



Tokyo Tech

離散構造とアルゴリズム (4-3) 問題の難しさ

高橋篤司

東京工業大学 工学院 情報通信系

4-3 (1) NPとP

■ アルゴリズム設計の理論的背景

➤ NP

- Nondeterministic Polynomial
 - 非決定性多項式
- 非決定性多項式時間アルゴリズムで解ける判定問題の集合

➤ P

- (Deterministic) Polynomial
 - (決定性)多項式
- (決定性)多項式時間アルゴリズムで解ける判定問題の集合

■ 解説書＋辞典

- Garey and Johnson, “Computers and Intractability,
A Guide to the Theory of NP-Completeness” ,
Freeman and Co., 1979

計算量理論のキーワード

- 計算複雑度(Computational Complexity)
 - 時間計算量
 - 空間計算量
- P, NP, NP完全(NP-complete)
 - 判定問題の特徴
- NP困難(NP-hard)
- 非決定性多項式時間アルゴリズム
 - Nondeterministic Polynomial Time Algorithm
- 多項式時間アルゴリズム
 - (Deterministic) Polynomial Time Algorithm
- 多項式時間還元 (Polynomial Time Reduction)

アルゴリズム

■ 決定性アルゴリズム

- 同一入力に対し, 出力は一意に定まる
 - 確率的アルゴリズム : 出力は一意に定まる
 - 乱数も入力の一部と考える

正当な
非決定性アルゴリズム

正解		出力
YES	↔	YES
No	↔	No

■ 非決定性アルゴリズム

- 同一入力に対し, 出力は異なることがある
- 判定問題を解く正当な非決定性アルゴリズム
 - 正解: Yes ⇒ 出力: YesまたはNo (常にNoはダメ)
 - 正解: No ⇒ 出力: No

非決定性アルゴリズム (Nondeterministic Algorithm)

- 判定問題(problem) $\Pi = (I, Q(x))$
 - 入力集合 I と質問 $Q(x)$ の組
- 答えが「Yes」か「No」である問題

■ Algorithm 4.2 (非決定性アルゴリズム)

- 入力: $s \in I$ (ただし $\Pi = (I, Q(x))$ は判定問題)
- 出力: 「Yes」or「No」

Step 1: (非決定性)

- Generate an evidence γ
(Pick up one arbitrary among exponential candidates)

Step 2: (決定性)

- Check the evidence γ
 - If the evidence is correct, then output YES
 - Otherwise, output NO

■ 非決定性多項式時間アルゴリズム

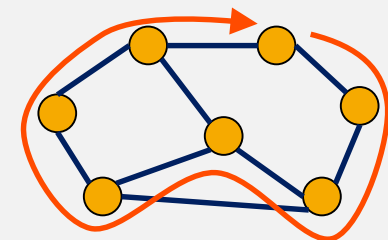
- 多項式時間で正当な出力
- Algorithm 4.2
 - Step 1: 証拠の生成が多項式時間
 - Step 2: 証拠の確認が多項式時間

正当な
非決定性アルゴリズム

正解	出力
YES	YES
No	No

問題: ハミルトングラフか?

証拠 γ : 点の順列



連結グラフ

■ 連結性判定問題(CON) (判定)

- 入力

■ グラフ G

- 質問

■ G は連結か?

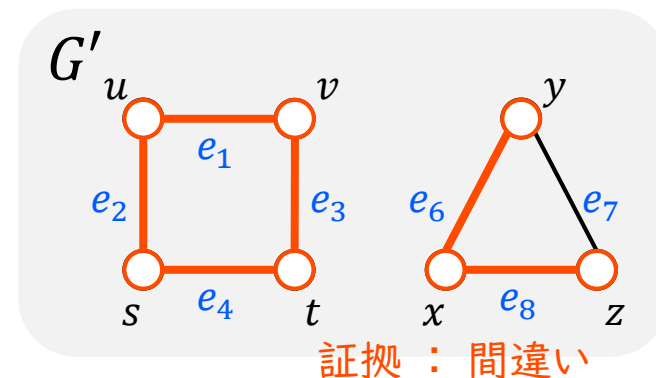
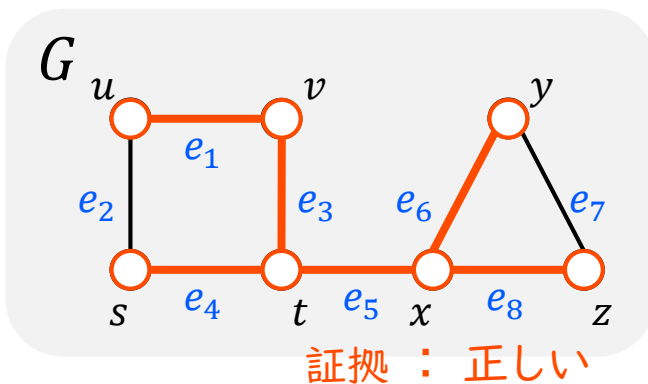
✓ 証拠の例

■ 点对間の路の集合, 全域木

$CON \in NP$

正当な
非決定性アルゴリズム

正解	出力
YES	YES
No	No



距離

■ 距離判定問題(DIS) (判定)

- 入力

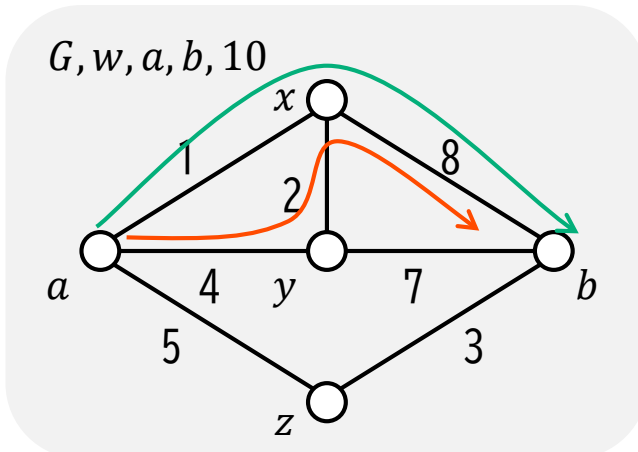
■ 連結グラフ G , 重み関数 $w: E(G) \rightarrow \mathbb{R}^+$, 2点 $u, v \in V(G)$, 非負実数 r

- 質問

■ $\text{dis}_{(G,w)}(u, v) \leq r$ か?

