実時間スケジューリングを想定したエレベータシステムへのモデル検査適用

藤原 聡子† 村田 由香里† 池田 信之†
株式会社 東芝†

1 はじめに

組込みシステムの仕様が複雑になる一方で，その信頼性や安全性に高い基準が求められている．特に，社会インフラシステムでは遅延制約等の実時間仕様を確実に充足する必要がある．そのため近年，設計段階においてシステムの仕様充足性を検証する手法として，モデル検査技術が注目されている[1]．モデル検査技術では，システムの設計を状態遷移モデルとして表現し，網羅的な検証を行うことで仕様充足性を保証することができる．我々は，今回，エレベータシステムのタスク設計に対して，モデル検査技術を適用し検証を行った．検査では，並行タスクの状態遷移モデルの記述が容易な SPIN ツール[2]を利用している．また，タスクの実行遅延を計測するため，タスクの優先度と実時間によるスケジューリングを想定したモデルを作成し検証を行っている．本論文では，モデル検査適用結果を報告し，その効果を検討する．

2 検査対象システム

2.1 SPIN による実時間検査

SPIN によるモデル検査は，検査対象の状態遷移モデルを専用言語 Promela で記述し，制約を検証式として与えたとき，そのモデルが検証式に違反しないかを網羅的に検査する技術である．本適用では，優先度付きの並行タスクを扱うため，モデル検査ツール SPIN と，μITRON 仕様のライブラリを提供するμIPRON[3]を用いた．ただし，Promela では時間の概念を記述することが困難であるため，時間ライブラリを作成した．時間処理ライブラリでは，時間を表す変数を用意し，処理毎に消費する時間を値として加算または減算していくことで，模擬的に時間経過を表現している．これにより，実時間によるスケジューリングを想定したモデル上で，タスクの実行遅延を計測することを可能とした．SPIN 上で時間処理ライブラリの時間消費関数を用いた模擬的な時間経過の例を図 1に示す．

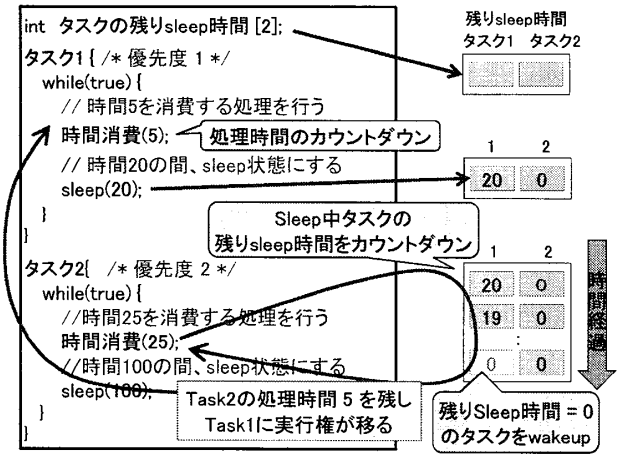

図 1：時間処理ライブラリによる時間経過の例

Model Checking for Real-Time Properties of Elevator Control System

† Satoko Fujiwara, Yukari Murata, Nobuyuki Ikeda, Toshiba Corporation

各タスクは，任意の時間を消費しながら処理を行い，任意の時間 sleep 状態になる動作を周期的に繰り返すモデルとして表わされる．本適用では，このようなタスクを周期タスクと呼ぶ．

2.2 システム構成

現在開発中のエレベータシステムの設計のうち，8つのタスクの動作をモデル検査の対象とした．タスクの動作例を図 2に示す．各タスクには，他のタスクへ公開する公開データがある．各タスクは優先度管理された周期タスクとして実装され，周期の先頭で他タスクの公開データを取得し，処理を行った後，自タスクの公開データを生成する．データ生成と参照の際には，排他制御のためにセマフォの取得・解放を行う．本適用では，優先度，タスクの処理時間，sleep 時間，データ参照関係に基づく動作タイミングによる実行遅延を検査対象とし，その他の処理はモデル化の対象外とした．

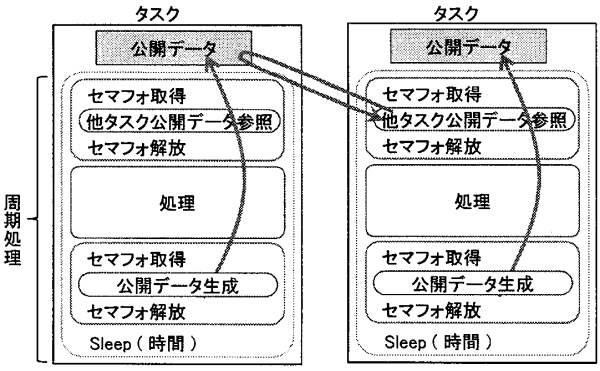

図 2：タスクの処理

3 モデル検査適用

3.1 状態遷移モデルの作成

リアルタイム仕様充足性として，重要なタスクの実行が許容範囲より大きく遅延しないことを保証するため，優先度逆転現象の有無とタスクの実行周期差の 2 つを検証項目とした．本適用では，公開データの生成・参照を行う 8 つの周期タスクに，

