情報処理学会論文誌 Vol.59 No.9 1749–1760 (Sep. 2018)

SAT技術を用いたペトリネットのデッドロック検出手法の提案

寸田 智也[1] 宋 剛秀[2] 番原 睦則[2] 田村 直之[2,a)] 井上 克巳[3]

受付日 2017年12月19日, 採録日 2018年6月8日

概要：本論文では，トークン数が整数値である一般のペトリネットを対象とし，そのデッドロック検出についてSAT技術を用いた手法を提案する．提案手法では，非負整数値であるトークン数を表現するために順序符号化を採用することで，既存のSAT型手法では対応できなかった一般のペトリネットでのデッドロック検出を実現した．また，既存SAT型手法で採用されていたモデル（連続発火モデルと呼ぶ）よりも短いステップ長でデッドロック検出が可能となる多重発火モデルを提案し，性能向上を実現した．評価実験では，Model Checking Contest 2017のベンチマーク問題を用いて，連続発火モデルと多重発火モデルを比較した．ほぼすべての問題で多重発火モデルのほうが優れていたが，特に初期マーキングのトークン数が比較的多い問題に対する効果が大きかった．また，Model Checking Contest 2017デッドロック検出部門での優勝ソルバLoLAおよび準優勝ソルバTapaalとの比較を行った．提案手法は，デッドロックを検出できた問題数ではLoLA，Tapaalより少なかったが，LoLAおよびTapaalを含めたすべてのソルバがデッドロック検出に失敗した問題での検出に成功し，提案手法の有効性が確認できた．

キーワード：ペトリネット，デッドロック検出，SAT技術，有界モデル検査

Proposal of SAT-based Method to Detect Deadlock of Petri Nets

Tomoya Sunda[1] Takehide Soh[2] Mutsunori Banbara[2] Naoyuki Tamura[2,a)] Katsumi Inoue[3]

Received: December 19, 2017, Accepted: June 8, 2018

Abstract: In this paper, we propose a SAT-based method to detect deadlock of general Petri nets in which more than one tokens are allowed for each place. In our approach, the transition relation of a Petri net is represented as constraints on integers and they are translated into SAT by order encoding, so that the deadlock of general Petri nets can be detected by a SAT solver, while existing SAT-based methods cannot be applied for them. Furthermore, in order to improve the performance, we introduced multiple firing model, which can detect deadlock with shorter steps than the model used in an existing SAT-based method, called successive firing model. We evaluated the successive firing model and the multiple firing model through a benchmark set of Model Checking Contest 2017. The multiple firing model showed better performance for almost all instances, and was especially effective for the instances in which there are many tokens at the initial marking. Through the comparison with the winner tool LoLA and the second place tool Tapaal of the contest, although the number of detected deadlocks are fewer than LoLA and Tapaal, we confirmed the effectiveness of the proposed method with some instances for which all tools including LoLA and Tapaal failed to detect deadlock.

Keywords: Petri nets, deadlock detection, SAT technologies, bounded model checking

1. はじめに

C.A. Petriによって提唱されたペトリネットは，コンピュータ・通信システムなどの並行的，非同期的，分散的，非決定的な動作のモデルであり，一般的な情報・制御システムの記述・設計・解析・検証に有用である[18]．本論文で対象とするデッドロックの検証を含め，その検証は重要な研究課題となっている．2011年からペトリネット

[1] 神戸大学大学院システム情報学研究科
Graduate School of System Informatics, Kobe University, Kobe, Hyogo 657–8501 Japan
[2] 神戸大学情報基盤センター
Information Science and Technology Center, Kobe University, Kobe, Hyogo 657–8501 Japan
[3] 国立情報学研究所情報学プリンシプル研究系
Principles of Informatics Research Division, National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
[a)] tamura@kobe-u.ac.jp

の検証を行うソフトウェアに関する国際コンテスト Model Checking Contest [*1] [8], [13] が毎年開催されている．

Model Checking Contest に参加したソルバの手法は明示的モデル検査（explicit model checking）と記号的モデル検査（symbolic model checking）に分類できる [13]．明示的モデル検査にはマーキンググラフ法などがあり，ペトリネットの状態そのものを取り扱っている．ソルバには，Model Checking Contest 2017 Reachability 部門で優勝した LoLA [27] や 2 番目に結果が良かった Tapaal [11] などがある．一方，記号的モデル検査では命題変数などを用いてペトリネットの状態が記号的に表され，二分決定グラフ（Binary Decision Diagram; BDD）や本論文でも使用する SAT ソルバなどが利用されている．決定グラフを用いたソルバには ITS-Tools [26]，MARCIE [7] などがあり，SAT ソルバを用いたものには Cunf [19] や文献 [17] がある．

命題論理の充足可能性判定（Satisfiability testing; **SAT**）は，与えられた命題論理式が真になる値割当てが存在するかどうかを判定する問題である [1], [9]．与えられた SAT 問題を解くプログラムである **SAT ソルバ**の性能が近年飛躍的に向上し [14], [15], [16]，システム検証 [2], [3], [4] を含め多くの分野への応用が広がっている．ペトリネットのデッドロック検証への応用も存在するが [17], [19]，SAT ソルバでは直接的には整数変数を扱うことができないため，これらでは各プレイスのトークン数が 1 以下の**安全ペトリネット**のみが対象となっていた．

そこで本論文では，SAT ソルバを用いて，トークン数が非負整数値である**一般のペトリネットでのデッドロック検出**を行う方法を提案する．

しかし，ペトリネットのモデルを単純に SAT 問題に変換（**SAT 符号化**という）した場合，デッドロック検出までのステップ長が長くなると，SAT 符号化の結果である命題論理式のサイズが大きくなりすぎ，SAT ソルバでの求解が行えないという問題点が生じる．そこで，本論文では，デッドロック検出までのステップ長を短くするための工夫として，複数回トランジションが発火する遷移を許すモデル（**多重発火モデル**と呼ぶ）を導入した．すなわち，本論文で提案する手法の特徴は以下のとおりである．

(1) SAT ソルバによる一般のペトリネットでのデッドロック検出の実現．
非負整数値であるトークン数を表現するために**順序符号化** [23], [24] を用い，ペトリネットの可達性を命題論理式の充足可能性として表現する．これにより，既存の SAT 型手法である文献 [17], [19] では対応できなかった一般のペトリネットでのデッドロック検出が可能となった．

(2) SAT ソルバによる効率良いデッドロック検出を可能とするための多重発火モデルの導入．
既存の SAT 型手法である文献 [17] で採用されていたモデル（連続発火モデルと呼ぶ）よりも短いステップ長でデッドロック検出が可能となるモデルを提案した．これにより全般に性能が向上したが，特にトークン数が比較的多い問題に対する効果が大きいことが分かった．

以下，2 章でペトリネットとそのデッドロックを定義し，3 章で本論文で利用する SAT 技術について説明する．4 章では提案する多重発火モデルを導入する．まず，安全ペトリネットを対象とした既存 SAT 型手法を一般のペトリネットに拡張した連続発火モデルを述べ，さらに多重発火モデルに拡張する．次に 5 章で多重発火モデルの SAT 符号化方法について説明し，6 章で SAT 型手法の実装方法を述べる．7 章では，Model Checking Contest 2017 のベンチマーク問題を用い，実装した 2 種類の手法および既存手法の比較実験を行い，提案手法について評価する．最後に，8 章で結論を述べる．

2. ペトリネットとデッドロック

$\mathbb{N}$ で 0 以上の整数の集合を表す．ペトリネットは，組 $(\mathbf{P}, \mathbf{T}, F, M_0)$ で与えられる [18]．ここで，$\mathbf{P}$ は**プレイス**の有限集合，$\mathbf{T}$ は**トランジション**の有限集合，$F : (\mathbf{P} \times \mathbf{T}) \cup (\mathbf{T} \times \mathbf{P}) \to \mathbb{N}$ は**アーク**の多重度（アークがない場合は 0）を与える関数，$M_0 : \mathbf{P} \to \mathbb{N}$ は初期**マーキング**である．ペトリネットの状態は，各プレイスでの**トークン**の個数で定まり，マーキング $M : \mathbf{P} \to \mathbb{N}$ により表される．また，$\bullet p$ でプレイス p の入力トランジションの集合，$p\bullet$ で出力トランジションの集合，$\bullet t$ でトランジション t の入力プレイスの集合，$t\bullet$ で出力プレイスの集合を表す．**図 1** にペトリネットの例を示す．ただし，アークの多重度が 1 の場合，その記載を省略している．

