個別の事例を対象としたモデル検査

M2012MM023　長谷康宏
指導教員：佐々木克巳

1　はじめに

本研究では，モデル検査に必要な準備をした上で，自分で選んだ製品である，電動ポットと自動車のルームランプに対するシステムに対して，モデル検査を行った．モデル検査に必要な準備には，[1],[2] を用いた．本稿では，自動車のルームランプシステムのモデル検査の例を挙げる．2 節でモデル検査に必要な準備，3 節で **CTL** のモデル検査の手法，4 節で自動車のルームランプシステムの例を説明する．

2　モデル検査に必要な準備

ここでは，様相論理 **CTL** について説明する．

2.1　CTL の論理式

この節では，様相論理 **CTL** の論理式について説明する．集合 **AP** を 1 つ定めておく．その元 $p \in \mathbf{AP}$ を原子論理式と呼ぶ．また，用いる論理記号は、$\wedge, \vee, \supset, \neg$ とパス量化子 **E**, **A** と時相演算子 **X**, **F**, **G**, **U**, **R** である．パス量化子と時相演算子をあわせて様相演算子という．様相演算子で，自動車のルームランプの例で用いるもののみを，直観的な意味とともに以下にまとめておく．

パス量化子 $\mathbf{A}\psi$：すべてのパスにおいて（$for\ All$）
時相演算子 $\mathbf{F}\psi$：ある未来（$in\ the\ Future$ ）
時相演算子 $\mathbf{G}\psi$：これからずっと（$Globally$）

CTL の状態論理式は，次のように定義する．以下，とくに必要のない限り， **CTL** の状態論理式を単に状態論理式という．

定義 2.1（**CTL** の状態論理式）
(1) $p \in \mathbf{AP} \Rightarrow p$ は状態論理式
(2) ϕ, ψ は状態論理式 $\Rightarrow \neg\phi, \phi \wedge \psi, \phi \vee \psi, \phi \to \psi$ は状態論理式
(3) ϕ, ψ は状態論理式 $\Rightarrow \mathbf{AX}\phi$, $\mathbf{EX}\phi$, $\mathbf{AF}\phi$, $\mathbf{EF}\phi$, $\mathbf{AG}\phi$, $\mathbf{EG}\phi$, $\mathbf{A}(\phi\mathbf{U}\psi)$, $\mathbf{E}(\psi\mathbf{U}\phi)$, $\mathbf{A}(\phi\mathbf{R}\psi)$, $\mathbf{E}(\phi\mathbf{R}\psi)$ は状態論理式

2.2　CTL の意味論

この節では，様相論理 **CTL** の意味論について説明する．クリプキフレームとそのフレームにおける **CTL** の論理式の真偽を定めたクリプキモデルを定義する．

定義 2.2 空でない集合 S と S 上の二項関係 R の組 (S, R) をクリプキフレームという．S の各元を可能世界または状態と呼び，R を到達可能関係と呼ぶ．

定義 2.3 3 つ組 $M = (S, R, V)$ は，次の条件を満たすとき，クリプキモデルという．また，V を付値関数と呼ぶ．
(1) (S, R) はクリプキフレーム
(2) $V : S \times \mathbf{AP} \to \{\top, \bot\}$

定義 2.4 クリプキフレーム $F = (S, R)$ における（無限）パスとは状態がなす無限の列 $\pi = s_0, s_1, \cdots$ であって $i = 0, 1, \cdots$ に対して，$s_i R s_{i+1}$ となるもののことをいう．パス $\pi = s_0, s_1, \cdots$ に対して，その s_i から始まる末尾を π^i とかくことにする．すなわち，π^i は無限パスで $\pi^i = s_i, s_{i+1}, \cdots$ である．また，無限パスの最初の有限部分を有限パスということにする．

定義 2.5 クリプキモデル $M = (S, R, V)$ が定まっているとき，各状態 $s \in S$ と各状態論理式 ϕ との関係 $M, s \models \phi$ を論理式の構成に関して帰納的に定める．詳細は省略する．

定義 2.6 二つの状態論理式を ϕ と ψ とする．すべてのクリプキモデル M とそのすべての状態 s に対して $M, s \models \phi \iff M, s \models \psi$ が成り立つとき，ϕ と ψ は論理的に同値であるといい，$\phi \cong \psi$ と表す．

