様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　６月　４日現在

機関番号：13302
研究種目：基盤研究（Ｃ）
研究期間：2009～2011
課題番号：21500009
研究課題名（和文）離散ダイナミクスの流体化によるシステムの安全性検証

研究課題名（英文）Safety Verification Based on Fluidification of Discrete Dynamics

研究代表者
平石　邦彦（KUNIHIKO HIRAISHI）
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：40251970

研究成果の概要（和文）：指数分布の発火遅延時間をもつ一般化確率ペトリネットに対して，各プレースにおける確率分布の分散を，流体モデル上のトランジションの区間発火速度で表現する方法を考案し，さらに，モデルが区間パラメータをもつ区分的線形システムで等価的に表現できることを示した。また，モデルのシミュレーションのために，常微分方程式に対する区間法を拡張した手法，および，連続状態システムに対する離散抽象化手法の一つである箱抽象化計算の高速化手法の２つを開発した。

研究成果の概要（英文）：For generalized stochastic Petri nets with exponentially distributed firing delay, we propose a method for approximating variance of the probability distribution in each place by introducing interval firing speeds on the fluid model. We next show that the models are equivalently represented by piecewise linear systems with interval parameters. For simulation of the models, two methods are proposed: one is an extension of the interval methods for ordinary differential equations, and the other is acceleration technique for the computation in the box abstraction, a discrete abstraction technique for continuous-state systems.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,800,000	540,000	2,340,000
2010 年度	800,000	240,000	1,040,000
2011 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：システム科学・工学
科研費の分科・細目：情報学・情報学基礎
キーワード：形式検証 ，形式手法，ハイブリッドシステム，実時間システム，性能評価

１．研究開始当初の背景

ソフトウェア工学の分野では，ソフトウェアの高信頼化を目的として形式技法（フォーマルアプローチ）という新しい設計手法が導入されつつある。これは，ソフトウェアに対する要求仕様や制約条件を数理的に取り扱い可能な形でモデル化し，設計の正しさを数学的に保障する手法である。近年，計算機の高性能化や新しい検証アルゴリズムの考案，高性能な定理証明系の出現により，その適用範囲は大きく広がりつつある。しかしながら，形式技法を多くの並行プロセスが存在するような情報システムに適用しようとしたとき，状態空間のサイ

ズがプロセス数に対して指数関数的に増加する状態空間爆発の問題が発生し，現実的な時間での検証を困難なものにしている。従来，有限ではあるが非常の多くの状態を持つシステムを取り扱うため，２分決定グラフによる状態空間表現，高速な SAT ソルバーによる有界モデル検査，述語抽象化による検証など，様々なアイデアが取り入れられてきたが，未だに状態空間爆発が実用規模のシステム検証を行う際の大きな障害であることに変わりはない。

２．研究の目的

本研究の目的は，離散ダイナミクスの流体化(fluidification)という近似手法を用いて，多数の同型な並行プロセスが動作する離散状態システムの安全性検証を高速に行う方法を開発することである。単に計算時間を削減するだけでなく，システム内で動作する並行プロセス数に対してスケーラブルな検証アルゴリズムの開発を目指す。ここでスケーラブルの意味は，並行プロセス数に対し計算時間が線形以下のオーダーになるという意味である。対象とするのは，多数の同型な並行プロセスからなる，確率的時間システムである。すなわち，状態遷移に関して遅延時間などに関する時間パラメータを含むような実時間システムである。

３．研究の方法

図１に確率ペトリネットにおける流体化の考え方を示す。左のプレース p_i から右のプレース p_j に遷移する発火率 λ_i が指数分布で与えられるならば，そのふるまいは各プレースのトークン数を表す連続変数 x_i，x_j に関する微分方程式で近似できる。このとき，微分方程式の解は指数分布の状態遷移における期待値に一致する。 各トランジションの発火に伴う状態遷移をこのような微分方程式で記述し，連立微分方程式系の解として可到達状態を近似的に計算するのが流体モデルの考え方である。

