A-003

拡張被覆グラフを用いた $L2/L3$ 活性判定器のペトリネットツール HiPS への実装

Implementation of $L2/L3$-Liveness Analyzer Using the Extension Coverability Graph to Petri Net Tool HiPS

三井 雄太 †　張江 洋次朗 ††　和崎 克己 ††
Yuta Mitsui　Yojiro Harie　Katsumi Wasaki

1. はじめに

ペトリネット（Petri net）は，事象発生の並列性，非同期性，非決定性を有する離散事象システムのふるまいを表す数学モデルであり，グラフィックツール，シミュレーションツール，および数学的方法論の 3 つの機能を同時に持っている [1][2]．グラフィックツールとしてシステム構造を可視的な表現で記述し，ペトリネットの中でトークンを使用することによりシステムの並列事象をシミュレーションできる．また数学的ツールとしてシステムの挙動を方程式や行列式を用いることでモデリングが可能である．ペトリネットの性質で，初期マーキングに依存するものを動的性質 (behavioral property) と呼ぶ．マーキング M_0 をマーキング M_n に変換する発火の系列が存在するとき，マーキング M_n はマーキング M_0 から可達 (reachable) であるという．

既存のペトリネットツールの記述性，操作性，再利用性の問題を解決するために，本学で開発されたペトリネット設計ツール HiPS (Hierarchical Petri net Simulator) がある (図 1)．ペトリネットベースでの効率的なモデル化を行うために，HiPS は直感的で一般的な操作方法の GUI を備え，ネットの階層化機能およびモデルの動作解析機能が実装されている．また，時間ペトリネットにも対応している．HiPS には様々な解析機能 [3] が備わっているが，いくつかの重要な性質を解析する機能が不足している．

本研究ではペトリネット設計ツール HiPS における解析機能として $L2/L3$ 活性判定器の設計および，その実装に必要な拡張被覆グラフ生成器を作成する．2 章ではペトリネットの動的性質について具体的に説明する．3 章では研究の対象である，非有界なネットと被覆グラフについて説明する．4 章では動的性質の解析のための拡張被覆グラフを提案する．5 章では $L2/L3$ 活性判定器の実装について説明し，6 章でペトリネットに解析器を適用させた例を示す．

2. ペトリネットの動的性質

ペトリネットの性質は初期マーキングに依存する動的性質と，初期マーキングと独立な構造的性質に分けられる．本研究の目的である活性は動的性質であり，解析方法も動的性質を利用している．

† 信州大学大学院総合理工学研究科，Graduate School of Science and Technology，Shinshu University.
†† 信州大学大学院総合工学系研究科，Interdisciplinaty Graduate School of Science and Technology，Shinshu University.

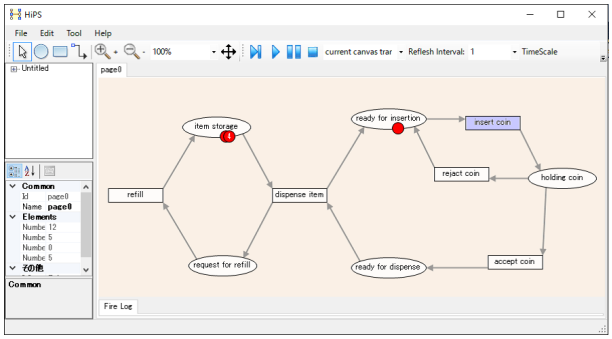

図 1　ペトリネット設計ツール HiPS

2.1. マーキング

ペトリネットにおいて，あるプレース p に対し，非負整数 k が割り当てられたとき，プレース p は k 個のトークンでマーキングされていると言い，この時トークンはプレース p 内の k 個の点として図示される．ペトリネットは，マーキングによりシステムの状態を表現し，m 個のプレースからなるペトリネット全体のマーキングは m 次元ベクトル M であらわされる．特にマーキングの初期状態を初期マーキング (initial marking) M_0 と呼び，マーキングはトランジションの発火により遷移する．

