



計算量理論

令和6年10月29日

担当 河村彰星 (京大)

- 多項式時間階層
- 多項式空間



P の定義 (復習)

多項式 $p: \mathbf{N} \rightarrow \mathbf{N}$ が存在し
どの入力 $x \in \{0, 1\}^*$ に対しても
時間 $\leq p(|x|)$ で停止

定義

言語 (language) $A \subseteq \{0, 1\}^*$ が **P** に属するとは
多項式時間限定な機械 M が存在し

任意の入力 $x \in \{0, 1\}^*$ に対し

$$x \in A \iff M \text{ は } x \text{ を受理}$$

が成立つことをいう

これを「 M が A を
認識する」という

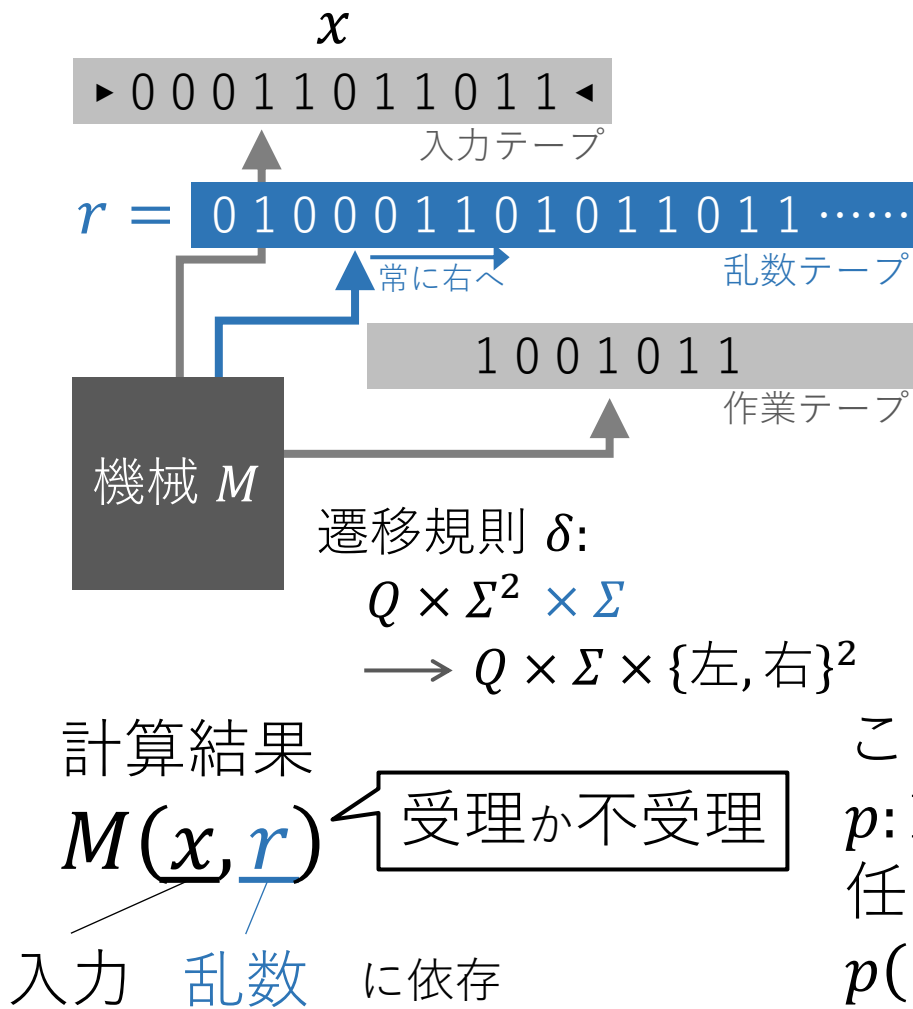


※ 今日は **P** などは言語 (判定問題) の集合とする

NP の定義はどこが変わる？ → 次頁～



非決定性機械



次の遷移が二つの分岐から
非決定的に選ばれる

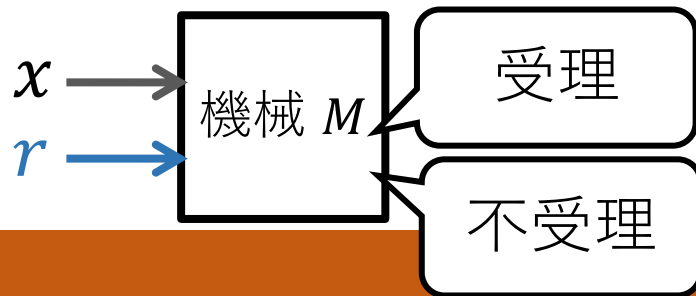


初めに「乱数テープ」上に
乱数列が無限に供給される
 $p(|x|)$ ビットで十分



この機械が
 $p: \mathbf{N} \rightarrow \mathbf{N}$ 時間限定であるとは
任意の x と任意の r について
 $p(|x|)$ 時間以内で停止すること

