物理情報システムに対するブラックボックス検査の構文的仕様強化による最適化

四十坊純也[1], 和賀正樹[2], 末永幸平[2]
[1] 京都大学工学部情報学科　[2] 京都大学大学院情報学研究科通信情報システム専攻

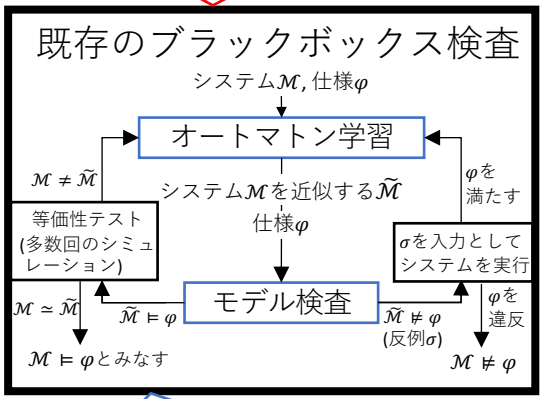
背景

物理情報システムは安全性が重要

- 物理的な特性が重要であるため網羅的な形式検証は難しい
- テスト手法の一つがブラックボックス検査

実行時間の長さが課題

既存のブラックボックス検査



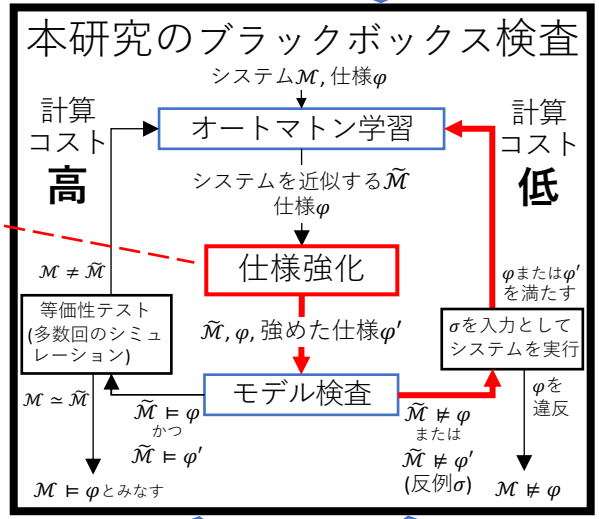
左のループはシステムとオートマトンの等価性テストにおいて、システムのシミュレーションを(多)数回実行するので時間がかかる

アイデア

仕様を書き換えて**強める**ことで右側のループを通りやすくする

仕様φ'が仕様φを強めた仕様であるとは、任意のオートマトン$\widetilde{\mathcal{M}}$に対して
$\widetilde{\mathcal{M}} \models \varphi' \Rightarrow \widetilde{\mathcal{M}} \models \varphi$
が成立するということ

本研究のブラックボックス検査



仕様強化の書き換え規則

記号↦は左側の式を右側の式に書き換える規則を表す

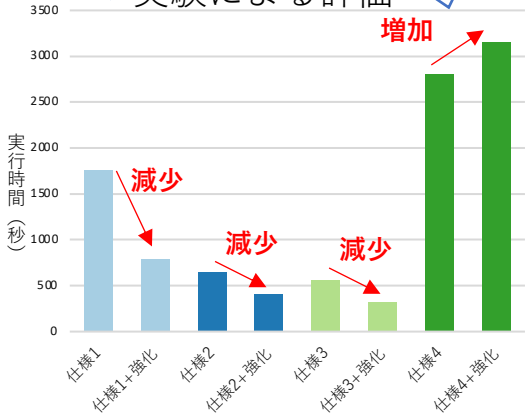
$$\varphi \vee \psi \mapsto \varphi \wedge \psi$$
$$\varphi \,\mathcal{U}\, \psi \mapsto \Box\varphi \wedge \Box \Diamond \psi$$
$$\Diamond\varphi \mapsto \Box \Diamond \varphi$$
$$\Box \Diamond \varphi \mapsto \Diamond \Box \varphi$$
$$\Diamond \Box \varphi \mapsto \Box\varphi$$

一般には、強めた仕様に対して得られる反例は元の仕様に対する反例ではない。しかし、仕様の性質を保つような強め方をすることで、得られた反例を元に行われるオートマトン学習が元の仕様の検査において有用であることが期待できる。

実験を行った多くの仕様では最適化に有用な書き換えが存在
⇨実行時間が減少

仕様の意味を強めすぎてしまうような書き換えしかない場合
⇨実行時間が増加

実験による評価



仕様 1	$\Box_{[0,26]}(v < 100) \vee \Box_{[28,28]}(v > 75)$
仕様 1 強化	$\Box_{[0,26]}(v < 100) \wedge \Box_{[28,28]}(v > 75)$
仕様 2	$\Box((g > 2) \vee ((g < 2)\ \mathcal{U}\ (v > 30)))$
仕様 2 強化	$\Box((g > 2) \vee (\Box(g < 2) \wedge \Box(\Diamond(v > 30))))$
仕様 3	$\Box((\Box_{[0,3]}(\omega > 4000)) \rightarrow (\Diamond_{[0,3]}(v > 100)))$
仕様 3 強化	$\Box((\Box_{[0,3]}(\omega > 4000)) \rightarrow (\Box_{[0,3]}(v > 100)))$
仕様 4	$\Box((g > 3) \vee (\omega < 4775) \vee \Diamond_{[0,2]}(g > 3))$
仕様 4 強化	$\Box((g > 3) \vee (\omega < 4775) \wedge \Diamond_{[0,2]}(g > 3))$