

単線自動閉そく装置の B メソッドによるモデル化と検証

寺田 夏樹 ((財) 鉄道総合技術研究所)

Modelling and verification with B-method for automatic block system for single lines

Natsuki Terada (Railway Technical Research Institute)

Formal methods are expected to increase reliability of software. We report application of B-method to semi-automatic and automatic block system for single line. In B-method, verification with theorem proving is available and codes are generated from the specification. We not only used B-method, but also used VDM, in which it is easier to describe specification. We also report how to combine VDM and B..

キーワード: フォーマルメソッド, VDM, B メソッド, 単線自動閉そく, 自動閉そく(特殊), 特殊自動閉そく, 証明 (formal methods, VDM, B method, automatic block system for single lines, semi-automatic block system, theorem proving)

1. はじめに

鉄道信号向け装置のソフトウェアの安全性向上策として我々は以前からフォーマルメソッド (formal methods, 形式的手法) によるソフトウェアの高信頼化手法に関心をもち、いくつかの検討結果について報告している⁽¹⁾⁽²⁾。しかし、さらなるフォーマルメソッドの鉄道信号への適用を目指すには、様々な信号システムについてフォーマルメソッドを用いたモデル化を行い、例示すべきと考えている。その際にはモデルの検証も実施された形で提供できるのが望ましい。この方針に基づき、鉄道の単線区間の運転方向を制御する単線自動閉そく装置および特殊自動閉そく装置 (軌道回路検知式) について VDM⁽³⁾ によりモデル化の検討を行い、B メソッド⁽⁴⁾ を用いて定理証明による検証を実施したので報告する。VDM も B もフォーマルメソッドの 1 手法であるが、記述の行いやすい VDM と証明機能の強力な B を組み合わせることでそれぞれの長所を生かすことを狙った。本報告では両手法の違いとその組み合わせ方についても述べる。

2. フォーマルメソッドについて

〈2・1〉 フォーマルメソッドとは フォーマルメソッドと呼ばれるものにも様々な定義があるが、基本的には数学的論理学的体系を持った仕様記述言語を用いて形式的に (言い換えると数学的に) 仕様を記述し、検証を行うことによりシステムの品質を上げるための技術の総称である。

形式的に仕様を記述することにより、仕様のあいまいさを排除できる。また形式的に仕様を記述することで、自動テストや自動証明などといった様々な形でコンピュータの

支援により仕様の検証を行うことが可能となる。早期段階での仕様の検証を十分に行うことにより信頼性やソフトウェアの生産性をあげる (下流工程からの手戻りを少なくする) のがフォーマルメソッドの狙いである。

フォーマルメソッドの草分けである Z や VDM は仕様の記述に重点を置いたモデル指向型手法として分類される。VDM や Z から派生した B メソッドなどでは仕様記述からプログラムを自動生成することが可能となっている。一方、SPIN⁽⁵⁾ や SMV など代表されるモデル検査法が最近注目されている。これらは対象を状態遷移システムとして記述し、その性質を検証するものである。変数が増えると状態爆発問題により検証不可能になるし、たとえ検証に成功してもそれがプログラムになるわけではないが、仕様段階での誤り発見に有効とされ、様々な成果が報告されている。

〈2・2〉 VDM および B メソッド 本報告では検証に B メソッドを使用した。これは仕様記述を証明により検証できること、仕様記述が最終的にプログラムにまで変換されることを重視したためである。B メソッドとは J.R.Abrial が開発した開発手法である。最初に抽象機械 (abstract machine) として仕様を記述し、その仕様が矛盾のないことを証明する。以後、元の仕様を詳細化した仕様を記述する。ここでいう詳細化とは演算結果をより決定的に、演算の前提条件をより広範囲に記述するということである。詳細化仕様は自身に矛盾がないだけでなく前の段階の仕様を満たすことを証明する必要がある。詳細化を繰り返し最終的にはプログラムに直接変換可能な形 (実装仕様) となり、これにより仕様を満たすことが証明によって保証されたプログラムが作成できる。パリの地下鉄等⁽⁶⁾ で実績がある。