NP の定義 (復習)



片側誤り
誤受理なし



↑ スライドを置いてあります

定義

言語 $A \subseteq \{0, 1\}^*$ が **NP** に属するとは
多項式 $p: \mathbf{N} \rightarrow \mathbf{N}$ と 多項式時間限定の機械 M とが存在し
任意の入力 x に対し

言語 $B \in \mathbf{P}$

$x \in A \iff$ 或る $r \in \{0, 1\}^{p(|x|)}$ が存在して

M は (x, r) を受理

$(x, r) \in B$

と言っても同じ

r は $x \in A$ であることの「証拠」

P と違って 非対称な定義であることに注意

($A \in \mathbf{NP}$ だからといって $\{0, 1\}^* \setminus A \in \mathbf{NP}$ なわけではない)



NP の定義 (復習)

「 $\exists P$ 」とか
名づけたほうが
良かったかも

定義 (再)

言語 $A \subseteq \{0, 1\}^*$ が **NP** に属するとは
或る多項式 $p: \mathbf{N} \rightarrow \mathbf{N}$ と言語 $B \in \mathbf{P}$ とが存在し
任意の $x \in \{0, 1\}^*$ に対し

$$x \in A \iff \text{或る } r \in \{0, 1\}^{p(|x|)} \text{ が存在して } (x, r) \in B$$

例えば次の問題は **NP** に属する

問題

SAT

入力

命題論理式 φ

答

φ は充足可能か

$$\because \varphi \in \text{SAT} \iff \text{或る } \underline{\text{真理値割当 } a} \text{ が存在して } \underline{a \text{ は } \varphi \text{ を充足}}$$

長さが φ と同程度以下

容易に (**P** で) 判る



言語 $A \subseteq \{0, 1\}^*$ が **coNP** に属するとは
補言語 $\{0, 1\}^* \setminus A$ が **NP** に属することをいう すなわち

定義

言語 $A \subseteq \{0, 1\}^*$ が **coNP** に属するとは
或る多項式 $p: \mathbf{N} \rightarrow \mathbf{N}$ と言語 $B \in \mathbf{P}$ とが存在し
任意の $x \in \{0, 1\}^*$ に対し

$$x \in A \iff \text{すべての } r \in \{0, 1\}^{p(|x|)} \text{ に対し } (x, r) \in B$$

例えば次の問題は **coNP** に属する

問題

UNSAT

入力

命題論理式 φ

答

φ は充足不能か

問題

VALID

入力

命題論理式 φ

答

φ は恒真か



$$\begin{aligned} \mathbf{P} &= \Sigma_0^{\mathbf{P}} = \Pi_0^{\mathbf{P}} \\ \mathbf{NP} &= \Sigma_1^{\mathbf{P}} \\ \mathbf{coNP} &= \Pi_1^{\mathbf{P}} \end{aligned}$$

定義

言語 $A \subseteq \{0, 1\}^*$ が $\Sigma_k^{\mathbf{P}}$ に属する ($k = 0, 1, 2, \dots$) とは
 或る多項式 $p: \mathbf{N} \rightarrow \mathbf{N}$ と言語 $B \in \mathbf{P}$ が存在し
 任意の $x \in \{0, 1\}^*$ に対し

$$x \in A \iff \exists r_k \in \{0, 1\}^{p(|x|)} \forall r_{k-1} \in \{0, 1\}^{p(|x|)} \dots \exists r_1 \in \{0, 1\}^{p(|x|)} \\ (x, r_1, \dots, r_k) \in B$$

∃ と ∀ が交互に現れる

k の偶奇に応じて ∀ か ∃

言語 $A \subseteq \{0, 1\}^*$ が $\Pi_k^{\mathbf{P}}$ に属するとは $\{0, 1\}^* \setminus A$ が $\Sigma_k^{\mathbf{P}}$ に属すること

例えば次の問題は $\Pi_2^{\mathbf{P}}$ に属する

問題

入力 命題論理式 φ

SHORTEST

答

φ は等価な論理式のうち (文字列として) 最短か

$$\because \varphi \in \text{SHORTEST} \iff \varphi \text{ より小さい } \underline{\text{すべての}} \text{ 論理式 } \psi \text{ に対し} \\ \underline{\text{或る}} \text{ 真理値割当 } a \text{ において } \varphi(a) \neq \psi(a)$$

