

# 理論計算機科学特論 (2026 年前学期)

計算複雑性の基礎

## 第 15 回

### 対話証明系 (3) : $PSPACE \subseteq IP$

岡本 吉央 (電気通信大学)

okamotoy@uec.ac.jp

2026 年 7 月 21 日

最終更新 : 2026 年 7 月 20 日 12:00

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)

- 8. Savitch の定理 :  $PSPACE = NPSPACE$  (6/2)
- 9. Immerman-Szelepcsényi の定理 :  $NL = coNL$  (6/9)
- 10. 交代性計算 :  $AP = PSPACE$  (6/16)
- 11. 多項式階層 :  $P = NP \Rightarrow P = PH$  (6/23)
- 12. 確率的計算 :  $PP, RP, BPP, ZPP$  (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] 対話証明系ってなに？

4/40

(interactive proof system)



アーサー (Arthur)  
王様

検証者 (verifier)



マーリン (Merlin)  
魔法使い

証明者 (prover)

# [復習] 対話証明系ってなに？

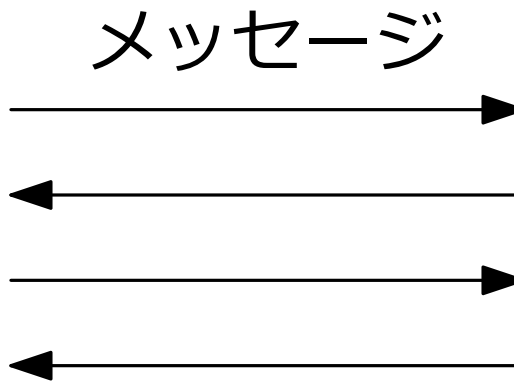
4/40

(interactive proof system)



アーサー (Arthur)  
王様

検証者 (verifier)



マーリン (Merlin)  
魔法使い

証明者 (prover)

# [復習] 対話証明系ってなに？

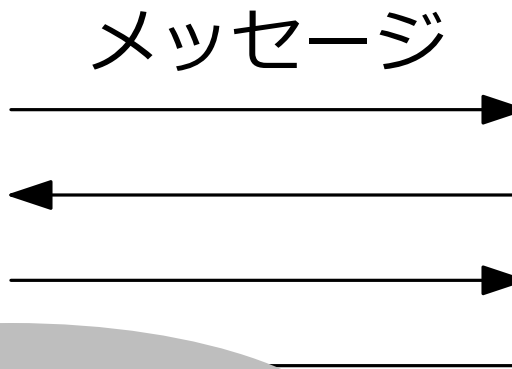
4/40

(interactive proof system)



アーサー (Arthur)  
王様

検証者 (verifier)



マーリン (Merlin)  
魔法使い

証明者 (prover)

# [復習] 対話証明系ってなに？ (続)

5/40

判定問題  $P$  を解きたい

入力  $I$



計算能力：低い



計算能力：高い

信頼できない



# [復習] 対話証明系ってなに？ (続)

5/40

判定問題  $P$  を解きたい

入力  $I$



正しく Yes/No を  
言いたい

計算能力：低い

アーサーに Yes と  
言わせたい

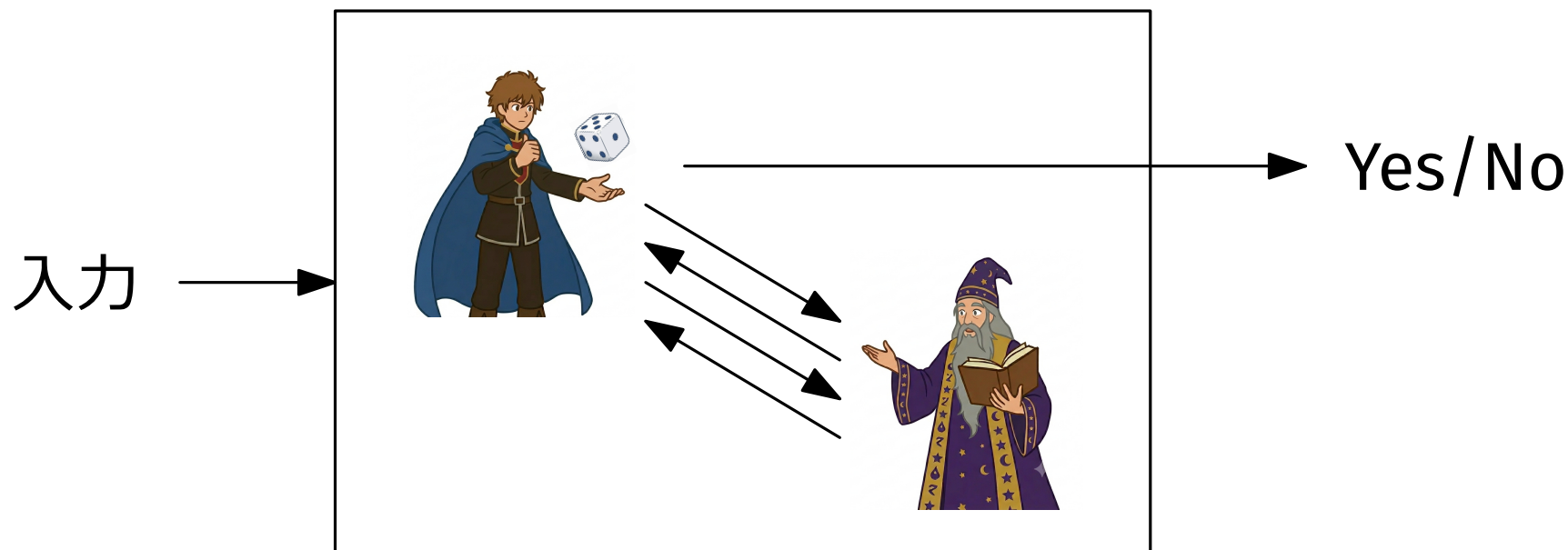


計算能力：高い  
信頼できない



## 対話証明系の設定

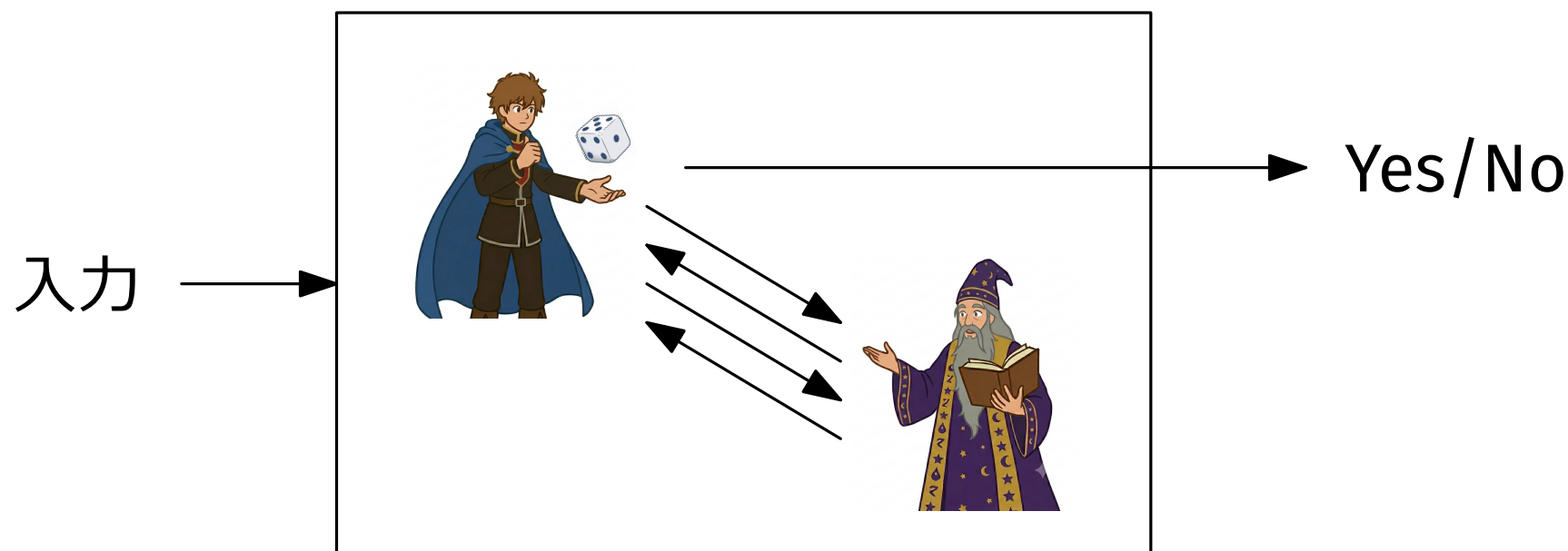
- 登場人物
  - 検証者** 多項式時間アルゴリズム + 乱数使用
  - 証明者** なんでも解ける (計算不能問題も解ける)
- 入力は両方に与えられる
- 出力は検証者が行う