補題 2.1　**CTL** の 10 種類の様相演算子は，すべて **EX**, **EG**, **EU** の 3 種類を用いてかける．ここでは，**EF**, **AG**, **AF** についてのみ示しておく．
(1) $\mathbf{EF}\phi \cong \mathbf{E}(\mathsf{True}\mathbf{U}\phi)$
(2) $\mathbf{AG}\phi \cong \neg\mathbf{EF}\neg\phi$
(3) $\mathbf{AF}\phi \cong \neg\mathbf{EG}\neg\phi$
ただし，True は，勝手な $p \in \mathbf{AP}$ を決めた時の $p \vee \neg p$ の略記である．

3　CTL のモデル検査

ここでは，[1] にしたがって，CTL のモデル検査の手法について説明する．基本的なモデル検査の手法は，以下に示すとおりである．

モデル検査の手法
(I) 検証したいシステムをクリプキモデル M として表す．
(II) 検証したい性質を状態論理式 ϕ として表す．
(III) モデル検査問題を解いて，状態の集合 $S(\phi) = \{s \mid M, s \models \phi\}$ を求める．公平性制約を加える場合もある．この集合の中に初期状態（システムの実行開始時の状態）が入っていれば，検証したい性質の正しさが保証される．

上の (I),(II),(III) を，以下の 3.1 節,3.2 節,3.3 節で説明する．ただし，(III) の公平性制約については，3.4 節で説

明する．

3.1 システムをクリプキモデル M で表す

この節では，検証したいシステムをクリプキモデル M として表現することを，例を挙げて説明する．

図 1 は，電子レンジのシステムを状態遷移図で表現したものである．この状態遷移図における 7 つの四角がシステムの状態を表し，矢印がシステムの計算過程を表す．各状態にかかれている $Start$,$Close$,$Heat$,$Error$ 等の意味は以下のとおりである．

- Start : 電子レンジのスタートボタンが押されている
- Close : 電子レンジのドアが閉まっている
- Heat : 調理するものが温まっている
- Error : エラーになっている
- ∼ : でない

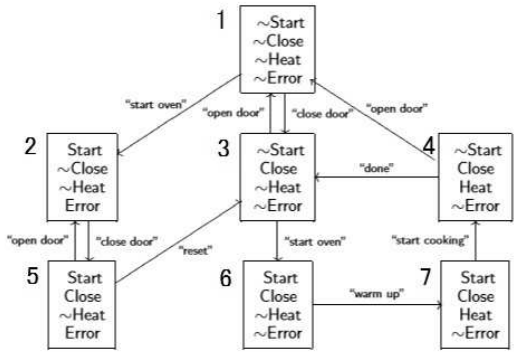

図 1 電子レンジの状態遷移図（出典 [1]）

これらの構成要素をクリプキモデルでは，

1. システムの状態をクリプキモデルの状態 $s \in S$
2. システムの計算過程をクリプキモデルの到達可能関係 R
3. $Start, Close, Heat, Error$ を $\mathbf{AP}$ の要素
4. 「$Start, \cdots$ が四角 s の中にかかれていること」を $V(s, Start) = \top, \cdots$
5. 「$\sim Start, \cdots$ が四角 s の中にかかれていること」を $V(s, Start) = \bot, \cdots$

と解釈する．この解釈によって，検証したいシステムをクリプキモデルとして表現できる．

3.2 検証したい性質を状態論理式 ϕ として表す

この節では，図 1 のシステムにおける検証したい性質の例を挙げて，それを状態論理式で表現する．

検証したい性質は，

- 「電子レンジのスタートボタンを押すと必ず中の物が温まる」

という性質である．これを

- 「これからずっと「電子レンジのスタートボタンを押せば，いつか必ず中の物が温まる」」

と解釈し，クリプキモデルのパスを用いて表現すると，

- 「すべてのパスにおいて,「電子レンジのスタートボタンを押せば，すべてのパスにおいて，ある未来必ず中の物が温まる」」

である．よって，これを状態論理式で表すと，

$$\mathbf{AG}(Start \rightarrow \mathbf{AF}Heat)$$

である．

3.3 $S(\phi)$ を求める

この節では，検証したしたい論理式 ϕ に対して， $S(\phi)$ を計算するアルゴリズムについて説明する．補題 2.1 より，チェックしたい $\mathbf{CTL}$ の状態論理式 ϕ は

$$p(p \in \mathbf{AP}),\ \neg\phi,\ \phi \vee \psi,\ \mathbf{EX}\phi,\ \mathbf{E}(\phi \mathbf{U} \psi),\ \mathbf{EG}\phi$$

