信号保安装置への定理証明技術の適用に関する研究

寺田, 夏樹

https://doi.org/10.15017/1543999

（別紙様式 2）

氏　　名　：寺田　夏樹

論 文 名　：信号保安装置への定理証明技術の適用に関する研究

区　　分　：甲

論　文　内　容　の　要　旨

鉄道の安全運行を支えているのが信号保安装置と呼ばれるものである．信号保安装置の機能としては，駅間において列車を正面衝突させない，あるいは追突させない．また駅構内において列車を正面衝突あるいは側面衝突させないなどといったものがある．

この信号保安装置には高い安全性が求められる．従来はリレーを用いていた．リレーには故障時の状態が一方に固定されるという非対称な故障特性があり，これを活用していた．これを電子化機器で実現しようとする際に，そのままでは非対称的な故障特性が得られないということが問題となった．そこで装置を多重化し，その不一致を検出した場合に装置を安全側に止めるという技術が実現した．その後，電子化機器のハードウェアに関して様々な課題はあったが，安全性を確保するという視点では技術的にはかなり確立されたものと考えられている．

しかし，信号保安装置に搭載されるソフトウェアについてはそれほど特別な技術は使われていない．基本的にはプログラムを誤らないように単純化するという考え方に基づいている．プログラム実行が異常となったことを検出する仕組みは備わっているものの，プログラムの正当性を確保する手段は依然としてレビューやテストによる所が大きい．

これに対し，本論文においてフォーマルメソッドによるソフトウェアの高信頼化手法の適用を試みた．フォーマルメソッドとは仕様の形式化を通じてプログラムやシステムの信頼性を向上化させるための技術である．そのうち，仕様から生成される条件を定理証明により仕様の誤りを見つけたり，仕様に誤りのないことを保証したりする厳密な検証に着目し，適用を試みた．信号保安装置の中でなるべく広い範囲をカバーするため，以下の３つの事例を選択し，検証の適用を試みた．

・静的な制御データの検証
・ブール型変数で記述可能な（リレーで構築可能な）動的な制御部分の検証
・ブール型変数では対応できない，数値計算部分の検証

その前に形式手法を用いたシステムのモデル化の習熟が必要であり，まずは VDM（Vienna Development Method）による連動装置のアニメーションを活用したモデル化を実施した．

静的な制御データの検証に関しては、ATC（自動列車制御装置）の制御データの基礎となる線区データベース（地理データ）に関して，VDM-SL で記述されたデータベース仕様から生成される証明責務の証明を行った．証明は the HOL system をバックエンドの証明エンジンとして利用する GUI を通じて行った．935 行の仕様に対し，188 の証明責務が生成され，これらの 9 割を自動，残りの 1 割を対話的に証明した．この検証を通じて、様々な知見を得た．

１つ目の知見として，証明責務をながめ，反例を探してインタプリタで確かめることで仕様の誤りを発見可能であるということが挙げられる．証明責務の自動生成は仕様の誤りを発見する上で重

要であり，自動証明ができなくとも，反例を確かめる手法で仕様の品質向上が可能と考えられる．

２つ目の知見として，自動証明ができれば，記述の誤りを見逃さずにすむ可能性がより高まり，仕様の品質をさらに向上させることが可能となるということが挙げられる．

また，証明を成功させるためには証明のテクニックを身につけることも必要ではあるものの，それ以上に仕様の理解も重要であることが挙げられる．そのためには仕様をわかりやすくする努力も必要であり，単純かつしっかりとした構造を構築する必要がある．

動的な制御部分の検証事例として，リレーで実装がなされている単線区間向け自動閉そく装置の検証に B メソッドを適用した．VDM でモデル化を行った上で，B メソッドの記述に直し，証明責務を生成して，証明を実施し，信号保安装置のうち，動的なシステムが検証可能であることを示した．また，3 種類の装置の検証を比較し，証明責務の生成状況の観察を行った。証明責務の生成に関しては，不変条件内や非決定的での論理和の使用，条件分岐等を用いることにより証明責務の生成数が増大することが分かった．また，同じことを別の表現で記述してしまうと自動証明できない証明責務が増大することが分かった．

これらの問題に対して，論理和の除去により証明責務を減らしたり，表明の使用により，証明責務の自動証明率を上げたりできることを示した．

数値計算部分の検証事例として，前述の ATC において，停止位置までの距離が与えられた場合の，車両に対する許容速度の計算部分に B メソッドを適用した．この計算には本来であれば平方根が必要で，浮動小数点計算であれば容易であるが，B メソッドは小数を扱わない．しかしながら，整数の範囲で必要とする精度の計算を行い，それを証明によって正当性を与えることができた．この検証を通じて，while ループの使用や乗除算の使用により証明責務が増大することが分かった．

また，この検証で使用した補助的な関数については，抽象変数と operation の組み合わせを定義し，それを詳細化する事で実装を行ったが，この手法は他の事例でも活用できる．

制御データの静的な検証，動的な制御部分の検証，論理演算で対応できない数値計算部分について定理証明技術が適用できた．これは信号保安装置の広い分野を網羅する代表例であり，証明の手間を別とすれば，この技術が信号保安装置に一般的に応用可能であることが示された．

この技法が広く導入されるにはまだまだ時間がかかるとは考えられるが，制御データ検証への適用の可能性や, 新しい装置への導入の可能性がある. 既存システムの参照モデルの作成と合わせて，信号保安装置の品質向上に資する事ができればよいと考えている．