↑スライドを置いてあります

計算量理論

令和5年11月14日

担当　河村彰星 (京大)

- 多項式時間階層
- 多項式空間

$\mathbf{P}$ の定義 (復習)

多項式 $p: \mathbf{N} \to \mathbf{N}$ 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 $\mathbf{P}$ 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

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

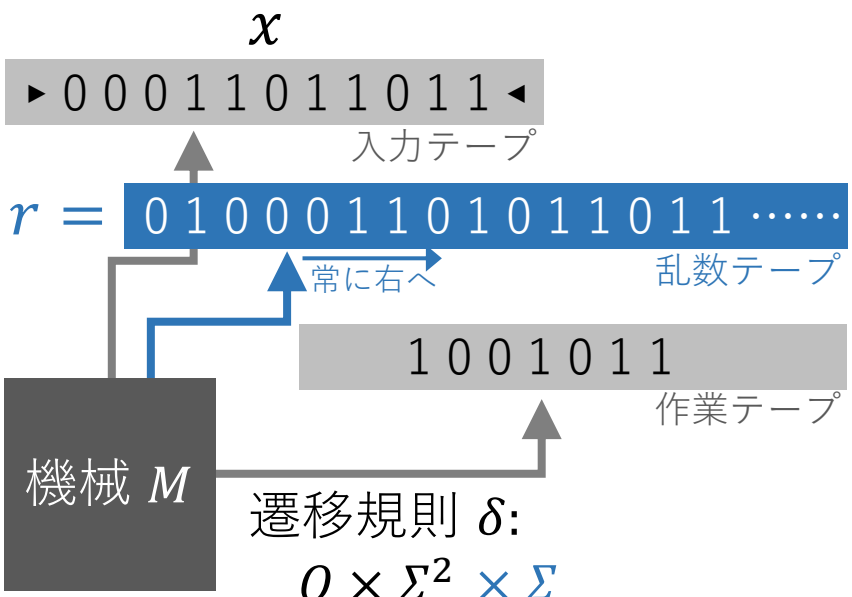
が成立つことをいう

これを「M が A を**認識**する」という

※ 今日は $\mathbf{P}$ などは言語 (判定問題) の集合とする

NP の定義はどこが変る？　→次頁～

非決定性機械



遷移規則 δ:

$Q \times \Sigma^2 \times \Sigma$

$\longrightarrow Q \times \Sigma \times \{左, 右\}^2$

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

計算結果

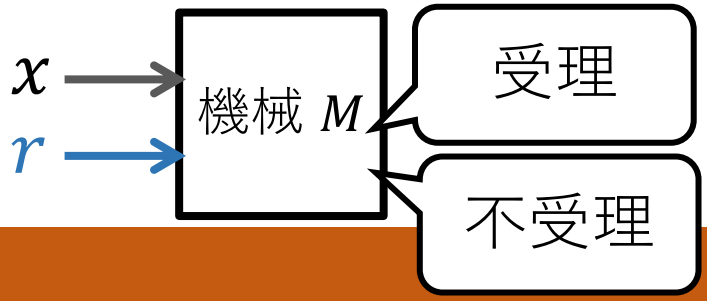
$M(x, r)$ ← 受理か不受理

入力　乱数　に依存

この機械が

$p: \mathbf{N} \to \mathbf{N}$ 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

定義

言語 $A \subseteq \{0,1\}^*$ が **NP** に属するとは
多項式 $p\colon \mathbf{N} \to \mathbf{N}$ 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 $B \in \mathbf{P}$

$x \in A \quad \Leftrightarrow \quad$ 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）

定義（再）

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

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

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

$\because$ $\varphi \in \mathrm{SAT}$ $\Leftrightarrow$ 或る真理値割当 a が存在して a は φ を充足

- 真理値割当 a：長さが φ と同程度以下
- a は φ を充足：容易に（**P** で）判る

↑スライドを置いてあります

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 $p\colon \mathbf{N} \to \mathbf{N}$ と言語 $B \in \mathbf{P}$ とが存在し
任意の $x \in \{0,1\}^*$ に対し