の形に制限されているとしてよい．

$S(\mathbf{EG}\phi)$ を求めるのには，次の準備が必要である．

定義 3.1 クリプキフレーム $F = (S, R)$ の強連結成分とは $C = (S', R')$ で次の条件を満たすもののことをいう．

(1) C は F の部分フレームである．すなわち，$S' \subseteq S$,$R' \subseteq R \cap (S' \times S')$ である．

(2) C は強連結である．すなわち，任意の状態 $s, s' \in S'$ に対して，s から s' への C の中での有限パスが存在する．

(3) C は極大である．すなわち，$C \subseteq C'$ でかつ C' が強連結ならば，$C' = C$ である．

さらに，この強連結成分 C が非自明とは次のようでないこという．

(4) S が 1 点集合，かつ，$R = \emptyset$ である．

この節の冒頭で示した 6 つの形の状態論理式に対して，次の定理が成り立つので，$S(\phi)$ を，論理式 ϕ の構成にしたがって計算することができる．この定理の (2) については，4 節での計算をしやすくするために加えている．

定理 3.1 $M = (S, R, V)$ をクリプキモデルとする．

(1) $\phi = p \in \mathbf{AP}$ のとき，$S(p) = \{s \in S \mid V(s, p) = T\}$

(2) $\phi = \psi \wedge \chi$ のとき，$S(\psi \wedge \chi) = S(\psi) \cap S(\chi)$

(3) $\phi = \psi \vee \chi$ のとき，$S(\psi \vee \chi) = S(\psi) \cup S(\chi)$

(4) $\phi = \neg\psi$ のとき，$S(\neg\psi) = S \backslash S(\psi)$

(5) $\phi = \mathbf{EX}\psi$ のとき，$S(\mathbf{EX}\psi) = \{s \in S \mid$ ある $s' \in S$ が存在して，$(s, s') \in R$ かつ $s' \in S(\psi)\}$

(6) $\phi = \mathbf{E}(\psi \mathbf{U} \chi)$ のとき，状態 $s \in S(\chi)$ のそれぞれからスタートして，R をさかのぼっていく．さかのぼっていくうち ψ が成り立っているうちは，その状態を $S(\mathbf{E}(\psi \mathbf{U} \chi))$ に加えていく．

(7) $\phi = \mathbf{EG}\psi$ のとき，$S(\mathbf{EG}\psi)$ は，次の 2 条件を満たす状態 $s \in S$ を全部集めた集合

(a) $s \in S(\psi)$

(b) $(S(\psi), R(\psi))$ の中に非自明な強連結成分 C があって，かつ s から C の中の状態 t に至る

$(S(\psi), R(\psi))$ の中の有限パスが存在する．

ただし，

$R(\phi) = R \cap (S(\phi) \times S(\phi))$

である．

3.4 公平性制約

この節では，公平性制約について述べる．3.2 節の状態論理式を ψ としたとき，3.3 節の方法で，$S(\psi)$ を計算すると，$S(\psi) = \{\ \}$ になる．これはモデル検査が失敗したことを表す．その理由は，「ドアをずっと開けたり閉めたり」というパスがあるためである．そこで，このようなパスは排除したい．このようなパスは，公平性制約をうまく定めることによって排除できることがある．

定義 3.2

(1) $M = (S, R, V)$ をクリプキモデルとするとき，集合 $\{S' \mid S' \subseteq S\}$ を M 上の公平性制約という．

(2) M のパス $\pi = s_0, s_1, \cdots$ に対して，状態の集合 $inf(\pi)$ を $inf(\pi) = \{\ s \in S \mid$ 無限にたくさんの $i \geq 0$ に対して，$s = s_i\ \}$ と定める．

