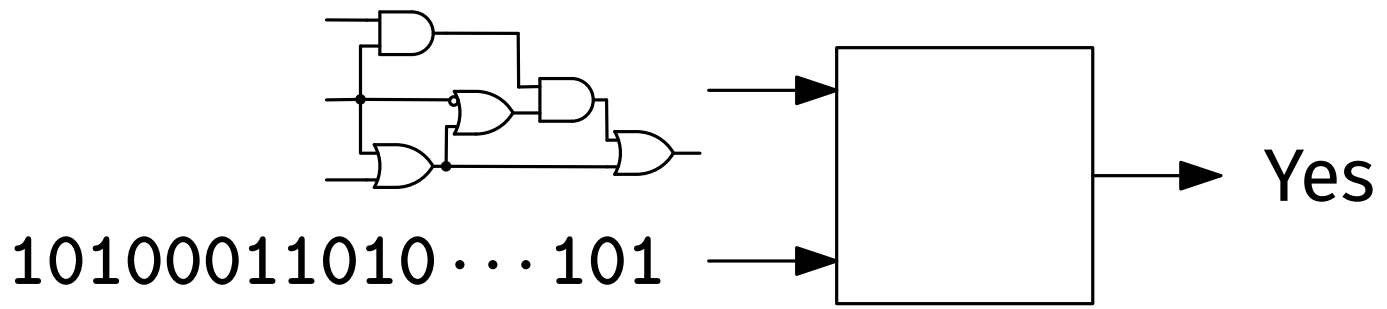


水増し充足可能性問題

関数 $h\colon \mathbb{N} \to \mathbb{N}$
(あとで定める；$h(n)$ は n の多項式時間で計算可能)

問題：水増し SAT

入力： 論理回路 C (符号長 $n = |C|$)
長さ $n^{h(n)}$ のビット列 b
出力： C が充足可能である $\Rightarrow$ Yes
C が充足可能でない $\Rightarrow$ No

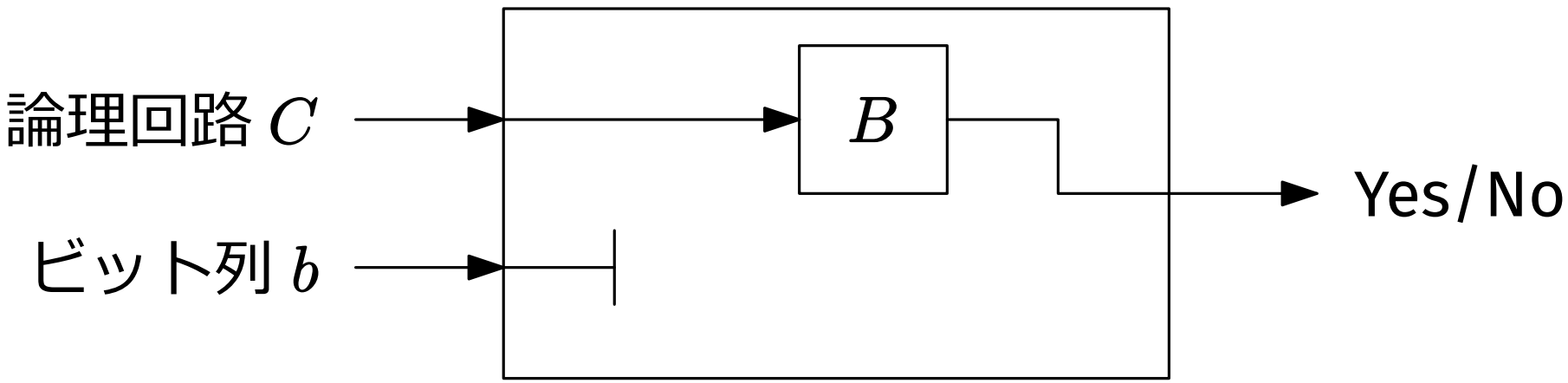


証明すること：(1) 水増し SAT $\in$ NP，(2) 水増し SAT $\notin$ P，
(3) 水増し SAT は NP 完全ではない

(1) 水増し SAT $\in$ NP

注：CIRCUIT-SAT は非決定性多項式時間で解ける

- B は CIRCUIT-SAT を解く非決定性多項式時間アルゴリズムだとする

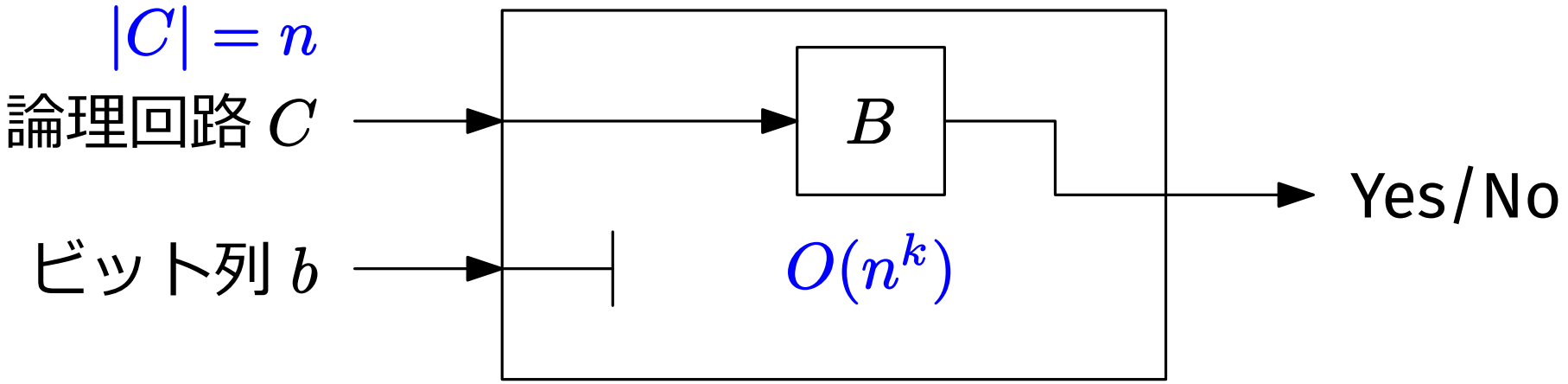


水増し SAT を解く非決定性アルゴリズム

(1) 水増し SAT $\in$ NP

注：CIRCUIT-SAT は非決定性多項式時間で解ける

- B は CIRCUIT-SAT を解く非決定性多項式時間アルゴリズムだとする



水増し SAT を解く非決定性アルゴリズム

- 時間計算量 $= O(n + n^{h(n)} + n^k) = O((n + n^{h(n)})^k)$
- $\therefore$ 非決定性多項式時間アルゴリズム

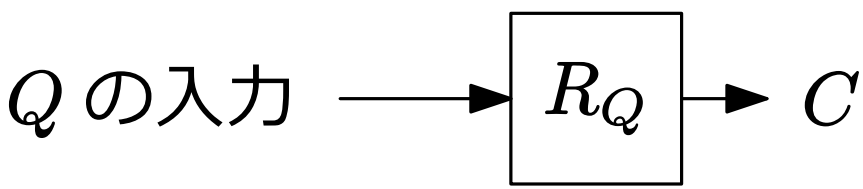
(2)？ 水増し SAT $\notin$ P

仮定

h が有界　　(∃ 定数 $u \in \mathbb{N}$, $h(n) \leq u$)

主張：水増し SAT は NP 完全　　($\because$ P $\neq$ NP $\Rightarrow$ 水増し SAT $\notin$ P)

- CIRCUIT-SAT は NP 完全なので，
  任意の問題 $Q \in$ NP に対して，
  Q から CIRCUIT-SAT への多項式時間帰着 R_Q が存在



