理論計算機科学特論 (2026 年前学期)

計算複雑性の基礎

第 12 回

確率的計算：PP, RP, BPP, ZPP

岡本 吉央　(電気通信大学)

okamotoy@uec.ac.jp

2026 年 6 月 30 日

最終更新：2026 年 6 月 29 日　11:38

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：$\mathrm{P} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}$ (5/12)
6. 階層定理：$\mathrm{P} \neq \mathrm{EXPTIME}$ (5/19)
7. Ladner の定理：$\mathrm{NP} - \mathrm{P} = \mathrm{NPC} \Rightarrow \mathrm{P} = \mathrm{NP}$ (5/26)

スケジュール (後半)

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 ⇒ P = PH (6/23)
12. **確率的計算：PP, RP, BPP, ZPP** (6/30)
13. 対話証明系 (1)：NP ⊆ MA ⊆ AM (7/7)
14. 対話証明系 (2)：IP ⊆ PSPACE (7/14)
15. 対話証明系 (3)：PSPACE ⊆ IP (7/21)

* 休み (授業のない日) (7/28)

本日の内容

内容

- **確率的** な動作を行う計算モデルを導入する
- 複雑性クラス PP，RP，coRP，BPP，ZPP を導入する
- **再実行** と **確率増幅** という重要な技法を紹介する
- (BPP $\subseteq \Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$ を証明する)

本編は 44 ページまで (それ以降は付録)

本日の内容

1. **確率的計算と複雑性クラス**
2. 再実行と確率増幅

確率的アルゴリズム

確率的アルゴリズム (randomized algorithm) では

命令 rand を使える

- 有限集合 X に対して，rand(X) とすると，
  X の要素を一様分布に従って 1 つ選べる
  - それにかかる時間 $= O(\log |X|)$ ステップ

注意：確率的な選択 $\neq$ 非決定的な選択

ポイント

- rand は普通のプログラムで (疑似的に) 実現できる

- $\leftrightarrow$ 非決定性の guess は実現できない

確率的アルゴリズム：例

この質問に正しく答えたい

集合 X $= \{2, 4, 6, 9\}$ の中に $a + b = 10$ となる $a, b \in X$ があるか？

確率的

```
a = rand(X)
b = rand(X)
if a + b == 10:
  return "Yes"
else:
  return "No"
end
```

非決定性

```
a = guess(X)
b = guess(X)
if a + b == 10:
  return "Yes"
else:
  return "No"
end
```

確率的アルゴリズム：例

この質問に正しく答えたい

集合 X $= \{2, 4, 6, 9\}$ の中に $a + b = 10$ となる $a, b \in X$ があるか？

確率的

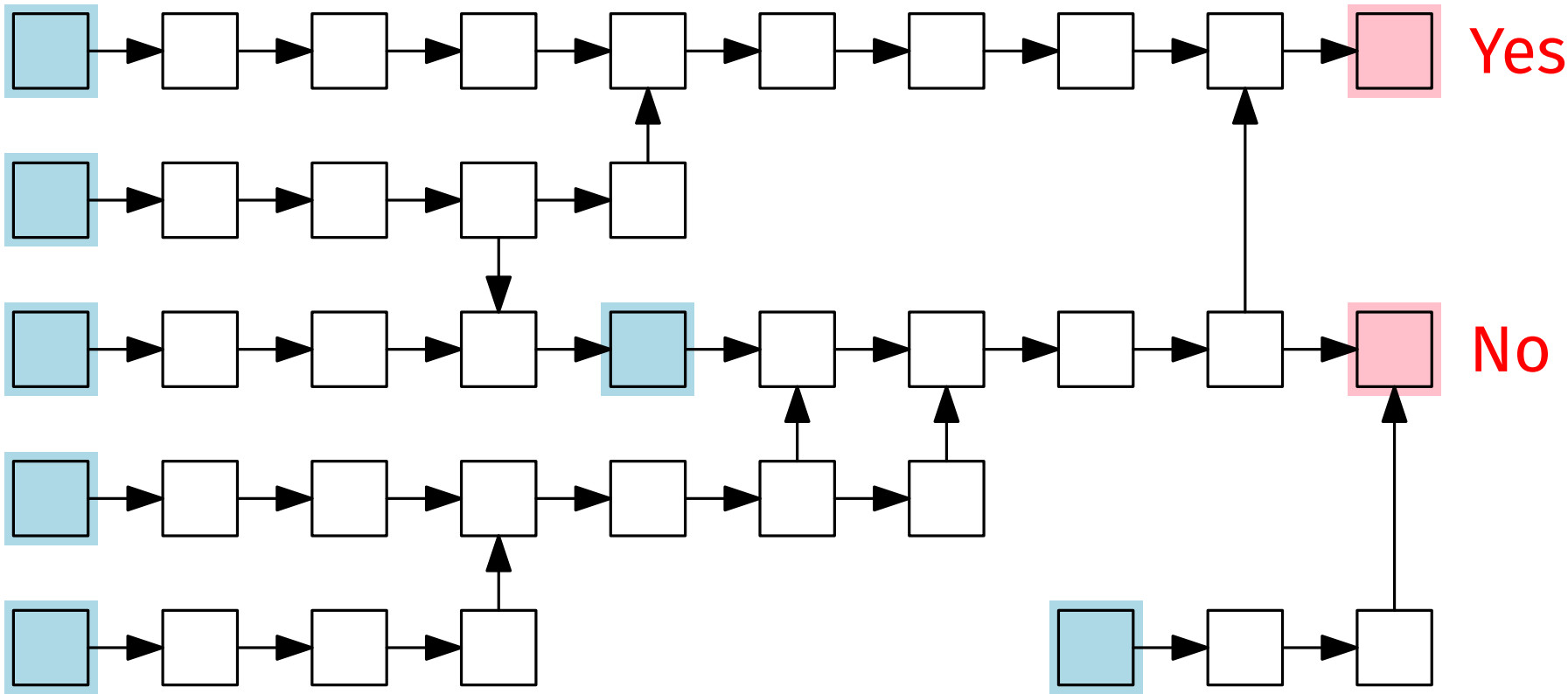
```
a = rand(X)
b = rand(X)
if a + b == 10:
  return "Yes"
else:
  return "No"
end
```

非決定性

```
a = guess(X)
b = guess(X)
if a + b == 10:
  return "Yes"
else:
  return "No"
end
```

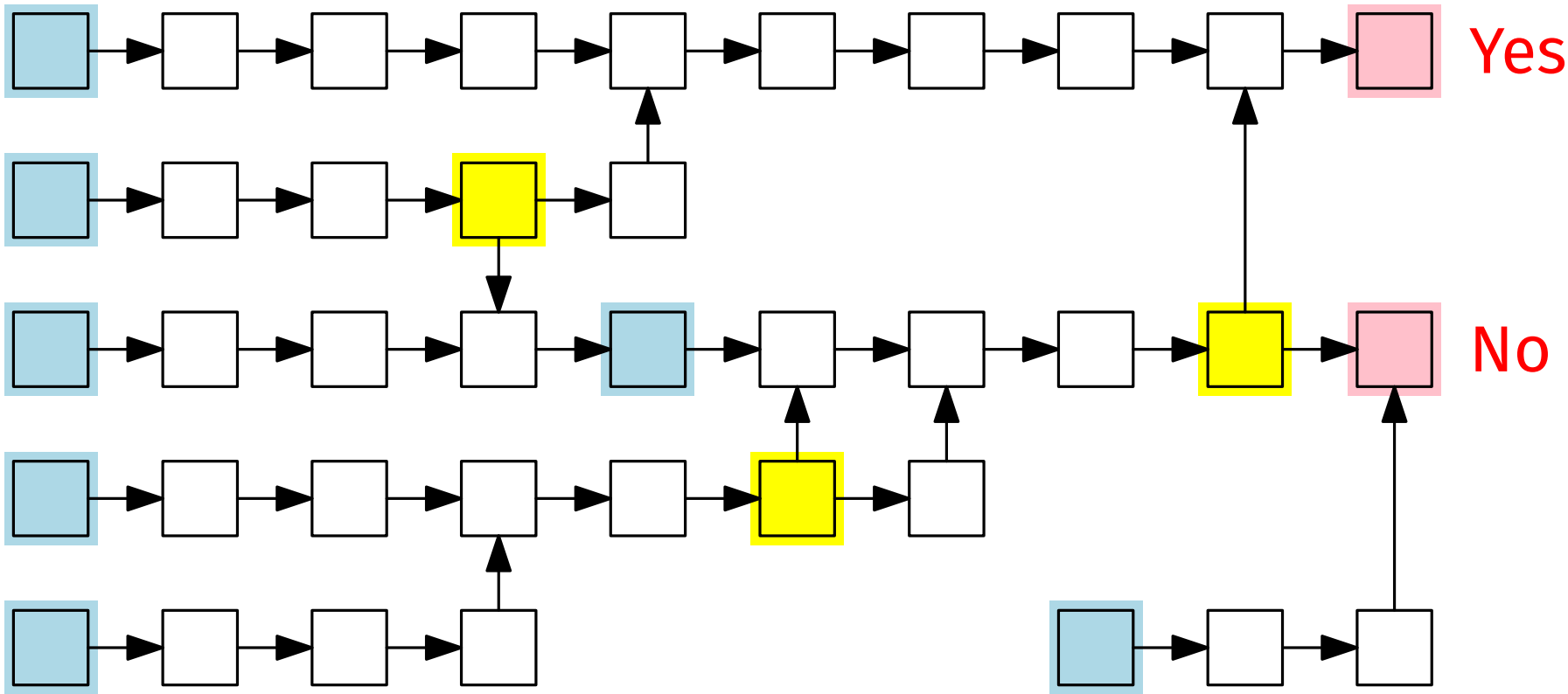
正しく Yes を出力する保証がない → 成功確率に着目 (後述)

確率的アルゴリズムと時点状況



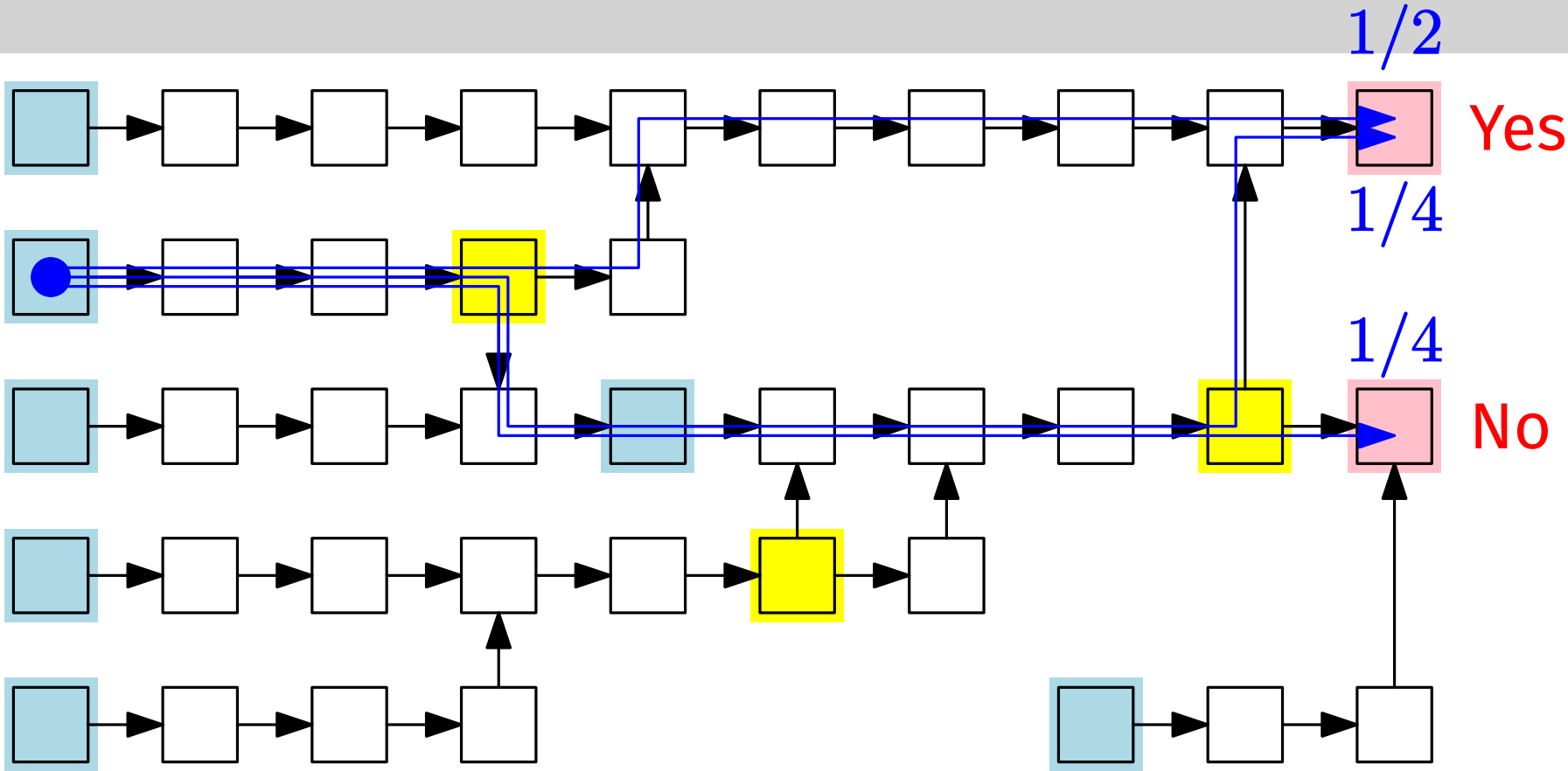
- 確率的アルゴリズムでは,
  各状況に対して次の状況が一意に決まるとは限らない
  (それでも，高々 2 つとする)
- rand = 次の状況の一様な選択