## 定義 (非形式)：プロトコル

対話証明系における **プロトコル** (protocol) とは,  
検証者と証明者が行う動作を定めたもの

検証者・証明者はプロトコルから逸脱しない



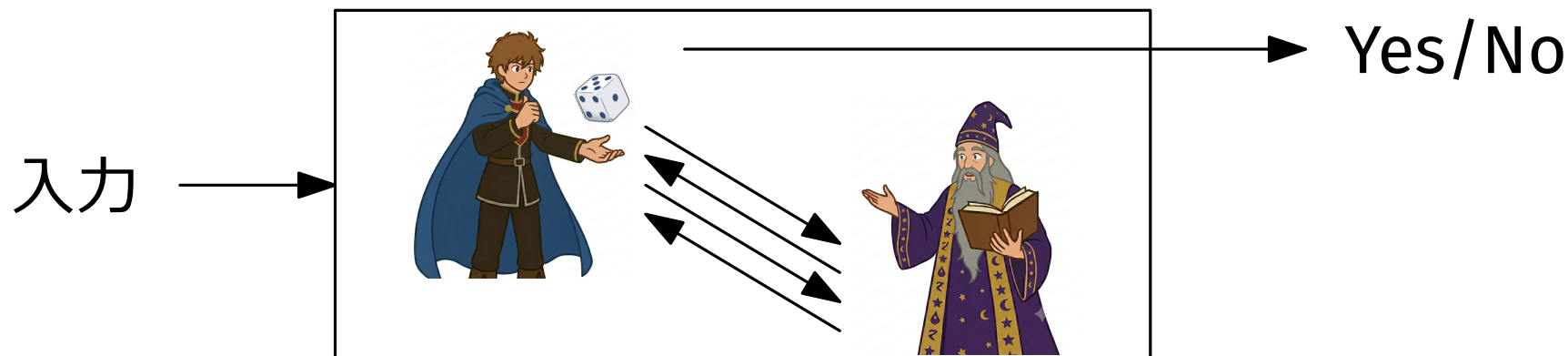
## プロトコル $A$ が判定問題 $P$ を解くとは

- 入力が  $P$  の Yes インスタンス  $\Rightarrow$   
証明者がうまく動作することで、次を満たす

$$\Pr_r(\text{検証者が Yes を出力}) \geq \frac{2}{3}$$

- 入力が  $P$  の No インスタンス  $\Rightarrow$   
証明者がどのように動作しても、次を満たす

$$\Pr_r(\text{検証者が No を出力}) \geq \frac{2}{3}$$



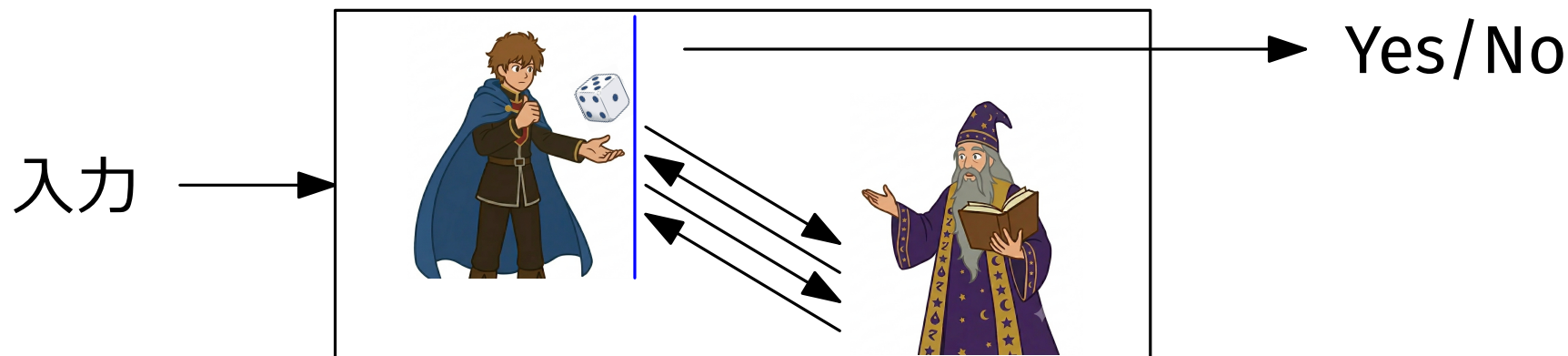
## 複雑性クラス IP

(Goldwasser, Micali, Rackoff '89)

**クラス IP** は次を満たすプロトコルで解ける問題全体

- プロトコルは 検証者 の動作から始まる
- 検証者と証明者が 多項式回のラウンド で動作を行う
- 検証者の乱数は証明者から 見えない (private coin)

IP = Interactive Proof



定理

(Shamir '92)

IP = PSPACE

前回おこなったこと

- $IP \subseteq PSPACE$  の証明
- $PSPACE \subseteq IP$  の証明の準備

今回おこなうこと

- $PSPACE \subseteq IP$  の証明

## 内容

- $PSPACE \subseteq IP$  の証明
- 対話証明系に関する補足



1.  $PSPACE \subseteq IP$  の証明
2. 対話証明系に関する補足

## 基本的なアイディア

- ある PSPACE 完全問題に対して,  
多項式ラウンドの対話証明系を構成する
- PSPACE 完全問題として QBF を考える
- QBF を解くために, **算術化** を行う

算術化 = arithmetization

いまから紹介する証明は Shamir ('92) の証明を  
Shen ('92) が簡素化したものに基づく

例：  $\varphi(x_1, x_2, x_3) = (\overline{x_1} \wedge (x_1 \vee x_2)) \vee (x_2 \vee x_3)$

論理演算



$$f(x_1, x_2, x_3) = x_2 + x_3 - x_2x_3$$

算術演算

例：  $\varphi(x_1, x_2, x_3) = (\overline{x_1} \wedge (x_1 \vee x_2)) \vee (x_2 \vee x_3)$

↓  
論理演算

- $\varphi(0, 0, 0) = 0$
- $\varphi(0, 0, 1) = 1$
- $\varphi(0, 1, 0) = 1$
- $\varphi(0, 1, 1) = 1$
- $\varphi(1, 0, 0) = 0$
- $\varphi(1, 0, 1) = 1$
- $\varphi(1, 1, 0) = 1$
- $\varphi(1, 1, 1) = 1$

