2A-3

形式的手法を用いた論理設計検証網羅性解析に関する一方式

山本 達也† 高山 浩一郎†‡

(株)富士通研究所† 富士通(株)‡

1．はじめに

SoC 設計の大規模化に伴い，論理設計の複雑度が増しており，論理検証にかかる時間の増大が一層問題となっている．従来行われているシミュレーションを用いたHDL ベースの期待値モデルを用いた手法では，正確な仕様分析やアサーション生成が求められているが，アサーションの抜けによる検証モレが生じる可能性や，検証空間を網羅する入力ベクタを生成することが困難である，という課題があった．これに対し，形式的検証では入力ベクタを必要としない点に特徴があるが，状態数が増えると検証が終息しないことから，大規模回路の検証にはやはり期待値モデルを用いた検証が行われてきた．

従来バスプロトコルなどのインタフェースの検証は，信号レベルのタイミング仕様を記述し，アサーションに変換することで検証が行われてきた．インタフェース仕様記述言語(CWL[1]等)を用いて，トランザクションのタイミングおよびパターンを記述することが可能である．一方でこれらはサイクルレベルで扱われており，抽象度が高いプロトコルレベルの検証へは適用できないという課題があった．

本報告では，論理シミュレーションと形式的手法を連携することで，大規模な設計に対するプロトコルレベルでの検証網羅性を解析，向上する手法を提案する．さらに，USB3.0 プロトコル[2]を例題として，提案手法のフィージビリティを確認した．

2．モデル検査ツール SPIN と Promela

プロトコル記述に適した形式的仕様記述言語として，モデル検査ツール SPIN[3]およびモデル記述言語 Promela(Process Meta Language)について説明する．Promela は非決定性の構文を持つ点に特徴があり，チャネル構文によってプロトコル仕様を容易に表現できる．

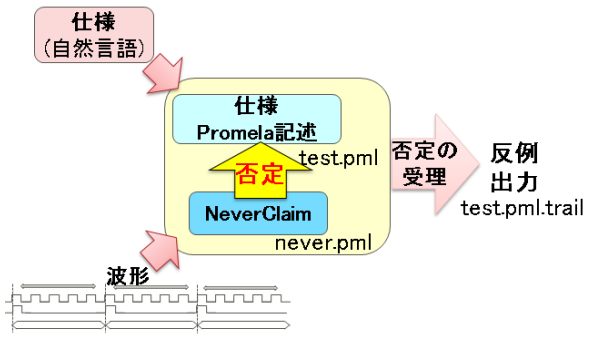

図 1. NeverClaim 記述

さらに，NeverClaim 構文を用いることで仕様モデルに対して，非成立の状態遷移モデルを定義可能である．

A method for coverage analysis of logic verification using a formal technique.
†Tatsuya Yamamoto Fujitsu Laboratories Ltd
‡Koichiro Takayama Fujitsu Ltd

SPIN モデルチェック実行時に NeverClaim で規定した条件に該当した場合に反例を出力する(図 1)．反例とは，非成立の状態遷移シーケンスを示す．

3．提案手法

提案する検証網羅性解析手法を図 2 に示す．仕様モデルと，シミュレーション結果から生成した動作シーケンスから生成した NeverClaim 制約を用いてモデル検査ツールによって反例を出力する．これにより，仕様に対してシミュレーションが網羅していないシーケンスを検出する．

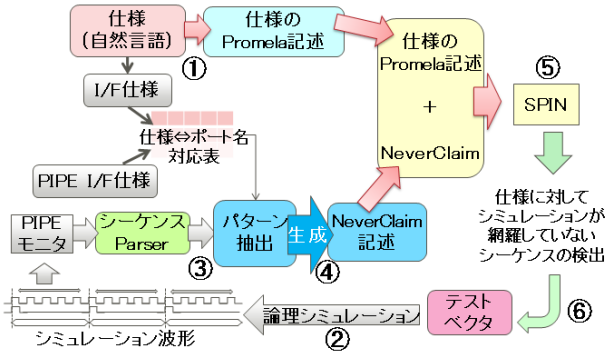

図 2. 提案する検証網羅性解析

従来の形式的検証と，本提案手法との比較を図 3 に示す．従来のモデル検査ツールによる形式的検証(図 3(a))では，仕様から生成したプロパティを基に，プロパティに違反するシーケンスを反例として出力する．