確率的アルゴリズムと時点状況



- 確率的アルゴリズムでは,
  各状況に対して次の状況が一意に決まるとは限らない
  (それでも，高々 2 つとする)
- rand = 次の状況の一様な選択

確率的アルゴリズムと時点状況



- 確率的アルゴリズムでは,
  各状況に対して次の状況が一意に決まるとは限らない
  (それでも，高々 2 つとする)
- rand = 次の状況の一様な選択

複雑性クラス PP

定義：PP (Gill '77)

クラス PP は次を満たす確率的アルゴリズム A が
存在する判定問題 P 全体のこと

- 任意の入力 I に対して,
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) > \frac{1}{2}$
  - I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) > \frac{1}{2}$

気分：コイントスよりはよい

A が使う確率性
(ランダム・ビット列)

PP = probabilistic polynomial time

複雑性クラス PP

定義：PP (Gill '77)

クラス PP は次を満たす確率的アルゴリズム A が
存在する判定問題 P 全体のこと

- 任意の入力 I に対して，
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow \boxed{\Pr_r(A(I) = \text{Yes})} > \frac{1}{2}$
  - I が No インスタンス $\Rightarrow \boxed{\Pr_r(A(I) = \text{No})} > \frac{1}{2}$

気分：コイントスよりはよい　　A の成功確率

PP $=$ probabilistic polynomial time

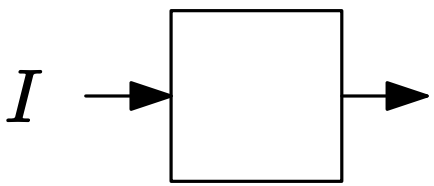
複雑性クラス PP

定義：PP (Gill '77)

クラス PP は次を満たす確率的アルゴリズム A が
存在する判定問題 P 全体のこと

- 任意の入力 I に対して，
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow \boxed{\Pr_r(A(I) = \text{Yes})} > \frac{1}{2}$
  - I が No インスタンス $\Rightarrow \boxed{\Pr_r(A(I) = \text{No})} > \frac{1}{2}$

気分：コイントスよりはよい　　A の成功確率



$$\Pr_r(I \text{ が Yes インスタンス} \mid A(I) = \text{Yes}) = \ ?$$

複雑性クラス PP：推定

仮定

- I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) = \frac{1}{2} + \varepsilon$
- I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) = \frac{1}{2} + \varepsilon$

例えば，$\varepsilon = \frac{1}{2^{|I|}}$

事象 $X =$「I が Yes インスタンス」, $Y =$「$A(I) = \text{Yes}$」として $\Pr(X) = p$ とする

$$\Pr(I \text{ が Yes インスタンス} \mid A(I) = \text{Yes})$$

$$= \Pr(X \mid Y)$$

$$= \frac{\Pr(Y \mid X)\Pr(X)}{\Pr(Y \mid X)\Pr(X) + \Pr(Y \mid \overline{X})\Pr(\overline{X})} \quad \leftarrow \text{Bayes の定理}$$

$$= \frac{(1/2 + \varepsilon) \cdot p}{(1/2 + \varepsilon) \cdot p + (1/2 - \varepsilon) \cdot (1 - p)} = \frac{(1 + 2\varepsilon) \cdot p}{1 + 2(2p - 1)\varepsilon} \approx p$$

∴ この成功確率保証 (仮定) では，情報がほとんど得られない

複雑性クラス RP

定義：RP (Gill '77)

クラス RP は次を満たす確率的アルゴリズム A が
存在する判定問題 P 全体のこと

- 任意の入力 I に対して,
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) \geq \frac{1}{2}$
  - I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) = 1$

気分：No インスタンスに対しては間違えない

RP = randomized polynomial time

複雑性クラス RP：推定

仮定

- I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) = \dfrac{1}{2}$
- I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) = 1$

事象 $X =$「I が Yes インスタンス」, $Y =$「$A(I) = \text{Yes}$」として
$\Pr(X) = p$ とする

$$
\begin{aligned}
&\Pr(I \text{ が Yes インスタンス} \mid A(I) = \text{Yes}) \\
&= \Pr(X \mid Y) \\
&= \frac{\Pr(Y \mid X)\Pr(X)}{\Pr(Y \mid X)\Pr(X) + \Pr(Y \mid \overline{X})\Pr(\overline{X})} \\
&= \frac{(1/2) \cdot p}{(1/2) \cdot p + 0 \cdot (1-p)} = 1
\end{aligned}
$$

∴ 出力が Yes のとき，その出力は必ず正しい

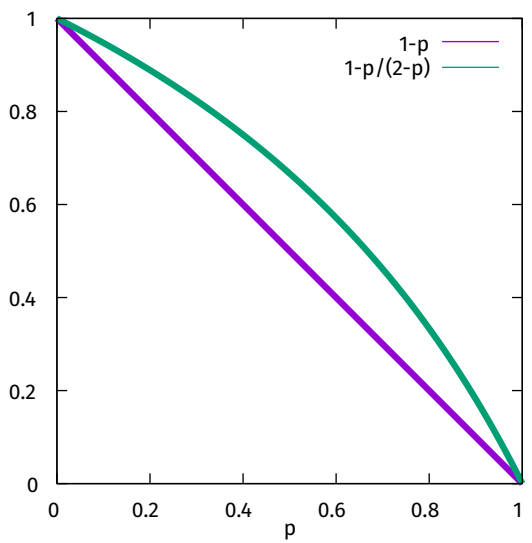
複雑性クラス RP：推定 (続)

仮定

- I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) = \dfrac{1}{2}$
- I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) = 1$

事象 $X =$「I が Yes インスタンス」, $Y =$「$A(I) = \text{Yes}$」として
$\Pr(X) = p$ とする

$$
\begin{aligned}
&\Pr(I \text{ が No インスタンス} \mid A(I) = \text{No}) \\
&= \Pr(\overline{X} \mid \overline{Y}) \\
&= \frac{\Pr(\overline{Y} \mid \overline{X}) \Pr(\overline{X})}{\Pr(\overline{Y} \mid \overline{X}) \Pr(\overline{X}) + \Pr(\overline{Y} \mid X) \Pr(X)} \\
&= \frac{1 \cdot (1-p)}{1 \cdot (1-p) + 1/2 \cdot p} = 1 - \frac{p}{2-p} \geq 1 - p
\end{aligned}
$$



∴ 出力が No のとき，必ず正しいわけではないが，情報はある

複雑性クラス coRP

coRP は次の性質を満たす

クラス coRP は次を満たす確率的アルゴリズム A が存在する判定問題 P 全体のこと

- 任意の入力 I に対して，
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) = 1$
  - I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) \geq \frac{1}{2}$

気分：Yes インスタンスに対しては間違えない

性質：出力が No のとき，その出力は必ず正しい

複雑性クラス BPP

定義：BPP (Gill '77)

クラス BPP は次を満たす確率的アルゴリズム A が存在する判定問題 P 全体のこと

- 任意の入力 I に対して,
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) \geq \frac{2}{3}$
  - I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) \geq \frac{2}{3}$

気分：Yes/No インスタンスのどちらも,
成功確率が大きい (が 1 とは限らない)

BPP = bounded-error probabilistic polynomial time

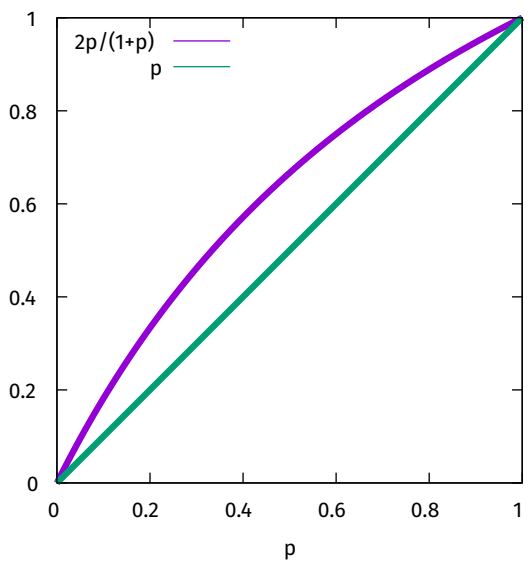
複雑性クラス BPP：推定

仮定

- I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) = \frac{2}{3}$
- I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) = \frac{2}{3}$

事象 $X =$「I が Yes インスタンス」, $Y =$「$A(I) = \text{Yes}$」として
$\Pr(X) = p$ とする

$$
\begin{aligned}
&\Pr(I \text{ が Yes インスタンス} \mid A(I) = \text{Yes}) \\
&= \Pr(X \mid Y) \\
&= \frac{\Pr(Y \mid X)\Pr(X)}{\Pr(Y \mid X)\Pr(X) + \Pr(Y \mid \overline{X})\Pr(\overline{X})} \\
&= \frac{(2/3)\cdot p}{(2/3)\cdot p + (1/3)\cdot(1-p)} = \frac{2p}{1+p} \geq p
\end{aligned}
$$



∴ 出力が Yes のとき，必ず正しいわけではないが，情報はある
(出力が No のときも同様)

複雑性クラス ZPP

定義：ZPP (Gill '77)

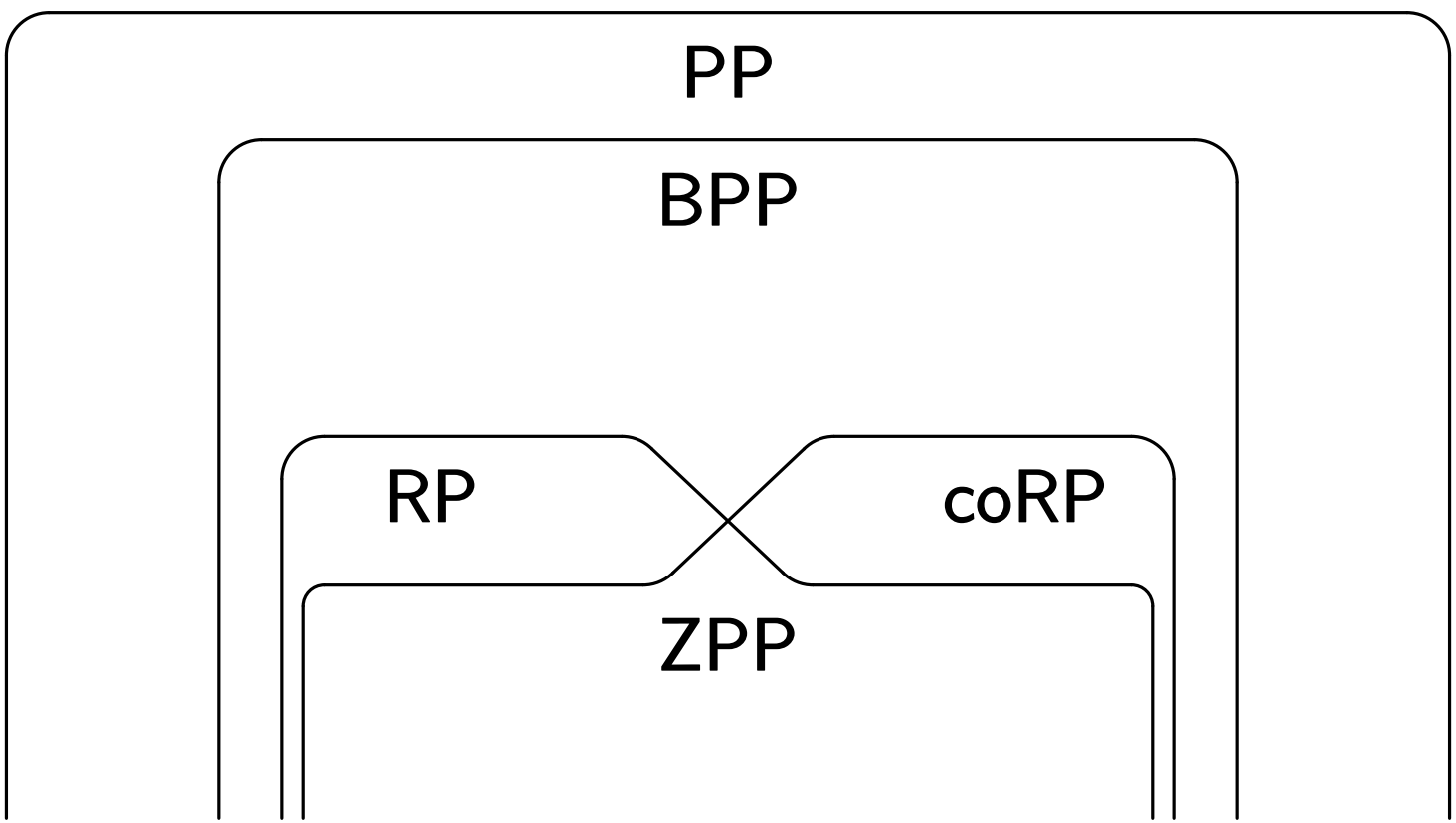
クラス ZPP は次を満たす確率的アルゴリズム A が存在する判定問題 P 全体のこと

- 任意の入力 I に対して，
  - 期待時間計算量が多項式
  - I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) = 1$
  - I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) = 1$

気分：必ず成功する
(しかし，最悪の場合，停止しないかもしれない)