(3) M のパス $\pi = s_0, s_1, \cdots$ が公平性制約 **FC** について公平であるとは次が成り立つことをいう．

すべての $P \in \mathbf{FC}$ に対して，$inf(\pi) \cap P \neq \emptyset$

集合

$$\mathbf{FC} = \{\{s \mid s \models Start \wedge Close \wedge \neg Error\}\}$$

は，3.1 節の電子レンジシステムにおける，公平性制約の例である．この制約で「ドアの開け閉め」のパスを排除できる．その理由をおおまかに述べておく．まず，図 3.1 より，$\mathbf{FC} = \{\{6, 7\}\}$ である．よって，「ドアの開け閉め」によるパスである

$$1, 3, 1, 3, \cdots \text{ や } 2, 5, 2, 5, \cdots$$

は **FC** について公平でないとわかる．すなわち，公平なパスのみを考えることにより，これらのパスを排除できることになる．

定義 3.3 クリプキモデル $M = (S, R, V)$ と公平性制約 **FC** を定めたとき，**CTL** の状態・パス論理式 ϕ が M と **FC** のもとで真であるという関係 $M, s \models_{\mathbf{FC}} \phi$ を論理式の構成に関して帰納的に定める．詳細は省略する．

$S_{\mathbf{FC}}(\phi) = \{s \in S \mid M, s \models_{\mathbf{FC}} \phi\}$ とする．以下，3.3 節と同様に $S_{\mathbf{FC}}(\phi)$ を求める方法を示す定理を述べる．

定義 3.4 $M = (S, R, V)$ をクリプキモデル，**FC** をその上の公平性制約とする．クリプキフレーム (S, R) の強連結成分 C が公平であるとは，各 $P_i \in \mathbf{FC}$ について $C \cap P_i \neq \emptyset$ が成り立つことをいう．

定理 3.2 $M = (S, R, V)$ をクリプキモデル，**FC** をその上の公平性制約とする．

(1) $M, s \models_{\mathbf{FC}} \mathbf{Fair} \Leftrightarrow s$ から始まる公平なパスが存在する

(2) $(p \in \mathbf{AP})$ に対して，$S_{\mathbf{FC}}(p) = S(p \wedge \mathbf{Fair})$

(3) $\phi = \psi \wedge \chi$ のとき，$S_{\mathbf{FC}}(\psi \wedge \chi) = S_{\mathbf{FC}}(\psi) \cap S_{\mathbf{FC}}(\chi)$

(4) $\phi = \psi \vee \chi$ のとき，$S_{\mathbf{FC}}(\psi \vee \chi) = S_{\mathbf{FC}}(\psi) \cup S_{\mathbf{FC}}(\chi)$

(5) $\phi = \neg\psi$ のとき，$S_{\mathbf{FC}}(\neg\psi) = S \backslash S_{\mathbf{FC}}(\psi)$

(6) $\phi = \mathbf{EX}\psi$ のとき，$S_{\mathbf{FC}}(\mathbf{EX}\psi) = \{s \in S \mid$ ある $s' \in S$ が存在して，$(s, s') \in R$ かつ $s' \in S_{\mathbf{FC}}(\psi)\}$

(7) $\phi = \mathbf{E}(\psi \mathbf{U} \chi)$ のとき，状態 $(s \in S_{\mathbf{FC}}\chi \wedge \mathbf{Fair})$ それぞれからスタートして，R をさかのぼっていく．さかのぼっていくうち ψ が成り立っているうちは，その状態を $S_{\mathbf{FC}}(\mathbf{E}(\psi \mathbf{U} \chi))$ に加えていく．

(8) $\phi = \mathbf{EG}\psi$ のとき，$S_{\mathbf{FC}}(\mathbf{EG}\psi)$ は，次の 2 条件を満たす状態 $s \in S$ を全部集めた集合

(a) $s \in S_{\mathbf{FC}}(\psi)$

(b) $(S_{\mathbf{FC}}(\psi), R_{\mathbf{FC}}(\psi))$ の中に非自明で公平な強連結成分 C があって，かつ s から C の中の状態 t に至る $(S_{\mathbf{FC}}(\psi), R_{\mathbf{FC}}(\psi))$ の中の有限パスが存在する．

ただし，

$R_{\mathbf{FC}}(\phi) = R_{\mathbf{FC}} \cap (S_{\mathbf{FC}}(\phi) \times S_{\mathbf{FC}}(\phi))$