これに対して提案手法(図 3(b))では，仕様に対してシミュレーションで網羅されていないシーケンスが反例として出力される．このシーケンスを参照して，シミュレーションの入力ベクタを改善することにより，仕様に対する論理シミュレーションの網羅性向上が可能となる．

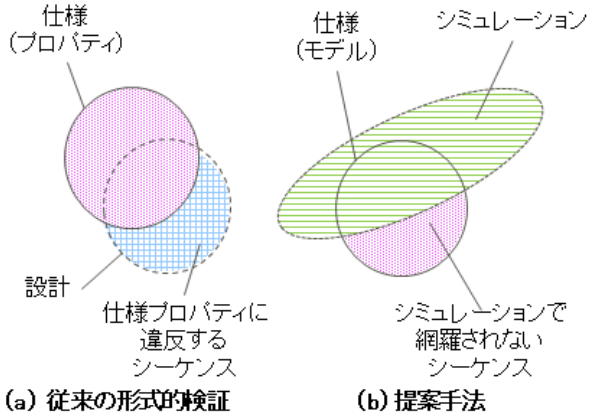

図 3. 従来手法と提案手法の比較

また，出力波形からシーケンスパターンへ抽象度を上げることで，従来サイクルレベルで扱っていたイン

タフェース検証に対して抽象度の高い検証や複数プロトコルレイヤを含む検証を可能とする．本提案の実行ステップを以下に示す．項目の数字は図 2 中の番号に対応する．

① インタフェースプロトコル仕様を形式的記述言語により記述(仕様モデル)
② 検証対象(設計)をテストベクタにてシミュレーション実行
③ 出力波形からシーケンスパターンを取得
④ シーケンスパターンを制約記述へ変換
⑤ 仕様モデルと制約記述に対しモデル検査ツール実行
⑥ モデル検査ツール反例出力を基に入力ベクタを改善

4．実験

(1) 仕様モデル

実験では，仕様モデルの記述対象として，USB3.0 プロトコル仕様[2]のバルク転送を選択した．プロトコルレイヤ及びリンクレイヤを含めた環境において正常系(U0)シングル転送に対してモデルを構築した．USB3.0 SuperSpeed モードでのプロトコルレイヤにおけるシングル転送を図 4 に示す．ここでは DPH(Data Packet Header)と DPP(Data packet Payload)について DP(Data Packet)として記載した．

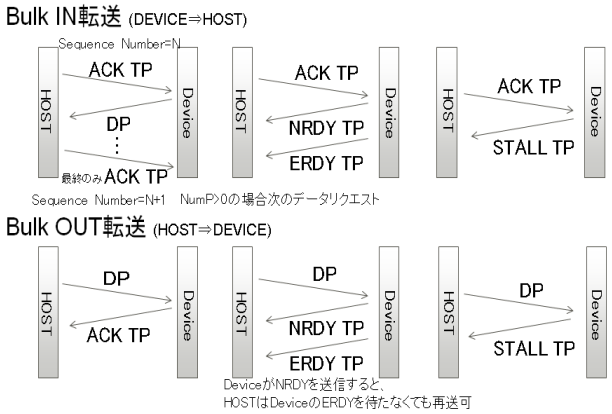

図 4. プロトコルレイヤでのシングル転送

前述の USB3.0 プロトコル仕様を Promela を用いて記述した．複数レイヤ含む仕様モデルを記述するために，USB3.0 のプロトコルレイヤおよびリンクレイヤのモデルを実装した(図 5)．

