数理解析研究所講究録
第1744巻 2011年 15-24

2010年度冬のLAシンポジウム[3]

動的リアルタイムハイブリッドCEGARによる動的再構成可能組込みシステムの設計検証

酒井 誠* 山根 智†

1 はじめに

近年，組込みシステムの多機能化により，設計が複雑化している．また，ネットワークや動的再構成可能プロセッサ等は動作中に構成が変化し，さらにハイブリッド性を持つため，シミュレーションで安全性を保証することが困難となってきている．この安全性を保証するためにはモデル検査が有効であるが，モデル検査では，網羅的な探索を行うため状態空間が大きくなり，メモリに載り切らないという状態爆発が問題となっている．この問題の解決法として，E.M.Clarkeらの抽象化精錬検証手法（CEGAR）[2]がある．また，ハイブリッドオートマトンに対する検証手法[1]もある．

そこで本研究では，動的に構成が変化するモデルを記述することができる動的線形ハイブリッドオートマトンを提案し，また，その検証手法として，CEGARを拡張した動的線形ハイブリッドCEGARを提案する．

2 動的線形ハイブリッドオートマトン

ここでは，本稿で用いる仕様記述言語である動的ハイブリッドオートマトンとその動作について定義する．表記のルールとして，$=$を「定義する（$\stackrel{\text{def}}{=}$）」，$==$を「等しい」，$:=$を「代入」の意味で用いる．

*金沢大学大学院自然科学研究科
†金沢大学

2.1 構文

変数評価と制約条件について定義する．

定義 1 (クロック評価)
Xを，非負の実数値を持つクロック変数の有限集合とする．このとき，$\nu : X \to \mathbb{R}_{\geq 0}$を，任意のクロック変数に非負の実数を割り当てる関数と定義し，これをクロック評価と呼ぶ．また，$\nu[X' := 0]$によって，集合$X' \subseteq X$の要素のクロック変数に対して0を，それ以外についてはνと同じ評価値を割り当てることを表す．さらに，Xのクロック評価の集合を$\mathcal{V}_X$で表す． □

定義 2 (サイクル評価)
Cを，非負の実数値を持つサイクル変数の有限集合とする．このとき，$\mu : C \to \mathbb{R}_{\geq 0}$を，任意のサイクル変数に非負の実数を割り当てる関数と定義し，これをサイクル評価と呼ぶ．Cのサイクル評価の集合を$\mathcal{U}_C$で表す． □

定義 3 (制約条件)
クロック，サイクル変数の制約条件を以下のように定義する．

$$\phi ::= x_1 \sim d \mid x_1 - x_2 \sim d \mid c \sim d \mid \phi_1 \wedge \phi_2 \mid true$$

ただし，$x_1; x_2 \in X$, $c \in C$, $d \in \mathbb{Z}$, $\sim \in \{<, \leq, >, \geq, ==\}$である．全ての制約条件の集合を$\Phi(X \cup C)$とする． □

定義 4 (変数の傾き)
各ロケーションへ割り付ける変数の傾きを以下のように定義する．

$$f_x ::= \dot{x} = m$$

$m \in \{0,1\}, \dot{x} \in \dot{X}$ は x の導関数 dx/dt である．この f_x の集合を $F(X)$ とする．

$$f_c ::= \dot{c} = n$$

$n \in \mathbb{N}, \dot{c} \in \dot{C}$ は c の周波数 dc/dt である．この f_c の集合を $F(C)$ とする． □

動的線形ハイブリッドオートマトンは動作中の構成変化を生成・消滅により表すことができるオートマトンである．生成・消滅アクションの出力アクションに対する入力アクションはそれぞれ1つずつであり，1対1対応で生成・消滅を行う．

定義 5 (動的線形ハイブリッドオートマトンの構文) 動的ハイブリッドオートマトンの構文 H は，$H = \langle L, l_0, X, C, I, Flow, Act, T, T_{init}, T_{end} \rangle$ で表される．

- ロケーションの有限集合 L.
- 初期ロケーション $l_0 \in L$.
- クロック変数の有限集合 X.
- サイクル変数の有限集合 C.
- ロケーションに不変条件 ϕ を割り当てる関数 $I : L \to \Phi(X \cup C)$.
- 各ロケーションに変数の傾きを与える関数 $Flow = \{flow_X\} \cup \{flow_C\}$．ただし，$flow_X : L \to F(X), flow_C : L \to F(C)$ である．
- アクションの有限集合 $Act = Act_{in} \cup Act_{out} \cup Act_\tau$．ここで，$Act_{in}$ は入力アクションの有限集合，Act_{out} は出力アクションの有限集合，Act_τ は内部アクションである．特に $Crt\_H_n \in Act$ はオートマトン H_n を生成するアクション，$Dst\_H_n \in Act$ はオートマトン H_n を消滅させるアクションとする．
- エッジの有限集合 $T \subseteq L \times \Phi \times Act \times 2^X \times L$．その要素は $(l, \phi, a, \lambda, l') \in T$ で表され，a は $a!, a?, a_\tau$ のいずれかである．
  - $l, l' \in L$ は遷移元及び遷移先ロケーション．
  - $\phi \in \Phi$ はガード条件．
  - $a!, a?, a_\tau \in Act$ はアクションである．ただし，遷移とともにアクションを出力するアクションを $a!$，出力アクションを受け取り遷移するアクションを $a?$，内部アクションを a_τ と表す．
  - $\lambda \subseteq X$ はリセットされるクロック変数の有限集合．
- T_{init} は，以下のいずれかである．
  - アクションがある時，$T_{init} \subseteq Act_{in} \times L$ その要素は $(a, l) \in T_{init}$ で表される．
    - $a \in Act_{in}$ は生成アクション．
    - $l \in L$ は生成されたオートマトンの初期ロケーション．
  - アクションがない時，$T_{init} \subseteq L$ その要素 $l \in T_{init}$ は初期ロケーション．

  生成アクションがないオートマトンの場合は，そのオートマトンは既に生成され，動作しているオートマトンであり，生成アクションがあるオートマトンは，アクションにより生成され動作し始めるオートマトンである．
- $T_{end} \subseteq L \times \Phi \times Act_{out}$ その要素は (l, ϕ, a) で表される．
  - $l \in L$ は遷移元のロケーション．
  - $\phi \in \Phi$ はガード条件．
  - $a \in Act_{out}$ は消滅アクション．

