入力値のみ保持する変数をもつEFSM群に対する動的性質検証システムの実装

2Z-6

平田雅之　山崎謙治　岡野浩三　谷口健一
大阪大学 大学院基礎工学研究科 情報数理系専攻

1　まえがき

オートマトンモデルに基づく形式的検証では，回路を有限状態機械でモデル化し，記号モデル検査法 [1] を用いることにより，与えられた性質を満たすことを証明する [2],[3]．著者らは，レジスタが扱え，かつ複数のEFSMが(非)同期に動作することにより並列動作が表されるモデル EFSM/int system をすでに提案した [4]．本原稿では，既に提案している自動検証アルゴリズムの概略と実装および例題への適応について述べる．

2　モデル

提案している EFSM/int system は複数の拡張有限状態機械機械 (EFSM/int+) により構成される．それぞれの EFSM/int+は，基本的には非同期遷移を行なうが，複数の EFSM/int+間における同期遷移を行なうこともできる．各 EFSM/int+はそれぞれ任意の整数入力値を保持するような独自のレジスタを持つ．他の EFSM/int+が持っているレジスタに値を入力することはできないが，その値を読み出すことは許している．

3　アルゴリズムの概略

検証性質は，対象となる回路をモデル化した拡張有限状態機械上の状態名とその状態におけるレジスタの値の線形論理式の組に時相演算子を付け加えることにより表している．例えば EF($[(x > 1 \ \& \ y > 2)]@a3$ && $[(x > 2 \ \& \ y < 4)]@b4$) は，与えられてた EFSM/int system において，いつか以下のような状態にたどりつくようなある初期状態が存在するという性質を表す．その状態では拡張有限状態機械 a においては状態が $a3$ であり，かつ拡張有限状態機械 b においては状態が $b4$ である．またそのときそれぞれレジスタ x の値は 1 より大きくかつ 2 より大きい，レジスタ y の値は 2 より大きく 4 より小さいという条件を満たしている．

そのような性質を表す式 f を，EFSM/int system が満たすことの判定は次のように行う．f の最小部分式から，それに対応する抽象状態* の集合を求める．ついで，式の構成に従い，帰納的に，各部分式に対応する抽象状態集合を制御状態名とレジスタの値の範囲に関する論理式として，順次求めていき，最終的に得られた式の充足可能性を判定する．得られた結果が求めたい判定結果となる．

4　アルゴリズムの実際と実装

ここでは EFf を例にして抽象状態の求め方を説明する．f とは抽象状態を表す式である．

まず，f により指定されている状態からバックトレースを行うことにより，f で指定されている状態に到達可能な状態を調べていく．バックトレースを行う際に，その遷移が可能かどうかを調べる．バックトレースの際には，遷移前の状態におけるレジスタの値がその遷移条件を見たし，かつ遷移後のレジスタが見たすべき条件を満たしているときのみ遷移可能であるとみなす．さらに同期遷移においては，同じ同期イベントにより行なわれる遷移全てにおいて遷移可能であることが必要である．

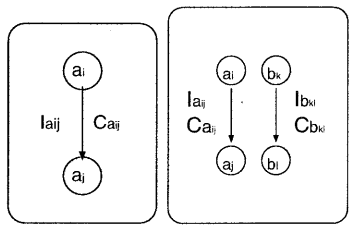

図 1: 非同期遷移 (左) と同期遷移 (右)

図 1 左のように非同期遷移の場合，a_j においてレジ

An implementation of Symbolic Model Checking Algorithm for a System consisting of Extended Finite Machines with Integer Input Registers.
Masayuki Hirata, Kenji Yamasaki, Kozo Okano and Kenichi Taniguchi
Graduate School of Engineering Science, Osaka University
Toyonaka-shi, Osaka, 560-8531, Japan

* 拡張有限状態機械中のある状態とその状態においてレジスタが満たすべき条件を満たすようなレジスタの値の組合せを抽象状態と呼ぶ

スタの値が満たすべき条件が α_{a_j} のとき，a_i でレジスタの値が満たすべき条件は $\exists x \exists y \ldots \exists z(C_{a_{ij}} \wedge \alpha_{a_j})$ (ただし $x, y, \ldots, z$ はこの遷移で値が入力されるレジスタに対応する変数である) となる．この条件式を Presburger 真偽判定ルーチンを用いてを充足不能であるかの判定を行ない，充足不能であれば，この条件式をこの状態における条件式集合から削除する．

