補間に基づく時間ペトリネットの非有界モデル検査

井川　直[†1]　横川智教[†1]　佐藤洋一郎[†1]
有本和民[†1]　近藤真史[†2]　宮崎仁[†2]

本稿では, 時間ペトリネットに補間に基づく非有界モデル検査手法を適用する枠組みを示す.

Unbounded Model Checking of Time Petri Nets with Interpolation

Nao Igawa,[†1] Tomoyuki Yokogawa,[†1] Yoichiro Sato,[†1]
Kazutami Arimoto,[†1] Masafumi Kondo[†2]
and Hisashi Miyazaki[†2]

We proposed a method to apply unbounded model checking with interpolation for formal verification of Time petri nets.

1. はじめに

大規模な非同期システムの性能評価を目的として時間ペトリネット (Time Petri Nets:TPN) に基づくモデル化が広く用いられている. 性能評価を行う上では, TPN はデッドロックフリーや状態への到達可能性等の性質を満たしている必要がある.TPN の特性検証への有界モデル検査の応用については報告されているが,[1] この枠組みではあらかじめ定められた範囲の状態空間しか探索できない. そこで本稿では, TPN の特性検証に補間定理に基づく非有界モデル検査手法[2] を適用するための枠組みを示す.

2. 時間ペトリネット

ペトリネットはプレイスの集合 P, トランジションの集合 T, アークの集合 $F \subseteq (P \times T) \cup (T \times P)$, 抑止アークの集合 $F_{in} \subset F$, 初期マーキング $M_0 \subseteq P$ から定義される. アークはプレイスとトランジションを結合する有向線である. プレイスはトークンをもつことができ, すべての入力プレイスがトークンをもつとき, 接続先のトランジションは発火し, 接続先の出力プレイスへトークンが移動する. 初期マーキングは初期状態でトークンをもつプレイスを表している. 抑止アークはプレイスからトランジションを結ぶアークの一種であり, 抑止アークによって結合されたプレイスがトークンをもつときトランジションは発火できない.

TPN はペトリネットにプレイス遅延を導入したもので, プレイス遅延はトークンが有効となるまでの時間をプレイスに割り当てる関数 $X : P \to (Z^+) \times (Z^+ \cup +inf)$ によって定義される. プレイス P_i の遅延は上界 u_i と下界 l_i をもち, p_i がトークンを獲得してから l_i から u_i の時間が経過するまでのいずれかの時刻でトークンかは有効となる. 入力プレイスのすべてのトークンが有効となった時点でトランジションは発火する.

3. 時間ペトリネットの非有界モデル検査

3.1 論理式表現

TPN の動作において, 時間の経過とトランジションの発火が個別に実行される. したがって, 1 ステップの遷移は時間経過の後に発火処理が実行されるものとして表現できる.TPN の状態 s をマーキングとトークンの経過時間から定義すると, 1 ステップを表す論理関数 $T(s, d, s')$ は, 時間経過による状態変化を表す論理式 $C(s, d, s')$ と発火のステップを表す論理式 $F(s, s')$ により, 以下のように表すことができる[1].

$$T(s, d, s') \equiv C(s, d, s'') \wedge F(s'', s')$$

s, s' および s'' は状態を表し, d は経過した時間を表す. ここで, $n = |T|$ として $F(s, s')$ は以下のように表す.

$$F(s, s') \equiv F_{t_1}(s, s_1) \wedge \cdots \wedge F_{t_n}(s_{n-1}, s')$$

†1 岡山県立大学
Okayama Prefectural University
†2 川崎医療福祉大学
Kawasaki University of Medical Welfare

$F_t(s_i, s_{i+1})$ はトランジション t によって s_i から s_{i+1} へと発火による遷移が可能であるかまたは $s_i = s_{i+1}$ のとき真となる論理式である. これにより，k ステップの遷移を表す論理式 $\mathcal{N}_k$ を以下のように求められる.

$$\begin{aligned}\mathcal{N}_k \equiv & I(s_0) \wedge T(s_0, d_1, s_{n+1}) \\ & \wedge T(s_{n+1}, d_2, s_{2(n+1)}) \\ & \wedge \cdots \wedge T(s_{(k-1)(n+1)}, d_k, s_{k(n+1)})\end{aligned}$$

また，検証する性質を満たす状態を表す論理式を $R(s)$ で与えられているとすると，k ステップ以内でその状態に到達するか否かは，論理式 $\mathcal{R}_k \equiv R(s_{k(n+1)})$ に対して論理式 $BMC_k = \mathcal{N}_k \wedge \mathcal{R}_k$ の充足可能性判定により求めることができる.

