

# 時相論理とモデルチェック



国立情報学研究所

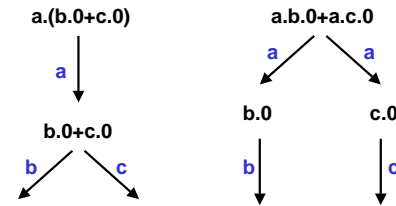
佐藤一郎

E-mail: ichiro@nii.ac.jp

Ichiro Satoh

## プロセス論理

論理学手法を利用したプロセスの使用記述と証明  
例:  $a.(b.0+c.0)$   $a.b.0+a.c.0$



Ichiro Satoh

## プロセス論理

構文:

$P ::= \text{true} \mid \text{false} \mid P \quad Q \mid \neg P \mid \langle a \rangle \mid [a]$

非形式的意味

true	真を表す
false	偽を表す
P Q	PかつQ
$\neg P$	Pの否定
$\langle a \rangle$	アクションaに関する可能様相演算子
[a]	アクションaに関する必然様相演算子

Ichiro Satoh

## プロセス論理

プロセス論理式によるプロセス表現

$a.(b.0+c.0) \models \langle a \rangle \langle b \rangle \text{true} \quad \langle c \rangle \text{true}$   
 $a.b.0+a.c.0 \models \langle a \rangle \langle b \rangle \text{true} \quad \langle a \rangle \langle c \rangle \text{true}$

Hoare論理の様相論理表現

Ichiro Satoh

## ▶ 時相論理

時相論理とは  
状態の遷移や時間の経過の観点よりシステムの性質を記述するための論理体系

代表的形式

- 線形時間時相論理  
LTL (Linear Time Temporal Logic)
- 分岐時間時相論理  
CTL (Computation Tree Logic)  
 $\mu$  計算 ( $\mu$ -calculus)
- モデル検査  
時相論理で表現された性質を  
システムが満たすかどうかを検査すること

Ichiro Satoh

## ▶ 様相論理

- |        |             |              |
|--------|-------------|--------------|
| ■ 可能性: | ~ は必然である    | ~ は可能である     |
| ■ 時間:  | いつでも ~ である  | ~ であるときがある   |
| ■ 場所:  | どこでも ~ である  | あるところで ~ である |
| ■ 確実性: | ~ でなければならない | ~ かもしれない     |
| ■ 信念:  | ~ を知っている    | ~ を信じている     |

$P$

$P$

Ichiro Satoh

## ▶ 様相論理

- 様相論理
- 必然性と可能性の論理
- 時相論理
- 知識と信念の論理
- 義務論理
- ダイナミック論理
- 内包論理

Ichiro Satoh

## ▶ 論理体系

古典論理 (classical logic)

命題論理

1 階述語論理 ... 導出原理, Prolog

非古典論理 (non-classical logic)

様相論理

高階論理

内包論理

多ソート論理

多値論理, fuzzy 論理

非単調論理

etc.

Ichiro Satoh

## ▶ 様相論理式

命題変数

$P, Q, R, \dots$

$\neg$  : 論理式

$\neg$  ... 「でない」  
... 「かつ」  
... 「または」  
... 「ならば」  
... 「とは同値」  
... 「は必然である」  
... 「は可能である」