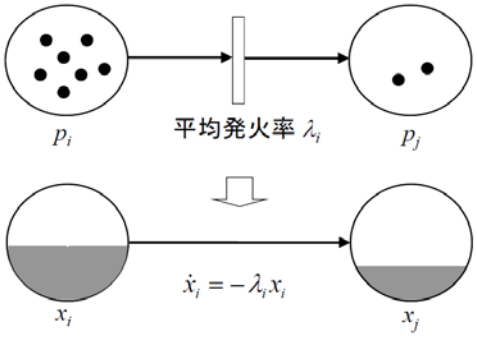

図１．流体モデルの考え方

上記の近似は，システムの平均的ふるまいを近似的に計算するものであり，１次モーメントに関する近似といえる。本研究では，2 次モーメントである分散を考慮した可到達状態の領域を近似的に計算することを目標とする。すなわち，確率分布の分散を用い，ある程度以上の確率で到達する状態の集合を近似的に求める方法を開発する。これにより，危険状態に到達する確率がある値以下であるといった形での安全性検証が可能になる。

４．研究成果

(1) 一般化確率ペトリネットのふるまいを近似する流体モデルの提案と区分的線形システムによる等価表現

一般化確率ペトリネット(GSPN: Generalized Stochastic Petri Nets)は，確率ペトリネットでは最もよく使用されるモデル化手法であり，システムの性能評価に用いられる。本研究では，GSPN における離散変数を連続変数で置き換え，発火率を発火速度に置き換え，さらに即時発火トランジションによる状態遷移を「流れのルーティング」の形で近似する RTCPN: Routing Timed Continuous Petri Nets を提案した。さらに，RTCPN のふるまいが区分的線形システムとして表現可能なことを証明した。

(2) 確率分布の分散を反映した流体化近似手法の開発

指数分布の発火遅延時間をもつ一般化確率ペトリネットにおいて，各プレースにおける確率分布の分散を，流体化モデルにおけるトランジションの区間発火速度で代替的に表現する方法を開発した。具体的には，平均 μ, 分散 σ^2 の確率分布を，区間 $[\mu - r\sigma,\ \mu + r\sigma]$（$r$ は区間幅を指定するパラメータ）の形で計算するために区間発火速度を導入した。すなわち，区間微分方程式

$$[\dot{x}_i] = -[\lambda_i][x_i]$$

の解として区間 $[\mu - r\sigma,\ \mu + r\sigma]$ が得られるような区間発火速度 $[\lambda_i]$ を計算するための方法を与えた。

提案手法は，各プレースのトークン数の確率分布がすべて独立であるときに正しいシミュレーション結果を与える。しかし，各プレースのトークン数の分布は一般には従属であるため，それを補完する情報としてプレースインバリアントを利用する方法を提案した。

(3) 区間パラメータを含む区分的線形システムに対する区間法の開発

本研究では，与えられた流体化モデルに対

し，初期状態から各時点における到達可能状態集合を逐次計算していくことにより安全性検証を行うことを想定しているが，このための方法として区間法(interval methods)を用いる。区間法とは常微分方程式の初期値問題に対する解法であり，テイラー展開における高次の項を無視したときの誤差を包含した解の区間を求めることができる。得られた結果は真の解をかならず包含することが保証される。

流体化近似においては，区間パラメータを含む区分的線形システムの解を区間の形で求める必要がある。区間法を区分的線形システムに適用する際に問題になるのがモード遷移（微分方程式の切り替え）の取り扱い方である。本研究では状態変数ベクトルの集合を，モードを決定する領域の境界で分割するアプローチを採用した。ただし，そのままでは分割数が非常に大きくなるので，領域数の膨張を低減するための計算方法について検討した。さらに，分割された多数の小領域に対する遷移計算を効率的に扱うためのデータ構造および実装方法を開発した。

