鉄道信号システムのモデル検査器SPINによる検証

大神, 茂之
九州大学大学院システム情報科学府知能システム学専攻 : 修士課程

清水, 亮
九州大学大学院システム情報科学府知能システム学専攻 : 修士課程

越村, 三幸
九州大学大学院システム情報科学研究院知能システム学部門

川村, 正
三菱電機(株)先端技術総合研究所

他

https://doi.org/10.15017/1516058

出版情報：九州大学大学院システム情報科学紀要. 10 (1), pp.33-38, 2005-03-25. 九州大学大学院システム情報科学研究院
バージョン：
権利関係：

九州大学大学院
システム情報科学紀要
第10巻 第1号 平成17年3月

Research Reports on Information Science and
Electrical Engineering of Kyushu University
Vol.10, No.1, March 2005

鉄道信号システムのモデル検査器SPINによる検証

大神茂之*・清水亮*・越村三幸**・川村正***・藤田博**・長谷川隆三**

Formal Verification of a Railway Interlocking System by the SPIN Model Checker

Shigeyuki OOGAMI, Ryo SHIMIZU, Miyuki KOSHIMURA, Tadashi KAWAMURA,
Hiroshi FUJITA and Ryuzo HASEGAWA

(Received December 24, 2004)

Abstract: The verification of safety requirements is a fundamental problem in railway signalling system design. Especially, specification of railway inter-locking systems, which control railway signals and points in a station in a safety-critical manner, becomes very complex and hard to verify. Recently in this fields, formal verification is expected to be a promising technique for verifying safety requirements. This paper describes how to verify a railway inter-locking specifications by the model checker SPIN which is a formal verification tool. In this method, a railway inter-locking system is described as a finite state machine and safety requirements are given by temporal logic formulas. Then, SPIN checks that the state machine satisfies the requirements.

Keywords: Formal verification, Railway interlocking system, Model checking, Modal logic

1. はじめに

鉄道信号システムは列車の運行制御を行うものであり，システムに障害や誤作動が起こると人の命に関わる重大な事故が起きる可能性がある．鉄道信号システムの中でも，中心的な役割を果たすのが連動装置である．連動装置の制御の仕様は連動図表と呼ばれる図と表で表されている．

連動装置の設計及び検査には人が時間をかけて行っているのが現状である．近年，鉄道信号システムの大規模化，高機能化に伴い，連動装置の行う制御は複雑化し，その安全性・信頼性を保証することは困難になっており，連動装置の設計及び検査にかかるコストは膨大なものになっている．

その解決策として，形式的手法の一つであるモデル検査による検証が注目されており，鉄道信号システムの検証に関しても幾つかの検証事例が報告されている[6),5)]．モデル検査はシステムが仕様通りに動作するかどうかを検証する技術であり，その手続きは完全に自動化されている．モデル検査は論理回路やプロトコルの検証ではすでに成功を納めており，他の分野でも期待される技術である[1)]．

モデル検査システムはいくつも提案されており，代表的なものとしてSPIN[2),3)]やSMV[4)]が知られている．本研究では，SPINを用いて信号システムを検証する．モデル検査では，検証対象となるシステムを有限状態オートマトンを用いてモデル化し，検査項目を時相論理式を用いて表現する．そして，オートマトンが時相論理式を満たすかどうかの検査を自動的に行う．

本論文では，二つのモデル化手法を提案し比較する．一つは，連動図表レベルの比較的抽象度の高い動作をモデル化するもの，もう一つは，より抽象度の低い，連動装置を構成するリレー回路の動作をモデル化するものである．