✓ 証拠の例

■ (G, w) の重み r 以下の (u, v) -路



9 証拠 : 正しい

14 証拠 : 間違い

$\text{DIS} \in \text{NP}$

正当な
非決定性アルゴリズム

正解	出力
YES	YES
No	No

グラフ同型

■ グラフ同型判定問題 (ISO) (判定)

ISO $\in$ NP

- 入力

■ グラフ G, H

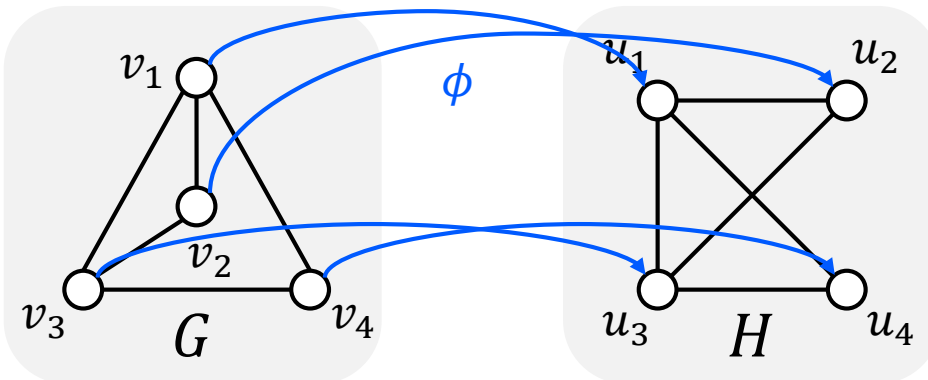
- 質問

■ G と H は同型か?

✓ 証拠の例

■ 同型写像 $\phi : V(G) \rightarrow V(H)$

$\phi(v_1) = u_1$
 $\phi(v_2) = u_2$
 $\phi(v_3) = u_3$
 $\phi(v_4) = u_4$



正当な
非決定性アルゴリズム

正解	出力
YES	YES
No	No

オイラーグラフ

■ 連結オイラーグラフ判定問題(C-EG) (判定)

$C-EG \in NP$

- 入力

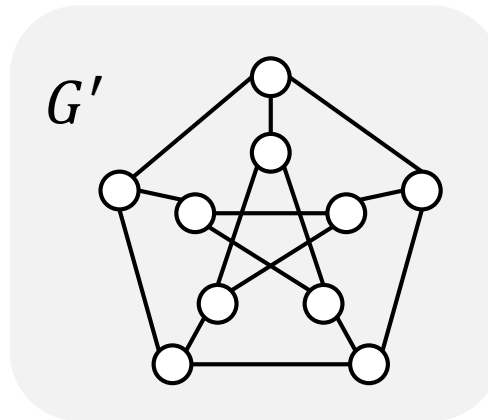
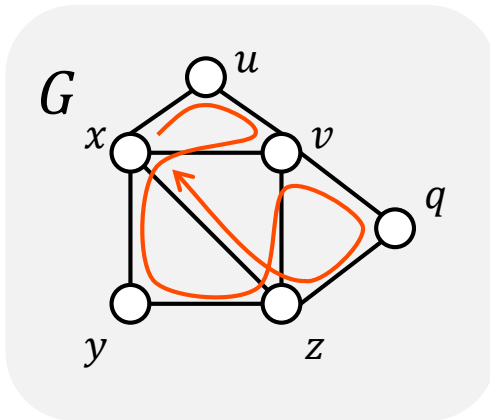
■ 連結グラフ G

- 質問

■ G はオイラーグラフか?

✓ 証拠の例

■ オイラー閉トレイル, 次数系列



正当な
非決定性アルゴリズム

正解	出力
YES	YES
No	No

ハミルトングラフ

■ ハミルトングラフ判定問題(HG) (判定)

$HG \in NP$

- 入力

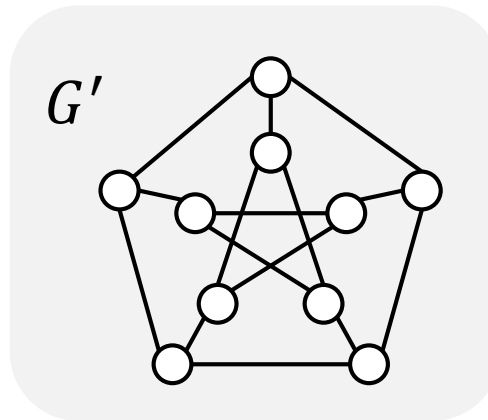
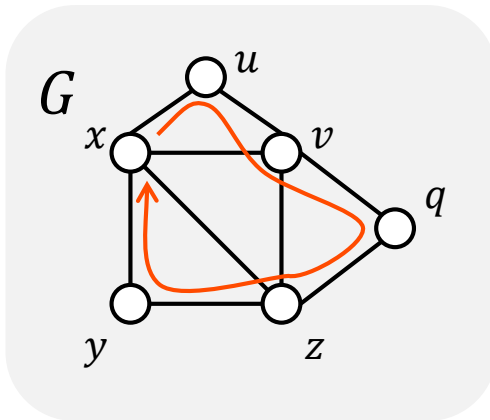
■ グラフ G

- 質問

■ G はハミルトングラフか?

✓ 証拠の例

■ ハミルトン閉路



正当な
非決定性アルゴリズム

正解	出力
YES	YES
No	No

ハミルトングラフ

■ 非ハミルトングラフ判定問題 (co-HG) (判定)

- 入力

■ グラフ G

- 質問

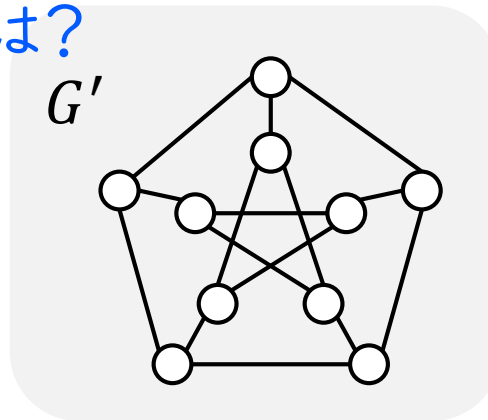
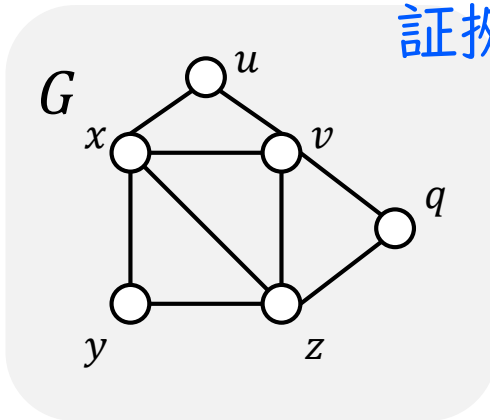
■ G はハミルトングラフではないか?