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

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

定義

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

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

言語 $A \subseteq \{0,1\}^*$ が $\boldsymbol{\Pi}_k^{\mathbf{P}}$ に属するとは $\{0,1\}^* \setminus A$ が $\boldsymbol{\Sigma}_k^{\mathbf{P}}$ に属すること

$$\mathbf{P} = \boldsymbol{\Sigma}_0^{\mathbf{P}} = \boldsymbol{\Pi}_0^{\mathbf{P}}$$
$$\mathbf{NP} = \boldsymbol{\Sigma}_1^{\mathbf{P}}$$
$$\mathbf{coNP} = \boldsymbol{\Pi}_1^{\mathbf{P}}$$

∃ と ∀ が交互に現れる

k の偶奇に応じて ∀ か ∃

例えば次の問題は $\boldsymbol{\Pi}_2^{\mathbf{P}}$ に属する

問題 SHORTEST

入力 命題論理式 φ

答 φ は等価な論理式のうち (文字列として) 最短か

$\because$ $\varphi \in$ SHORTEST $\iff$ φ より小さい**すべての**論理式 ψ に対し
或る真理値割当 a において $\varphi(a) \neq \psi(a)$

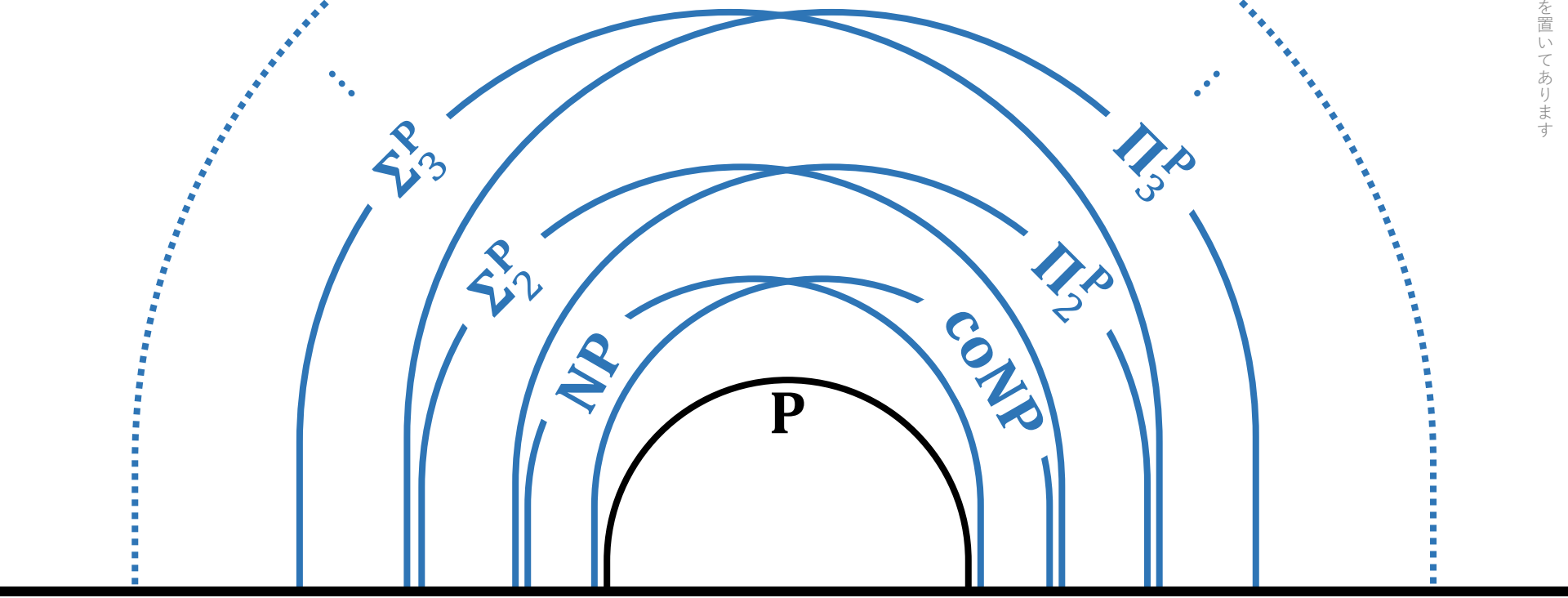
問題 ∀∃SAT

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

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 $\varphi(a,b) =$ 真

多項式時間階層

$$\mathbf{PH} = \bigcup_{k \in \mathbf{N}} \boldsymbol{\Sigma}_k^{\mathbf{P}}$$

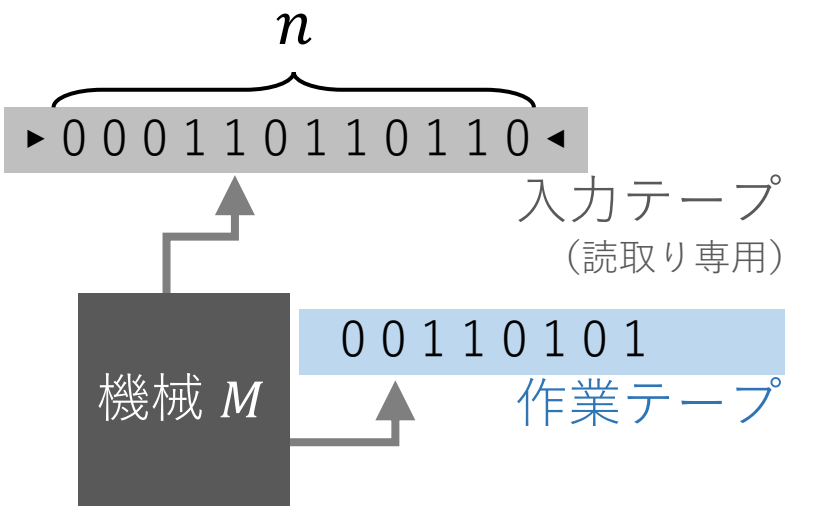


包含関係は図の通りだが
等しいか否か (真の包含 $\subsetneq$ であるか) は判っていない
(もし $\mathbf{NP} = \mathbf{P}$ なら上記の集合はすべて等しいことになる)

↑スライドを置いてあります

σ 空間限定の機械（$\sigma: \mathbf{N} \to \mathbf{N}$）

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