問題

入力

命題論理式 $\varphi = \varphi(\vec{X}, \vec{Y})$

TAQSAT

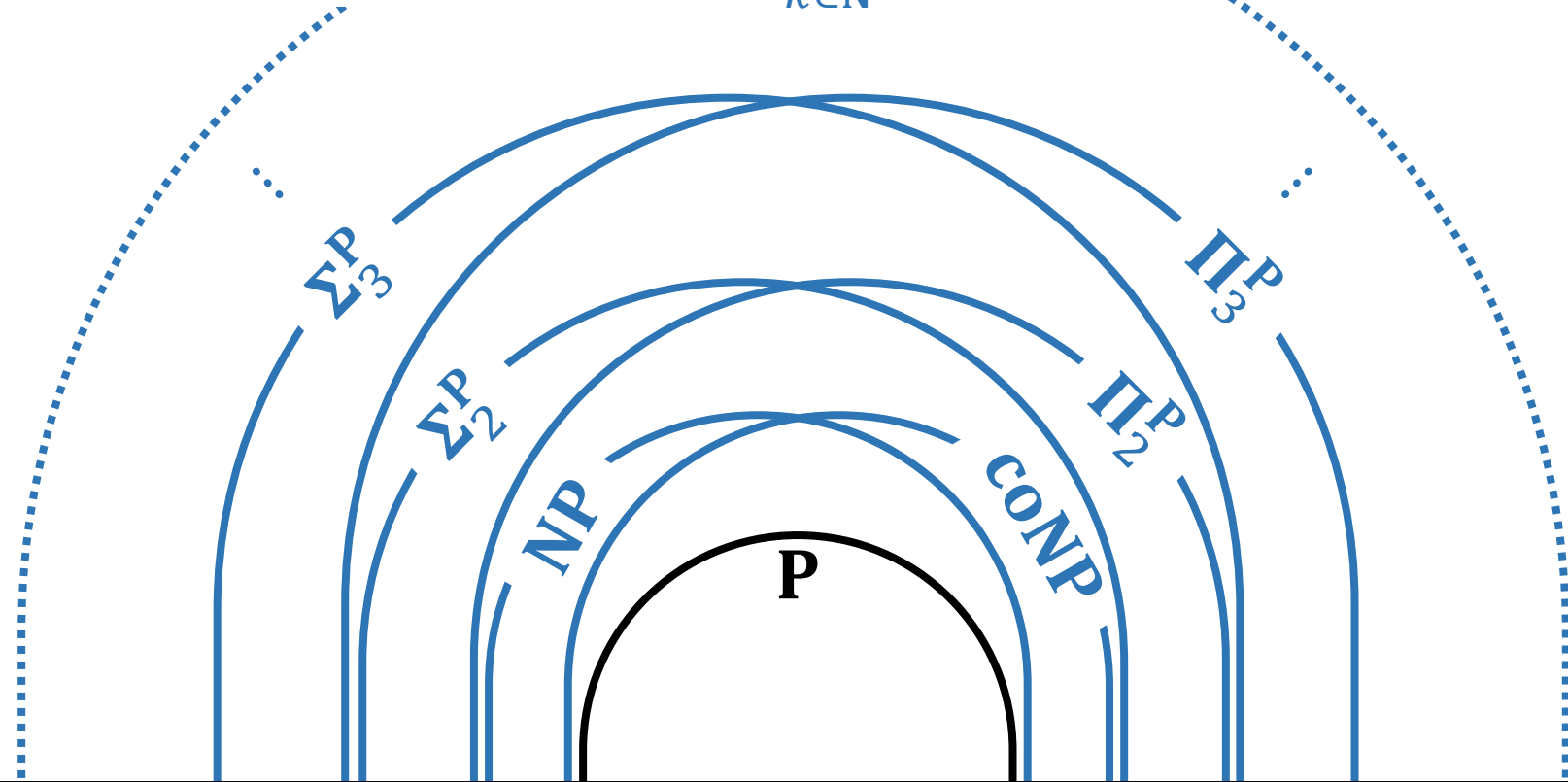
答

$\vec{X}$ への任意の割当 a に対し $\vec{Y}$ への割当 b が存在し $\varphi(a, b) = \text{真}$



多項式時間階層

$$PH = \bigcup_{k \in \mathbb{N}} \Sigma_k^P$$

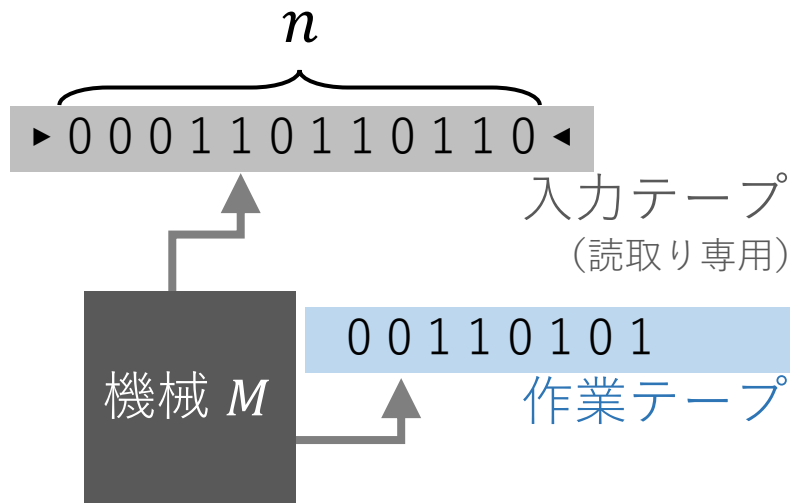


包含関係は図の通りだが
等しいか否か (真の包含 $\subsetneq$ であるか) は判っていない
(もし $NP = P$ なら上記の集合はすべて等しいことになる)