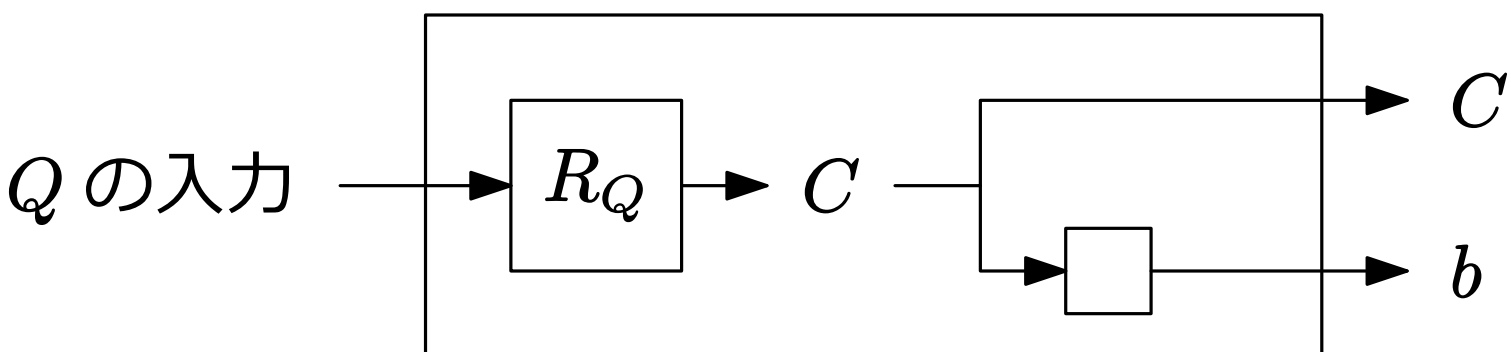
(2)？ 水増し SAT $\notin$ P

仮定

h が有界　　(∃ 定数 $u \in \mathbb{N}$, $h(n) \leq u$)

主張：水増し SAT は NP 完全　　($\because$ P $\neq$ NP $\Rightarrow$ 水増し SAT $\notin$ P)

- CIRCUIT-SAT は NP 完全なので，
  任意の問題 $Q \in$ NP に対して，
  Q から CIRCUIT-SAT への多項式時間帰着 R_Q が存在



(長さ $\leq |C|^u$)

- これは Q から水増し SAT への多項式時間帰着

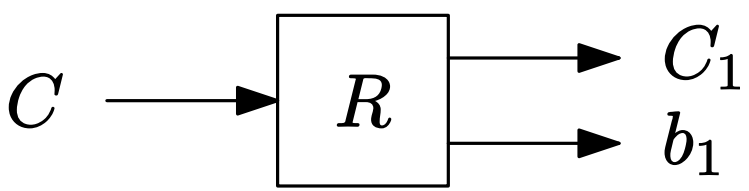
(3)？ 水増し SAT は NP 完全ではない

仮定

h は非有界

主張：P $\neq$ NP $\Rightarrow$ 水増し SAT は NP 完全ではない

- 水増し SAT が NP 完全だと仮定すると
  CIRCUIT-SAT から水増し SAT への多項式時間帰着 R が存在



(符号長 $= |C_1|^{h(|C_1|)}$)

- R が多項式時間帰着なので,
  出力の符号長 $= O(|C_1| + |C_1|^{h(|C_1|)}) = O(|C|^k)$
  (k は定数)

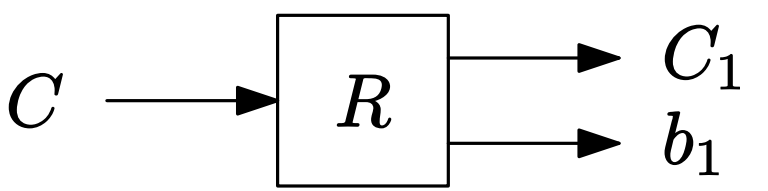
(3)？ 水増し SAT は NP 完全ではない

仮定

h は非有界

主張：P $\neq$ NP $\Rightarrow$ 水増し SAT は NP 完全ではない

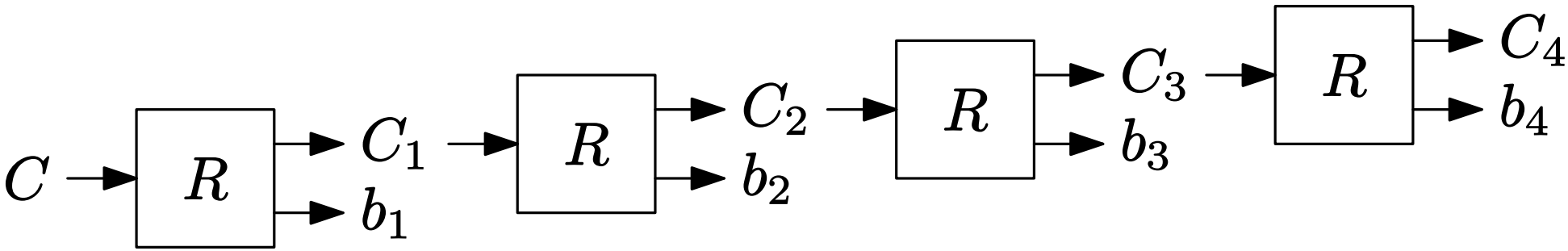
- 水増し SAT が NP 完全だと仮定すると
  CIRCUIT-SAT から水増し SAT への多項式時間帰着 R が存在



(符号長 $= |C_1|^{h(|C_1|)}$)

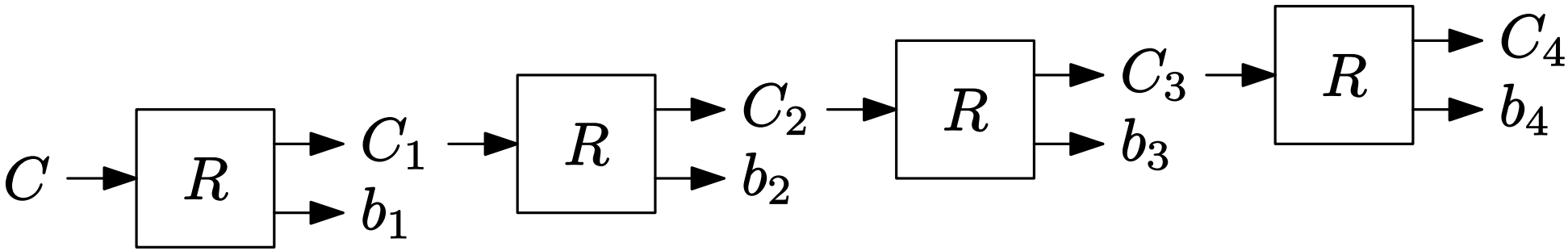
- R が多項式時間帰着なので,
  出力の符号長 $= O(|C_1| + |C_1|^{h(|C_1|)}) = O(|C|^k)$
  (k は定数)
- $\therefore |C_1| = o(|C|)$　($|C_1|$ のオーダーは $|C|$ より真に小さい)

(3)？ 水増し SAT は NP 完全ではない 続



$|C_1| = o(|C|)$ $|C_2| = o(|C_1|)$ $|C_3| = o(|C_2|)$

(3)？ 水増し SAT は NP 完全ではない 続



$$|C_1| = o(|C|) \qquad |C_2| = o(|C_1|) \qquad |C_3| = o(|C_2|)$$

- これを多項式回繰り返すと，回路の符号長が定数になる
  - 例えば，$|C_{i+1}| \leq \frac{1}{2}|C_i|$ となっているとすると，

$$N = \log_2 |C| \Rightarrow |C_N| \leq \frac{1}{2}|C_{N-1}| \leq \cdots \leq \frac{1}{2^N}|C| = 1$$

