時相論理とモデルチェッキング

国立情報学研究所

佐藤一郎
E-mail: ichiro@nii.ac.jp

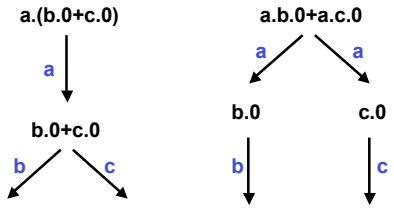
復習：代数的関係

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 $R \subseteq A \times A$ $(= A^2)$

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



プロセス論理

構文:
P ::= true | false | P ∧ Q | ¬P | <a> | [a]

非形式的意味

true	真を表す
false	偽を表す
P ∧ Q	PかつQ
¬P	Pの否定
<a>	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

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) |- <a>(<b>true ∧<c>true)
a.b.0+a.c.0 |- <a><b>true ∧ <a><c>true

Hoare論理の様相論理表現

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）
  μ計算（μ-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

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*

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

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.

様相論理式

命題変数

$P, Q, R, \ldots$

α, β: 論理式

- $\neg\alpha$ … 「αでない」
- $\alpha \wedge \beta$ … 「αかつβ」
- $\alpha \vee \beta$ … 「αまたはβ」
- $\alpha \Rightarrow \beta$ … 「αならばβ」
- $\alpha \Leftrightarrow \beta$ … 「αとβは同値」
- $\Box\alpha$ … 「αは必然である」
- $\Diamond\alpha$ … 「αは可能である」

$\Box\alpha = \neg\Diamond\neg\alpha$

$\Diamond\alpha = \neg\Box\neg\alpha$

様相論理式(例)

P … 「晴れている」

Q … 「風が吹いている」

$\Box\alpha$ … 「どこでもαである」

$\Box P \Rightarrow P$

「どこでも晴れているならば, 晴れている」

$\Box(P \wedge Q)$

「どこでも晴れていて風が吹いている」

様相論理式(例)

P … 「晴れている」

Q … 「風が吹いている」

$\Box\alpha$ … 「どこでもαである」

$\Box(P \wedge Q) \Rightarrow \Box P \wedge \Box Q$

「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」

様相論理式（例）

P　…「晴れている」
Q　…「風が吹いている」
$\Box\alpha$　…「どこでもαである」
$\Box(P \wedge Q) \Rightarrow \Box P \wedge \Box Q$
「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」
$\Box(P \vee Q) \Rightarrow \Box P \vee \Box Q$
「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」

様相論理式（例）

P　…「銀行は潰れる」
$\Box\alpha$　…「αは必然である」
$\Diamond\alpha$　…「αは可能である（あり得る）」

$\Box P \Rightarrow P$
「銀行は潰れることは必然であるならば、銀行は潰れる」
$\Box P \Rightarrow \Diamond P$
「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」

様相論理式（例）

P　…「学生は勉強する」
$\Box\alpha$　…「αでなければならない」
$\Diamond\alpha$　…「αでもよい」

$\Box P \Rightarrow P$
「学生は勉強しなければならないならば，
学生は勉強する」
$\Box P \Rightarrow \Diamond P$
「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」

様相論理式（例）

P　…「太陽は西から昇る」
$\Box\alpha$　…「αであることを信じている」

$\Box P \Rightarrow P$
「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」

様相論理式（例）

□α　…「αであることを知っている」

□α ⇒ □□α

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

¬□α ⇒ □¬□α

「αであることを知らないならば，
α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

□α　　◇α

現在の場所・時刻とは別の場所・時刻における
αの真理値を考慮する

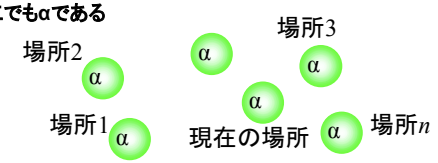
場所・時刻　…　可能世界（possible world）

可能世界ごとに論理式を解釈

Ichiro Satoh

可能世界意味論

□α　…　どこでもαである

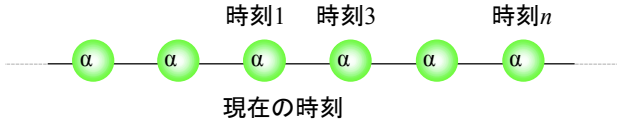


◇α　…　どこかではαである

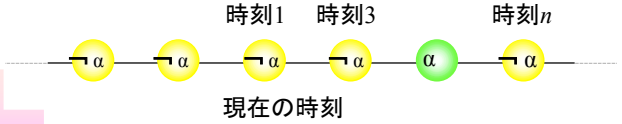
Ichiro Satoh

可能世界意味論

□α　…　いつでもαである



◇α　…　いつかはαである



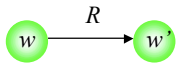
Ichiro Satoh

Kripke 構造（structure）

$M=\langle W, R, V\rangle$
$W\neq\varphi$
　$w\in W$ … 可能世界（possible world），世界
$R\subseteq W^2$
　W上の到達関係（accessibility relation）

Kripke 構造

$M=\langle W, R, V\rangle$
$W\neq\varphi$
　$w\in W$ … 世界（world）
$R\subseteq W^2$
　W上の到達関係（accessibility relation）
　wRw' … 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）



Kripke構造の解釈

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

命題変数 P に対して，
　$\models_{M, w} P$　iff　$V(P, w)=T$
$\models_{M, w}\neg\alpha$　iff　$\models_{M, w}\alpha$でない
$\models_{M, w}\alpha\wedge\beta$　iff　$\models_{M, w}\alpha$ かつ $\models_{M, w}\beta$
$\models_{M, w}\alpha\vee\beta$　iff　$\models_{M, w}\alpha$ または $\models_{M, w}\beta$

