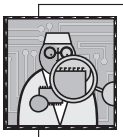

学位論文題目　Feature Interaction Verification of Telecommunication Services and Home Network Services Using Model Checking（邦訳：電話通信システムおよび情報家電システムにおける競合問題に対するモデル検査を用いた検証）

取得年月　2009 年 3 月　　**学位種別**　博士（情報）　　**大学**　大阪大学

氏　名　松尾 尚文（新日鉄ソリューションズ（株））

推薦研究会　ソフトウェア工学

推薦文　本論文は，機能競合の網羅的な検出を行うことを目的とし，電話通信システムや情報家電システムを対象に，システムや環境を表現する手法を提案し，それに基づき非有界モデル検査技術を適用することで，効率的・効果的な検出ができることを示しており，実問題を扱った良質の研究として推薦する．

ユーザの多様な要望に対応するため，既存の機器に新たな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．しかし，複数のサービスを組み合わせて利用する際に，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，Web サービスや情報家電システムといったシステムでは，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では，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，機能競合の原因の特定も困難である．

このような複雑な動作をするシステムに対する検証手法として，モデル検査手法が注目されている．モデル検査とは，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ているかどうかを検証する手法である（**図 -1**）．モデル検査では，状態空間の探索が網羅的に行われるために，多くの実行パターンを持つシステムの検証に適している．また，システムが性質を満たさない場合，性質の違反が起こる状態までの実行列を反例として出力する．この反例を利用することで性質の違反の原因を特定することができる．

本論文では，このモデル検査手法を利用し，機能競合問題を検証する手法を提案する．まず，Unbounded モデル検査を用いて，電話通信システムの競合を検証する手法を提案する．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．提案する方法を適用することで，論理式の大きさを約 60 ～ 90％程度削減することができる．具体的な電話通信システムの 7 つのサービスの 21 組について機能競合の検証を行うことで，従来の Unbounded モデル検査手法に比べ，短時間での検証が可能となることを示す．

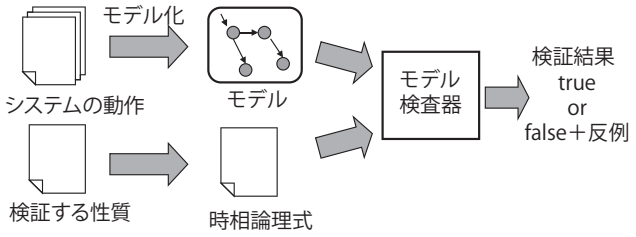

図 -1　モデル検査の流れ

次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を提案する．情報家電システムは，ネットワークで接続された家電機器を協調させて利用することで，新たなサービスを生み出す．このシステムは，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．そのため，システム全体の動作の検証を行うためには，システムを取り巻く環境を扱う必要がある．そこで，本論文ではこのような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，システムのモデル内で分類した機能競合が発生するかを，モデル検査ツール SPIN を用いて検証する手法を提案する．検証の結果，機能競合が発生する場合，反例を調べることで，機能競合が発生する動作シナリオを得ることができる．提案手法の有効性を示すために 4 つのサービスの例に対して，機能競合の検証を行った結果を示す．さらに，反例から得られた，機能競合が発生する動作シナリオについても述べる．

（平成 22 年 3 月 30 日受付）