2.2. 可達性

マーキング M_0 からマーキング M_n へ至る発火系列 $\sigma = M_0 t_1 M_1 t_2 M_2 ... t_n M_n$ が存在するとき M_n は M_0 から可達であるといい，$M_0[\sigma > M_n$ と記す．ここで，$t_1, t_2, ..., t_n$ はトランジションである．ネット (N, M_0) において，M_0 から可達なすべてのマーキングの集合を $R(M_0)$ と表し，M_0 から始まるすべての発火系列の集合を $L(M_0)$ と記す．

2.3. 被覆性

ペトリネット (N, M_0) におけるマーキング M は，ネット内のすべてのプレース p に対して，$M_1(p) \geq M(p)$ となるようなマーキング M_1 が $R(M_0)$ にあれば被覆可能であるという．

2.4. 活性レベルの定義

ペトリネットの動的性質の一つに活性がある．ペトリネット (N, M_0) に対し，初期マーキング M_0 からどのマーキングに到達していようと，ネット内の任意のトランジションを，そのマーキングから何らかの発火系列を通して発火可能にするならば，活性であると呼ぶ．これは，どのような発火系列が選ばれようと，活性ペトリ

ネットがデッドロックのない操作を保証することを意味する．活性は多くのシステムの理想的な性質である．しかしながら，大規模なシステムにとってこの厳しい性質を検証することは，コストの面から困難である．それゆえ，活性条件を緩和した，表 1 に示す活性のレベルが定義されている [1]．

ネット内のすべてのトランジションが，Lk-live ($k = 1,2,3,4$) ならば，ペトリネット (N, M_0) は，Lk-live であると呼ばれる．$L4$-live は，最も強い活性レベルであり，先に定義した活性に相当する．トランジションが，Lk-live であって，$L(k+1)$-live でない場合 ($k = 1,2,3$)，strictry Lk-live であると呼ぶ．以降では Lk-live，または Lk 活性と表記している場合，strictly Lk-live を意味している．

3. 非有界ネット

ペトリネットは，M_0 から可達な任意のマーキングにおいて，各プレース内のトークンの数がある有限な数 k を越えなければ，k-有界，あるいは単に有界であると呼ばれる．トークンの数が有限な数で抑えられないプレースを含む可達なマーキングが存在する場合，非有界であると呼び，そのネットは非有界ネットと呼ばれる．

3.1. 被覆木法と被覆グラフ

ペトリネット (N, M_0) を考える．初期マーキング M_0 から発火可能なトランジションを 1 回発火することにより，発火可能なトランジションと同数の「新しい」可達マーキングを得ることができる．それぞれの新しいマーキングから，またさらに新しい可達マーキングを得ることができる．この木表現は，ネットが有界でなければ，無限に大きくなってしまう．木を有限に抑えるために，特別な記号 ω を導入した被覆木が生成される [1]．ω は「無限」を表すと考えることができる．被覆グラフは，ラベルづけされた有効グラフ $G = (V, E)$ である．ノードの集合 V は，被覆木内のすべての異なったマーキングを持つノードの集合であり，アークの集合 E は，$M_i[t_k > M_j$ であるような単一のトランジション発火を表現しているトランジション t_k でラベル付けされたアークの集合である．ここで M_i および M_j は V の要素である．

3.2. 被覆グラフの情報欠落の問題

従来の被覆グラフには情報の欠落がある．$L2/L3$ 活性判定のときに障害となる情報の欠落は，ω によって畳み込まれた状態のトークンが $\{0, 1\}$ となるか不明なことに起因する．

表 1　活性レベル

$L1$-live	トランジション t が，$L(M_0)$ のある発火系列において少なくとも 1 回は発火可能である．
$L2$-live	任意の正整数 k に対し，トランジション t が，$L(M_0)$ のある発火系列において，少なくとも k 回は発火可能である
$L3$-live	トランジション t が，$L(M_0)$ のある発火系列において，無限回現れる
$L4$-live	トランジション t が，$R(M_0)$ のすべてのマーキングに対して $L1$-live である．