ペトリネットはトランジションの**発火**により次のマーキングへと遷移する．トランジション t はすべての入力プレイスが対応するアークの多重度以上のトークンを持つときのみ発火可能となる．t の発火でマーキング M から M' に遷移することを $M \xrightarrow{t} M'$ で表す．$M \xrightarrow{t} M'$ は以下のように定義できる．

$$M \xrightarrow{t} M' \overset{\text{def}}{\Longleftrightarrow} \forall p \in \mathbf{P}\ (M(p) \geq F(p,t) \wedge M'(p) = M(p) + F(t,p) - F(p,t)) \quad (1)$$

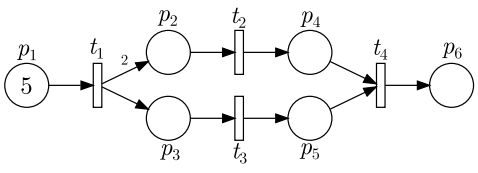


図 1 ペトリネットの例
Fig. 1 Example of a Petri net.

[*1] http://mcc.lip6.fr

また，$M \to M'$ を以下のように定義し，これを標準遷移あるいは $\to$ 遷移と呼ぶ．

$$M \to M' \overset{\text{def}}{\Longleftrightarrow} \exists t \in \mathbf{T}\ (M \xrightarrow{t} M') \tag{2}$$

初期マーキング M からマーキング M' へ遷移可能であるようなトランジションの発火系列が存在するとき，マーキング M' は M から**可達**であるといい，$M \to^* M'$ で表す．すなわち，$\to^*$ は $\to$ の反射的推移的閉包であり，$M = M'$ の場合も含む．

デッドロックとは，すべてのトランジションが発火可能でないようなマーキングを意味する．デッドロックが初期マーキングから可達であるとき，そのペトリネットはデッドロックを持つという．ペトリネットがデッドロックを持つことは以下のように表せる．

$$\exists M\,(M_0 \to^* M \wedge \forall t \in \mathbf{T}\, \exists p \in {\bullet t}\,(M(p) < F(p,t)) \tag{3}$$

3. 利用する SAT 技術

以下では，本論文で利用する SAT 技術について述べる．

3.1 SAT ソルバとインクリメンタル SAT 解法

SAT ソルバに与える命題論理式は，**連言標準形**（Conjunctive Normal Form; CNF）で記述する必要がある [1], [9]．連言標準形の式（**CNF 式**）は，複数の**節**の連言（AND）であり，各節は複数の**リテラル**の選言（OR）である．各リテラルは，命題変数あるいは命題変数の否定である．

SAT ソルバは，与えられた CNF 式が充足可能（SAT）か充足不能（UNSAT）かを判定し，充足可能ならその値割当てを出力する．近年の SAT ソルバは，求解過程で発生する矛盾から得られる**学習節**を利用して探索の枝刈りを行う CDCL アルゴリズムなどの高速化技術が取り入れられており，その性能は飛躍的に向上している [15], [16]．

また，本論文で使用する GlueMiniSat [14] を含め多くの SAT ソルバは**インクリメンタル SAT 解法**と呼ばれる方法に対応している [5]．インクリメンタル SAT 解法では，SAT ソルバを起動したまま，関連した複数の SAT 問題を連続して解くことが可能になる．したがって，SAT ソルバが獲得した学習節が保持され，効率良い解探索が実現できる．本論文では，文献 [20] で提案された iSAT Library [*2] を用い，インクリメンタル SAT 解法を導入する．

3.2 SAT 符号化

与えられた制約をすべて満たすことができるような変数の値の割当てが存在するかどうかを判定する問題を**制約充足問題**（Constraint Satisfaction Problem; CSP）という．特に，制約中に現れる変数が有限範囲の整数値だけをとる CSP を有限領域 CSP という．後述のように，ペトリネットのステップ長およびトークン数などの上限が与えられた場合，その範囲内でデッドロックが生じるかどうかは，有限領域 CSP の充足可能性の判定問題として定式化できる．

有限領域 CSP については，与えられた問題を SAT 問題に符号化する手法が活発に研究開発されている [25]．特に，加減乗除などの演算が含まれている制約に対しては，順序符号化 [23], [24] が有効であることが知られている [12]．順序符号化では，整数変数 x とそのとりうる値 a に対し，$x \le a$ を意味する 1 つの命題変数を割り当てる．とりうる値が d 個であるような整数変数を符号化した結果の節数は $O(d)$ であり，2 変数を含む制約（たとえば $x \ge y$）に対する節数は $O(d)$，3 変数を含む制約（たとえば $z \ge x + y$）に対する節数は $O(d^2)$ となる．順序符号化では整数変数のとりうる範囲の推論が SAT ソルバの単位伝播で実現されており，他の SAT 符号化より高速な実行が可能である [25]．実際に，順序符号化を採用した **SAT 型制約ソルバ**である Sugar [*3] [24] は，ショップ・スケジューリング問題および 2 次元ストリップパッキング問題で未知だった最適値決定に成功するなど，多くの問題に対し有望な手法であることが示されている．

3.3 有界モデル検査

SAT ソルバを用いて動的なシステムの検証を行う手法として，**有界モデル検査**（Bounded Model Checking; BMC）[2], [3], [4] がある．この方法では，システムにおける状態遷移の**ステップ長**の上限 k を与え，時刻 0 から時刻 k までの状態遷移の系列 $M_0 \to M_1 \to \cdots \to M_k$ において，ある性質 P を満たす状態 M_i が存在するかどうかを SAT ソルバを用いて判定する．有界モデル検査は，特にハードウェアの検証において，それまで用いられていた BDD による方法より，大規模な問題に対処可能な手法として有効性が示されている [4]．

今，状態 M_0 が初期状態であることを式 $I(M_0)$ で，状態 M_i から M_{i+1} への遷移関係を式 $T(M_i, M_{i+1})$ で，状態 M_i が性質 P を満たすことを式 $P(M_i)$ で表すと，上記の系列の存在は

$$I(M_0) \wedge \bigwedge_{i=0}^{k-1} T(M_i, M_{i+1}) \wedge \bigvee_{i=0}^{k} P(M_i)$$

という式の充足可能性判定問題と同等になる．すなわち，上記を CNF 式として表したものが SAT であれば時刻 k までに性質 P を満たす状態が存在し，UNSAT であれば存在しない．

有界モデル検査では，ステップ長の上限 k の値を徐々に増やしながら判定することが通常である．このとき，前述のインクリメタル SAT 解法と組み合わせることで，性能

[*2] http://bach.istc.kobe-u.ac.jp/iSATLib/

[*3] http://bach.istc.kobe-u.ac.jp/sugar/

が向上することが知られている [5]．本論文でも，前述の GlueMiniSat および iSAT Library を用い，インクリメンタル SAT 解法を導入した有界モデル検査を実現する．

4. 多重発火モデルの提案

本章では，安全ペトリネットを対象とした既存 SAT 型手法を一般のペトリネットに拡張した連続発火モデルを述べ，さらに多重発火モデルに拡張する．

4.1 連続発火モデル

ペトリネットのデッドロック検出に関し，SAT 技術を用いた既存手法として Ogata らの方法 [17] がある．各プレイスのトークン数が 1 以下である安全ペトリネットだけを対象としているが，そのアイデアは一般のペトリネットに適用できる．ここでは，それを**連続発火モデル**と呼ぶ．連続発火モデルを用いると，標準遷移を用いた場合に比べてかなり短いステップ長でデッドロックを検出することが可能になる．