✓ 証拠の例

■ ???

co-HG が NP に属すかは不明

ハミルトングラフのとき
常に No と出力できる
証拠は?



正当な
非決定性アルゴリズム

正解		出力
YES	↔	YES
No	↔	No

素数

■ 素数判定問題 (PRIMES) (判定)

- 入力
 - 自然数 n
- 質問
 - n は素数か?

✓ 証拠の例

- No の証拠 : n の素因数分解
- Yes の証拠 : ???
 - Agrawal-Kayal-Saxena 素数判定法 (2002)
 - $\text{PRIMES} \in \text{P}$

co-PRIMES $\in \text{NP}$
PRIMES $\in \text{NP}$

正当な
非決定性アルゴリズム

正解		出力
YES		YES
No		No

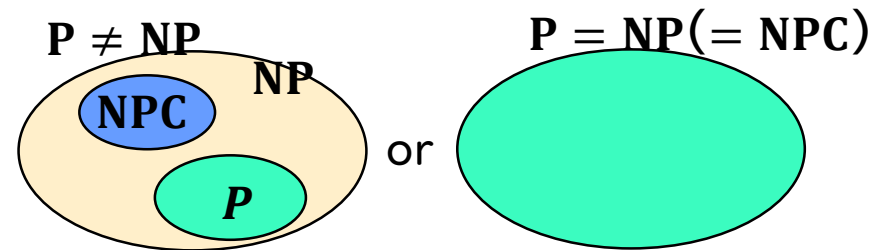
P ≠ NP予想

■ 判定問題 (Yes/No問題)

- NP : 判定問題の集合
 - **N**ondeterministic **P**olynomial time algorithmあり
- P : 判定問題の集合
 - (Deterministic) **P**olynomial time algorithmあり
- NPC: NPの中の最も難しい判定問題の集合
 - NPCのある問題が多項式時間で解ける ⇒
NPに属すすべての問題が多項式時間で解ける
 - NP完全 (NP-complete) 問題
 - 判定問題 ∈ NPC
 - SAT, 3-SAT, COL, HG, IS, TS, ...

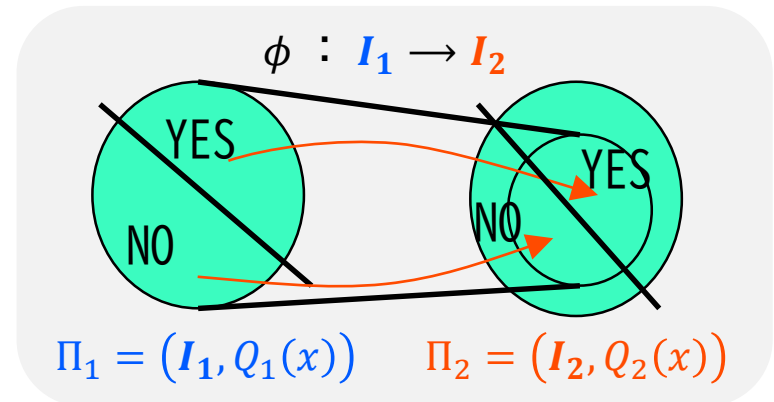
➤ 事実: $P \subseteq NP$

➤ 予想: $P \neq NP$



4-3 (2) 多項式時間還元

- 多項式時間還元 (polynomial time reduction)
 - 判定問題間の問題の難しさの関係を与える
 - どちらが難しくはないか?
- 判定問題 $\Pi_1 = (I_1, Q_1(x))$ から判定問題 $\Pi_2 = (I_2, Q_2(x))$
 - 多項式時間還元 $\phi: I_1 \rightarrow I_2$
 - Yes/Noの性質を保ったまま
 - 多項式時間で変換できる
 - $\phi: I_1 \rightarrow I_2$ が存在 $\Rightarrow \Pi_1 \propto \Pi_2$
- $\Pi_1 \propto \Pi_2$
 - ✓ Π_2 が多項式時間で解ける $\Rightarrow \Pi_1$ は多項式時間で解ける
 - Π_1 を解く多項式時間アルゴリズム
 - 入力 I_1 を入力 I_2 に多項式時間で変換
 - I_2 の解を多項式時間で得て I_1 の解として出力
 - ✓ Π_1 が難しく, Π_2 が易しいということはない



Π_1		Π_2
易	$\longleftrightarrow$	易
難	$\longleftrightarrow$	難

多項式時間還元の例: $HG \propto TS$

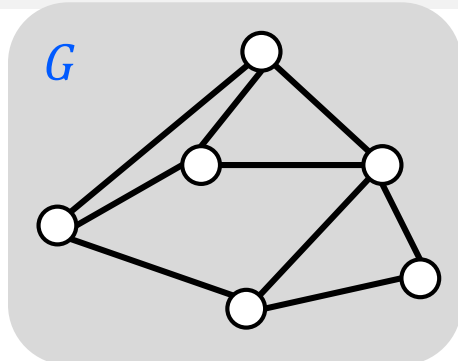
■ ハミルトングラフ判定問題 (HG)

- 入力 : グラフ G
- 質問 : G はハミルトングラフか?

■ 巡回セールスマン判定問題 (TS)

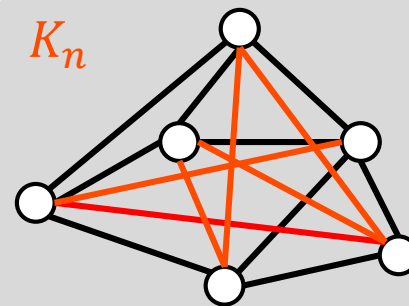
- 入力 : K_n , $w : E(K_n) \rightarrow \mathbb{R}^+$, r
- 質問 : (K_n, w) に **重み r 以下のハミルトン閉路** は存在するか?