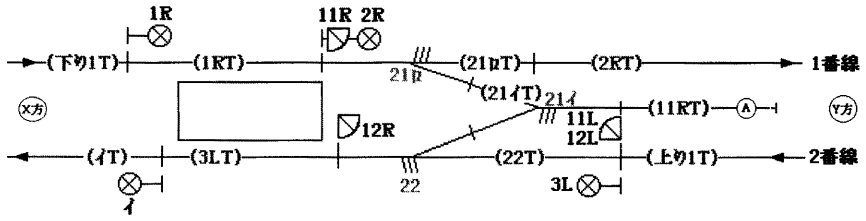
2. 連動装置

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のが連動装置である．連動装置は以下の制御を実現する．

- 進路上に他の列車がいない，転てつ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る．
- 進行信号が現示されている間は，オペレータが間違った操作をしても進路上の転てつ器は転換しない．

信号機やその他の機器，列車の状態によって転てつ器を転換できないようにすることを鎖錠と呼び，鎖錠を解くことを解錠と呼ぶ．

平成16年12月24日受付
* 知能システム学専攻修士課程
** 知能システム学部門
*** 三菱電機(株)先端技術総合研究所



名称		番号	鎖錠	信号制御	進路鎖錠	接近または保留鎖錠
場内信号機	X方-1番線	1R	11L	1RT		下り2T 下り1T [90秒]
出発信号機	1番線-Y方	2R	21	21ロT 2RT	(21ロT)	下り2T 下り1T(但[1R] 1RT [90秒]
場内信号機	Y方-2番線	3L	22	22T 3LT(21イT (但21)	(22T)	上り2T 上り1T [90秒]
出発信号機	1番線-A	11R	[21]	21ロT 21イT 11RT	(21ロT 21イT)	1RT [30秒]
同上	A-1番線	11L	1R [21]	21イT 21ロT 1RT	(21ロT 21イT)	11RT [30秒]
同上	2番線-A	12R	21 [22]	22T 21イT 11RT	(22T)(21イT)	3LT [30秒]
同上	A-2番線	12L	21 [22]	21イT 22T 3LT	(21イT)(22T)	11RT [30秒]
同上	2番線-X方	イ		イT		
名称		番号	鎖錠	てつ鎖鎖錠	進路鎖錠	接近または保留鎖錠
転轍機	(2動)	21		21イT 21ロT		
同上		22		22T(21イT (但21)		

Fig. 1　An interlocking table.

2.1 連動図表

連動装置の制御の仕様は，連動図表と呼ばれる図と表で表される．連動図は機器及びその配置を表している．**Fig. 1**は,『信号入門』[7]に例題として掲載されている連動図表である．実線は線路を表し，線路上の縦線で区切られた各区分には軌道回路が設置され，区分内の列車の有無を検知する．**Fig. 1**を例として，軌道，転てつ器，信号機について簡単に述べる．

- 軌道(track): 軌道は,「下1T」,「1RT」といったようにTが最後についている名前で表現されている．軌道は線路の区切られた一部分のことで，その上に列車がいるかどうかを判定する回路にそれぞれ対応している．
- 転てつ器(point): 転てつ器は,「21イ」,「21ロ」,「22」といったような名前で表現されている．転てつ器は列車の進行方向を切り替えるスイッチの役目を果たしている．例えば21ロは,「1RT」-「21ロT」-「2RT」と，[1RT」-「21ロT」-「21イT」-「11RT」という2つの進路を切り替える役割を担っている．連動図において，転てつ器には三本のひげのような棒が記載されている．転てつ器がこのひげのような棒の方向に向いているときを「定位」，そうでないときを「反位」，どちらでもないときを「中立」と呼んでいる．転てつ器が定位もしくは反位に鎖錠されていないときに列車が通過すると，脱線の危険がある．また,「21イ」「21ロ」のように，最後のカタカナを除いて同じ名前の転てつ器は，一体となって方向を変更する．すなわち,「21イ」が定位のときは,「21ロ」も定位である．
- 信号機(signal): 信号機は,「1R」「2R」「3L」などの名前で表現されている．例えば，信号「1R」は列車が「下り1T」にいるときに「1RT」に進むための信号であり,「11R」は列車が「1RT」にいるときに「11RT」方面に進むための信号である．信号機にも「定位」と「反位」があり，原則として停止信号が「定位」，進行信号が「反位」と定められている．

