Modal Mu Calculus

北陸先端科学技術大学院大学 先端科学技術研究科（青木研究室）

長谷川 央

2022-12-11

自己紹介

名前
長谷川 央（ハセガワ アキラ）

経歴

1997	愛知県豊田市で生まれる
2016	名古屋大学教育学部附属中・高卒
2016–2020	三重大学 総合情報処理センター主催 講習会「パソコン分解講習会」TA
2019	三重大学 総合情報処理センター主催 講習会「Linux 実践入門」講師
2020	北陸先端科学技術大学院大学 入学

はじめに

形式検証の 1 つとしてモデル検査がある

モデル検査を使うとプログラムやシステムの振る舞い（動作）を模したモデルに対して様々な性質が成り立つかを数学的に検証できる

例えば，交差点の信号のシステムをモデル化したとしたら，信号が同時に全て青になるタイミングが存在しないかを数学的に確かめられる

モデル検査の全体像と今回の内容

- Modeling
  検査対象システムの振る舞い（動作）を形式的に記述
- Specification
  検査対象システムの満たすべき性質を時相論理などで記述
- Verification
  Model Checker に上 2 行程の生成物を与えることで（半）自動的に行われる

今回は Specification で使用する時相論理を軽く一通り見た後，μ-Calculus の導入を行う

（本格的な内容は次回以降やれたらいいなと思っている）

Modeling: Kripke structure

モデル検査で使用される状態遷移系の代表例

Kripke structure を使って動作を記述する

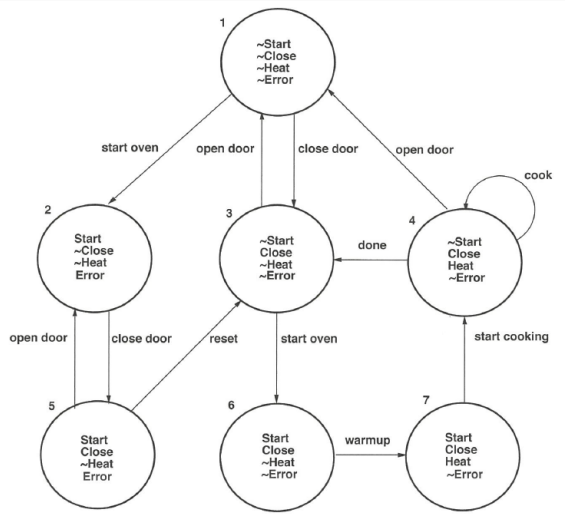
定義[1]
$M = (S, S_0, R, AP, L)$, where

- S is a set of states,
- $S_0 \subseteq S$ is the set of initial states,
- $R \subseteq S \times S$ is a *transition relation*,
- AP is the set of atomic propositions, and
- $L : S \to 2^{AP}$ is a function that labels each state with set of those atomic proposisions that are true in that state.

The transition relation R must be left total, that is, $\forall s \in S\ \exists s' \in S\ R(s, s')$.

[1] Clarke Jr, Edmund M., et al. *Model checking*. MIT press, 2018.

Kripke structure の使用例: 電子レンジ



Clarke Jr, Edmund M., et al. *Model checking*. MIT press, 2018, p. 57.

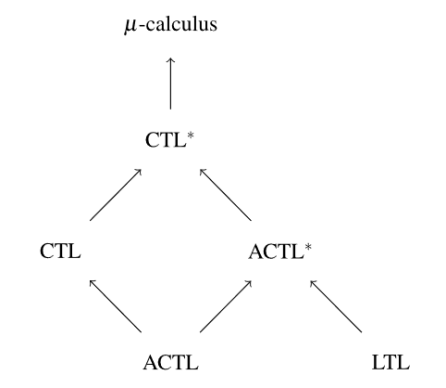
モデル検査のプロセス

- Modeling
  検査対象システムの振る舞い（動作）を形式的に記述
- Specification
  検査対象システムの満たすべき性質を時相論理などで記述
- Verification
  Model Checker に上 2 行程の生成物を与えることで（半）自動的に行われる