ZPP = zero-error probabilistic polynomial time

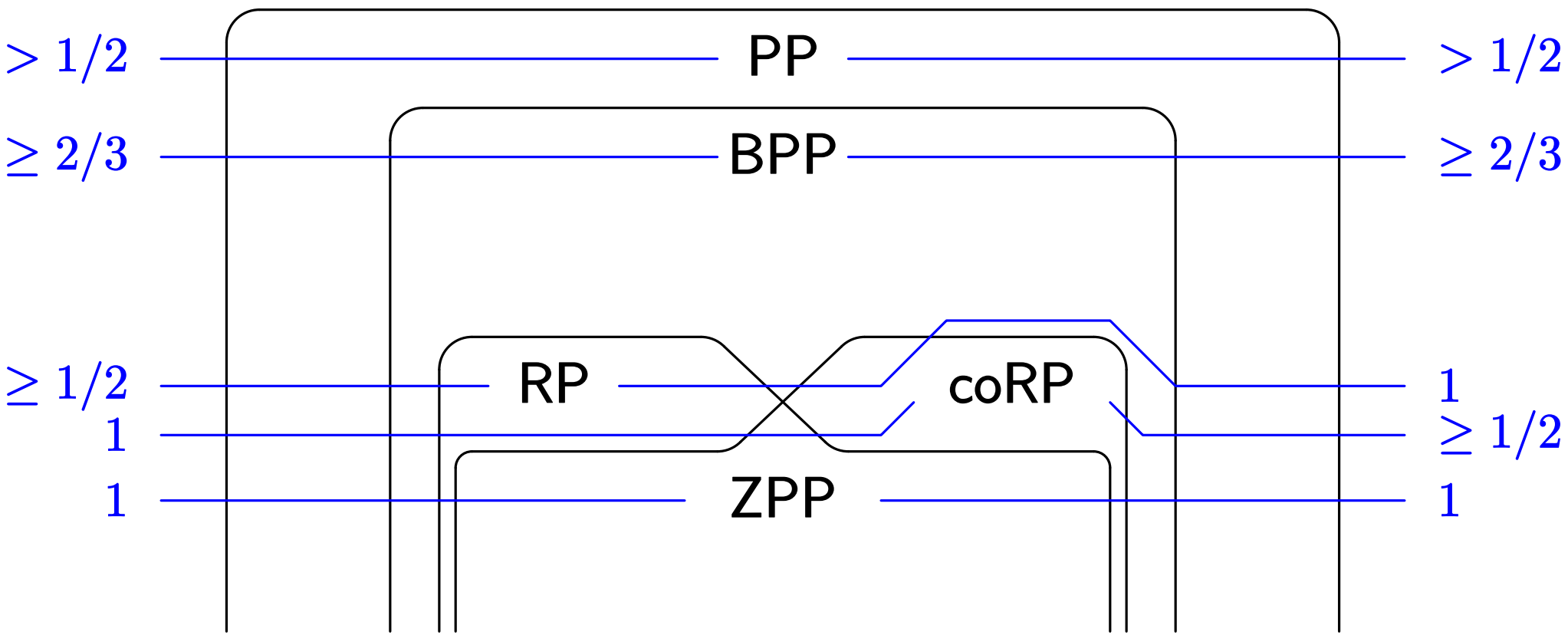
確率的複雑性クラス



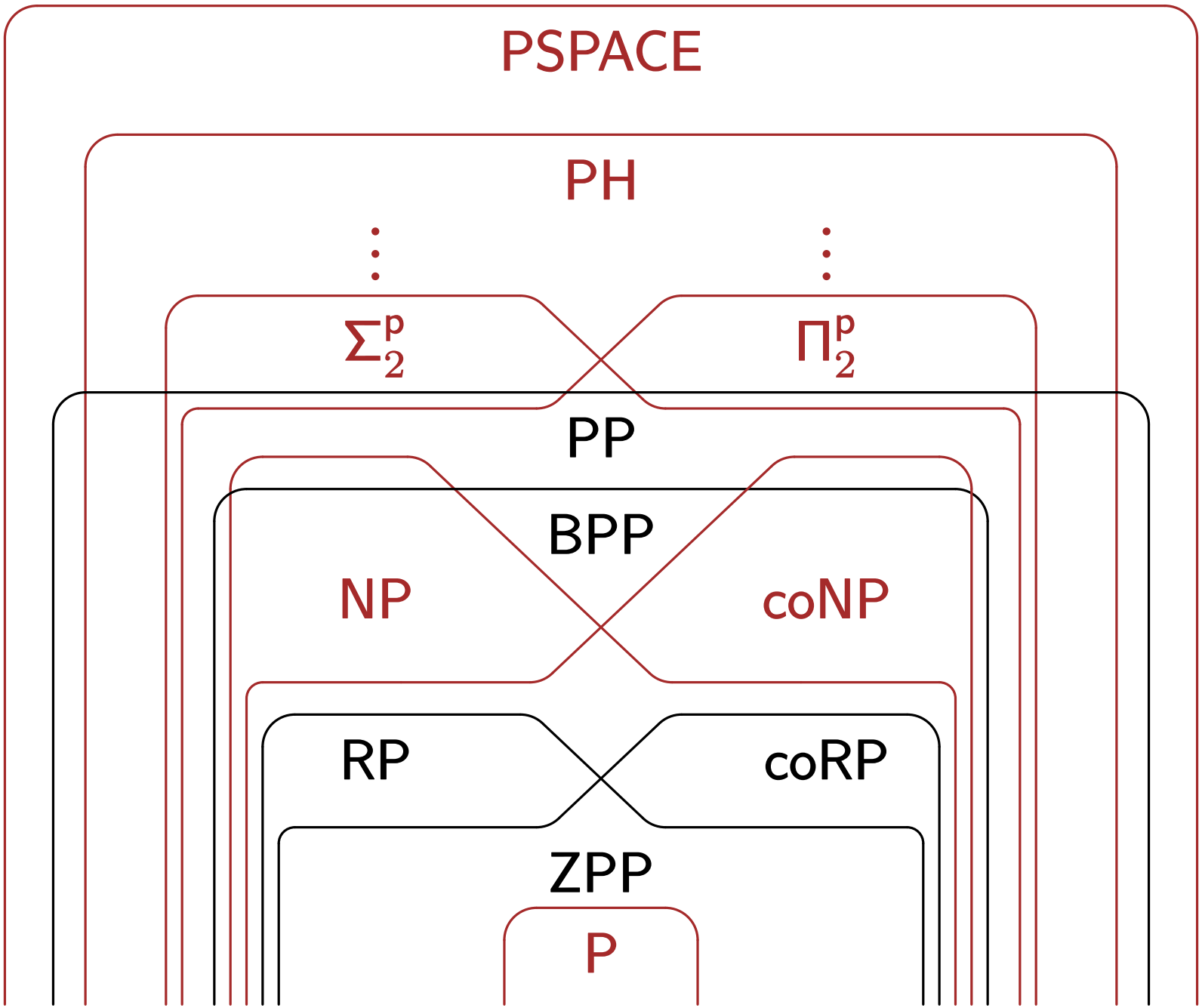
確率的複雑性クラス

入力が Yes インスタンスの
ときの成功確率

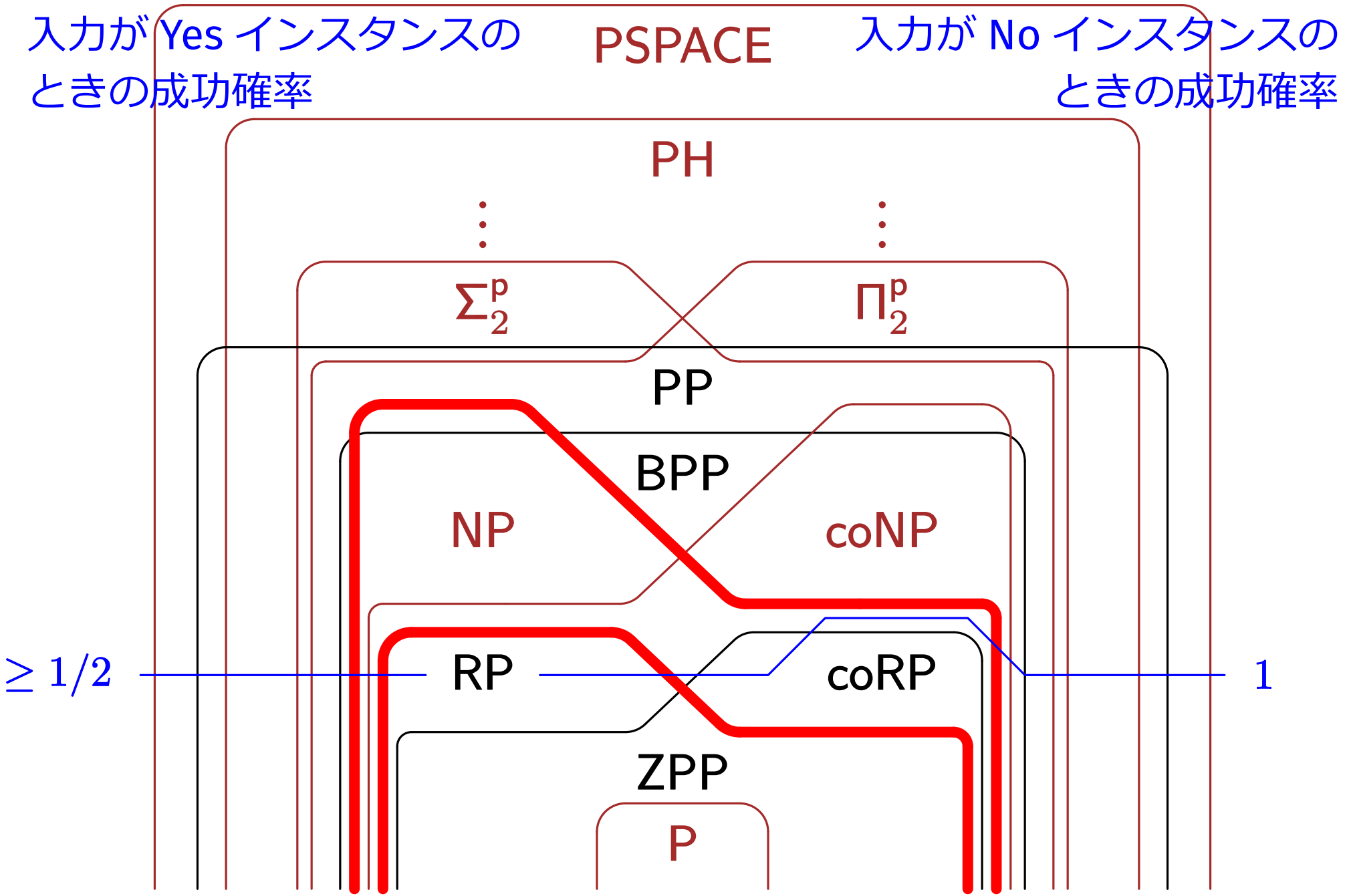
入力が No インスタンスの
ときの成功確率



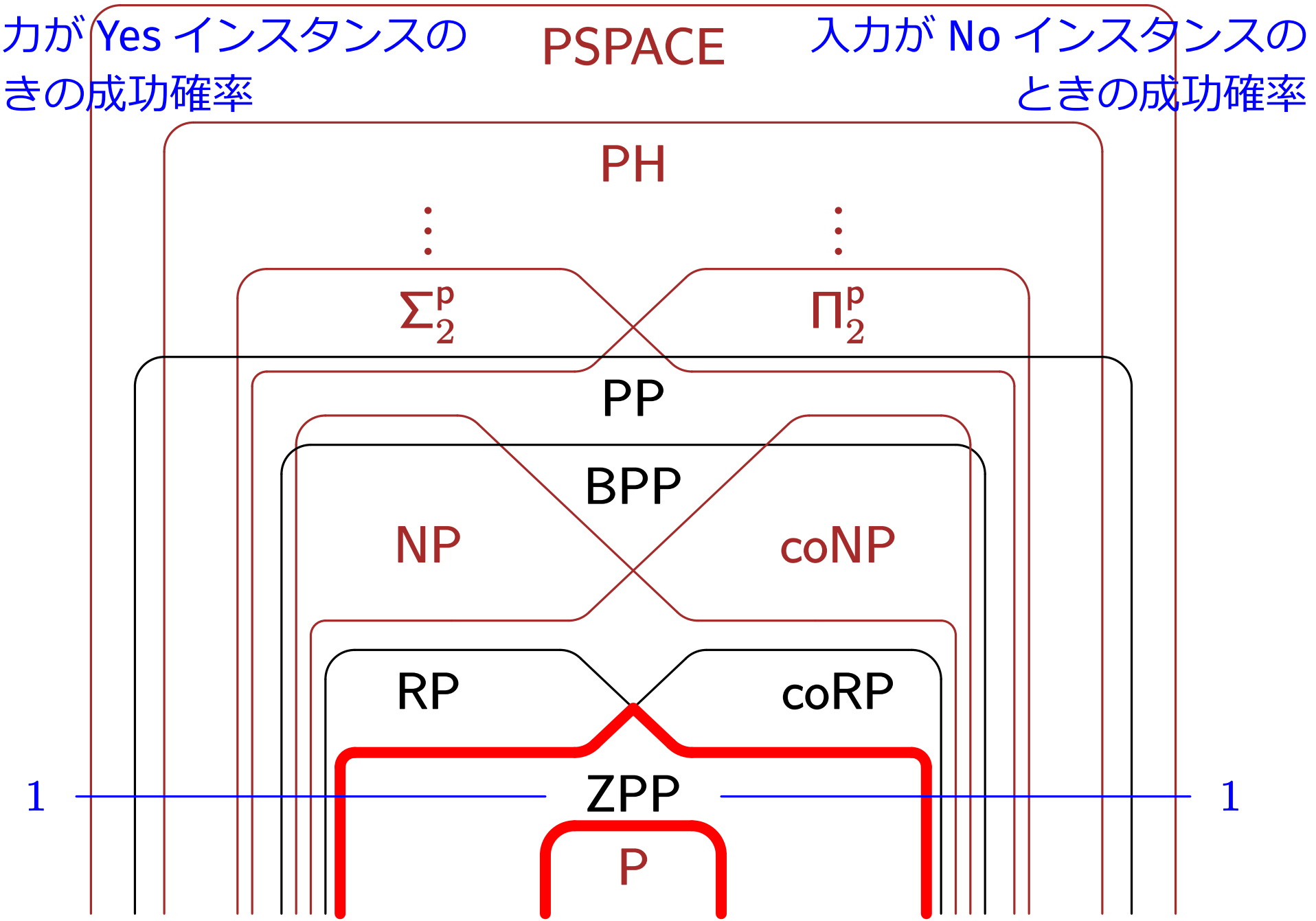
確率的複雑性クラス



確率的複雑性クラス


入力が Yes インスタンスのときの成功確率
PSPACE
入力が No インスタンスのときの成功確率
PH
Σ_2^p
Π_2^p
PP
BPP
NP
coNP
$\geq 1/2$
RP
coRP
1
ZPP
P