$f(x_1, x_2, x_3) = x_2 + x_3 - x_2x_3$

算術演算

- $f(0, 0, 0) = 0$
- $f(0, 0, 1) = 1$
- $f(0, 1, 0) = 1$
- $f(0, 1, 1) = 1$
- $f(1, 0, 0) = 0$
- $f(1, 0, 1) = 1$
- $f(1, 1, 0) = 1$
- $f(1, 1, 1) = 1$

例：  $\varphi(x_1, x_2, x_3) = (\overline{x_1} \wedge (x_1 \vee x_2)) \vee (x_2 \vee x_3)$

算  
術  
化



論理演算

- $\varphi(0, 0, 0) = 0$
- $\varphi(0, 0, 1) = 1$
- $\varphi(0, 1, 0) = 1$
- $\varphi(0, 1, 1) = 1$
- $\varphi(1, 0, 0) = 0$
- $\varphi(1, 0, 1) = 1$
- $\varphi(1, 1, 0) = 1$
- $\varphi(1, 1, 1) = 1$

$$f(x_1, x_2, x_3) = x_2 + x_3 - x_2x_3$$

算術演算

- $f(0, 0, 0) = 0$
- $f(0, 0, 1) = 1$
- $f(0, 1, 0) = 1$
- $f(0, 1, 1) = 1$
- $f(1, 0, 0) = 0$
- $f(1, 0, 1) = 1$
- $f(1, 1, 0) = 1$
- $f(1, 1, 1) = 1$

---

論理演算       $\longrightarrow$       算術演算

---

$$x \wedge y$$

$$xy$$

$$x \vee y$$

$$1 - (1 - x)(1 - y)$$

$$\overline{x}$$

$$1 - x$$

---

この手順を  
再帰的に  
適用する

---

論理演算       $\longrightarrow$       算術演算

---

$$x \wedge y$$

$$xy$$

$$x \vee y \equiv \overline{\overline{x} \wedge \overline{y}}$$

$$1 - (1 - x)(1 - y)$$

$$\overline{x}$$

$$1 - x$$

---

この手順を  
再帰的に  
適用する

---

論理演算  $\longrightarrow$  算術演算

---

$$x \wedge y$$

$$xy$$

$$x \vee y \equiv \overline{\overline{x} \wedge \overline{y}}$$

$$1 - (1 - x)(1 - y)$$

$$\overline{x}$$

$$1 - x$$

---

この手順を  
再帰的に  
適用する

例 :  $(\overline{x_1} \wedge (x_1 \vee x_2)) \vee (x_2 \vee x_3)$



$$1 - (1 - (1 - x_1)(1 - (1 - x_1)(1 - x_2)))(1 - (1 - (1 - x_2)(1 - x_3)))$$



---

論理演算  $\longrightarrow$  算術演算

---

$$x \wedge y$$

$$xy$$

$$x \vee y \equiv \overline{\overline{x} \wedge \overline{y}}$$

$$1 - (1 - x)(1 - y)$$

$$\overline{x}$$

$$1 - x$$

---

この手順を  
再帰的に  
適用する

例 :  $(\overline{x_1} \wedge (x_1 \vee x_2)) \vee (x_2 \vee x_3)$

$\downarrow$

$$1 - (1 - (1 - x_1)(1 - (1 - x_1)(1 - x_2)))(1 - (1 - (1 - x_2)(1 - x_3)))$$

これは  $x_1, x_2, x_3$  に関する多項式

- 変数の数 = 元の論理式  $\varphi$  の変数の数
- 各変数の次数  $\leq |\varphi|$  (論理式  $\varphi$  の符号長)

**問題：** QBF (量化論理式問題, 限定論理式問題)

**入力：** 命題論理式  $\varphi(X)$  ( $X$  は変数集合)

$X$  の分割  $X_1, X_2, \dots, X_k$

**出力：**  $\exists X_1 \forall X_2 \dots \forall X_k: \varphi(X) = 1 \Rightarrow \text{Yes}$

$\forall X_1 \exists X_2 \dots \exists X_k: \varphi(X) = 0 \Rightarrow \text{No}$

QBF = Quantified Boolean Formula problem

( $\exists, \forall$  を quantifier (量化子, 限定子, 限量子) と呼ぶ)

注 1 : SAT は  $X = X_1$  の場合に対応

注 2 :  $X_k$  の前は「 $\exists$ 」でもよい ( $k$  は偶数でも奇数でもよい)

性質 (証明しない)

(Stockmeyer, Meyer '73)

QBF は PSPACE 完全

問題 : QBF (量化論理式問題, 限定論理式問題)

入力 : 命題論理式  $\varphi(X)$  ( $X$  は変数集合)

$X$  の分割  $X_1, X_2, \dots, X_k$

出力 :  $\exists X_1 \forall X_2 \dots \forall X_k : \varphi(X) = 1 \Rightarrow \text{Yes}$

$\forall X_1 \exists X_2 \dots \exists X_k : \varphi(X) = 0 \Rightarrow \text{No}$

例 :  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

$X = \{x, y, z\}, \quad X_1 = \{x\}, X_2 = \{y\}, X_3 = \{z\}$

問題 : QBF (量化論理式問題, 限定論理式問題)

入力 : 命題論理式  $\varphi(X)$  ( $X$  は変数集合)

$X$  の分割  $X_1, X_2, \dots, X_k$

出力 :  $\exists X_1 \forall X_2 \dots \forall X_k : \varphi(X) = 1 \Rightarrow \text{Yes}$

$\forall X_1 \exists X_2 \dots \exists X_k : \varphi(X) = 0 \Rightarrow \text{No}$

例 :  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

$X = \{x, y, z\}, \quad X_1 = \{x\}, X_2 = \{y\}, X_3 = \{z\}$

2 人ゲームだと思ふとよい

•  $x = 1$  とする  $\rightsquigarrow \varphi(1, y, z) = \bar{y} \vee \bar{z}$

問題 : QBF (量化論理式問題, 限定論理式問題)

入力 : 命題論理式  $\varphi(X)$  ( $X$  は変数集合)

$X$  の分割  $X_1, X_2, \dots, X_k$

出力 :  $\exists X_1 \forall X_2 \dots \forall X_k : \varphi(X) = 1 \Rightarrow \text{Yes}$

$\forall X_1 \exists X_2 \dots \exists X_k : \varphi(X) = 0 \Rightarrow \text{No}$

例 :  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

$X = \{x, y, z\}, \quad X_1 = \{x\}, X_2 = \{y\}, X_3 = \{z\}$

2 人ゲームだと思ふとよい

- $x = 1$  とする  $\rightsquigarrow \varphi(1, y, z) = \bar{y} \vee \bar{z}$ 
  - $y = 0$  とする  $\rightsquigarrow \varphi(1, 0, z) = 1$
  - $y = 1$  とする  $\rightsquigarrow \varphi(1, 1, z) = \bar{z}$

問題 : QBF (量化論理式問題, 限定論理式問題)

入力 : 命題論理式  $\varphi(X)$  ( $X$  は変数集合)

$X$  の分割  $X_1, X_2, \dots, X_k$

出力 :  $\exists X_1 \forall X_2 \dots \forall X_k : \varphi(X) = 1 \Rightarrow \text{Yes}$

$\forall X_1 \exists X_2 \dots \exists X_k : \varphi(X) = 0 \Rightarrow \text{No}$