  これにより，指定されたオートマトンが消滅する．

□

例 1 (動的線形ハイブリッドオートマトンの例) 5つの動的線形ハイブリッドオートマトン H_1, H_2, H_3, H_4, H_5 の例を図 1 に示す．斜めの矢印が付いたロケーションが初期ロケーションを表し，生成アクションが付いていないオートマトン

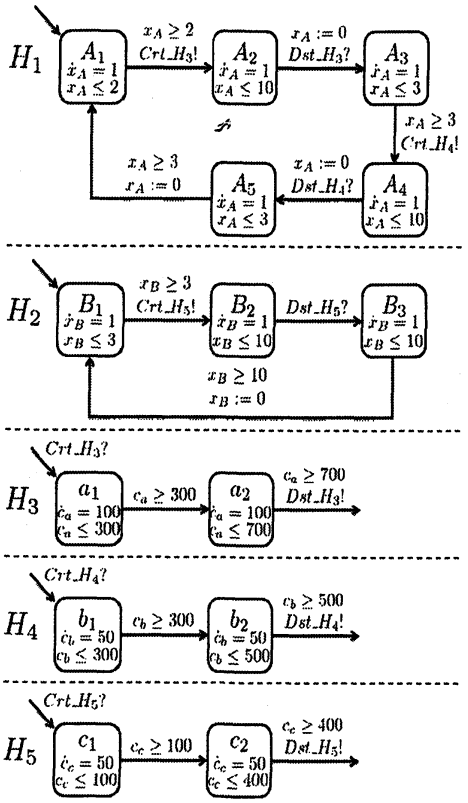

図 1: 動的線形ハイブリッドオートマトンの例

は，最初から動作しているオートマトンである．図では H_1, H_2 が最初から動作しているオートマトンで，H_3, H_4, H_5 は生成アクションにより生成され動作し始めるオートマトンである．また，H_3, H_4, H_5 にあるように，遷移先のロケーションがなく，遷移に消滅アクションが付いている遷移によりオートマトンが消滅する．

定義 6 (動的線形ハイブリッドオートマトンの並列合成) 2 つの動的線形ハイブリッドオートマトン H_1, H_2 の並列合成は，$H_1||H_2$ として $H_1||H_2 = \langle L_{H_1||H_2}, l_{0H_1||H_2}, X_{H_1||H_2}, C_{H_1||H_2}, I_{H_1||H_2}, Flow_{H_1||H_2}, Act_{H_1||H_2}, T_{H_1||H_2}, T_{initH_1||H_2}, T_{endH_1||H_2} \rangle$ によって定義される．ここでは，H_2 を新たに合成する動的線形ハイブリッドオートマトンとする．

- $L_{H_1||H_2} = L^{=}_{H_1} \cup (L^{*}_{H_1} \times L_{H_2})$．ただし，$L^{*}_{H_1}$ は以下に示すようなロケーション集合である．また，$L^{=}_{H_1} = L_{H_1} \setminus L^{*}_{H_1}$ とする．
  - H_2 に $Crt\_H_2?$ アクションと $Dst\_H_2!$ アクションがある場合，$L^{*}_{H_1}$ は，L_{H_1} の中で $Crt\_H_2!$ アクションが付いている遷移の遷移先ロケーションから $Dst\_H_2?$ アクションが付いている遷移の遷移元ロケーションの間で到達可能なロケーション集合．
  - H_2 に $Crt\_H_2?$ アクションがなく $Dst\_H_2!$ アクションがある場合，$L^{*}_{H_1}$ は，L_{H_1} の中で l_{0H_1} から $Dst\_H_2?$ アクションが付いている遷移の遷移元ロケーションの間で到達可能なロケーション集合．
  - H_2 に $Crt\_H_2?$ アクションがなく $Dst\_H_2!$ アクションがない場合，または，$Crt\_H_2?$ アクションがあり $Dst\_H_2!$ アクションがない場合，$L^{*}_{H_1} = L_{H_1}$．
- $l_{0H_1||H_2} = l^{*}_{0}$．ただし，$l^{*}_{0}$ は $l_{0H_1} \in L^{*}_{H_1}$ のとき $l^{*}_{0} = \{l_{0H_1}, l_{0H_2}\}$，$l_{0H_1} \notin L^{*}_{H_1}$ のとき $l^{*}_{0} = l_{0H_1}$ とする．
- $X_{H_1||H_2} = X_{H_1} \cup X_{H_2}$．
- $C_{H_1||H_2} = C_{H_1} \cup C_{H_2}$．
- $I_{H_1||H_2} = I^{*}$．ただし，I^{*} は，$L^{*}_{H_1}$ に対しては $I^{*} = I_{H_1} \cap I_{H_2}$，$L^{=}_{H_1}$ に対しては $I^{*} = I_{H_1}$ とする．
- $Flow_{H_1||H_2} = Flow^{*}$．ただし，$Flow^{*}$ は，$L^{*}_{H_1}$ に対しては $Flow^{*} = \{flow_{H_1}\} \cup \{flow_{H_2}\}$，$L^{=}_{H_1}$ に対しては $Flow^{*} = flow_{H_1}$ とする．
- $Act_{H_1||H_2} = (Act_{H_1} \setminus Act_{inoutH_1}) \cup (Act_{H_2} \setminus Act_{inoutH_2}) \cup Act_{\tau H_1||H_2}$．ただし，$Act_{inoutH_1}, Act_{inoutH_2}$ は合成対象のオートマトンに入力アクション及び出力アクションに対応したアクションが存在するアクションの有限集合であり，それらは並列合成後，内部アクションの有限集合 $Act_{\tau H_1||H_2}$ となる．