Specification: 時相論理

Specification（性質の記述）では時相論理を使用する

種類は様々だが主に LTL や CTL が使用される



Edmund M, Clarke Jr, et al. *Handbook of Model Checking*. Springer

Specification の例 電子レンジ

検査する仕様の例 (CTL)：$\mathbf{AG}(Start \rightarrow \mathbf{AF}\ Heat)$

意味：どのような場合でもスタートボタンが押されたら，そのうち加熱される

CTL*の構文

CTL*は state formulas の集合

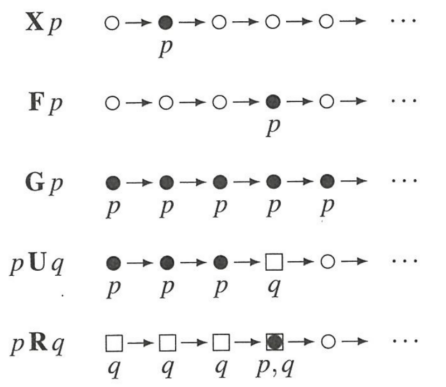
- state formulas
  $\varphi ::= p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mathbf{E}\psi \mid \mathbf{A}\psi$
- path formulas
  $\psi ::= \varphi \mid \neg\psi \mid \psi_1 \vee \psi_2 \mid \psi_1 \wedge \psi_2 \mid \mathbf{X}\psi \mid \mathbf{F}\psi \mid \mathbf{G}\psi \mid \psi_1 \mathbf{U} \psi_2 \mid \psi_1 \mathbf{R} \psi_2$

LTL と CTL の構文

LTL の構文
$\varphi ::= p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mathbf{X}\varphi \mid \mathbf{F}\varphi \mid \mathbf{G}\varphi \mid \varphi_1 \mathbf{U} \varphi_2$

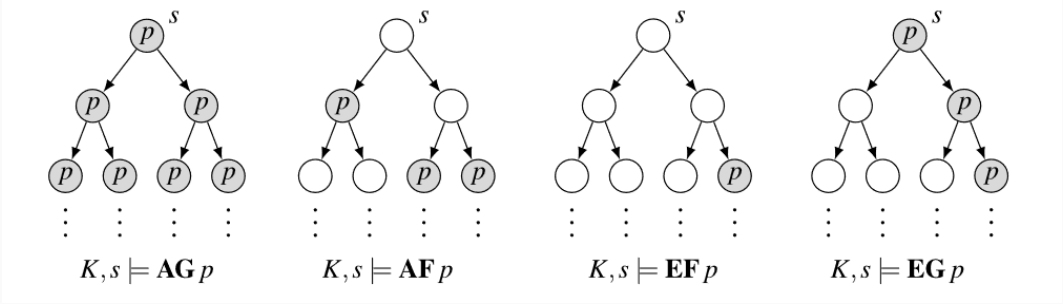
CTL の構文
$\varphi ::= p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mathbf{AX}\varphi \mid \mathbf{EX}\varphi \mid \mathbf{AF}\varphi \mid \mathbf{EF}\varphi \mid \mathbf{AG}\varphi \mid \mathbf{EG}\varphi \mid \mathbf{A}(\varphi_1 \mathbf{U} \varphi_2) \mid \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2)$

LTL のイメージ



Clarke Jr, Edmund M., et al. Model checking. MIT press, 2018, p. 39

CTL のイメージ


s
p
$K, s \models \mathbf{AG}\, p$
$K, s \models \mathbf{AF}\, p$
$K, s \models \mathbf{EF}\, p$
$K, s \models \mathbf{EG}\, p$

CTL*のよくある使用例

	Sub-logic	Formula	Intuition	Counterexample
1	CTL, LTL	$\mathbf{AG}p$	p is an invariant	finite path leading to $\neg p$
2	CTL, LTL	$\mathbf{AF}p$	p must eventually hold	infinite path (lasso-shaped) without p
3	CTL, (negated) LTL	$\mathbf{EF}\neg p$	$\neg p$ is reachable	substructure with all reachable states, all containing p
4	CTL, LTL	$\mathbf{AG}(p \vee \mathbf{X}p) = \mathbf{AG}(p \vee \mathbf{AX}p)$	p holds at least every other state	finite path leading to $\neg p$ twice in a row
5	CTL, LTL	$\mathbf{AGF}p = \mathbf{AGAF}p$	p holds infinitely often	infinite path (lasso) on which p occurs only finitely often
6	CTL, LTL	$\mathbf{AG}(p \rightarrow \mathbf{F}q) = \mathbf{AG}(p \rightarrow \mathbf{AF}q)$	every p is eventually followed by q	finite path leading to p, but no q now nor on the infinite path (lasso) afterwards
7	CTL, (boolean combination of) LTL	$(\mathbf{AGF}p) \wedge \mathbf{EF}\neg p$	both 3 and 5 hold	either counterexample for $\mathbf{AGF}p$ or for $\mathbf{EF}\neg p$
8	CTL only	$\mathbf{AGEX}p$	reachability of p in one step is an invariant	finite path leading to a state whose successors all have $\neg p$
9	CTL only	$\mathbf{AG}(p \vee \mathbf{AXAG}q \vee \mathbf{AXAG}\neg q)$	once p does not hold, either q or $\neg q$ become invariant in one step	finite path leading to $\neg p$ from which two finite extensions reach q and $\neg q$
10	LTL only	$\mathbf{AFG}p$	p must eventually become an invariant	infinite path (lasso) on which $\neg p$ occurs infinitely often
11	LTL only	$\mathbf{A}(\mathbf{GF}p \rightarrow \mathbf{GF}q)$	if p holds infinitely often, so does q	infinite path (lasso) on which p occurs infinitely often, but q does not