例 :  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

$X = \{x, y, z\}, \quad X_1 = \{x\}, X_2 = \{y\}, X_3 = \{z\}$

2人ゲームだと思つとよい

- $x = 1$  とする  $\leadsto \varphi(1, y, z) = \bar{y} \vee \bar{z}$ 
  - $y = 0$  とする  $\leadsto \varphi(1, 0, z) = 1$
  - $y = 1$  とする  $\leadsto \varphi(1, 1, z) = \bar{z}$ 
    - $z = 0$  とする  $\leadsto \varphi(1, 1, 0) = 1 \quad \Rightarrow$  出力は Yes

例：  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

↓ 算術化

$$f(x, y, z) = (1 - (1 - x)(1 - y)(1 - z))(1 - xyz)$$

例：  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

↓ 算術化

$$f(x, y, z) = (1 - (1 - x)(1 - y)(1 - z))(1 - xyz)$$

$$\exists x \forall y \exists z: (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$$

↓

$$\sum_{a \in \{0,1\}} \prod_{b \in \{0,1\}} \sum_{c \in \{0,1\}} (1 - (1 - a)(1 - b)(1 - c))(1 - abc)$$



例 :  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

↓ 算術化

$$f(x, y, z) = (1 - (1 - x)(1 - y)(1 - z))(1 - xyz)$$

$$\exists x \forall y \exists z: (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$$

↓

$$\sum_{a \in \{0,1\}} \prod_{b \in \{0,1\}} \sum_{c \in \{0,1\}} (1 - (1 - a)(1 - b)(1 - c))(1 - abc)$$

$$= \prod_{b \in \{0,1\}} \sum_{c \in \{0,1\}} (1 - (1 - b)(1 - c)) + \prod_{b \in \{0,1\}} \sum_{c \in \{0,1\}} (1 - bc)$$

例：  $\varphi(x, y, z) = (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$

↓ 算術化

$$f(x, y, z) = (1 - (1 - x)(1 - y)(1 - z))(1 - xyz)$$

$$\exists x \forall y \exists z: (x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$$

↓

$$\sum_{a \in \{0,1\}} \prod_{b \in \{0,1\}} \sum_{c \in \{0,1\}} (1 - (1 - a)(1 - b)(1 - c))(1 - abc)$$

$$= \prod_{b \in \{0,1\}} \sum_{c \in \{0,1\}} (1 - (1 - b)(1 - c)) + \prod_{b \in \{0,1\}} \sum_{c \in \{0,1\}} (1 - bc)$$

$$= \sum_{c \in \{0,1\}} c + \sum_{c \in \{0,1\}} (1 - c) = 2$$

$$\varphi \xrightarrow{\text{算術化}} f$$

観察

$$\exists x_1 \forall x_2 \dots \forall x_n : \varphi(x_1, x_2, \dots, x_n) = 1$$

$$\Leftrightarrow \sum_{a_1 \in \{0,1\}} \prod_{a_2 \in \{0,1\}} \dots \prod_{a_n \in \{0,1\}} f(a_1, a_2, \dots, a_n) > 0$$

証明の概略 :  $\varphi$  の変数の数に関する帰納法

□

$$\varphi \xrightarrow{\text{算術化}} f$$

観察

$$\exists x_1 \forall x_2 \dots \forall x_n : \varphi(x_1, x_2, \dots, x_n) = 1$$

$$\Leftrightarrow \sum_{a_1 \in \{0,1\}} \prod_{a_2 \in \{0,1\}} \dots \prod_{a_n \in \{0,1\}} f(a_1, a_2, \dots, a_n) > 0$$

記法

$$: \quad f_0() = \sum_{a_1 \in \{0,1\}} \prod_{a_2 \in \{0,1\}} \dots \prod_{a_n \in \{0,1\}} f(a_1, a_2, \dots, a_n)$$

$$f_1(x_1) = \prod_{a_2 \in \{0,1\}} \dots \prod_{a_n \in \{0,1\}} f(x_1, a_2, \dots, a_n)$$

$$\vdots \quad \quad \quad \vdots$$

## 問題点

$f_1(x_1)$  の次数が大きくなり過ぎるかもしれない

$$\text{例 : } \prod_{a \in \{0,1\}} (x + a + 1) = (x + 1)(x + 2)$$

$\therefore$  検証者が多項式時間で処理できない

$$\boxed{\text{記法}} : f_0() = \sum_{a_1 \in \{0,1\}} \prod_{a_2 \in \{0,1\}} \cdots \prod_{a_n \in \{0,1\}} f(a_1, a_2, \dots, a_n)$$

$$f_1(x_1) = \prod_{a_2 \in \{0,1\}} \cdots \prod_{a_n \in \{0,1\}} f(x_1, a_2, \dots, a_n)$$

$$\vdots \qquad \vdots$$

## 観察

任意の関数  $p: \mathbb{R} \rightarrow \mathbb{R}$  に対して,  $a \in \{0, 1\}$  のとき,

$$p(a) = (1 - a) \cdot p(0) + a \cdot p(1)$$

つまり, 算術化においては, 次の変換で結果は変わらない

$$f(x_1, x_2, \dots, x_n)$$

↓

$$(1 - x_n)f(x_1, x_2, \dots, 0) + x_nf(x_1, x_2, \dots, 1)$$

## 観察

任意の関数  $p: \mathbb{R} \rightarrow \mathbb{R}$  に対して,  $a \in \{0, 1\}$  のとき,

$$p(a) = (1 - a) \cdot p(0) + a \cdot p(1)$$

つまり, 算術化においては, 次の変換で結果は変わらない

$$f(x_1, x_2, \dots, x_n)$$

$$\downarrow R_n$$

$$(1 - x_n)f(x_1, x_2, \dots, 0) + x_nf(x_1, x_2, \dots, 1)$$

## 記法: $R_i$

$$R_i f(x_1, \dots, x_i, \dots, x_n)$$

$$= (1 - x_i)f(x_1, \dots, 0, \dots, x_n) + x_if(x_1, \dots, 1, \dots, x_n)$$

$$f(x_1, x_2, x_3) = x_1^2(2 - x_2)^3 x_3 + (1 - x_1)x_3(2 - x_3) \quad \text{のとき}$$

$$\begin{aligned} R_1 f(x_1, x_2, x_3) &= (1 - x_1)(0^2(2 - x_2)^3 x_3 + (1 - 0)x_3(2 - x_3)) \\ &\quad + x_1(1^2(2 - x_2)^3 x_3 + (1 - 1)x_3(2 - x_3)) \\ &= (1 - x_1)x_3(2 - x_3) + 2x_1(2 - x_2)^3 x_3 \end{aligned}$$

$$\begin{aligned} R_2 R_1 f(x_1, x_2, x_3) &= R_2((1 - x_1)x_3(2 - x_3) + x_1(2 - x_2)^3 x_3) \\ &= (1 - x_2)((1 - x_1)x_3(2 - x_3) + x_1(2 - 0)^3 x_3) \\ &\quad + x_2((1 - x_1)x_3(2 - x_3) + x_1(2 - 1)^3 x_3) \\ &= (1 - x_1)x_3(2 - x_3) + x_1(8 - 7x_2)x_3 \end{aligned}$$

$$\begin{aligned} R_3 R_2 R_1 f(x_1, x_2, x_3) &= R_3((1 - x_1)x_3(2 - x_3) + x_1(8 - 7x_2)x_3) \\ &= (1 - x_3)((1 - x_1)0(2 - 0) + x_1(8 - 7x_2)0) \\ &\quad + x_3((1 - x_1)1(2 - 1) + x_1(8 - 7x_2)1) \\ &= x_3(1 + 7x_1(1 - x_2)) \end{aligned}$$



便宜上, 次も定義する

$$E_i f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 0, \dots, x_n) + f(x_1, \dots, 1, \dots, x_n)$$

( $\exists x_i$  に対応)

$$A_i f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 0, \dots, x_n) \cdot f(x_1, \dots, 1, \dots, x_n)$$