確率的複雑性クラス


入力が Yes インスタンスのときの成功確率
PSPACE
入力が No インスタンスのときの成功確率
PH
Σ_2^p
Π_2^p
PP
BPP
NP
coNP
RP
coRP
1
ZPP
1
P

確率的複雑性クラス：包含関係

確率的複雑性クラスの間の関係

- $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$ (次に説明)
- $\mathrm{RP} \subseteq \mathrm{BPP}$, $\mathrm{coRP} \subseteq \mathrm{BPP}$ (次に説明)
- $\mathrm{BPP} \subseteq \mathrm{PP}$ (定義から直ちに)

確率的複雑性クラスと多項式階層の間の関係

- $\mathrm{NP} \cup \mathrm{coNP} \subseteq \mathrm{PP} \subseteq \mathrm{PSPACE}$ (今までと同様 (付録))
- $\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$ (Sipser, Lautemann)
- $\mathrm{RP} \subseteq \mathrm{NP}$, $\mathrm{coRP} \subseteq \mathrm{coNP}$ (定義から直ちに)
- $\mathrm{P} \subseteq \mathrm{ZPP}$ (定義から直ちに)

未解決問題

これらの「$\subseteq$」が「$=$」か？

注意：多項式時間確率的アルゴリズム？

慣習

「多項式時間確率的アルゴリズム」といったら，普通は BPP が要請するようなものを指す

定義：BPP (Gill '77)

クラス BPP は次を満たす確率的アルゴリズム A が存在する判定問題 P 全体のこと

- 任意の入力 I に対して，
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow \Pr_r(A(I) = \text{Yes}) \geq \frac{2}{3}$
  - I が No インスタンス $\Rightarrow \Pr_r(A(I) = \text{No}) \geq \frac{2}{3}$

- PP の要請は弱すぎる
- RP, coRP, ZPP の要請は強すぎる

注意：用語

次の用語が (ほぼ) 区別なく用いられる

- 確率的アルゴリズム
- 乱数使用アルゴリズム
- 乱択アルゴリズム

英語においても，次の用語が (ほぼ) 区別なく用いられる

- probabilistic algorithm
- randomized algorithm
- stochastic algorithm

本日の内容

1. 確率的計算と複雑性クラス
2. **再実行と確率増幅**

確率的複雑性クラス：包含関係 (再掲)

確率的複雑性クラスの間の関係

- $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$ (今から説明)
- $\mathrm{RP} \subseteq \mathrm{BPP}$, $\mathrm{coRP} \subseteq \mathrm{BPP}$ (今から説明)
- $\mathrm{BPP} \subseteq \mathrm{PP}$ (定義から直ちに)

確率的複雑性クラスと多項式階層の間の関係

- $\mathrm{NP} \cup \mathrm{coNP} \subseteq \mathrm{PP} \subseteq \mathrm{PSPACE}$ (今までと同様 (付録))
- $\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$ (Sipser, Lautemann)
- $\mathrm{RP} \subseteq \mathrm{NP}$, $\mathrm{coRP} \subseteq \mathrm{coNP}$ (定義から直ちに)
- $\mathrm{P} \subseteq \mathrm{ZPP}$ (定義から直ちに)

$ZPP = RP \cap coRP$

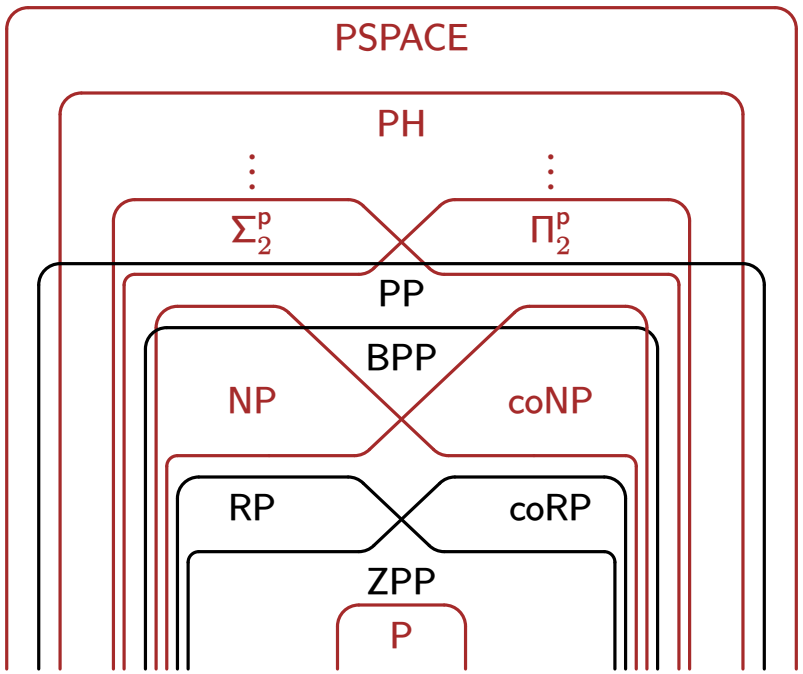
性質 (Gill '77)

$ZPP = RP \cap coRP$

次の 2 つを分けて証明する

1. $ZPP \subseteq RP$, $ZPP \subseteq coRP$
2. $RP \cap coRP \subseteq ZPP$

1 の coRP に対する証明は
1 の RP に対する証明と同様なので,
省略する



ZPP $\subseteq$ RP (1)

証明：$P \in$ ZPP とする

- P に対して，次を満たす確率的アルゴリズム A が存在
  - 期待時間計算量が多項式 ($\leftarrow |I|^k$ とする)
  - 成功確率が 1
- このとき，次のような確率的アルゴリズム B を考える

1. 入力に対して A を走らせる
2. $2|I|^k$ ステップ未満で停止する
   $\Rightarrow$ A の出力を B の出力とする
3. $2|I|^k$ ステップ未満で停止しない
   $\Rightarrow$ No を出力し，全体を停止する

ZPP $\subseteq$ RP (1)

証明：$P \in$ ZPP とする

- P に対して，次を満たす確率的アルゴリズム A が存在
  - 期待時間計算量が多項式 ($\leftarrow |I|^k$ とする)
  - 成功確率が 1
- このとき，次のような確率的アルゴリズム B を考える

1. 入力に対して A を走らせる
2. $2|I|^k$ ステップ未満で停止する
   $\Rightarrow$ A の出力を B の出力とする
3. $2|I|^k$ ステップ未満で停止しない
   $\Rightarrow$ No を出力し，全体を停止する

B の性質 (1)：必ず多項式時間で停止する

ZPP $\subseteq$ RP (1)

証明：$P \in$ ZPP とする

- P に対して，次を満たす確率的アルゴリズム A が存在
  - 期待時間計算量が多項式 ($\leftarrow |I|^k$ とする)
  - 成功確率が 1
- このとき，次のような確率的アルゴリズム B を考える

1. 入力に対して A を走らせる
2. $2|I|^k$ ステップ未満で停止する
   $\Rightarrow$ A の出力を B の出力とする
3. $2|I|^k$ ステップ未満で停止しない
   $\Rightarrow$ No を出力し，全体を停止する

B の性質 (3)：I が No インスタンス $\Rightarrow$ 必ず No を出力

ZPP $\subseteq$ RP (2)

B の性質 (2)：I が Yes インスタンス $\Rightarrow \Pr(\text{Yes を出力}) \geq 1/2$

- $\Pr(A$ が $2|I|^k$ ステップ以内に停止しない$)$

$$= \Pr(A \text{ の時間計算量} \geq 2|I|^k) \leq \frac{\mathrm{E}[A \text{ の時間計算量}]}{2|I|^k} = \frac{1}{2}$$

Markov の不等式

- 確率的アルゴリズム B （A の期待時間計算量 $= |I|^k$）

1. 入力に対して A を走らせる
2. $2|I|^k$ ステップ未満で停止する
   $\Rightarrow$ A の出力を B の出力とする
3. $2|I|^k$ ステップ未満で停止しない
   $\Rightarrow$ No を出力し，全体を停止する

ZPP $\subseteq$ RP (2)

B の性質 (2)：I が Yes インスタンス $\Rightarrow \Pr(\text{Yes を出力}) \geq 1/2$

- $\Pr(A$ が $2|I|^k$ ステップ以内に停止しない$)$
  $= \Pr(A$ の時間計算量 $\geq 2|I|^k) \leq \dfrac{\mathrm{E}[A \text{ の時間計算量}]}{2|I|^k} = \dfrac{1}{2}$
- $\therefore \Pr(\text{Yesを出力}) = \Pr(2|I|^k$ ステップ未満で停止$) \geq \dfrac{1}{2}$

$\therefore P \in$ RP

- 確率的アルゴリズム B （A の期待時間計算量 $= |I|^k$）

1. 入力に対して A を走らせる
2. $2|I|^k$ ステップ未満で停止する
   $\Rightarrow A$ の出力を B の出力とする
3. $2|I|^k$ ステップ未満で停止しない
   $\Rightarrow$ No を出力し，全体を停止する

[復習] Markov の不等式

性質：Markov の不等式

期待値を持つ非負確率変数 X と正実数 t に対して，

$$\Pr(X \geq t) \leq \frac{\mathrm{E}[X]}{t}$$

前のページの証明では，次のようにして利用

$$X = (A \text{ の時間計算量})$$
$$t = 2|I|^k$$

$$\Pr(A \text{ の時間計算量} \geq 2|I|^k) \leq \frac{\mathrm{E}[A \text{ の時間計算量}]}{2|I|^k} = \frac{1}{2}$$

[復習] Markov の不等式

性質：Markov の不等式

期待値を持つ非負確率変数 X と正実数 t に対して，

$$\Pr(X \geq t) \leq \frac{\mathrm{E}[X]}{t}$$

証明：X が離散確率変数のときのみ証明 (連続も同様)

$$\begin{aligned}
\mathrm{E}[X] &= \sum_{i \geq 0} i \cdot \Pr(X = i) \\
&= \sum_{0 \leq i < t} i \cdot \Pr(X = i) + \sum_{i \geq t} i \cdot \Pr(X = i) \\
&\geq \sum_{i \geq t} t \cdot \Pr(X = i) = t \Pr(X \geq t)
\end{aligned}$$

□

RP ∩ coRP ⊆ ZPP (1)

証明：$P \in$ RP ∩ coRP とする

- $P \in$ RP なので，
  P に対して，次を満たす確率的アルゴリズム B_1 が存在
  - 時間計算量が多項式
  - 入力が Yes インスタンスのとき，成功確率 $\geq 1/2$
  - 入力が No インスタンスのとき，成功確率 $= 1$
  - 注：出力が Yes のとき，その出力は必ず正しい
- $P \in$ coRP なので，
  P に対して，次を満たす確率的アルゴリズム B_2 も存在
  - 時間計算量が多項式
  - 入力が Yes インスタンスのとき，成功確率 $= 1$
  - 入力が No インスタンスのとき，成功確率 $\geq 1/2$
  - 注：出力が No のとき，その出力は必ず正しい

RP ∩ coRP ⊆ ZPP (2)

- このとき，次のような確率的アルゴリズム A を考える

1. 入力に対して B_1, B_2 を独立に走らせる
2. B_1 の出力が Yes ⇒ Yes を出力して，停止
3. B_2 の出力が No ⇒ No を出力して，停止
4. B_1 の出力が No，かつ，B_2 の出力が Yes ⇒
   ステップ 1 に戻って，再実行 (restart)

RP ∩ coRP ⊆ ZPP (2)

- このとき，次のような確率的アルゴリズム A を考える

1. 入力に対して B_1, B_2 を独立に走らせる
2. B_1 の出力が Yes ⇒ Yes を出力して，停止
3. B_2 の出力が No ⇒ No を出力して，停止
4. B_1 の出力が No，かつ，B_2 の出力が Yes ⇒ ステップ 1 に戻って，再実行 (restart)

A の性質 (2)：入力が Yes インスタンスのとき，成功確率 $= 1$

$\because$ B_1 の出力が Yes のとき，必ず正しい
B_2 は Yes インスタンスに対して，必ず Yes を出力

A の性質 (3)：入力が No インスタンスのとき，成功確率 $= 1$

$\because$ B_2 の出力が No のとき，必ず正しい
B_1 は No インスタンスに対して，必ず No を出力

RP ∩ coRP ⊆ ZPP (2)

- このとき，次のような確率的アルゴリズム A を考える

1. 入力に対して B_1, B_2 を独立に走らせる
2. B_1 の出力が Yes ⇒ Yes を出力して，停止
3. B_2 の出力が No ⇒ No を出力して，停止
4. B_1 の出力が No，かつ，B_2 の出力が Yes ⇒ ステップ 1 に戻って，再実行 (restart)

A の性質 (1)：期待計算量が多項式 (?)