HG : ハミルトングラフ判定問題



$$n = |V(G)|$$

TS : 巡回セールスマン判定問題



ハミルトン閉路の重み

w

— 1 ($e \in E(G)$)

— 2 ($e \notin E(G)$)

$$r := n$$

$$\begin{cases} n & G \text{ の辺のみ} \\ \geq n+1 & \text{その他の辺含む} \end{cases}$$

G はハミルトングラフ $\Leftrightarrow (K_n, w)$ の最小ハミルトン閉路の重みは n

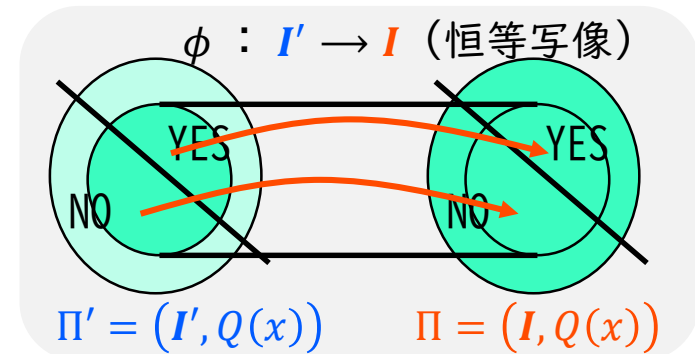
多項式時間還元の性質

■ 定理 (Theorem 4.4) (部分問題)

- 判定問題 $\Pi = (I, Q(x)) \in \text{NP}$
- Π の部分問題 $\Pi' = (I', Q(x))$, $I' \subseteq I$
 $\Rightarrow \Pi' \propto \Pi$

□ 証明:

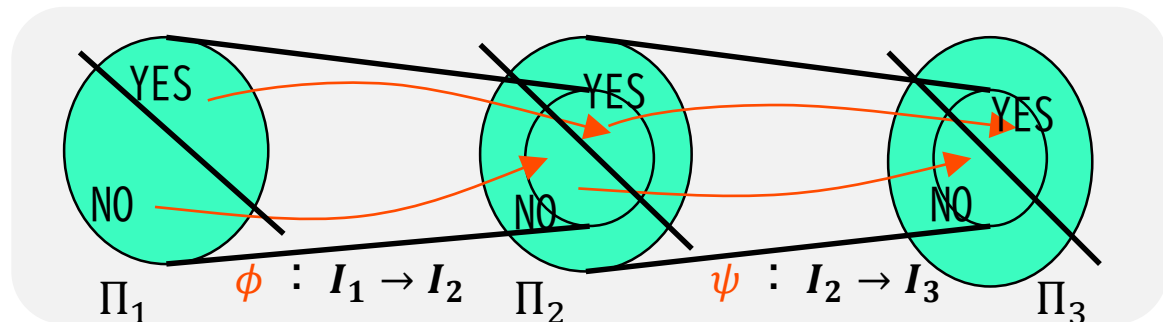
- 恒等写像 $\phi: I' \rightarrow I$ は多項式時間還元 ■



■ 定理 (Theorem 4.5) 多項式時間還元は推移律を満たす

□ 証明: $\Pi_1 = (I_1, Q_1(x))$, $\Pi_2 = (I_2, Q_2(x))$, $\Pi_3 = (I_3, Q_3(x))$

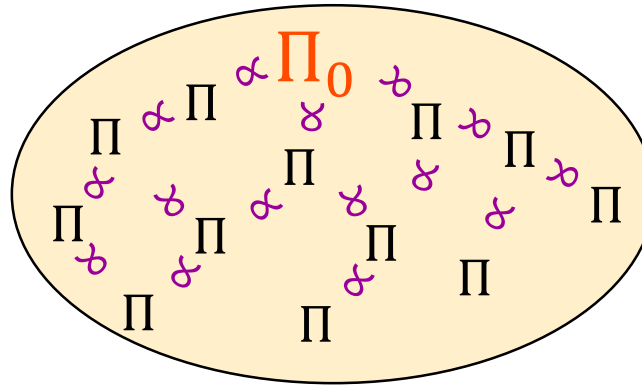
- $\phi: \Pi_1$ から Π_2 へ の多項式時間還元, $\psi: \Pi_2$ から Π_3 へ の多項式時間還元
 $\Rightarrow \psi \circ \phi$ は Π_1 から Π_3 へ の多項式時間還元
- $\Pi_1 \propto \Pi_2, \Pi_2 \propto \Pi_3$
 $\Rightarrow \Pi_1 \propto \Pi_3$ ■



4-3 (3) NP完全

■ NP完全問題 Π_0

- $\Pi_0 \in \text{NP}$
- $\forall \Pi \in \text{NP}, \Pi \propto \Pi_0$



Π_1		Π_2
易	$\longleftrightarrow$	易
難	$\longleftrightarrow$	難

✓ 任意のNP問題よりも易しくはないNP問題

✓ $P \neq \text{NP}$ ならば, 多項式時間アルゴリズムは存在しない問題

- NP完全ならば, 多項式時間アルゴリズムは諦める

- 近似アルゴリズム
- 発見的手法

NP完全性

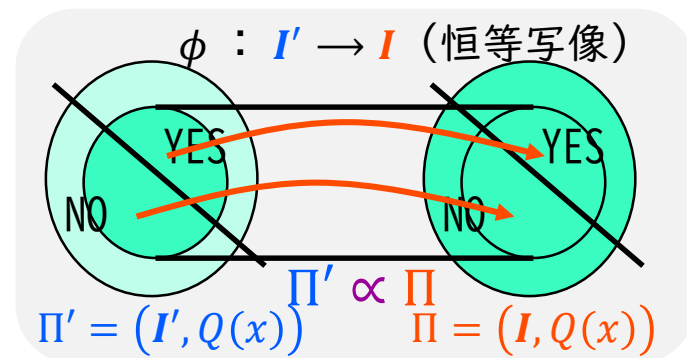
- **定理** (Theorem 4.6) 判定問題 $\Pi \in \text{NP}$ は,
あるNP完全問題 Π' に対して, $\Pi' \propto \Pi$ ならば, NP完全

□ 証明:

- $\forall \Pi'' \in \text{NP}, \Pi'' \propto \Pi'$ ($\because$ NP完全の定義) かつ $\Pi' \propto \Pi$
 $\Rightarrow \forall \Pi'' \in \text{NP}, \Pi'' \propto \Pi$ ($\because$ 定理4.5) ■

➤ NP完全性を示す典型的な手段

- **系** (Corollary 4.1)
判定問題 $\Pi \in \text{NP}$ は,
部分問題 Π' がNP完全ならば
NP完全



NP完全性の誤った解釈

- 判定問題 Π を解けと要求されている
- 多項式時間アルゴリズムが構成できない
- Π を, あるNP完全問題 Π_0 に多項式時間還元 ($\Pi \propto \Pi_0$)
 - Π に対する発見的手法の開発を目指す
- ✓ $\Pi \propto \Pi_0$ は, NP完全の定義から自明
 - これだけでは Π の計算複雑度は不明
 - 発見的手法開発の免罪符にはならない
- $\Pi_0 \propto \Pi$ が示されたならば
 - あるNP完全問題 Π_0 が, 解きたい問題 Π が解けると, 解ける
 - この状況はあり得ない
 - 問題 Π に対する発見的手法を開発する

4-3 (4) 充足可能性判定問題

■ 充足可能性判定問題 (Satisfiability, SAT) (判定)

- 入力 : CNFで表現されたブール関数 f
 - CNF
 - Conjunctive Normal Form, 和積形, NOT-OR-AND
- 質問 : f は充足可能か?