(4) 区分的線形システムの述語抽象化の高速化に関する研究

流体化モデルのシミュレーションを高速に行うための方法として述語抽象化(predicate abstraction)に着目し，計算の高速化のための新しい近似手法を開発した。述語抽象化とは，状態空間を与えられた述語集合により分割し，その上の離散的状態遷移で近似する手法である。しかし，述語により抽象化された状態空間は述語数の指数関数的な数の離散状態を含むため，計算の効率化が必要である。

本研究では，矩形により状態空間を分割する箱抽象化(box abstraction)の手法に着目し（図２），個々の箱間の遷移関係を計算するのではなく，複数の箱を含む拡張領域間の遷移関係の論理演算により，箱間の遷移関係を近似的に計算する手法を提案した。また，遷移関係の論理演算を高速に実行するために，データ構造として２分決定グラフを採用した。

平成 21－22 年度は２次元の状態空間に対して箱抽象化の高速化に関する研究を行い，平成 23 年度には手法の多次元への拡張を行った。計算機実験により計算速度および近似精度を評価し，提案手法の有効性を確認した。

(5) ワークフローシステムへの適用

提案手法による安全性検証をワークフローシステムの例題に適用し，厳密解法と比較することで有効性を確認した。図３は学術論文誌における論文査読プロセスを GSPN によりモデル化したものである。投稿された論文は 1 回目の査読により採録，条件付き採録，不採録のいずれかの結果になる。条件付き採録の場合は，2 回目の査読により条件付き採録，不採録のいずれかの結果になる。査読期間をトランジション発火の遅延時間で，採録，条件付き採録，不採録の決定は即時発火トランジションの重みとして確率的に与えた。投稿論文数に対して十分な数の編集委員が存在するかどうかを検証するのが例題の目的である。具体的には，プレース editor pool のトークン数 x_p が低い確率でしか 0 にならないことを検証することになる。

計算機実験の結果，提案手法で計算された区間は厳密解法により得られる区間を含むことが確認された（図４，図５）。また，厳密解法では状態数が 2,598,960 となり，計算時間は 335 秒かかったが，提案手法では計算は 1 秒以内で終了し，提案手法の優位性が示された。

