【56】

氏名・(本籍)	邵(しょう)　峰(ほう)　晶(しょう)
学位の種類	工学博士
学位記番号	第9771号
学位授与の日付	平成3年3月26日
学位授与の要件	基礎工学研究科　物理系専攻 学位規則第5条第1項該当
学位論文題目	**順序機械によってモデル化された通信プロトコルの検証法及びそのＯＳＩセションプロトコルへの適用**
論文審査委員	(主査) 教授　嵩　忠雄 (副査) 教授　都倉　信樹　教授　谷口　健一　教授　宮原　秀夫 教授　菊野　亨　教授　藤井　護

論文内容の要旨

本論文では，通信プロトコルの検証に関する研究のうち，プロトコルにおける不変式やeventualityの検証法と検証の効率を向上させる方法及びそのＯＳＩセションプロトコルへの適用に関する研究がまとめられている。

第1章では，研究の動機づけと新しい成果について概説する。本論文では，プロトコル機械を有限状態の順序機械，プロトコル機械間の通信路を長さに制限のないＦＩＦＯキューでモデル化する。このようなモデルでは，多くの検証アルゴリズムが通信路の有界性を仮定している。しかし，通信路の有界性は一般に判定不能である。本論文の検証法は，通信路上に存在し得るデータ単位の系列の集合を包含する正規集合を指定することにより，通信路の有界性を仮定せずに，検証すべき条件式を論理式として簡潔に表現できる。

第2章では，プロトコルのモデル化とそれに関連する諸概念の定義を行う。

第3章では，与えられたプロトコルⅡにおける検証すべき性質を，(a)プロトコル機械の指定された状態成分が指定された値をもつことを表す式と，(b)通信路上のデータ単位の系列が指定された正規集合に属することを表す式とを原子式とする命題理論式を用いて記述する。与えられたⅡ上の論理式Ｆ，Ｇと正整数ｋに対して，(Ｆ，Ｇ，ｋ)－eventuality(Ｆを満たす任意の合成状態から，どのような遷移を行っても高々ｋ回の遷移で論理式Ｇを満たす合成状態に必ず到達するという性質)が判定可能であることを示す。さらに，与えられたⅡにおいて次の(1)－(3)がそれぞれ成り立つための判定可能な十分条件を示している。(1)与えられた論理式Ｆが不変式であること，(2)デッドロック状態に到達不能であること，(3)与えられたデータ単位の部分集合Σ_0について，通信路上に現れるΣ_0に属するデータ単位の総個数が有

界であること。

第4章では，検証の効率を向上させるための方法として，プロトコル機械の分解とプロトコルの縮退を導入する。

第5章では，本検証法のＯＳＩセションプロトコルへの適用について述べる。まず，セションプロトコルの主要部であるカーネル，半二重，大同期，小同期機能単位のそれぞれについて，そのコネクション確立・データ転送・コネクション解放フェーズに関する部分を取り上げ，もとのプロトコルにおける検証問題ができるだけ忠実に反映されるように有限状態のプロトコル機械$FSPM_A$，$FSPM_B$を抽出する。また，$FSPM_A$と$FSPM_B$からなるプロトコルＦＳＰにおいて成り立つと予想される4個のeventualityを記述し，試作した検証システムを用いてこれらが成り立つことを検証した結果について述べる。検証時間を短縮するため，実際に，導入されたプロトコル機械の分解とプロトコルの縮退を利用して，ＦＳＰから規模のより小さい三つのプロトコルを求めることにより，この三つのプロトコルにおけるeventualityの検証問題に帰着して検証を行う。さらに，上記のeventualityが成り立つことを用いて，性質「トランスポート層以下の下位層にエラーがなく，$FSPM_A$，$FSPM_B$がプロトコルＦＳＰで許された送受信動作のみを行うならば，$FSPM_A$，$FSPM_B$は常に正常な送受信を行える状態を取り続けることができる（デッドロック状態にもプロトコルエラー状態にも陥らない）」，「通信路上に現れる制御信号の総個数は有界である」を検証する。検証すべき問題の一部をプロトコル機械の分解や縮退を行わずに検証した結果と比較することにより，規模のより小さいプロトコルの検証問題に帰着することの有効性についても述べる。また，もとのプロトコルについて，ＦＳＰに関する検証結果から，どのような結論が得られるかについて述べる。

第6章では，本研究で得られた主な結果と今後に残された問題点について述べる。

論文審査の結果の要旨

本論文では，二つの有限状態順序機械とそれらを持続する長さに制限のない2本のＦＩＦＯキューによってモデル化された通信プロトコルの形式的検証法と，その検証法を利用したＯＳＩセションプロトコルの検証について述べられている。

本論文の検証法では，与えられたプロトコルにおける検証すべき性質を，(1)プロトコル機械の指定された状態成分が指定された値をもつことを表す式と，(2)通信路上のデータ単位の系列が指定された正規集合に属することを表す式とを原子式とする命題論理式を用いて記述する。二つのプロトコル機械の状態と2本の通信路上に存在する送受信系列からなる任意の4字組を合成状態と呼ぶ。本論文では基本的な結果として，与えられたプロトコルと論理式Ｆ，Ｇと正整数ｋに対し，（Ｆ，Ｇ，ｋ）－eventuality（Ｆを満たす任意の合成状態からどのような遷移を行っても，高々ｋ回の遷移で論理式Ｇを満たす合成状態に必ず到達するという性質）が成り立つかどうかが判定可能であることが示されている。また，検証の効率を向上させるため，プロトコルの分解と縮退を利用した検証法が提案されている。

さらに，本検証法に基づく検証例としてＯＳＩセションプロトコルの主要部であるカーネル，半二重，大同期，小同期機能単位に関する部分から抽出された有限状態のプロトコル機械$ＦＳＰＭ_{A}$，$ＦＳＰＭ_{B}$からなるプロトコルＦＳＰが取り上げられている。まず，プロトコルＦＳＰにおいて成り立つと予想される4個のeventualityが記述され，試作した検証システムを用いてこれらが成り立つことが機械的に検証されている。実際には，検証に要する時間を短縮するため，プロトコルの分解と縮退を利用して，プロトコルＦＳＰから規模のより小さい三つのプロトコルを求め，この三つのプロトコルにおけるeventualityの検証問題に帰着して検証が行われている。さらに，上記のeventualityが成り立つことを用いて，性質「トランスポート層以下の下位層にエラーがなく，$ＦＳＰＭ_{A}$，$ＦＳＰＭ_{B}$がプロトコルＦＳＰで許された送受信動作のみを行うならば，$ＦＳＰＭ_{A}$，$ＦＳＰＭ_{B}$は常に正常な送受信を行える状態を取り続けることができる（デッドロック状態にもプロトコルエラー状態にも陥らない）」，「通信路上に現れる制御信号の総個数は有界である」が成り立つことが検証されている。また，検証すべき問題の一部について，プロトコルの分解や縮退を利用した場合と，それらを利用しない場合を，検証に要したＣＰＵ時間と生成された論理式の大きさについて比較することにより，プロトコルの分解や縮退の利用が如何に有効であるかを示している。

これらの研究成果は，通信プロトコルの形式的検証法に寄与するところが大きく，学位論文として価値あるものと認める。