ただし、B メソッドは仕様の証明を重視するあまり記述上の制約が大きいという点、日本語対応でない。そこで仕様記述には日本語対応で、別の手法である VDM を併用した。VDM も B と同じモデル指向型手法に分類されるが歴史は VDM の方が古い。仕様を記述し、その記述を実行することでその問題点を洗い出すラピッドプロトタイピングのサポートがその主眼となっている。証明機能は現時点では提供されていないが、仕様に矛盾がないことを示すために証明すべき責務（証明責務）は生成される。これをチェック項目として活用することも可能である。現在 VDM には ISO 標準化された VDM-SL とこれをオブジェクト指向化した VDM++があるが、今回は VDM++を使用した。

3. 単線自動閉そく装置のモデル化と検証

〈3・1〉 単線自動閉そく装置 単線区間の閉そく方式にはいくつかの種別がある。

- (1)自動閉そく式
- (2)自動閉そく式（特殊）
- (3)特殊自動閉そく式（軌道回路検知式）
- (4)特殊自動閉そく式（電子符号照査式）（通称電子閉そく）
- (5)タブレット閉そく式
- (6)スタフ閉そく式

このうち(1),(2)の自動閉そく式では駅間に軌道回路が設備されており、列車が駅間に在線している間は軌道回路が落下し、それにより駅間の運転方向が変わらないような仕組みになっている。(1)では1駅間複数閉そくであり、商用軌道回路等による3位の現示や駅間の複数列車の走行が可能となっている。(2)では駅間1閉そくであり、軌道回路は列車の検知のみの役割となっている。一方、(3),(4)の特殊自動閉そく式では駅間に軌道回路が設備されていない。その代わりに、(3)では区間の両端に列車の進入進出検知のための軌道回路により、(4)では駅に設置した地上装置および車上の車載器間の伝送により、駅間での列車の存在を認識し、運転方向が変わらないようにする仕組みとなっている。

このうち、共通して方向回線と呼ばれる回線を使用している(1)~(3)の装置を対象にモデル化を実施した。これらの装置は表1に示すようなリレーにより実現されているが、実際には閉そく装置として単独に存在するわけではなく、

表 1 閉そく装置に実装されるリレー

略称	リレー名称	備考
LYR	左方向てこ反応リレー	L 方向発駅に設備
RYR	右方向てこ反応リレー	R 方向発駅に設備
LFR	左方向運転方向てこ反応リレー	RYR と対
RFR	右方向運転方向てこ反応リレー	LYR と対
FLR*	運転方向鎖錠リレー	FR を保持する
FR*	運転方向リレー	三位
FCR*	運転方向てこ保持リレー	到着側の LFR,RFR を保持
FKR*	運転方向表示リレー	

駅にある連動装置の一部として実装されている。ここではすでに実績のあるこれらの結線図を検証するのではなく、閉そく機能だけを取り出して装置化した場合に安全性が検証できるかどうかという視点でモデル化を行った。そのためリレーに対して1対1で変数に対応させるのではなく、リレーが実現している機能に着目してモデル化を行った。

閉そく機能の中心となるのは方向回線と運転方向てこである。CTC(中央制御装置)化した場合やARC(自動進路制御)を用いる場合は詳細において若干異なるが、機能としては(1)~(3)ともほぼ共通で以下のとおりとなっている。

- ・両駅の間でこを一致させることにより方向回線が構成される（取扱上は着駅側から取り扱う）。方向回線は到着側から電源が印加される。
- ・一度方向回線が構成されると到着側の方向てこを扱っても運転方向は変わらない。
- ・出発側の方向てこについては、出発進路の設定、出発進路の進路鎖錠の成立、駅間の在線等により鎖錠される。この間に方向てこを扱っても運転方向は変わらない。

