論文 / 著書情報
Article / Book Information

題目(和文)	リアクティブシステム仕様の実現可能性検証における計算量削減方式に関する研究
Title(English)	
著者(和文)	島川昌也
Author(English)	Masaya Shimakawa
出典(和文)	学位:博士（工学）, 学位授与機関:東京工業大学, 報告番号:甲第9664号, 授与年月日:2014年9月25日, 学位の種別:課程博士, 審査員:米崎　直樹,佐伯　元司,権藤　克彦,渡部　卓雄,西崎　真也
Citation(English)	Degree:, Conferring organization: Tokyo Institute of Technology, Report number:甲第9664号, Conferred date:2014/9/25, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（論文博士）

論　文　要　旨　（和文2000字程度）

（Summary）

報告番号	乙 第　　号	氏　名	島川 昌也

本論文は，「リアクティブシステム仕様の実現可能性検証における計算量削減方式に関する研究」と題し，6章から成る．

第1章「はじめに」では，研究の背景，目的，アプローチ，主要な結果を述べている．リアクティブシステム仕様の実現可能性に関する検証は，仕様記述において見過ごされがちな危険な状況に陥る可能性を検出することができるが，一般に極めて煩雑な計算コストの高い処理を伴う．本研究は，そのような実現可能性検証における計算量削減を目的として，i)検証する性質の制限，ii)仕様の構文制限の2つのアプローチから研究を行っている．

第2章「リアクティブシステム仕様の実現可能性」では，リアクティブシステム仕様の実現可能性に関する諸概念の定義を与えている．

第3章「強充足可能性判定問題の計算量」は，i)のアプローチによる計算量削減の考察である．すなわち，森らによって導入された実現可能性の必要条件である強充足可能性について，その判定問題の計算量を与えている．強充足可能性は実現可能性の必要条件ではあるが，現実的な仕様については実現不能であるならば強充足不能でもあるとの議論もあり，この性質の判定によって仕様の多くの欠陥を検出できると考えられている．ここでは，線形時間論理（LTL）で記述されたリアクティブシステム仕様の強充足可能性判定問題が，EXPSPACE完全であることを証明している．上界は，指数オーダーの計算領域を用いて判定を行える手続きを与えることで証明している．下界は，EXPSPACE完全であることが知られているEXP-CORRIDOR TILING問題が,強充足可能性判定問題の補問題に多項式帰着可能であることを示すことで証明している．これにより，強充足可能性判定は，2EXPTIME完全であることが知られている実現可能性判定より難しくないことが明らかになった．さらに，強充足可能性判定問題について，時間オペレータの入れ子の深さを2までと制限しても，その計算量は落ちずにEXPSPACE完全のままであることも証明している．

第4章「有界強充足可能性判定」では，i)のアプローチによる計算量削減法として，強充足可能性判定における探索を有界な範囲に制限した有界検査法を提案している．ここでは，強充足可能性をより制限した有界強充足可能性の概念を導入し，その判定手続きを与えている．有界強充足可能性は,サイズkの繰り返し構造として表現される反例のみを考慮するように強充足可能性を制限した性質であり，その判定では高速なSATソルバを用いることができる．強充足不能な仕様は，比較的小さな繰り返し構造として表現される反例を持つことが多く，この性質の判定で多くの欠陥を発見できると予想される．ここでは，有界強充足可能性判定問題の計算量がco-NEXPTIME完全であることを示し，有界強充足可能性判定が強充足可能性判定以下の難しさであることも明らかにしている．さらに実験により，本手法が強充足可能性や実現可能性の判定に比べて大きな仕様を取り扱え，小さな繰り返し構造として表現される反例の存在を効率的に調べられることを示し，その有効性について

述べている．

第5章「実現可能性判定に適したLTLサブセット」は，ii)のアプローチによる計算量削減に関するもので，実現可能性判定で必要となる決定性ωオートマトン構成を簡単化する観点から構文を制限したLTLのサブセットLTL^{ep}とその双対であるLTL^{gp}を，決定性ωオートマトン構成法とともに提案している．実現可能性判定が難しいのは，その判定において仕様と等価な決定性ωオートマトンが必要となるためである．その構成には，Safraの構成法と呼ばれる決定化手続きが用いられるが，それは極めて煩雑であり，各種効率化を施しにくい．LTL^{ep}とLTL^{gp}では，このような問題を避けられることを示している． LTL^{ep}とLTL^{gp}は，その仕様からある構造的な特徴を持つ非決定性ωオートマトンを構成できるという性質を持つ．提案した構成法では，その構造的特徴を利用し，Safraの構成法よりも簡潔な手続きで，非決定性ωオートマトンを決定化することが可能であることを示している．さらに，構文を制限した仕様について実験を行い，本手法によってより大規模な仕様を取り扱え，効率的に決定性ωオートマトン構成・実現可能性判定が行えることを示し，その有効性を主張している．

第6章「まとめ」では，本論文で得られた成果を要約している．

以上要するに，本論文は，リアクティブシステムの動作仕様記述段階での欠陥を現実的なコストで発見する手法について新たな道を切り開いたものである．

（論文博士）

論　文　要　旨（英文）　（300語程度）

報告番号	乙 第　　号	氏　名	島川 昌也

Realizability verification of reactive system specifications can detect dangerous situations that may arise, which were not expected while drawing the specifications. However, such verification typically involves complex and intricate analyses. The purpose of this thesis is to reduce the complexity of realizability verification. Two approaches are followed: restriction of the verification properties, and restriction of the specification syntax. The thesis consists of 6 chapters.

Chapter 1 gives a description of the background, states the aims of the work, and outlines the approaches used in this research. Chapter 2 provides the definitions of the notions employed.

Chapter 3 describes complexity reduction via the restriction of verification properties, i.e., introducing strong satisfiability. Strong satisfiability is a necessary condition for realizability, and is introduced to classify unrealizable specifications. It is recognized that many practical unrealizable specifications are also strongly unsatisfiable. Moreover, this chapter provides proof that the strong satisfiability problem for specifications written in linear temporal logic (LTL) is EXPSPACE-complete and, therefore, is easier to solve than, or of equal difficulty to, the realizability problem that is 2EXPTIME-complete.

Chapter 4 describes a bounded-checking method, in which search scope for checking strong satisfiability is bounded. This is another way of restricting verification properties. This chapter details bounded strong satisfiability, together with a method for checking this property. Bounded strong satisfiability restricts counterexamples of strong satisfiability to those represented by loop structures of size k; then an efficient SAT solver can be utilized to check this property. Moreover, this chapter describes experimental results that show the effectiveness of the method.

Chapter 5 considers complexity reduction via restriction of syntax of which language is used in specifications. In general, realizability verification translates specifications into deterministic omega-automata using Safra's determinization. It is, however, very intricate, and also it is difficult to get an efficient implementation of it. This chapter introduces LTL subsets LTL^{ep} and LTL^{gp}, which restrict the syntax of LTL from the viewpoint of simplifying the construction of deterministic omega-automata, together with a construction method for deterministic omega-automata. In this chapter, it is proved that specifications written in LTL^{ep} and LTL^{gp} can be transformed into deterministic omega-automata via a simpler determinization procedure than Safra's determinization. Experimental results that demonstrate the effectiveness of the method are presented.

Chapter 6 summarizes the thesis.