■ 例

- $F = (a \vee b) \wedge (\neg a \vee \neg b \vee c) \wedge (\neg a \vee \neg c)$
 - F is satisfiable
 - $a = 1, b = 0, c = 0 \Rightarrow F = 1$
- $F = (a \vee b) \wedge (a \vee \neg b) \wedge (\neg a \vee b) \wedge (\neg a \vee \neg b)$
 - F is unsatisfiable

Boolean Logic

■ Boolean variable

- $a, b \in \mathbb{B} = \{0, 1\} = \{\text{False}, \text{True}\}$

■ Unary operator

$\neg$: NOT

■ Binary operator

$\wedge$: AND, $\vee$: OR

■ Truth Table

a	$\neg a$
0	1
1	0

a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

a	b	$a \vee b$
0	0	0
0	1	1
1	0	1
1	1	1

a	b	c	$a \vee b$	$(a \vee b) \wedge c$
0	0	0	0	0
0	0	1	0	0
0	1	0	1	0
0	1	1	1	1
1	0	0	1	0
1	0	1	1	1
1	1	0	1	0
1	1	1	1	1

SATのNP完全性

■ **定理** (Theorem 4.7) SATはNP問題 ($\text{SAT} \in \text{NP}$)

□ 証明:

- f を構成する論理変数への値の割当は, f が充足可能であることの証拠となる ■

■ **定理** (Theorem 4.8) SATはNP完全 ($\text{SAT} \in \text{NPC}$)

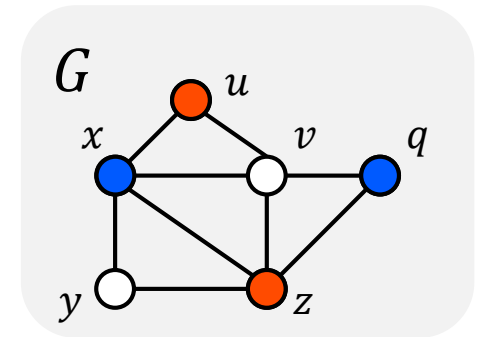
□ 証明の概要(Cook):

- アルゴリズムの挙動はチューリング機械で表現できる
- 入力の大きさの多項式オーダーのブール関数で, チューリング機械の出力を記述できる
- 任意のNP問題はSATに多項式時間還元できる ■

3彩色判定問題

■ 3彩色判定問題(3-COL) (判定)

- 入力
 - グラフ G
- 質問
 - G を3彩色できるか?



■ グラフの彩色

- 隣接点に同色が割り当てられないように, 点に色を割り当てる

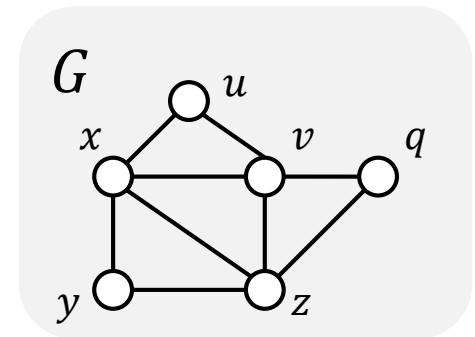
多項式時間還元の例: 3-COL $\propto$ SAT

➤ 3彩色の証拠をブール関数で表現

- 正しい彩色 $\Leftrightarrow$ ブール関数が充足

■ グラフ $G = (V, E)$ の3彩色の証拠

- 3色が使われる
- 各点は1色
- 隣接点は異なる色



■ $V(G) = \{v_1, v_2, \dots, v_n\}$, $E(G) = \{e_1, e_2, \dots, e_m\}$

- 各点 v_i に対して, 色 1, 2, 3 に対応する3変数 x_{i1}, x_{i2}, x_{i3}

- $x_{ij} = \begin{cases} 1 & \text{if 点 } v_i \text{ は色 } j \\ 0 & \text{otherwise} \end{cases}$

多項式時間還元の例: 3-COL $\propto$ SAT

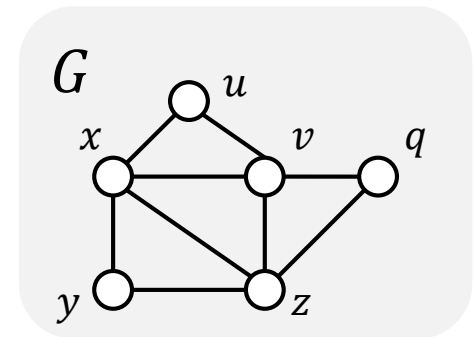
➤ 3彩色の証拠をブール関数で表現

- 点 v_i は色1, 2, 3いずれか1色 (少なくとも1色かつ2色でない)

$$P_i = (x_{i1} \vee x_{i2} \vee x_{i3}) \wedge (\overline{x_{i1}} \vee \overline{x_{i2}}) \wedge (\overline{x_{i1}} \vee \overline{x_{i3}}) \wedge (\overline{x_{i2}} \vee \overline{x_{i3}})$$

- ✓ すべての点は1色

$$\bigwedge_{i \in V(G)} P_i$$



- 隣接点 v_i と v_j は異なる色 (隣接点は同色ではない)

$$Q_{(i,j)} = (\overline{x_{i1}} \vee \overline{x_{j1}}) \wedge (\overline{x_{i2}} \vee \overline{x_{j2}}) \wedge (\overline{x_{i3}} \vee \overline{x_{j3}})$$

- ✓ すべての隣接点は異なる色

$$\bigwedge_{(i,j) \in E(G)} Q_{(i,j)}$$

4-3 (5) NP完全問題

■ 3充足可能性判定問題 (3-SAT) (判定)

- 入力 : 各和節が3リテラルからなるCNF表現のブール関数 f
 - リテラル: 肯定形もしくは否定形の変数
- 質問 : f は充足可能か?