空間の制限 $\left(\begin{array}{l} \text{記憶領域の量を} \\ \sigma: \mathbf{N} \rightarrow \mathbf{N} \text{ に限定するとは?} \end{array} \right)$

機械 M に x を入力して計算



入力の長さ n のとき
(停止し それまでに)

作業テープ上で
最初の位置から
左右に $O(\sigma(n))$ 個以内
までの桁目しか訪れない

定義

σ 空間限定の機械により認識される言語全体を
Space($\sigma(n)$) で表す



定義

$$\mathbf{PSPACE} = \bigcup_{k \in \mathbb{N}} \mathbf{Space}(n^k)$$

多項式空間

$$\mathbf{L} = \mathbf{Space}(\log n)$$

対数空間

入力よりも小さい作業領域！

まとめると……

対数空間

〔多項式 p が存在して
 $n \mapsto \log p(n)$ 空間限定〕

多項式時間

〔多項式 p が存在して
 p 時間限定〕

多項式空間

〔多項式 p が存在して
 p 空間限定〕

指数時間

〔多項式 p が存在して
 $n \mapsto 2^{p(n)}$ 時間限定〕

……の機械によって認識される言語の全体がそれぞれ

L

$\subseteq$

後で

P

$\subseteq$

自明

PSPACE

$\subseteq$

後で

EXP

問題
SR₌入力 書換え規則の集合 R と文字列 $w, w' \in \Sigma^*$ R の各規則は $u \rightarrow v$ という形 ($u, v \in \Sigma^*, |u| = |v|$)文字列の一部を u から v に書換えることができるという意味答 R による書換えを次々と w に施して w' にできるかつまり
 $xuy \Rightarrow_R xvy$
とできる $w \Rightarrow_R^* w'$ と
書くこと
にする

例

入力

 $R \begin{cases} aab \rightarrow bbb \\ aba \rightarrow baa \end{cases}$ $w = aababab$ $w' = bbbbbb$

答

受理

$$\left(\begin{array}{l} aababab \Rightarrow_R bbbabab \Rightarrow_R \\ bbbbaab \Rightarrow_R bbbbbb \\ \text{とできるので} \end{array} \right)$$

定理 (後で示す)

SR₌ $\in$ PSPACE問題
SR₌¹SR₌ と同じだが R による書換えを次々と w に施すと
可能な書換え方が毎回一通りしか
ないことが保証されている

(例えば左の入力例はこれを満たさない)

定理

SR₌¹ $\in$ PSPACE

∴ 書換えを実際に順次行ってみればよい



定理

PH $\subseteq$ PSPACE

定義 (再)

言語 A が Σ_k^P に属するとは
多項式 $p: \mathbf{N} \rightarrow \mathbf{N}$ と多項式時間関数
任意の入力 x に対し

$$x \in A \iff \exists r_k \in \{0, 1\}^{p(|x|)} \forall r_{k-1} \in \{0, 1\}^{p(|x|)} \dots \exists r_1 \in \{0, 1\}^{p(|x|)} \\ (x, r_1, \dots, r_k) \in B$$

$\therefore$ すべての $r_1, \dots, r_k$ について
ひたすら調べ尽せば
よい



問題
QBF

与えられた量化命題論理式

命題変数

真 (1) か偽 (0) の値をとる

$$Q_n X_n \cdot Q_{n-1} X_{n-1} \dots Q_1 X_1 \cdot \varphi(X_1, \dots, X_n)$$

の真偽を判定せよ

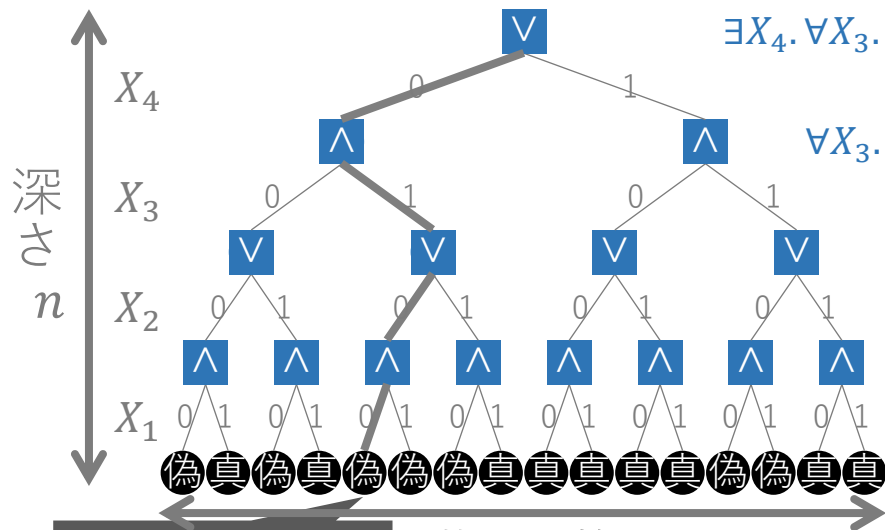
量化子 ($\forall$ か $\exists$)