今回は、両駅が列車を送出する条件にならないこと、着駅でのてこ操作が無効になる等の検証を行うこととした。

〈3・2〉 自動閉そく式（特殊）の VDM モデル化 まず3方式の中で最も単純な自動閉そく（特殊）についてモデル化を行った。まずモデルを方向回線と駅装置の2つに分割した。駅装置については、それぞれに運転方向リレーに相当する変数「運転方向」と、運転方向鎖錠リレーに相当する変数「運転方向鎖錠」、方向てこに相当する「方向てこ」などを記述した。起点方駅装置および終点方駅装置はそのリレー名称で共通なものが多いため駅装置クラスを作成して、その継承として終点方駅装置クラスを記述した。駅装置クラスを図1に示す。

```

class 駅装置
types
  public てこ型 = <設定> | <未設定>; --<設定>=反位
  public 鎖錠型 = <鎖錠> | <解錠>;
instance variables
  public 位置 : 方向回線`位置型;
  public 進路てこ : てこ型;
  public 進路鎖錠 : 鎖錠型;
  public 方向てこ : 方向回線`方向型;
  public 運転方向 : 方向回線`方向型;
  public 運転方向鎖錠 : 鎖錠型;
  public 反対側方向 : 方向回線`方向型;
  public 方向回線在線 : 方向回線`在線型;
  inv .... (不変条件)
end 駅装置

```

図 1 駅装置の VDM モデル

方向回線は3本の回線で構成される2対の回線である。1対は方向てこを制御するための回線、もう1対は軌道回路の条件を照査してFKRを動作させるための回線である。方向回線の状態は両駅のてこの状態と軌道回路の状態で記述

できる。これらを踏まえた方向回線のモデルを図 2 に示す

```
class 方向回線
types
  public 在線型 = <在線> | <非在線>;
  public 方向型 = <下り> | <上り>;
  public 位置型 = <起点方> | <終点方>
instance variables
  public 方向 : map 位置型 to 方向型;
  public 在線 : 在線型;
inv dom 方向 = {<起点方>, <終点方>} and
  not (方向(<起点方>) = <下り> and
    方向(<終点方>) = <上り>);
end 方向回線
```

図 2 方向回線の VDM モデル

〈3・3〉 自動閉そく式（特殊）の B モデル化 VDM での記述を B で書き直す。現在 B メソッドでは日本語がサポートされていないが、コード化を意識した場合 ASCII 文字で記述することは避けられないため、VDM で概念を整理できれば大きな問題ではないと考える。

VDM++ と B とでは構造化の仕組みに違いがあるが、VDM++ の各クラスを 1 つの抽象機械として対応させればシステムの構造を大きく変える必要はない。しかしながら、VDM では逐次演算が記述できるのに対し、B の抽象機械では逐次演算を記述できない、一方 B では演算の事後条件を直接表現できないなど細かいところではさまざまな表現の違いが存在する。このことを考えると VDM での記述の時点なるべく逐次演算を使用せずに事前事後の状態変数の条件を記述するようにする。一方、B では非決定的選択の表現を用いて VDM の事後条件を記述する。これは有る制約を満たす変数を用いて記述するということである。

その他にも VDM の関数に相当するものが B では提供されず、演算で記述するか、マクロとして記述する必要があるなど、モジュール内の記述には制約が多いので注意が必要である。

B での表現の例を図 3 に示す。

```
xx <- DownSet =
  ANY dir WHERE
    dir : DIRECTION &
    ((direction = up & directlock = unlock)
      => dir = down) &
    ((direction = down or directlock = lock)
      => dir = direction) &
    transition(direction, directlock, oppositedirect,
      dir, directlock, oppositedirect)
THEN
  Set(routelever, routelock, down, dir, directlock,
    oppositedirect, existence) ||
  xx := dir
END;
```

図 3 B モデルの例

〈3・4〉 B モデルの詳細化と証明 詳細化段階では、より詳細化した演算を記述する。詳細化段階においては演算結果が詳細化前の段階の条件を満たすように演算を記述することが求められる。ここで前の段階に遷移条件や不変条

