正則時相論理のモデルチェック法の改良と設計検証への適用

3M－7

藤井 寛　濱口 清治　平石 裕実　矢島 脩三

京都大学工学部

1．はじめに

VLSI技術の進歩に伴い、設計される論理回路が大規模化している現在、設計が正しいことを保証するための形式的検証手法の確立が重要となっている。我々はこれまでに、εフリー正則時相論理（εフリーＲＴＬ）を用いた、順序機械の検証手法を示し[1]、これに基づく設計検証システムを作成した[2]。しかし、この方法では設計対象のデータが非常に大きくなるため問題があった、ここではその点を改良した方法を示す。

2．εフリーＲＴＬ[1]

εフリーＲＴＬは、通常の命題論理に３つの時相演算子、○，□，：を加えたものである。

［定義１］εフリーＲＴＬのシンタックス

原始命題の集合をＡＰで表わし、以下に定義するεフリーＲＴＬ式全体の集合をＬＦで表わす。このとき、次に上げる(1)～(3)を有限回適用して得られるもののみが、εフリーＲＴＬ式である。

(1)　$p\in AP$のとき、$p\in LF$.

(2)　$\eta\in LF$のとき、$(\sim\eta),(\Box\eta),(\bigcirc\eta)\in LF$.

(3)　$\eta,\xi\in LF$のとき、$(\eta\vee\xi),(\eta:\xi)\in LF$.　□

εフリーＲＴＬ式は線形モデル上で真偽値が定められる。(Σ,I)をεフリーＲＴＬの線形モデルという。ここに、Σは状態の集合、Ｉは各状態$s\in\Sigma$において真となる原始命題の集合を与える関数$I:\Sigma\rightarrow 2^{AP}$である

［定義２］εフリーＲＴＬ式の真偽値

Σ上の長さ１以上の系列を$\sigma\in\Sigma^{+}(\sigma=s_0\cdots s_n$とする)と表わす。また$\sigma(i)$は$\sigma$のｉ番目の状態、$|\sigma|$は$\sigma$の長さを表わす。$M,\sigma\vDash\eta$は、線形モデルＭの状態系列$\sigma$に対しεフリーＲＴＬ式$\eta$が真であることを表わす。Ｍが明らかなときはＭを省略する。

$p\in AP$、$\eta,\xi\in LF$であり、また、σの長さが２以上のとき $\sigma_1=s_1\cdots s_n$とする。このとき、状態系列σにおけるεフリーＲＴＬ式の真偽を次のように定義する。

(1) $\sigma\vDash p$　iff　$p\in I(\sigma(1))$

(2) $\sigma\vDash(\sim\eta)$　iff　$\sigma\nvDash\eta$

(3) $\sigma\vDash(\eta\vee\xi)$　iff　$\sigma\vDash\eta$　または　$\sigma\vDash\xi$

(4) $\sigma\vDash(\bigcirc\eta)$　iff　$|\sigma|\geq 2$　かつ　$\sigma_1\vDash\eta$

(5) $\sigma\vDash(\Box\eta)$
　　iff　$\sigma_i\vDash\eta$　なる$\sigma_i\in\Sigma^{+}$　$(1\leq i\leq m)$が存在して、$\sigma=\alpha_1\alpha_2\cdots\alpha_m$と表わせる。

(6) $\sigma\vDash(\eta:\xi)$
　　iff　$\sigma_1\vDash\eta$　かつ　$\sigma_2\vDash\xi$なる$\sigma_1,\sigma_2\in\Sigma^{+}$
　　が存在して、$\sigma=\alpha_1\alpha_2$と表わせる。□

3．順序機械の設計検証

εフリーＲＴＬを用いて順序機械の設計検証を行う問題を考える。設計として、２値の入出力信号をもつ順序機械を対象にする。仕様としては、順序機械の各信号線に対し原始命題を割り当て、設計対象の順序機械の入出力の系列が満たすべき性質をεフリーＲＴＬ式Specで記述したもので与える。このとき、設計検証の問題は、設計対象の順序機械のすべての可能な有限長の入出力の系列に対して、ＲＴＬ式Specが真になることを確かめることになる。

［定義３］構造モデルとその上での真偽判定

$K=(\Sigma,m,R,\Sigma_0)$を構造モデルという。ここで、(Σ,I)はεフリーＲＴＬの線形モデル、ＲはΣ上の２項関係で、任意の状態$s\in\Sigma$に対して$(s,s')\in R$となる状態ｓ'が存在するものとし、Σ_0は初期状態の集合を表わすとする。構造モデルＫにおいて、状態$s\in\Sigma_0$からのＫ上の有限長のパスσの中で$\sigma\vDash\eta$となるものが存在するとき、ηはＫのもとで真である(K-true)という。また、それ以外のときＫのもとで偽である（K-false)という。□

順序機械Ｍの設計検証としては、Ｍの初期状態からのすべての入出力に１対１対応するパスを持つ構造モデルＫを構成し、～SpecがK-falseになることを確かめればよい。

順序機械Ｍに対応する構造モデルＫは次のようにして作る。Ｋの各状態s_kはＭの状態遷移図の枝に１対１対応しており、状態s_i,s_jが$(s_i,s_j)\in R$となるのは、順序機械の、s_iに対応している状態遷移の遷移先の状態をｓとするとき、s_jがｓからの状態遷移に対応しているとき、かつそのときに限る。

これまでに、構造モデルＫとεフリーＲＴＬ式ηに対し、ηがK-trueとなるかを調べるモデルチェックアルゴリズムを用いた順序機械の設計検証システムを作成した。しかし、決定性順序機械Ｍの状態数を$|S|$、Ｍの状態遷移図の枝の数を$|E|$、入力信号の数を$|X|$とすると、Ｍに対応する構造モデルのサイズは、
$O(|\Sigma|)=O(|E|)=O(|S|2^{|X|})$

Improved version of model checking of RTL and its application to design verification.