$\equiv$   $\Rightarrow$   $\Leftarrow$

Ichiro Satoh

## ▶ 様相論理式 (例)

$P$  ... 「晴れている」

$Q$  ... 「風が吹いている」

... 「どこでも である」

$P \supset P$

「どこでも晴れているならば、晴れている」

$(P \supset Q)$

「どこでも晴れていて風が吹いている」

Ichiro Satoh

## ▶ 様相論理式 (例)

$P$  ... 「晴れている」

$Q$  ... 「風が吹いている」

... 「どこでも である」

$(P \supset Q) \supset P \supset Q$

「どこでも晴れていて風が吹いているならば、  
どこでも晴れていて、かつ、どこでも風が吹いている」

Ichiro Satoh

## ▶ 様相論理式 (例)

$P$  ... 「晴れている」

$Q$  ... 「風が吹いている」

... 「どこでも である」

$(P \supset Q) \supset P \supset Q$

「どこでも晴れていて風が吹いているならば、  
どこでも晴れていて、かつ、どこでも風が吹いている」

$(P \supset Q) \supset P \supset Q$

「どこでも晴れているか風が吹いているならば、  
どこでも晴れているか、または、どこでも風が吹いている」

Ichiro Satoh

## ▶ 様相論理式(例)

$P$  ... 「銀行は潰れる」  
... 「は必然である」  
... 「は可能である(あり得る)」

$P$   $P$

「銀行は潰れることは必然であるならば、銀行は潰れる」

$P$   $P$

「銀行は潰れることは必然であるならば、銀行は潰れることがありえる」

Ichiro Satoh

## ▶ 様相論理式(例)

$P$  ... 「学生は勉強する」  
... 「でなければならない」  
... 「でもよい」

$P$   $P$

「学生は勉強しなければならないならば、  
学生は勉強する」

$P$   $P$

「学生は勉強しなければならないならば、  
学生は勉強してもよい」

Ichiro Satoh

## ▶ 様相論理式(例)

$P$  ... 「太陽は西から昇る」  
... 「であることを信じている」

$P$   $P$

「太陽は西から昇ることを信じているならば、  
太陽は西から昇る」

Ichiro Satoh

## ▶ 様相論理式(例)

... 「であることを知っている」

「であることを知っているならば、  
であることを知っていることを知っている」

$\neg$   $\neg$

「であることを知らないならば、  
であることを知らないことを知っている」

Ichiro Satoh

## ▶ 可能世界意味論

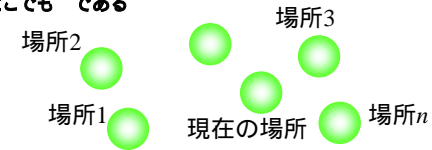
現在の場所・時刻とは別の場所・時刻における  
の真理値を考慮する

場所・時刻 ... 可能世界 (possible world)  
可能世界ごとに論理式を解釈

Ichiro Satoh

## ▶ 可能世界意味論

... どこでも である



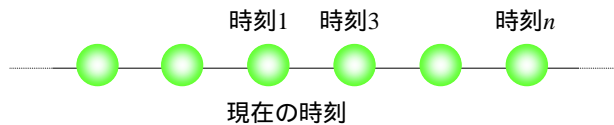
... どこかでは である



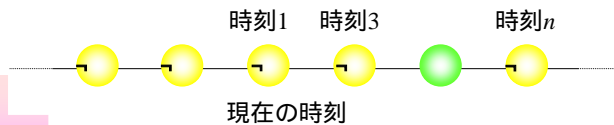
Ichiro Satoh

## ▶ 可能世界意味論

... いつでも である



... いつかは である



Ichiro Satoh

## ▶ Kripke 構造 (structure)

$M = \langle W, R, V \rangle$

$W$

$w \in W \dots$  可能世界 (possible world), 世界

$R \subseteq W^2$

$W$ 上の到達関係 (accessibility relation)

Ichiro Satoh

## Kripke 構造

$M = \langle W, R, V \rangle$

$W$

$w \in W \dots$  世界(world)

$R \subseteq W^2$

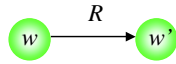
$W$ 上の到達関係 (accessibility relation)

$wRw' \dots w'$  は  $w$  から到達可能

$V : P \times W \rightarrow \{T, F\}$

$P$  : すべての命題変数からなる集合

真理値割当 (truth value assignment)



Ichiro Satoh

## Kripke構造の解釈

$M = \langle W, R, V \rangle$  : Kripke 構造

論理式  $\phi$  は構造  $M$  の世界  $w \in W$  において真  
( $\models_M, w \phi$ )

命題変数  $P$  に対して,

$\models_M, w P$  iff  $V(P, w) = T$

$\models_M, w \neg \phi$  iff  $\not\models_M, w \phi$  でない

$\models_M, w \phi \wedge \psi$  iff  $\models_M, w \phi$  かつ  $\models_M, w \psi$

$\models_M, w \phi \vee \psi$  iff  $\models_M, w \phi$  または  $\models_M, w \psi$

Ichiro Satoh

## Kripke構造の解釈

$M = \langle W, R, V \rangle$  : Kripke 構造

論理式  $\phi$  は構造  $M$  の世界  $w \in W$  において真  
( $\models_M, w \phi$ )

$\models_M, w \phi$

iff  $\models_M, w \phi$  ならば  $\models_M, w \phi$

$\models_M, w \phi$

iff  $\models_M, w \phi$  と  $\models_M, w \phi$  は必要十分

Ichiro Satoh

## Kripke構造の解釈

$M = \langle W, R, V \rangle$  : Kripke 構造

論理式  $\phi$  は構造  $M$  の世界  $w \in W$  において真  
( $\models_M, w \phi$ )