$\mathbf{Fair} = \mathbf{EG}\mathsf{True}$

である．

4 自動車のルームランプシステムの例

ここでは，自動車のルームランプシステムを例に挙げ，前章の冒頭で示した手順で，モデル検査を行う．

(I) 図 2 は，自動車のルームランプシステムの状態遷移図である．システムの状態は，7 つの文 *on*,*switch*, *brightlight*, *key_open*, *door_open*, *darklight*, *error* で決定される．各文の意味を示す．

- *on*：ルームランプのスイッチが押されている
- *switch*：ルームランプが点滅している
- *brightlight*：ルームランプが全点灯している
- *darklight*：ルームランプが半点灯している
- *key_open*：車の鍵が開いている
- *door_open*：車のドアが開いている
- *error*：エラーになっている

7 つの要因があるので，$2^7 = 128$ 通りの状態が考えられる．図 2 では，128 通りのうち 9 通りを対象としたシステムを表している．以下，7 つの文を **AP** の要素とし，3.1 節と同様に，図 2 の状態遷移図をクリプキモデルとして考える．

(II) 検証したい文は，「解錠したら，明るいルームランプまたは暗いルームランプが必ず点灯する」という文である．これを論理式で表現すると，

$$\mathbf{AG}(key\_open \rightarrow \mathbf{AF}(darklight \vee brightlight))$$

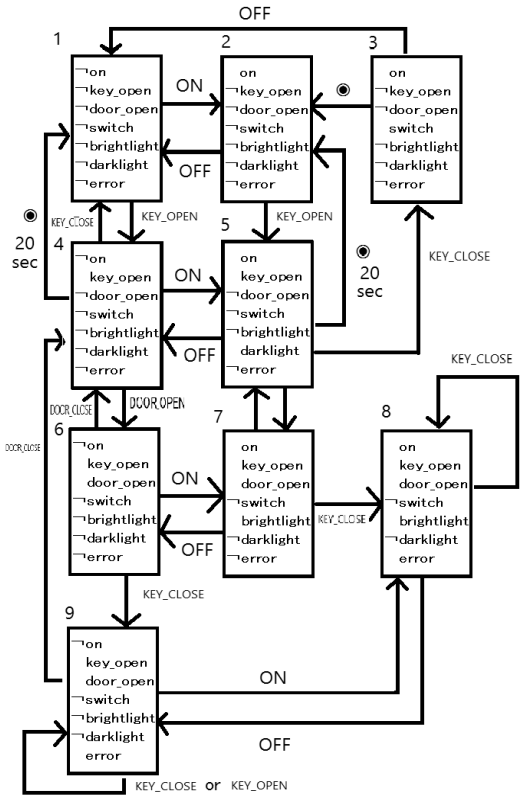

図 2 ルームランプシステムの状態遷移図

である．この論理式を ϕ とおく．

(III) まず，補題 2.1 より ϕ の $\mathbf{AG}, \mathbf{AF}$ を $\mathbf{EU}, \mathbf{EG}$ で表現した状態論理式 ψ を求めると以下のようになる．
$\neg\mathbf{E}(\mathsf{True}\mathbf{U}(key\_open \wedge (\mathbf{EG}\neg(darklight \vee brightlight))))$
次に，$S(\psi)$ を求める．ここでは，公平性制約は考えない．

(1) $S(darklight) = \{5\}$ $(\because$ 図 2$)$

(2) $S(brightlight) = \{7, 8\}$ $(\because$ 図 2$)$

(3) $S(darklight \vee brightlight) = \{5, 7, 8\}$
$(\because (1), (2),$ 定理 3.1(3)$)$

(4) $S(\neg(darklight \vee brightlight)) = \{1, 2, 3, 4, 6, 9\}$
$(\because (3),$ 定理 3.1(4)$)$

(5) $\{1, 2, 4, 6, 9\}$ は，$S(\neg(darklight \vee brightlight))$ の強連結成分である． $(\because (4),$ 定義 3.1$)$

(6) $S(\mathbf{EG}\neg(darklight \vee brightlight))$
$= \{1, 2, 3, 4, 6, 9\}$ $(\because (4), (5),$ 定理 3.1(7)$)$