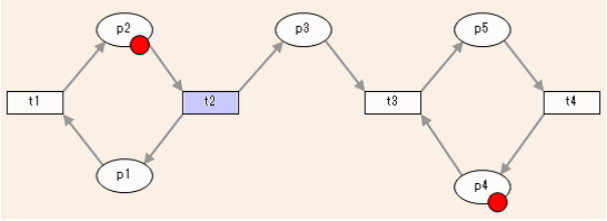

図 2　ペトリネットモデル例 1

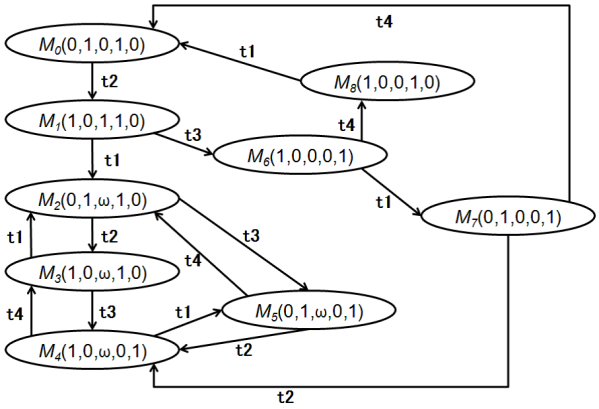

図 3　図 2 のネットに対する被覆グラフ

例えば，図 2 に示すような非有界ネットにおいて，t_3 は p_3 にトークンがなければ発火できない．つまり p_0 にトークンを供給する t_1, t_2 の繰り返し発火回数を k 回としたとき，プレース p_3 にはトークンが k 個格納されるから，トランジション t_3 が発火できるのは k 回以内となる．しかし，図 3 の被覆グラフを見ると，一旦 ω になると t_3 は制限なく発火可能であるかのように表現されている．

トークンを減少させるトランジションを発火させ続けると，いずれトークンが無くなり他のトランジションを発火させなければならない．従来の被覆グラフでは他のトランジションを発火せずに，無限に発火可能なトランジションとして検知されてしまう．従ってトークンが減少するプレースに基づいたループ検知を正しく行えないと活性レベルを正しく解析できない．

4. 拡張被覆グラフの提案と構成

被覆グラフにおける情報の欠損を解決するために，拡張被覆グラフを提案する．拡張被覆グラフは，従来の被覆グラフにおける無限を表す状態を 3 値に拡張したアルゴリズムによって生成される（Algorithm 1）．具体的には無限状態 ω を，プレース内トークン数の増加（Nu）・一定（Nc）・減少 (Nd) に拡張することにより，被覆している部分のトークン数の増減を表す．トークン数の増加・減少のステップ幅は 1 に限定する（ordinary）．拡張被覆グラフでは 2 以上の自然数は N を用いて表現することから，N*（または N*遷移）と表す．トークン数が減少している Nd に遷移するトランジションがある場合，ガード条件を付けて分岐するトランジションを生成する．従来の被覆グラフでは 1 以上の被覆可能ならば ω に置換していたが，拡張被覆グラフでは有界部と N*に

