ハイブリッドシステムの述語抽象化計算の高速化に関する研究

田中　祐輔 (710045)

北陸先端科学技術大学院大学 情報科学研究科

2009 年 2 月 5 日

キーワード: ハイブリッドシステム，安全性検証，述語抽象化，BDD(二分決定グラフ)，到達可能性.

ハイブリッドシステムとは，微分方程式に代表される連続ダイナミクス，および，有限オートマトンに代表される離散ダイナミクスの両方を持ったシステムである．組込みシステムの解析や設計に有効であり，多くのアプリケーションに対する数学的モデルとして使われている．その例としては，自動車や自動運転システム，航空交通管理システム，生産システム，化学プロセス，ロボット工学，プラント制御，リアルタイム通信ネットワーク，リアルタイム回路などがあり，制御理論や計算機科学の分野において非常に多くの研究がなされている．ハイブリッドシステムの解析に関する研究の一つとしてシステム検証があり，その中心的問題として安全性検証問題がある．安全性検証問題とは，初期状態から探索を始め，安全でない状態に到達するかどうかを判定する問題である．もし，安全でない状態に到達した場合は，そのシステムは安全でない．ハイブリッドシステムにおける安全性検証問題は一般的に決定不能であることが分かっている．そこで，ハイブリッドシステムでの到達可能な状態を近似的に計算する述語抽象化という手法が提案されている．

述語抽象化とは，複雑な無限状態システムから抽象的な有限状態システムに変換する手法である．ソースコードの検証において実績のある述語抽象化は，変数の値そのものではなく，述語により連続状態空間を抽象状態空間に分割することで，実数値間の遷移から領域間の遷移を考えることが出来る．しかし，抽象状態は連続状態の上近似をとるため，元の連続状態空間では安全性が保証されているが，抽象状態空間では安全でない抽象状態に到達してしまう可能性がある．これは領域間の遷移を考えるので，遷移先が増加し，その結果，安全でない抽象状態に到達する可能性が存在するためである．その可能性を排除するために，反例を用いて抽象状態を精練する手法がある．反例とは安全でない抽象状態に到達してしまうとレースであり，抽象状態空間に反例が存在しないならば，システムが安全であると判断できる．抽象状態空間において反例が存在し，なおかつ，元の連続状態空間においても反例が存在するならば，新しい述語を追加し，もう一度探索を開始する．

この反例による精練を用いて詳細に検査することで，安全でない抽象状態に到達する可能性を低減することが出来る．しかしながら，述語抽象化において述語の数の増加に伴い，抽象状態の数が増加し，その結果，抽象状態から抽象状態への遷移計算回数が指数関数的に増加するという問題が発生する．また，抽象状態への遷移計算自体が複雑となる場合がある．この遷移計算回数が増加すると，安全性検証問題の計算時間が膨大となる．実用的なシステムにおいては，述語の数が膨大になると予想されるため，これらの問題が実用的なシステムへの適用の妨げになると考えられる．

以上を踏まえ，本研究では，これらの問題の解決法を提案し，述語抽象化における安全性検証問題での抽象状態から抽象状態への遷移計算回数を低減し，述語抽象化計算の高速化を目的とする．抽象状態から抽象状態への遷移計算回数が指数関数的に増加するという問題に対しては，集合の包含関係を用いる．集合と集合の積集合から到達可能な集合は集合から到達可能な集合の積集合によって上近似される性質を述語抽象化における遷移計算に用いる．抽象状態から遷移先の状態の計算を行う際に，抽象状態を包含する抽象状態の集合積を用いることで，遷移先の状態の上近似を計算し，遷移計算回数の低減を図る．初期時刻の抽象状態から到達可能な抽象状態は，初期時刻の抽象状態を包含する抽象状態から到達可能な抽象状態の集合積を用いることで，上近似を取ることが出来る．述語抽象化における従来の遷移計算は各抽象状態から到達可能な抽象状態を計算するのに対して，抽象状態の集合積を用いて到達可能な抽象状態を計算することで，各抽象状態から到達可能な抽象状態を計算する必要がなく，遷移計算回数の低減することがが考えられる．

本研究では，ハイブリッドシステムのモデルとして離散時間区分的線形システムを扱う．格子状の離散時間区分的線形システムを扱うことで，拡大抽象状態の選択を容易にしている．この離散時間区分的線形システムにおいて各抽象状態から到達可能な抽象状態の計算を行い，従来手法と提案する抽象状態の集合積を用いる手法との比較を行う．また，さらなる計算回数低減のため，モード遷移のない線形システムにおいても遷移計算を行い，従来手法と提案手法とを比較する．次に，抽象状態から抽象状態への計算自体が複雑であるという問題に対しては，二分決定グラフ (BDD: Binary Decision Diagram) を適用することで計算の効率化を図る．抽象状態は 0-1 変数で表現可能であり，抽象状態の遷移はブール代数で表現するので，抽象状態から到達可能な抽象状態の決定に BDD を用いることが出来る．したがって，本研究では，従来手法と集合の包含関係を適用させた提案手法との遷移計算に BDD を用いて比較を行い，検証する．