報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目　通信プロセスモデルに対する時間拡張と実時間ソフトウェア開発への応用

氏　　名　栗原 寛明

論　文　内　容　の　要　旨

本論文では，実時間システムの振舞い解析と検証の基礎となる形式モデルを与えることを目的として，通信プロセスモデルであるπ計算に時間の概念を導入して拡張した体系を提案する．また，その体系に基づいて

- 振舞いの等価性を表す関係
- 振舞いの時間的タイミングの違いを表す関係
- タイムアウトに着目した時間待ち動作の抽象化手法
- 実時間システムを構成するソフトウェアのモデル化手法

を提案する．

実時間システムは動作に時間制約が存在する並行システムであり，与えられた時間制約を満たしながら動作することが要求される．実時間システムの動作の正しさは，計算結果の正しさだけでなく，結果を得るまでに経過した時間の長さが時間制約を満たしているか否かに依存する．実時間システムの動作は，実時間性と並行性により非決定的である．そのため，いつでも正常に動作することを確認することは容易ではない．例えば，動作テストによってすべての動作をテストすることは，動作の非決定性により簡単ではない．また，実時間性により時間の経過を考慮したテストを行う必要があり，行うべきテストの数が非常に多くなる．

実時間システムは携帯電話，交通管理システム，自動車のブレーキングシステムなど多岐に渡る分野で広く利用されている．実時間システムの多くは機器に組み込まれた組込みシステムであり，停止することなく動作することが要求される．また，ブレーキングシステムやペースメーカのように誤動作が人命に重大な影響を及ぼすシステムもあり，高い信頼性が要求される．そのため，動作テストを行うだけ

ではなく，コストが大きくなっても形式的な検証手法によりシステムの動作の正しさを網羅的に示し保証することが必要である．

並行システムを対象とする形式手法として通信プロセスモデルがよく知られている．通信プロセスモデルは並行計算のモデルであり，計算を入出力ではなく外部環境との相互作用や通信に着目してモデル化する．通信に着目することで入出力に基づくモデルよりも動作を詳細にモデル化することが可能であるのと同時に，相互にデータを送受信しながら全体としての計算を進める並行システムのモデルに適している．Milner による CCS，Hoare による CSP，Milner, Parrow, Walker による π 計算といった通信プロセスモデルが知られている．

実時間システムは並行システムでもあるため，通信プロセスモデルによってモデル化することが可能である．しかし，従来の通信プロセスモデルは時間の概念を扱う仕組みを持たないため，時間に関する動作や時間の長さを表現できない．そこで本論文では，実時間システムの動作を時間に関する動作も含めて精密にモデル化するために，通信プロセスモデルに時間を導入する拡張を提案する．特に，通信プロセスモデルの中でも高い表現能力を持つ π 計算を対象に拡張を行う．センサやアクチュエータ，制御ユニットをオブジェクトとみなすと実時間システムはオブジェクト指向システムと考えられ，π 計算にはオブジェクトのモデル化に適した特徴が存在する．

時間拡張された π 計算による実時間システムのモデルを用いて振舞い解析を行うために，振舞いの等価性を表す関係と，振舞いのタイミングの違いを表す関係を定義する．振舞いの等価性を表す関係は，従来の π 計算における双模倣関係に基づき時間に関する動作の等価性を表現できるよう拡張した関係である．振舞いのタイミングの違いを表す関係も双模倣関係に基づいているが，時間の待ち方が異なり一方が他方よりも常に早く動作する場合も関係付けられる．システム全体を対象とする振舞い解析はコストが高いため，システムを分割し部分ごとに解析できることが望ましい．そのためには関係が合同的性質を持つことが重要である．本論文で提案する 2 種類の関係はいずれも前提条件のない合同的性質は持たないが，合同的性質が成立するための十分条件を示す．

本論文で提案する π 計算の時間拡張は時間に関して非常に細かい意味論を提供する．そのため，実時間システムの時間に関する動作を詳細に調べることが可能であり，デッドラインなどの時間制約に関する性質の解析に有用である．しかし，細かい意味論は詳細な解析を可能にする一方で，状態を細かく分割しているため解析のコストを増大させる．時間に関する動作はタイムアウトによってモデル化できることが知られており，時間に関する動作の特徴としてタイムアウトの発生を残しながら動作を抽象化する手法を提案する．抽象化を行うことにより状態数を削減することができる．抽象化を行って振舞いが等価であれば，抽象化する前のモデルも

時間の関係しない動作とタイムアウトについては振舞いが等価であることを示す．このことにより，時間の関係しない性質を示すためには抽象化を行ってから示せばよい．提案する抽象化は，実時間システムの動作をタイムアウトを捉えられる形で従来のπ計算によってモデル化することを可能にし，従来のπ計算に対する等価性判定手法，検証手法およびツールの応用を可能にする．

実時間システムの動作を最も詳細かつ直接的に表現しているのはシステムを構成するソフトウェアである．そこで，実時間システムの動作を時間拡張されたπ計算によってモデル化する一つの手法として，プログラムから時間拡張されたπ計算による表現へ変換する規則を与える．時間に関する動作を直接的に記述するための構文を持つリアルタイムオブジェクト指向言語の意味論を変換規則の集合として定義する．変換規則によりプログラムを変換することで，実時間システムの動作を表現した形式的記述が得られる．実時間システム開発の設計段階においてシステムの動作を時間拡張されたπ計算を用いて記述されていれば，実装したプログラムを変換して得られる記述と振舞いを比較することで正しく実装が行われたか確認することができる．