様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 ２２ 日現在

機関番号：５３３０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ００８９

研究課題名（和文）形式的プロパティ検証の完全性指標の定義とその応用

研究課題名（英文）Development of Coverage Metric for Formal Property Verification

研究代表者
松本　剛史（Matsumoto, Takeshi）

石川工業高等専門学校・電子情報工学科・准教授

研究者番号：４０５３６１４０

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：システム検証の一種であるプロパティ検証と呼ばれる、システムが仕様（プロパティ）を満たすかどうかを確かめる検証方法を対象として、検証がどの程度網羅的に行われているかを示す指標となる検証カバレッジを提案し、その評価を行った。検証においては、システム全体のうち、どの程度の部分が検証できているかを知ることが重要であるが、プロパティ検証ではそのような指標が存在しないため、指標の確立は重要である。本研究では、システムの状態遷移が変化することによって、検証結果がその影響によって変化した場合、検証したプロパティによってその状態遷移が網羅されていると考え、これに基づく検証カバレッジを提案し、評価結果を示した。

研究成果の学術的意義や社会的意義
現在、多くの電子情報機器は大規模なシステムであり、その正しさの検証を効率的に行うことが重要になっている。検証においては、検証対象システムの一部だけを検証しても誤り(バグ)を全て見つけることができないため、どの程度網羅的に検証が行われているかを把握することが必要である。本研究では、システム検証の一種であるプロパティ検証を対象として、検証がどの程度網羅的に行われているかを示す指標を提案し、いくつかの例題において評価を行った。これにより、どれ程のプロパティを検証すれば十分であるかを知る指標とすることができ、さらには、検証結果に対する信頼性・説明可能性が高まることが期待できる。

研究成果の概要（英文）：Property checking, which is a kind of formal verification of state transition systems, verifies that a system under verification satisfies a given property for any input patterns. In this work, we propose a verification coverage of property checking to estimate how much sufficiently a system is verified. Our proposed coverage is based on a ratio of state transitions which affects verification results. A state transition is considered to be covered by a property when the result of property checking differs from the original result by removing the transition. We proposed a coverage metric based on this idea and showed evaluation results for example systems and properties.

研究分野：VLSI設計支援

キーワード：プロパティ検証　回路検証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

現在、多くの電子情報機器は多くのハードウェアとソフトウェアプログラムによって構成される大規模なシステムであり、その規模は急速に増加しており、設計開発期間の長期化が大きな問題となっている。これは、設計に要する期間が長期化していることに加えて、実際の開発期間の 6 割～8 割を占める設計の正しさの検証やデバッグに要する期間が長期化しているためである。本研究では、高い抽象度でシステム全体の設計を行う高位設計を対象として、検証の効率化に寄与できる技術の開発を行う。高位設計においては、後工程におけるバグ発見によって生じる設計のやり直しを防ぐために、動作の正しさの検証が非常に重要である。本研究では、検証の中でも、テストパタンに依存しない形式手法に着目する。形式検証の１つとして、設計が与えられた性質(プロパティ)を満たすことを数学的に証明するプロパティ検証がある。近年、プロパティ検証のベースとなっているモデル検査技術の向上により、高位設計やハードウェア設計を対象とする商用検証ツールも利用されている。プロパティ検証とは、システムの仕様（例えば、「リセット信号が入力されると、システムはリセット状態に必ず戻る」など）を記述して、それをモデル検査ツール等のツールを用いて検証するため、記述されないプロパティは当然検証されることがなく、システムの動作仕様をいかに網羅的にプロパティとして記述するか、に検証の質が大きく依存する。実際に、プロパティの漏れ・不足による設計誤りの見落としは大きな問題となっている。しかし、一方で、プロパティ集合がシステム仕様をどの程度網羅しているかを計る指標については、あまり研究がなされていない。そのような指標が確立されれば、どれ程のプロパティを用意すれば検証が十分と言えるのか、を知ることができ、検証結果に対する信頼性・説明可能性は飛躍的に高まる。さらに、その指標に基づくプロパティ生成の自動化への道も開けると考えられる。

２．研究の目的

（１）プロパティ検証における検証カバレッジの提案
プログラムのカバレッジと同様に、プロパティ検証における検証の網羅性を表す指標である検証カバレッジを提案する。本研究では、システムは有限状態機械として表されるものとし、プロパティによって網羅された状態数や遷移数に基づいた検証カバレッジを提案することを考える。

（２）提案検証カバレッジを計算する方法の考案
（１）において、有限状態機械に対して定義されたプロパティの網羅性指標（カバレッジ）は、実際のシステム例やプロパティ例に対して、できるだけ短い計算時間で計算する必要がある。そこで、モデル検査ツール等の既存手法・ツールを用いて、提案検証カバレッジを計算する方法を確立することを目指す。

（３）提案検証カバレッジの評価
提案検証カバレッジおよびカバレッジ計算方法の妥当性を評価するために、いくつかのシステム例・プロパティ例について、カバレッジ計算とその結果の評価を行う。特に、プロパティごとにカバレッジにどのような差が生じるか、プロパティによってカバレッジ計算に要する時間が異なるのか、といった点を明らかにすることを目指す。