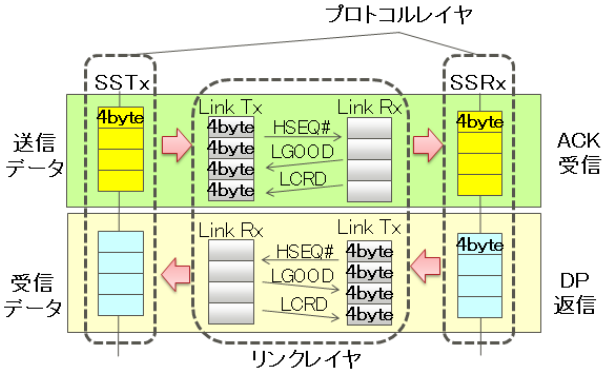

図 5. 実装したモデル上での転送

(3) NeverClaim 制約

USB3.0 における SuperSpeed モードの仕様では，ACK 毎に DP を転送する必要はなく，転送パケット数(NumP)が 0 でない限り DP を連続で転送可能であり，NumP=0 のタイミングで ACK を転送し終了する．(図 6(a))．

一方，ここで想定した動作では NumP での判定がなく ACK 毎に DP を転送する(図 6(b))，そのためシミュレーション波形から得られた NeverClaim(図 6(c))と USB3.0 仕様における SuperSpeed モードバルク(シングル)転送に対して記述したモデルを用いて SPIN 実行を行うと，DP の連続転送に対して NeverClaim が受理され，trail ファイル[3]が出力される．

図 6(c)ではプロトコルレイヤの TP および，リンクレイヤにおけるパケットに対する NeverClaim 記述を示した．NeverClaim 記述に複数レイヤに対する制約を併記することで，複数レイヤを含む NeverClaim 制約付 SPIN 実行が可能である．

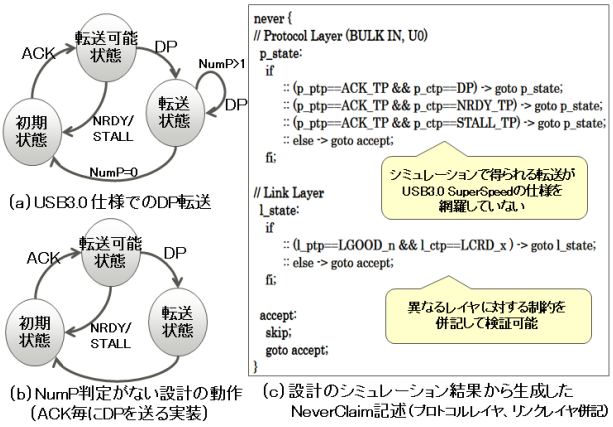

図 6. NeverClaim 受理の様子

SPIN から出力される trail ファイル(反例)には，SPIN 上のステップ実行結果と，NeverClaim 制約に書かれた状態が含まれる．これを参照することで，シミュレーションで未カバーな状態遷移を選定が可能である．また，この状態遷移パスを，シミュレーションの入力ベクタを生成時に活用することで仕様に対するシミュレーションの網羅性を向上する情報として活用できる．

5．まとめ

本報告では，論理シミュレーションと形式的手法を連携し，検証網羅性を解析する一手法を提案し，USB3.0 仕様のバルク転送に対して実装した Promela モデルを用いて反例を抽出する仕組みを示した．今後，実シミュレーション波形からの NeverClaim の生成を行い，モデルの拡張により USB3.0 仕様全体の検証に対する検証網羅性解析手法を構築する予定である．

参考文献

[1] 岩下洋哲ほか：インタフェース仕様記述言語 CWL とその応用．第 15 回 回路とシステムワークショップ，2002.04.22，p.305-310.
[2] Universal Serial Bus 3.0 Specification http://www.usb.org/developers/docs/documents_archive/
[3] SPIN(v6.2.5)/Promela http://spinroot.com/