■ 例

$$- f = (a \vee b \vee c) \wedge (\neg a \vee \neg b \vee c) \wedge (a \vee \neg c \vee \neg d)$$

3-SATのNP完全性

■ **定理 (Theorem 4.9)** 3-SATはNP完全 (3-SAT $\in$ NPC)

□ **証明:** SAT $\propto$ 3-SATを示す

- 充足可能性を保ちつつ, 各節を, 3リテラルの節 (複数) に変換

■ SATの入力 f に含まれないブール変数 y を用意

✓ 1リテラル節

■ $(x) \Rightarrow (x \vee y_1 \vee y_2) \wedge (x \vee y_1 \vee \overline{y_2}) \wedge (x \vee \overline{y_1} \vee y_2) \wedge (x \vee \overline{y_1} \vee \overline{y_2})$

✓ 2リテラル節

■ $(x_1 \vee x_2) \Rightarrow (x_1 \vee x_2 \vee y) \wedge (x_1 \vee x_2 \vee \overline{y})$

✓ k リテラル ($k \geq 4$)

■ $(x_1 \vee x_2 \vee \dots \vee x_k) \Rightarrow (x_1 \vee x_2 \vee y_1) \wedge (\overline{y_1} \vee x_3 \vee y_2) \wedge$
 $(\overline{y_2} \vee x_4 \vee y_3) \wedge \dots \wedge (\overline{y_{k-3}} \vee x_{k-1} \vee x_k)$

- 得られる3-SATの入力サイズは, $|f|$ の多項式オーダー ■

➤ 2-SATは線形時間で判定可能 (P)

■ $(a \vee b) \equiv (\neg a \rightarrow b) \equiv (\neg b \rightarrow a)$

3-COLのNP完全性

■ **定理 (Theorem 4.10)** 3-COLはNP完全 (3-COL $\in$ NPC)

□ 証明: 3-SAT $\propto$ 3-COLを示す

- $\phi : f \mapsto G(f)$

■ 3-SATのブール関数 f は充足可能 $\Leftrightarrow$ グラフ $G(f)$ は3彩色可能

■ $V(G(f))$

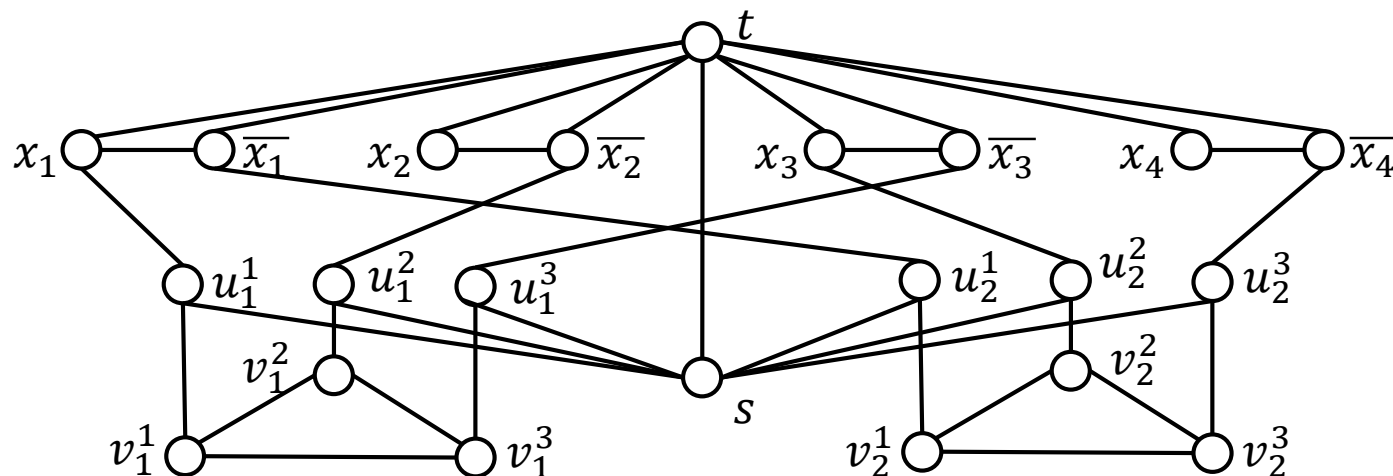
- 各ブール変数 x_i に対して2点 $x_i, \bar{x}_i$ (リテラル点)

- 各節 C_i に対して6点 $u_i^1, u_i^2, u_i^3, v_i^1, v_i^2, v_i^3$

- 2点 s, t

$E(G(f))$ の詳細は略

✓ $f = (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_3 \vee \bar{x}_4)$ に対応する $G(f)$



3-COLのNP完全性

■ **定理 (Theorem 4.10)** 3-COLはNP完全 (3-COL $\in$ NPC)

□ 証明 (cont.):

- $G(f)$ が3彩色できるならば, 一般性を失わず, s は赤, t は青で彩色とする

■ 変数 x_i

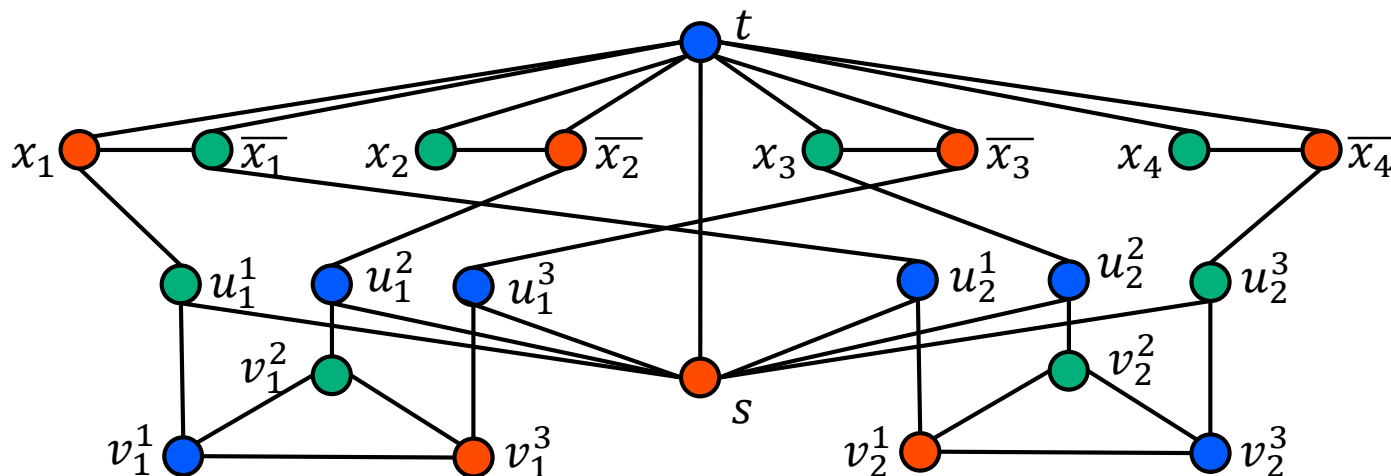
- リテラル点 $x_i, \bar{x}_i$ は赤または緑 (赤リテラル点が充足と考える)