- つまり，CIRCUIT-SAT は多項式時間で解ける
- 仮定 P $\neq$ NP と CIRCUIT-SAT の NP 完全性に矛盾

ここまでのまとめ

問題：水増し SAT

入力： 論理回路 C (符号長 $n = |C|$)
長さ $n^{h(n)}$ のビット列 b

出力： C が充足可能である $\Rightarrow$ Yes
C が充足可能でない $\Rightarrow$ No

P $\neq$ NP $\Rightarrow$

(1) 水増し SAT $\in$ NP

(2) 水増し SAT $\notin$ P　　(仮定：h は有界)

(3) 水増し SAT は NP 完全ではない　　(仮定：h は非有界)

ここまでのまとめ

問題：水増し SAT

入力： 論理回路 C (符号長 $n = |C|$)
長さ $n^{h(n)}$ のビット列 b

出力： C が充足可能である $\Rightarrow$ Yes
C が充足可能でない $\Rightarrow$ No

P $\neq$ NP $\Rightarrow$

(1) 水増し SAT $\in$ NP　　両立しない (証明は不完全)

(2) 水増し SAT $\notin$ P　　(仮定：h は有界)

(3) 水増し SAT は NP 完全ではない　　(仮定：h は非有界)

ここまでのまとめ

問題：水増し SAT

入力： 論理回路 C (符号長 $n = |C|$)
長さ $n^{h(n)}$ のビット列 b

出力： C が充足可能である $\Rightarrow$ Yes
C が充足可能でない $\Rightarrow$ No

P $\neq$ NP $\Rightarrow$

(1) 水増し SAT $\in$ NP　　両立しない (証明は不完全)

(2) 水増し SAT $\notin$ P　　(仮定：h は有界)

(3) 水増し SAT は NP 完全ではない　　(仮定：h は非有界)

解決策 h をとてもとてもゆっくりと増加する関数にする

本日の内容

1. Ladner の定理の証明：概要
2. **Ladner の定理の証明：詳細**
3. NP 中間問題の候補

hの定義

クラス P に属するすべての問題に対する

すべての多項式時間アルゴリズムの列挙

$$A_1 \quad A_2 \quad A_3 \quad A_4 \quad \cdots$$

h の定義

クラス P に属するすべての問題に対する

すべての多項式時間アルゴリズムの列挙

$$A_1 \quad A_2 \quad A_3 \quad A_4 \quad \cdots \qquad\qquad A_{\log_2 \log_2 n}$$

$h(n) = \min \{ i \leq \log_2 \log_2 n \mid$

A_i は $|I| \leq \log_2 n$ であるすべての入力 I に対して
水増し SAT を $O(|I|^i)$ 時間で解く $\}$

そのような $i \leq \log_2 \log_2 n$ がない $\Rightarrow h(n) = \lfloor \log_2 \log_2 n \rfloor$

注：これは $h(n)$ を再帰的に定義している

$h(n)$ の計算

$A_1 \quad A_2 \quad A_3 \quad A_4 \quad \cdots \qquad\qquad A_{\log_2 \log_2 n}$

$$h(n) = \min \{ i \leq \log_2 \log_2 n \mid$$

A_i は $|I| \leq \log_2 n$ であるすべての入力 I に対して
水増し SAT を $O(|I|^i)$ 時間で解く $\}$

性質

$h(n)$ は n の多項式時間で計算できる

証明：アルゴリズムを与えればよい

1. 再帰的に $h(m)$ をすべての $m \leq \log_2 n$ に対して計算
2. $|I| \leq \log_2 n$ を満たすすべての入力 I を作成
3. 各 I を $A_1, \ldots, A_{\log_2 \log_2 n}$ で解いて，実行時間を記録

Ladner の定理の証明：補題 (1)

補題

水増し SAT $\in$ P $\quad\Leftrightarrow\quad$ h が有界

証明 ($\Rightarrow$)：水増し SAT $\in$ P と仮定

- 水増し SAT を多項式時間で解くアルゴリズム A が存在
- A は列挙の中にあるので，ある u に対して $A = A_u$
- $h(n)$ の定義より，$n > 2^{2^u}$ ならば $h(n) \leq \log_2 \log_2 n \leq u$
- $\therefore h$ は有界 $\square$

$$h(n) = \min \{ i \leq \log_2 \log_2 n \mid \left.\begin{array}{l} A_i \text{ は } |I| \leq \log_2 n \text{ であるすべての入力 } I \text{ に対して} \\ \text{水増し SAT を } O(|I|^i) \text{ 時間で解く} \end{array}\right\}$$

Ladner の定理の証明：補題 (2)

補題

水増し SAT $\in$ P　$\Leftrightarrow$　h が有界

証明 ($\Leftarrow$)：$h(n)$ が有界だと仮定

- h の取りうる値は有限なので，ある $i \in \mathbb{N}$ に対して $h(n) = i$ となる n が無限に存在
- $\therefore A_i$ は水増し SAT を多項式時間で解く　□

$$h(n) = \min \{ i \leq \log_2 \log_2 n \mid \begin{array}{l} A_i \text{ は } |I| \leq \log_2 n \text{ であるすべての入力 } I \text{ に対して} \\ \text{水増し SAT を } O(|I|^i) \text{ 時間で解く} \end{array} \}$$

Ladner の定理の証明：補題 (2)

補題

水増し SAT $\in$ P $\quad\Leftrightarrow\quad$ h が有界

証明 ($\Leftarrow$)：$h(n)$ が有界だと仮定

- h の取りうる値は有限なので，ある $i \in \mathbb{N}$ に対して $h(n) = i$ となる n が無限に存在
- $\therefore A_i$ は水増し SAT を多項式時間で解く $\square$

特に，水増し SAT $\notin$ P $\Rightarrow$ h は非有界 (無限に大きくなる)

$$h(n) = \min\{i \le \log_2 \log_2 n \mid \begin{array}{l} A_i \text{ は } |I| \le \log_2 n \text{ であるすべての入力 } I \text{ に対して} \\ \text{水増し SAT を } O(|I|^i) \text{ 時間で解く} \end{array} \}$$

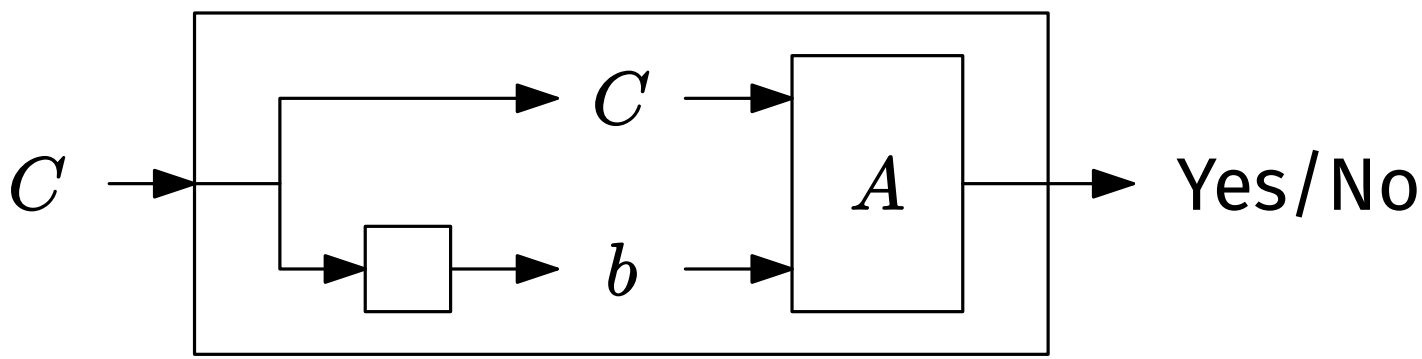
Ladner の証明：(2) 水増し SAT $\notin$ P

証明すべき性質 (2)

