MathSAT を用いた safe Time Petri Net の非有界モデル検査手法

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]

概要：本論文では， TPN の時間制約を差分論理によって表現することで，充足可能性判定に基づく非有界モデル検査を高速化するための手法を提案する．

1. まえがき

大規模な非同期システムの性能評価は時間ペトリネット (TPN) によるモデルにシミュレーションを実施することで行われる．性能評価は，TPN がシステムを正しくモデル化しているか検証する必要がある．

本論文では，論理式の充足可能性判定に基づく形式検証手法の一つである非有界モデル検査を用いて TPN の検証を行うための手法について述べる．

2. TPN の非有界モデル検査

2.1 TPN

TPN はペトリネットに遅延を導入したモデルである．本論文では，TPN のサブクラスの一つで，プレイス遅延を導入した P-TPN を検証の対象とする．$P\text{-}TPN = (P, T, F, F_{in}, M_0, X)$ はプレイスの集合 P，トランジションの集合 T，それらを接続するアークの集合 $F \subseteq (P \times T) \cup (T \times P)$, 抑止アークの集合 $F_{in} \subset F$, 初期マーキング $M_0 \subseteq P$, プレイス遅延 $X : P \to (Z^+) \times (Z^+ \cup +inf)$ によって定義される．

$t \in T$ へのアークをもつプレイスを t の入力プレイス，t からのアークをもつプレイスを t の出力プレイスといい，それぞれ $\bullet t$, $t\bullet$ と記す．TPN の状態は，プレイスへのトークンの割当てで表現され，これをマーキングという．プレイスが獲得したトークンが有効になるまでの時間は，定められたプレイス遅延によって決定される．$p_i \in P$ の遅延は関数 X によって下限 l_i と上限 u_i の組として与えられる．トークンは獲得後， l_i から u_i の時間が経過するまでに有効となり，すべての入力プレイスのトークンが有効となったときトランジションは発火し，出力プレイスへとトークンが移動する．また，抑止アークからの入力プレイスを抑止プレイスといい，$\circ t$ と記す．抑止プレイスが有効なトークンをもつとき，トランジションの発火が抑制される．

2.2 有界モデル検査

TPN の状態 s は，プレイスのベクトル表現 $\mathbf{p} = (p_1, \cdots, p_l)$ に対する二つの l 次ベクトル $\mathbf{m} = (m_1, \cdots, m_l)$ および $\mathbf{x} = (x_1, \cdots, x_l)$ から定義される $(l = |P|)$．m_i は p_i がトークンをもつとき真となる二値変数であり，x_i は p_i が獲得したトークンの経過時間を表す変数である．ここで，t の発火により状態 s から s' へと遷移することを $s \xrightarrow{t} s'$ と記し，時間 x の経過で状態 s から s' に遷移することを $s \xrightarrow{x} s'$ と記す．状態 s がある集合 S に属しているときかつそのときのみ真となる二値関数 $\mathcal{S}(s)$ を S の特性関数という．同様に，遷移関係の特性関数も，状態 s から s' へ遷移するときかつそのときのみ真となる二値関数 $\mathcal{T}(s, s')$ として定義できる．

有界モデル検査では，論理式 $\mathcal{N}_k \wedge \mathcal{R}_k$ の充足可能性判定として特性検証を実現する．初期状態の特性関数を I とすると，$\mathcal{N}_k = I(s_0) \wedge \mathcal{T}(s_0, s_1) \wedge \cdots \wedge \mathcal{T}(s_{k-1}, s_k)$ は初期状態 s_0 から s_k に k ステップで到達することを表す特性関数であり，また，$\mathcal{R}_k$ は $s_1, \cdots, s_k$ のいずれかの状態で与えられた特性が満たされることを表す特性関数である．ここで，時間の経過およびトランジション発火による状態の変化をステップと呼ぶことにする．もし，$\mathcal{N}_k \wedge \mathcal{R}_k$ が充足可能なら，初期状態から k ステップ以内で特性が満たされることが証明される．

2.3 非有界モデル検査

有界モデル検査では k ステップ以内到達可能な状態の

[†1] 現在，岡山県立大学
Presently with Okayama Prefectural University
[†2] 現在，川崎医療福祉大学
Presently with Kawasaki University of Medical Welfare

探索を行うため，安全性のように全状態の探索が必要となる特性は検証できない．非有界モデル検査では，論理式が充足不能と判定されたときに副次的に得られる補間論理式 (interpolant) を用いて状態空間を上方近似することで，全探索を実現する．補間論理式 P は，二つの論理式 A，B に対して，$A \wedge B$ が充足不能のとき得られる論理式で，(1) $P \wedge B$ が充足不能，(2) $A \rightarrow P$，(3) P は A と B に共通の変数のみをもつ，という 3 つの条件を満たすものである．ここで，$A = I(s_0) \wedge \mathcal{T}(s_0, s_1)$，$B = \mathcal{T}(s_1, s_2) \wedge \cdots \wedge \mathcal{T}(s_{k-1}, s_k) \wedge \mathcal{R}_k$ とおくと，補間論理式 P として，初期状態から 1 ステップで到達可能な状態の上方近似集合を求められる．この P を I と置き換えて充足可能性判定を繰り返すことで探索空間を拡張し，求める状態への到達不可能性 (安全性) を検証することが可能となる．