■ 節 C_i

- u_i^j は青または緑 $\Rightarrow v_i^j$ の3彩色のためは全部青はダメ

- u_i^j が緑のためには赤リテラル点と隣接 $\Rightarrow$ 節に赤リテラル点 (3彩色可能 $\Leftrightarrow$ 充足可能)

✓ $G(f)$ の変数割り当て $x_1 = 1, x_2 = x_3 = x_4 = 0$ に対応する彩色



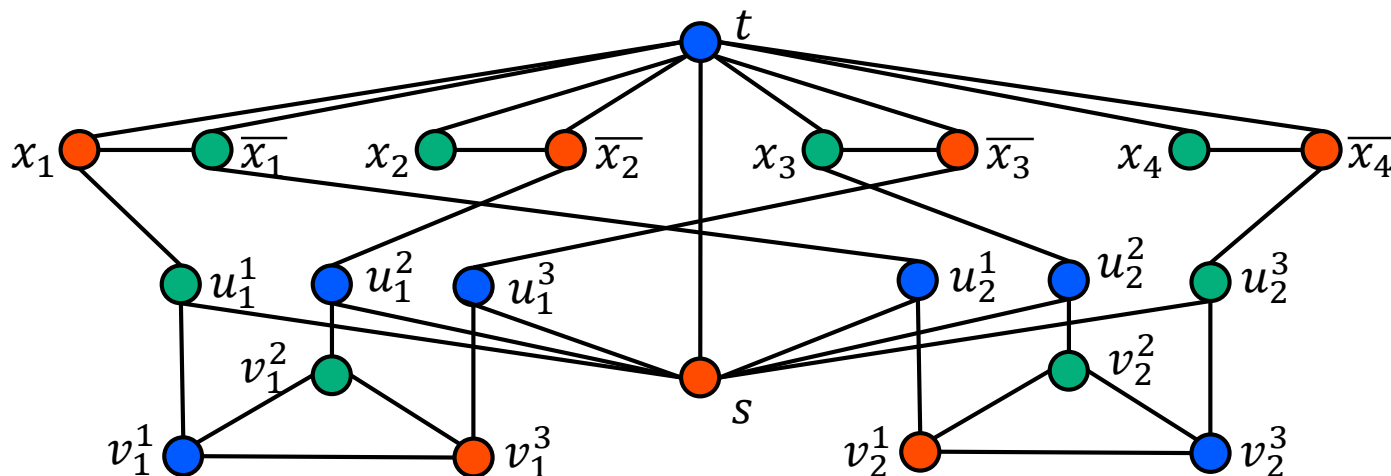
3-COLのNP完全性

■ **定理 (Theorem 4.10)** 3-COLはNP完全 ($3\text{-COL} \in \text{NPC}$)

□ **証明 (cont.)**:

- f が充足可能 $\Leftrightarrow G(f)$ は3彩色可能
- $\phi : f \mapsto G(f)$
 - 3-SATから 3-COLへの多項式時間還元
 - $|V(G(f))| = 2l + 6c + 2$, $|E(G(f))| = 3l + 12c + 1$
 - l : リテラル数, c : 節数

✓ $f = (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_3 \vee \overline{x_4})$ に対応する $G(f)$



NP完全問題

➤ $\text{SAT} \propto 3\text{-SAT} \propto 3\text{-COL} \propto \text{SAT}$

■ 定理 (Theorem 4.11)

- ハミルトングラフ判定問題(HG)はNP完全 ($\text{HG} \in \text{NPC}$)
- 独立点集合判定問題(IS) はNP完全 ($\text{IS} \in \text{NPC}$)

□ 証明 (詳細略)

- $\text{HG} \in \text{NP}$, $3\text{-SAT} \propto \text{HG}$
- $\text{IS} \in \text{NP}$, $3\text{-SAT} \propto \text{IS}$

■ 系 (Corollary 4.2)

- 巡回セールスマン判定問題(TS) はNP完全 ($\text{TS} \in \text{NPC}$)

□ 証明: $\text{TS} \in \text{NP}$, $\text{HG} \propto \text{TS}$

巡回セールスマン問題

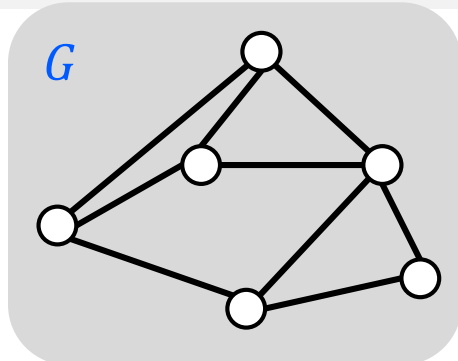
■ 三角巡回セールスマン判定問題 (T-TS) (判定)

- 入力 : K_n , $w : E(K_n) \rightarrow \mathbb{R}^+$, r (三角不等式を満たす)
- 質問 : (K_n, w) に重み r 以下のハミルトン閉路は存在するか?