連続発火モデルでは，トランジションの順序を定める必要がある．すなわち，$l = |\mathbf{T}|$ とし，トランジションを適当な順序で並べたものを $t_1, t_2, \ldots, t_l$ とする．この順序は任意でよいが，たとえば，6.1 節で述べるようにペトリネット内のプレイスを深さ優先でたどった順序が考えられる．

このとき，$M \xrightarrow{t} M'$ を以下のように定義する．

$$M \xrightarrow{t} M' \overset{\text{def}}{\Longleftrightarrow} (M \xrightarrow{t} M') \vee (M = M') \tag{4}$$

さらに，$M \to_c M'$ をマーキング M から M' への連続発火遷移あるいは $\to_c$ 遷移と呼び，以下のように定義する．

$$M \to_c M' \overset{\text{def}}{\Longleftrightarrow} M = M_0 \xrightarrow{t_1} M_1 \xrightarrow{t_2} \cdots \xrightarrow{t_l} M_l = M' \tag{5}$$

すなわち，$\to_c$ 遷移では，その中で複数の別々のトランジションが連続して発火することが許されている．

可能な $\to_c$ 遷移の例を**図 2** に示す．トランジションの順序は t_1，t_2 としている．まず，左端のマーキング $(p_1, p_2, p_3, p_4) = (1, 0, 0, 0)$ で t_1 は発火可能だから，$\xrightarrow{t_1}$ により $(0, 1, 1, 0)$ または $(1, 0, 0, 0)$ に遷移できる．次に $(0, 1, 1, 0)$ で t_2 は発火可能だから $(0, 1, 0, 1)$ または $(0, 1, 1, 0)$ に遷移する．一方で $(1, 0, 0, 0)$ では t_2 は発火できないから，$\xrightarrow{t_2}$ により $(1, 0, 0, 0)$ にのみ遷移する．すなわち，マーキング $(1, 0, 0, 0)$ から可能な $\to_c$ 遷移先は，右端に示す $(0, 1, 0, 1)$，$(0, 1, 1, 0)$，$(1, 0, 0, 0)$ の 3 通りになる．

$\to_c{}^*$ を $\to_c$ の反射的推移的閉包とする．明らかに $M \to^* M'$ と $M \to_c{}^* M'$ は同値であり，可達性は変わらない．また，M から k ステップの $\to$ 遷移で M' へ到達できるとき，k ステップ以下の $\to_c$ 遷移で到達できる．

図 1 に示したペトリネットについて，標準遷移と連続発火のそれぞれに対し，デッドロック検出に必要なステップ長の違いを示す．初期マーキングは $(p_1, p_2, p_3, p_4, p_5, p_6) = (5, 0, 0, 0, 0, 0)$ である．

標準遷移を用いた場合，各ステップで 1 つのトランジションしか発火できない．したがって，まず t_1 が発火する $\to$ 遷移を 5 回繰り返して $(0, 10, 5, 0, 0, 0)$ に遷移した後，10 回の t_2 発火と 5 回の t_3 発火，さらに 5 回の t_4 発火を経てデッドロック $(0, 0, 0, 5, 0, 5)$ に遷移する．すなわち，合計で 25 ステップが必要となる．

一方，連続発火モデルでトランジションの順序を t_1，t_2，t_3，t_4 とした場合，最初の $\to_c$ 遷移中で t_1，t_2，t_3，t_4 の順に発火することにより，1 ステップでマーキング $(4, 1, 0, 0, 0, 1)$ に遷移できる．その後，$(3, 2, 0, 0, 0, 2) \to_c (2, 3, 0, 0, 0, 3) \to_c \cdots \to_c (0, 0, 0, 5, 0, 5)$ と遷移することにより，合計 9 ステップでデッドロックの検出が可能である．

後述の 5.5 節で述べるように，$\to$ と $\to_c$ を SAT 符号化した場合の節数はほぼ同等である．したがって，デッドロック検出に必要なステップ数が大幅に短くなる連続発火モデルのほうが優れていると考えられる．

4.2 多重発火モデル

同じトランジションが，連続して複数回発火することを

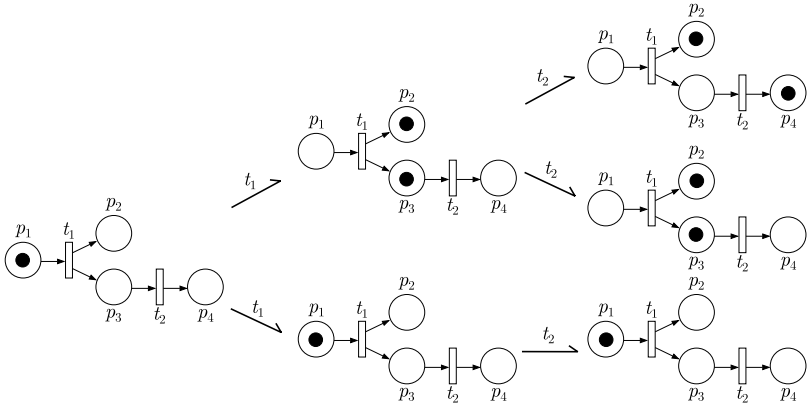


図 2 可能な $\to_c$ 遷移の例
Fig. 2 Example of possible $\to_c$ transition.

多重発火と呼ぶ．連続発火モデルの遷移 $M \xrightarrow{t} M'$ において，t の多重発火を認めた**多重発火モデル**を導入する．多重発火モデルでは，連続発火モデルよりさらに短いステップ長でデッドロックに到達できる．なお，以下では連続発火モデルと同様にトランジションの順序を $t_1, t_2, \ldots, t_l$ のように定める．

マーキング M から t が n（$n \geq 0$）回発火して M' に遷移することを $M \xrightarrow{t^n} M'$ で表し，以下のように定義する．

$$M \xrightarrow{t^n} M' \overset{\text{def}}{\Longleftrightarrow} \forall p \in \mathbf{P}\ (M(p) \geq nF(p,t) \wedge M'(p) = M(p) + n(F(t,p) - F(p,t))) \quad (6)$$

また，$M \to_m M'$ をマーキング M から M' への多重発火遷移あるいは $\to_m$ 遷移と呼び，以下のように定義する．

$$M \to_m M' \overset{\text{def}}{\Longleftrightarrow} \exists n_1, n_2, \ldots, n_l \in \mathbb{N}\ (M = M_0 \xrightarrow{t_1^{n_1}} M_1 \xrightarrow{t_2^{n_2}} \cdots \xrightarrow{t_l^{n_l}} M_l = M') \quad (7)$$

$n_j = 0$ の場合には $M_{j-1} = M_j$ となることに注意すると，$\to_m$ 遷移中の各 t_j の多重発火回数 n_j を 1 以下に制限した場合，連続発火での $\to_c$ 遷移に相当することが分かる．

$\to_m{}^*$ を $\to_m$ の反射的推移的閉包とする．明らかに $M \to_m{}^* M'$ は，$M \to^* M'$ および $M \to_c{}^* M'$ と同値であり，可達性は変わらない．また，M から k ステップの $\to_c$ 遷移で M' へ到達できるとき，k ステップ以下の $\to_m$ 遷移で到達できる．

図 1 に示したペトリネットについて，連続発火モデルと多重発火モデルの各々に対し，デッドロック検出に必要なステップ長を示す．なお，トランジションの順序は t_1，t_2，t_3，t_4 の順とする．また，初期マーキングは $(p_1, p_2, p_3, p_4, p_5, p_6) = (5, 0, 0, 0, 0, 0)$ である．

連続発火モデルの場合，前述のように合計 9 ステップが最短である．

一方，多重発火モデルの場合，最初の $\to_m$ 遷移で $t_1^5, t_2^{10}, t_3^5, t_4^5$ の発火により，1 ステップでデッドロック $(0, 0, 0, 5, 0, 5)$ に遷移できる．なお，トランジションの順序を t_1，t_2，t_4，t_3 とした場合には，最短で 2 ステップが必要となる．このように，トランジションの順序に依存して変化するが，連続発火モデルよりかなり短いステップ長でデッドロックに到達することが可能になる．

