信号通信情報

信号設備の安全性に関する仕様検証手法の適用検討

寺田夏樹　遠山喬

フォーマルメソッドを用いて信号装置の仕様を数学的に検証する手法について，単線区間向けの閉そく装置を例として行った。具体的には

・一旦方向回線が設定されると，着駅で方向てこを扱っても設定が保持される。

・両駅での方向回線の設定が同時に列車を出発させる条件にならない。

といった閉そく装置の安全要件が常に満たされるかどうかということを検証した。

本報告では2つの手法で検証した。1つめはBメソッドと呼ばれる手法であり，仕様が問題ないことを保証するために必要な項目が自動的に生成されるので，これをコンピュータ支援によって証明するものである。もう1つはSMTソルバと呼ばれる手法で，条件を満たす変数の値の組み合わせを探索し，問題がある変数値がないことを通じて仕様に問題がないことを検証するものである。

表　2つの検証手法の比較

	Bメソッド	SMTソルバ (Satisfiability Modulo Theories)
検証手段	定理証明 (公理からの推論)	充足解の探索
例題の検証時間	数日～数週間	数秒
変数の数	多くても数百程度（1つのモジュールでは数十程度）	最大 10^6 以上
自然数や集合の扱い	対応可能	可能だが，探索時間が急激に増える
プログラムの生成	機能あり	機能なし