被覆する非有界部の境界を明示するためにトークン数が $\{0, 1\}$ の場合は有界部としてトークン数が 2 以上で被覆可能な場合 N*に被覆する．

4.1. 拡張被覆グラフ生成器の実装

拡張被覆グラフ生成アルゴリズムを Algorithm 1 に示す．拡張被覆グラフは深さ優先探査によって生成される．まず，初期マーキング M_0 から任意の発火可能なトランジションを発火させ新たなマーキングを得る．次に，新たなマーキングが被覆可能か解析を行う．被覆可能なマーキングが生成されたとき，N*に置き換えるプレースが発火したトランジションの入力プレースであるか，出力プレースであるかによって Nu・Nc・Nd の判定を行う．そして，新たなマーキングは新規マーキングであるか，既存のマーキングであるか判定を行う．新規マーキングであった場合，そのマーキングをまた任意の発火可能なトランジションを発火させる手続きに再帰呼び出しする．既存のマーキングであった場合，別の任意の発火可能なトランジションを発火させ，別の新たなマーキングを得て，再び判定を行う．そのマーキングにおいて発火可能なトランジションをすべて発火させ，すべての判定を終了したら，1 つ前のマーキングに戻り，また発火可能なすべてのトランジションを発火させ，判定を行う．そのとき置換される記号は Nu である．Nd を含むマーキングへの遷移がある場合，前状態のマーキング番号と Nd となるプレースを記録し，有界部への新たなアークの生成を行う．このとき記録されたプレースのトークン数は 2 から 1 に減少したときであり，N*から 1 に置換し新しいマーキングとして処理が行われる．これを初期マーキングがすべての判定を終了するまで行う．

拡張被覆グラフの条件より，実際のトークン数から N*への置換が行われるのはトークン数が 1 から 2 に増加したときである (必ず置換されるとは限らない)．

Algorithm 1 拡張被覆グラフ生成アルゴリズム

ステップ 1： 初期マーキング M_0 に根と付記し，「新」としておく．
ステップ 2： 「新」マーキングがある間，以下を繰り返す．
ステップ 2.1： 新マーキング M を，選択する．
ステップ 2.2： 根から M までの経路上のマーキングに M と同一のものがあれば，M を，「既存」として別の新マーキングに進む．
ステップ 2.3： M において，発火可能なトランジションがなければ，M を「終端」とする．
ステップ 2.4： M に発火可能なトランジションがある間，すべての発火可能なトランジション t に対して，以下の処理を行う．
ステップ 2.4.1： M において t を発火することによって得られるマーキング M' を求める．
ステップ 2.4.2： 根から M' までの経路に，すべてのプレース p に対して，$M'(p) > 1$ でかつ $M'(p) \geq M''(p)$ でかつ $M' \neq M''$ であるような M'' が存在すれば，すなわち M'' が $M'(p) > 1$ で被覆であれば，$M'(p) > M''(p)$ であるようなすべての p に対して，$M'(p)$ を N*で置き換える．N*に対して，以下の処理を行う．
ステップ 2.4.2.1： N*は，直前のマーキング $M(p)$ のトークン数と比較し，1 増加していれば Nu，同数であれば Nc，1 減少していれば Nd とする．
ステップ 2.4.3： M' をノードとして取り入れる，M から M' へのアークを描き，t と付記する，M' を「新」とする．
ステップ 2.4.3.1： $M'(p)$ が Nd のとき，Nd を 1 に置き換え，M から M' へのアークを描き，t と付記する．