次を示せば十分：再実行の回数の期待値 ≤ 多項式

RP ∩ coRP ⊆ ZPP (3)

入力が Yes インスタンスであるとき

- $\Pr(B_1$ の出力が No$) \leq \frac{1}{2}$
- $\Pr(B_2$ の出力が Yes$) = 1$
- したがって,

  $\Pr(B_1$ の出力が No，かつ，B_2 の出力が Yes$) \leq \frac{1}{2} \cdot 1 = \frac{1}{2}$

- 確率的アルゴリズム A

1. 入力に対して B_1, B_2 を独立に走らせる
2. B_1 の出力が Yes $\Rightarrow$ Yes を出力して，停止
3. B_2 の出力が No $\Rightarrow$ No を出力して，停止
4. B_1 の出力が No，かつ，B_2 の出力が Yes $\Rightarrow$
   ステップ 1 に戻って，再実行 (restart)

RP ∩ coRP ⊆ ZPP (3)

入力が No インスタンスであるとき

- $\Pr(B_1$ の出力が No$) = 1$
- $\Pr(B_2$ の出力が Yes$) \leq \frac{1}{2}$
- したがって，

  $\Pr(B_1$ の出力が No，かつ，B_2 の出力が Yes$) \leq 1 \cdot \frac{1}{2} = \frac{1}{2}$

- 確率的アルゴリズム A

1. 入力に対して B_1, B_2 を独立に走らせる
2. B_1 の出力が Yes $\Rightarrow$ Yes を出力して，停止
3. B_2 の出力が No $\Rightarrow$ No を出力して，停止
4. B_1 の出力が No，かつ，B_2 の出力が Yes $\Rightarrow$ ステップ 1 に戻って，再実行 (restart)

RP ∩ coRP ⊆ ZPP (3)

- つまり，入力が Yes/No インスタンスのどちらであっても，再実行を行う確率 $\leq \frac{1}{2}$
- $\therefore$ 再実行回数の期待値 ≤ 2 □

(注：ベルヌーイ試行)

- 確率的アルゴリズム A

1. 入力に対して B_1, B_2 を独立に走らせる
2. B_1 の出力が Yes ⇒ Yes を出力して，停止
3. B_2 の出力が No ⇒ No を出力して，停止
4. B_1 の出力が No，かつ，B_2 の出力が Yes ⇒ ステップ 1 に戻って，再実行 (restart)

RP $\subseteq$ BPP，coRP $\subseteq$ BPP

性質 (Gill '77)

RP $\subseteq$ BPP，coRP $\subseteq$ BPP

以下，RP $\subseteq$ BPP のみを証明する (coRP も同様)

定義の復習

	RP	BPP
Yes インスタンス	成功確率 $\geq \frac{1}{2}$	成功確率 $\geq \frac{2}{3}$
No インスタンス	成功確率 $= 1$	成功確率 $\geq \frac{2}{3}$

RP $\subseteq$ BPP (1)

証明：$P \in$ RP とする

- P に対して，次を満たす確率的アルゴリズム B が存在
  - 多項式時間で停止
  - 入力が Yes インスタンスのとき，成功確率 $\geq \frac{1}{2}$
  - 入力が No インスタンスのとき，成功確率 $= 1$
  - 注：出力が Yes のとき，その出力は正しい

RP $\subseteq$ BPP (1)

証明：$P \in$ RP とする

- P に対して，次を満たす確率的アルゴリズム B が存在
  - 多項式時間で停止
  - 入力が Yes インスタンスのとき，成功確率 $\geq \frac{1}{2}$
  - 入力が No インスタンスのとき，成功確率 $= 1$
  - 注：出力が Yes のとき，その出力は正しい

- P に対して，次の確率的アルゴリズム A を考える

1. B を 2 回独立に実行
2. B の出力が Yes・Yes のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が Yes・No のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が No・Yes のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が No・No のとき $\Rightarrow$ No を出力して，停止

RP $\subseteq$ BPP (2)

A の性質 (1)：多項式時間で停止する

$\because$ B は多項式時間で停止する

A の性質 (3)：No インスタンスに対して，成功確率 $= 1$

$\because$ No インスタンスに対して，B の成功確率 $= 1$

$\therefore$ A で「No・No」に必ずなり，正しく No を出力する

- 確率的アルゴリズム A

1. B を 2 回独立に実行
2. B の出力が Yes・Yes のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が Yes・No のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が No・Yes のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が No・No のとき $\Rightarrow$ No を出力して，停止

RP $\subseteq$ BPP (3)

A の性質 (2)：Yes インスタンスに対して，成功確率 $\geq \frac{3}{4}$

$\because \Pr(B$ が Yes を出力$) \geq \frac{1}{2}$

$\therefore \Pr(B$ が 2 回中 1 回は Yes を出力$) \geq 1 - \left(\frac{1}{2}\right)^2 = \frac{3}{4}$

したがって，$P \in$ BPP

- 確率的アルゴリズム A

1. B を 2 回独立に実行
2. B の出力が Yes・Yes のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が Yes・No のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が No・Yes のとき $\Rightarrow$ Yes を出力して，停止
   B の出力が No・No のとき $\Rightarrow$ No を出力して，停止

確率増幅 (RP の場合)

Yes インスタンスに対して,

B を 1 回実行 $\Rightarrow$ 成功確率 $\geq \frac{1}{2} = 1 - \frac{1}{2}$

B を 2 回実行 $\Rightarrow$ 成功確率 $\geq \frac{3}{4} = 1 - \frac{1}{2^2}$

確率増幅 (RP の場合)

Yes インスタンスに対して,

B を 1 回実行 $\Rightarrow$ 成功確率 $\geq \frac{1}{2} = 1 - \frac{1}{2}$

B を 2 回実行 $\Rightarrow$ 成功確率 $\geq \frac{3}{4} = 1 - \frac{1}{2^2}$

B を 3 回実行 $\Rightarrow$ 成功確率 $\geq \frac{7}{8} = 1 - \frac{1}{2^3}$

B を k 回実行 $\Rightarrow$ 成功確率 $\geq 1 - \frac{1}{2^k}$

確率増幅

(probability amplification)

確率増幅から得られる性質 (RP の場合)

性質：RP と確率増幅

$P \in \mathrm{RP} \Rightarrow$ 任意の多項式 p に対して，
次を満たす確率的アルゴリズム A が存在

- P の任意の入力 I に対して，
  - 必ず多項式時間で停止する
  - I が Yes インスタンス $\Rightarrow$

$$\Pr_r(A(I) = \mathrm{Yes}) \geq 1 - \frac{1}{2^{p(|I|)}}$$

  - I が No インスタンス $\Rightarrow \Pr_r(A(I) = \mathrm{No}) = 1$

$p(|I|)$ が独立実行の回数に対応する

意味：成功確率は任意に 1 へ近づけられる

確率増幅 (BPP の場合)

成功確率 $= \frac{2}{3}$ のアルゴリズム A に対して，次を考える

1. A を独立に 3 回実行する
2. A の出力が Yes 3 回，No 0 回 のとき，Yes を出力して停止
   A の出力が Yes 2 回，No 1 回 のとき，Yes を出力して停止
   A の出力が Yes 1 回，No 2 回 のとき，No を出力して停止
   A の出力が Yes 0 回，No 3 回 のとき，No を出力して停止

つまり，多数決 (majority vote)

確率増幅 (BPP の場合)

成功確率 $= \frac{2}{3}$ のアルゴリズム A に対して，次を考える

1. A を独立に 3 回実行する
2. A の出力が Yes 3 回，No 0 回 のとき，Yes を出力して停止
   A の出力が Yes 2 回，No 1 回 のとき，Yes を出力して停止
   A の出力が Yes 1 回，No 2 回 のとき，No を出力して停止
   A の出力が Yes 0 回，No 3 回 のとき，No を出力して停止

つまり，多数決 (majority vote)

Yes インスタンスに対して，

$$\text{成功確率} = \left(\frac{2}{3}\right)^3 + 3\left(\frac{2}{3}\right)^2 \frac{1}{3} = \frac{20}{27} \quad (\text{注} : \frac{2}{3} = \frac{18}{27})$$

No インスタンスも同じ

確率増幅 (BPP の場合) 続

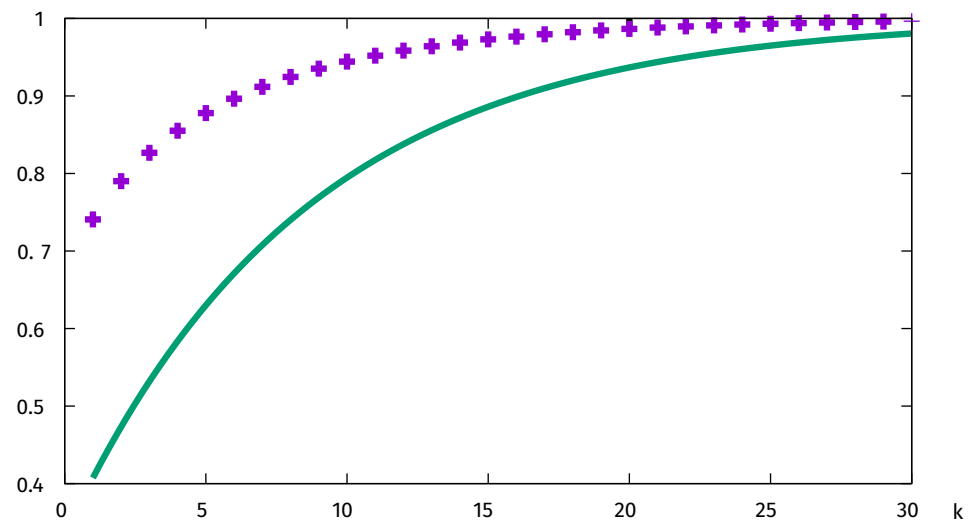
成功確率 $= \frac{2}{3}$ のアルゴリズム A に対して，次を考える

1. A を独立に $2k+1$ 回実行する (k は定数)
2. A の出力の過半数が Yes のとき，Yes を出力して停止
   A の出力の過半数が No のとき，No を出力して停止

Yes インスタンスに対して，

$$\text{成功確率} = \sum_{i=0}^{k} \binom{2k+1}{i} \left(\frac{2}{3}\right)^{2k+1-i} \left(\frac{1}{3}\right)^{i}$$

$$\geq 1 - \frac{2}{3}\left(\frac{8}{9}\right)^{k}$$



No インスタンスも同じ

確率増幅 (BPP の場合) 続

成功確率 $= \frac{2}{3}$ のアルゴリズム A に対して，次を考える

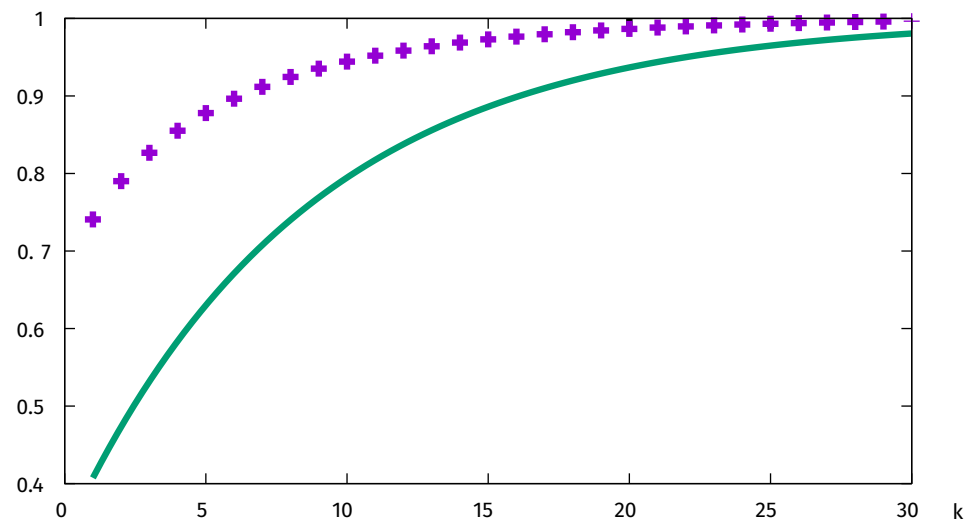
1. A を独立に $2k+1$ 回実行する (k は定数)
2. A の出力の過半数が Yes のとき，Yes を出力して停止
   A の出力の過半数が No のとき，No を出力して停止

Yes インスタンスに対して，

$$\text{成功確率} = \sum_{i=0}^{k} \binom{2k+1}{i} \left(\frac{2}{3}\right)^{2k+1-i} \left(\frac{1}{3}\right)^{i}$$

$$\geq 1 - \frac{2}{3}\left(\frac{8}{9}\right)^{k}$$

付録



No インスタンスも同じ

確率増幅から得られる性質 (BPP の場合)

性質：BPP と確率増幅

$P \in \mathrm{BPP} \Rightarrow$ 任意の多項式 p に対して，
次を満たす確率的アルゴリズム A が存在

- P の任意の入力 I に対して，
  - 必ず多項式時間で停止する
  - $\Pr_r(A\text{の出力が正しい}) \geq 1 - \frac{2}{3}\left(\frac{8}{9}\right)^{p(|I|)}$