P $\neq$ NP $\Rightarrow$ 水増し SAT $\notin$ P

証明：水増し SAT $\in$ P と仮定

- 補題より，h は有界 ($\exists$ 定数 u, $h(n) \leq u$)
- A を水増し SAT の多項式時間アルゴリズムとする



SAT の多項式時間アルゴリズム　　注：$|b| \leq |C|^u$

- SAT の NP 完全性と P $\neq$ NP に矛盾　□

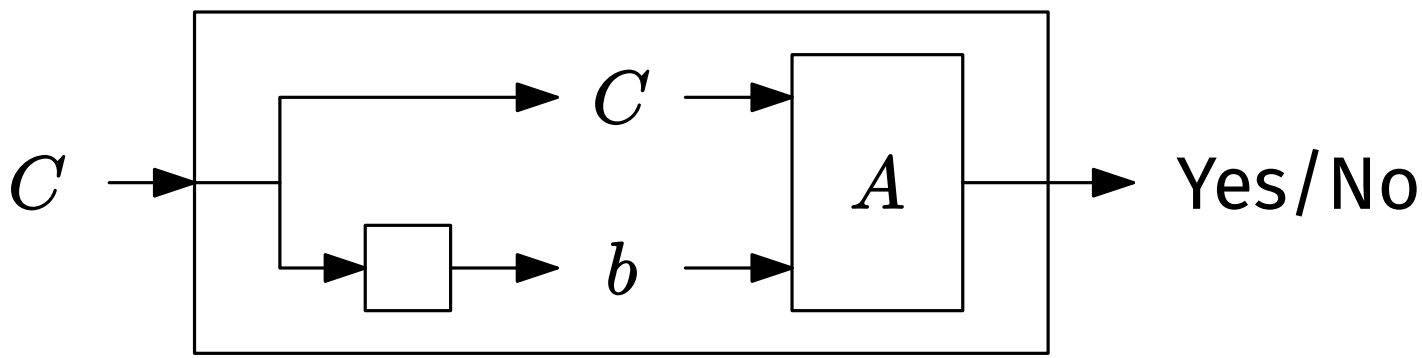
Ladner の証明：(2) 水増し SAT $\notin$ P

証明すべき性質 (2)

P $\neq$ NP $\Rightarrow$ 水増し SAT $\notin$ P

証明：水増し SAT $\in$ P と仮定

- 補題より，h は有界 ($\exists$ 定数 u, $h(n) \leq u$)
- A を水増し SAT の多項式時間アルゴリズムとする



SAT の多項式時間アルゴリズム　　注：$|b| \leq |C|^u$

- SAT の NP 完全性と P $\neq$ NP に矛盾　□

帰結 (補題より)：$h(n)$ は非有界 (無限に大きくなる)

Ladner の証明：(3) NP 完全ではない

証明すべき性質 (3)

$P \neq NP \Rightarrow$ 水増し SAT は NP 完全ではない

証明：水増し SAT $\notin$ P なので，h は非有界

- $\therefore$ 水増し SAT が NP 完全でないことは 16–17 ページで証明済み

□

Ladner の定理：まとめ

性質：Ladner の定理 (Ladner '75)

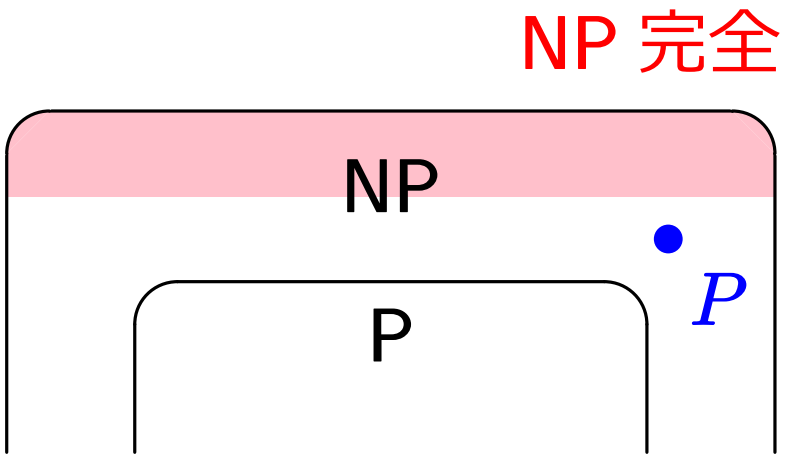
P $\neq$ NP $\Rightarrow$

次をすべて満たす判定問題 P が存在する

- $P \in$ NP
- $P \notin$ P
- P は NP 完全ではない

知られている証明

- Ladner による原証明
  対角線論法を使う
- Impagliazzo による証明
  水増し論法を使う



本日の内容

1. Ladner の定理の証明：概要
2. Ladner の定理の証明：詳細
3. NP **中間問題の候補**

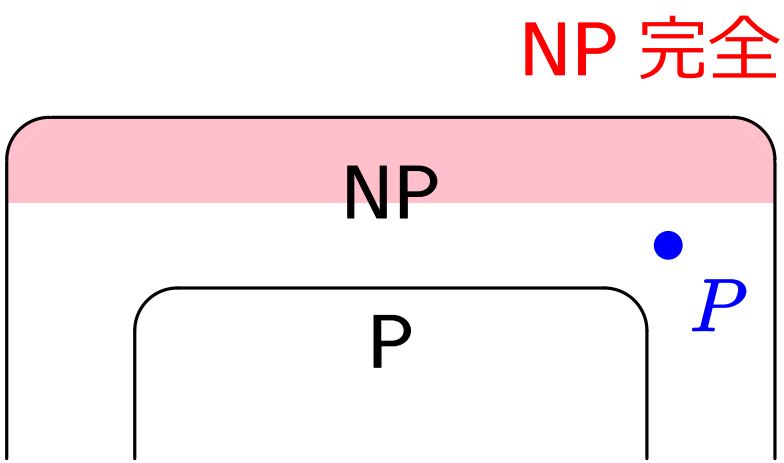
Ladner の定理と NP 中間問題

Ladner の定理は次と同値

$P \neq NP \Rightarrow$ NP 中間問題が存在する

Ladner の定理の証明の帰結

- $P \neq NP \Rightarrow$
  水増し SAT は NP 中間



疑問

- 自然な NP 中間問題はあるか？
  (水増し SAT は かなり人工的)

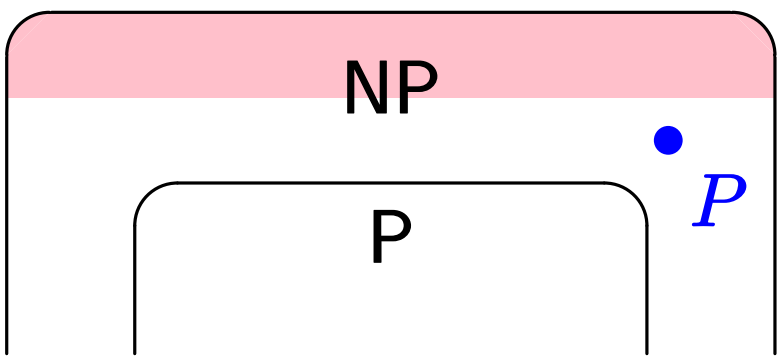
Ladner の定理と NP 中間問題

Ladner の定理は次と同値

$P \neq NP \Rightarrow$ NP 中間問題が存在する

Ladner の定理の証明の帰結

- $P \neq NP \Rightarrow$
  水増し SAT は NP 中間



疑問

- 自然な NP 中間問題はあるか？
  (水増し SAT は かなり人工的)