5. 多重発火モデルの SAT 符号化

Sugar などの既存の SAT 型制約ソルバの利用を前提とすると，多重発火モデルの SAT 符号化には，$\to_m$ 遷移やデッドロックの条件などを有限領域 CSP の制約として記述すれば十分であり，その後の SAT 符号化自体は SAT 型制約ソルバに行わせることが可能である．そのため，ここでは対応する制約の説明を中心に行う．

5.1 整数変数の導入と初期マーキングの制約

多重発火モデルでの状態遷移の系列 $M_0 \to_m M_1 \to_m \cdots \to_m M_k$ において，各 $\to_m$ は，さらにトランジション $t_1, t_2, \ldots, t_l$ に対する遷移 $\xrightarrow{t_j^{n_j}}$ の列である（$n_j \geq 0$）．すなわち遷移 $M_i \to_m M_{i+1}$ は，$M_i = M_{i,0}$ および $M_{i+1} = M_{i,l}$ とすると，遷移の系列

$$M_{i,0} \xrightarrow{t_1^{n_{i,1}}} M_{i,1} \xrightarrow{t_2^{n_{i,2}}} \cdots \xrightarrow{t_l^{n_{i,l}}} M_{i,l}$$

として表現できる．

そこで，制約で使用する整数変数を以下のように導入する．

$$\begin{aligned} &m_p^{il+j} \quad (p \in \mathbf{P},\ 0 \leq i < k,\ 0 \leq j < l) \\ &m_p^{kl} \quad (p \in \mathbf{P}) \\ &f_t^i \quad (t \in \mathbf{T},\ 0 \leq i < k) \end{aligned} \quad (8)$$

ここで，変数 m_p^{il+j} および m_p^{kl} は上記の $M_{i,j}(p)$ に対応する．変数 $f_{t_j}^i$ は上記の $n_{i,j}$ に対応し，M_i から M_{i+1} への $\to_m$ 遷移中で t が多重発火する回数を表している．どちらも 0 以上の値をとるが，その上限の定め方については 6.3 節で述べる．なお，$f_{t_j}^i$ の上限を 1 に制限した場合，連続発火モデルに対応する．

このとき，M_0 すなわち $M_{0,0}$ が初期マーキングであるという条件 I は，以下のような制約で記述できる．

$$I \overset{\text{def}}{\Longleftrightarrow} \bigwedge_{p \in \mathbf{P}} m_p^0 = M_0(p) \quad (9)$$

5.2 $\to_m$ 遷移の制約

遷移 $M_{i,j-1} \xrightarrow{t_j^{n_{i,j}}} M_{i,j}$ は以下のような制約で表すことができる．

$$\begin{aligned} &m_p^{il+j-1} \geq F(p,t_j) f_{t_j}^i && (p \in {\bullet t_j}) \\ &m_p^{il+j} = m_p^{il+j-1} - F(p,t_j) f_{t_j}^i && (p \in {\bullet t_j} \backslash t_j{\bullet}) \\ &m_p^{il+j} = m_p^{il+j-1} + F(t_j,p) f_{t_j}^i && (p \in t_j{\bullet} \setminus {\bullet t_j}) \\ &m_p^{il+j} = m_p^{il+j-1} + (F(t_j,p) - F(p,t_j)) f_{t_j}^i && (p \in {\bullet t_j} \cap t_j{\bullet}) \\ &m_p^{il+j} = m_p^{il+j-1} && (p \in \mathbf{P} \backslash ({\bullet t_j} \cup t_j{\bullet})) \end{aligned} \quad (10)$$

これらはトランジション t_j が $n_{i,j}$ 回発火したときのマーキング $M_{i,j-1}$ と $M_{i,j}$ の関係を表している．1 行目により，$M_{i,j-1}$ で t_j が発火可能な最大回数以下の任意の値が $n_{i,j}$ に対して許され，特に 0 であれば発火しないことを意味する．

この制約 (10) を $T_{i,j}$ とおくと，$M_i \to_m M_{i+1}$ すなわち $M_{i,0} \to_m M_{i,l}$ に対する制約 T_i は以下のように表せる．

$$T_i \overset{\text{def}}{\Longleftrightarrow} \bigwedge_{j=1}^{l} T_{i,j} \quad (11)$$

ここで，変数 m_p^{il+j} は $|\mathbf{P}|\cdot k\cdot l$ 個が導入されている．しかし，$p\in\mathbf{P}\backslash(\bullet t_j\cup t_j\bullet)$ の場合，m_p^{il+j} と m_p^{il+j-1} は同じ値になる．そこで，これらを同じ変数と見なし m_p^{il+j} を m_p^{il+j-1} で置き換えれば省略することが可能である [17]．

以下に図 1 のペトリネットを例にとり，制約 T_0 を示す．

$$
\begin{aligned}
&m_{p_1}^0 \geq f_{t_1}^0, && m_{p_1}^1 = m_{p_1}^0 - f_{t_1}^0,\\
&m_{p_2}^1 = m_{p_2}^0 + 2f_{t_1}^0, && m_{p_3}^1 = m_{p_3}^0 + f_{t_1}^0,\\
&m_{p_2}^1 \geq f_{t_2}^0, && m_{p_2}^2 = m_{p_2}^1 - f_{t_2}^0,\\
&m_{p_4}^1 = m_{p_4}^0 + f_{t_2}^0, &&\\
&m_{p_3}^1 \geq f_{t_3}^0, && m_{p_3}^2 = m_{p_3}^1 - f_{t_3}^0,\\
&m_{p_5}^1 = m_{p_5}^0 + f_{t_3}^0, &&\\
&m_{p_4}^1 \geq f_{t_4}^0, && m_{p_4}^2 = m_{p_4}^1 - f_{t_4}^0,\\
&m_{p_5}^1 \geq f_{t_4}^0, && m_{p_5}^2 = m_{p_5}^1 - f_{t_4}^0,\\
&m_{p_6}^1 = m_{p_6}^0 + f_{t_4}^0 &&
\end{aligned}
$$

1，2 行目は $T_{0,1}$ すなわち $M_{0,0}\xrightarrow{t_1^{n_{0,1}}} M_{0,1}$ に対応する制約である．変数 m_p^0 はマーキング $M_{0,0}$ でのプレイス p のトークン数を表しており，変数 $f_{t_1}^0$ はトランジション t_1 の多重発火回数 $n_{0,1}$ を表している．以下 3，4 行目が $T_{0,2}$，5，6 行目が $T_{0,3}$，7 から 9 行目が $T_{0,4}$ に対応する制約である．

なお，この例で上記の変数の置き換えが行われている点に注意されたい．たとえば，$T_{0,1}$ に対し式 (10) をそのまま適用した場合，プレイス p_4 に関する制約 $m_{p_4}^1 = m_{p_4}^0$ が必要になる．これは，他の箇所で本来 $m_{p_4}^1$ である部分を $m_{p_4}^0$ で置き換えることで，省略することが可能である．

5.3 デッドロック検出の制約

マーキング M_i がデッドロックである条件は以下の制約 D_i で表現できる．

$$D_i \overset{\text{def}}{\Longleftrightarrow} \bigwedge_{t\in T}\bigvee_{p\in\bullet t}(m_p^{il} < F(p,t)) \tag{12}$$

ただし，トランジション t の入力プレイスの集合 $\bullet t$ が空の場合，$\bigvee_{p\in\bullet t}(m_p^{il} < F(p,t))$ は偽を表すとする．したがって，そのようなトランジションがあればデッドロックは生じない．多重発火モデルでの $\rightarrow_m$ 遷移はトランジションが 1 つも発火しない場合も含んでいる．すなわち，i ステップ目より前にデッドロックが発生する場合にも，D_i は充足可能となる．したがって，k ステップ目以内でデッドロックする条件は D_k として表せる．