連動表は各進路ごとに現場機器の連動仕様を記述する．

2.2 連動装置の種類

連動装置にはリレー回路によって構成されている継電連動装置とマイクロコンピュータ制御の電子連動装置の2種類がある．継電連動装置のリレー回路に関しては標準結線が定められており，連動仕様を構成する各パターンごとにリレー回路の標準的な構成が定められている．電子連動装置の連動機能の構成法は，大筋で連動装置の構成を引き継いでおり，その標準結線をプログラム化したものである．

2.3 連動装置の動作の流れ

継電連動装置では，リレーの動作によって純電気的な鎖錠を行い，信号機・転てつ器等の間に連鎖関係をつけている．連鎖の流れは**Fig. 2**のようになっている．今，ある信号てこを反位に扱った場合，まず最初にてこリレー(LR,RR)が動作し，該当転てつ器に対して転換指令が出

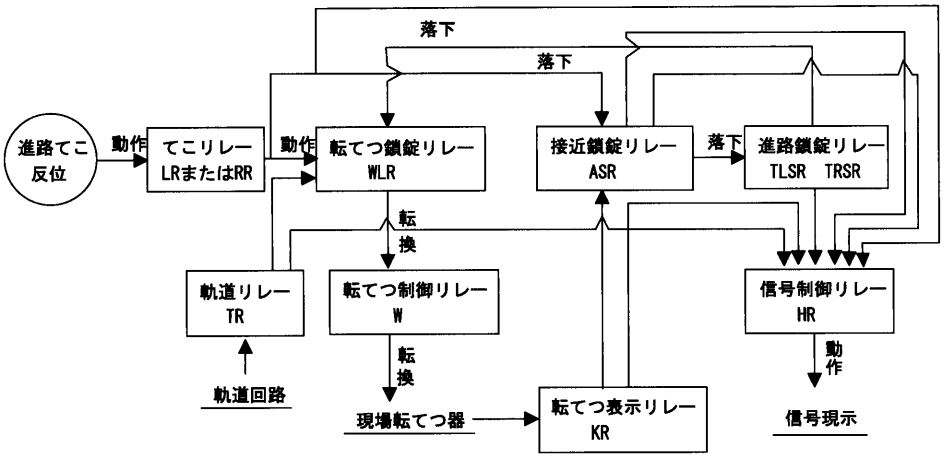


Fig. 2 An overview of signal propagations of relays.

る．しかしこの場合無条件に転てつ器が転換しては大変危険であるから，関係する軌道回路に列車または車両がいないこと，すなわちてつ査鎖錠がかかっていない条件として軌道リレー(TR)が動作していること，またその進路を支障する他からの進路が構成していないこと，すなわち進路鎖錠リレー(TLSR,TRSR)が動作していることをチェックして転てつ鎖錠リレー(WLR)が動作する．WLRが動作することにより転てつ制御リレー(W)の鎖錠が解錠し，初めて現場にあるWが所定の方向に動作，転てつ器が指令どおりに転換し，転てつ表示リレー(KR)が定位または反位に動作する．

このように関係する転てつ器が全部所定の方向に転換したことと，てこリレーが動作していることをチェックし，接近鎖錠リレー(ASR)が落下，続いて進路鎖錠リレー(TLSR,TRSR)が落下する．進路鎖錠リレーが落下することにより転てつ制御回路の鎖錠回路が断たれ，転てつ鎖錠リレー(WLR)が落下，転てつ制御リレー(W)を鎖錠，すなわち転てつ器の鎖錠を完了する．ここに信号てこを取り扱ったことにより関係転てつ器を転換，鎖錠という一連の動作がなされたわけである．

次にてこリレーの動作，軌道リレーの動作，転てつ鎖錠リレーの落下，転てつ表示リレーが所定の方向に動作していること，接近鎖錠リレーの落下，進路鎖錠リレーの落下等をチェックし信号制御リレー(HR)が動作する．

