JAIST Repository
https://dspace.jaist.ac.jp/

Title	モデル検査におけるゴール指向分析を用いた外部入力値の時系列変化の制約による状態削減手法
Author(s)	乾，道孝
Citation	
Issue Date	2014-09
Type	Thesis or Dissertation
Text version	ETD
URL	http://hdl.handle.net/10119/12286
Rights	
Description	Supervisor:鈴木　正人，情報科学研究科，博士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

氏名	乾　道孝			
学位の種類	博士(情報科学)			
学位記番号	博情第 309 号			
学位授与年月日	平成 26 年 9 月 24 日			
論文題目	モデル検査におけるゴール指向分析を用いた外部入力値の時系列変化の制約による状態削減手法			
論文審査委員	主査	鈴木　正人	北陸先端科学技術大学院大学	准教授
		緒方　和博	同	教授
		落水　浩一郎	同	特任教授
		吉岡　信和	国立情報学研究所	准教授
		岸　知二	早稲田大学	教授

論文の内容の要旨

We propose methods to apply a technology for behavior verification of embedded systems containing sensors and actuators. As the applied technology in recent years, model checking techniques are used in many cases. On running the model checking, it needs to reduce a state number for the verification because information based on the external environment of sensors and actuators systems is enormous and the information is included as the state. As generally methods to reduce the state number, there are abstraction methods or input limitation methods.

In this paper, we focus on a limitation method that limits a range of the time-series variation of sensor values. To extract the range, we need to focus on these values and to analyze a scenario (“worst case scenario”) which the range of the variations is max.

However, it is difficult to extract these values because the values that should be focused are different by properties to verify the model. Also, it is difficult to eliminate contexts that are not needed for extracting the range when analyzing the use case because there are no information about the relationship between the use case and contexts　in general requirement specifications.

To alleviate these problems, we propose EIVP (Extraction method of Input Values related to a verification Property) which use existed goal-oriented analysis and GWEU (Goal-oriented analysis of the Worst case scenario with Eliminating Unnecessary contexts).
Also, we determined the feasibility of our method by performing case studies.

By the results of our research, the occurrence probability of state explosion can be reduced in

comparison with the conventional, against the design verification for systems based on sensor and actuator.
Also, the results contribute as an effective means to ensure the reliability of the software system.

Key words: model-checking, goal-oriented analysis, embedded systems, contexts, time-series variation.

論文審査の結果の要旨

当博士論文はモデル検査において検査対象の複雑化により検証が不可能になる現象である状態爆発を回避することを目的として、２種類のゴール指向分析に基づく新たな入力空間の制限方法の提案、有効性について論じたものである。モデル検査は網羅的な検証が可能な技術としてソフトウェアの信頼性向上には欠くことのできない手段となっており、特に組込みシステムの開発においてその効果は顕著である。しかし組込みシステムの多くは自然界の物理量をセンサによって計測しそれに対する応答を計算してアクチュエータを制御するものであり、入力値が連続的であるなどの理由により状態爆発を発生しやすい。一般に入力空間の制限方法には抽象化により状態数を減らす方法、入力変数の数や変化範囲を制限する方法などがあるが、従来方法では連続的な入力値およびその履歴を必要とするシステムに対する削減の効果が十分ではないという問題点があった。本論文は動作に支配的な影響を与える変数(入力変数)およびその変量が最大となるシステムの動作状況(ワーストケースシナリオ)に着目し、ゴール指向分析法KAOSに新たに2種類の分解規則を追加することで拡張した手法によりワーストケースシナリオを発見、それに基づいて状態数の削減を示したものである。最初にEIVP(Extraction method of Input Variable related to a verification Property)という手法により支配的な入力変数を抽出し、プロトタイピングにより変数の変化幅の最大値を決定する。さらにGWEU(Goal-oriented analysis of Worst case scenario with Eliminating Unnecessary contexts)という手法により最大変化幅を与える状況（ワーストケースシナリオ）およびその条件を特定する。ただしワーストケースシナリオは現実のシステムでは発生しない状況(水温t > 100など)を含んでいることがあるが、提案手法のゴール指向分析により作成されたゴール木中にそれは障害として出現する。障害を解決することによりさらに入力空間を制限することが可能である。自立制御型移動ロボットによるライントレーサと、電子ポットの温度制御の2つの事例にこの手法を適用し、作業者の経験や判断を必要とするものの最大85%の状態数削減に成功している。以上、本論文は、組込みシステムのモデル検査における状態爆発を回避する新しい手法を構築し、事例によりその有効性を示したものであり、学術的、工学的に貢献するところが大きい。よって博士（情報科学）の学位論文として十分価値あるものと認めた。