現状

- 自然な NP 中間問題は知られていない
- しかし，自然な NP 中間問題の候補はある

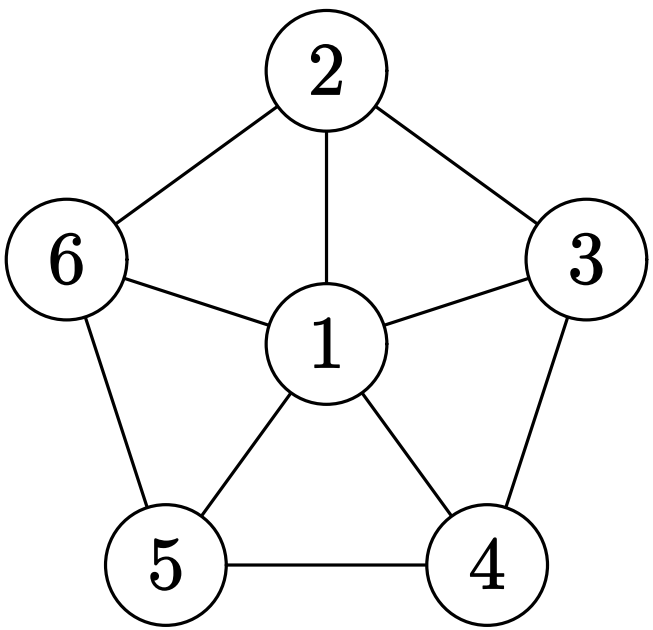
グラフの同型写像

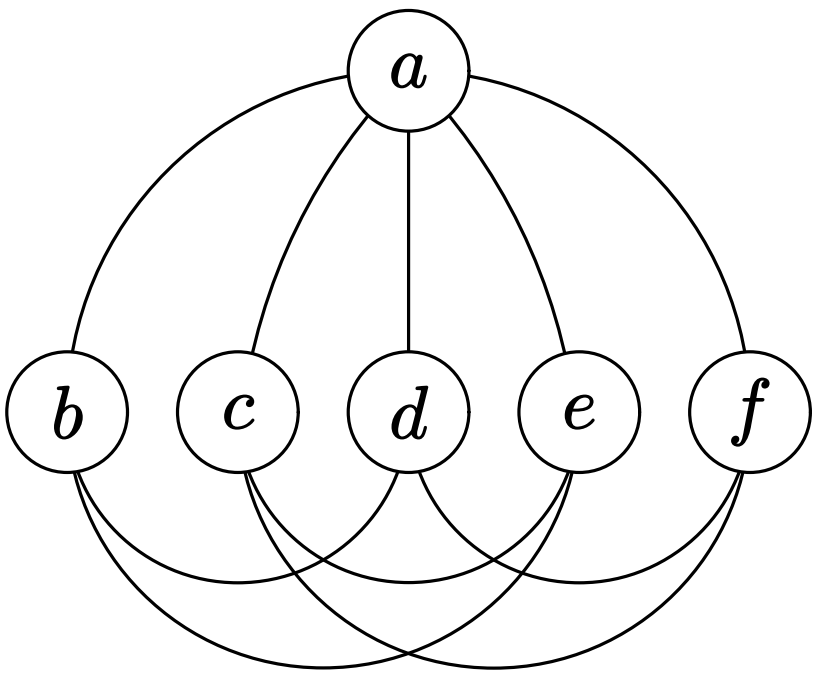
無向グラフ $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

定義：グラフの同型写像 (graph isomorphism)

G_1 から G_2 への **同型写像** とは，
全単射 $\varphi\colon V_1 \to V_2$ で次を満たすもの

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{\varphi(u), \varphi(v)\} \in E_2$$





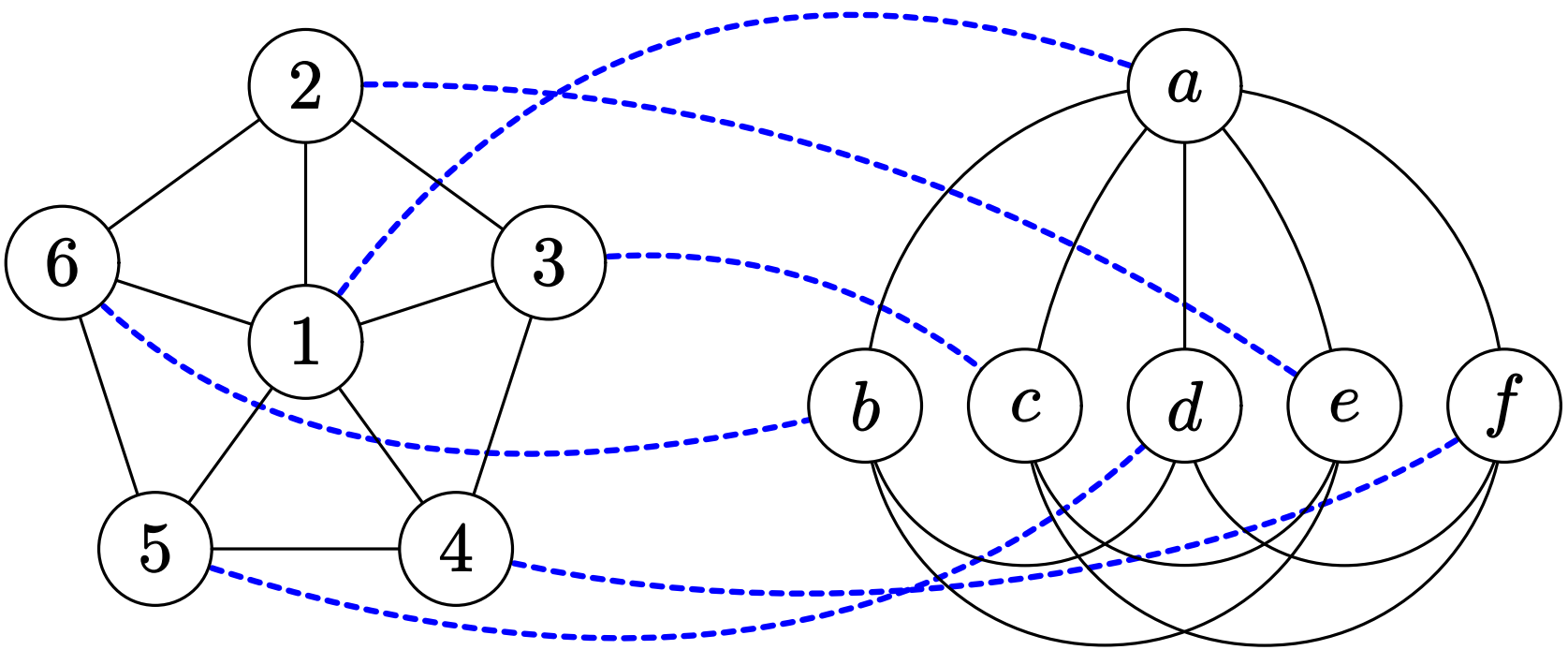
グラフの同型写像

無向グラフ $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

定義：グラフの同型写像 (graph isomorphism)

G_1 から G_2 への **同型写像** とは，
全単射 $\varphi\colon V_1 \to V_2$ で次を満たすもの

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{\varphi(u), \varphi(v)\} \in E_2$$