$\models_M, w \phi$

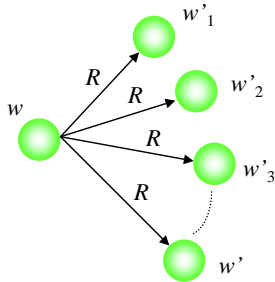
iff  $wRw'$  を満たすすべての  $w'$  に対して,  
 $\models_M, w' \phi$

$w$  から到達可能なすべての  $w'$  に対して,  $\models_M, w' \phi$

Ichiro Satoh

## Kripke構造の解釈

$\models_{M,w}$   
iff  $wRw'$ を満たすすべての  $w'$  に対して,  
 $\models_{M,w'}$



Ichiro Satoh

## Kripke構造の解釈

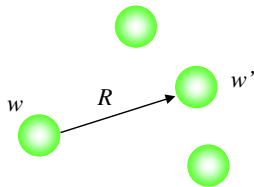
$M = \langle W, R, V \rangle$  : Kripke 構造  
論理式  $\phi$  は構造  $M$  の世界  $w \in W$  において真  
( $\models_{M,w} \phi$ )

$\models_{M,w}$   
iff  $wRw'$ を満たすある  $w'$  に対して,  
 $\models_{M,w'}$   
 $w$  から到達可能なある  $w'$  に対して,  $\models_{M,w'}$

Ichiro Satoh

## Kripke構造の解釈

$\models_{M,w}$   
iff  $wRw'$ を満たすある  $w'$  に対して,  
 $\models_{M,w'}$



Ichiro Satoh

## 分岐時相論理の構文

時相論理(CTL:Computation Tree Logic)

CTL式

原子命題

通常の演算子 :  $\wedge, \vee, \neg$  (not),

時相演算子 : EX, EF, EG, EU,

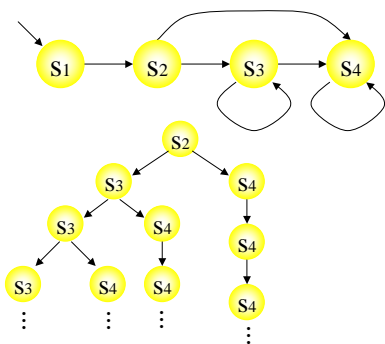
AX, AF, AG, AU

Ichiro Satoh

## 分岐時相論理

CTL式の真偽値

状態グラフ (state graph) 上の状態とそこから始まるパスを考える



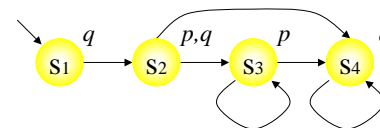
Ichiro Satoh

## 分岐時相論理の解釈

CTL式の真偽値

CTL式  $\phi$  が状態  $s$  で成立する (  $\phi$  が  $s$  で真 ):  $s \models \phi$

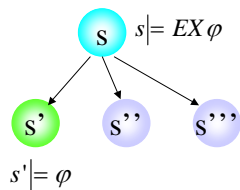
原子命題,  $\wedge$ ,  $\vee$ ,  $\neg$  (not),  $\rightarrow$ : その状態だけで真偽値が決まる



Ichiro Satoh

## 分岐時相論理の解釈

CTL式の真偽値  $s \models EX \phi \Leftrightarrow s$  のある次の状態  $s'$  で

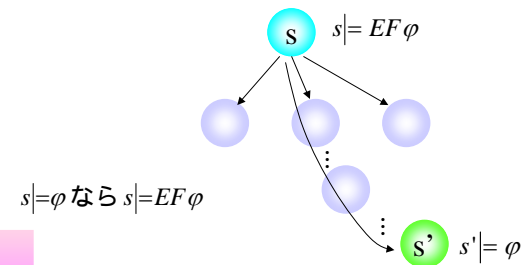


Ichiro Satoh

## 分岐時相論理の解釈

CTL式の真偽値

$s \models EF \phi \Leftrightarrow s$  から始まるあるパス中に  $s' \models \phi$  なる  $s'$  が存在



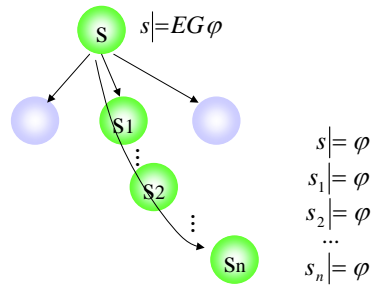
Ichiro Satoh



## 分岐時相論理の解釈

### CTL式の真偽値

$s \models EG\varphi$  から始まるあるパス中では、  
そのパス中のすべての状態  $s$  において  $s' \models \varphi$