3. SPIN による検証

3.1 形式的検証

形式手法を用いた検証（形式的検証）とは，状態遷移系として記述されたシステムが論理式で表現された要求仕様（検査項目）を満たすか否かを数学的方法を用いて検証することである．一般にシステムの誤動作は「バグ」と呼ばれる．バグを発見するためには通常，仕様書の査読，製作完了後のテストが行われるが，バグが発見されるのは製作完了後のテストの結果によることが多い．製作完了後に見つかったこのようなバグに対しては膨大な改修作業を必要とするため，開発コストの上昇を招くという問題がある．この問題を解決するため，システム製作前の段階で経験や知識に依存しない形式手法を用いてシステム検証を行うことに期待が寄せられている．

3.2 モデル検査

モデル検査とは形式的検証を行う手法の一つで，モデルと呼ばれる有限個の状態を持つ仮想システムが検査項目を満たすか否かを，機械的かつ網羅的に検査することである．これを計算機上で自動的に行うツールをモデル検査ツールと呼ぶ．モデル検査は全ての状態を検査するため，検査項目を満たさないケースが一つでも存在するならば必ず発見が可能である．従来のテストによる検証方法は網羅的なものではないため，「めったに起こらないバグ」を発見しにくいという欠点があり，この欠点は鉄道システムのような安全性が重要視されるシステムの検証に関して大きな問題となりうる．この問題の解決の糸口として，モデル検査を用いた形式的検証が注目されている．

3.3 SPIN によるモデル検査

SPIN(Simple Promela Interpreter) はモデル検査ツールの一つであり，仕様記述言語として Promela(Protocol/Process Meta Language) と呼ぶ言語を用いて，並行システムの検証を行うことができる．SPINは線形時相論理でのモデル検査を行い，システムの安全性，信頼性を検証できる．

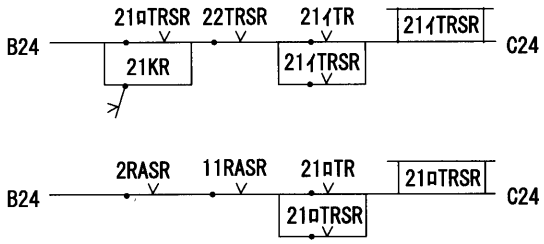


Fig. 3　Relays for locking a route.

SPINの原理はとても明確なものである．有限状態のモデルをAとし，検証したい項目を線形時相論理式で表したものをBとする．モデルAにおいて検証項目Bを満たすかどうかを検証する場合，SPINではモデルAのオートマトンと$\neg B$のオートマトンを生成し，それらを掛け合わせたオートマトンを作る．そのオートマトンをA$\otimes\neg$ Bとするとき，A$\otimes\neg$ Bが何も受理できないならば，モデルAにおいて検証項目Bを満たし，何か受理できるならば検証項目Bを満たさないということを証明できる．

4. 連動装置の仕様の検証

本研究では連動図表から直接仕様をモデル化し安全性を検証する方法と，継電連動装置を構成しているリレー回路をモデル化しその安全性の検証を行う方法で連動装置の仕様の検証をしている．前者の方法を検証方法1，後者を検証方法2としそれぞれについて以下で説明する．

4.1 検証方法1

列車プロセスを二つ作成する．信号機や転てつ器といった連動装置の状態は，全て変数の値として表現する．

4.1.1 列車と信号機のモデル化

列車プロセスは，現在地と目的地を変数の形で保持する．列車は意思を持たず，たとえ目の前に他の列車が存在しようが，ひたすら目的地に向けて突き進むとする．停止信号で列車が次に進めない場合は，連動図表に基づきその信号を進行信号に転換する事が可能かどうかの検査を行い，可能な場合は，転てつ器の鎖錠等のしかるべき処置を行ったのち進行信号を現示させる。

4.2 検証方法2

リレー回路，列車，転てつ器，オペレータをPromelaでモデル化する．

4.2.1 リレー回路のモデル化

リレー回路の各リレーは，落下している状態，動作している状態の2つの状態を持つ．各リレーそれぞれに対して，落下する条件，動作する条件をPromelaで記述することでリレー回路のモデル化を行う．