✓ NP完全

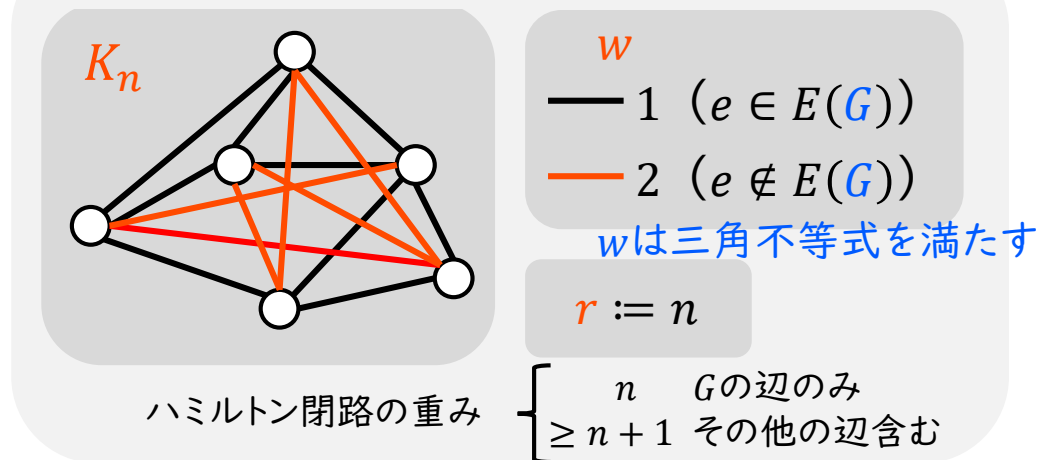
- T-TS $\in$ NP
- $HG \propto$ T-TS は既に示した
 - TSへの多項式時間還元はT-TSへの多項式時間還元でもある

HG : ハミルトングラフ判定問題



$$n = |V(G)|$$

TS : 巡回セールスマン判定問題



G はハミルトングラフ $\Leftrightarrow (K_n, w)$ の最小ハミルトン閉路の重みは n

巡回セールスマン問題

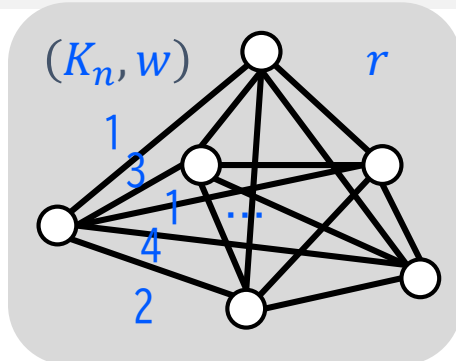
■ 最大巡回セールスマン判定問題 (MAX-TS) (判定)

- 入力 : K_n , $w : E(K_n) \rightarrow \mathbb{R}^+$, r
- 質問 : (K_n, w) に **重み r 以上のハミルトン閉路** は存在するか?

✓ NP完全

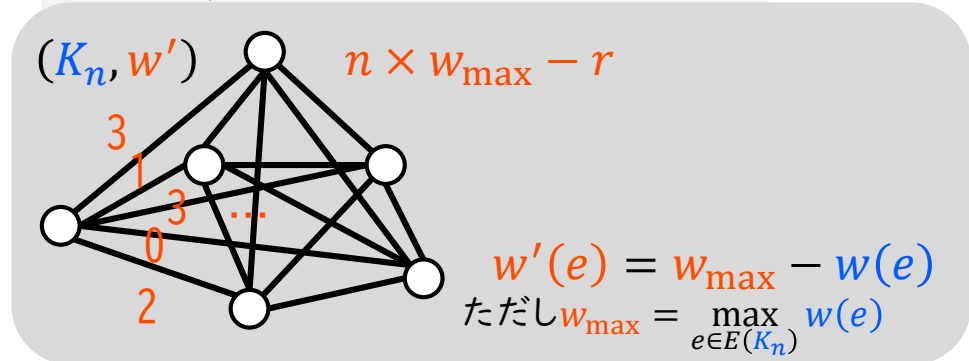
- MAX-TS $\in$ NP
- TS $\propto$ MAX-TS

TS:巡回セールスマン判定問題



重み a のハミルトン閉路

MAX-TS:最大巡回セールスマン判定問題



重み $n \times w_{\max} - a$ のハミルトン閉路

重み r 以下のハミルトン閉路が存在 $\Leftrightarrow$ 重み $n \times w_{\max} - r$ 以上のハミルトン閉路が存在

グラフ同型

■ グラフ同型判定問題 (ISO) (判定)

$ISO \in NP$

- 入力

■ グラフ G, H

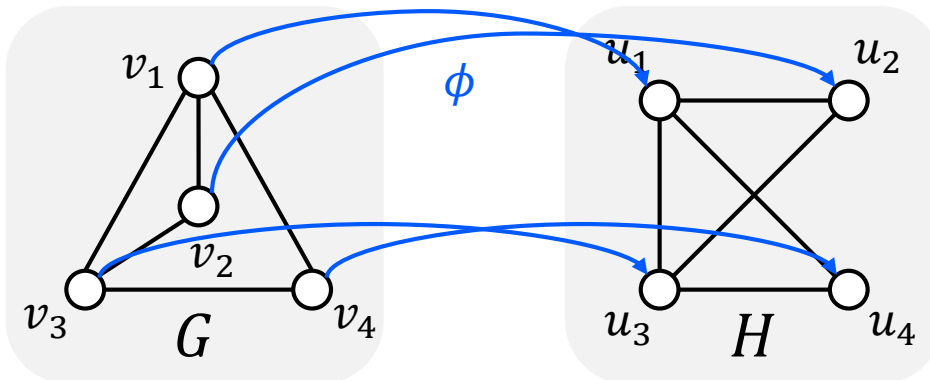
- 質問

■ G と H は同型か?

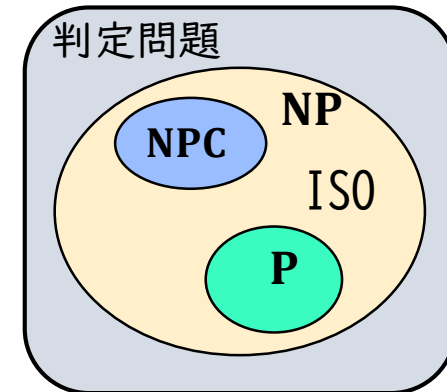
✓ 証拠の例

■ 同型写像 $\phi : V(G) \rightarrow V(H)$

$\phi(v_1) = u_1$
 $\phi(v_2) = u_2$
 $\phi(v_3) = u_3$
 $\phi(v_4) = u_4$



$P \neq NP$ の場合



$ISO \notin NPC$
 $ISO \notin P$

P ≠ NP予想

■ 判定問題 (Yes/No問題)

- NP : 判定問題の集合
 - **N**ondeterministic **P**olynomial time algorithmあり
- P : 判定問題の集合
 - (Deterministic) **P**olynomial time algorithmあり
- NPC: NPの中の最も難しい判定問題の集合
 - NPCのある問題が多項式時間で解ける ⇒
NPに属すすべての問題が多項式時間で解ける
 - NP完全 (NP-complete) 問題
 - 判定問題 ∈ NPC
 - SAT, 3-SAT, COL, HG, IS, TS, ...

➤ 事実: $P \subseteq NP$

➤ 予想: $P \neq NP$

