【13】

氏名	松尾尚文（まつおたかふみ）
博士の専攻分野の名称	博士（情報科学）
学位記番号	第　２３０５６　号
学位授与年月日	平成21年３月24日
学位授与の要件	学位規則第４条第１項該当 情報科学研究科情報システム工学専攻
学位論文名	Feature Interaction Verification of Telecommunication Services and Home Network Services Using Model Checking （電話通信システムおよび情報家電システムにおける競合問題に対するモデル検査を用いた検証）
論文審査委員	（主査） 教授　菊野　亨 （副査） 教授　尾上　孝雄　　教授　楠本　真二　　准教授　土屋　達弘

論文内容の要旨

ユーザの多様な要望に対応するため，既存の機器に機能を付け加えることで新たなサービスが開発されている．このようなサービスの開発は，サービス提供者ごとに個別に行われている．そのため，複数のサービスを組合せて利用する際に，それぞれのサービスの動作が干渉し，開発者の意図しない動作をしてしまう場合がある．このような問題は機能競合問題と呼ばれる．

高信頼なサービスを提供するためには，機能競合の発生をどのように防ぐかが重要となる．しかし，電話通信システムをはじめとするシステムでは，複数の機器がネットワークを通じて接続され，並行動作する．このような並行システムは，機器の実行順序などにより，非常に多くの実行パターンを持つため，テストによる機能競合の検出は困難である．また，並行システムでは，機能競合の再現性が低く，原因の特定も困難である．

本研究では，システムの網羅的な検証が可能なモデル検査を利用し，並行システムで発生する機能競合を検証する手法について，以下の2つの観点から研究を行った．

1つ目は電話通信システムのサービス間の機能競合を対象として，Unboundedモデル検査を用いた検証手法についての研究を行った．Unboundedモデル検査はSAT（充足可能性判定）を利用したモデル検査手法である．しかし，従来手法を機能競合の検証に適用すると，システムの動作を表現する論理式が非常に大きくなり，結果として検証に時間がかかってしまう．そこで，システムの並行性に注目し，より効率的にシステムの動作を論理式で表現する方法を提案し，その論理式の表現方法を利用するUnboundedモデル検査手法を示す．提案した手法の有効性を示すために具体的なサービスを対象に比較を行い，検証時間が大幅に改善されることを示す．

2つ目に情報家電システムにおいて発生する機能競合の検証法についての研究を行った．情報家電システムは，ユーザに快適な生活環境を提供することを目的としているため，システムの動作検証を行うには，システムを取り巻く環境を扱う必要がある．そこで，本論文では情報家電システムの動作を形式的に表現するモデルを提案する．さらに，このシステムのモデルを用いて，情報家電システムで発生する競合を特定，分類する．そして，機能競合が発生するかを，モデル検査を用いて検証する手法を提案する．また，4つの具体的なサービスの例に対して機能競合の検証を行い，提案手法の有効性を示す．

論文審査の結果の要旨

近年のオープンな並行システムの開発では，既存の機器にユーザの欲する新しいサービスあるいは機能を動的に付け加えることが求められる．サービス毎に独立にシステム開発が行われるため，これらを組み合わせたとき予期しない，深刻な問題（競合と呼ぶ）の発生が警告されている．一方，大規模な並行システムの設計検証法として，モデル検査手法が注目されている．モデル検査では，システムを状態空間で表現し，その状態空間内で，与えられた性質が満たされるかどうかを検証する．

本論文では競合の解決に関する２つの研究課題に挑戦している．まず，Unbounded モデル検査を用いたシステムの高速検証を試みている．Unbounded モデル検査では，システムの動作を表現した論理式の充足可能性を調べる．しかし，電話通信システムの場合，システムの動作を記述する論理式が大きくなるため，実用的な時間での検証が出来なかった．そこで，並行動作する遷移の実行前と実行後で変化する状態変数だけに注目した論理式の表現法を考案した．その結果，論理式の大きさを約60～90 パーセント削減することに成功した．具体的な電話通信システム上の７つのサービスについて適用実験を行い，従来の検査手法に比べ，大幅な時間短縮が出来た．

次に，情報家電システムの動作状況を厳密に表現するため，新たにシステムモデルを提案した．提案したモデルでは，システムをサービス，機器，環境の３層で表現する．環境を変数で，機器を関数で，サービスを関数の呼び出し列として記述する．このシステムモデルを用いて，情報家電システム上で発生する競合を特定し，分類した．そして，分類した競合が発生するかどうかを，モデル検査ツール SPIN を用いて検証する．4 つのサービスの例に対して競合の検証を行った結果，検証そのものはせいぜい数 10 秒程度で行えることが分かった．更に，競合が発生する具体的な動作シナリオを反例から得ることも出来た．

これらの研究成果は，並行システムの信頼性を向上させるための検証技能の分野において，非常に大きな貢献をするものである．よって，博士（情報科学）の学位論文として価値のあるものと認める．