以上で，デッドロック検出のための制約が得られた．多重発火モデルでの $\rightarrow_m$ 遷移のステップ長 k およびトークン数と多重発火回数の上限が与えられたとき，以下の制約は，その範囲内でデッドロックがあるとき，かつそのときに限り充足可能である．

$$I \wedge \bigwedge_{i=0}^{k-1} T_i \wedge D_k \tag{13}$$

5.4 SAT 符号化の例

制約 (13) を Sugar などの SAT 型制約ソルバに与えることで SAT 符号化は自動的に行える．したがって，ここでは簡単な例に対する順序符号化の結果のみを示す．たとえば，図 1 のペトリネットでの遷移 $M_{0,0}\xrightarrow{t_1^{n_{0,1}}} M_{0,1}$ で，プレイス p_1 に対する制約は以下のようになる．

$$m_{p_1}^0 \geq f_{t_1}^0, \qquad m_{p_1}^1 = m_{p_1}^0 - f_{t_1}^0$$

順序符号化では各変数 x と各値 a に対し，$x\leq a$ を意味する命題変数を導入する．今，トークン数および多重発火回数の上限を 3 とする．このとき，$m_{p_1}^0$ に対して $m_{p_1}^0\leq 0$，$m_{p_1}^0\leq 1$，$m_{p_1}^0\leq 2$ を表す 3 つの命題変数が導入される．また，制約 $m_{p_1}^0 \geq f_{t_1}^0$ の符号化で以下の 3 つの節が得られる．

$$\neg(m_{p_1}^0\leq 0)\vee(f_{t_1}^0\leq 0), \qquad \neg(m_{p_1}^0\leq 1)\vee(f_{t_1}^0\leq 1)$$
$$\neg(m_{p_1}^0\leq 2)\vee(f_{t_1}^0\leq 2)$$

これらは，それぞれ $m_{p_1}^0$ が a 以下ならば $f_{t_1}^0$ も a 以下であるという条件を表している．

制約 $m_{p_1}^1 = m_{p_1}^0 - f_{t_1}^0$ は $m_{p_1}^1 \geq m_{p_1}^0 - f_{t_1}^0$ と $m_{p_1}^1 \leq m_{p_1}^0 - f_{t_1}^0$ の 2 つの制約に分解され，各々が SAT 符号化される．$m_{p_1}^1 \geq m_{p_1}^0 - f_{t_1}^0$ に対する節は以下のようになる．

$$
\begin{aligned}
&(m_{p_1}^0\leq 0)\vee\neg(f_{t_1}^0\leq 0)\vee\neg(m_{p_1}^1\leq 0)\\
&(m_{p_1}^0\leq 1)\vee\neg(f_{t_1}^0\leq 0)\vee\neg(m_{p_1}^1\leq 1)\\
&(m_{p_1}^0\leq 1)\vee\neg(f_{t_1}^0\leq 1)\vee\neg(m_{p_1}^1\leq 0)\\
&(m_{p_1}^0\leq 2)\vee\neg(f_{t_1}^0\leq 0)\vee\neg(m_{p_1}^1\leq 2)\\
&(m_{p_1}^0\leq 2)\vee\neg(f_{t_1}^0\leq 1)\vee\neg(m_{p_1}^1\leq 1)\\
&(m_{p_1}^0\leq 2)\vee\neg(f_{t_1}^0\leq 2)\vee\neg(m_{p_1}^1\leq 0)
\end{aligned}
$$

たとえば 5 行目は，$f_{t_1}^0$ と $m_{p_1}^1$ が 1 以下ならば，$m_{p_1}^0$ は 2 以下であるという条件を表している．

5.5 SAT 符号化後の節数

ここでは，標準遷移 $\rightarrow$，連続発火モデルの $\rightarrow_c$ 遷移，多重発火モデルの $\rightarrow_m$ 遷移のそれぞれについて，SAT 符号化後の節数を評価する．ただし，簡単のためトークン数上限と多重発火回数上限をともに N とする．

まず，標準遷移 $\rightarrow$ は式 (1) と (2) で与えられる．式 (1) 中の $M(p)\geq F(p,t)$ に対する節数は $O(1)$ であり，$M'(p)=M(p)+F(t,p)-F(p,t)$ に対する節数は $O(N)$ であるから，式 (1) に対する節数は $O(|\mathbf{P}|\cdot N)$ となる．また，式 (2) は $|\mathbf{T}|$ 個の式 (1) の選言である．したがって，標準遷移 $M\rightarrow M'$ を SAT 符号化した節数は $O(|\mathbf{P}|\cdot|\mathbf{T}|\cdot N)$

となる．

次に，連続発火モデルの $\rightarrow_c$ 遷移は式 (4) と (5) で与えられる．式 (4) 中の $M \xrightarrow{t} M'$ に対する節数は $O(|\mathbf{P}|\cdot N)$ であり，$M = M'$ に対する節数は $O(|\mathbf{P}|\cdot N)$ であるから，式 (4) に対する節数は $O(|\mathbf{P}|\cdot N)$ となる．したがって，$M \rightarrow_c M'$ を SAT 符号化した節数は $O(|\mathbf{P}|\cdot|\mathbf{T}|\cdot N)$ となり，標準遷移の場合と同程度である．

最後に，多重発火モデルの $\rightarrow_m$ 遷移は式 (6) と (7) で与えられる．式 (6) 中の $M(p) \geq nF(p,t)$ に対する節数は $O(N)$ であり，$M'(p) = M(p) + n(F(t,p) - F(p,t))$ に対する節数は $O(N^2)$ であるから，式 (6) に対する節数は $O(|\mathbf{P}|\cdot N^2)$ となる．したがって，$M \rightarrow_m M'$ を SAT 符号化した節数は $O(|\mathbf{P}|\cdot|\mathbf{T}|\cdot N^2)$ となり，$M \rightarrow_c M'$ の場合の N 倍である．

このように 1 ステップあたりで見ると，$\rightarrow_m$ 遷移に対する節数は $\rightarrow_c$ 遷移より多くなるが，$\rightarrow_m$ 遷移ではデッドロック検出に必要なステップ長を抑えることができ，デッドロックの検出に必要な合計の節数では少なくなる可能性がある．

6. 多重発火モデルの SAT 解法の実装

前章で提案した多重発火モデルの制約では，トランジションの順序，トークン数および多重発火回数の上限が未定であり，実装においてはそれらを定める必要がある．また，3.3 節で述べたように，有界モデル検査では時刻 0 から時刻 k までの状態遷移の系列 $M_0 \rightarrow_m M_1 \rightarrow_m \cdots \rightarrow_m M_k$ において，デッドロック条件 D を満たす状態 M_i が存在するかどうかを判定し，デッドロックが検出できなければステップ長 k を増加させる必要がある．

そこで，本章ではこれらを含め以下の項目について，採用した実装方法を説明する．

(1) トランジションの順序の決定方法
(2) ステップ長の上限 k の増加方法
(3) トークン数および多重発火回数の上限の決定方法
(4) インクリメンタル SAT 解法の導入方法

6.1 トランジションの順序の決定方法

本論文の実装では，アルゴリズムの詳細は異なっているが，文献 [17] と同様の深さ優先探索を採用した．

深さ優先探索を用いる方法では，ペトリネットを有向グラフと見なし，初期マーキングでトークンを持つプレイスを 1 つ選び，そこから深さ優先探索でペトリネットをたどる．新たなプレイス（またはトランジション）をたどれなくなった場合，まだたどっていないプレイスのうち，初期マーキングでトークンを持つプレイスを 1 つ選び，再度深さ優先探索でたどる．そこでトランジションをたどった順に順序を設定する．たとえば，図 1 の場合，t_1，t_2，t_4，t_3 の順となる．

幅優先探索による方法も考えられるが，深さ優先探索のほうがより遠いプレイスまでトークンが移動する可能性が高くなり，デッドロック検出までのステップ長が短くなると考えられる．

なお，文献 [17] の方法では，入力側のプレイスがすでにたどられた場合にのみ，その先へ進む．したがって，図 1 の場合，t_1，t_2，t_3，t_4 の順となり，違いが生じる．しかし本論文での実装方法のほうが単純で，それほど差は大きくないが予備実験の結果でも良かったため，上記の方法を採用した．