今回のテーマ：Modal μ-Calculus

μ-Calculus は CTL*よりも表現力が高い

一部の人が好んで使用している

(modified) Kripke structure 上で意味論が定義されている

「シンボル a によって遷移する path 上に p が真となる状態が無限回現れる」ことを

$$\nu Y.\mu X.(p \wedge \langle a \rangle Y) \vee \langle a \rangle X$$

と書く

A Modified Kripke structure

$M = (S, T, L)$, where

- a non empty set of states S;
- a set of transitions T, such that for each transition $a \in T$, $a \subseteq S \times S$; and
- a mapping $L : s \rightarrow 2^{AP}$ that gives the set of atomic propositions true in the state.

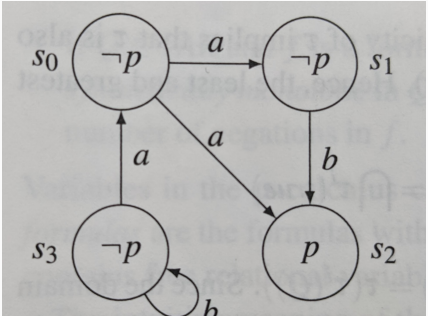


Figure 16.1
A modified Kripke structure.

μ-Calculus の Syntax

VAR を S の部分集合を表す変数の集合とする
また $a \in T,\ Q \in VAR$ とすると，μ-Calculus の Syntax は次のように書ける

$$\varphi = p \in AP \mid X \in VAR \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid [a]\varphi \mid \langle a \rangle \varphi \mid \nu Q.\varphi \mid \mu Q.\varphi$$

μ-Calculus の Semantics

M を Transition System，$e : VAR \to 2^S$ とし，式 f が真となる状態の集合を $[\![f]\!]_M e$ と書く

$true = S,\ false = \emptyset$ とし，$\tau(W) = [\![f]\!]_M e[Q \leftarrow W]$（$Q$ を W に置き換えるという意味）とする．このとき μ-Calculus の Semantics は次のように書ける

$$[\![p]\!]_M e = \{s \mid p \in L(s)\}$$

$$[\![Q]\!]_M e = e(Q)$$

$$[\![\neg f]\!]_M e = S \setminus [\![f]\!]_M e$$

$$[\![f \wedge g]\!]_M e = [\![f]\!]_M e \cap [\![g]\!]_M e$$

$$[\![f \vee g]\!]_M e = [\![f]\!]_M e \cup [\![g]\!]_M e$$

$$[\![\langle a \rangle f]\!]_M e = \{s \mid \exists t[s \xrightarrow{a} t \wedge t \in [\![f]\!]_M e]\}$$

$$[\![[a] f]\!]_M e = \{s \mid \forall t[s \xrightarrow{a} t \wedge t \in [\![f]\!]_M e]\}$$

$$[\![\mu Q.f]\!]_M e = \bigcap_i \tau^i(false) \text{ (the least fix point of the predicate transformer } \tau)$$

$$[\![\nu Q.f]\!]_M e = \bigcup_i \tau^i(true) \text{ (the greatest fix point of the predicate transformer } \tau)$$

μ-Calculus の μ と ν の例 (1/3)

以下の遷移系の上で $[\![\nu Q_1.(p \vee \langle b \rangle Q_1)]\!]_M e$ と $[\![\mu Q_2.(p \vee \langle b \rangle Q_2)]\!]_M e$ を考える