３．研究の方法

（１）プロパティ検証に対する検証カバレッジの定義
プログラムやハードウェア設計記述で既に用いられているカバレッジを参考にして、また、いくつかのシステム例・プロパティ例において直観的にシステムのどの部分の正しさが検証されているのかを考察することにより、プロパティ検証における検証カバレッジの定義を考案する。プロパティ検証では、プロパティごとに検証結果（システムがプロパティを満たす、または、満たさない）が得られることから、システムを表す有限状態機械のどの範囲がプロパティの成否に関わっているのかを表すことを考える。そこで、既存のカバレッジのうち、ミューテーション解析で用いられているものが参考になると考えられる。

（２）提案検証カバレッジの計算方法の考案
（１）で考案される検証カバレッジにもよるが、カバレッジの計算は既存のモデル検査ツールまたは SAT ソルバ（命題論理式の充足可能性判定を行うソフトウェア）を用いて行うことを検討する。本研究では、提案検証カバレッジの評価を当面の目的とするため、ハードウェア設計記述言語 Verilog HDL を用いて、検証対象システムを記述する。この Verilog HDL 記述に対して、検

証カバレッジの計算に必要となる記述を追加し、それを既存モデル検査ツールまたは SAT ソルバに与えることによって、検証カバレッジを計算する方法を採用する。

（3）提案検証カバレッジの評価
（2）で考案した計算方法によって提案検証カバレッジの評価を行い、カバレッジの計算に要する時間やプロパティごとのカバレッジ値について評価を行う。評価対象としては、車感応式信号機の制御システムに対するプロパティ 14 個とエレベータ制御システムに対するプロパティ 4 個を用いる。プロパティは、時相論理 LTL によって記述する。

４．研究成果

（1）検証カバレッジの提案
本研究では、検証対象の状態遷移システムにおいて、システムが持つ状態遷移のうち、その有無がプロパティ検証の検証結果に影響を与える割合によって、プロパティ網羅性を表す検証カバレッジとすることを提案する。検証対象の状態遷移システムに対してあるプロパティを検証した結果と、検証対象のシステムからある状態遷移を削除して得られるシステムで同じプロパティを検証した結果が異なるのであれば、削除された状態遷移はプロパティの検証でチェックされていると考えられる。そのため、そのプロパティの検証において、削除された状態遷移を網羅していると言ってよいと考えられる。

（2）提案検証カバレッジの計算
（1）の検証カバレッジを計算するためには、原理的には、検証対象システムの状態遷移の 1 つ 1 つについて、その遷移を削除したシステムを作成し、モデル検査ツールを用いて検証結果が遷移の削除によって変化するかどうかを調べればよい。しかし、この方法では、ある程度大きなシステムの検証は不可能である。そこで、本研究では、システムに検証カバレッジ計算用の外部入力信号を用意して、その信号によって、状態遷移を削除するか（実際には、状態遷移を削除すると、ダミー状態に遷移するようにする）削除しないかを制御し、検証結果を変化させるような入力信号が存在するかを SAT ソルバによって求めることとした。この方法で、検証カバレッジの計算をしたところ、信号機制御システムに対して 1 プロパティあたり 1 秒以内の時間で、提案検証カバレッジが計算できることを確認できた。

（3）提案検証カバレッジの評価結果
（2）で計算された検証カバレッジを解析したところ、プロパティによって、カバレッジの値は大きく異なることが分かった。例えば、評価に用いたプロパティの中には、システムで成立しないプロパティも含まれているが、そのようなプロパティでは、どの状態遷移を削除しても成り立たず（つまり、検証結果が変化せず）、提案検証カバレッジでは値がゼロとなるものがあった。また、「常に、信号の赤・青・黄の 1 つ以上が点灯する」というプロパティ例では、どの状態遷移を削除した場合にも、検証結果がプロパティ成立から不成立に変化したため、カバレッジは 100%となった。このように、プロパティごとに検証カバレッジは異なる値が得られており、提案検証カバレッジは、プロパティがシステムの状態遷移のうちどの程度の影響を受けるかを知るための 1 つの指標になり得ることを示せた。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 河上悠輝，松本剛史
２．発表標題 プロパティ検証における検証カバレッジの定義と評価
３．学会等名 令和元年度北陸地区学生による研究発表会
４．発表年 2020年

１．発表者名 道畑萌絵，松本剛史
２．発表標題 学生実験用CPU回路のデバッグ支援に関する研究
３．学会等名 平成30年度北陸地区学生による研究発表会
４．発表年 2019年

１．発表者名 山元美奈，松本剛史
２．発表標題 FPGAが搭載されたSoC上での画像処理の実装と評価
３．学会等名 平成29年度北陸地区学生による研究発表会
４．発表年 2018年

１．発表者名 山本巧，松本剛史
２．発表標題 SAT問題への定式化によるブレッドボード回路の自動配線
３．学会等名 平成29年度北陸地区学生による研究発表会
４．発表年 2018年

１．発表者名 Qinhao Wang, Amir Masoud Gharehbaghi, Takeshi Matsumoto, Masahiro Fujita
２．発表標題 High-Level Engineering Change Through Programmable Datapath and SMT Solvers
３．学会等名 IEEE International Symposium on Circuits and Systems（国際学会）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関