B の実装段階では逐次代入が可能であり、詳細化として逐次代入による演算を記述し、その演算結果が常に抽象機械の演算を満たすことを証明することとなる。

必要な証明責務の大部分は自動的に証明される。残りはツールを使って対話的に証明を行う必要がある。今回記述した不変条件と状態遷移に関してはそれを満たしたまま実行できることを確認した。証明の数を表 2 に示す。これは抽象機械での証明から実装段階の証明までを含んだものである。合わせて抽象機械での B の記述行数を示した。今回はおよそ 8 割の証明責務が自動的に証明されたことになる。

表 2 証明の数（自動閉そく式（特殊））

モジュール	行数(B)	証明責務	自動証明	対話的証明
起点方駅装置	209	99	85	14
終点方駅装置	209	99	85	14
方向回線	60	21	17	4
全体システム	207	243	195	48
計		462	382	80

〈3・5〉 単線自動閉そく式のモデル化と証明

続いて単線自動閉そく式のモデル化を行った。単線自動閉そく式の場合、駅中間に閉そくが複数あり、軌道回路に現示情報の伝送を担わせるため、運転方向により軌道回路の送電方向が変わったり、列車の在線状況により送電の極性が変わったりする。標準結線図^⑧では下り用の送受信器と上り用の送受信器が設備され、方向回線が下りに設定されれば下り用の送受信器が使用され、上に設定すれば上り用の送受信器が使用される。方向回線は設定された方向の軌道回路のいずれかが落下すると鎖錠される。

方向回線に関するモデルについては〈3.2〉節と大きな違いがない。一方、軌道回路に関して現示の制御部分を含めるとモデルが複雑となる。そこで軌道回路部分を別のクラスとして表現した。証明を行った結果を表 3 に示す。軌道回路モデルが複雑となった結果、全体としても複雑となり、全体システムの証明の数が大幅に増えているのが分かる。

駅装置や方向回線も数が増えているが、これは鎖錠の条件となる軌道回路が複数となったことによる。

表 3 証明の数（単線自動閉そく式）

モジュール	行数(B)	証明責務	自動証明	対話的証明
起点方駅装置	217	183	159	24
終点方駅装置	217	157	133	24
方向回線	69	48	42	6
軌道回路（駅間）	118	471	257	214
全体システム	333	9160	8435	725
計		10019	9026	993

〈3・6〉 特殊自動閉そく式のモデル化と検証 最後に特殊自動閉そく式(軌道回路検知式)のモデル化である。この方式では駅間に軌道回路が設備されない。その代わり駅間に列車が出入りすることを検出するCTとOTと呼ばれる2つの短小軌道回路を両駅に設ける。その上で列車が駅間に在線している場合に方向回線を鎖錠するための方向鎖錠保持リレー(FSR)を設け、出発側のCT進入時から到着側のCT通過時まで方向鎖錠を保持させるようにしている。FSRの挙動は構内の軌道回路の落下・動作の順序に大きく依存しており、この点が前2つのシステムと大きく違う所である。また方向回線は2本で構成されており列車の到着については到着側から送出する電源を一時的に転極することで出発側に伝達する仕組みである。さらに列車が退行することを考慮し、列車が停車場内に残った状態から退行後に扱う退行解錠ボタンや停車場外に進出した後に退行するために扱う場内代用てこが設備され、取扱いの手順も決められている。また出発信号が出ていないのにも関わらず列車が出発しようとするのを検出する誤出発検知リレーも設備される。つまり駅間に列車が在線していないことを保証するために駅構内のリレーの数は格段に増えている。

モデル化では両駅のOT、CTや駅構内のホームトラックと、進路上の軌道回路を記述した。また、実際には様々なリレーの状態によって表現される列車位置を記号で表現することとした。VDMの記述では以下のとおりとなる。

列車位置型 = <なし> | <ホーム> | <進路内> | <CT> | <OTCT> | <OT> | <駅間> | <接近> | <到着>

なお、線路閉鎖はモデルから除外し、場内代用てこや退行解錠ボタン、誤出発検知リレーはモデルに含めた。

各列車位置において各軌道回路が落下・動作した場合に、装置が新たな列車位置をどう認識するかを結線図を元に網羅的に調べた。この中には装置として想定していない動作も含まれるが、無定義にはできないため筆者の判断で列車位置を割り当てることとした。この割り当てについては議論を行うことにより多くの人にとってより妥当なものとなると考えている。その割り当てを元に仕様記述を行った。