6.2 ステップ長の上限 k の増加方法

一般に，SAT ソルバでは SAT の判定よりも UNSAT の判定のほうが時間を要する．有界モデル検査では，デッドロックを検出できるまで複数回 UNSAT の判定が生じる．そのため，できるだけ UNSAT の判定回数が少なくなるようにステップ長 k を増加させるほうが好ましい．

予備実験として，ステップ長 k を 1 ずつ増やす場合，1.5 倍ずつ増やす場合，2 倍ずつ増やす場合の 3 通りを比較した．その結果，2 倍ずつ増やす場合の結果が比較的良かったため，本論文の実装ではその方法を採用した．

6.3 トークン数および多重発火回数の上限の決定方法

5 章で述べた制約を SAT 符号化するためには，各プレイスのトークン数を表す変数 m_p^{il+j} および各トランジションの多重発火回数を表す変数 f_t^i の上限を定める必要がある．上限を小さく設定すると，デッドロックを検出できない可能性があり，逆に大きく設定すると SAT 符号化後の節数が増大し，求解速度が低下する恐れがある．

そこで，本研究ではこれらの上限値をおおまかに見積もって初期値とし，一定のステップ長以内でデッドロックを検出できない場合は，その上限を増加させる方法を採用した．

まず，各プレイス p のトークン数の上限を $N(p)$ とし，その初期値の決め方について説明する．初期マーキング M_0 でのトークン数の最大値 $\max_{p\in\mathbf{P}} M_0(p)$ を N_0 で表し，アークの多重度の最大値 $\max_{(u,v)\in\{\mathbf{P}\times\mathbf{T}\}\cup\{\mathbf{T}\times\mathbf{P}\}} F(u,v)$ を W で表す．このとき，$N(p)$ の初期値を以下のように定める．

$$N(p) = \max(N_0, W) \tag{14}$$

定めた上限 $N(p)$ の範囲内でデッドロックが検出できるとは限らないため，デッドロック検出に失敗した場合（すなわち，結果が UNSAT だった場合）には，$N(p)$ の値を増加させ再度デッドロック検出を行う必要がある．$N(p)$ の増加方法については，$k \leq 64$（すなわち最初の 7 回）の間は上記の初期値を用い，その後，k が 2 倍されるごとに $N(p)$ も 2 倍する方法を採用した．

次に，各トランジション t の多重発火回数の上限を $N(t)$

Algorithm 1 インクリメンタル SAT 解法を用いたデッドロック検出手続き

```
1: k' = 0; k = 1
2: 各プレイス p に対し，N(p) を式 (14) から計算
3: φ = I を SAT 符号化した節集合
4: loop
5:    各トランジション t に対し，N(t) を式 (15) から計算
6:    φ = (I, T_0, ..., T_{k-1} を SAT 符号化した節集合)
7:    if φ ∪ (D_k を SAT 符号化した節集合) が充足可能 then
8:       break /* デッドロック検出 */
9:    end if
10:   k' = k; k = 2k
11:   各プレイス p に対し，N(p) の値を更新
12: end loop
```

とし，その決め方について説明する．$N(t)$ は，現在の $N(p)$ の値から可能な多重発火回数を計算して定めるのが妥当である．すなわち，以下のようにして求める方法を採用した．

$$N(t) = \min\left(\min_{p\in\bullet t}\left\lfloor\frac{N(p)}{F(p,t)}\right\rfloor, \min_{p\in t\bullet}\left\lfloor\frac{N(p)}{F(t,p)}\right\rfloor\right) \quad (15)$$

6.4 インクリメンタル SAT 解法の利用

本論文のシステムは，インクリメンタル SAT 解法が利用可能な SAT ソルバである GlueMiniSat [14] と，それを利用する API ライブラリである iSAT Library [20] を利用して実装した．

Algorithm 1 に，インクリメンタル SAT 解法を用いたデッドロック検出のアルゴリズムの概要を示す．アルゴリズム中で I，T_i，D_i は式 (13) 中の制約を表している．また，k は有界モデル検査のステップ長を表し，k' は 1 回前の k の値を表す．まず，I のみを SAT 符号化し，ϕ に代入する（3 行目）．6 行目で ϕ に制約 I および $T_0, \ldots, T_{k-1}$ を SAT 符号化した節を代入する．ただし，$N(p)$ の値が更新されていない場合は，増加した制約 $T_{k'}, \ldots, T_{k-1}$ に対応する節を ϕ にインクリメンタルに追加するだけでよい．7 行目では，k ステップ以内にデッドロックが存在するという条件 D_k を仮定として SAT ソルバで求解している．この仮定は，SAT ソルバに節として永続的に追加されるわけではない．したがって，その結果が UNSAT であったとしても，解探索の途中で獲得された学習節は次のループでも保持され，再利用される．

7. 評価実験

評価実験には Model Checking Contest 2017 Reachability Deadlock 部門の問題から選んだ 297 問を使用した．これらの問題はデッドロックがないことが証明されていない問題（デッドロックがあることが分かっている問題もしくはデッドロックの有無が分かっていない問題）である．

最初の実験では，以下の 2 通りの手法について比較する．

(1) 連続発火モデル

(2) 多重発火モデル

次の実験では，Model Checking Contest 2017 の優勝および準優勝システムと比較を行い，提案手法の有効性について評価する．

なお，実行時間はすべて Ubuntu 14.04（Xeon 3.5 GHz，メモリ 16 GB）上で計測し，デッドロック検出までの制限時間は 3,600 秒とした．なお，この制限時間は Model Checking Contest 2017 での設定と同一である．

7.1 2 通りの手法の比較

本論文での提案手法である連続発火モデルと多重発火モデルの比較を行う．連続発火モデルは既存の SAT 型手法である文献 [17] を一般のペトリネットに拡張したものが対応し，多重発火モデルは連続発火モデルに多重発火を導入した手法である．なお，安全ペトリネットについては，多重発火モデルと既存の SAT 型手法 [17] は同じ手法となる．

まず**図 3** に，与えられた時間内に何問デッドロックを検出できているかを表すグラフを示す．たとえば，500 秒以内にデッドロックを検出できた問題数は，$y = 500$ と交差した点での x の値となる．このグラフを見ると，どの制限時間に対しても多重発火モデルのほうが優れており，制限時間が延びるにつれ徐々にその差がひらいている．

表 1 により詳細な比較結果を示す．合計 297 問ある問題を，初期マーキング M_0 でのトークン数の最大値 $N_0 = \max_{p\in\mathbf{P}} M_0(p)$ により分類し，$N_0 = 1$ の場合，N_0 が 2 以上 10 以下の場合などに分けて示している．N_0 の欄の右側は，その分類における問題数である．また，連続発火モデルと多重発火モデルのそれぞれに対し，3,600 秒の制限時間内にデッドロックを検出できた問題を「解けた問題数」に，解けた問題に対するステップ長（Algorithm 1 でデッドロックを検出したときの k の値）の平均値を「平均ステップ長」に，解けた問題に対する CPU 時間（秒）の平均値を「平均 CPU 時間（秒）」に示している．

まず「解けた問題数」を比較すると，多重発火モデルのほうが合計で 15 問多く，N_0 のどの範囲においても連続発火モデル以上になっている．N_0 が大きくなるにつれて解けた問題数の差が大きくなっており，特に $N_0 \geq 11$ の場合に差が生じている．これは，平均 CPU 時間を見ても同様の傾向になっている．

すなわち，初期マーキングでのトークン数の最大値 N_0 が大きい問題について，多重発火モデルがより優れているといえる．ただし，N_0 が小さい問題についても連続発火モデルとほぼ同等である．

これは，4.2 節で示したように，多重発火モデルのほうがより短いステップ長でデッドロックに到達できるためだと考えられる．N_0 が大きいほど多重発火できる回数が増え，より効果が大きくなる．このことは表 1 の「平均ステップ長」の値からも確認できる．たとえば，N_0 が 21 以上 50