Fig. 1の連動図表のうち進路11Rの進路鎖錠を実現するリレー回路の一部を**Fig. 3**に示す．

B24からC24の向きに電流が流れればリレーは動作し，電流が途切れるとリレーは落下する．21イTRSRが動作する条件は，(「21ロTRSRが動作しているor21KR がN接点である」＆「22TRSRが動作している」＆「21イTRが動作している」) である．逆に21イTRSRが落下する条件は，(「21ロTRSRが落下している＆21KR がN接点ではない」or 「22TRSRが落下している」)である．これをPromelaで記述すると次のようになる．

- 21イTRSRが動作する条件

```
:: (((r_21roTRSR==1 || r_21KR==Normal)
&& r_22TRSR==1 && r_21iTR==1)
&& r_21iTRSR==0) -> r_21iTRSR=1;
```

- 21イTRSRが落下する条件

```
:: (((r_21roTRSR==0 && r_21KR!=Normal)
|| r_22TRSR==0) &&  r_21iTRSR==1)
-> r_21iTRSR=0;
```

すべてのリレーについて落下条件，動作条件を記述する．

4.2.2 列車のモデル化

右から左に進行する列車と，左から右へ進行する列車の2種類に分ける．列車一台につき一つのプロセスを作成し，それぞれに初期位置と目的地を与える．列車は信号機を確認したとき停止信号ならば，信号機の手前の軌道で停止しておく，進行信号を確認すると前に進む．また転てつ器が配置されている軌道上に列車がいる場合，転てつ器の向いている方向が正しいかどうかを確認し，誤った方向を向いているときは列車の位置をERRORに移し，その時点で検証の失敗とする．

4.2.3 転てつ器のモデル化

転てつ器には4つの状態があるものとし，定位の状態，反位の状態，反位から定位に転換途中の状態，定位から反位に転換途中の状態をもつ．転てつ制御リレー(W)が反位への転換指令を出す場合，定位の状態から定位から反位へ転換途中の状態に移行し，反位の状態へ移行する．逆も同様である．

4.2.4 オペレータのモデル化

オペレータは設定したい進路の信号てこを転換する役割を果たす．列車プロセス一つに対し，オペレータプロセス一つを作成する．オペレータプロセスには出発点と目的地点を与え，その間の含まれる信号てこを反位にする．列車が目的地に到着したときに，反位にした信号てこを定位に戻す．

4.3 検証結果

Table 1は，二台の列車が共に目的地に到達できるかどうかの検証結果を示している．Resultの○は検証に成功したことを，×は到達できない例がSPINによって示されたことを表す．Statesは検証の際に探索した状態数，

Table 1 Verification of train reachability.

Route		Verification 1			Verification 2		
Train1	Train2	Result	States	Memory	Result	States	Memory
下り 2 T→ 1 RT	1 RT→ 2 RT	○	70367	14.398	○	888	3.044
下り 2 T→ 1 RT	1 RT→ 1 1 RT	○	70466	14.398	○	1278	3.147
下り 2 T→ 1 RT	1 1 RT→ 1 RT	○	284203	50.238	×	168	3.044
下り 2 T→ 1 RT	1 1 RT→ 3 LT	○	859	2.724	○	1848	3.147
下り 2 T→ 1 RT	上り 2 T→ 3 LT	○	659	2.724	○	2253	3.147
下り 2 T→ 1 RT	3 LT→ 1 1 RT	○	884	2.724	○	1876	3.147
1 RT→ 2 RT	1 1 RT→ 1 RT	○	109648	21.054	×	645	3.044
1 RT→ 2 RT	1 1 RT→ 3 LT	○	1029	2.724	○	1610	3.147
1 RT→ 2 RT	上り 2 T→ 3 LT	○	789	2.724	○	2114	3.147
1 RT→ 2 RT	3 LT→ 1 1 RT	○	1059	2.724	○	1622	3.147
1 RT→ 1 1 RT	1 1 RT→ 1 RT	×	5054	3.441	×	124	3.044
1 RT→ 1 1 RT	1 1 RT→ 3 LT	○	105164	20.235	×	736	3.044
1 RT→ 1 1 RT	3 LT→ 1 1 RT	○	393466	68.67	×	275	3.044
1 1 RT→ 3 LT	上り 2 T→ 3 LT	○	184950	33.649	×	272	3.044
1 1 RT→ 3 LT	3 LT→ 1 1 RT	×	5054	3.441	×	126	3.044
1 1 RT→ 1 RT	上り 2 T→ 3 LT	○	859	2.724	○	3252	3.249
1 1 RT→ 1 RT	3 LT→ 1 1 RT	○	85835	16.856	×	127	3.044
3 LT→ 1 1 RT	上り 2 T→ 3 LT	○	119904	22.692	×	148	3.044