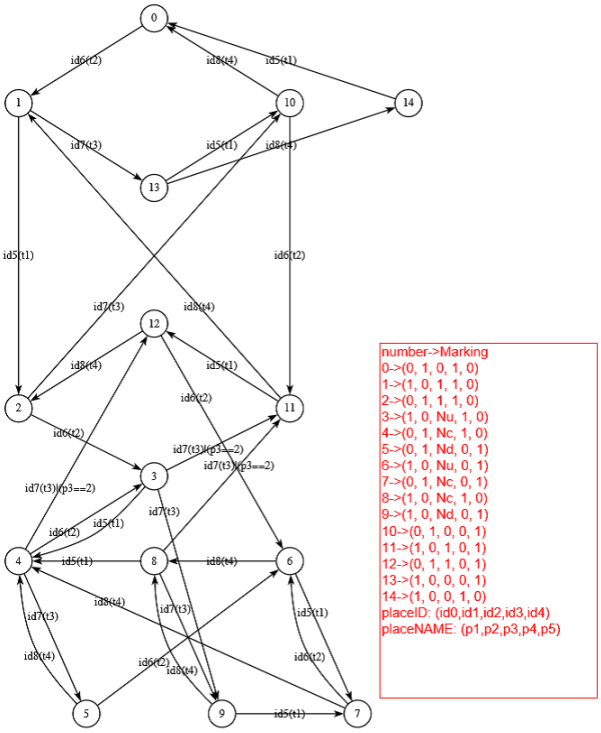

図 4 図 2 のネットに対する拡張被覆グラフ

4.2. 拡張被覆グラフの例

被覆グラフは生成された被覆木をグラフとして表現したものである．図 2 のペトリネットに対する拡張被覆グラフを図 4 に示す．例えば従来の被覆グラフ M_3, M_4 状態間の遷移は，プレース p_3 に対するトークン減少のループであるが，有界部分への遷移が欠落している．一方，拡張被覆グラフ M_8, M_9 状態間の遷移も同様のループであるが，有界部分の状態 M_{11} への遷移が生成されており，可逆性等の性質が正しく判定できる．

5. $L2/L3$ 活性判定と実装

$L2$(または $L3$) 活性であるということは，任意の自然数回 (または無限回) トランジションを発火可能とする発火系列 σ が存在するということである．拡張被覆グラフから得られる発火系列は生成状態数を有限に抑えるため，反復している発火系列を有限長のループ構造として得ることができる．つまり，$L2/L3$ となるトランジションはループ構造になっている発火系列に含まれてい

る．よって，発火系列のループ構造を調べることによって $L2/L3$ 活性判定を行う．

$L2$ 活性と $L3$ 活性の違いは発火ループが終了するか否かである．$L3$ 活性と判定されるループでは，すべてのプレースにおいてトークン数が増加する，または一定である．$L2$ 活性と判定されるループでは，いずれかのプレースにおいてトークン数が減少し，いずれトークン数が 0 となり，ループから脱出する．つまり，被覆グラフで新たに追加された有界部への遷移が存在するマーキングを含むループ構造の場合，$L2$ 活性のループである．ループ構造が複数ある場合，無限回発火する発火系列が一つでも存在すれば $L3$ 活性であるので，トランジションが含まれるループの中に $L3$ 活性と判定されるループが一つでも存在すれば，そのトランジションは $L3$ 活性である．トランジションが含まれるループがすべて $L2$ 活性と判定されるループであれば，そのトランジションは $L2$ 活性である．

6. 適用例

$L2/L3$ 活性判定の適用例として，図 5 のペトリネットモデルに対し活性判定を行う．トランジション t_0 はプレース p_1，p_3 の両方にトークンが入ることがないため，不活性である．トランジション t_1 はプレース p_1 からプレース p_3 へトークンが移動する際に 1 度だけ発火するので，$L1$ 活性である．トランジション t_2 はプレース p_2 のトークン数だけ発火可能となる．p_2 のトークン数はトランジション t_3 の発火回数に依存し，t_2 は無限回発火する発火系列を持たないため $L2$ 活性である．トランジション t_3 はトランジション t_1 が発火するまで発火可能であり，t_1 が発火しなければ無限回発火可能であるため，$L3$ 活性である．

図 6 の拡張被覆グラフから，t_0 は一度も発火していないことがわかる．t_1 は発火しているが，ループ構造に含まれていない．M_6 の t_2 と M_4 の $t3$ に自己ループ構造が存在している．M_6 からは有界部への遷移が存在しているが，M_4 からは有界部への遷移が存在しない．ペトリネットツール HiPS へ，4.1 節で提案した拡張被覆生成アルゴリズムならびに 5 節で説明した $L2/L3$ 判定器を実装した．図 5 のペトリネットモデルを HiPS ツール上で入力し解析を行ったところ，図 7 に示すユーザ出力を得た．

7. まとめと今後の課題

本研究では，HiPS の拡張被覆グラフ生成器，および拡張被覆グラフを用いた L2/L3 活性判定器の実装を行った．拡張被覆グラフ生成器は，従来の被覆 (可達) グラフ生成器の機能は保ちながら，被覆した部分の増減を判別できるようにしたことで，新たなグラフの作成，また新たな発火系列の生成を実現した．$L2/L3$ 活性判定器は，拡張被覆グラフ生成器から得られる発火系列を用いることで，トークンが減少するループを判別し，$L2/L3$ 活性について解析することを実現した．