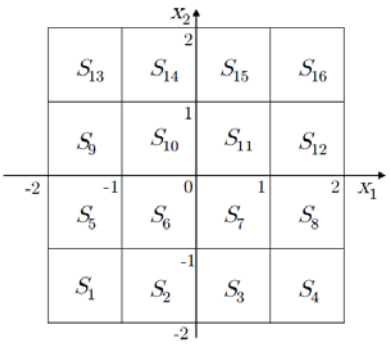

図２．箱抽象化（2 次元の場合）

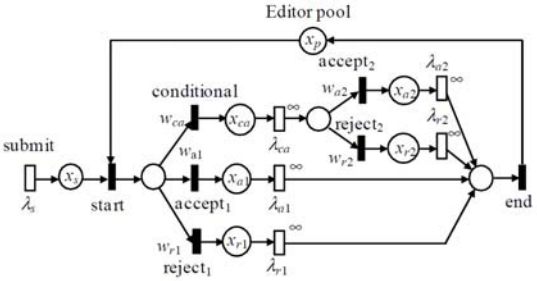

図３．論文査読プロセスのモデル

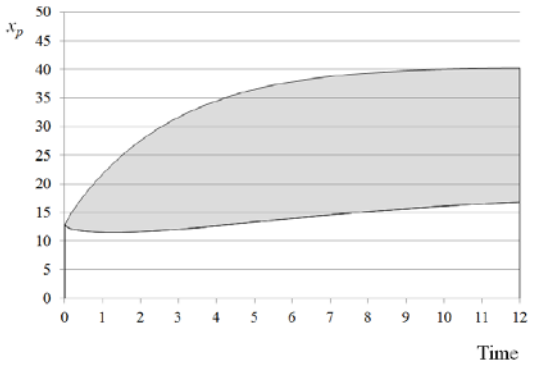

図４．提案手法で計算された x_p の区間

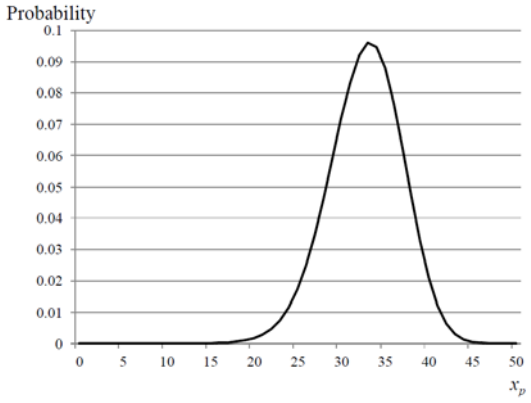

図５．厳密解法による x_p の確率分布

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 7 件）
① Kunihiko Hiraishi: Simulating Stochastic Discrete Event Systems by Difference Equations with Interval Parameters, Proc. IEEE IECON2011, pp.3669-3674 (2011) 査読有
② K. Hiraishi and K. Kobayashi: An Approximation Algorithm for Box Abstraction of Transition Systems on Real Vector Fields, 計測自動制御学会第 48 回離散事象システム研究会予稿集, pp.49-56 (2010) 査読無
③ Kunihiko Hiraishi: On Analysis of a Class of Timed Continuous Petri Nets and Its Applications, Proc. SICE Annual Conference 2010, pp.2253-2259 (2010) 査読有
④ Koichi Kobayashi and Kunihiko Hiraishi: MLD-Based Modeling of Hybrid Systems with Parameter Uncertainty, IEICE Trans. Fundamentals, Vol.E92-A, No.11, pp.2745-2754 (2009) 査読有
⑤ 平石邦彦, 小林孝一: ハイブリッドシステムにおける述語抽象化計算の効率化, 計測自動制御学会第 45 回離散事象システム研究会予稿集, pp.53-58 (2009) 査読無
⑥ Kunihiko Hiraishi and Koichi Kobayashi: A Faster Approximation Technique for Predicate Abstraction of Hybrid Systems, Proc. ICCAS- SICE2009, pp.1717-1721 (2009) 査読有
⑦ Koichi Kobayashi and Kunihiko Hiraishi: Analysis and Control of Hybrid Systems with Parameter Uncertainty Based on Interval Methods, Proc. 2009 American Control Conference, pp.3632-3637 (2009) 査読有

〔学会発表〕（計 6 件）
① Kunihiko Hiraishi: Simulating Stochastic Discrete Event Systems by Difference Equations with Interval Parameters, IEEE IECON2011, 2011/11/07-10, Melbourne, Australia
② K. Hiraishi, K. Kobayashi: An Approximation Algorithm for Box Abstraction of Transition Systems on Real Vector Fields, 計測自動制御学会離散事象システム研究会, 2010/12/9, 名古屋市, 愛知
③ Kunihiko Hiraishi: On Analysis of a Class of Timed Continuous Petri Nets and Its Applications, SICE Annual Conference 2010, 2010/08/18-21, Taipei, Taiwan
④ 平石邦彦, 小林孝一: ハイブリッドシステムにおける述語抽象化計算の効率化, 計測自動制御学会第 45 回離散事象システム研究会, 2009/12/7, 港区, 東京
⑤ Kunihiko Hiraishi and Koichi Kobayashi: A Faster Approximation Technique for Predicate Abstraction of Hybrid Systems, ICCAS-SICE2009, 2009/8/18-21, 福岡市, 福岡
⑥ Koichi Kobayashi and Kunihiko Hiraishi: Analysis and Control of Hybrid Systems with Parameter Uncertainty Based on Interval Methods, 2009 American Control Conference, 2009/6/10-12, St. Louis, USA

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕
ホームページ等
なし

６．研究組織
(1)研究代表者
平石　邦彦（HIRAISHI KUNIHIKO）
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：40251970

(2)研究分担者
小林　孝一（KOBAYASHI KOICHI）
北陸先端科学技術大学院大学・情報科学研究科・助教
研究者番号：50452115

(3)連携研究者　なし