までの枡目しか訪れない

定義

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

↑スライドを置いてあります

定義

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

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	多項式時間	多項式空間	指数時間
多項式 p が存在して $n \mapsto \log p(n)$ 空間限定	多項式 p が存在して p 時間限定	多項式 p が存在して p 空間限定	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

$$\mathbf{L} \subseteq \mathbf{P} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP}$$

後で　自明　後で

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 $u \to v$ 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

つまり $xuy \Rightarrow_R xvy$ とできる

答 R による書換えを次々と w に施して w' にできるか

$w \Rightarrow_R^* w'$ と書くことにする

例

入力

$$R \begin{cases} \text{aab} \to \text{bbb} \\ \text{aba} \to \text{baa} \end{cases}$$

$w = \text{aababab}$

$w' = \text{bbbbbbb}$

答 受理

$\text{aababab} \Rightarrow_R \text{bbbabab} \Rightarrow_R \text{bbbbaab} \Rightarrow_R \text{bbbbbbb}$ とできるので

定理（後で示す）

$SR_= \in \mathbf{PSPACE}$

問題 $SR_=^1$

$SR_=$ 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さない）

定理

$SR_=^1 \in \mathbf{PSPACE}$

$\because$ 書換えを実際に順次行ってみればよい

↑スライドを置いてあります

定理

$\mathbf{PH} \subseteq \mathbf{PSPACE}$

定義 (再)

言語 A が $\boldsymbol{\Sigma}_k^{\mathbf{P}}$ に属するとは
多項式 $p\colon \mathbf{N} \to \mathbf{N}$ と多項式時間[illegible]
任意の入力 x に対し

