情報制御システムのモデル検査に対する分割アプローチと課題

小飼 敬[†1] 宮島卓巳[†2]
小山恭平[†2] 上田賀一[†2]

モデル検査の状態爆発の対策として，情報制御システムを相互関係があるサブシステムごとに分割して検証モデル化を行い，部分モデル間の相互関係に関する情報を検証モデルの外部で管理し，検証を行う方法とその課題について述べる．

Partitioning Approach to Model Checking of Information Control System and its Problems

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

As a countermeasure of state explosion of model checking, our approach makes models to interrelated each subsystem, and manages the correlations between the models outside of model checking. This study describes the problems of our approach.

1. はじめに

形式手法の1つである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正当性を満足するかどうかを検査することができる．本研究では，情報制御システムを対象として，実用的なシステムの規模を検証可能とすることである．これまでの研究[1)]では，情報制御システムのモデルをモデル検査器SPINの記述言語Promelaに変換し，検証する手法を提案している．本研究では大規模な情報制御システムをサブシステムごとに分けてモデル化し，サブシステム間で相互に作用する情報を共通で管理するモデル分割手法を提案する．これにより，検証するモデルを部分モデル化したそれぞれのモデルに対して段階的に検証することが可能となる．本研究では，3駅から構成される列車運行に関する情報制御システムに対して，サブシステムをモデル化し，それぞれのモデルに対して段階的に検証を行った．

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る．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．情報制御システムでは，センサーが外部環境からデータを取得し，その値が抽象化された離散値へ変換され，制御システムの入力値となる．情報制御システムは入力値をもとにルールを適用し，設備の状態を更新する．このような動作を1周期とし，繰り返し実行する．

3. モデル検査方法の提案

3.1 相互関係のある情報制御システム

相互関係のある情報制御システムとは，情報制御システムをサブシステムで分割した際に，サブシステム間の設備状態に物理的制約による関係，または制御ルールによる関係があるシステムである．物理的制約による関係がある例として，複数駅間の列車運行制御のモデルがある．サブシステムを個々の駅とすると，相互関係は駅間の区間における列車の在線状態となる．また，制御ルールによる関係がある例として，複数エレベータの制御システムがある．サブシステムを各エレベータとすると，各エレベータは他のエレベータと連携するために必要な情報を相互関係として持つ．本研究では，サブシステム間に関わり合うルールをグローバルルールと呼び，対して1つのサブシステムで

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

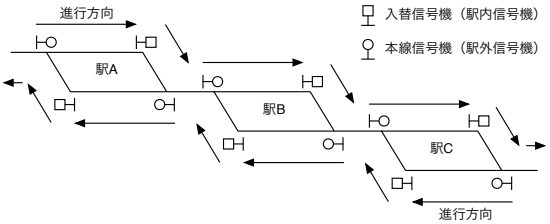

図 1　適用事例の路線モデル

のルールをローカルルールと呼ぶ．このように他のサブシステムの状態に応じて制御判断が変わるようなグローバルルールで結びついているものが相互関係のある情報制御システムである．

3.2　モデルの分割

相互関係のある情報制御システムをサブシステムごとに分割し，これらを部分的にモデル化する．部分的なモデル化により，1 回の検証で対象とするモデルの規模が小さくなるため，検証時の網羅探索における状態爆発を防ぐことができる．しかしながら，そのまま部分的なモデルに分割した場合，他のサブシステムの情報を持たないため，グローバルルールを適用できなくなる．そこで，グローバルルールを含めた部分的なモデルの状態に対して網羅探索をする．

4. 適 用 事 例

図 1 の路線モデルでは，列車の在線状態から信号機を制御し，列車は信号機の点灯状態から次の進路へ進むことができるかを決定する．列車の進行は非決定的に行い，列車が進んだ場合は，路線モデルの状態が変化したとみなす．通常，信号機は管轄する進路内に列車が在線していない場合は青色点灯となる．

図 1 の路線モデルを部分的なモデルに分割する場合，駅 A, B, C それぞれを部分的なモデルとして検証する．部分的なモデルとして検証する際の概念図を図 2 に示す．グローバルルールとして，駅間で扱うための情報となる「回避ルール」を 4 つとした．

表 1　各モデルの状態遷移数と実行時間

対象モデル	回避ルールの有無	取得状態遷移数	デッドロック数	実行時間
全体モデル	無	1,654,312	241	431m44s
全体モデル	有	1,650,952	241	426m42s
駅 A のみ	無	97,368	576	15m40s
駅 A のみ	有	96,392	752	13m4s
駅 B のみ	無	422,352	5,616	66m58s
駅 B のみ	有	415,520	7,032	62m24s
駅 C のみ	無	97,368	576	12m23s
駅 C のみ	有	96,392	752	13m20s

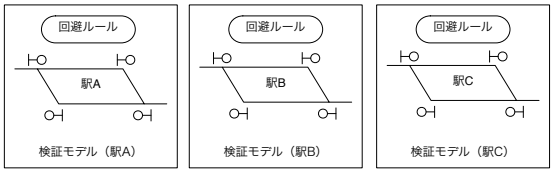

図 2　分割した部分的なモデル

実験結果を表 1 に示す．取得した状態遷移数が，回避ルールの無いモデルの方が多いことから，これらの遷移がデッドロックへ向かう遷移であることが分かる．実行時間はモデル分割した場合の方が圧倒的に短い．これは初期状態として設定する状態数が，全体モデルで 527,337 個あるのに対して，駅 A のみで 45,648 個，駅 B のみで 176,384，駅 C のみで 45,648 個と規模を縮小できたためである．今回の適用事例では相互関係に用いる情報が比較的小さいため実行時間が短かったと考えられる．この相互関係に用いる情報が多くなるほど初期状態数が増加するため，相互関係への依存が高いシステム程本手法の有効性は低くなると考えられる．

5. 課題とまとめ

本研究では，情報制御システムのモデル検査において，段階的に検証を行い，その際に情報制御システムをサブシステムごとに分割して検証する方法を提案した．相互関係の依存度が比較的小さなモデルに対しては，本手法が有効であることが確認できた．

しかし，サブシステムに分割する際に，情報制御システムにおける制御判断を，グローバルルールとローカルルールに分けるめたの一般的な手段を確立できていない．また，本手法は，相互関係の依存度が大きいモデルに対しては不向きな手法であるが，どの程度の依存度までなら，実用的なモデル検査が可能なのかも明確にはなっていない．今回扱った列車運行に路線モデルの場合は分割しやすい例であったが，今後は様々な例を対象として検討を続ける必要がある．

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) 柳翔太, 小飼敬, 上田賀一, 大久保訓, 高橋勇喜, 中野利彦: 情報制御システム記述モデル検証用記述への変換と効率的検証, 日本ソフトウェア科学会第 27 回大会, 7C-1 (2010).