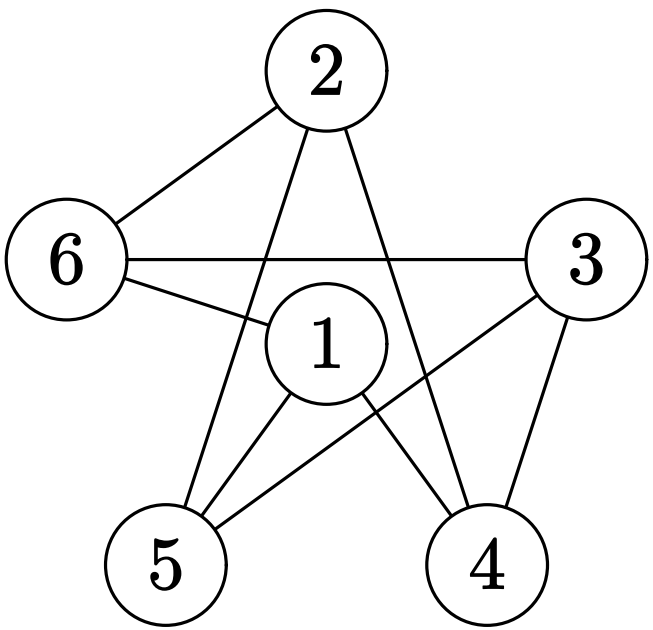
グラフの同型写像：例

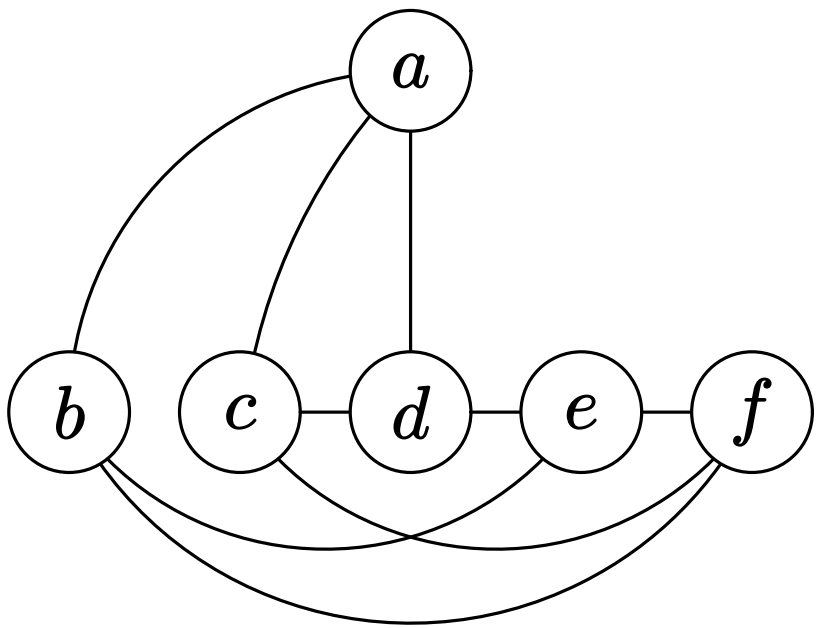
無向グラフ $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

定義：グラフの同型写像 (graph isomorphism)

G_1 から G_2 への **同型写像** とは，
全単射 $\varphi\colon V_1 \to V_2$ で次を満たすもの

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{\varphi(u), \varphi(v)\} \in E_2$$





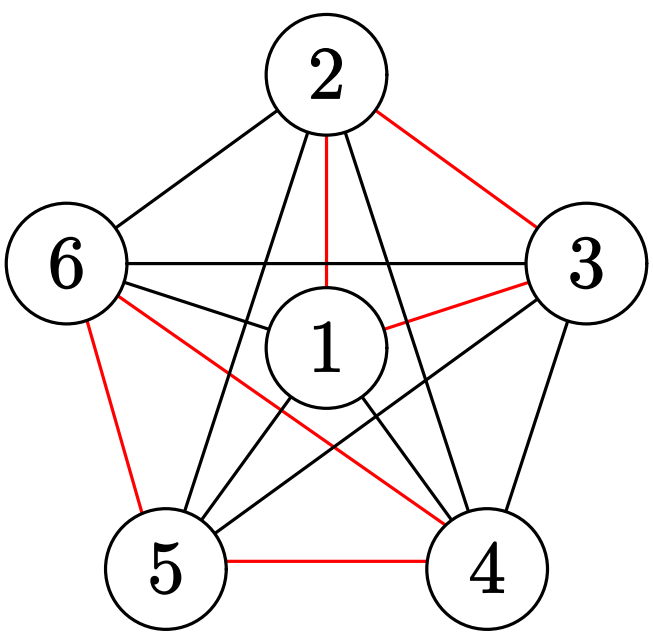
グラフの同型写像：例

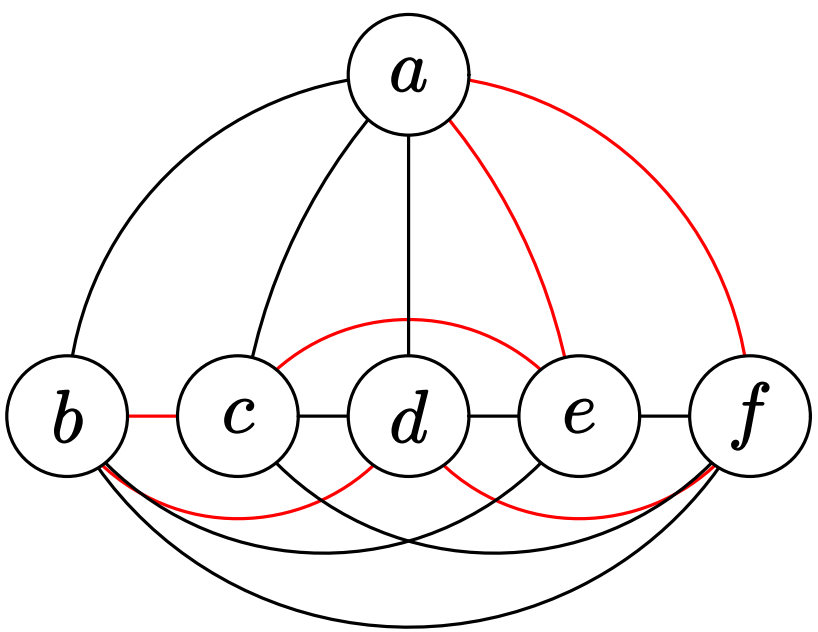
無向グラフ $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

定義：グラフの同型写像 (graph isomorphism)

G_1 から G_2 への **同型写像** とは，
全単射 $\varphi\colon V_1 \to V_2$ で次を満たすもの

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{\varphi(u), \varphi(v)\} \in E_2$$





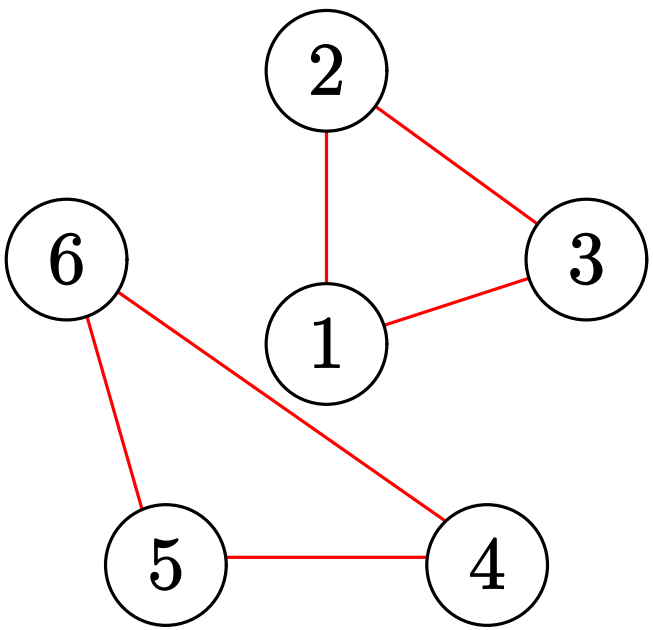
グラフの同型写像：例

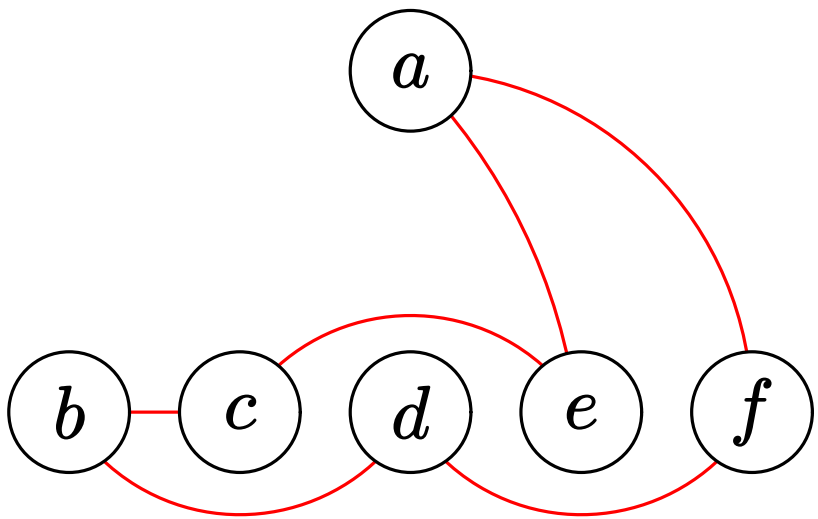
無向グラフ $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

