Efficient Black-Box Checking with Specification-Guided Abstraction

松本 翼[1], 渡邉 知樹[2], 末永 幸平[1], 和賀 正樹[1]

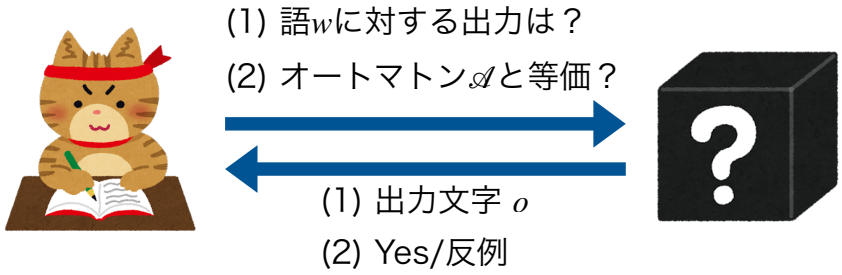
[1] 京都大学, [2] 総合研究大学院大学/国立情報学研究所

目的

ブラックボックスシステムを効率的にテストする

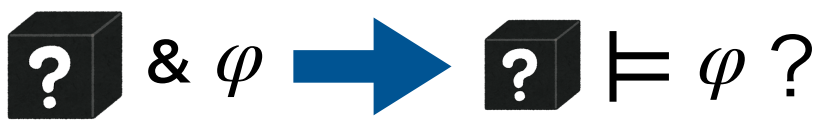
能動的オートマトン学習 [Angluin '87]

ブラックボックスなオートマトンを対話的に学習



ブラックボックス検査 [Peled et al. '99]

ブラックボックスシステムにおいて仕様に反する入力を探索



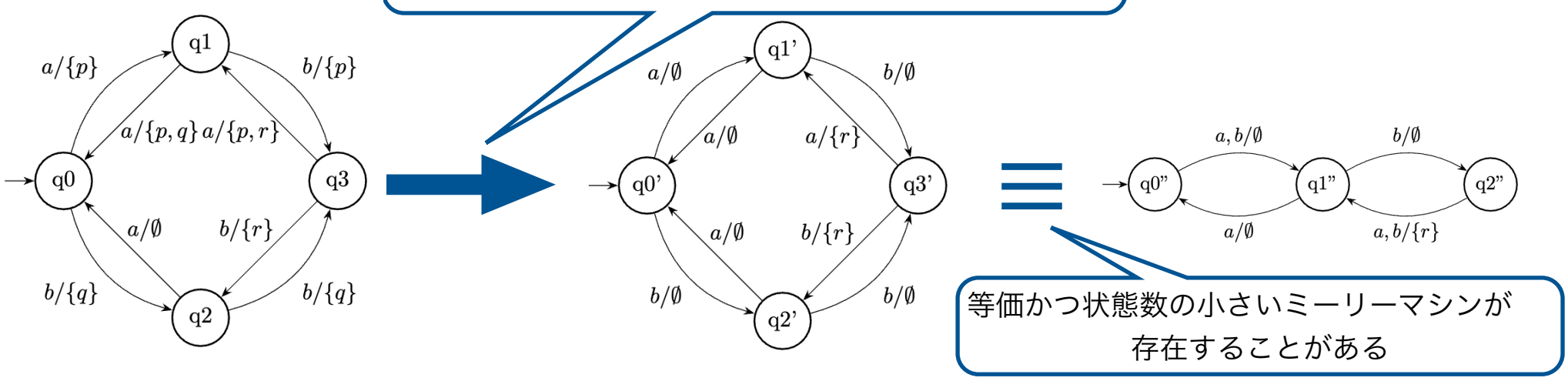
オートマトン学習とモデル検査を用いる

課題：システムの状態数が大きいと時間がかかる

アプローチ：仕様の充足/非充足を保存するミーリーマシンの抽象化を定義

例：仕様 $\varphi = F(r)$

仕様の充足/非充足が保存されるように出力を変換
(rが含まれているかだけを考慮すれば良い)



等価かつ状態数の小さいミーリーマシンが存在することがある

Disjunct-Sensitive Abstraction

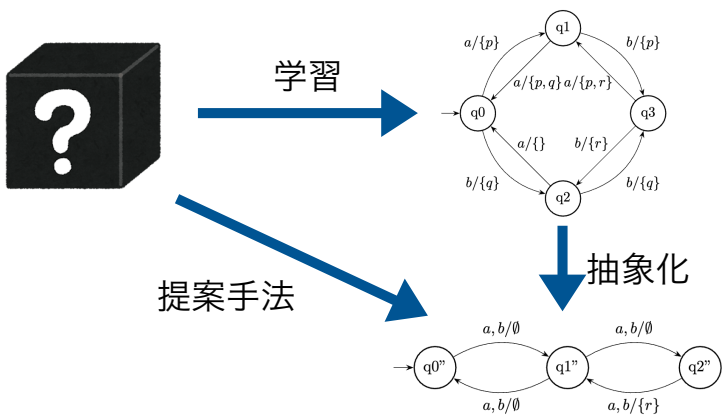
ブラックボックス検査では∨の全オペランドをfalsifyする必要
→ ∨ のオペランドに関する情報が有用

例：$\varphi = G(p \vee q)$ の時

通常の抽象化では $\{p\}, \{q\}, \{p,q\}$ は区別されないが、
disjunct-sensitive abstractionでは互いに区別

∨のオペランドの充足/非充足を保存

抽象化されたミーリーマシンの直接学習



本研究では出力文字の等価性の拡張によって抽象化

- Nerode congruenceにおける等価性を自然に拡張することで既存の学習アルゴリズムと同様に学習

定理：抽象化の正当性

元のミーリーマシンと抽象化されたミーリーマシンは仕様の充足に関して等価である

実験

自動変速機のシミュレーションモデルと複数の仕様、3つの手法で実験

→抽象化をすると速くなる例/遅くなる例がともに存在
部分的な抽象化では検査時間が改善

検査にかかった平均時間 (単位：秒)

式	抽象化なし	部分的に抽象化	抽象化あり
φ_1	-	-	393.4
φ_2	868.75	887.01	554.44
φ_3	703.86	323.67	1081.3

$\varphi_1 = \{G(g = 1 \implies \omega < r) \mid r \in \{4400,4450,4500,4550\}$
$\varphi_2 = \{G(g = 3 \implies v < 20), G(g = 3 \implies F_{[0,5]}(v < 20))\}$
$\varphi_3 = \{G((v < 105 \wedge g < 3) \vee \omega < 4650)\}$