Memory : Mega byte

Table 2 Verification of possibility of train crash.

Route		Verification 1			Verification 2		
Train1	Train2	Result	States	Memory	Result	States	Memory
下り 2 T→ 1 RT	1 RT→ 2 RT	○	546	2.622	○	1068	3.044
下り 2 T→ 1 RT	1 RT→ 1 1 RT	○	621	2.622	○	1429	3.147
下り 2 T→ 1 RT	1 1 RT→ 1 RT	○	621	2.622	○	1388	3.147
下り 2 T→ 1 RT	1 1 RT→ 3 LT	○	859	2.724	○	2016	3.147
下り 2 T→ 1 RT	上り 2 T→ 3 LT	○	659	2.724	○	2433	3.249
下り 2 T→ 1 RT	3 LT→ 1 1 RT	○	884	2.724	○	2044	3.147
1 RT→ 2 RT	1 1 RT→ 1 RT	○	457	2.622	○	1012	3.044
1 RT→ 2 RT	1 1 RT→ 3 LT	○	1029	2.724	○	1790	3.147
1 RT→ 2 RT	上り 2 T→ 3 LT	○	789	2.724	○	2308	3.147
1 RT→ 2 RT	3 LT→ 1 1 RT	○	1059	2.724	○	1802	3.147
1 RT→ 1 1 RT	1 1 RT→ 1 RT	○	71	2.622	○	273	3.044
1 RT→ 1 1 RT	1 1 RT→ 3 LT	○	606	2.622	○	1589	3.147
1 RT→ 1 1 RT	3 LT→ 1 1 RT	○	699	2.724	○	1806	3.147
1 1 RT→ 3 LT	上り 2 T→ 3 LT	○	501	2.622	○	62371	8.472
1 1 RT→ 3 LT	3 LT→ 1 1 RT	○	71	2.622	○	305	3.044
1 1 RT→ 1 RT	上り 2 T→ 3 LT	○	859	2.724	○	3233	3.249
1 1 RT→ 1 RT	3 LT→ 1 1 RT	○	271	2.622	○	1191	3.044
3 LT→ 1 1 RT	上り 2 T→ 3 LT	○	476	2.622	○	12195	4.069

Memory : Mega byte

Memoryは検証に要したメモリ量をメガバイト単位で示している．

Table 2は，二台の列車が衝突するかどうかの検証結果を示している．Resultの○は衝突しないことが示されたことを，×は，衝突する例がSPINによって示されたこと表す．

4.3.1 目的地到達の検証について

検証方法1，2の双方で×となっているのは，列車1と2が互いに対向進路をとっている場合で，この時は互いに目的地に到達できない．また検証方法1で○，検証方法2で×と結果が異なっているのは7例あるが，この違いは以下の理由による．