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

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

↑スライドを置いてあります

問題
QBF

与えられた量化命題論理式

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

の真偽を判定せよ

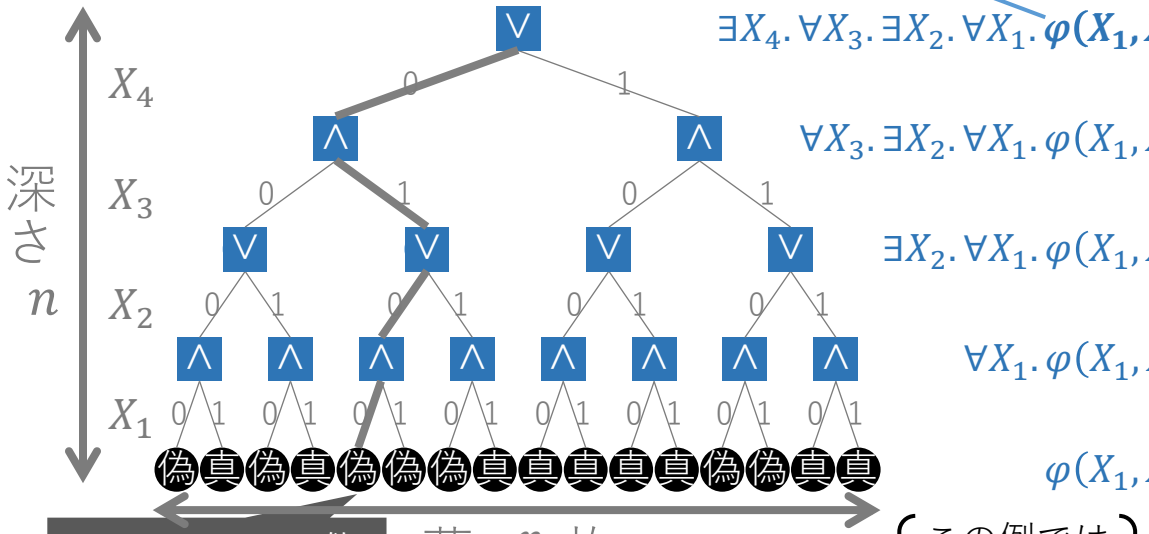
命題変数
真 (1) か偽 (0) の値をとる

量化子 (∀ か ∃)

定理

QBF ∈ **PSPACE**

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



$\exists X_4 . \forall X_3 . \exists X_2 . \forall X_1 . \varphi(X_1, X_2,$

$\forall X_3 . \exists X_2 . \forall X_1 . \varphi(X_1, X_2,$

$\exists X_2 . \forall X_1 . \varphi(X_1, X_2,$

$\forall X_1 . \varphi(X_1, X_2,$

$\varphi(X_1, X_2, X_3, X_4)$

$\varphi(0,0,1,0) =$ 偽
容易に計算できる

葉 2^n 枚

(この例では $n = 4$)

$\mathrm{QBF}(\forall x . \psi(x)) = \mathrm{QBF}(\psi(0)) \wedge \mathrm{QBF}(\psi(1))$

$\mathrm{QBF}(\exists x . \psi(x)) = \mathrm{QBF}(\psi(0)) \vee \mathrm{QBF}(\psi(1))$