(7) $S(key\_open) = \{4, 5, 6, 7, 8, 9\}$ $(\because$ 図 2$)$

(8) $S(key\_open \wedge \mathbf{EG}\neg(darklight \vee brightlight))$
$= \{4, 6, 9\}$ $(\because (6), (7),$ 定理 3.1(2)$)$

(9) $S(\mathbf{E}(\mathsf{True}\mathbf{U}(key\_open \wedge \mathbf{EG}\neg(darklight \vee brightlight)))) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
$(\because (8),$ 定理 3.1(6)$)$

(10) $S(\psi) = \{\quad\}$ $(\because (9),$ 定理 3.1(4)$)$

$S(\psi)$ が空集合になったので，モデル検査はうまくいかなかった．

公平性制約がある場合を考える．公平性制約を「ルームランプのスイッチが常にオンでかつ，車の鍵が開いている」つまり，$\mathbf{FC} = \{\{s \mid s \models on \wedge key\_open\}\} = \{\{5, 7, 8\}\}$ とする．この $\mathbf{FC}$ のもとで $S_{\mathbf{FC}}(\psi)$ を求める．

(1) 1 からはじまる公平なパス $1, 2, 5, 7, 5, 7, \cdots$ がある．
$(\because$ 図 2, 定義 3.3$)$

(2) 各状態からはじまる公平なパスがある．
$(\because$ 図 2, 定義 3.3$)$

(3) $S_{\mathbf{FC}}(\mathbf{Fair}) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
$(\because (1), (2),$ 定理 3.2(1)$)$

(4) $S_{\mathbf{FC}}(darklight) = \{5\}$ $(\because (3),$ 定理 3.2(2)$)$

(5) $S_{\mathbf{FC}}(brightlight) = \{7, 8\}$
$(\because (3),$ 定理 3.2(2)$)$

(6) $S_{\mathbf{FC}}(darklight \vee brightlight) = \{5, 7, 8\}$
$(\because (4), (5),$ 定理 3.2(4)$)$

(7) $S_{\mathbf{FC}}(\neg(darklight \vee brightlight))$
$= \{1, 2, 3, 4, 6, 9\}$ $(\because (6),$ 定理 3.2(5)$)$

(8) $S_{\mathbf{FC}}(\neg(darklight \vee brightlight))$ の任意の部分集合 C に対して，$C \cap \{5, 7, 8\} = \emptyset (\because (7))$

(9) $S_{\mathbf{FC}}(\neg(darklight \vee brightlight))$ の公平な強連結成分は存在しない． $(\because (8),$ 定義 3.4$)$

(10) $S_{\mathbf{FC}}(\mathbf{EG}\neg(darklight \vee brightlight)) = \{\quad\}$
$(\because (6), (9),$ 定理 3.2(8)$)$

(11) $S_{\mathbf{FC}}(key\_open) = \{4, 5, 6, 7, 8, 9\}$
$(\because (3),$ 図 2$)$

(12) $S_{\mathbf{FC}}(key\_open \wedge \mathbf{EG}\neg(darklight \vee brightlight))$
$= \{\quad\}$ $(\because (10), (11),$ 定理 3.2(3)$)$

(13) $S_{\mathbf{FC}}(\mathbf{E}(\mathsf{True}\mathbf{U}(key\_open \wedge (\mathbf{EG}\neg darklight \vee brightlight)))) = \{\quad\}$ $(\because (12),$ 定理 3.2(7)$)$

(14) $S_{\mathbf{FC}}(\psi) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
$(\because (13),$ 定理 3.2(5)$)$

$S_{\mathbf{FC}}(\phi) = S_{\mathbf{FC}}(\psi) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ になったので，公平性制約 $\mathbf{FC}$ のもとで，モデル検査が成功した．

5 おわりに

モデル検査の研究では，モデル検査を行うまでの準備が大変あると感じた．特に状態遷移図の作成で製品の状態を網羅できているかというところで苦労した．

今後，モデル検査の準備段階をスムーズに行えば，確実で，迅速な製品の品質保証ができると思った．

参考文献

[1] 蓮尾一郎 :『モデル検査入門』. http: //www.kurims.kyoto-u.ac.jp/ cs/lecture2009 /lecture09ModelChecking.pdf

[2] Edmund M. Clarke, Jr., Orna Grumberg, and Doron A.Peled : Model Checking. The MIT Press, London, 1999.