Hiroshi FUJII,Kiyoharu HAMAGUCHI,Hiromi HIRAISHI,Shuzo YAJIMA
Kyoto University

$O(|R|)=O(|E|2^{|X|})=O(|S|2^{2|X|})$
となり、順序機械のサイズに対して、構造モデルのサイズが入力線数の指数倍なり、構造モデルを格納するのに多くの領域が必要であるという問題がある。この点を解決するために、構造モデルを作らずに設計検証を行う方法を述べる。

4．モデルチェックアルゴリズム

［定義4］εフリーＲＴＬ式の微分

εフリーＲＴＬ式ηの状態ｓによる微分η/sつぎのように定義される。

(1) $p/s \triangleq V_T$ ･･･ $p \in I(s)$のとき
$p/s \triangleq V_F$ ･･･ それ以外のとき
(2) $(\sim\eta)/s \triangleq \sim(\eta/s)$
(3) $(\eta \vee \xi)/s \triangleq (\eta/s) \vee (\xi/s)$
(4) $(\bigcirc\eta)/s \triangleq \eta$
(5) $(\Box\eta)/s \triangleq$
$(\eta/s) \vee \{(\eta/s) : \Box\eta\} \vee \Box\eta$
･･･ $s \vdash \eta$のとき
$(\eta/s) \vee \{(\eta/s) : \Box\eta\}$
･･･ それ以外のとき
(6) $(\eta : \xi)/t \triangleq$
$\xi \vee \{(\eta/s) : \xi\}$ ･･･ $s \vdash \eta$のとき
$(\eta/s) : \xi$ ･･･ それ以外のとき

□

η/sについては次の性質がなりたつ。長さ２以上の有限長系列$\sigma=s_0s_1\cdots$に対し、$\sigma \vdash \eta$となる必要十分条件は$\sigma_1 \vdash \eta/s_0$である。

順序機械の初期状態からの可能な有限長の入出力系列σの中に$\sigma \vdash \eta$となるものが存在するかどうか調べるモデルチェックアルゴリズムを示す。

［アルゴリズム］
入力：Mealy型順序機械Ｍとεフリーｒｔｌ式η
出力：$\sigma \vdash \eta$となるものが存在するならtrue、
さもなくばfalse
方法：Ｍの初期状態s_0に対して、次にあげる手続き Check（M,s_0,η）を適用する。

```
procedure Check (M, s, η) ;
  x = label (s, η );
  if x = 'F' then return false;
  if x = 'C' then return false;
  addlabel (s, η, 'C') ;
  for sから出るすべての枝t do
    if ηが長さ1の系列stに対して真 then
        return true;
    else if Check (M, next (s, t), η/st)
                              = true then
        return true;
  addlabel (s, η, 'F') ;
  return false;
end of procedure;
```

Check（Ｍ，ｓ，η）は順序機械Ｍの状態ｓからの入出力の系列σのうち、$\sigma \vdash \eta$となるものがある（ｓにおいてηが真である）かどうかを調べる。
addlabel（ｓ，η，ｘ）は状態ｓのラベルに、ηの値がｘであることを登録する。label（ｓ，η）は状態ｓにおいてηの値がラベルとして登録されているならその値を返し、登録されていないなら空を返す。ラベルはそれぞれ'Ｔ'がηはｓにおいて真であることを、'Ｆ'がηはｓにおいて偽であることを、'Ｃ'がｓにおけるηの真偽値を調査中であることを示している。また、s_tは枝ｔに対応する、ＲＴＬのモデルの状態とする。next(s,t)は順序機械の状態ｓの遷移ｔによる次状態である。

この手続きはＲＴＬ式ηと順序機械Ｍを入力とし、ηがＭの状態ｓにおいて真ならばtrueを返し、そうでないならfalseを返す。

5．モデルチェッカの設計検証への適用

４．で述べたアルゴリズムに基づくモデルチェッカをsun3/60上に実現し、実際の順序機械の設計検証に適用した。表１、表２はＤＭＡコントローラ[3]の設計検証に関する、記憶量、実行時間のデータである。ＤＭＡコントローラは、272状態の決定性順序機械として与えられ、信号線数は入力５、出力15である。仕様のεフリーＲＴＬ式は89個の演算子をもつ。また、設計は仕様を満たしている。

表１に、順序機械とそれから得られる構造モデルの状態数、枝数を示す。また、表２には、構造モデル上でのモデルチェックによって設計検証をおこなった場合の処理時間および、今回のモデルチェックアルゴリズムを用いた場合の処理時間を示す。

6．おわりに

εフリーＲＴＬのモデルチェックアルゴリズムを改良し設計検証への適用を行った。更に改良すべき点として、式の微分の効率化等が考えられる。

	順序機械	構造モデル
状態数	272	8704
枝数	8704	278528

表１：順序機械、構造モデルの状態数、枝数

	順序機械	構造モデル
CPU時間（秒）	56.1	77.8

表２：処理時間

参考文献
[1]平石、矢島：正則時相論理による論理設計検証について，電子情報通信学会技術研究報告，COMP87-67，1987.
[2]藤井、浜口、平石、矢島：正則時相論理による論理設計検証システム，1989年電子情報通信学会春季全国大会予稿集A-257
[3]E.M.Clarke,S.Bose,M.C.Browne,and O.Grumberg: The Design and Verification of Finite State Hardware Controllers. Technical Report CMU-CS-87-145,Carnegie Mellon University,1987.