

Title	Symbolic Bisimulation Checking and Decomposition of Real-Time Service Specifications
Author(s)	中田, 明夫
Citation	大阪大学, 1997, 博士論文
Version Type	VoR
URL	https://doi.org/10.11501/3129118
rights	
Note	

Osaka University Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

Osaka University

氏 名	なか た あき お 中 田 明 夫
博士の専攻分野の名称	博 士 (工 学)
学 位 記 番 号	第 1 3 2 1 9 号
学 位 授 与 年 月 日	平成 9 年 3 月 25 日
学 位 授 与 の 要 件	学位規則第 4 条第 1 項該当 基礎工学研究科物理系専攻
学 位 論 文 名	Symbolic Bisimulation Checking and Decomposition of Real-Time Service Specifications (実時間サービス仕様の記号的双模倣性検証および分解)
論 文 審 査 委 員	(主査) 教 授 谷 口 健 一 (副査) 教 授 藤 井 護 教 授 菊 野 亨

論 文 内 容 の 要 旨

本論文は、形式仕様記述言語を用いて高信頼実時間分散システムを設計、検証することを目的として、システムの仕様間の等価性判定および全体仕様（サービス仕様）から複数の分散配置された計算機の動作仕様への分解についての研究をまとめたものである。

記述言語としては ISO で標準化されている形式仕様記述言語 LOTOS に基づいた言語を採用した。LOTOS は通信動作の実行順序を構造的に指定するための選択、並列、割り込みなどの構文を持つ言語である。しかし、LOTOS はシステムの実時間性を記述する能力を持っていない。そこで、本研究ではまず実時間分散システムの記述言語の例として、LOTOS を時間制約を記述できるように拡張した言語 LOTOS/T を考案した。LOTOS/T は LOTOS の構文を受け継ぎ、それに加えて各動作の時間制約を論理式で記述する能力をもつ。例えば、ある入出力動作を現在時刻が 3 以下である間に必ず実行し、その実行時刻を変数 x に代入するなどといった記述が可能である。変数に代入された値を任意の後続動作の時間制約で参照することによって、一般に連続しない動作間の時間制約を記述できる。本論文では言語 LOTOS/T の構文と意味を形式的に定義している。さらに、具体的なシステムの記述例を与え、言語の有用性を示している。

一方、実時間分散システム仕様の等価性としては双模倣等価性（双模倣性）を採用した。双模倣等価性は 2 つのシステムがお互いに相手の入出力動作系列の実行を模倣し続けることができるという性質であり、分散通信システムの最も基本的な等価性として認知されている。そこで本研究の二番目の内容として、従来より広いクラスの実時間分散システム仕様の双模倣等価性を判定する方法を考案している。本判定法ではまず実時間分散システムを、遅延による遷移および入出力動作による遷移をもち、各状態にパラメータ変数、各遷移に移行条件式を記述できる状態遷移モデルで表現することによって、時間値によって無限となる状態空間を縮約している。さらに、このモデルでは遅延遷移と動作遷移が必ず交互に実行されるように実時間システムを記述する。このモデルを対象に、与えられた状態対からそれらを等価とするようなパラメータに関する最も弱い条件式を導出するアルゴリズムを考案している。このことにより、双模倣等価性判定問題が論理式の充足可能性判定問題へ帰着できる。また、LOTOS/T 記述からこのモデルへの変換法も与え、本判定法が LOTOS/T のような時間制約の記述能力を持つ言語に対して適用可能であることを示している。

第三に、LOTOS/T で記述された実時間分散システムのサービス仕様（全体仕様）をノード間の通信動作を含む

個々のノードの動作仕様に分解する方法を与えている。従来は LOTOS/T のように並列、割り込みなどの構文を持つ実時間システム記述言語を対象とした分解法は提案されていなかった。提案する分解法では、ノード間の通信路はエラーがなく、伝送遅延の最大値が定数でおさえられること、および、各ノードは正確な時計を持っていることを仮定する。そして、全体仕様の他に、各入出力動作の各ノード（計算機）への配置、および各ノード間の通信遅延の最大値が与えられているとする。このとき、サービス仕様の構造から各動作の実行順序を解析して必要なノード間のメッセージ交換動作を特定し、それらのメッセージの遅延が最大であった場合でもサービス仕様の時間制約が満足されるような時間制約を各ノードの動作に加えることによって、サービスを正しく実現する各ノードの仕様を自動導出する。また、そのとき加える時間制約を最も弱いものになっている。

論文審査の結果の要旨

本論文では、実時間分散システム仕様の記述言語の例として、ISO で標準化されている形式仕様記述言語 LOTOS を時間制約を記述できるように拡張した言語 LOTOS/T を提案し、実時間分散システムの仕様間の等価性の検証法、および、全体仕様を複数の分散配置された計算機の動作仕様へ分解する方法を与えている。

従来、実時間分散システム仕様の等価性検証は時間値によってシステムの状態数が増加するなどの理由で一般に困難であることが知られており、LOTOS/T などのような記述能力の高い言語に対しても適用可能な等価性検証法が求められていた。本論文では、まず、各遅延遷移および動作遷移に遷移条件式を記述することによって、従来のモデルでは時間値によって無限となっていた状態空間を縮約した実時間分散システムの表現モデルを考案している。このモデルでは、遷移条件式を記述する論理体系には決定可能であること以外の制限を課さず、そのかわりに、遅延と動作が必ず交互に実行されるという、現実の実時間システムの表現には差し支えない制限を課している。次いで、このモデルの任意の状態対の等価性判定問題を論理式の充足可能性判定問題へ帰着することによって解く方法を示し、さらに、LOTOS/T 記述からこのモデルへの変換法を与え、提案する手法が LOTOS/T のような実用的な記述能力を持つ言語に対しても適用可能であることを示している。このように、従来より広いクラスの実時間分散システム仕様の等価性を判定する方法を与え、理論的にも実用面にも意義のある成果を上げている。

さらに、LOTOS/T のような並行言語で記述された実時間分散システムの全体仕様を計算機間の通信動作を含む個々の計算機の動作仕様に分解する方法を与えている。従来このような時間制約付きの並行言語に対する分解法は提案されていなかった。提案する方法では、通信遅延の最大値が与えられていると仮定し、遅延が最大の場合においても全体仕様の時間制約を満たすことが保証されるような時間制約を各計算機の動作に課するという方針を採用しており、通信遅延を変更できないネットワーク上での実時間分散システムの実現に有用である。また、その際に課される時間制約を最も弱いものに留める工夫もしている。これらの成果は理論的に興味深く、工学的にも有効性が高いといえる。

以上のように、本論文は、LOTOS などの並行言語を用いた高信頼実時間分散システムの設計および検証技術の進展に貢献しており、博士（工学）論文として価値あるものと認める。