( $\forall x_i$  に対応)

便宜上, 次も定義する

$$E_i f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 0, \dots, x_n) + f(x_1, \dots, 1, \dots, x_n)$$

( $\exists x_i$  に対応)

$$A_i f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 0, \dots, x_n) \cdot f(x_1, \dots, 1, \dots, x_n)$$

( $\forall x_i$  に対応)

このとき, 算術化で解くことは次に対応する

$$\exists x_1 \forall x_2 \dots \forall x_n : \varphi(x_1, x_2, \dots, x_n) = 1$$

$\Updownarrow$

$$E_1 R_1 A_2 R_2 R_1 \dots A_n R_n R_{n-1} \dots R_1 f(x_1, x_2, \dots, x_n) > 0$$

便宜上, 次も定義する

$$E_i f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 0, \dots, x_n) + f(x_1, \dots, 1, \dots, x_n)$$

( $\exists x_i$  に対応)

$$A_i f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 0, \dots, x_n) \cdot f(x_1, \dots, 1, \dots, x_n)$$

( $\forall x_i$  に対応)

このとき, 算術化で解くことは次に対応する

$$\exists x_1 \forall x_2 \dots \forall x_n : \varphi(x_1, x_2, \dots, x_n) = 1$$

$\Updownarrow$

$$\underline{E_1 R_1 A_2 R_2 R_1 \dots A_n R_n R_{n-1} \dots R_1 f(x_1, x_2, \dots, x_n) > 0}$$

$O(n^2)$  個の記号 (多項式で収まっている)

$$\frac{E_1 R_1 A_2 R_2 R_1 \dots A_n R_n R_{n-1} \dots R_1 f(x_1, x_2, \dots, x_n)}{= f_0()}$$

$$\begin{aligned} & E_1 R_1 A_2 R_2 R_1 \dots A_n R_n R_{n-1} \dots R_1 f(x_1, x_2, \dots, x_n) \\ & \hline & = f_0() \\ & \hline & = f_1(x_1) \end{aligned}$$

$$\frac{E_1 R_1 A_2 R_2 R_1 \dots A_n R_n R_{n-1} \dots R_1 f(x_1, x_2, \dots, x_n)}{= f_0()}$$

$$= f_1(x_1)$$

$$= Sg(x)$$

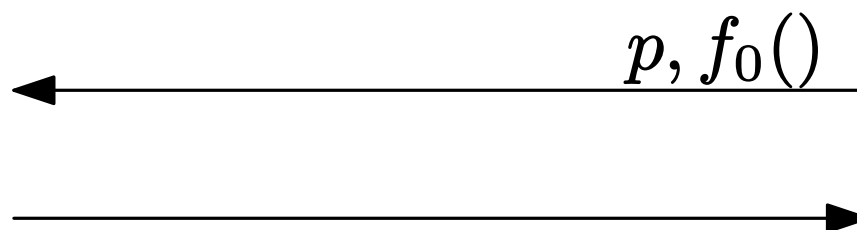
$$= g(x)$$

$$\begin{aligned} & \frac{E_1 R_1 A_2 R_2 R_1 \dots A_n R_n R_{n-1} \dots R_1 f(x_1, x_2, \dots, x_n)}{=} f_0() \\ & \frac{=} f_1(x_1) \\ & \frac{=} Sg(x) \\ & \frac{=} g(x) \end{aligned}$$

## プロトコルで行うこと

- $Sg(x)$  が正しいときに,  
 $g(x)$  が正しいことを (乱数で) 検証する

0. (検証者) スキップ
1. (証明者) 十分大きな素数  $p$  と  $f_0()$  を送付
2. (検証者)  $p$  が素数であることと  $f_0() > 0$  を確認  
( $\leadsto$  そうでないとき, ただちに No を出力)  
証明者に次のメッセージを要求

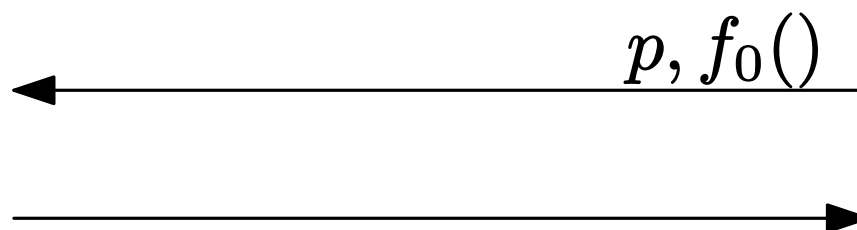




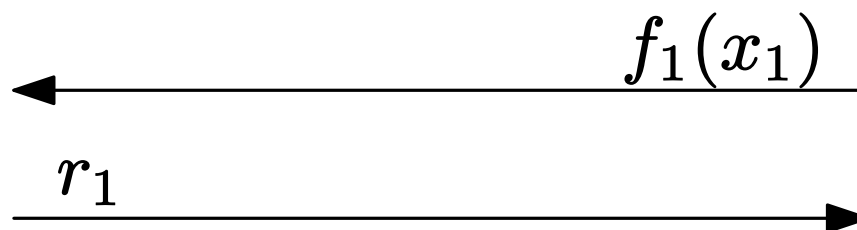
0. (検証者) スキップ
1. (証明者) 十分大きな素数  $p$  と  $f_0()$  を送付
2. (検証者)  $p$  が素数であることと  $f_0() > 0$  を確認  
( $\leadsto$  そうでないとき, ただちに No を出力)  
証明者に次のメッセージを要求

注 : 素数判定  $\in$  RP (Miller '76, Rabin '80)

素数判定  $\in$  P (Agrawal, Kayal, Saxena '04)



3. (証明者)  $f_1(x_1)$  を送付
4. (検証者)  $f_0() = f_1(0) + f_1(1)$  を確認  
( $\leadsto$  「 $\neq$ 」 のとき, ただちに No を出力)  
 $r_1 \in \{0, 1, \dots, p-1\}$  をランダムに作成し, 送付



仮定 :  $Sg(x_1, \dots, x_j)$  が正しいことを検証済

$j$ . (証明者)  $g(r_1, \dots, r_{j-1}, x_j)$  を送付

$j+1$ . (検証者)  $S$  によって場合分け

$S = E_j$  のとき

$Sg(r_1, \dots, r_{j-1}, x_j) = g(r_1, \dots, r_{j-1}, 0) + g(r_1, \dots, r_{j-1}, 1)$   
を確認 ( $\sim$ 「 $\neq$ 」のとき, ただちに No を出力)



$\longleftarrow g(r_1, \dots, r_{j-1}, x_j)$



仮定 :  $Sg(x_1, \dots, x_j)$  が正しいことを検証済

$j$ . (証明者)  $g(r_1, r_2, \dots, r_{j-1}, x_j)$  を送付

$j+1$ . (検証者)  $S$  によって場合分け

$S = A_j$  のとき

$Sg(r_1, \dots, r_{j-1}, x_j) = g(r_1, \dots, r_{j-1}, 0) \cdot g(r_1, \dots, r_{j-1}, 1)$   
を確認 ( $\sim$  「 $\neq$ 」 のとき, ただちに No を出力)



$\xleftarrow{g(r_1, \dots, r_{j-1}, x_j)}$



仮定 :  $Sg(x_1, \dots, x_j)$  が正しいことを検証済

$j$ . (証明者)  $g(r_1, r_2, \dots, r_{j-1}, x_j)$  を送付

$j+1$ . (検証者)  $S$  によって場合分け

$S = R_j$  のとき, 乱数  $r_j \in \{0, \dots, p-1\}$  を作って

$Sg(r_1, \dots, r_{j-1}, r_j) =$

$(1 - r_j)g(r_1, \dots, r_{j-1}, 0) + r_jg(r_1, \dots, r_{j-1}, 1)$

を確認 ( $\leadsto$  「 $\neq$ 」 のとき, ただちに No を出力)