- $T_{H_1||H_2} \subseteq L_{H_1||H_2} \times \Phi_{H_1||H_2} \times Act_{H_1||H_2} \times 2^{X_{H_1||H_2}} \times L_{H_1||H_2}$. ただし，$\Phi_{H_1||H_2} = \Phi_{H_1} \cup \Phi_{H_2}$. $2^{X_{H_1||H_2}} = 2^{X_{H_1} \cup X_{H_2}}$ であり，その要素 t は 2 つの遷移 $(l_{H_1}, \phi_{H_1}, a_{H_1}, \lambda_{H_1}, l'_{H_1})$ と $(l_{H_2}, \phi_{H_2}, a_{H_2}, \lambda_{H_2}, l'_{H_2})$ に対して，以下の規則によって決まる.
  - $l_{H_1}, l'_{H_1} \in L^{\bar{*}}_{H_1}$ のとき，$t = (l_{H_1}, \phi_{H_1}, a_{H_1}, \lambda_{H_1}, l'_{H_1})$.
  - $l_{H_1}, l'_{H_1} \in L^{*}_{H_1}$ のとき，
    - $a_{H_1} \in Act_{\tau H_1}$ または，H_2 に $a_{H_1} \in Act_{inH_1}$ もしくは $a_{H_1} \in Act_{outH_1}$ に対応するアクションがないとき，$t = ((l_{H_1}, l_{H_2}), \phi_{H_1}, a_{H_1}, \lambda_{H_1}, (l'_{H_1}, l_{H_2}))$.
    - $a_{H_2} \in Act_{\tau H_2}$ または，H_1 に $a_{H_2} \in Act_{inH_2}$ もしくは $a_{H_2} \in Act_{outH_2}$ に対応するアクションがないとき，$t = ((l_{H_1}, l_{H_2}), \phi_{H_2}, a_{H_2}, \lambda_{H_2}, (l_{H_1}, l'_{H_2}))$.
    - $a_{H_1} \in Act_{inH_1}$ かつそのアクションに対応した $a_{H_2} \in Act_{outH_2}$ または，$a_{H_1} \in Act_{outH_1}$ かつそのアクションに対応した $a_{H_2} \in Act_{inH_2}$ がある時，そのアクションは $a \in Act_{\tau H_1||H_2}$ となり，$t = ((l_{H_1}, l_{H_2}), \phi_{H_1} \wedge \phi_{H_2}, a, \lambda_{H_1} \cup \lambda_{H_2}, (l'_{H_1}, l'_{H_2}))$
- T_{init} は以下のいずれかである.
  - $T_{init} \subseteq L_{H_1||H_2} \times Act_{\tau H_1||H_2} \times L_{H_1||H_2}$. その要素 t は $t = (l_{H_1||H_2}, a, l'_{H_1||H_2})$ で表される.
    - $l_{H_1||H_2}, l'_{H_1||H_2} \in L_{H_1||H_2}$ は遷移先及び遷移元ロケーション.
    - $a \in Act_{\tau H_1||H_2}$ は生成アクション.
  - $T_{init} \subseteq L_{H_1||H_2}$ その要素 $l_{H_1||H_2} \in T_{init}$ はロケーション.
- $T_{end} \subseteq L_{H_1||H_2} \times \Phi_{H_1||H_2} \times Act_{\tau H_1||H_2} \times L_{H_1||H_2}$. その要素 t は $t = (l_{H_1||H_2}, \phi_{H_1||H_2}, a, l'_{H_1||H_2})$ で表される.

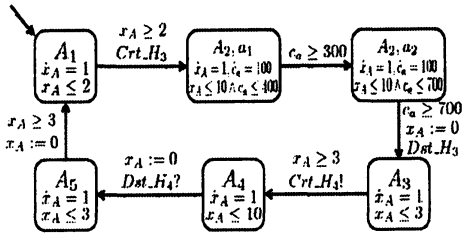

図 2: 動的線形ハイブリッドオートマトンの並列合成の例

  - $l_{H_1||H_2}, l'_{H_1||H_2} \in L_{H_1||H_2}$ は遷移元及び遷移先ロケーション.
  - $\phi_{H_1||H_2} \in \Phi_{H_1||H_2}$ はガード条件.
  - $a \in Act_{\tau H_1||H_2}$ は消滅アクション.

□

例 2 (動的線形ハイブリッドオートマトンの並列合成の例) 図 1 のオートマトン H_1, H_3 の並列合成の例を図 2 に示す. この例では，$L^{*}_{H_1} = \{A_2\}$ であるため，並列合成した後のロケーション集合 $L_{H_1||H_3} = \{A_1, (A_2, a_1), (A_2, a_2), A_3, A_4, A_5\}$ となる. また，アクション Crt_H_3, Dst_H_3 は内部アクション集合 $Act_{\tau H_1||H_3}$ の要素となる.

2.2 意味

次に，意味について定義する.

定義 7 (動的線形ハイブリッドオートマトンの状態) 動的線形ハイブリッドオートマトンの状態は $q = (l, \mu, \nu)$ である.

- $l \in L$ はロケーション.
- $\mu : C \to \mathbb{R}_{\ge 0}$ はサイクル評価.
- $\nu : X \to \mathbb{R}_{\ge 0}$ はクロック評価. □

定義 8 (動的線形ハイブリッドオートマトンの意味) 動的線形ハイブリッドオートマトン $H = \langle L, l_0, X, C, I, Flow, Act, T, T_{init}, T_{end} \rangle$ の意味は，$\mathcal{M} = \langle Q, \Rightarrow, q_0 \rangle$ として定義される.

- Q は状態 q の集合.
- $\Rightarrow$ は時間遷移 $\Rightarrow_\delta$ と離散遷移 $\Rightarrow_d$ の和集合.
  - 時間遷移
    任意の状態 $(l,\mu,\nu) \in Q$ と時間経過 $t \in \mathbb{R}_{\geq 0}$ に対し，$l' = l$ かつ $\mu' = \mu + flow_C(l)t \in I(l)$ かつ $\nu' = \nu + flow_X(l)t \in I(l)$ の時かつその時に限り $(l,\mu,\nu) \Rightarrow_\delta (l,\mu',\nu')$ である.
  - 離散遷移
    * アクション a が生成，消滅アクションでない時，任意の状態 $(l,\mu,\nu) \in Q$ に対し，ロケーション l からのエッジ $(l,\phi,a,\lambda,l') \in T$ が存在し，μ,ν が ϕ を満たし，かつ $\mu \in I(l'),\nu'[\lambda := 0] \in I(l')$ となるとき $(l,\mu,\nu) \Rightarrow_d (l',\mu',\nu')$ である.
    * アクション a が生成アクションの時，任意の状態 $(l_1,\mu_1,\nu_1) \in Q$ に対し，ロケーション l_1 からのエッジ $(l_1,\phi,a,\lambda,(l_1',l_2)) \in T$ が存在し，μ_1,ν_1 が ϕ を満たし，かつ $\mu_1 \in I(l_1'),\nu_1'[\lambda := 0] \in I(l_1')$ となるとき $(l_1,\mu_1,\nu_1) \Rightarrow_d ((l_1',l_2),(\mu_1',\mu_2),(\nu_1',\nu_2))$ である．ここで，l_2 は新たに生成された動的線形ハイブリッドオートマトンの初期ロケーションであり，μ_2,ν_2 のすべての評価は 0 である．状態集合 Q は $Q = \bar{Q_1^*} \cup (Q_1^* \times Q_2)$ となる．ここで，Q_1^* は既に生成されている動的線形ハイブリッドオートマトンの生成アクションが付いている遷移の遷移先の状態から消滅アクションが付いている遷移の遷移元の状態までの間で到達可能な状態集合，$\bar{Q_1^*}$ は $\bar{Q_1^*} = Q_1 \backslash Q_1^*$ であり，Q_2 は新たに生成された動的線形ハイブリッドオートマトンの状態集合を表す.
    * アクション a が消滅アクションの時，任意の状態 $((l_1,l_2),(\mu_1,\mu_2),(\nu_1,\nu_2)) \in Q$ に対し，ロケーション (l_1,l_2) からのエッジ $((l_1,l_2),\phi,a,\lambda,l_1') \in T$ が存在し，μ_1,μ_2,ν_1,ν_2 が ϕ を満たし，かつ $\mu_1 \in I(l_1'),\nu_1'[\lambda := 0] \in I(l_1')$ となるとき $((l_1,l_2),(\mu_1,\mu_2),(\nu_1,\nu_2)) \Rightarrow_d (l_1',\mu_1',\nu_1')$ である．状態集合 Q は $Q = \bar{Q_1^*} \cup (Q_1^* \times Q_2)$ から $Q = Q_1$ となる．ここで，Q_1 は生成されている動的線形ハイブリッドオートマトンの状態集合であり，Q_2 は消滅する動的時間オートマトンの状態集合を表す.
- $q_0 \in Q$ は初期状態.
  初期状態とは，初期ロケーション l_0 において全てのサイクル評価及びクロック評価が 0 の状態である.