定理

QBF $\in$ PSPACE

例

$$\exists X_4 \cdot \forall X_3 \cdot \exists X_2 \cdot \forall X_1 \cdot (X_2 \vee \neg X_3) \wedge (X_1 \vee X_4)$$



$$\varphi(0, 0, 1, 0) = \text{偽}$$

容易に計算できる

この例では
 $n = 4$

$$\begin{aligned} \text{QBF}(\forall x. \psi(x)) &= \text{QBF}(\psi(0)) \wedge \text{QBF}(\psi(1)) \\ \text{QBF}(\exists x. \psi(x)) &= \text{QBF}(\psi(0)) \vee \text{QBF}(\psi(1)) \end{aligned}$$

深さ優先探索

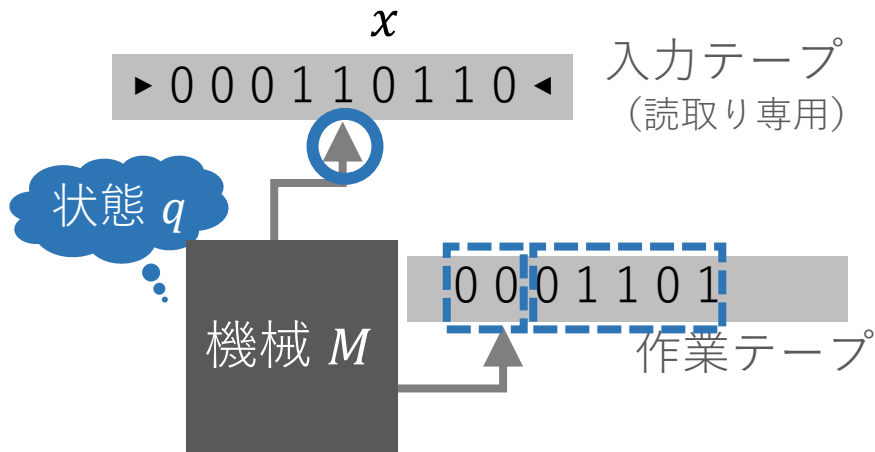
➡ 空間量 $O(n)$



定理

$$\text{PSPACE} \subseteq \text{EXP}$$

※ 同様に $\text{L} \subseteq \text{P}$



例えば上図の状況を文字列で
「...」00[$q, 5$]01101「...」
のように表すことにする (時点表示)

- ◆ 状態
- ◆ 入力テープ上の現在位置
- ◆ 作業テープの内容 (現在位置より左の部分・右の部分)

証明概略

- 或る瞬間の時点表示から次の瞬間の時点表示は (M と x によって) 決まる
- 機械 M が多項式空間限定なら時点表示は入力長 $|x|$ の指数個 (多項式 q が存在して $2^{q(|x|)}$ 個以内)



指数時間以内で停止



定理 (再)