3.2 補間に基づく非有界モデル検査

有界モデル検査では制限された状態空間のみを探索するため， 安全性のように全状態の探索が必要な特性は検証できない. そこで補間を用いた探索範囲の拡張[2] を導入する. 補間は同値でない論理式 A，B に対し，$A \wedge B$ が充足不能であるとき得られる以下の 3 つの条件を満たす論理式 P である.

(1) $P \wedge B$ が充足不能
(2) $A \rightarrow P$ が充足可能
(3) P は A と B の共通の変数からなる論理式

ここで，BMC_k を以下のように $PREF$ と $SUFF^k$ の部分論理式へと分割する.

$$\begin{aligned}PREF &= I(s_0) \wedge T(s_0, d_1, s_{n+1}) \\ SUFF^k &= \bigwedge_{1 \le i \le k} T(s_{i*n}, d_{i+1}, s_{i(n+1)}) \\ &\quad \wedge R(s_{k*(n+1)})\end{aligned}$$

$PREF \wedge SUFF^k$ が充足可能ならば性質を満たす状態 s_{k*n} に到達可能である. 充足不能であれば $PREF$ と $SUFF^k$ から補間 $Inter$ を生成する，補間の条件 (3) から $Inter$ は s_n に関する論理式である. したがって，条件 (2) より，$Inter(s_n)$ は初期状態から 1 ステップで到達可能な状態すべてで真になる. この $Inter(s_n)$ を初期状態 $I(s_0)$ と置き換えて新たに

$$PREF = Inter(s_n) \wedge T(s_0, d_1, s_{n+1})$$

として再び充足可能性判定を行う. この処理を繰り返していくと $Inter$ は最終的に初期状態から到達可能なすべての状態で真となるような論理式となる. このとき判定結果が充足不能であれば，求める状態へは到達不能との結論が得られる. 充足可能という結果が得られた場合，$Inter$ は到達可能状態の上方近似であるため，得られた割り当てが偽反例である可能性がある. このときはステップ数 k を延長した上で再度 BMC_k の充足可能性判定を行う. 状態空間は有限なので，いつかこの手続きは終了する.

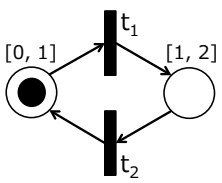

図 1 初期状態 s_0
Fig. 1 Initial state s_0

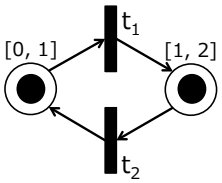

図 2 目的状態 s_R
Fig. 2 Object state s_R

4. 適 用 例

図 1 の TPN に対してから図 2 のマーキング s_R への到達不可能性の検証を行った結果を示す. 充足可能性判定および補間の生成は SMTInterpol[3] を用いる. まず，$k = 1$ のとき BMC^k，$PREF$，$SUFF^k$ は以下のようになる.

$$\begin{aligned}BMC^1 &= PREF \wedge SUFF^1 \\ PREF &= I(s_0) \wedge T(s_0, d_1, s_R) \\ &= I(s_0) \wedge C(s_0, d_1, s_1) \\ &\quad \wedge F_{t_1}(s_1, s_2) \wedge F_{t_2}(s_2, s_R) \\ SUFF^1 &= R(s_R)\end{aligned}$$

結果として BMC^1 は充足不能となり，補間 $Inter = \neg m_2$ が得られた.BMC^1 を

$$BMC^{1'} = Inter(s_0) \wedge T(s_0, d_1, s_R) \wedge R(s_R)$$

に置換して再度検証すると，$BMC^{1'}$ は充足不能となり，得られた補間は $\neg m_2$ となる. これは $Inter(s_0)$ と同値となる. したがって，s_0 から到達可能な全状態を表す論理式として $Inter(s_0)$ が得られたこととなり，s_0 から s_R へは到達不可能であることが示される.

5. お わ り に

本論文では補間に基づく非有界モデル検査を TPN へと適用するためのアプローチについて示した. 今後の課題は提案法の実装および大規模な TPN に対する適用実験である.

参 考 文 献

1) T.Yokogawa et al.: Bounded model cheking of Time Petri Nets using SAT solver， IEICE Electronics Express， vol.12， no.2， pp.1-7， 2015.
2) T.Matsuo et al.，: Feature Interaction Verification Using Unbounded Model Checking with Interpolation，IEICE TRANS. INF. & SYST.，vol. E92-D， no.6， pp. 1250-1259， 2009.
3) SMTInterpol，https://ultimate.informatik.uni-freiburg.de/smtinterpol/