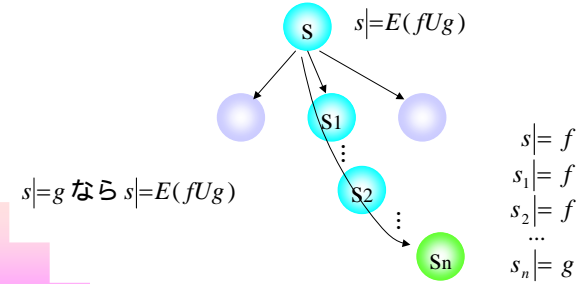


Ichiro Satoh

## 分岐時相論理の解釈

### CTL式の真偽値

$s \models E(fUg)$  から始まるあるパス中では、 $g$ が  
成り立つまで  $f$  が成り立ちつづける

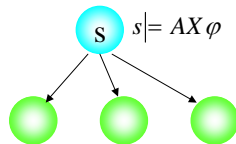


Ichiro Satoh

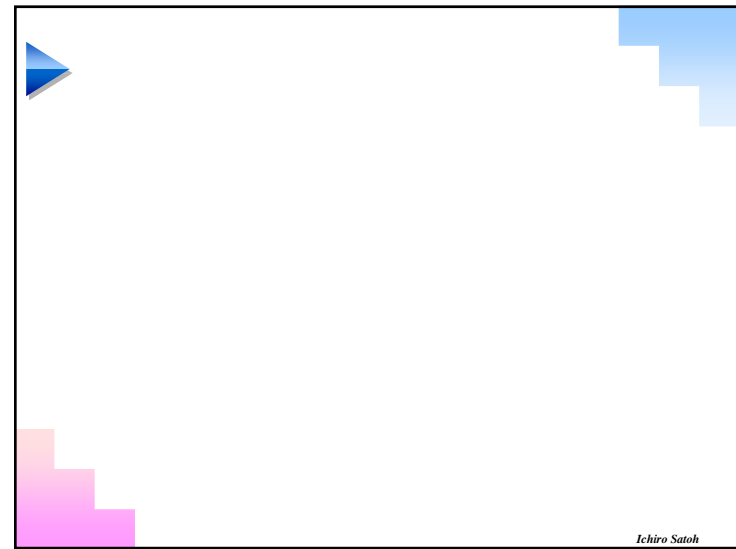
## 分岐時相論理の解釈

### CTL式の真偽値

$s \models AX\varphi$  のすべての次の状態  $s'$  で  $s' \models \varphi$



Ichiro Satoh



## ▶ 様相論理の応用

- 知識の表現と推論
- 自然言語理解, 自然言語処理
- プログラムの仕様記述・検証

Ichiro Satoh

## ▶ 様相論理式

命題変数 (propositional variable)

$P, Q, R, \dots$

論理結合子 (logical connective)

- $\neg$  (否定, negation)
- (連言, conjunction)
- (選言, disjunction)
- (含意, implication)
- (同値, equivalence)

様相演算子 (modal operator)

- (必然, necessity)
- (可能, possibility)

Ichiro Satoh

## ▶ 様相論理式の非形式的意味

命題変数

$P, Q, R, \dots$

, : 論理式

- $\neg$  ... 「でない」
- ... 「かつ」
- ... 「または」
- ... 「ならば」
- ... 「と は同値」
- ... 「は必然である」
- ... 「は可能である」

$\Rightarrow$   $\neg$

$\Rightarrow$   $\neg$

Ichiro Satoh

## ▶ 様相論理体系

次の公理と推論規則を含む公理系

公理

(PC) 命題論理のすべての恒真式

(K) ( ) ( )

K ... Kripke

Ichiro Satoh

## ▶ 様相論理体系

推論規則 (inference rule)  
(MP)

\_\_\_\_\_

(N) \_\_\_\_\_

MP ... modus ponens (分離規則)

N ... necessiation (必然化規則)

Ichiro Satoh

## ▶ 様相論理体系

公理

(D):

(T):

(B):  $\neg$   $\neg$

(4):

(5):  $\neg$   $\neg$

体系

K, KD, KT, KB, K4, K5, KDB, KD4, KD5, KTB, KT4, KT5,  
KB4, K45, KD45

Ichiro Satoh

## ▶ 復習: 代数的関係

集合  $A$  と集合  $B$  の直積 (direct product)

$$A \times B = \{ (x, y) \mid x \in A, y \in B \}$$

集合  $A$  から集合  $B$  への 2項関係

$$R \subseteq A \times B$$

要素  $a$  から要素  $b$  へ関係  $R$  がある

$$(a, b) \in R$$

$$a R b$$

集合  $A$  上の 2項関係  $R \subseteq A \times A (= A^2)$

Ichiro Satoh