定義：グラフの同型写像 (graph isomorphism)

G_1 から G_2 への **同型写像** とは，
全単射 $\varphi\colon V_1 \to V_2$ で次を満たすもの

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{\varphi(u), \varphi(v)\} \in E_2$$

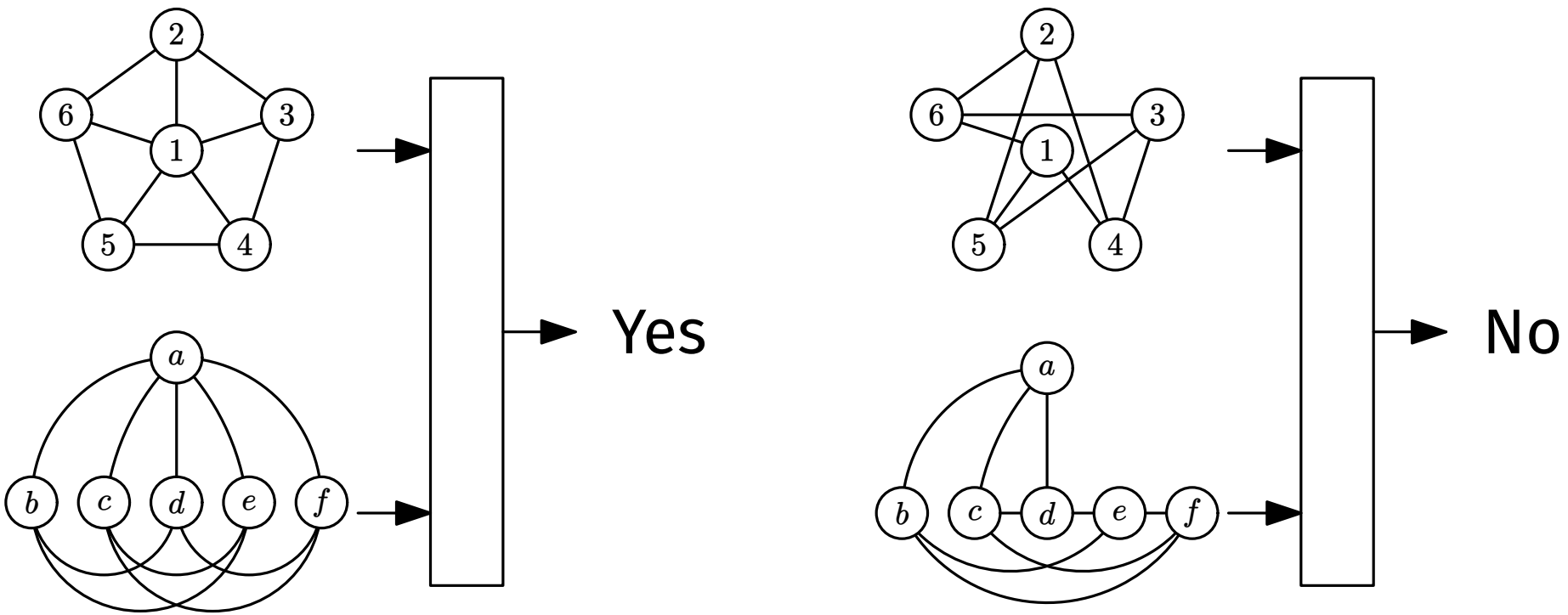




グラフ同型性問題

問題：グラフ同型性問題 (graph isomorphism problem)

入力： 無向グラフ G_1, G_2
出力： G_1 から G_2 への同型写像がある ⇒ Yes
G_1 から G_2 への同型写像がない ⇒ No



グラフ同型性問題について

問題：グラフ同型性問題 (graph isomorphism problem)

入力： 無向グラフ G_1, G_2
出力： G_1 から G_2 への同型写像がある $\Rightarrow$ Yes
G_1 から G_2 への同型写像がない $\Rightarrow$ No

知られていること

- グラフ同型性問題 $\in$ NP (次ページ)

未解決問題

- グラフ同型性問題は NP 完全？
- グラフ同型性問題 $\overset{?}{\in}$ P

グラフ同型性問題は NP 中間問題の有力な候補

グラフ同型性問題 $\in$ NP

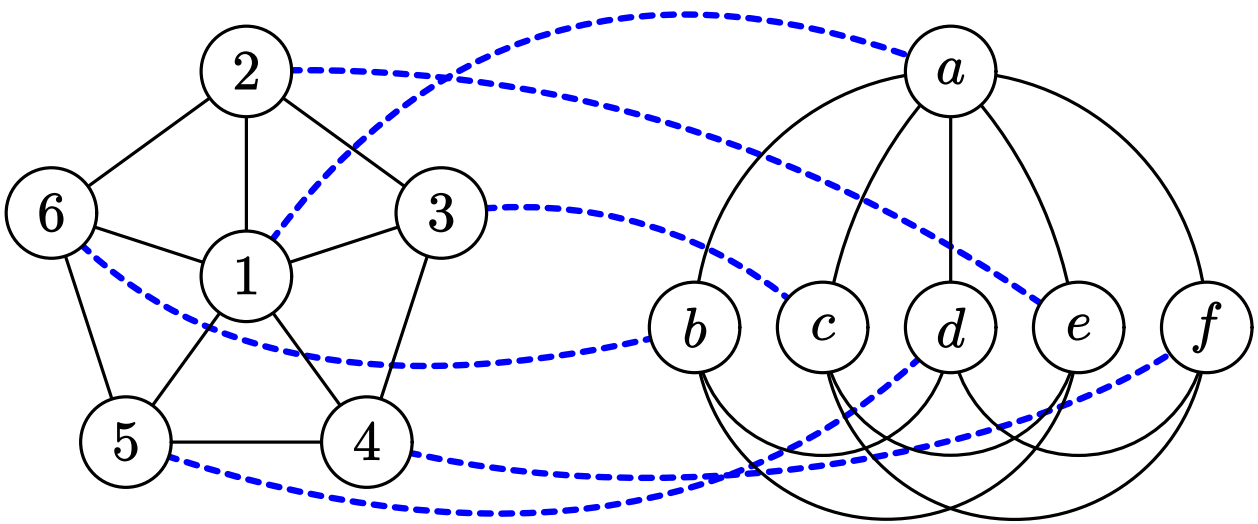
性質：グラフ同型性問題と非決定性

グラフ同型性問題 $\in$ NP

証明：次は非決定性多項式時間アルゴリズム

1. 同型写像 φ を guess
2. φ が同型写像であることを確認

□



グラフ同型性問題に関する事実

未解決問題

- グラフ同型性問題は NP 完全？
- グラフ同型性問題 $\overset{?}{\in}$ P

知られていること

- グラフ同型性問題 $\in$ NP (前ページ)
- グラフ同型性問題が NP 完全
  $\Rightarrow \Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$ (Boppana, Hastad, Zachos '87)
- グラフ同型性問題とグラフの同型写像の数え上げ問題は多項式時間同値 (Mathon '79)
- グラフ同型性問題は $\exp(O(\log n)^{O(1)})$ 時間で解ける (Babai '17+)