$\xleftarrow{g(r_1, \dots, r_{j-1}, x_j)}$





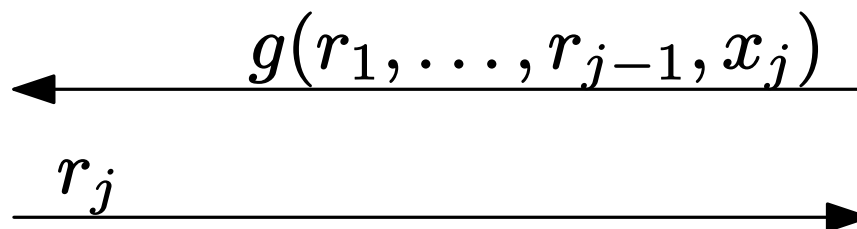
仮定 :  $Sg(x_1, \dots, x_j)$  が正しいことを検証済

$j$ . (証明者)  $g(r_1, r_2, \dots, r_{j-1}, x_j)$  を送付

$j+1$ . (検証者)  $S$  によって場合分け

...

$r_j \in \{0, \dots, p-1\}$  をランダムに作成し, 送付

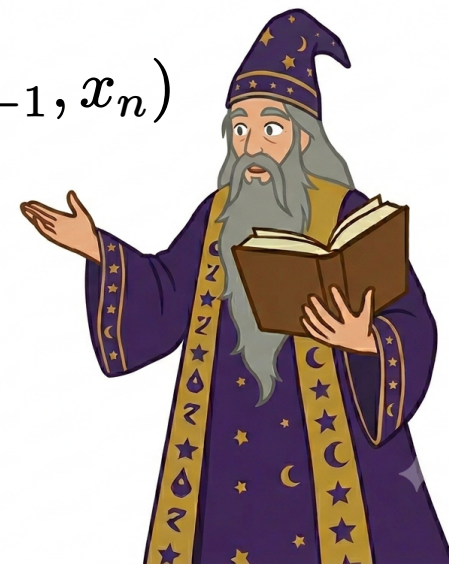
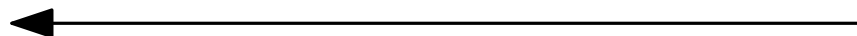


## 最後のステップ. (検証者)

$r_n \in \{0, 1, \dots, p-1\}$  をランダムに作成し,  
最後に送られた多項式  $(r_1, \dots, r_n) = f(r_1, \dots, r_n)$  を確認  
 $\leadsto$  「=」 のとき Yes, 「 $\neq$ 」 のとき No を出力



最後に送られた多項式  $(r_1, \dots, r_{n-1}, x_n)$

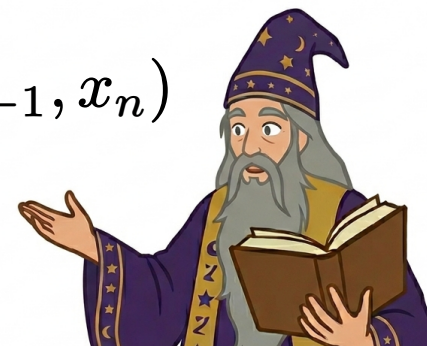
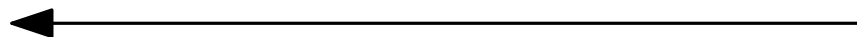


## 最後のステップ. (検証者)

$r_n \in \{0, 1, \dots, p-1\}$  をランダムに作成し,  
最後に送られた多項式  $(r_1, \dots, r_n) = f(r_1, \dots, r_n)$  を確認  
 $\leadsto$  「=」 のとき Yes, 「 $\neq$ 」 のとき No を出力