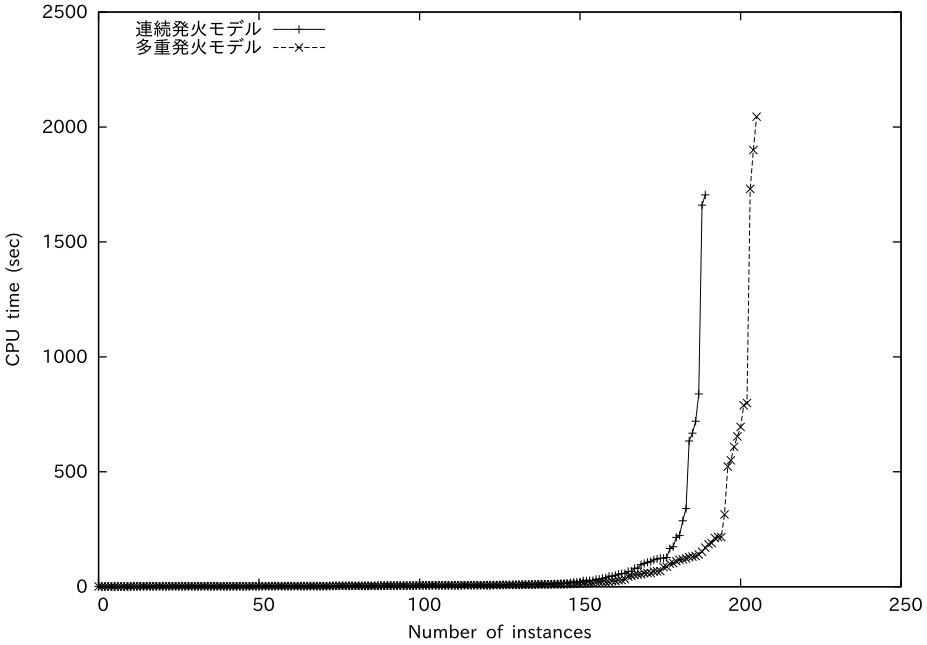


図 3 各手法で与えられた制限時間内にデッドロックを検出できた問題数

Fig. 3 Number of instances succeeded to detect deadlock within a given amount of time by each method.

表 1 各手法でデッドロックを検出できた問題数，平均ステップ長，平均 CPU 時間（N_0 は M_0 中のトークン数の最大値）

Table 1 Number of instances succeeded to detect deadlock, average number of steps, average CPU times by each method (N_0 is the maximum number of tokens in M_0).

		連続発火モデル			多重発火モデル		
N_0	問題数	解けた問題数	平均ステップ長	平均 CPU 時間（秒）	解けた問題数	平均ステップ長	平均 CPU 時間（秒）
1	161	142	6.9	228.1	142	6.7	231.0
2〜10	69	38	21.5	1,415.0	38	20.0	1,422.0
11〜20	16	5	21.0	2,318.0	6	15.0	2,059.0
21〜50	15	5	29.0	1,611.0	8	4.0	416.0
51〜	36	0	—	—	11	7.0	316.1
合計	297	190			205		

以下の場合，連続発火モデルでデッドロックを検出するには平均 29 ステップを要したが，多重発火モデルではわずか 4 ステップとなっている．このように，デッドロックに到達するまでのステップ長が短く済むことが性能向上に寄与したと考えられる．

7.2 既存手法との比較

次に提案手法である多重発火モデルと SAT 型でない既存手法との比較結果を**表 2** に示す．比較には，Model Checking Contest 2017 Reachability 部門の優勝ソルバである LoLA と，2 番目に結果が良かった Tapaal を用いた．LoLA，Tapaal は SAT 型手法ではなく，ともにマーキンググラフを用いた手法である．マーキンググラフはペトリネットの状態を展開していく手法である．

制限時間内にデッドロックを検出できた数を比較したところ，$N_0 \geq 2$ では提案手法が他手法よりも劣っていた．これは，節数がトークン数上限 N_0 の 2 乗に比例して増加することが一因だと考えられる．このような問題では，対数符号化法 [6], [10] を使用することで解ける可能性があり，今後の検討課題である．また，$N_0 = 1$ の場合では LoLA と

表 2 各手法でデッドロックを検出できた問題数

Table 2 Number of instances succeeded to detect deadlock by each method.

N_0	問題数	多重発火モデル	LoLA	Tapaal
1	161	142	143	129
2〜10	69	38	63	59
11〜20	16	6	15	10
21〜50	15	8	14	12
51〜	36	11	30	31
合計	297	205	265	241

表 3 Angiogenesis-PT での結果
Table 3 Results of Angiogenesis-PT.

問題名	N_0	多重発火モデル CPU 時間（秒）	多重発火モデル メモリ使用量（バイト）	LoLA CPU 時間（秒）	LoLA メモリ使用量（バイト）
Angiogenesis-PT-10	10	1.19	4,979,764	3.35	402,292
Angiogenesis-PT-15	15	1.36	4,986,748	36.97	2,171,764
Angiogenesis-PT-20	20	1.59	5,094,012	132.65	6,628,212
Angiogenesis-PT-25	25	1.35	5,092,920	Timeout	—
Angiogenesis-PT-50	50	1.62	5,115,492	—	Memory over

ほぼ同等で，Tapaal よりも優れていた．

しかし，LoLA，Tapaal が解けず，提案手法のみが解けた問題が 9 問あった．うち 7 問が Model Checking Contest 2017 に参加したいずれのソルバでもデッドロックを検出できなかった問題である．そのうちの Angiogenesis-PT の問題について，LoLA との比較結果を**表 3** に示す．

Angiogenesis-PT はプレイス数，トランジション数，アーク数は一定で，初期マーキングにおけるトークン数がパラメータとなっている問題である．表 3 での N_0 は初期マーキングでの各プレイスのトークン数の最大値を表している．表を見ると，提案手法は N_0 の値にかかわらず，CPU 時間とメモリ使用量はほぼ一定である．一方，LoLA では，N_0 が増加するにつれ CPU 時間とメモリ使用量が増大し，$N_0 = 25$ で 3,600 秒の制限時間内で終了せず，$N_0 = 50$ では 16 GB のメモリでメモリオーバとなっている．Angiogenesis-PT は多重発火が有効な問題であり，N_0 が増加するにつれ節数は増大するが，ステップ長は増加せずほぼ一定の時間で解けている．

LoLA はペトリネットの状態を展開していく手法を用いているが，この手法は状態空間爆発が起こりやすい．一方，提案手法の場合，多重発火が有効な問題では，CPU 時間およびメモリ使用量がそれほど増加せずに，より大きなトークン数に対応できている．この点は他手法にない大きな特徴といえる．しかし，一般にどのような問題に対して優れているのかについては，現時点では明確でなく今後の研究課題である．

8. おわりに

本論文では，SAT ソルバを用いて一般のペトリネットでのデッドロック検出を行う方法を述べた．提案手法の特徴は以下のとおりである．

(1) SAT ソルバによる一般のペトリネットでのデッドロック検出の実現．
非負整数値であるトークン数を表現するために**順序符号化** [23], [24] を用いた．これにより，既存の SAT 型手法である文献 [17], [19] では対応できなかった一般のペトリネットでのデッドロック検出が可能となった．

(2) SAT ソルバによる効率良いデッドロック検出を可能とするための多重発火モデルの導入．
既存の SAT 型手法である文献 [17] で採用されていたモデル（連続発火モデルと呼ぶ）よりも短いステップ長でデッドロック検出が可能となるモデルを提案した．これにより全般に性能が向上したが，特にトークン数が比較的多い問題に対する効果が大きいことが分かった．

SAT 型でない既存手法との比較では，Model Checking Contest 2017 デッドロック検出部門で優勝したツール LoLA と，2 番目に性能が良かった Tapaal と比較した．提案手法は，デッドロックを検出できた問題数では既存手法より少なかったが，既存手法がいずれもデッドロックの検出に失敗した問題での検出に成功し，提案手法の有効性が確認できた．