□

定義 9 (パス)
遷移系 $\mathcal{M} = \langle Q, \Rightarrow, q_0 \rangle$ 上の初期状態 q_0 から有限または無限列 $\omega = q_0 \Rightarrow q_1 \Rightarrow q_2 \Rightarrow \cdots$ をパスと定義する.

□

定義 10 (到達可能性問題)
動的線形ハイブリッドオートマトン $H = \langle L, l_0, X, C, I, Flow, Act, T, T_{init}, T_{end} \rangle$ と望ましくないロケーションであるターゲットロケーションの集合 L_{target} が入力されたとき，H の遷移系 $\mathcal{M} = \langle Q, \Rightarrow, q_0 \rangle$ 上でターゲットロケーション $l_{target} \in L_{target}$ を持つ状態 $q_{target} = (l_{target}, \nu)$ に到達するパス ω_{ce} が存在する場合，かつその時に限り，出力は *"reachable"* となり，それ以外は *"not reachable"* となる．出力が *"reachable"* となるときのパス ω_{ce} を反例と呼ぶ. □

3 動的線形ハイブリッドCEGAR

動的線形ハイブリッド CEGAR の流れは図 3 のような図で表される.

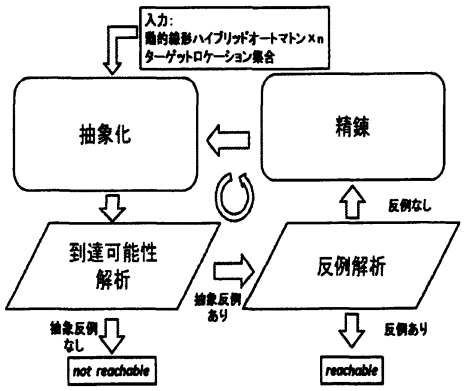

図 3: 動的線形ハイブリッド CEGAR の流れ

3.1 述語抽象化

ここでは，述語抽象化について定義する．述語抽象化は状態爆発を抑制するために用いられる手法であり，実数変数であるサイクル評価，クロック評価を述語を用いて抽象化することにより状態爆発を抑制している．

定義 11 (抽象化述語)
クロック変数の集合 X に関する抽象化述語 ψ を

$$\psi ::= true \mid x_1 \sim n \mid x_1 - x_2 \sim n \mid c_1 \sim n \mid$$

$$u_1c_1 + u_2c_2 \sim n \mid x_1 + u_1c_1 \sim n \mid -x_1 + u_1c_1 \sim n$$

と定義する．ただし，$u_1, u_2 \in \mathbb{Z}\backslash\{0\}, x \in X, c_1, c_2 \in C$，$n \in \mathbb{N}$，$\sim \in \{<, \leq, >, \geq\}$ である．ロケーション l における抽象化述語の有限集合を $\Psi^l = \{\psi_0^l, \cdots, \psi_{n-1}^l\}$ とする．また，全てのロケーションにおける抽象化述語の有限集合を $\Psi = \{\Psi^{l_0} \cup \cdots \cup \Psi^{l_{n-1}}\}$ とする． □

定義 12 (述語抽象化・具体化)
X はクロック変数の有限集合であり，$\mathcal{V}_X$ は対応するクロック評価の集合，C はサイクル変数の有限集合であり，$\mathcal{U}_C$ は対応するサイクル評価の集合であるとする．抽象化述語の有限集合 $\Psi^l = \{\psi_0^l, \cdots, \psi_{n-1}^l\}$ が与えられたとき，タイミング制約抽象化関数 $\alpha : L \times \mathcal{U}_C \times \mathcal{V}_X \to L \times \mathcal{B}$ は以下のように定義される．

$$\alpha((l, \mu, \nu))(i) = (l, \psi_i^l\mu, \psi_i^l\nu)$$

また，具体化関数 $\gamma : L \times \mathcal{B} \to L \times 2^{\mathcal{U}_C \cup \mathcal{V}_X}$ は以下のように定義される．

$\gamma((l, b)) = \{(l, \mu, \nu) \in L \times \mathcal{U}_C \times \mathcal{V}_X \mid I(l) \wedge \bigwedge_{i=0}^{n-1} \psi_i^l\mu \equiv b^l(i) \wedge \bigwedge_{i=0}^{n-1} \psi_i^l\nu \equiv b^l(i)\}$ □

抽象化述語と抽象化・具体化関数を用いて抽象構造を構築する．抽象構造は，大き目の近似になるように構築する．大き目の近似とは，具体構造が持つ遷移を抽象構造に全て持たせることで，抽象化に健全性を持たせる近似である．