Kripke構造の解釈

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

$\models_{M, w}\alpha\Rightarrow\beta$
　iff　$\models_{M, w}\alpha$ならば $\models_{M, w}\beta$
$\models_{M, w}\alpha\Leftrightarrow\beta$
　iff　$\models_{M, w}\alpha$と $\models_{M, w}\beta$は必要十分

Kripke構造の解釈

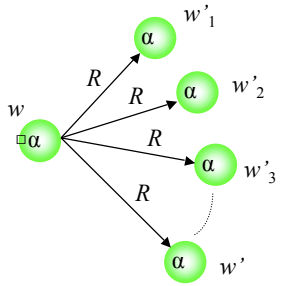
$M=\langle W, R, V\rangle$：Kripke 構造
論理式αは構造 M の世界 $w \in W$ において真
（$\models_{M, w} \alpha$）

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

w から到達可能なすべてのw' に対して，$\models_{M, w'} \alpha$

Kripke構造の解釈

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



Kripke構造の解釈

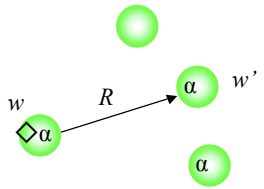
$M=\langle W, R, V\rangle$：Kripke 構造
論理式αは構造 M の世界 $w \in W$ において真
（$\models_{M, w} \alpha$）

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

w から到達可能なある w' に対して，$\models_{M, w'} \alpha$

Kripke構造の解釈

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



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：∨，∧，¬ (not), →

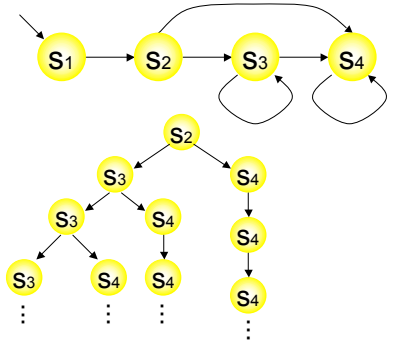
時相演算子：EX, EF, EG, EU,

AX, AF, AG, AU

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

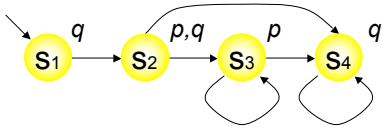


分岐時相論理の解釈

CTL式の真偽値

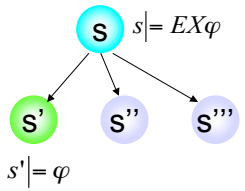
CTL式 が状態sで成立する(がsで真): $s \models \varphi$

原子命題, ∨，∧，¬ (not), → :その状態だ けで真偽値が決まる



分岐時相論理の解釈

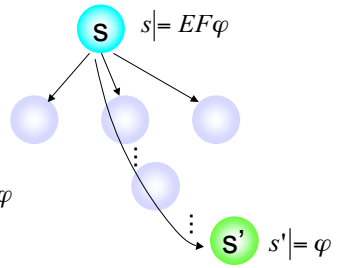
CTL式の真偽値 $s \models EX\varphi \Leftrightarrow s$ のある次の状態s'で



分岐時相論理の解釈

CTL式の真偽値

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

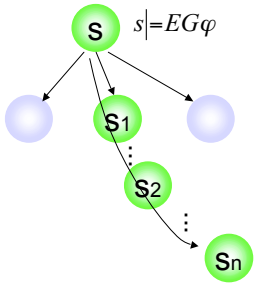


$s \models \varphi$ なら $s \models EF\varphi$

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 $s' \models \varphi$

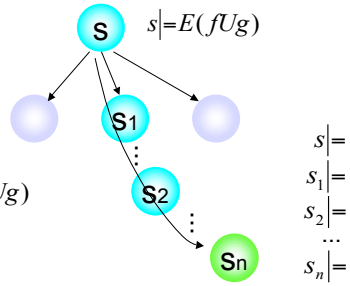


$s \models \varphi$
$s_1 \models \varphi$
$s_2 \models \varphi$
…
$s_n \models \varphi$

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



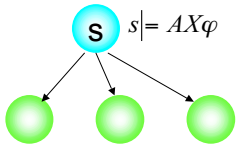
$s \models g$ なら $s \models E(fUg)$

$s \models f$
$s_1 \models f$
$s_2 \models f$
…
$s_n \models g$

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 $s' \models \varphi$



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

様相論理式

命題変数（propositional variable）

P, *Q*, *R*, …

論理結合子（logical connective）

¬ （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）

様相論理式の非形式的意味

命題変数

P, *Q*, *R*, …

α, β：論理式

¬α　…「αでない」
α∧β　…「αかつβ」
α∨β　…「αまたはβ」
α⇒β　…「αならばβ」
α⇔β　…「αとβは同値」
□α　…「αは必然である」
◇α　…「αは可能である」

□α＝¬◇¬α
◇α＝¬□¬α

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） $\Box(\alpha \Rightarrow \beta) \Rightarrow (\Box\alpha \Rightarrow \Box\beta)$

K … Kripke

Ichiro Satoh

様相論理体系

推論規則（inference rule）

（MP） α, $\alpha \Rightarrow \beta$ / β

（N） α / $\Box\alpha$

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）: $\Box\alpha \Rightarrow \Diamond\alpha$

（T）: $\Box\alpha \Rightarrow \alpha$

（B）: $\neg\alpha \Rightarrow \Box\neg\Box\alpha$

（4）: $\Box\alpha \Rightarrow \Box\Box\alpha$

（5）: $\neg\Box\alpha \Rightarrow \Box\neg\Box\alpha$

体系

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

Ichiro Satoh