今後は $L2/L3$ 活性判定の結果を用いて，$L4$ 活性判定器の実装を行っていく．サイフォン・トラップに関するサブクラスである TCC ネットに対する活性についての必要十分条件はすでに研究が行われている [4]．その条件を用いて，TCC ネットについての $L4$ 活性判定器を実装を行っていき，段階的に一般ペトリネットについての $L4$ 活性判定器の実装を目指す．

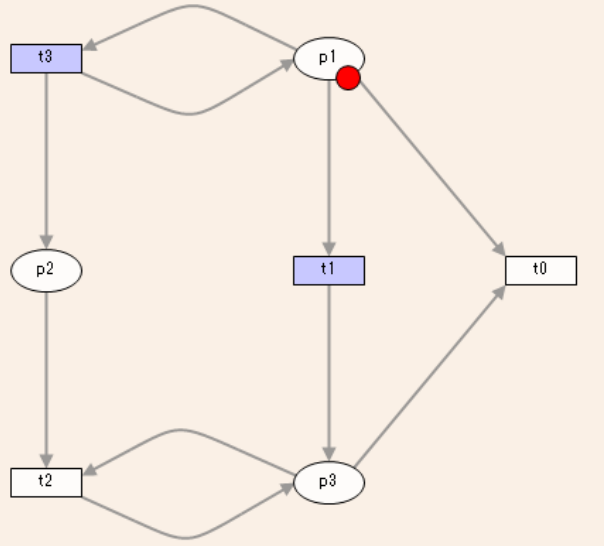

図 5　ペトリネットモデル例 2

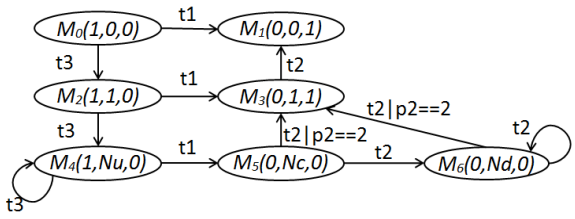

図 6　図 5 のネットに対する拡張被覆グラフ

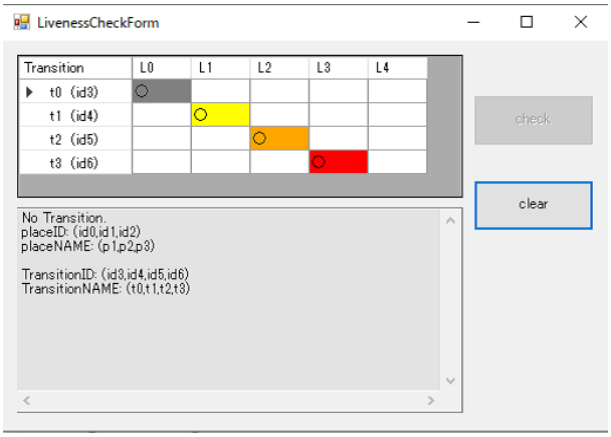

図 7　図 5 のネットに対する活性判定結果

参考文献

[1] T. Murata：“Petri Nets: Properties, Analysis and Applications”, Proc. of the IEEE, 77(4), (1989)
[2] J.L. ピーターソン：“ペトリネット入門　情報システムのモデル化”, 共立出版 (1984)
[3] 張江洋次朗，和崎克己：“ペトリネット設計検証ツール HiPS における On-the-fly LTL モデル検査器”，FIT2015（第 14 回情報科学技術フォーラム）講演論文集, (A-015), 139-142, (2015)
[4] 花川清孝，松本忠：“TCC ネットと SCC ネットの活性と可到達性” 電子情報通信学会技術研究報告. CAS, 回路とシステム, 95(351), 39-46, (1995)