鉄道信号システムの連動論理検証

6 J－4

川村 正　　金森 直
三菱電機(株)先端技術総合研究所

1．はじめに

鉄道信号システムは、障害や誤動作が重大な事故につながるため、安全性に関して厳しい基準が求められている。駅構内の信号機や分岐器（転轍器）の制御を行う装置は連動装置と呼ばれ、鉄道信号システムの保安機能に関して中心的な役割を果たす。連度装置の行う制御は比較的小規模な駅でも複雑になり、その検査には膨大なコストがかけられている。本研究では、論理回路検証の分野で用いられているモデル検査法によって連動装置の制御論理の形式的検証を行う方法を提案する。

2．連動装置

鉄道信号システムは、列車の位置検知と分岐器・転轍器の制御を行い、制御盤からの操作に従って信号機等で列車に進行・停止の指示を与えることによって列車の運行制御を行う。特に駅構内では交通が輻輳するため、列車の進行に際して、

（1）進路上に他の列車がいない、分岐器が必要な方向を向いている、他の列車の進路と交錯していないことをチェックした上で信号機に進行信号を表示させ、

（2）列車が進行中は進路上の転轍器は転換しない

ことが必要である。このような機能を連動と呼び、オペレータの操作に従ってこの機能を実現するシステムを連動装置と呼ぶ。また、連動装置の制御論理を連動論理と呼ぶ。

連動装置の制御仕様は連動図表と呼ばれる図と表で表わされる。連動装置及び連動図表の詳細については文献[7,8]に詳しい。

3．モデル検査法を用いた連動論理の形式的検証

ソフトウェアや回路の大規模複雑化に伴い、それらのソフトウェアや回路が与えられた仕様を満足するかどうかを完全に保証するための形式的検証法が重要性を増している。鉄道システムの分野でも、鉄道総研が事務局となり安全性技術に豊富な経験を持つ専門家の参加によって 1996 年に作成されたガイドライン「列車運転制御システムの安全性技術指針」の中で、事前安全性解析のための技術として形式的手法が推奨されており[6]、またいくつかの試みがなされている[2,4,5]。これらを踏まえて、本研究では、連動図表で表わされた連動論理の形式的検証を試みる。

3．1　モデル検査法

モデル検査法は論理回路検証の分野で成功を納めている形式的検証法である[1,3]。この方法は、検証すべき仕様を時相論理式で、検証対象のシステムを有限状態機械（Kripke 構造）で記述し、この有限状態機械上で時相論理式が成り立つかどうかを証明するものである。本研究では、モデル検査法を用いて連動論理の形式的検証を行う。

Verification of Railway Interlocking Systems
Tadashi Kawamura and Tadashi Kanamori
Mitsubishi Electric Corporation
8-1-1,Tsukaguchi-Honmachi,Amagasaki,Hyogo,661-8661,Japan

3．2　連動装置の記述

連動装置に加えて信号機、転轍器、軌道回路などの現場機器や信号てこ、転轍てこなどの制御盤上の機器及び列車の動作を有限状態機械で記述する。連動装置については、連動図表で表わされた情報を基にその連動論理を有限状態機械によって記述する。現場機器や制御盤上の機器、列車についてはそれぞれの動作に応じて有限状態機械で記述する。

3．3　検証項目

本研究では以下のような検証項目を設定した。

（1）進路内到達可能：進路上の任意の軌道区間に列車が到達できる。

（2）進路外到達不可能：進路外の軌道区間に列車は到達できない。

（3）脱線・割り出しなし：進路の設定方向と分岐器の方向が一致している。

（4）危険転換なし：列車がある軌道区間内にあるとき、その区間内の分岐器の転換が行われない。

（5）衝突なし：一つの軌道区間内に複数の列車が同時に進入しない。

（6）接触なし：接触の危険のある軌道区間には同時に列車が進入しない。

3．4　実験

論理検証システムｓｍｖ[3]を用いて検証実験を行った。使用した計算機はDOS/Vマシンで CPU は Pentium II 266MH、OS は Linux である。検証の対象を3進路以下、通過する列車が2台までに限定とすると前節（1）～（6）のいずれの検証項目に対しても、検証時間は1秒以内、消費メモリ量は1.5MB以下で検証可能である。しかしながら、一般にモデル検査法では検証対象の規模に対して計算時間・消費メモリ量が指数関数的に大きくなることが知られており、どの程度の規模の駅まで検証が可能であるかは今後更なる実験・検討が必要である。

5．おわりに

鉄道信号システムのように安全性が非常に重視される分野においては、形式的手法の重要性は今後ますます増していくと考えられる。本研究では連動論理の形式的検証を試みた。今後の課題として、検証できる規模の限界を探り実用規模の駅への適用の試み、検証項目の適切さの検討、連動図表作成やソフトウェア生成も含めたツール化などがあげられる。

参考文献

[1] Bernardeschi,C., Fantechi,A., Gnesi,S., Larosa,S.,Mongardi,G. and Romano, D. : A Formal Verification Environment for Railway Signaling System Design, Formal Method in System Design, Vol.12,pp.139-161,1998.

[2] Burch,J.R., Clarke,E.M., Mcmillan,K.L. and Dill,D.L. : Sequential Circuit Verification Using Symbolic Model Checking, in Proc. of 27th Design Automation Conference, pp.46-51, 1990.

[3] McMillan, K. : Symbolic Model Checking, Kluwer Academic Publishers, 1993.

[4] 福岡、福田：ペトリネットによる連動仕様の検証、鉄道総研報告 Vol.9,No.11,1995.

[5] 平尾、福田：鉄道信号におけるソフトウェア安全性技術、日本鉄道技術協会 Vol.41,No.5,1998.

[6] 平尾、渡辺：列車保安制御システムの安全性技術指針、鉄道総研報告 Vol.10,No.11,1996.

[7]（社）日本鉄道電気技術協会編：信号入門、1988.

[8]（社）日本鉄道電気技術協会編：連動装置、鉄道技術者のための電気概論 信号シリーズ5、1993.