また図 1 右のように同期遷移の場合，a_j，b_l においてそれぞれレジスタの値が満たすべき条件を α_{a_j},α_{b_l} のとき，a_i,b_k でレジスタの値が満たすべき条件はそれぞれ，$\exists x \exists y \ldots \exists z(C_{a_{ij}} \wedge C_{b_{kl}} \wedge \alpha_{a_j})$, $\exists x \exists y \ldots \exists z(C_{a_{ij}} \wedge C_{b_{kl}} \wedge \alpha_{b_l})$ (ただし $x, y, \ldots, z$ はこの遷移で値が入力されるレジスタに対応する変数である) となる．非同期遷移のときと同様に，この条件式の充足不能性を調べ，充足不能であれば削除する．同期遷移の実行条件より，バックトレース後の状態におけるレジスタの値が満たすべき条件として，他の EFSM/int+におけるレジスタの条件が係わってくる．

このようにバックトレースを続けることにより，初期状態におけるレジスタの値が満たすべき条件を求めることができる．バックトレースは，新たな抽象状態が出現しなくなるまで行なう．検査対象となるモデルには閉路におけるレジスタ値の変更に関する制約などを課しているので，一定回数閉路をバックトレースするとそれ以降その閉路のバックトレースにおいては新たな抽象状態を求める必要がないことがわかっている．よって検証におけるバックトレースは有限回で停止できる [4]．

このようにして求めた抽象状態に少なくとも 1 つの初期状態が含まれているかどうかを調べることにより，EFf を判定する．

与えられた拡張有限状態機械と性質から，最終的に，Presburger 文が得られる．この式を Omega などの Presburger 文真偽判定処理系で処理することにより，真偽判定が行なえる．

与えられた拡張有限状態機械と性質から，Presburger 文を導く処理系のプロトタイプを Perl で作成している．

5 評価実験の例題

今回の評価用の例題として以下のようなオークションシステムを記述した．この記述ではオークション参加者が 2 人であり，1 人あたり最大 3 回まで入札ができ，3 つの拡張有限状態機械から構成されている．それぞれの状態数は，20，9，9 で構成されている．またレジスタ数は合計 7 つである．図 2 で示すようにバイヤー A，および B はそれぞれの入札金額をオークショニアに伝えることができ (tender)，オークショニアはその入札金額の大小を判定し，少ない金額の入札者に再入札を促す (invitation)．

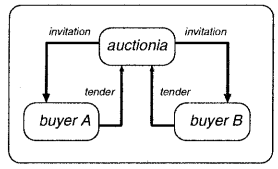

図 2: オークションシステム

この記述に対して検証性質としては，

- どのような入力に対してもバイヤー A と B が同時に落札することはない
- どのような入力に対しても高い入札を行ったバイヤーが落札する
- ある入力に対しては，一人のバイヤーが 3 回入札することなしに落札することがある

といったものが考えられる．この例題ではレジスタにはバイヤーの入札金額の候補などが入力される．これらの各性質と EFSM から導かれる Presburger 文は，それぞれ数百程度のトークン数である．

6 あとがき

本稿では著者らが以前提案したモデルに対するアルゴリズムの概略と実装方針について述べた．また適用例題についても述べた．

今後の課題としては，評価実験を行ない，それをもとに検証時間を短縮することが考えられる†．

また今回提案したモデルの拡張などが挙げられる．

参考文献

[1] Clarke, E. M., Grumberg, O. and Peled, D. A.: *Model Checking*, The MIT Press (1999).

[2] Chan, W., Anderson, R., Beame, P. and Notkin, D.: Combining Constraint Solving and Symbolic Model Checking for a Class of Systems with Non-linear Constraints, in *Proc. of 9th Int'l Conf. on CAV*, Vol. 1254 of *LNCS*, pp. 316–327, Springer-Verlag (1997).

[3] 竹中崇, 岡野浩三, 東野輝夫, 谷口健一:整数入力値を保持するレジスタをもつ EFSM に対する記号モデル検査アルゴリズム, 第 13 回 回路とシステム軽井沢ワークショップ 論文集, pp. 555–560 (2000).

[4] 平田雅之, 岡野浩三, 谷口健一:入力値のみ保持する変数を持つ EFSM 群に対する動的性質の検証, 信学技報, Vol. SS2000 No. 24, pp. 9-16 (2000).

† 検証においては充足不能性を判定することが頻繁におこる．1 回の判定における時間は，対象となる Presburger 文の長さと関係があるため Presburger 文の短縮が必要である．また判定回数自体の削減等も考えられる．