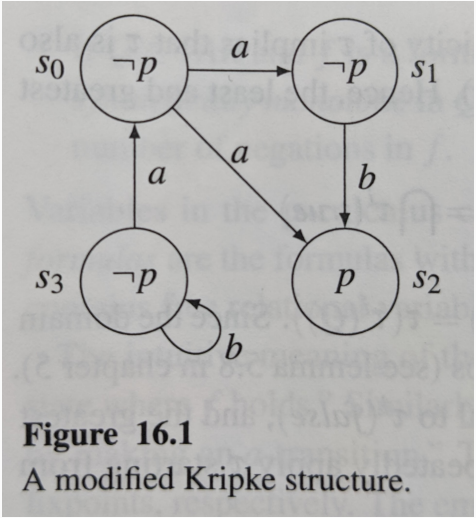


Figure 16.1
A modified Kripke structure.

μ-Calculus の μ と ν の例 (2/3)

$[\![\nu Q_1.(p \vee \langle b \rangle Q_1)]\!]_M e$ を考える

定義より $\tau(W) = [\![p \vee \langle b \rangle Q_1]\!]_M e[Q_1 \leftarrow W]$

$$
\begin{aligned}
\tau^1(true) &= [\![p \vee \langle b \rangle Q_1]\!]_M e[Q_1 \leftarrow true] \\
&= [\![p]\!]_M e[Q_1 \leftarrow true] \cup [\![\langle b \rangle Q_1]\!] e[Q_1 \leftarrow true] \\
&= \{s_2\} \cup \{s \mid \exists t[s \xrightarrow{b} t \wedge t \in [\![Q_1]\!]_M e[Q_1 \leftarrow true]]\} \\
&= \{s_2\} \cup \{s \mid \exists t[s \xrightarrow{b} t \wedge t \in true]\} \\
&= \{s_2\} \cup \{s_1, s_3\} \\
&= \{s1, s_2, s_3\} \\
\tau^2(true) &= \tau(\tau(true)) = \tau(\{s_1, s_2, s_3\}) = \{s_2\} \cup \{s_1, s_2, s_3\} = \{s_1, s_2, s_3\}
\end{aligned}
$$

よって，$[\![\nu Q_1.(p \vee \langle b \rangle Q_1)]\!]_M e = \{s_1, s_2, s_3\}$

μ-Calculus の μ と ν の例 (3/3)

$[\![\mu Q_2.(p \vee \langle b \rangle Q_2)]\!]_M e$ を考える
(there is sequence of b-transitions leading to a state where p holds)
$\tau(W)$ の定義は ν のときと同じ; $\tau(W) = [\![p \vee \langle b \rangle Q_2]\!]_M e[Q_2 \leftarrow W]$

$$\begin{aligned}\tau^1(false) &= [\![p \vee \langle b \rangle Q_2]\!]_M e[Q_2 \leftarrow false] \\ &= [\![p]\!]_M e[Q_2 \leftarrow false] \cup [\![\langle b \rangle Q_2]\!] e[Q_2 \leftarrow false] \\ &= \{s_2\} \cup false = \{s_2\}\end{aligned}$$

$$\begin{aligned}\tau^2(false) &= \tau(\{s_2\}) \\ &= \{s_2\} \cup [\![\langle b \rangle Q_2]\!]_M e[Q_2 \leftarrow \{s_2\}] \\ &= \{s_2\} \cup \{s_1\} = \{s_1, s_2\}\end{aligned}$$

$$\begin{aligned}\tau^3(false) &= \tau(\{s_1, s_2\}) \\ &= \{s_2\} \cup [\![\langle b \rangle]\!]_M e[Q_2 \leftarrow \{s_1, s_2\}] \\ &= \{s_2\} \cup \{s \mid \exists t[s \xrightarrow{b} t \wedge t \in \{s_1, s_2\}\} \\ &= \{s_2\} \cup \{s_1\} = \{s_1, s_2\}\end{aligned}$$

よって，$[\![\mu Q_2.(p \vee \langle b \rangle Q_2)]\!]_M e = \{s_1, s_2\}$

まとめ

- モデル検査で使用される様相論理には様々な種類があるがそれぞれに利点・欠点がある
- モデル検査ツールで多く使われている様相論理は CTL, LTL である
- 研究などで μ-calculus を使用している人もいる
- μ-Calculus は不動点計算を使って意味論を定義している