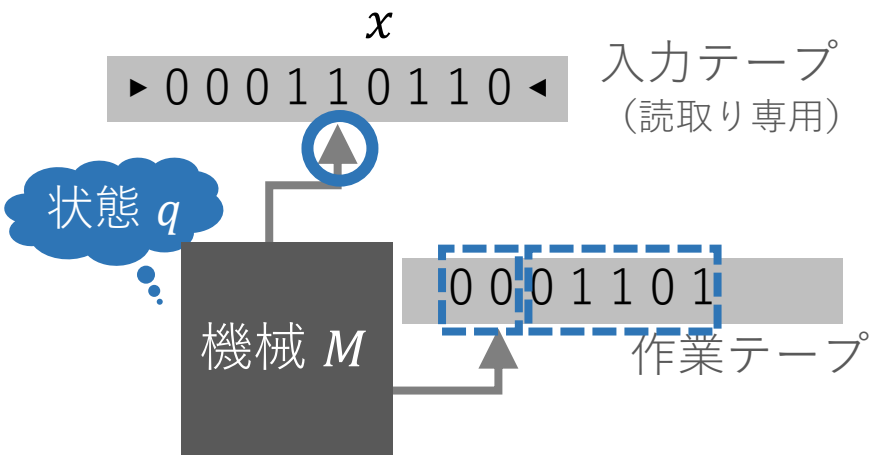
深さ優先探索
➡ 空間量 $O(n)$

↑スライドを置いてあります

定理

PSPACE ⊆ EXP

※ 同様に **L ⊆ 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

↑スライドを置いてあります

定理（再）

$SR_{=} \in \mathbf{PSPACE}$

※ $\Sigma = \{a, b\}$ 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

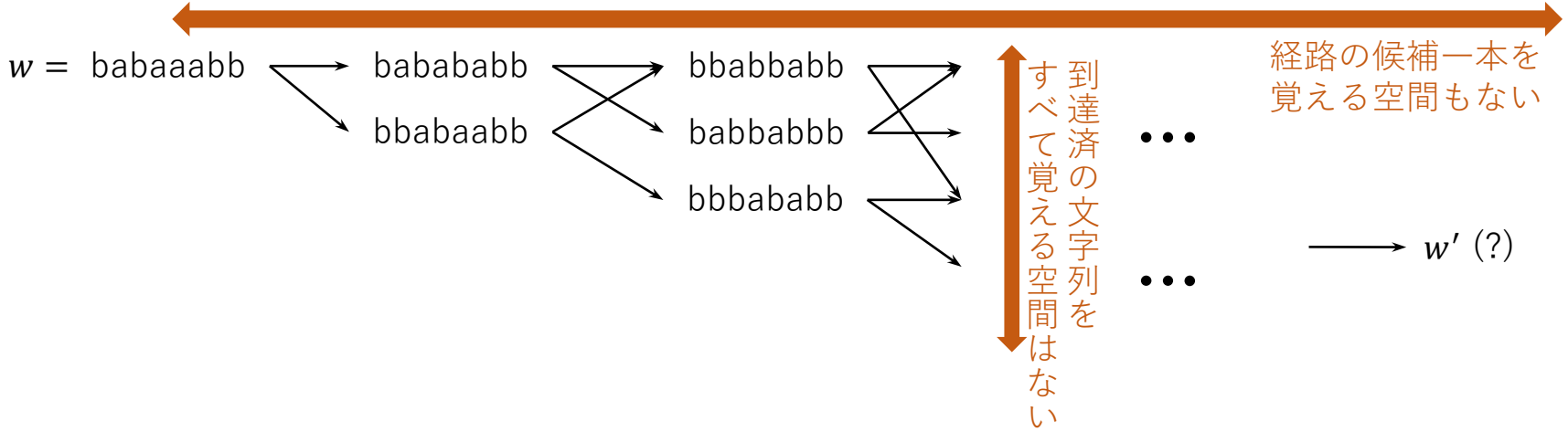
入力の長さが n である（w の長さ $< n$）とき

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）

$\mathrm{SR}_{=} \in \mathbf{PSPACE}$

問題 $\mathrm{SR}_{=}$

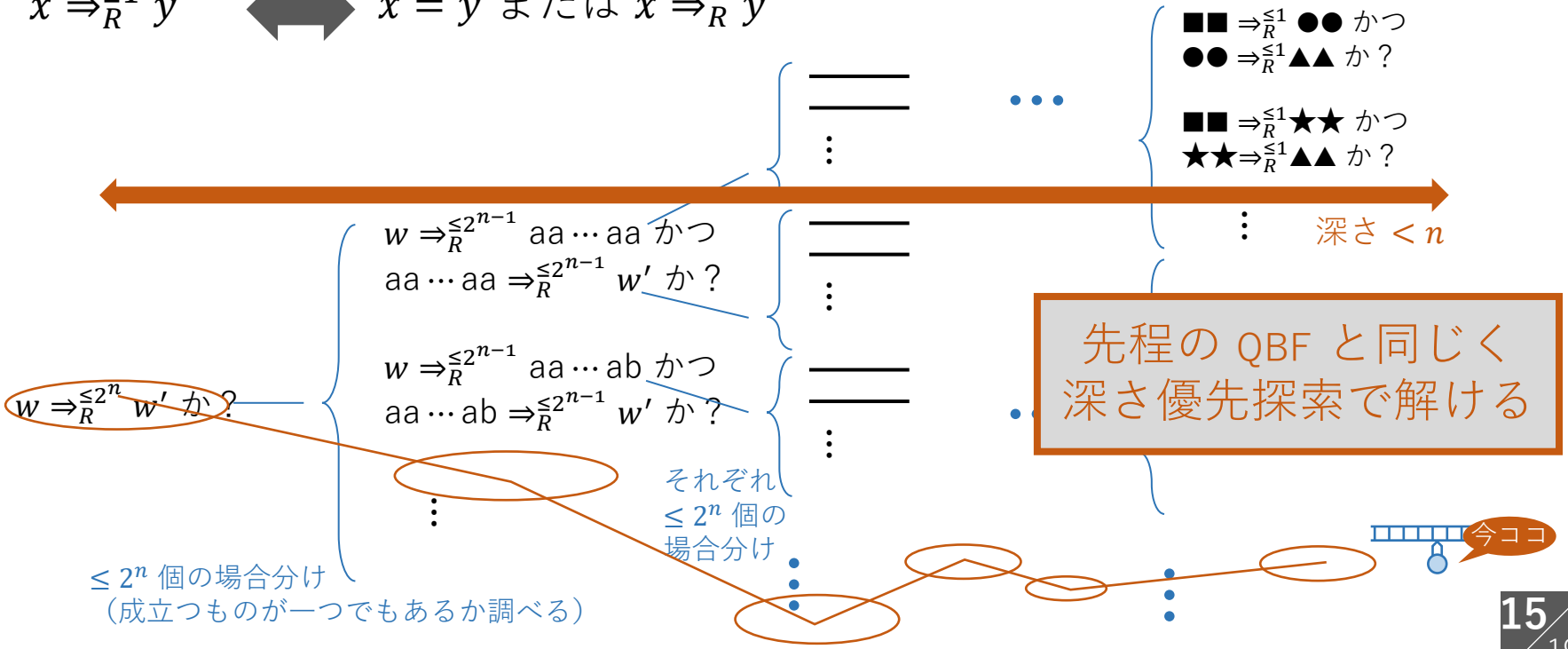
入力 (R, w, w') 但し R は長さを保つ書換え規則の集合

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

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

$x \Rightarrow_R^{\leq 1} y$ ⟺ $x = y$ 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

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

定理

SPACE_EVAL は **PSPACE** 完全

証明 言語 $A \in \mathbf{PSPACE}$ を任意に取る

多項式 $p: \mathbf{N} \to \mathbf{N}$ と A を認識する p 空間限定の機械 M が存在する

変換 $x \mapsto \left(M, x, 0^{p(|x|)}\right)$ は A から SPACE_EVAL への多項式時間帰着

定理

$\mathrm{SR}^1_=$ 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「$\mathrm{SR}_=$ は **NPSPACE** 完全」とも判る

ところが $\mathrm{SR}_= \in$ **PSPACE** なのだから

定理 [Savitch 1970]

$$\mathbf{NPSPACE} = \mathbf{PSPACE}$$

定理

QBF は **PSPACE** 完全

問題 $\mathrm{SR}_=$

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）

$\mathrm{SR}_=$ を QBF に帰着する

先ほど $\mathrm{SR}_= \in$ **PSPACE** を示したときと同じ次の関係を用いる

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

「$\exists\, w$」は「或る $w \in \Sigma^{<n}$ が存在して」
「$\forall\, w$」は「任意の $w \in \Sigma^{<n}$ に対し」の意