$SR_= \in PSPACE$

※ $\Sigma = \{a, b\}$ として考える

問題
 $SR_=$

入力

(R, w, w') 但し R は
長さを保つ書換え規則の集合

答

$w \Rightarrow_R^* w'$ か

入力の長さが n である (w の長さ $< n$) とき

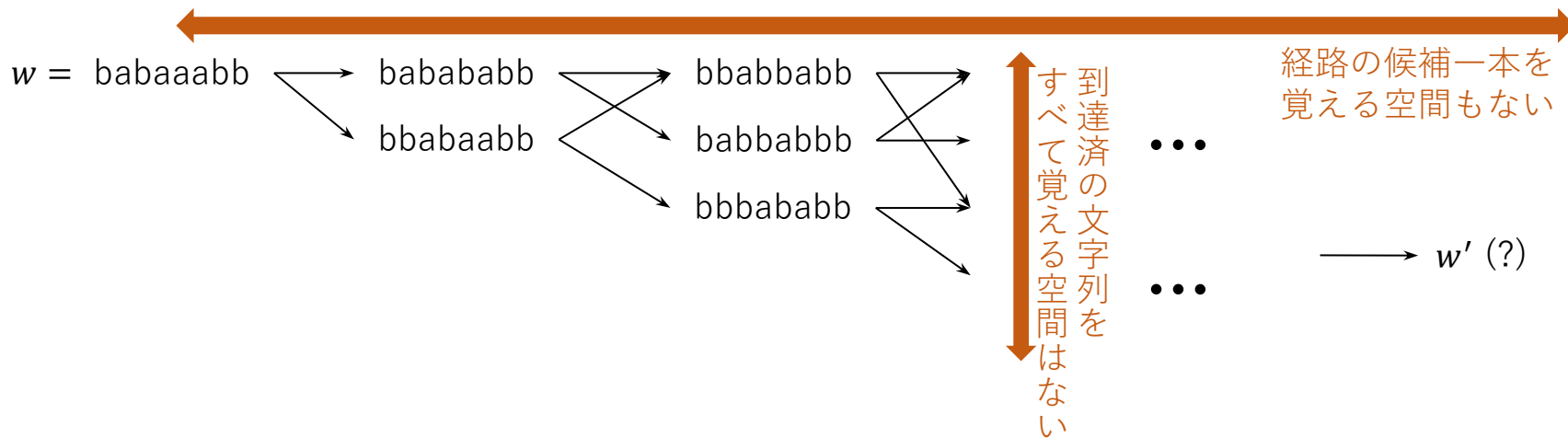
w から書換えにより生じ得る文字列も長さ $< n$ であり その個数は $< 2^n$

したがって $w \Rightarrow_R^{\leq 2^n} w'$ かどうか調べればよい

書換え 2^n 回以内で w から w' が得られる

という意味

しかし 素朴な方法では長さ $\leq 2^n$ の経路すべてを調べることはできない





定理 (再)

$SR_= \in PSPACE$

問題
 $SR_=$

入力

(R, w, w') 但し R は
長さを保つ書換え規則の集合

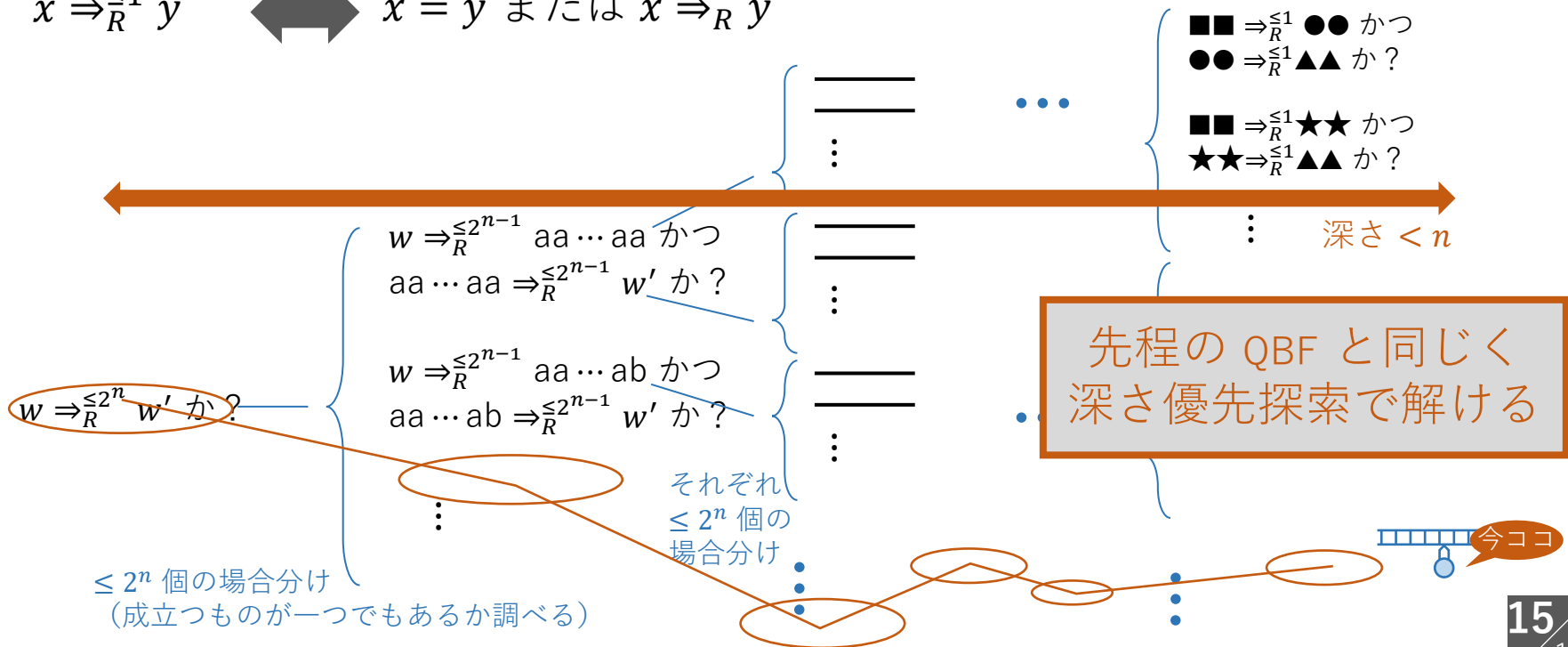
答

$w \Rightarrow_R^* w'$ か

$w \Rightarrow_R^{\leq 2^n} w'$ かどうか 次の関係を再帰的に用いて調べればよい

$x \Rightarrow_R^{\leq 2^{i+1}} y \iff$ 或る $z \in \Sigma^{< n}$ が存在して $x \Rightarrow_R^{\leq 2^i} z$ かつ $z \Rightarrow_R^{\leq 2^i} y$