$p(|I|)$ が独立実行の回数に対応する

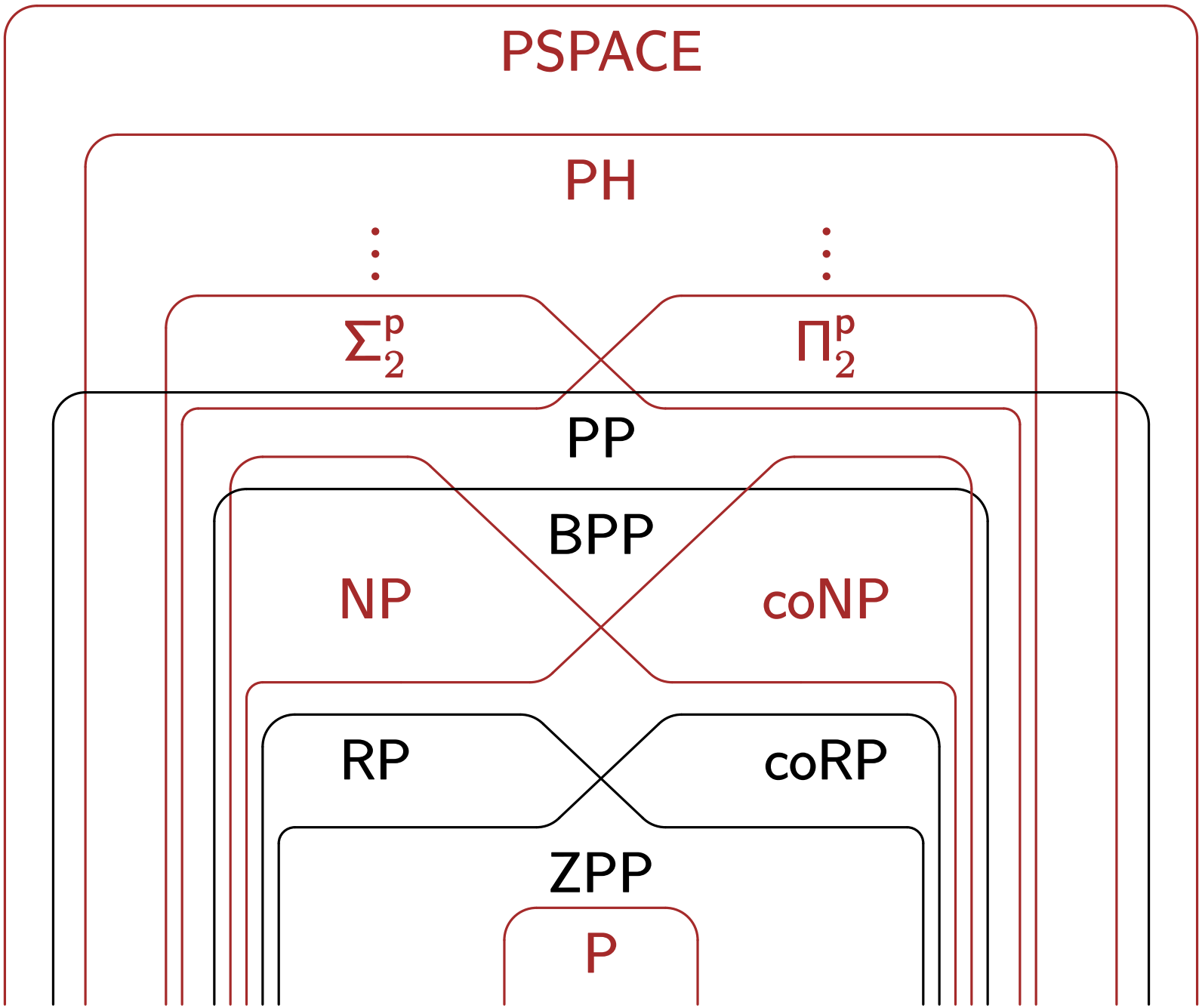
意味：成功確率は任意に 1 へ近づけられる

本日のまとめ

内容

- **確率的** な動作を行う計算モデルを導入する
- 複雑性クラス PP，RP，coRP，BPP，ZPP を導入する
- **再実行** と **確率増幅** という重要な技法を紹介する
- (BPP $\subseteq \Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$ を証明する)

[再掲] 確率的複雑性クラス



戸田の定理

次の定理は，PP と PH の関係を表す重要な事実

事実：戸田の定理 (Toda '91)

PH に属する任意の問題は
PP のある問題を 1 回解ければ，多項式時間で解ける

戸田の定理は よく $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ と書かれる

戸田の定理

次の定理は，PP と PH の関係を表す重要な事実

事実：戸田の定理 (Toda '91)

PH に属する任意の問題は
PP のある問題を 1 回解ければ，多項式時間で解ける

戸田の定理は よく $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ と書かれる

戸田　誠之助（とだ・せいのすけ）

- 「戸田の定理」でゲーデル賞受賞 ('98)
- 電通大 学士 ('82)，修士 ('84)
- 国文研 助手 → 電通大 助手
- 東工大 博士 ('91)
- → 電通大 助教授 → 日大 助教授
  → 日大 教授 → 日大 名誉教授

doi:10.1093/ietisy/e89-d.8.2388

次回の予告

内容

- **インタラクション** を伴う計算モデルを導入して計算資源として **ラウンド数** を考える
- 複雑性クラス AM，MA，IP を導入する
- これらの関係といままでの複雑性クラスの関係を考察する

クイズ

Q

1.

2.

3.

4.

1. **確率増幅のための計算**
2. $\mathsf{NP} \cup \mathsf{coNP} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE}$
3. $\mathsf{BPP} \subseteq \Sigma_2^{\mathsf{p}} \cap \Pi_2^{\mathsf{p}}$

確率増幅のための計算 (1)

目標：次の不等式を導出する

任意の整数 $k \geq 1$ に対して

$$\sum_{i=0}^{k} \binom{2k+1}{i} \left(\frac{2}{3}\right)^{2k+1-i} \left(\frac{1}{3}\right)^{i} \geq 1 - \frac{2}{3}\left(\frac{8}{9}\right)^{k}$$

確率増幅のための計算 (1)

目標：次の不等式を導出する

任意の整数 $k \geq 1$ に対して

$$\sum_{i=0}^{k} \binom{2k+1}{i} \left(\frac{2}{3}\right)^{2k+1-i} \left(\frac{1}{3}\right)^{i} \geq 1 - \frac{2}{3}\left(\frac{8}{9}\right)^{k}$$

次の不等式を証明すれば十分

任意の整数 $k \geq 1$ に対して

$$\sum_{i=k+1}^{2k+1} \binom{2k+1}{i} \left(\frac{2}{3}\right)^{2k+1-i} \left(\frac{1}{3}\right)^{i} \leq \frac{2}{3}\left(\frac{8}{9}\right)^{k}$$

$\because$ $\displaystyle\sum_{i=0}^{2k+1} \binom{2k+1}{i} \left(\frac{2}{3}\right)^{2k+1-i} \left(\frac{1}{3}\right)^{i} = 1$ (二項定理)

確率増幅のための計算 (2)

補題 1

整数 k, i に対して，$2 \leq k+1 \leq i \leq 2k$ ならば

$$\frac{\binom{2k+1}{i+1}\left(\frac{2}{3}\right)^{2k+1-(i+1)}\left(\frac{1}{3}\right)^{i+1}}{\binom{2k+1}{i}\left(\frac{2}{3}\right)^{2k+1-i}\left(\frac{1}{3}\right)^{i}} \leq \frac{1}{2}$$

次の不等式を証明すれば十分

任意の整数 $k > 1$ に対して

$$\sum_{i=k+1}^{2k+1} \binom{2k+1}{i}\left(\frac{2}{3}\right)^{2k+1-i}\left(\frac{1}{3}\right)^{i} \leq \frac{2}{3}\left(\frac{8}{9}\right)^{k}$$

確率増幅のための計算 (2)

補題 1

整数 k, i に対して，$2 \leq k+1 \leq i \leq 2k$ ならば

$$\frac{\binom{2k+1}{i+1}\left(\frac{2}{3}\right)^{2k+1-(i+1)}\left(\frac{1}{3}\right)^{i+1}}{\binom{2k+1}{i}\left(\frac{2}{3}\right)^{2k+1-i}\left(\frac{1}{3}\right)^{i}} \leq \frac{1}{2}$$

証明：

$$\text{左辺} = \frac{\frac{(2k+1)!}{(2k+1-(i+1))!(i+1)!}}{\frac{(2k+1)!}{(2k+1-i)!i!}}\frac{\frac{1}{3}}{\frac{2}{3}} = \underline{\frac{1}{2}\cdot\frac{2k+1-i}{i+1}}$$

$i = k+1$ のとき最大

$$\leq \frac{k}{2k+4} \leq \frac{1}{2}$$

□

確率増幅のための計算 (3)

補題 2

任意の整数 $k \geq 1$ に対して

$$\binom{2k+1}{k+1} \leq 4^k$$

証明：二項定理より

$$\binom{2k+1}{0} + \cdots + \binom{2k+1}{k} + \binom{2k+1}{k+1} + \cdots + \binom{2k+1}{2k+1} = 2^{2k+1}$$

確率増幅のための計算 (3)

補題 2

任意の整数 $k \geq 1$ に対して

$$\binom{2k+1}{k+1} \leq 4^k$$

証明：二項定理より

$$\underbrace{\binom{2k+1}{0} + \cdots + \binom{2k+1}{k}}_{= 2^{2k} = 4^k} + \underbrace{\binom{2k+1}{k+1} + \cdots + \binom{2k+1}{2k+1}}_{= 2^{2k} = 4^k} = 2^{2k+1}$$

$$\therefore \quad \binom{2k+1}{k+1} \leq 4^k \qquad \square$$

確率増幅のための計算 (4)

$$\sum_{i=k+1}^{2k+1} \binom{2k+1}{i} \left(\frac{2}{3}\right)^{2k+1-i} \left(\frac{1}{3}\right)^{i}$$

$$\leq \sum_{i=k+1}^{2k+1} 4^k \left(\frac{2}{3}\right)^{k} \left(\frac{1}{3}\right)^{k+1} \cdot \left(\frac{1}{2}\right)^{i-(k+1)}$$

$$= \frac{1}{3}\left(\frac{8}{9}\right)^{k} \sum_{j=0}^{k} \left(\frac{1}{2}\right)^{j}$$

$$\leq \frac{1}{3}\left(\frac{8}{9}\right)^{k} \sum_{j=0}^{\infty} \left(\frac{1}{2}\right)^{j} = \frac{1}{3}\left(\frac{8}{9}\right)^{k} \cdot \frac{1}{1-\frac{1}{2}} = \frac{2}{3}\left(\frac{8}{9}\right)^{k} \qquad \square$$

付録

1. 確率増幅のための計算
2. $\mathsf{NP} \cup \mathsf{coNP} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE}$
3. $\mathsf{BPP} \subseteq \Sigma_2^{\mathsf{p}} \cap \Pi_2^{\mathsf{p}}$

PP $\subseteq$ PSPACE

性質 (Gill '77)

PP $\subseteq$ PSPACE

証明の方針：

$P \in$ PP

$\exists$ アルゴリズム A:

- 多項式時間

- Yes インスタンス $\Rightarrow$ 成功確率 $> 1/2$
- No インスタンス $\Rightarrow$ 成功確率 $> 1/2$

PP $\subseteq$ PSPACE

性質 (Gill '77)

PP $\subseteq$ PSPACE

証明の方針：

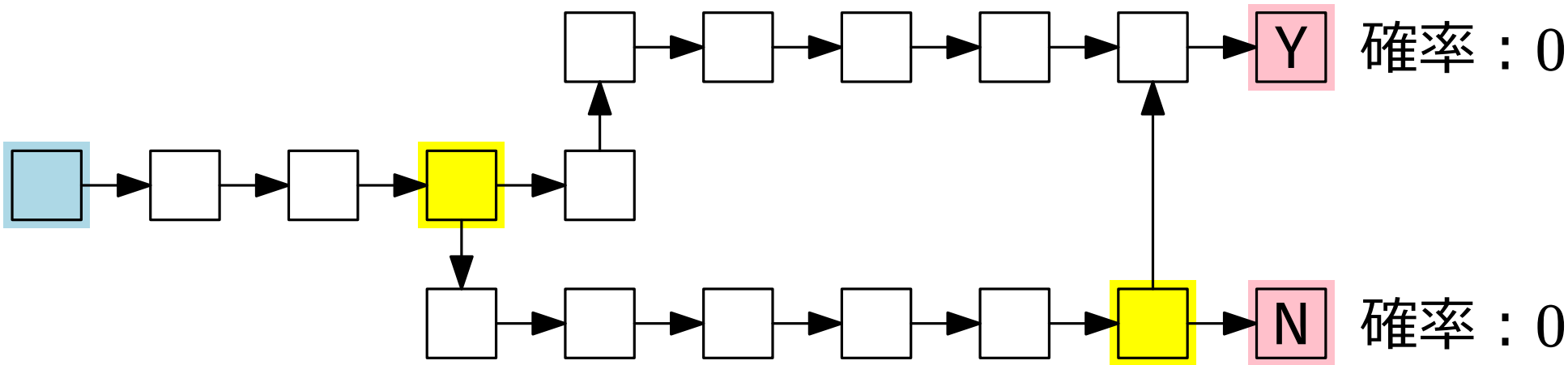
$P \in$ PP

$\exists$ アルゴリズム A: ⟶ 次のアルゴリズム B を構成

- 多項式時間
- Yes インスタンス $\Rightarrow$ 成功確率 $> 1/2$
- No インスタンス $\Rightarrow$ 成功確率 $> 1/2$