$$\iff \exists\, z\ \forall\, u, v$$

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

これを再帰的に用いて

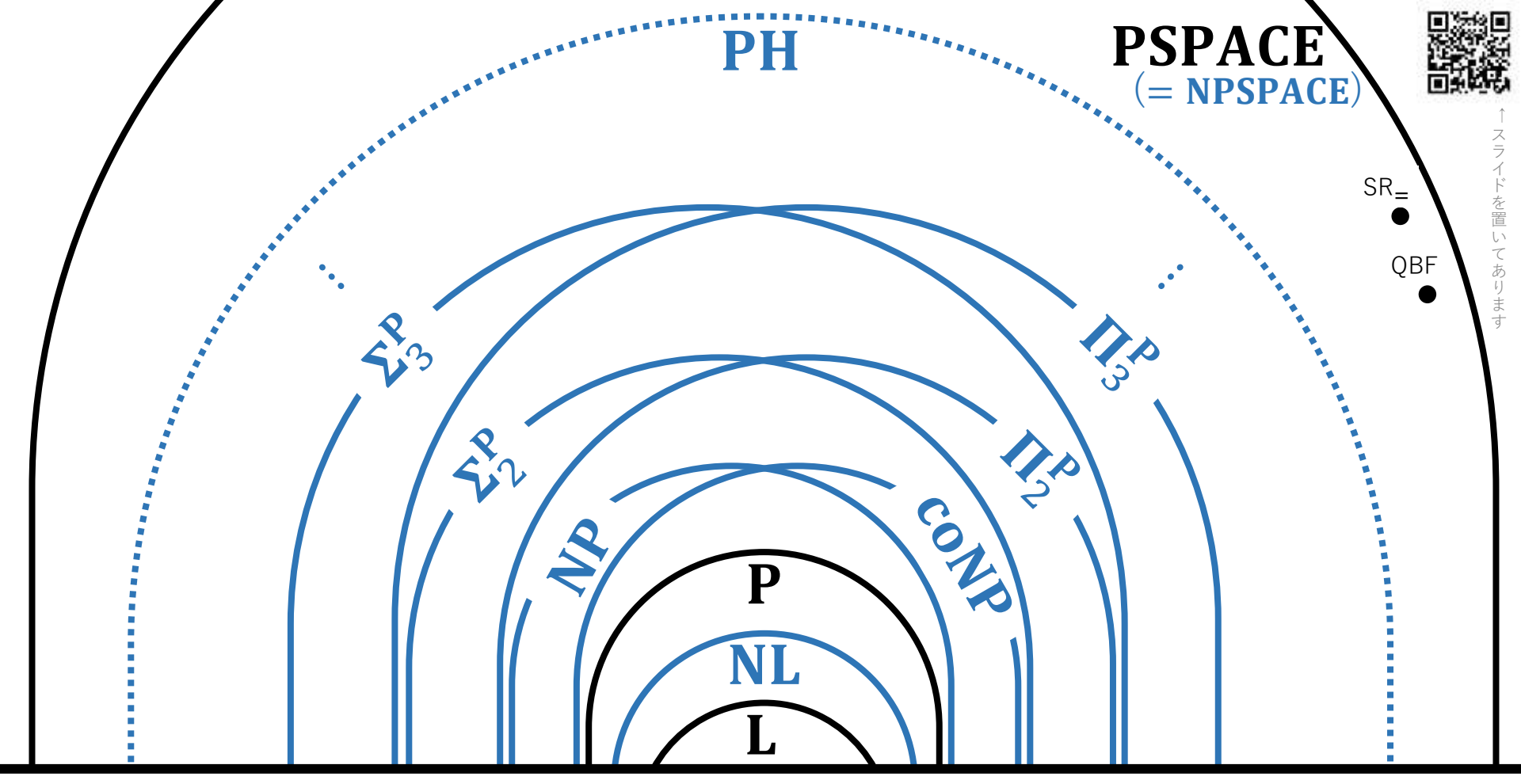
$$w \Rightarrow_R^{\leq 2^n} w' \iff$$

$$\exists\, z_n\ \forall\, u_n, v_n\quad \exists\, z_{n-1}\ \forall\, u_{n-1}, v_{n-1}\quad \cdots\cdots\ \exists\, z_1\ \forall\, u_1, v_1$$

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



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
$\mathbf{L} \subsetneq \mathbf{PSPACE}$ 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 $\mathbf{coNP}$ 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 $\mathbf{NP}$ 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 $\mathbf{NP} = \mathbf{P}$ ならば $\mathbf{PH} = \mathbf{P}$ であると述べた．一般に，もし $\boldsymbol{\Sigma}_{k+1}^{\mathbf{P}} = \boldsymbol{\Sigma}_{k}^{\mathbf{P}}$ ならば $\mathbf{PH} = \boldsymbol{\Sigma}_{k}^{\mathbf{P}}$ であることを示せ．

↑スライドを置いてあります

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

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

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 $\mathrm{SR}_{=}$ 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 $\mathrm{SR}^{1}_{=}$ 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化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．

↑スライドを置いてあります