$x \Rightarrow_R^{\leq 1} y \iff x = y$ または $x \Rightarrow_R y$





問題
SPACE_EVAL

入力 機械 M と $x \in \{0, 1\}^*$ と $s \in \mathbf{N}$ の組 $(M, x, 0^s)$
答 M に x を入力すると空間量 $\leq s$ で受理するか

定理

任意の $A \in \mathbf{PSPACE}$ に対し
 A から SPACE_EVAL への多項式時間帰着が存在

SPACE_EVAL は **PSPACE** 完全

証明 言語 $A \in \mathbf{PSPACE}$ を任意に取る

多項式 $p: \mathbf{N} \rightarrow \mathbf{N}$ と A を認識する p 空間限定の機械 M が存在する
変換 $x \mapsto (M, x, 0^{p(|x|)})$ は A から SPACE_EVAL への多項式時間帰着



定理

$SR_{=}^1$ は **PSPACE** 完全

証明概略

SPACE_EVAL (前頁) からの帰着による

与えられた

- ◆ 機械 M
- ◆ 文字列 x
- ◆ 空間制限 0^s

を

- ◆ 時点表示を一時刻進めることを表す書換え規則集合 R
- ◆ 最初の時点表示 w
- ◆ 受理の時点表示 w'

に変換

NP と同様に定義

同様に考えると「 $SR_{=}$ は **NPSPACE** 完全」とも判る

ところが $SR_{=} \in \mathbf{PSPACE}$ なのだから

定理 [Savitch 1970]

NPSPACE = PSPACE



定理

QBF は **PSPACE** 完全

問題
SR₌

入力

(R, w, w') 但し R は
長さを保つ書換え規則の集合

答

$w \Rightarrow_R^* w'$ か

$w \Rightarrow_R^{\leq 2^n} w'$ かどうかを
調べれば良い (先述)

SR₌ を QBF に帰着する

先ほど SR₌ ∈ **PSPACE** を示したときと同じ次の関係を用いる

$$x \Rightarrow_R^{\leq 2^{i+1}} y \iff \exists z (x \Rightarrow_R^{\leq 2^i} z \text{ かつ } z \Rightarrow_R^{\leq 2^i} y) \iff \exists z \forall u, v$$

(もし $(u, v) = (x, z)$ または $= (z, y)$ ならば $u \Rightarrow_R^{\leq 2^i} v$)

これを再帰的に用いて

$$\underline{w \Rightarrow_R^{\leq 2^n} w'} \iff \exists z_n \forall u_n, v_n \quad \exists z_{n-1} \forall u_{n-1}, v_{n-1} \quad \cdots \exists z_1 \forall u_1, v_1$$

もし $(u_n, v_n) = (w, z_n)$ または $= (z_n, w')$ ならば
 もし $(u_{n-1}, v_{n-1}) = (u_n, z_{n-1})$ または $= (z_{n-1}, v_n)$ ならば