最後に送られた多項式  $(r_1, \dots, r_{n-1}, x_n)$



正当性の証明は  $\#SAT \in IP$  のとき (前回) と同様に行える  $\square$

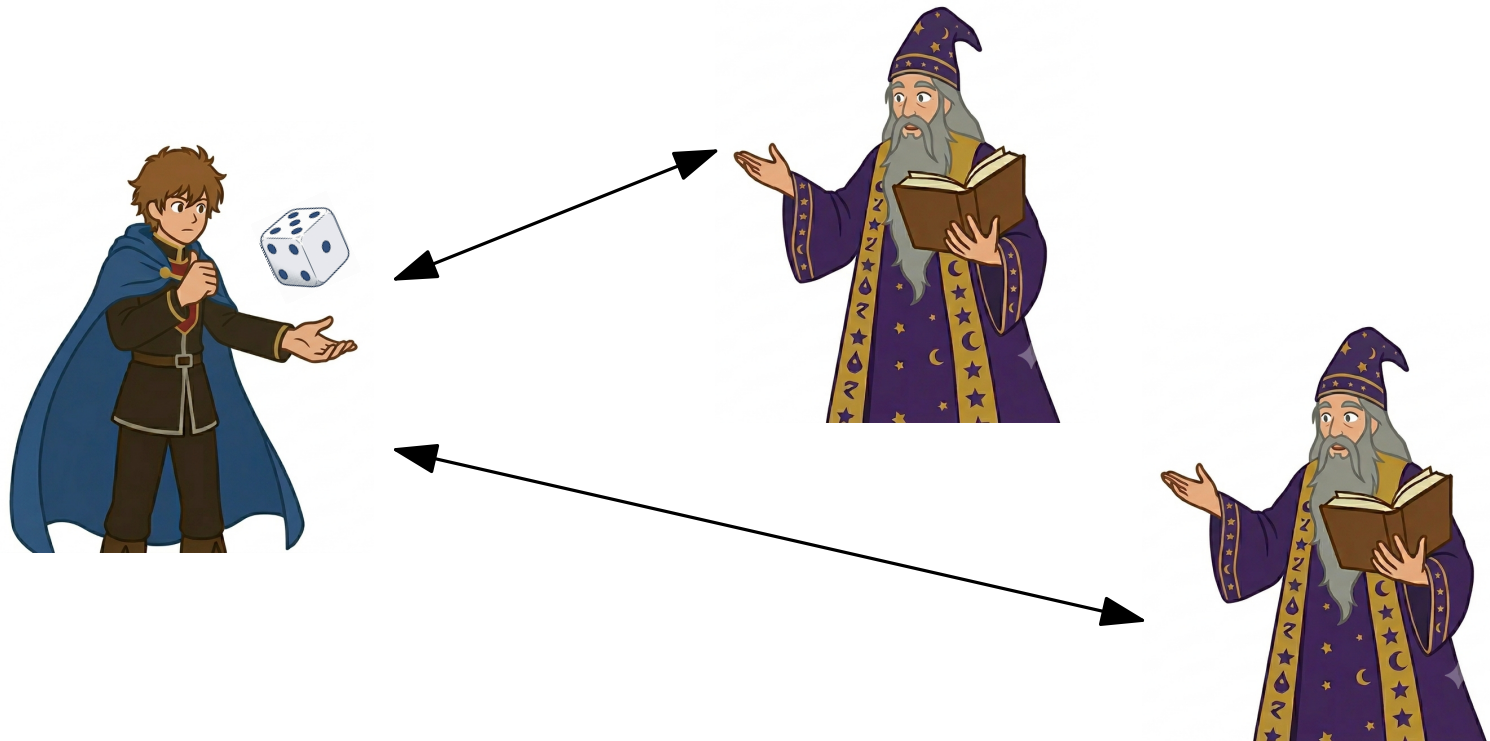


1. PSPACE  $\subseteq$  IP の証明
2. **対話証明系に関する補足**

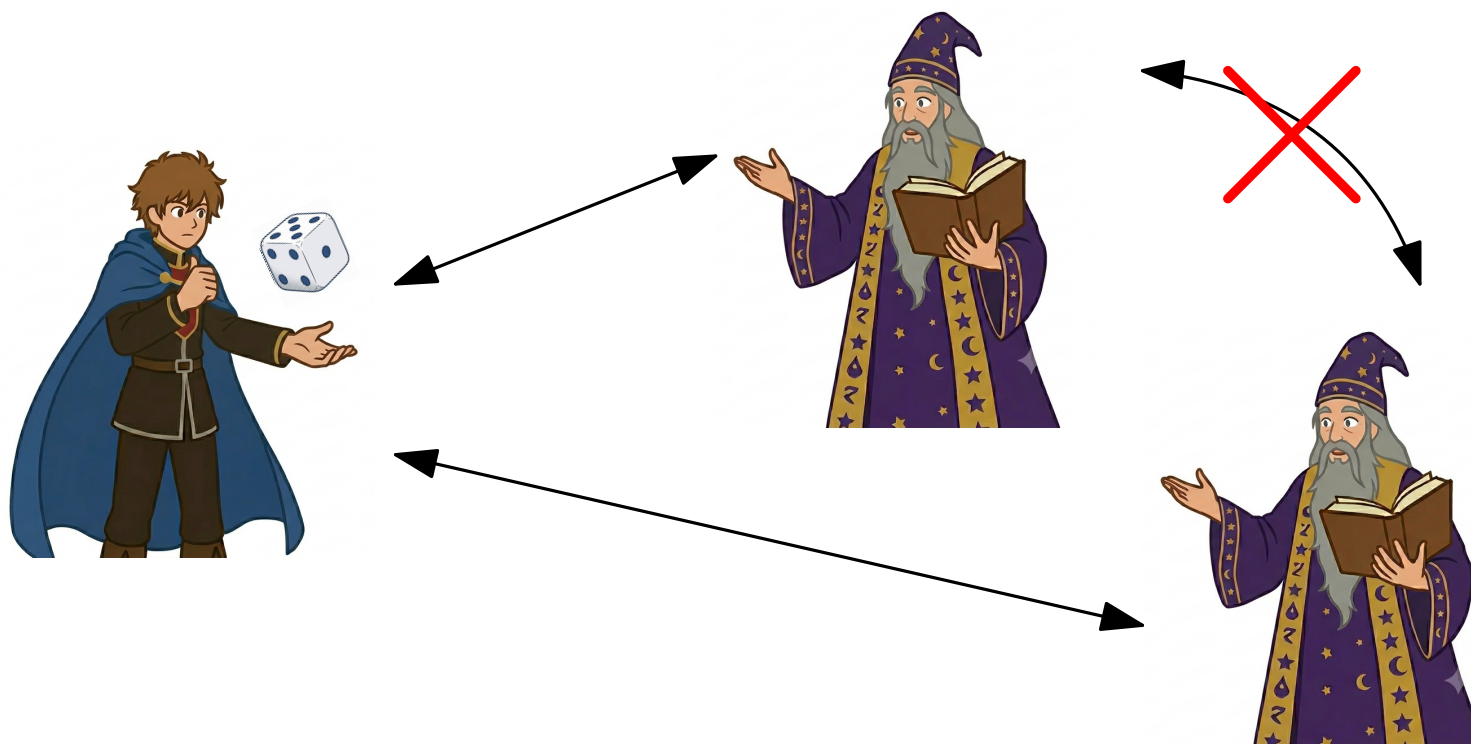
## 疑問

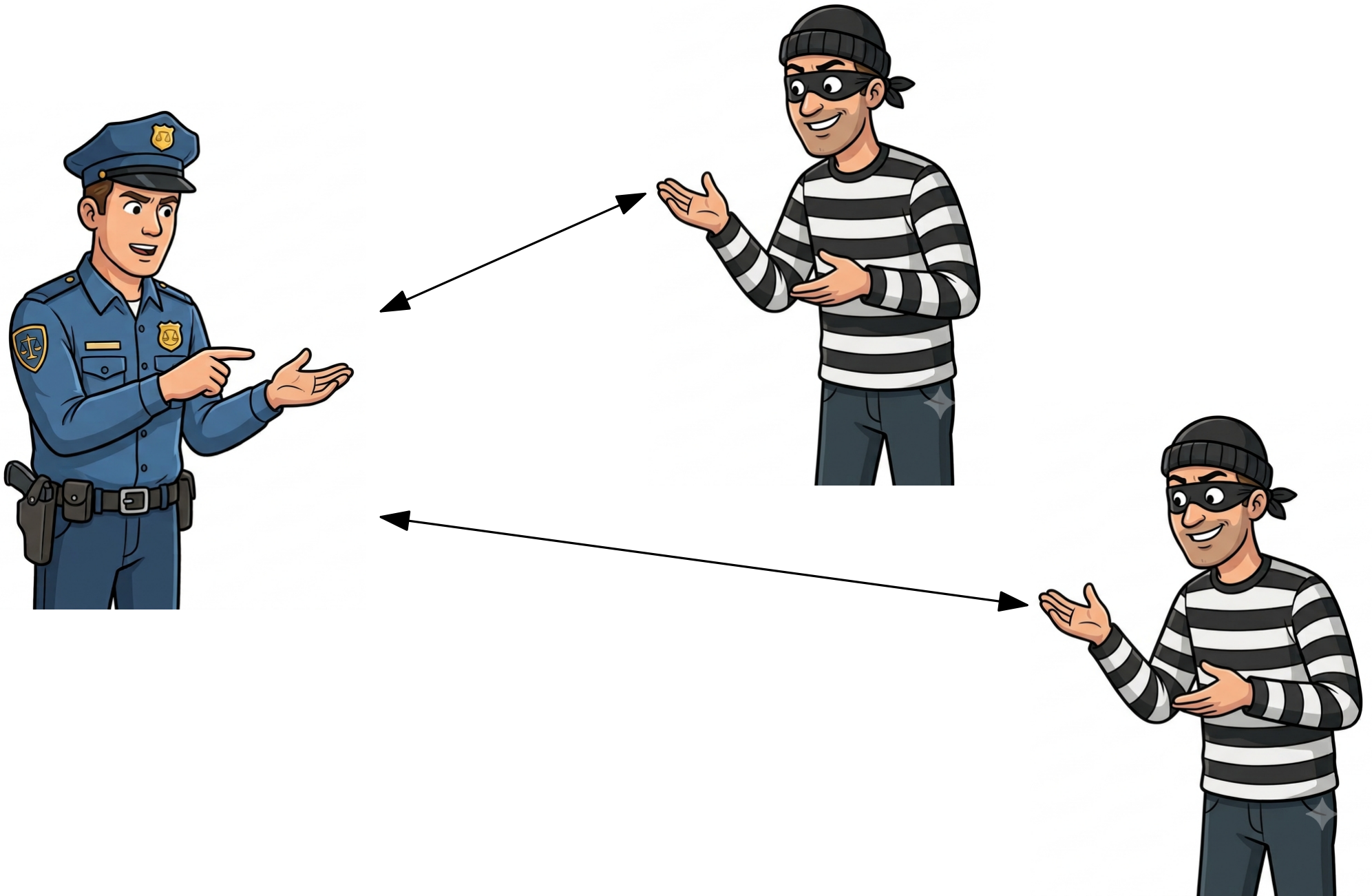
証明者が複数いると、どうなるか？

- 2 人いると、計算能力は上がるか？
- 3 人いると、計算能力は上がるか？



- 証明者の間の通信は許さない  
(そうでないと, 一人の証明者と変わらない)
- 乱数は private coin  
(そうでないと, 一人の証明者と変わらない)