定義 13 (抽象動的線形ハイブリッドオートマトン)
$H = \langle L, l_0, X, C, I, Flow, Act, T, T_{init}, T_{end}\rangle$ に対する抽象動的線形ハイブリッドオートマトン $H^{\mathcal{A}} = \langle Q^{\mathcal{A}}, q_0^{\mathcal{A}}, \Psi, Act^{\mathcal{A}}, T^{\mathcal{A}}, T_{init}^{\mathcal{A}}, T_{end}^{\mathcal{A}}\rangle$ は次の要素からなる．

- 抽象状態の有限集合 $Q^{\mathcal{A}} = L \times \mathcal{B}$.
- 抽象初期状態 $q_0^{\mathcal{A}} = (l_0, b_0^{l_0})$．ただし，$q_0 \in \gamma(l_0, b_0^{l_0})$ とする．
- 抽象化述語の集合 Ψ.
- アクションの有限集合 $Act^{\mathcal{A}} = Act$.
- $T^{\mathcal{A}} \subseteq Q^{\mathcal{A}} \times Act^{\mathcal{A}} \times Q^{\mathcal{A}}$．その要素は $(q^{\mathcal{A}}, a, q'^{\mathcal{A}})$ で表され，a は $a!, a?, a_\tau$ のいずれかである．
  - $q^{\mathcal{A}}, q'^{\mathcal{A}} \in Q^{\mathcal{A}}$ は遷移元及び遷移先抽象状態である．
  - $a \in Act^{\mathcal{A}}$ はアクションである．ただし，遷移とともにアクションを出力するアクションを $a!$，出力アクションを受け取り遷移するアクションを $a?$，内部アクションを a_τ と表す．
- T_{init} は以下のいずれかである．
  - アクションがある時，$T_{init}^{\mathcal{A}} \subseteq Act^{\mathcal{A}} \times Q^{\mathcal{A}}$．その要素は 2 つ組 $(a, q^{\mathcal{A}})$ で表される．
    - $a \in Act_{in}^{\mathcal{A}}$ は生成アクション.

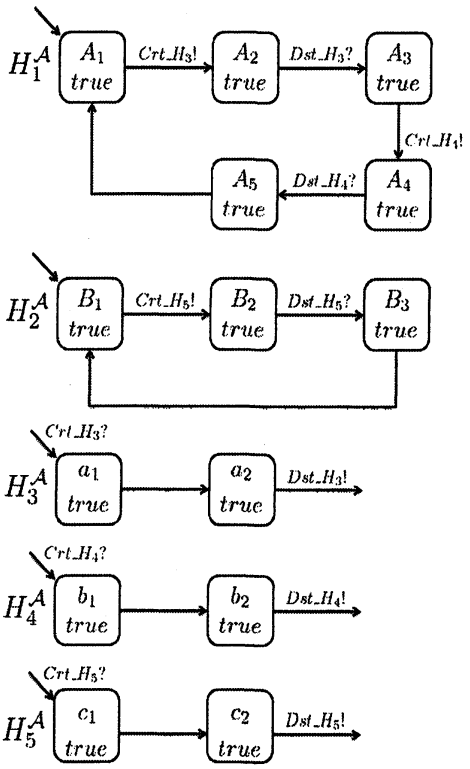

図 4: 抽象動的線形ハイブリッドオートマトンの例

* $q^{\mathcal{A}} \in Q^{\mathcal{A}}$ は生成されたオートマトンの抽象初期状態.

– アクションがない時, $T^{\mathcal{A}}_{init} \subseteq Q^{\mathcal{A}}$. その要素 $q^{\mathcal{A}} \in T^{\mathcal{A}}_{init}$ は抽象初期状態.

- $T^{\mathcal{A}}_{end} \subseteq Q^{\mathcal{A}} \times Act^{\mathcal{A}}$. その要素は $(q^{\mathcal{A}}, a)$ で表される.

– $q^{\mathcal{A}} \in Q^{\mathcal{A}}$ は遷移元の抽象状態である.

– $a \in Act^{\mathcal{A}}_{out}$ は消滅アクションである.

□

例 3 (抽象動的線形ハイブリッドオートマトンの例) 図 *1* を述語 *true* によって述語抽象化すると図 *4* のようになり, 動作は (l, μ, ν) という無限の状態から $(l, true)$ という有限の状態で表現される.

定義 14 (抽象動的線形ハイブリッドオートマトンの並列合成) 2 つの抽象動的線形ハイブリッドオートマトンの並列合成は, $H_1^{\mathcal{A}} || H_2^{\mathcal{A}}$ として $\langle Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, q^{\mathcal{A}}_{0H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, \Psi_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, Act^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, T^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, T^{\mathcal{A}}_{initH_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, T^{\mathcal{A}}_{endH_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \rangle$ によって定義される. ここでは, $H_2^{\mathcal{A}}$ を新たに合成する抽象動的線形ハイブリッドオートマトンとする.

- $Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} = Q^{\bar{\mathcal{A}}*}_{H_1^{\mathcal{A}}} \cup (Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}} \times Q^{\mathcal{A}}_{H_2^{\mathcal{A}}})$. ただし, $Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}}$ は以下に示すような抽象状態集合である. また, $Q^{\bar{\mathcal{A}}*}_{H_1^{\mathcal{A}}} = Q^{\mathcal{A}}_{H_1^{\mathcal{A}}} \setminus Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}}$ とする.

  – $H_2^{\mathcal{A}}$ に $Crt\_H_2?$ アクションと $Dst\_H_2!$ アクションがある場合, $Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}}$ は, $Q^{\mathcal{A}}_{H_1^{\mathcal{A}}}$ の中で $Crt\_H_2!$ アクションが付いている遷移の遷移先抽象状態から $Dst\_H_2?$ アクションが付いている遷移の遷移元抽象状態の間で到達可能な抽象状態集合.

  – $H_2^{\mathcal{A}}$ に $Crt\_H_2?$ アクションがなく $Dst\_H_2!$ アクションがある場合, $Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}}$ は, $Q^{\mathcal{A}}_{H_1^{\mathcal{A}}}$ の中で $q^{\mathcal{A}}_{0H_1^{\mathcal{A}}}$ から $Dst\_H_2?$ アクションが付いている遷移の遷移元抽象状態の間で到達可能な抽象状態集合.

  – $H_2^{\mathcal{A}}$ に $Crt\_H_2?$ アクションがなく $Dst\_H_2!$ アクションがない場合, または, $Crt\_H_2?$ アクションがあり $Dst\_H_2!$ アクションがない場合, $Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}} = Q^{\mathcal{A}}_{H_1^{\mathcal{A}}}$.

