情報制御システムに対するモジュラ検証と課題

小飼 敬[†1] 宮島 卓巳[†2] 上田 賀一[†2]

実践的なモデルに対してモデル検査を適用する場合，状態爆発が発生する可能性が高い．本研究では，検査対象のシステムをいくつかのサブシステムに分割して検証するモジュラ検証の方法とその課題について述べる．

Modular Verification for Information Control System and its Problems

Kei Kogai,[†1] Takumi Miyajima[†2] and Yoshikazu Ueda[†2]

A model checking of a practical model might have state explosions since the scale of its model could be large. This study describes our approach, which divide an information control system into subsystems and verify the subsystems.

1. はじめに

モデル検査は，システムの状態を網羅的に探索し，それぞれの状態に対して検査目的に対する正当性を検査する手法である．より実践的なシステムに対してモデル検査する場合，このシステムの状態モデルでの探索範囲が爆発的に増加するため，この問題に対処する必要がある．著者らは，これまでの研究で，検査時に探索する情報制御システムの状態空間に対し，状態爆発を防ぐための段階的な検査方法の開発に取り組んできた.[1)] この検査方法は，状態空間を分割しながら，小さな領域ごとにモデル検査を適用する 1 次処理と，分割した領域間の横断をつなぎあわせて探索する 2 次処理から構成されている．

本研究では，最小領域に分割しても状態爆発が発生するケースや分割した領域数が膨大になケースが想定される情報制御システムに対して，サブシステムに分割し，これらをモジュラ検証する方法を提案する．また，列車運行システムを事例として，本手法を適用し，その効果を確認した．

2. 情報制御システム

情報制御システムは，作業員が手作業で行う設備の制御に関するノウハウをルールとして体系化し，そのルールをもとに自動または半自動で設備を制御するシステムのことであり，主に電力や列車運行などのインフラ系の制御システムとして使用される．センサによって外部環境から取得されたデータは，抽象化された離散値へ変換され，システムへの入力値となる．情報制御システムはこのような入力値をもとにルールを適用し，設備の状態を更新する．システムの状態は，設備の状態を表す属性の組み合わせによって表現される．

†1 茨城工業高等専門学校
National Institute of Technology, Ibaraki College
†2 茨城大学
Ibaraki University

3. モデル検査方法

3.1 段階的検証

本研究のモデル検査は，以下の 2 つの段階に分けて処理する．

1 次処理 モデル検査で着目したい属性が関わるシステムの全ての状態について，状態遷移を取得する．この処理において得られた状態遷移を本論文では部分遷移と呼ぶ．

2 次処理 1 次処理で取得した部分遷移をつなぎ，状態遷移モデルを生成する．この状態遷移モデル上で，モデル検査の制約を満たすかどうかを探索し，この制約に違反する状態に到達した際はこの状態を反例として出力する．

3.2 モジュラ検証

システムを分割して検証するモジュラ検証において，本研究では，検査対象全体を対象システム，検査対象全体の振舞いモデルを全体モデル，対して分割後の検査対象をサブシステム，サブシステムの振舞いモデル

を部分モデルと呼ぶ．

情報制御システムを各サブシステムが協調する対象システムとしてモデル化する際，これらのサブシステム間の相互関係は，次のような 2 種類の関係に分類できる．

物理的制約による相互関係　あるサブシステムを構成している設備が，別のサブシステムを構成している設備と同一である

制御ルールによる相互関係　あるサブシステムにおいて，別のサブシステムの状態に依存する制御ルールが存在している

モジュラ検証においてサブシステムを検証する際，他のサブシステムとの相互関係を表現するために，1 次処理では相互関係に必要な他のサブシステムの状態を加えた状態遷移を生成する．2 次処理では，対象システムの構造を基に各サブシステムの状態を合成することで，サブシステムをまたいで状態モデル探索して検証できる．

4. 適 用 事 例

本手法を適用した列車運行システムの路線構成を図 1 に示す．これをサブシステムに分割すると図 2 のような路線構成となる．この路線構成において，通常の信号機の制御ではデッドロックが発生する．(例：駅 B のホームに列車が 2 台在線している時，駅 A と駅 C からそれぞれ駅 B に向けて列車が進行する場合）このデッドロックが発生しないようにするために，入替信号機（駅内信号機）を制御するルールに回避ルール（進行方向先進路の在線状況を確認して青色点灯に変える）を追加する．この適用事例において，サブシステム間の相互関係は以下のようになる．

物理的制約　サブシステム間で重なる軌道回路の状態

制御ルール　入替信号機に追加した回避ルール

この事例への検査方法に対する検査の総実行時間を表 1 に示す．モジュラ検証により実行時間を削減できたことが確認できる．また，この事例のデッドロックは最低でも 4 台の列車によって発生するため，それを前提に 4 台の制限を設けた場合は，さらに削減できることが確認できる．モジュラ検証する場合，サブシステム間の結合度が低いほど相互関係に用いる状態が少なくなり，検証に必要となる遷移関係を削減する効果が期待できると考えられる．

表 1　検査法に対する総実行時間

手法	回避策	実行時間
段階的検査	なし	1208m00s(486m48s)
	あり	1179m52s(460m19s)
モジュラ検証	なし	531m02s(143m06s)
	あり	523m57s(142m34s)
モジュラ検証 (4 台制限)	なし	166m38s(143m00s)
	あり	165m57s(142m28s)

※括弧内の時間は DB 登録の時間を除いた実行時間．

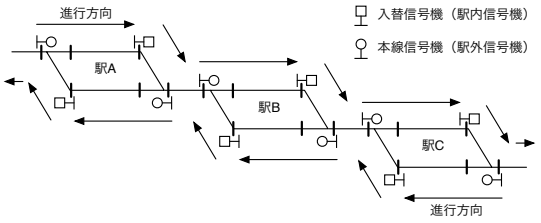

図 1　適用事例の路線構成

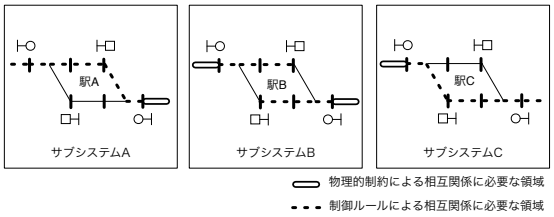

図 2　適用事例を分割した路線構成

5. 課題とまとめ

本研究では，情報制御システムをいくつかのサブシステムに分割し，それぞれのサブシステムごとに振舞いモデルを作成した後に，モジュラ検証する手法を提案した．本手法による効果は，分割モデル間の結合度が低いほど有効である．

今後の課題としては，2 次処理時の探索アルゴリズムの改善が挙げられる．今回使用した探索アルゴリズムは単純な深さ優先探索であったため，循環した状態遷移などにも対応できるよう改良する必要がある．また，段階的手法のみでは検証が困難な大きさの規模の情報制御システムに対してモジュラ検証を適用し，本研究で提案した方法の有効性をさらに評価してく必要がある．

謝辞　本研究を進めるにあたり，適切な助言をくださいました株式会社日立製作所 武澤 隆之氏，山形 知行氏に感謝致します．本研究は JSPS 科研費 25330075 の助成を受けたものである．

参 考 文 献

1) 小山恭平, 小飼敬, 上田賀一, 山形知行, 武澤隆之: 情報制御システムに対する SPIN を用いた段階的モデル検査手法, 日本ソフトウェア科学会第 30 回大会, 一般 3-5 (2013).