グラフ同型性問題に関する事実

未解決問題

- グラフ同型性問題は NP 完全？
- グラフ同型性問題 $\overset{?}{\in}$ P

知られていること

- グラフ同型性問題 $\in$ NP (前ページ)

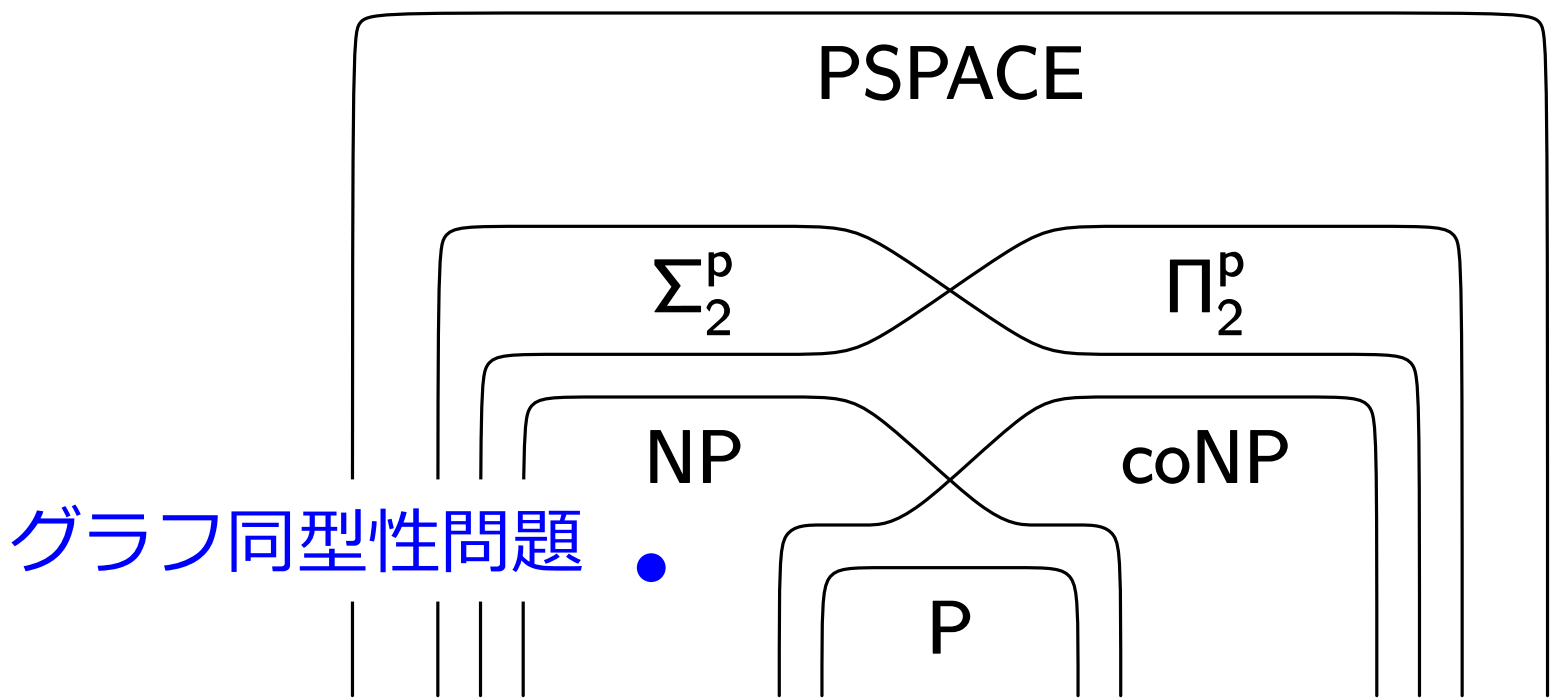
NP 完全ではないことの示唆

- グラフ同型性問題が NP 完全 $\Rightarrow \Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$ (Boppana, Hastad, Zachos '87)
- グラフ同型性問題とグラフの同型写像の数え上げ問題は多項式時間同値 (Mathon '79)
- グラフ同型性問題は $\exp(O(\log n)^{O(1)})$ 時間で解ける (Babai '17+)

グラフ同型性問題に関する事実　続

知られていること

- グラフ同型性問題 $\in$ NP
- グラフ同型性問題が NP 完全
  $\Rightarrow \Sigma_2^p = \Pi_2^p$ (Boppana, Hastad, Zachos '87)



Σ_2^p, Π_2^p は第 10 回の授業で扱う予定

本日のまとめ

性質：Ladner の定理 (Ladner '75)

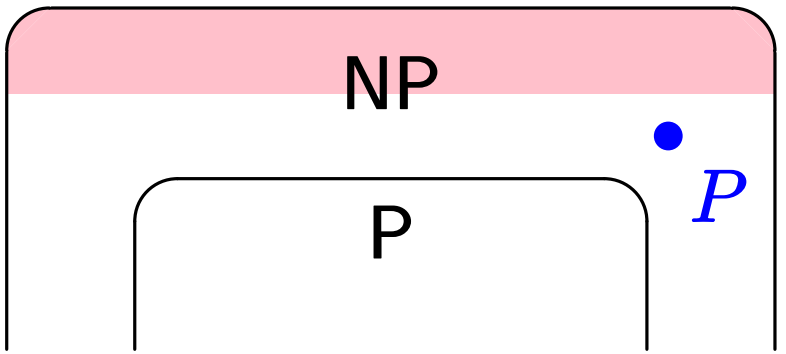
P $\neq$ NP $\Rightarrow$

次をすべて満たす判定問題 P が存在する

- $P \in$ NP
- $P \notin$ P
- P は NP 完全ではない

そのような P の候補

- グラフ同型性問題



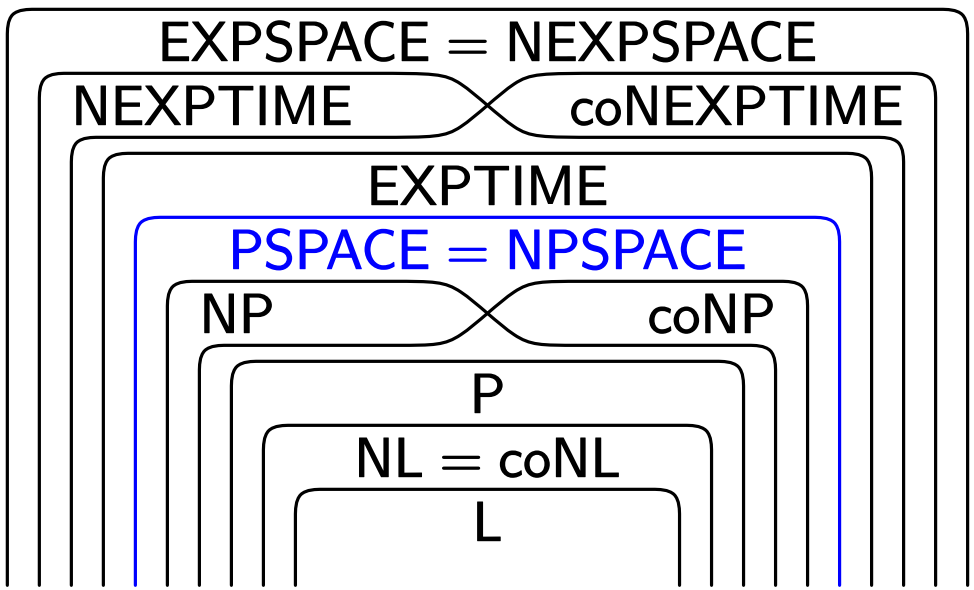
次回の予告

目標

次の「Savitch の定理」を証明する

- PSPACE = NPSPACE

そのために，NPSPACE 完全問題を 1 つ紹介する



クイズ

Q

1.

2.

3.

4.