- 多項式領域で，A が Yes を出力する確率を計算
- 計算した確率 $> 1/2 \Rightarrow$ Yes を出力
- 計算した確率 $\leq 1/2 \Rightarrow$ No を出力

PP $\subseteq$ PSPACE：証明

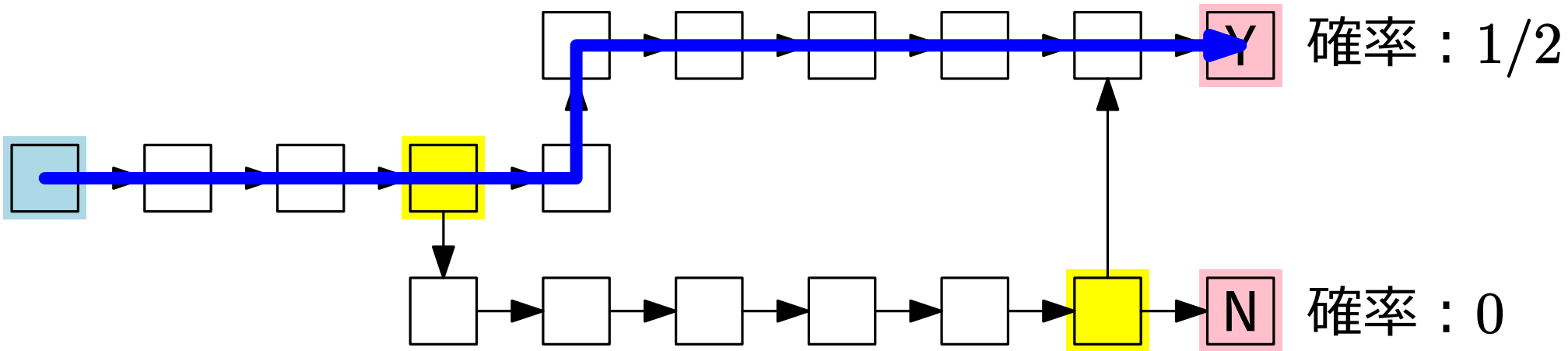


アルゴリズム B の構成

- $A(I)$ の時点状況が作るグラフで深さ優先探索を行う
- 作業領域で覚えること：現在の経路，分岐における選択
  ($\because$ 領域計算量 $= O($多項式$(|I|))$
- Yes に到達する確率 $> 1/2 \Rightarrow$ Yes を出力
  Yes に到達する確率 $\leq 1/2 \Rightarrow$ No を出力
  ($\because$ 出力は正しい)

□

PP $\subseteq$ PSPACE：証明

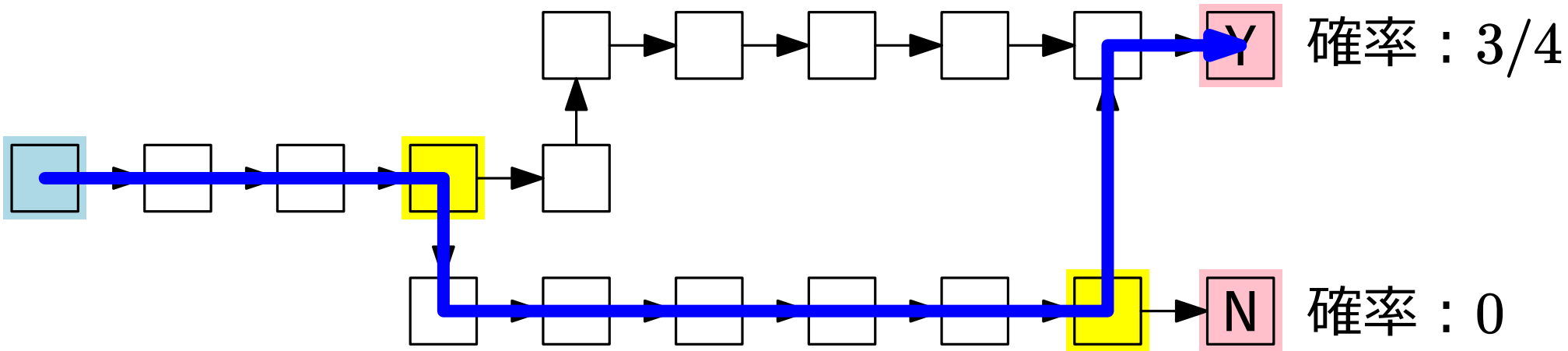


アルゴリズム B の構成

- $A(I)$ の時点状況が作るグラフで深さ優先探索を行う
- 作業領域で覚えること：現在の経路，分岐における選択
  ($\because$ 領域計算量 $= O($多項式$(|I|))$
- Yes に到達する確率 $> 1/2 \Rightarrow$ Yes を出力
  Yes に到達する確率 $\leq 1/2 \Rightarrow$ No を出力
  ($\because$ 出力は正しい)

□

PP $\subseteq$ PSPACE：証明

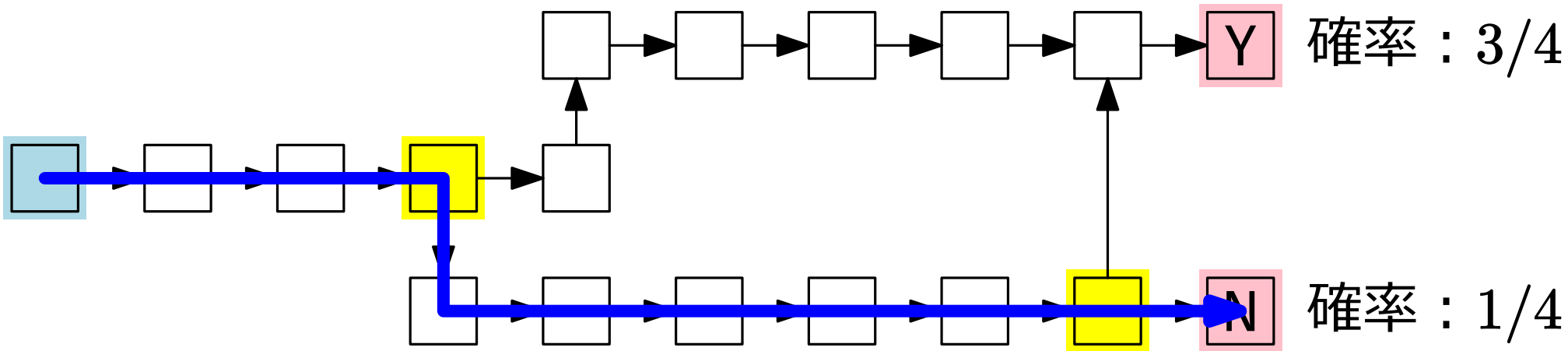


アルゴリズム B の構成

- $A(I)$ の時点状況が作るグラフで深さ優先探索を行う
- 作業領域で覚えること：現在の経路，分岐における選択
  ($\because$ 領域計算量 $= O($多項式$(|I|))$
- Yes に到達する確率 $> 1/2 \Rightarrow$ Yes を出力
  Yes に到達する確率 $\leq 1/2 \Rightarrow$ No を出力
  ($\because$ 出力は正しい)

□

PP $\subseteq$ PSPACE：証明



アルゴリズム B の構成

- $A(I)$ の時点状況が作るグラフで深さ優先探索を行う
- 作業領域で覚えること：現在の経路，分岐における選択
  ($\because$ 領域計算量 $= O($多項式$(|I|))$
- Yes に到達する確率 $> 1/2 \Rightarrow$ Yes を出力
  Yes に到達する確率 $\leq 1/2 \Rightarrow$ No を出力
  ($\because$ 出力は正しい)

□

NP ⊆ PP

性質 (Gill '77)

NP ⊆ PP

証明の方針：CNF-SAT (NP 完全) に対して
次を満たす確率的アルゴリズム A を作る

連言標準形論理式の充足可能性問題 (CNF-SAT)

入力： 連言標準形の論理式 φ
出力： φ が充足割当を持つ ⇒ Yes
φ が充足割当を持たない ⇒ No

- 時間計算量が多項式
- φ が充足割当を持つ $\Rightarrow \Pr(\text{Yes を出力}) > \frac{1}{2}$
- φ が充足割当を持たない $\Rightarrow \Pr(\text{No を出力}) > \frac{1}{2}$

NP $\subseteq$ PP：証明 (1)

アルゴリズム A：入力は論理式 φ ($n =$ 変数の数)

1. $\alpha :=$ 一様ランダムな真理値割当 $\in \{0,1\}^n$
2. $\varphi(\alpha) = 1 \Rightarrow$ Yes を出力
3. $\varphi(\alpha) = 0 \Rightarrow$
   - 確率 $\frac{1}{2} - \frac{1}{2^{n+1}}$ で Yes を出力

     確率 $\frac{1}{2} + \frac{1}{2^{n+1}}$ で No を出力

性質 1：時間計算量が多項式

- 注：使う乱数の数 $= 2n + 1$ ビット

NP $\subseteq$ PP：証明 (2)

アルゴリズム A：入力は論理式 φ ($n =$ 変数の数)

1. $\alpha :=$ 一様ランダムな真理値割当 $\in \{0,1\}^n$
2. $\varphi(\alpha) = 1 \Rightarrow$ Yes を出力
3. $\varphi(\alpha) = 0 \Rightarrow$
   - 確率 $\frac{1}{2} - \frac{1}{2^{n+1}}$ で Yes を出力，$\frac{1}{2} + \frac{1}{2^{n+1}}$ で No を出力

性質 2：φ が充足割当を持つ $\Rightarrow \Pr(\text{Yes を出力}) > \frac{1}{2}$

- $p := \Pr(\alpha \text{ が充足割当}) \geq 1/2^n$
- $\Pr(\text{Yes を出力}) = \Pr(\alpha \text{ が充足割当である}) +$
  $\Pr(\alpha \text{ が充足割当でない}) \cdot (\frac{1}{2} - \frac{1}{2^{n+1}})$
  $= p + (1-p)(\frac{1}{2} - \frac{1}{2^{n+1}})$
  $= (\frac{1}{2} + \frac{1}{2^{n+1}})p + (\frac{1}{2} - \frac{1}{2^{n+1}})$
  $\geq (\frac{1}{2} + \frac{1}{2^{n+1}})\frac{1}{2^n} + (\frac{1}{2} - \frac{1}{2^{n+1}})$
  $= \frac{1}{2} + \frac{1}{2^{2n+1}} > \frac{1}{2}$

NP $\subseteq$ PP：証明 (3)

アルゴリズム A：入力は論理式 φ ($n =$ 変数の数)

1. $\alpha :=$ 一様ランダムな真理値割当 $\in \{0,1\}^n$
2. $\varphi(\alpha) = 1 \Rightarrow$ Yes を出力
3. $\varphi(\alpha) = 0 \Rightarrow$
   - 確率 $\frac{1}{2} - \frac{1}{2^{n+1}}$ で Yes を出力，$\frac{1}{2} + \frac{1}{2^{n+1}}$ で No を出力

性質 3：φ が充足割当を持たない $\Rightarrow \Pr(\text{No を出力}) > \frac{1}{2}$

- $\Pr(\alpha \text{ が充足割当}) = 0$
- $\Pr(\text{No を出力}) = \frac{1}{2} + \frac{1}{2^{n+1}} > \frac{1}{2}$

$\square$

coNP ⊆ PP

性質 (Gill '77)

coNP ⊆ PP

証明の方針：CNF-UNSAT (coNP 完全) に対して
次を満たす確率的アルゴリズム A' を作る

連言標準形論理式の充足不能性問題 (CNF-UNSAT)

入力： 連言標準形の論理式 φ
出力： φ が充足割当を持たない $\Rightarrow$ Yes
φ が充足割当を持つ $\Rightarrow$ No

- 時間計算量が多項式
- φ が充足割当を持つ $\Rightarrow \Pr(\text{Yes を出力}) > \frac{1}{2}$
- φ が充足割当を持たない $\Rightarrow \Pr(\text{No を出力}) > \frac{1}{2}$

coNP $\subseteq$ PP：証明

アルゴリズム A'：入力は論理式 φ ($n =$ 変数の数)

1. $\alpha :=$ 一様ランダムな真理値割当 $\in \{0,1\}^n$
2. $\varphi(\alpha) = 1 \Rightarrow$ No を出力
3. $\varphi(\alpha) = 0 \Rightarrow$
   - 確率 $\frac{1}{2} - \frac{1}{2^{n+1}}$ で No を出力

     確率 $\frac{1}{2} + \frac{1}{2^{n+1}}$ で Yes を出力

これは，アルゴリズム A の出力 Yes/No を反転させたもの

- $\therefore$ 欲しい 3 つの性質は A と同様に成り立つ $\square$

付録

1. 確率増幅のための計算
2. $\mathsf{NP} \cup \mathsf{coNP} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE}$
3. $\mathsf{BPP} \subseteq \Sigma_2^{\mathsf{p}} \cap \Pi_2^{\mathsf{p}}$

$\mathsf{BPP} \subseteq \Sigma_2^{\mathsf{p}}$

性質：Sipser-Lautemann の定理

$\mathsf{BPP} \subseteq \Sigma_2^{\mathsf{p}} \cap \Pi_2^{\mathsf{p}}$

(Sipser '83, Lautemann '83)

$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{p}}$

性質：Sipser-Lautemann の定理

$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$

(Sipser '83, Lautemann '83)