- $q^{\mathcal{A}}_{0H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} = q_0^{\mathcal{A}*}$. ただし, $q_0^{\mathcal{A}*}$ は $q^{\mathcal{A}}_{0H_1^{\mathcal{A}}} \in Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}}$ のとき $q_0^{\mathcal{A}*} = \{q^{\mathcal{A}}_{0H_1^{\mathcal{A}}}, q^{\mathcal{A}}_{0H_2^{\mathcal{A}}}\}$, $q^{\mathcal{A}}_{0H_1^{\mathcal{A}}} \notin Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}}$ のとき $q_0^{\mathcal{A}*} = q^{\mathcal{A}}_{0H_1^{\mathcal{A}}}$ とする.

- $\Psi_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} = \Psi_{H_1^{\mathcal{A}}} \cup \Psi_{H_2^{\mathcal{A}}}$.

- $Act^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} = (Act^{\mathcal{A}}_{H_1} \setminus Act^{\mathcal{A}}_{inoutH_1}) \cup (Act^{\mathcal{A}}_{H_2} \setminus Act^{\mathcal{A}}_{inoutH_2}) \cup Act^{\mathcal{A}}_{\tau H_1||H_2}$. ただし, $Act^{\mathcal{A}}_{inoutH_1}$, $Act^{\mathcal{A}}_{inoutH_2}$ は合成対象のオートマトン中に入力アクションおよび出力アクションに対応したアクションが存在するアクションの有限集合であり, それらは並列合成後, 内部アクションの有限集合 $Act^{\mathcal{A}}_{\tau H_1||H_2}$ となる.

- $T^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \subseteq Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \times Act^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$. その要素 $t^{\mathcal{A}}$ は2つの遷移 $(q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, a_{H_1^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}})$ と $(q^{\mathcal{A}}_{H_2^{\mathcal{A}}}, a_{H_2^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_2^{\mathcal{A}}})$ に対して，以下の規則によって決まる．
  - $q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}} \in Q^{\bar{\mathcal{A}}*}_{H_1^{\mathcal{A}}}$ のとき，$t^{\mathcal{A}} = (q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, a_{H_1^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}})$.
  - $q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}} \in Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}}$ のとき，
    - $a_{H_1^{\mathcal{A}}} \in Act_{\tau H_1^{\mathcal{A}}}$ または，$H_2^{\mathcal{A}}$ に $a_{H_1^{\mathcal{A}}} \in Act_{inH_1^{\mathcal{A}}}$ もしくは $a_{H_1^{\mathcal{A}}} \in Act_{outH_1^{\mathcal{A}}}$ に対応するアクションがないとき，$t^{\mathcal{A}} = ((q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q^{\mathcal{A}}_{H_2^{\mathcal{A}}}), a_{H_1^{\mathcal{A}}}, (q'^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q^{\mathcal{A}}_{H_2^{\mathcal{A}}})$.
    - $a_{H_2^{\mathcal{A}}} \in Act_{\tau H_2^{\mathcal{A}}}$ または，$H_1^{\mathcal{A}}$ に $a_{H_2^{\mathcal{A}}} \in Act_{inH_2^{\mathcal{A}}}$ もしくは $a_{H_2^{\mathcal{A}}} \in Act_{outH_2^{\mathcal{A}}}$ に対応するアクションがないとき，$t^{\mathcal{A}} = ((q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q^{\mathcal{A}}_{H_2^{\mathcal{A}}}), a_{H_2^{\mathcal{A}}}, (q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_2^{\mathcal{A}}})$.
    - $a_{H_1^{\mathcal{A}}} \in Act_{inH_1^{\mathcal{A}}}$ かつそのアクションに対応した $a_{H_2^{\mathcal{A}}} \in Act_{outH_2^{\mathcal{A}}}$ のとき，または，$a_{H_1^{\mathcal{A}}} \in Act_{outH_1^{\mathcal{A}}}$ かつそのアクションに対応した $a_{H_2^{\mathcal{A}}} \in Act_{inH_2^{\mathcal{A}}}$ がある時，そのアクションは $a \in Act_{\tau H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ となり，$t^{\mathcal{A}} = ((q^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q^{\mathcal{A}}_{H_2^{\mathcal{A}}}), a, (q'^{\mathcal{A}}_{H_1^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_2^{\mathcal{A}}})$.
- $T_{initH_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ は以下のいずれかである．
  - $T^{\mathcal{A}}_{initH_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \subseteq Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \times Act^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \times Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$. その要素 $t^{\mathcal{A}}$ は $t^{\mathcal{A}} = (q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, a_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}})$ で表される．
    - $q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \in Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ は遷移先及び遷移元抽象状態．
    - $a_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \in Act^{\mathcal{A}}_{\tau H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ は生成アクション．
  - $T_{initH_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \subseteq Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ その要素 $q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \in T_{initH_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ は抽象状態．
- $T^{\mathcal{A}}_{endH_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \subseteq Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \times Act^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \times Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$. その要素 $t^{\mathcal{A}}$ は $t^{\mathcal{A}} = (q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, a_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}})$ で表される．

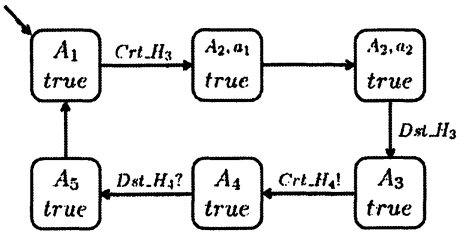

図 5: 抽象動的線形ハイブリッドオートマトンの例

  - $q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}, q'^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \in Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ は遷移元及び遷移先抽象状態．
  - $a_{H_1^{\mathcal{A}}||H_2^{\mathcal{A}}} \in Act^{\mathcal{A}}_{\tau H_1^{\mathcal{A}}||H_2^{\mathcal{A}}}$ は消滅アクション．

□

例 4 (抽象動的線形ハイブリッドオートマトンの並列合成の例) 図 4 のオートマトン H_1, H_3 の並列合成の例を図 5 に示す．この例では，$Q^{\mathcal{A}*}_{H_1^{\mathcal{A}}} = \{(A_2, true)\}$ であるため，並列合成した後の抽象状態集合 $Q^{\mathcal{A}}_{H_1^{\mathcal{A}}||H_3^{\mathcal{A}}} = \{(A_1, true), ((A_2, a_1), true), ((A_2, a_2), true), (A_3, true), (A_4, true), (A_5, true)\}$ となる．また，アクション Crt_H_3, Dst_H_3 は内部アクション集合 $Act^{\mathcal{A}}_{\tau H_1^{\mathcal{A}}||H_3^{\mathcal{A}}}$ の要素となる．