3. 非有界モデル検査の高速化

3.1 差分論理

差分論理は線形制約の部分論理であり，各制約を変数 x, y と定数 c に対して，$x - y \bowtie c$ ($\bowtie$ は等・不等号) という形に限定したものである．差分論理は重み付きの有向グラフにおける負閉路の探索として解の有無が判定でき，高速な処理が可能となる．

提案手法では，TPN の状態 s を $\mathbf{m}$ と $\mathbf{x}$，そして大域的な時刻を表す変数 c によって定義する．x_i には p_i がトークンを獲得した時点での c の値が格納される．これにより，プレイス遅延による時間の経過は $x' = x \wedge c' - c > 0$ という差分論理上の不等式として表現できる．

3.2 差分論理を用いた TPN の論理式表現

1 ステップを表す特性関数 $\mathcal{T}(s, s')$ は，時間経過を表す論理式 C とトランジションの発火を表す論理式 F の論理積として以下の通り定義できる．

$$\mathcal{T}(s, s') \stackrel{\text{def}}{=} C(s, s'') \wedge F(s'', s').$$

状態 s で t が発火可能および発火不能であることを表す特性関数 $En_t(s)$ および $Ds_t(s)$ は以下のように定義される．

$$En_t(s) \stackrel{\text{def}}{=} \bigwedge_{p_i \in {}^\bullet t} (m_i \wedge u_i \leq c - x_i) \wedge \bigwedge_{p_i \in t^\circ} \neg(m_i \wedge l_i \leq c - x_i).$$

$$Ds_t(s) \stackrel{\text{def}}{=} \bigvee_{p_i \in {}^\bullet t} \neg(m_i \wedge l_i \leq c - x_i) \vee \bigvee_{p_i \in t^\circ} (m_i \wedge u_i \leq c - x_i).$$

TPN では，発火可能なトランジションは時間経過無く発火するため，C は以下のように定義される．

$$C(s, s') \stackrel{\text{def}}{=} \bigwedge_{t \in T} \neg En_t(s) \wedge \bigwedge_{p_i \in P} (x'_i = x_i \wedge m'_i \leftrightarrow m_i)$$
$$\wedge (c' - c > 0) \vee \bigwedge_{p_i \in P} (x'_i = x_i \wedge m'_i \leftrightarrow m_i) \wedge (c' - c = 0).$$

ここで，m'_i および x'_i は，状態 s' における m_i および x_i の値を表す変数である．

$s \xrightarrow{t} s'$ または $s = s'$ であることを表す特性関数を $F_t(s, s')$ とすると，F は以下のように定義される ($n = |T|$)．

$$F(s, s') \stackrel{\text{def}}{=} F_{t_1}(s, s_1) \wedge \cdots \wedge F_{t_n}(s_{n-1}, s').$$

そして，$F_t(s, s')$ は以下のように定義される．

$$F_t(s, s') \stackrel{\text{def}}{=} \neg Ds_t(s) \wedge \bigwedge_{p_i \in t^\bullet} (m'_i \wedge x'_i = c) \wedge (c' - c = 0)$$
$$\wedge \bigwedge_{p_i \in {}^\bullet t \setminus t^\bullet} (\neg m'_i \wedge x'_i = x_i) \wedge \bigwedge_{p_i \in P \setminus ({}^\bullet t \cup t^\bullet)} (m' \leftrightarrow m_i \wedge x'_i = x_i)$$
$$\vee \bigwedge_{p_i \in P} (x'_i = x_i \wedge m'_i \leftrightarrow m_i) \wedge (c' - c = 0).$$

以上のように求めた $\mathcal{T}(s, s')$ と $I(s)$ を用いて $\mathcal{N}_k$ を求めることができる．

定義より $\mathcal{T}(s, s')$ は $s = s'$ でも真となるため，求める特性を満たす状態の特性関数が $R(s)$ ならば，$\mathcal{R}_k \stackrel{\text{def}}{=} R(s_{k(n+1)})$ と定義される．例えば，求める特性がデッドロック状態とすると，特性関数 $R_d(s)$ は以下のように定義できる．

$$R_d(s) \stackrel{\text{def}}{=} \bigwedge_{t \in T} \neg En_t(s) \wedge \bigwedge_{p_i \in P} (m_i \rightarrow u_i \leq c - x_i).$$

表 1 非有界モデル検査の実行時間

ステップ数	補間回数	時間 (sec.) 従来表現	時間 (sec.) 提案表現
1	1	0.05	0.50
	2	0.52	0.47
2	1	0.10	0.09
	2	2.20	0.10
	3	—	2.10
3	1	0.24	0.20
	2	0.29	0.18
	3	5.30	0.25
	4	—	5.80
4	1	0.47	0.28
	2	0.32	8.00
	3	7.30	—
5	1	0.39	0.42
	2	0.55	0.69
	3	19.00	16.00
6	1	0.96	0.60
	2	0.69	0.90
	3	1.00	1.10
	4	1.60	0.60
総実行時間 (sec.)		40.97	38.28

4. 評価実験

$|P| = 26$, $|T| = 18$ の TPN に対して非有界モデル検査を適用し，比較実験を行った．充足可能性判定には MathSAT を用いている．実験結果を表 1 に示す．提案手法では，より短い時間で検証が終了したことが示されている．

5. あとがき

本論文では，TPN を対象とした非有界モデル検査の高速化を指向した論理式表現を提案し，従来表現との比較実験を通してその効果を示した．今後の課題としてより規模の大きな TPN への適用実験と既存の検証ツールとの比較実験が挙げられる．