次を証明すれば十分

$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{p}}$

なぜか？

- $\mathrm{BPP} = \mathrm{coBPP}$ (BPP と補問題の定義)
- $\mathrm{co}\Sigma_2^{\mathrm{p}} = \Pi_2^{\mathrm{p}}$ ($\Sigma_2^{\mathrm{p}}, \Pi_2^{\mathrm{p}}$ の性質 (前回))
- したがって，$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{p}}$ ならば
  $\mathrm{BPP} = \mathrm{coBPP} \subseteq \mathrm{co}\Sigma_2^{\mathrm{p}} = \Pi_2^{\mathrm{p}}$

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (1)

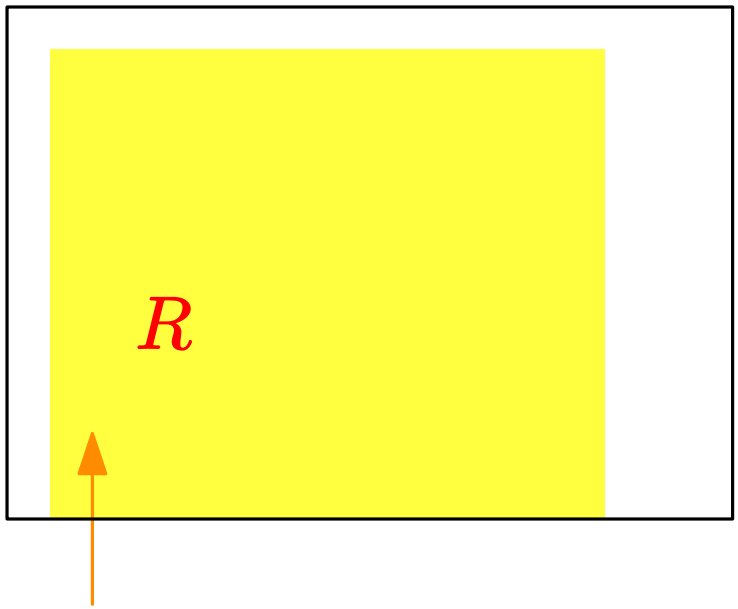
証明：$P \in$ BPP として，入力の符号長を n とする

- P に対して，次を満たす確率的アルゴリズム A が存在
  - 時間計算量が多項式
  - 成功確率 $\geq 2/3$
- 確率増幅により，時間計算量が多項式のままで
  成功確率 $\geq 1 - \dfrac{1}{2^n}$ とできる
- 確率増幅適用後の 時間計算量を n^k として (k は定数)，
  A が使うランダムビット列を $r \in \{0,1\}^{n^k}$ とする
- つまり，
  A を成功に導くランダムビット列の総数 $\geq 2^{n^k}\left(1 - \dfrac{1}{2^n}\right)$

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (2)

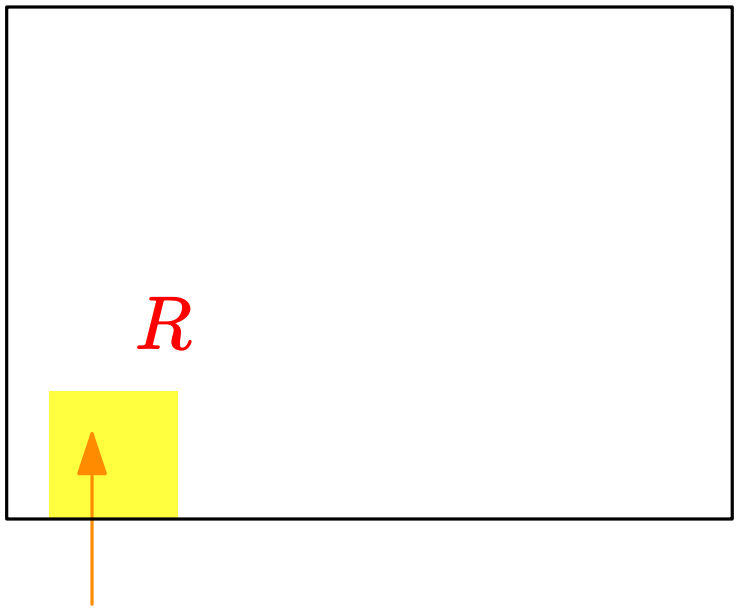
I が Yes インスタンス：

長さ n^k のビット列全体



I が No インスタンス：

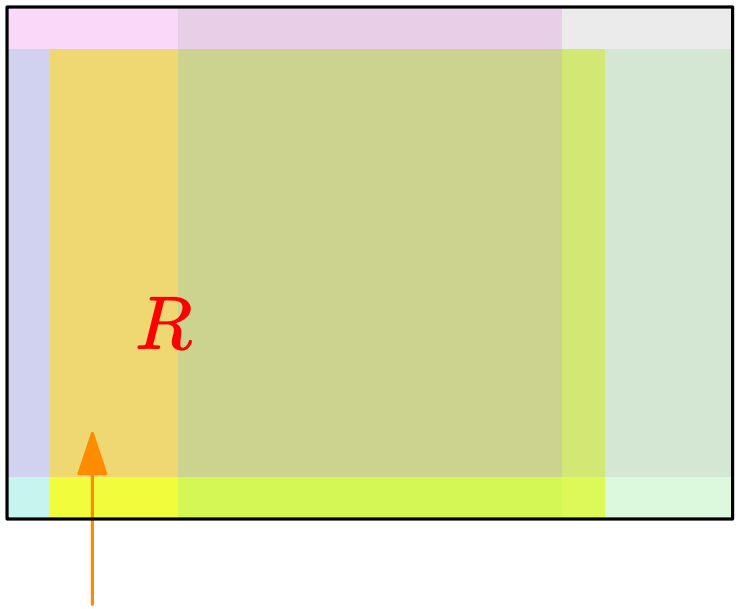
長さ n^k のビット列全体



BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (2)

I が Yes インスタンス：

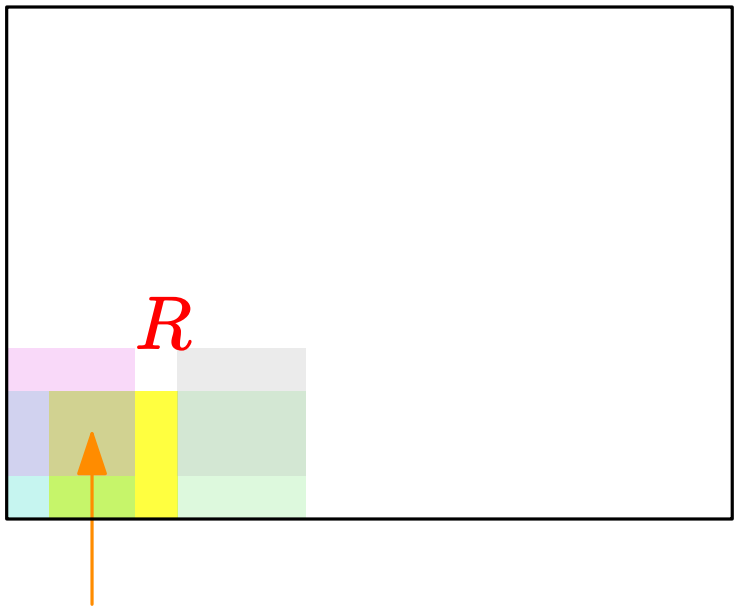
長さ n^k のビット列全体



うまく n^k 回
平行移動させると
全体を覆える

I が No インスタンス：

長さ n^k のビット列全体



どんなふうに n^k 回
平行移動させても
全体を覆えない

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (3)

設定：正整数 $2 \leq \ell < m$，$R \subseteq \{0,1\}^m$

補題 1 (Lautemann '83)

$|R| \leq 2^m/2^\ell \Rightarrow$
任意のビット列 $y_1, \ldots, y_m \in \{0,1\}^m$ に対して
$\{0,1\}^m \neq \{r \oplus y_i \mid r \in R, i \in \{1,\ldots,m\}\}$

ビットごとの XOR (2 を法とする加法)

ここまでの状況に対応させると

- $\ell = n$，$m = n^k$
- R：A に Yes を出力させるランダムビット列全体の集合
- $|R| \leq 2^m/2^\ell$：I が No インスタンスであるとき

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (3)

設定：正整数 $2 \leq \ell < m$，$R \subseteq \{0,1\}^m$

補題 1 (Lautemann '83)

$|R| \leq 2^m/2^\ell \Rightarrow$
任意のビット列 $y_1, \ldots, y_m \in \{0,1\}^m$ に対して
$\{0,1\}^m \neq \{r \oplus y_i \mid r \in R, i \in \{1,\ldots,m\}\}$

証明：$y \in \{0,1\}^m$ に対して，$R \oplus y := \{r \oplus y \mid r \in R\}$ と書く

- $$|\text{右辺}| = \left|\bigcup_{i=1}^{m}(R \oplus y_i)\right| \leq \sum_{i=1}^{m}|R \oplus y_i| = \sum_{i=1}^{m}|R|$$
$$\leq m2^m/2^\ell < 2^m = |\text{左辺}|$$
- $\therefore$ 左辺 $\neq$ 右辺 □

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (4)

設定：正整数 $2 \leq \ell < m$，$R \subseteq \{0,1\}^m$

補題 2 (Lautemann '83)

$|R| \geq 2^m(1 - 1/2^\ell) \Rightarrow$
あるビット列 $y_1, \ldots, y_m \in \{0,1\}^m$ が存在して
$\{0,1\}^m = \{r \oplus y_i \mid r \in R, i \in \{1, \ldots, m\}\}$

$\oplus$：ビットごとの XOR (2 を法とする加法)

ここまでの状況に対応させると

- $\ell = n$，$m = n^k$
- R：A に Yes を出力させるランダムビット列全体の集合
- $|R| \geq 2^m(1 - 1/2^\ell)$：$I$ が Yes インスタンスであるとき

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (4)

設定：正整数 $2 \leq \ell < m$，$R \subseteq \{0,1\}^m$

補題 2 (Lautemann '83)

$|R| \geq 2^m(1 - 1/2^\ell) \Rightarrow$
あるビット列 $y_1, \ldots, y_m \in \{0,1\}^m$ が存在して
$\{0,1\}^m = \{r \oplus y_i \mid r \in R, i \in \{1, \ldots, m\}\}$

証明：$y_1, \ldots, y_m$ の選び方の総数 $= (2^m)^m$ (重複を許す)

- $y_1, \ldots, y_m$ と $x \in \{0,1\}^m$ を選んで 1 つ固定したとき，
  $x \notin$ 右辺 $\Leftrightarrow$ すべての $i = 1, \ldots, m$ に対して，$x \notin R \oplus y_i$
  $\Leftrightarrow$ すべての $i = 1, \ldots, m$ に対して，$x \oplus y_i \notin R$
- 固定した $x \in \{0,1\}^m$ に対して，
  $x \oplus z \notin R$ を満たす $z \in \{0,1\}^m$ の総数 $= 2^m - |R|$
  $\leq 2^m/2^\ell$

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (5)

証明 (続き)：

- $y_1, \ldots, y_m$ の中で次を満たすものの総数を考える
  - $\exists\, x \in \{0,1\}^m, \forall\, i = 1, \ldots, m$: $x \oplus y_i \notin R$

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (5)

証明 (続き)：

- $y_1, \ldots, y_m$ の中で次を満たすものの総数を考える
  - $\exists\, x \in \{0,1\}^m, \forall\, i = 1, \ldots, m\colon x \oplus y_i \notin R$
- そのような $y_1, \ldots, y_m$ の総数 $\leq 2^m \cdot 2^m / 2^\ell = 2^{2m-\ell}$
- 一方，$y_1, \ldots, y_m$ の選び方の総数は 2^{m^2} だったので，ある選び方によって，上の性質は満たされない
- つまり，ある $y_1, \ldots, y_m$ に対して，
  - $\forall\, x \in \{0,1\}^m, \exists\, i = 1, \ldots, m\colon x \oplus y_i \in R$
- $\therefore$ そのような $y_1 \ldots, y_m$ に対して
  $\{0,1\}^m = \{r \oplus y_i \mid r \in R, i \in \{1, \ldots, m\}$ □

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (6)

交代性アルゴリズム B：

1. $i = 1, \ldots, n^k$ に対して
   - $y_i :=$ guess-$\exists(\{0,1\}^{n^k})$
2. $x :=$ guess-$\forall(\{0,1\}^{n^k})$
3. $i = 1, \ldots, n^k$ に対して
   3-1. $r = x \oplus y_i$ をランダムビット列として，$A(I)$ を実行
   3-2. $A(I)$ が Yes を出力 $\Rightarrow$ Yes を出力して停止
4. ここまで来たら，No を出力して停止

- 補題 2 $\Rightarrow$ 3-2 で Yes を出力する y_i が必ず存在
- 補題 1 $\Rightarrow$ 3-2 で Yes を出力することはない

$\therefore$ これは正しいアルゴリズム

BPP $\subseteq \Sigma_2^{\mathrm{p}}$：証明 (6)

交代性アルゴリズム B：

1. $i = 1, \ldots, n^k$ に対して
   - $y_i :=$ guess-$\exists(\{0,1\}^{n^k})$
2. $x :=$ guess-$\forall(\{0,1\}^{n^k})$
3. $i = 1, \ldots, n^k$ に対して
   - 3-1. $r = x \oplus y_i$ をランダムビット列として，$A(I)$ を実行
   - 3-2. $A(I)$ が Yes を出力 $\Rightarrow$ Yes を出力して停止
4. ここまで来たら，No を出力して停止

交代性は「$\exists\forall$」でのみ現れる

$\therefore P \in \Sigma_2^{\mathrm{p}}$

- 補題 2 $\Rightarrow$ 3-2 で Yes を出力する y_i が必ず存在
- 補題 1 $\Rightarrow$ 3-2 で Yes を出力することはない

$\therefore$ これは正しいアルゴリズム