定義 15 (抽象動的線形ハイブリッドオートマトンの意味) 動的線形ハイブリッドオートマトン $H = \langle L, , l_0, X, C, I, flow, Act, T, T_{init}, T_{end}\rangle$ の動作を表す遷移系 $\mathcal{M} = \langle Q, \Rightarrow, q_0\rangle$ と抽象化述語の集合 Ψ が与えられたとき，抽象動的線形ハイブリッドオートマトンの意味は $\mathcal{M}^{\mathcal{A}} = \langle Q^{\mathcal{A}}, \Rightarrow^{\mathcal{A}}, q_0^{\mathcal{A}}\rangle$ として定義される．

- $Q^{\mathcal{A}} = L \times \mathcal{B}$.
- 遷移関係は以下のいずれかである．
  - アクションが生成，消滅アクションでない時，$(l, b^l) \Rightarrow^{\mathcal{A}} (l', b^{l'})$ iff $\exists \mu, \mu' \in \mathcal{U}_C, \exists \nu, \nu' \in \mathcal{V}_X$ $s.t.$ $((l, \mu, \nu) \in \gamma((l, b^l)))$ $\wedge$ $((l', \mu', \nu') \in \gamma((l', b^{l'}))).(l, \mu, \nu) \Rightarrow (l', \mu', \nu')$.

– アクションが生成アクションの時，
$(l_1, b^{l_1}) \Rightarrow^{\mathcal{A}} ((l'_1, l_2), (b^{l'_1}, b^{l_2}))$ iff
$\exists \mu_1, \mu'_1, \mu_2 \in \mathcal{U}_C, \exists \nu_1, \nu'_1, \nu_2 \in \mathcal{V}_X$ $s.t.$
$((l_1, \mu_1, \nu_1) \in \gamma((l_1, b^{l_1}))) \wedge$
$(((l'_1, l_2), (\mu'_1, \mu_2), (\nu'_1, \nu_2)) \in$
$\gamma(((l'_1, l_2), (b^{l'_1}, b^{l_2})))).(l_1, \mu_1, \nu_1) \Rightarrow$
$((l'_1, l_2), (\mu'_1, \mu_2), (\nu'_1, \nu_2))$.
ここで，(l_2, b^{l_2}) は新たに生成された抽象動的線形ハイブリッドオートマトンの初期状態である．また，抽象状態集合 $Q^{\mathcal{A}}$ は $Q^{\mathcal{A}} = \bar{Q_1^{\mathcal{A}*}} \cup (Q_1^{\mathcal{A}*} \times Q_2^{\mathcal{A}})$ となる．ここで，$Q_1^{\mathcal{A}*}$ は既に生成されている抽象動的時間オートマトンのせいせアクションが付いている遷移の遷移先の状態から消滅アクションが付いている遷移の遷移元の状態までの間で到達可能な状態集合，$\bar{Q_1^{\mathcal{A}*}}$ は $\bar{Q_1^{\mathcal{A}*}} = Q_1^{\mathcal{A}} \setminus Q_1^{\mathcal{A}*}$ であり，$Q_2^{\mathcal{A}}$ は新たに生成された抽象動的時間オートマトンの状態集合を表す．

– アクションが消滅アクションの時，
$((l_1, l_2), (b^{l_1}, b^{l_2})) \Rightarrow^{\mathcal{A}} (l'_1, b^{l'_1})$ iff
$\exists \mu_1, \mu'_1, \mu_2 \in \mathcal{U}_C, \exists \nu_1, \nu'_1, \nu_2 \in \mathcal{V}_X$ $s.t.$
$(((l_1, l_2), (\mu_1, \mu_2), (\nu_1, \nu_2)) \in$
$\gamma(((l_1, l_2), (b^{l_1}, b^{l_2})))) \wedge ((l'_1, \mu'_1, \nu'_1) \in$
$\gamma((l'_1, b^{l'_1}))).((l_1, l_2), (\mu_1, \mu_2), (\nu_1, \nu_2))$
$\Rightarrow (l'_1, \mu'_1, \nu'_1)$.
ここで，(l_2, b^{l_2}) は消滅する抽象動的時間オートマトンの状態である．抽象状態集合 $Q^{\mathcal{A}}$ は $Q^{\mathcal{A}} = \bar{Q_1^{\mathcal{A}*}} \cup (Q_1^{\mathcal{A}*} \times Q_2^{\mathcal{A}})$ から $Q^{\mathcal{A}} = Q_1^{\mathcal{A}}$ となる．ここで，$Q_1^{\mathcal{A}}$ は生成されている抽象動的時間オートマトンの状態集合であり，$Q_2^{\mathcal{A}}$ は消滅する抽象動的時間オートマトンの状態集合を表す．

- $q_0^{\mathcal{A}} = (l_0, b_0^{l_0})$.

□

定義 16 (遷移関係の具体化)
遷移関係 $\Rightarrow^{\mathcal{A}}$ を具体化する関数 $\gamma(\Rightarrow^{\mathcal{A}})$ を以下のように定義する．

- アクションが生成，消滅アクションでない時，$\gamma(\Rightarrow^{\mathcal{A}}) = \{((l, \mu, \nu), (l', \mu', \nu')) \in Q \mid \exists b^l, b^{l'}.(l, b^l) \Rightarrow^{\mathcal{A}} (l', b^{l'}) \wedge (l, \mu, \nu) \in \gamma((l, b^l)) \wedge (l', \mu', \nu') \in \gamma((l', b^{l'}))\}$.

- アクションが生成アクションの時，$\gamma(\Rightarrow^{\mathcal{A}}) = \{((l_1, \mu_1, \nu_1), ((l'_1, l_2), (\mu'_1, \mu_2), (\nu'_1, \nu_2))) \in Q \mid \exists b^{l_1}, b^{l'_1}, b^{l_2}.$
$(l_1, b^{l_1}) \Rightarrow^{\mathcal{A}} ((l'_1, l_2), (b^{l'_1}, b^{l_2})) \wedge (l_1, \mu_1, \nu_1) \in \gamma((l_1, b^{l_1})) \wedge ((l'_1, l_2), (\mu'_1, \mu_2), (\nu'_1, \nu_2)) \in \gamma(((l'_1, l_2), (b^{l'_1}, b^{l_2})))\}$.