優先度・処理時間・sleep 時間を設定し，検査を実施している．

3.2 優先度逆転現象の検出

優先度逆転現象とは，優先度の高いタスクと低いタスクが資源を競合する際に，優先度の低いタスクが高いタスクより先行して実行される現象である．優先度逆転現象が発生すると，高優先度のタスクが長い待ち状態となり実行制約に違反する可能性がある．想定のタスク設計において優先度逆転現象が発生する場合の高優先度タスクの待ち時間が長くならないことを確認するため，優先度逆転現象の有無を確認する．

モデル検査による検証の結果，最高優先度のタスクが 100 周実行される間に，5 回の優先度逆転現象発生を検出した．優先度逆転現象による高優先度タスクの待ち時間を短縮するためには，各タスクの処理時間を短くする，セマフォ保持時間を短くする等の方法がある．また，優先度逆転現象の発生は優先度継承機能をセマフォに実装することで解消できる[4]．

3.3 タスクの周期差の計測

本適用の検査対象システムでは，各タスクは他タスクのデータを参照して自タスクの公開データを生成する．参照先のデータが生成されてから実際に参照されるまでに大きな遅延がある場合，データ落ちや，参照先のデータ間の不整合が生じる可能性があるため，各タスクの遅延制約を保証する必要がある．

検査対象システムには，直接参照と間接参照の 2 つのデータ参照関係がある．タスクの直接参照と間接参照の例を図 3に示す．検査対象タスクはタスク x と y の公開データを直接参照している．また，タスク y は，自タスクの公開データを作成するためにタスク x を直接参照している．そのため，検査対象タスクはタスク x を直接参照し，かつ，タスク y を経由してタスク x を間接参照している．今回の検査では，直接参照関係にあるタスク間の最大周期差の計測と，直接参照関係と間接参照関係を持つタスクの最大周期差の計測を行った．

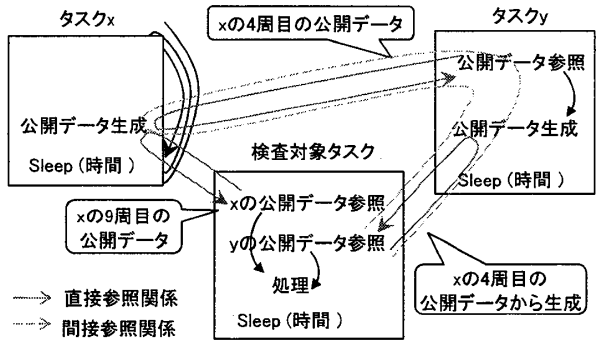

図 3：直接参照と間接参照を行うタスクの例

3.3.1 直接参照するタスクの最大周期差

最高優先度タスクの公開データを直接参照する A から D までのタスク 4 つを検証対象とした．計測結果を表 1に示す．タスク D は，最高優先度タスクの公開データ生成から最大 700ms 遅れて参照する場合があり，タスクの実行遅延が問題となる可能性が高い．最大時間差を短縮するためには，各タスクの処理時間を抑える必要がある．例えば，タスク設計の変更，キャッシュの利用，タスクスケジューリング方法の変更などの方法により，タスクの処理時間を短縮できる．

表 1：直接参照の最大差計測結果

対象タスク	タスクA	タスクB	タスクC	タスクD
直接参照するタスクの最大周期差 [回]	2	5	6	14
〃 最大時間差 [ms]	150	250	300	700

3.3.2 直接・間接参照を行うタスクの最大周期差

対象タスクがタスク x の公開データを直接参照するタイミングと間接参照するタイミングに大きな差が生じる場合，データ不整合となる可能性が高い．該当する 3 つのタスクを対象として最大周期差を計測した結果を表 2に示す．表 2によると，直接参照と間接参照のタイミングには大きな差がなく，問題の生じる可能性が低いことを確認できた．

表 2：直接・間接参照の最大差計測結果

対象タスク	タスクB	タスクC	タスクD
直接参照と間接参照するタスクの最大周期差[回]	2	1	2

3.4 モデル検査適用の効果

組込みシステムのリアルタイム仕様充足性検証として，エレベータシステムの設計に対しモデル検査適用を行った．本適用では，モデル検査ツール SPIN を採用し，優先度と実時間を考慮した状態遷移モデルを作成した検証により，優先度逆転による遅延制約違反の可能性を検出でき，モデル検査適用の有効性が確認できた．

4 今後の取り組み

今後，処理時間や Sleep 時間の変更に伴い再検査を繰り返し実施することにより，さらなる品質の向上に努める．

参考文献

[1] 高田沙都子，“産業用コントローラに対するモデル検査適用事例”，ソフトウェア品質シンポジウム 2008，(2008)

[2] SPIN model checker, http://spinroot.com/spin/whatispin.html

[3] μIPRON, http://aoki-www.jaist.ac.jp/~toshiaki/modulez/tinyd0/index.php?id=2

[4] Qing Li, Caroline Yao, “リアルタイム組込み OS”，株式会社翔泳社，(2005)