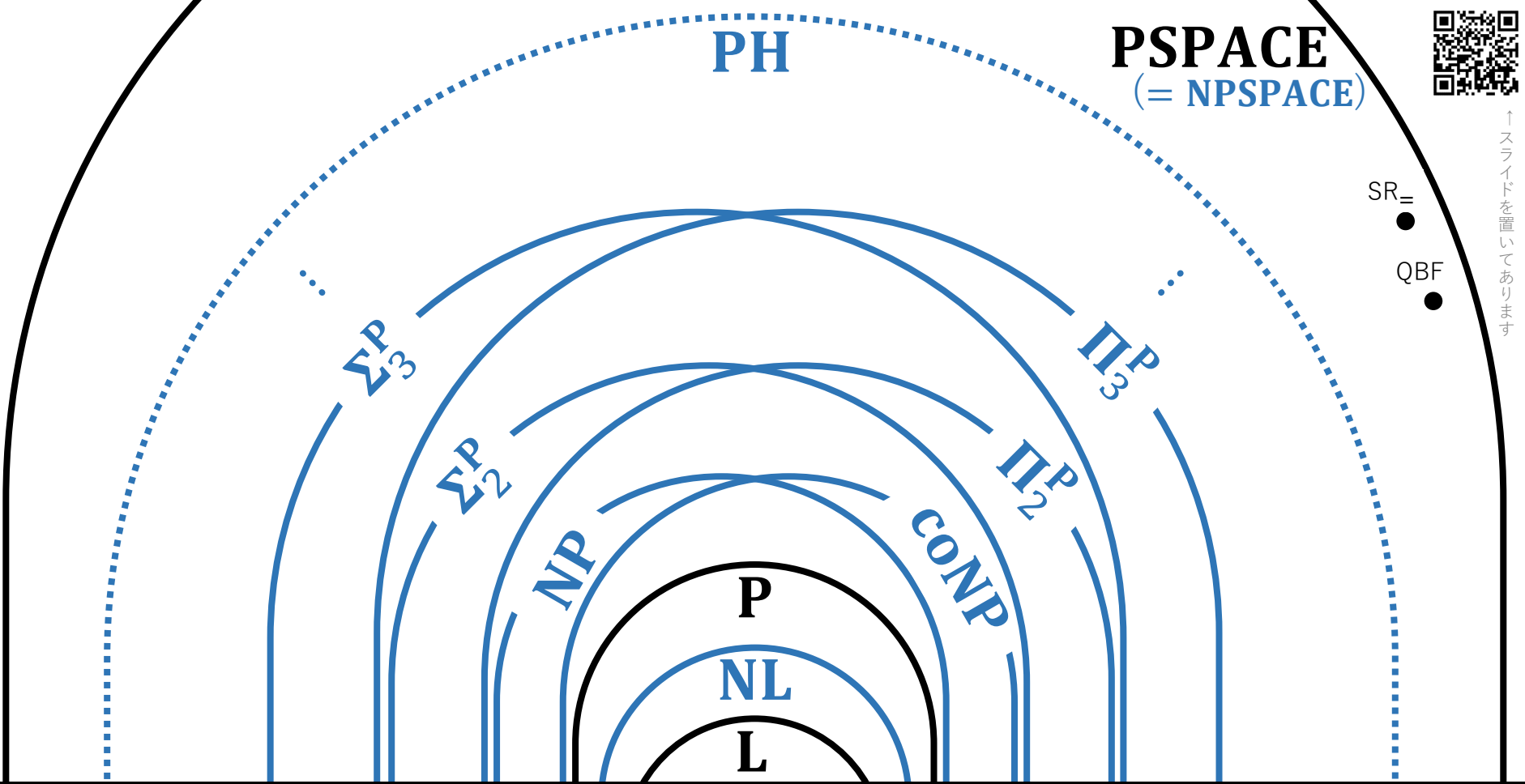
 もし $(u_1, v_1) = (u_2, z_1)$ または $= (z_1, v_2)$ ならば $u_1 \Rightarrow_R^{\leq 1} v_1$)

これを
量化命題論理式として
書くことができる



↑
スライドを置いてあります

SR=
●
QBF
●



包含関係は図の通りだが
等しいか否か（真の包含 $\subsetneq$ であるか）については
 $L \subsetneq PSPACE$ であること以外は証明されていない



演習 (1/3)

1. スライド5頁では **coNP** の定義を二つ, 「すなわち」の前後に述べた. 第一の定義 (4頁で定義した **NP** を用いたもの) と第二の定義 (5頁の赤い定義枠の中) が等価であることを示せ.
2. スライド7頁で, もし **NP = P** ならば **PH = P** であると述べた. 一般に, もし $\Sigma_{k+1}^P = \Sigma_k^P$ ならば **PH = Σ_k^P** であることを示せ.



演習 (2/3)

3. スライド9頁で **PSAPCE** と **L** の定義を見た太郎君は,
PSPACE (や **P**) の定義にある「 k 乗」を **L** にも付けて

$$\mathbf{PolyL} = \bigcup_{k \in \mathbf{N}} \mathbf{Space}((\log n)^k)$$

というものを考えるべきではないかと思った.

13頁の「同様に $\mathbf{L} \subseteq \mathbf{P}$ 」の議論を説明するとともに, 同じやり方で $\mathbf{PolyL} \subseteq \mathbf{P}$ とはいえないことを確認せよ. なお実際, $\mathbf{PolyL} \subseteq \mathbf{P}$ か否かは未解決である.



演習 (3/3)

4. スライド10頁の言語 $SR_{\leq}$ の定義にあった $|u| = |v|$ という条件を外して得られる言語 SR が, 判定不能であることを示せ. 必要なら17頁にある $SR_{\leq}^1$ の **PSPACE** 完全性の議論の細部は既知とし, それとの違いについてのみ説明すればよい.
5. スライド12頁で言語 **QBF** を見た次郎君が「**PH** は5頁のように **P** の言語に何度か交替する量子子を付けた形に書ける言語からなり, その交替の回数 k が幾つでもよいわけだから, **QBF** は **PH** に属する」と主張している. この説が何故おかしいか, 次郎君にわかるように説明せよ.