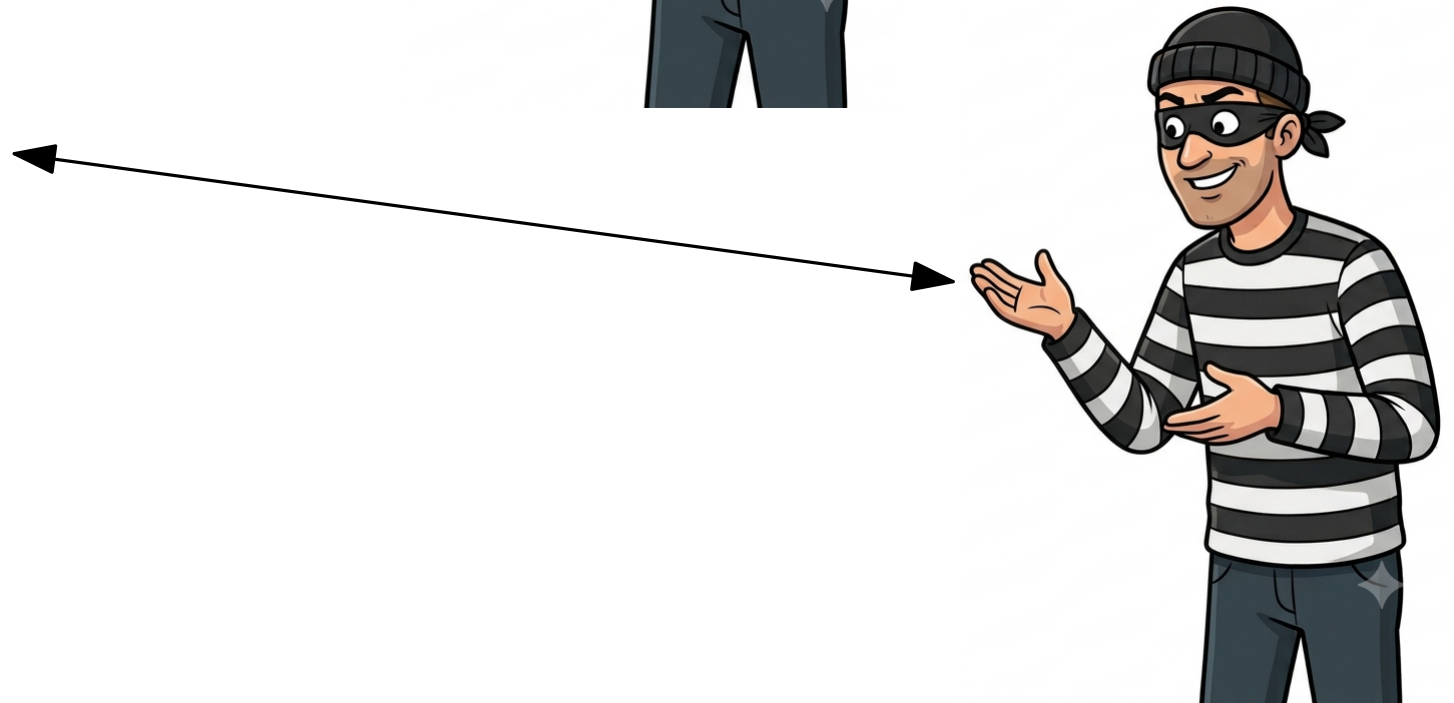




無罪/有罪を  
判断したい



「無罪」と  
判断させたい



## 複数の証明者：知られていること

- IP の 2 証明者バージョン = IP の 3 証明者バージョン  
= IP の 4 証明者バージョン  
= IP の  $k$  証明者バージョン  
( $k$  は定数)

(Ben-Or, Goldwasser, Kilian, Wigderson '88)

- IP の 2 証明者バージョン = NEXPTIME  
(Babai, Fortnow, Lund '91)

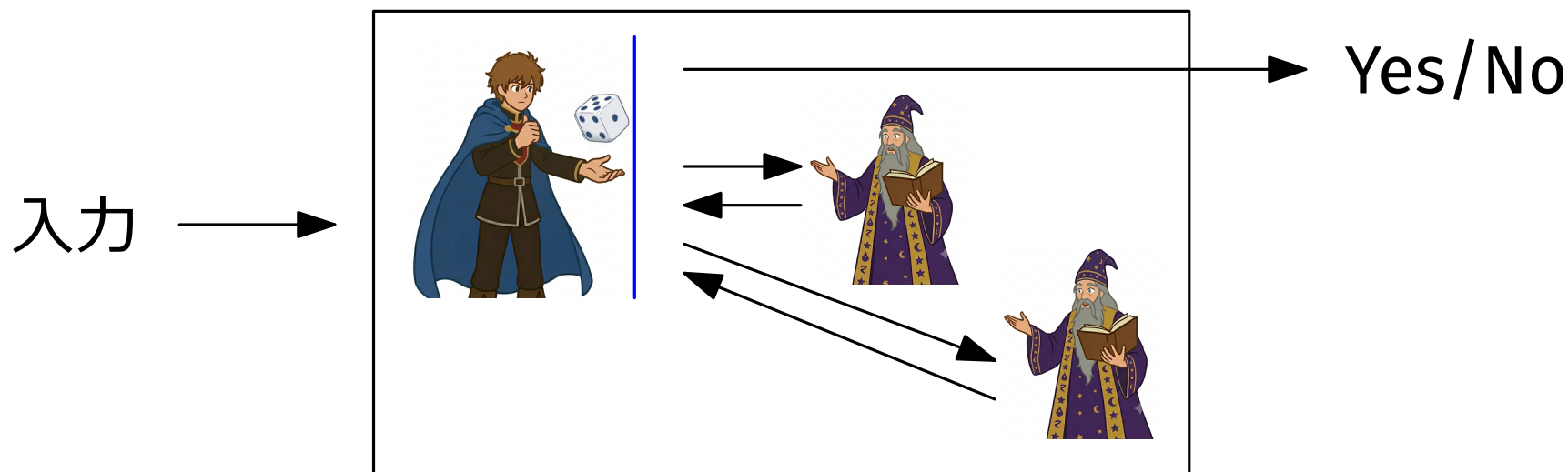
## 複雑性クラス MIP

**クラス MIP** は次を満たすプロトコルで解ける問題全体

- 証明者は 2 人 で, 証明者どうしの通信はできない
- 検証者と証明者が 多項式回のラウンド で動作を行う
- 検証者の乱数は証明者から 見えない (private coin)

(Ben-Or, Goldwasser, Kilian, Wigderson '88)

MIP = Multi-prover Interactive Proof





## 複雑性クラス MIP

**クラス MIP** は次を満たすプロトコルで解ける問題全体

- 証明者は 2 人 で, 証明者どうしの通信はできない
- 検証者と証明者が 多項式回のラウンド で動作を行う
- 検証者の乱数は証明者から 見えない (private coin)

(Ben-Or, Goldwasser, Kilian, Wigderson '88)

MIP = Multi-prover Interactive Proof

前のページの 2 番目の事実の言い換え

MIP = NEXPTIME



## 本日のまとめ

- $IP = PSPACE$  の証明を完了した
- 複数の証明者を持つ対話証明系を導入し,  
 $MIP = NEXPTIME$  となることを紹介した

Q

1.

2.

3.

4.