その結果例えば軌道落下・動作に対応する演算に関しては、列車位置やその時の軌道回路の状態によって場合分けをすることとなり、複雑となった。駅装置の記述の仕方を工夫して、起点方・終点方を共通のモジュールで記述できるようにしたが、それでも単線自動閉そくでは起点・終点それぞれ217行であるのに対し、特殊自動閉そく式では604

表4 証明の数(特殊自動閉そく式)

モジュール	行数(B)	証明責務	自動証明	対話的証明
駅装置(起点・終点計)	604	11370	9763	1607
方向回線	103	112	85	27
全体システム	342	25989	25482	507
計		37471	35330	2141

行となっており記述が増えていることが分かる。

証明の結果は表4のとおりである。駅装置や全体システムで証明の数が非常に多くなっている。これは駅構内の軌道回路の状態による条件分岐が多くなったためであると考えられる。条件分岐を使用すると、分岐した後の状態に対してそれぞれ不変条件等が満たされることを証明する必要がある。その結果1つ条件分岐することで証明の数がほぼ倍となってしまう。実際には似たような証明が多いため、証明の数だけ負担が増えたとは必ずしも言えないが、証明に要する時間は証明の数に応じて増えていくため、さらに証明を減らす工夫が必要と考えられる。

例えば証明の数を減らすためには軌道回路の状態と列車位置に記述を検討し直し、根本的に記述を分かりやすく記述する工夫を検討することも必要であると考えられる。この検討し直しが記述の明確さにつながり、より適切なモデル化の例示となるものと考えられる。

4. まとめ

フォーマルメソッドによる単線自動閉そく装置の検証を行った。まずVDM++でモデル化し、Bメソッドを使用して証明をしつつコード化した。記述した性質が満たされることについては証明機能により証明することができた。Bでは記述が制約が多いため、VDMをまず用いてこれにより記述時に考えを整理したが、これはBを直接使うよりも有効であると考えられる。

なお、単線自動閉そくと特殊自動閉そくを比較すると特殊自動閉そくの方が軌道回路の動作・落下の順番による挙動の変化がより大きく、より順序回路的になることからモデル化や証明の手間が大きくなった。特殊自動閉そく式のモデルについてはとりあえず証明はできたものの記述が複雑であり、モデル化の例示としてはまだ十分とは言えない。記述と考えとが一致しているかの妥当性にも欠けるため、特殊自動閉そく式のモデル化についてはさらに検討を進めたいと考えている。

文 献

- (1) 寺田, 福田: 「デジタル ATC データベースの証明による検証」, 信学技報, Vol. 101, No. 505, FTS2001-73, (2001)
- (2) 寺田, 高橋, 荻野, 「段階的詳細化に基づくシステムの高信頼化技法」, 信学技報, Vol.97, No.98, DC2005-65, (2005)
- (3) J. Fitzgerald, P. G. Larsen: "Modelling Systems -- Practical Tools and Techniques in Software Development," Cambridge University Press, (1998)
- (4) Abrial J-R: "The B-Book: Assigning programs to meanings," Cambridge University Press (1998).
- (5) G. J. Holzmann: The SPIN Model Checker, Addison-Wesley(2004)
- (6) A. Faivre, P. Benoit: "Safety critical software of meteor developed with the B formal method and vital coded processor," Proceeding of WCRR99, Tokyo (1999)
- (7) 「閉そく装置」, 鉄道技術者のための電気概論, 日本鉄道電気技術協会, (1993)
- (8) 「継電連動装置標準結線図」, 日本鉄道電気技術協会 (1987)
- (9) 「継電連動装置(CTC 関連及び ARC)標準結線図」, 日本鉄道電気技術協会 (2000)