謝辞 本研究は JSPS 科研費 16H02803 の助成を受けたものである．

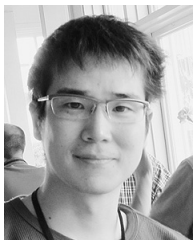
参考文献

[1] 番原睦則，鍋島英知：SAT 技術の進化，情報処理，Vol.57, No.8, pp.704–709 (2016).
[2] 番原睦則，田村直之：SAT によるシステム検証，人工知能学会誌，Vol.25, No.1, pp.122–129 (2010).
[3] Biere, A.: Bounded Model Checking, *Handbook of Satisfiability*, pp.457–481, IOS Press (2009).
[4] Biere, A., Cimatti, A., Clarke, E.M. and Zhu, Y.: Symbolic Model Checking without BDDs, *Proc. 5th International Conference on Tools and Algorithms for Construction and Analysis of Systems* (*TACAS 1999*), LNCS, Vol.1579, pp.193–207 (1999).
[5] Eén, N. and Sörensson, N.: Temporal Induction by Incremental SAT Solving, *Electronic Notes in Theoretical Computer Science*, Vol.89, No.4 (2003).
[6] Gelder, A.V.: Another Look at Graph Coloring via Propositional Satisfiability, *Discrete Applied Mathematics*, Vol.156, No.2, pp.230–243 (2008).
[7] Heiner, M., Rohr, C., Schwarick, M. and Tovchigrechko, A.A.: MARCIE's Secrets of Efficient Model Checking, *Trans. Petri Nets and Other Models of Concurrency XI*, LNCS, Vol.9930, pp.286–296 (2016).
[8] Hillah, L.M. and Kordon, F.: Petri Nets Repository: A tool to benchmark and debug Petri Net tools, *Proc. 38th International Conference on Petri Nets and Other Models of Concurrency*, LNCS, Vol.10258, pp.125–135 (2017).
[9] 井上克巳，田村直之：SAT ソルバーの基礎，人工知能学会誌，Vol.25, No.1, pp.57–67 (2010).
[10] Iwama, K. and Miyazaki, S.: SAT-Variable Complex-

ity of Hard Combinatorial Problems, *Proc. IFIP 13th World Computer Congress*, pp.253–258 (1994).
[11] Jensen, J.F., Nielsen, T., Oestergaard, L.K. and Srba, J.: TAPAAL and Reachability Analysis of P/T Nets, *Trans. Petri Nets and Other Models of Concurrency XI*, LNCS, Vol.9930, pp.307–318 (2016).
[12] Knuth, D.E.: *Satisfiability*, *The Art of Computer Programming*, Vol.4, Fascicle 6, Addison-Wesley Professional (2015).
[13] Kordon, F., Garavel, H., Hillah, L., Paviot-Adet, E., Jezequel, L., Rodríguez, C. and Hulin-Hubard, F.: MCC 2015 — The 5th Model Checking Contest, *Trans. Petri Nets and Other Models of Concurrency XI*, LNCS, Vol.9930, pp.262–273 (2016).
[14] 鍋島英知，岩沼宏治，井上克巳：GlueMiniSat 2.2.5：単位伝搬を促す学習節の積極的獲得戦略に基づく高速 SAT ソルバー，コンピュータソフトウェア，Vol.29, No.4, pp.146–160 (2012).
[15] 鍋島英知，岩沼宏治，井上克巳：SAT ソルバーの最近の進展，情報処理，Vol.57, No.8, pp.724–729 (2016).
[16] 鍋島英知，宋 剛秀：高速 SAT ソルバーの原理，人工知能学会誌，Vol.25, No.1, pp.68–76 (2010).
[17] Ogata, S., Tsuchiya, T. and Kikuno, T.: SAT-Based Verification of Safe Petri Nets, *Proc. 2nd International Conference on Automated Technology for Verification and Analysis* (*ATVA 2004*), pp.79–92 (2004).
[18] 奥川峻史：ペトリネットの基礎，共立出版 (1995).
[19] Rodríguez, C. and Schwoon, S.: Cunf: A Tool for Unfolding and Verifying Petri Nets with Read Arcs, *Proc. 11th International Symposium on Automated Technology for Verification and Analysis* (*ATVA 2013*), pp.492–495 (2013).
[20] 迫 龍哉，宋 剛秀，番原睦則，田村直之，鍋島英知，井上克巳：インクリメンタル SAT 解法ライブラリとその応用，コンピュータソフトウェア，Vol.33, No.4, pp.16–29 (2016).
[21] 寸田智也，宋 剛秀，番原睦則，田村直之：SAT 技術を用いたペトリネットのデッドロック検出手法の提案，2017 年度人工知能学会全国大会（第 31 回）論文集 (2016).
[22] 寸田智也，宋 剛秀，番原睦則，田村直之：SAT 技術を用いた正規ペトリネットのデッドロック検出手法の提案，日本ソフトウェア科学会第 33 回大会，pp.513–521 (2016).
[23] Tamura, N., Taga, A., Kitagawa, S. and Banbara, M.: Compiling Finite Linear CSP into SAT, *Constraints*, Vol.14, No.2, pp.254–272 (2009).
[24] 田村直之，丹生智也，番原睦則：SAT 変換に基づく制約ソルバーとその性能評価，コンピュータソフトウェア，Vol.27, No.4, pp.183–196 (2010).
[25] 田村直之，丹生智也，番原睦則：制約最適化問題と SAT 符号化，人工知能学会誌，Vol.25, No.1, pp.77–85 (2010).
[26] Thierry-Mieg, Y.: Symbolic Model-Checking Using ITS-Tools, *Proc. 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems* (*TACAS 2015*), pp.231–237 (2015).
[27] Wolf, K.: Running LoLA 2.0 in a Model Checking Competition, *Trans. Petri Nets and Other Models of Concurrency XI*, LNCS, Vol.9930, pp.274–285 (2016).

寸田 智也

2016 年神戸大学工学部情報知能工学科卒業．同年同大学大学院システム情報学研究科情報科学専攻博士前期課程入学．2018 年同大学院修了．システム情報学修士．制約プログラミング，SAT 技術の応用に興味を持つ．



宋 剛秀 （正会員）

2004 年神戸大学工学部電気電子工学科卒業．2006 年同大学大学院自然科学研究科電気電子工学専攻修了．サントリー（株）を経て，2011 年総合研究大学院大学複合科学研究科情報学専攻博士後期課程修了．博士（情報学）．2012 年より神戸大学情報基盤センター助教．制約プログラミング，SAT 技術およびそれらの応用に興味を持つ．日本ソフトウェア科学会，人工知能学会各会員．

番原 睦則 （正会員）

1994 年神戸大学理学部数学科卒業．1996 年同大学大学院自然科学研究科博士課程前期数学専攻修了．1996 年国立奈良工業高等専門学校助手．1998 年同校講師．2003 年より神戸大学情報基盤センター講師．2007 年同准教授．博士（工学）．論理プログラミング，制約プログラミング，SAT 技術等に興味を持つ．日本ソフトウェア科学会，人工知能学会各会員．

田村 直之 （正会員）

1980 年神戸大学理学部物理学科卒業．1985 年同大学大学院自然科学研究科博士課程システム科学専攻修了．学術博士．1985 年日本 IBM 東京基礎研究所入社．1988 年神戸大学工学部勤務．2003 年より神戸大学情報基盤センター教授．論理プログラミング，制約プログラミング，SAT 技術等に興味を持つ．日本ソフトウェア科学会，人工知能学会各会員．

井上 克巳 （正会員）

1982 年京都大学工学部数理工学科卒業．1984 年同大学大学院工学研究科数理工学専攻修了．京都大学博士（工学）．松下電器産業（株），（財）新世代コンピュータ技術開発機構，豊橋技術科学大学，神戸大学を経て，2004 年より国立情報学研究所．現在，同情報学プリンシプル研究系教授および総合研究大学院大学複合科学研究科情報学専攻教授．2015 年東京工業大学大学院情報理工学研究科客員教授，2016 年より同情報理工学院情報工学系特任教授．人工知能，論理プログラミングに興味を持つ．日本ソフトウェア科学会，人工知能学会，AAAI 各会員．