- 2台の列車の目的地が同じ場合，検証方法2ではどちらかが目的地に到達できない．検証方法1では目的地に到達した列車の位置をCLEARに移すのでもう1台も目的地に到達できるため検証に失敗しない．(下り2T→1RT，11RT→1RT)，(1RT→11RT，3LT→11RT)，(11RT→3LT，上り2T→3LT)の組み合わせで起こる．検証方法2において検証方法1と同様の処理をすることで，検証に成功すると考えられる．
- 検証方法2では進路設定の順序により両方の列車が進むことができなくなる場合があるからである．例えば列車1が1RT→2RTの進路を設定し，列車2が11RT→1RTの進路を設定した場合，列車2の進路を先に設定する(11Lの信号てこを反位にする)と21の転てつ器が反位に鎖錠される．この時列車1が1RTにいるため信号11Lは進行信号にならず，列車2は進むことはできずに，お互い進むことができなくなる．これを解消するにはこの状態になった時，列車2の進路設定を取り消し(11Lの信号てこを定位にする)，列車1の進路設定(1Rの信号てこを反位にする)を優先させるようにoperatorをモデル化する必要ある．検証方法1では列車2が11Lの信号を進行信号にするようoperatorに要求しても列車が1RTにいるため進行信号にできない．その場合もう一方の列車1の要求を処理するようにモデル化してあるので列車1が進みその後1RTに列車がいないことを確認して列車2が1RTに到達する．同様のことが(1RT→11RT,11RT→3LT)，(11RT→1RT,3LT→11RT)，(3LT→11RT,上り2T→3LT)の組み合わせで起こる．

4.3.2 衝突可能性の検証について

どちらの検証方法でも衝突する可能性はないという結果を得られた．状態数，メモリ使用量共に検証方法2よりも1のほうが小さくなっている．

5. 今後の課題

本論文では，モデル検査器SPINを用いた鉄道信号システムの検証手法を提案し，その検証結果を報告した．抽象度の異なる二つのモデル化手法を用いて**Fig. 1**で示される駅の信号システムをモデル化し，列車の到達可能性と衝突可能性についての検証を行った．抽象度の低いモデル化を行っている検証方式2に比べ，抽象度の高い検証方式1の方が，必ずしも探索空間が狭いわけではない，という結果が得られている．この原因を探る必要がある．

我々の目標は実用規模の駅のシステムの安全性を検証することであるが，現状ではまだ多くの課題が残っている．その主なものをここで挙げる．

- モデル化が正しいかどうかの検証．リレー回路の記述が間違っているとその検証で得られるものに意味はなくなる．モデル化の正しさをどのように証明するかは重要な問題である．
- 効率の良いモデル化を考える．どう記述するのが状態数が少ないのか，効率が良いのかを考える必要性がある．

今回の検証では，最も大規模な検証でも必要メモリ量は50メガバイト程度であった．最近は数ギガバイトのメモリを搭載したPC(Personal Computer)も珍しくはなくなってきている．このようなPCでどの程度の規模の駅までの検証ができるかどうかの実験も今後行う必要がある．

謝　辞

本研究の一部は，日本学術振興会科学研究費補助金・基盤研究(A)(2)(課題番号：15200002) の補助を受けた．

参考文献

1) Edmund M. Clarke, Jr., Orna Grumberg, and Doron A. Peled. *Model Checking*, The MIT Press, 1999.
2) Gerard J. Holzmann. "The Model Checker SPIN", *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING*, Vol.23, No.5, pp.279-295, 1997.
3) Gerard J. Holtzmann. *The SPIN Model Checker - Primer and Reference Manual*, Addison-Wesley, 2003.
4) Michael Huth and Mark Ryan. *Logic in Computer Science -Modelling and Reasoning about Systems*, Second Edition, Cambridge, 2004.
5) 亀山幸義，中島一「ケーススタディ：モデル検査と定理証明を用いた鉄道信号制御システムの検証」，シンポジウム「システム検証の科学技術」予稿集，独立行政法人 産業技術総合研究所，pp.82-91，2004.
6) 川村正「モデル検査法を用いた鉄道信号システムの連動仕様検証」，信学技法FTS98-128，pp.39-46，1999.
7) 「信号入門」，社団法人 日本鉄道電気技術協会，1988.
8) 「連動装置 [改訂版]」，社団法人 日本鉄道電気技術協会，2002.