- アクションが消滅アクションの時，$\gamma(\Rightarrow^{\mathcal{A}}) = \{((((l_1, l_2), (\mu_1, \mu_2), (\nu_1, \nu_2)), (l'_1, \mu'_1, \nu'_1)) \in Q \mid \exists b^{l_1}, b^{l'_1}, b^{l_2}.((l_1, l_2), (b^{l_1}, b^{l_2})) \Rightarrow^{\mathcal{A}} (l'_1, b^{l'_1}) \wedge ((l_1, l_2), (\mu_1, \mu_2), (\nu_1, \nu_2)) \in \gamma(((l_1, l_2), (b^{l_1}, b^{l_2}))) \wedge (l'_1, \mu'_1, \nu'_1) \in \gamma((l'_1, b^{l'_1}))\}$.

□

定義 17 (抽象パス)
遷移系 $\mathcal{M}^{\mathcal{A}} = \langle Q^{\mathcal{A}}, \Rightarrow^{\mathcal{A}}, q_0^{\mathcal{A}} \rangle$ 上の抽象初期状態から有限または無限列 $\omega^{\mathcal{A}} = q_0^{\mathcal{A}} \Rightarrow^{\mathcal{A}} q_1^{\mathcal{A}} \Rightarrow^{\mathcal{A}} q_2^{\mathcal{A}} \Rightarrow^{\mathcal{A}} \cdots$ を抽象パスと定義する． □

定義 18 (抽象反例)
動的線形ハイブリッドオートマトン $H = \langle L, l_0, X, C, I, Flow, Act, T, T_{init}, T_{end} \rangle$ とターゲットロケーションの集合 L_{target} が入力されたとき，H の抽象構造 $\mathcal{M}^{\mathcal{A}} = \langle Q^{\mathcal{A}}, \Rightarrow^{\mathcal{A}}, q_0^{\mathcal{A}} \rangle$ 上でターゲットロケーション $l_{target} \in L_{target}$ を含む抽象ターゲットロケーション $l_{target}^{\mathcal{A}}$ を持つ状態 $q_{target}^{\mathcal{A}} = (l_{target}^{\mathcal{A}}, b^{l_{target}^{\mathcal{A}}})$ に到達するパス $\omega_{ce}^{\mathcal{A}}$ を抽象反例と呼ぶ． □

3.2 到達可能性解析

到達可能性解析では，抽象反例が存在するかどうかを深さ優先探索で解析する．解析では，抽象反例が見つかった時点で次で説明する反例解析を行う．

3.3 反例解析

ここでは，抽象反例が具体モデル上で再現できるかを調べる．具体的には，抽象反例 $\omega_{ce}^{\mathcal{A}}$ を具体モデル上で辿り，各抽象状態の具体化がある，すなわち，$\Rightarrow \in \gamma(\Rightarrow^{\mathcal{A}})$ となるような元の遷移系における反例 $\omega_{ce} = q_0 \Rightarrow \cdots \Rightarrow q_i \Rightarrow \cdots \Rightarrow q_{target}$ が存在するかを判定する（ただし $q_i = (l_i, \zeta_i)$）．計算法としては，ターゲットから後方に向かって，現在の状態に遷移可能な状態集合を求めていく．これは最弱前条件 [3] の考え方に基づいている．また，遷移に生成アクションがある場合，そのオートマトンは生成される前の構成になるため，使用されている変数を削除する．この時点の領域が削除対象となる変数がすべて 0 という領域を含まれなければ抽象反例は再現できない偽反例である．遷移に消滅アクションがある場合，そのオートマトンで使用される変数 $X \cup C$ に対して領域を $\mathcal{V}_X \mathcal{U}_C$ として追加する．これらの操作を行い，初期状態を含む集合が得られたら，反例であることが分かる．途中で空集合となったときは，その抽象反例は具体モデルでは再現できないので，偽反例であることが分かる．

3.4 精錬

ここでは，精錬について説明する．精錬では，反例解析で偽反例と判定された抽象反例が再び現れないように述語を追加し，抽象状態を分割する．例えば以下のような抽象反例 $\omega_{ce}^{\mathcal{A}}$ の $q_0^{\mathcal{A}} \Rightarrow^{\mathcal{A}} \cdots \Rightarrow^{\mathcal{A}} q_j^{\mathcal{A}} \Rightarrow^{\mathcal{A}} \cdots \Rightarrow^{\mathcal{A}} q_{last}^{\mathcal{A}}$ について，反例解析によって $q_k^{\mathcal{A}} \Rightarrow^{\mathcal{A}} q_{k+1}^{\mathcal{A}}$ という遷移の部分で偽反例になったとする．このとき，$q_{k+1}^{\mathcal{A}}$ の状態には，$q_k^{\mathcal{A}}$ から遷移できる状態集合と遷移できない状態集合が存在すると考えられる．このことから反例解析で空ゾーンとなる直前の $q_{k+1}^{\mathcal{A}}$ の状態を分割することで，同一の反例を消すことができる．

定理 1 (提案 CEGAR の正当性)
動的時間オートマトン群とターゲットロケーションが入力されたとき，提案 *CEGAR* はターゲットに到達しないならば *"not reachable"*，到達するならば *"reachable"* を出力する．

[証明] 抽象構造は大き目の近似になるように構築しているため，到達可能性解析で到達不可能ならば *"not reachable"* と判定できる．
また，到達可能性解析で到達可能となった場合は反例解析で具体構造上で解析を行うため，抽象化を行わない場合と等しい結果が得られる． □

4 まとめ

本稿では，動作中に構成が変化するハイブリッドシステムに対して有効な動的線形ハイブリッド CEGAR の提案を行った．提案法では，現在動作しているオートマトンのみを並列合成して検証を行えるように動的線形ハイブリッドオートマトンを提案し，到達可能性解析時に動作中のオートマトンを並列合成できるような仕組みを考案した．

今後の課題として実装実験を行い，定量的なデータから本稿の有効性を確認することがあげられる．

参考文献

[1] Alur, R., Dang, T., and Ivančić, F.: Counterexample-guided predicate abstraction of hybrid systems, *Theoretical Computer Science*, Vol. 354(2006), pp. 250–271.

[2] Clarke, E. M., Grumberg, O., Jha, S., Lu, Y., and Veith, H.: Counterexample-Guided Abstraction Refinement, *LNCS*, Vol. 1855(2000), pp. 154–169.

[3] Henzinger, T. A., Nicollin, X., Sifakis, J., and Yovine, S.: Symbolic model checking for real-time systems, *Information and Computation 111(2)*, 1994, pp. 193–244.