平成19年度トップエスイー修了制作

プロトコル合成における 合成プロトコルの性質・制約の検証

早稲田大学大学院基幹理工学研究科　髙橋竜一　ryu1-t@nii.ac.jp

開発における問題点

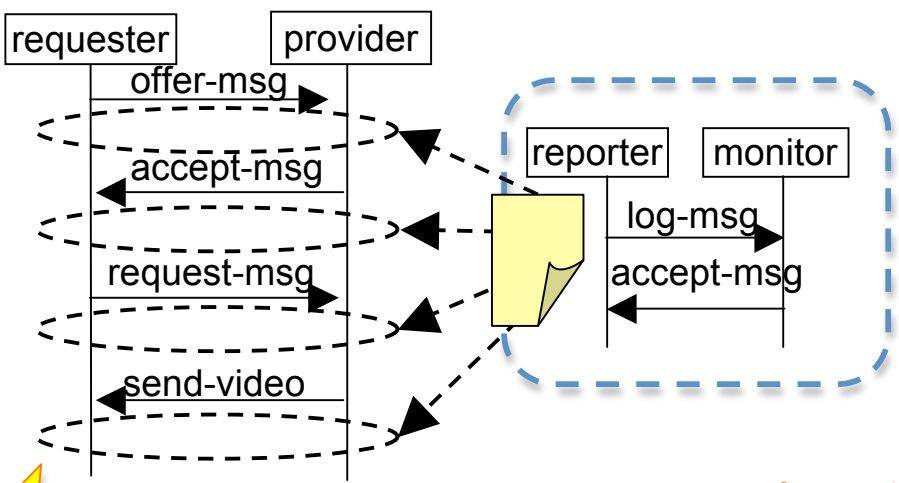
プロトコル合成は協調プロトコルを部品化し，複数の協調プロトコルを合成する事で複雑な協調プロトコル作成する手法である．
合成によって得られた協調プロトコルは目的の性質や制約を保持しているかを検証する必要があるが，手動でチェックするのは非常にコストが高い．

手法・ツールの適用による解決

複雑な協調プロトコルの検証はツールを用いることが望ましい．本課題では合成によって得られた協調プロトコルの記述（WS-CDL）をモデル検証言語（PROMELA）に変換する変換ルールを作成する．変換した記述は検証ツール（SPIN）を用いて網羅的な検証が可能になる．

プロトコル合成とその問題

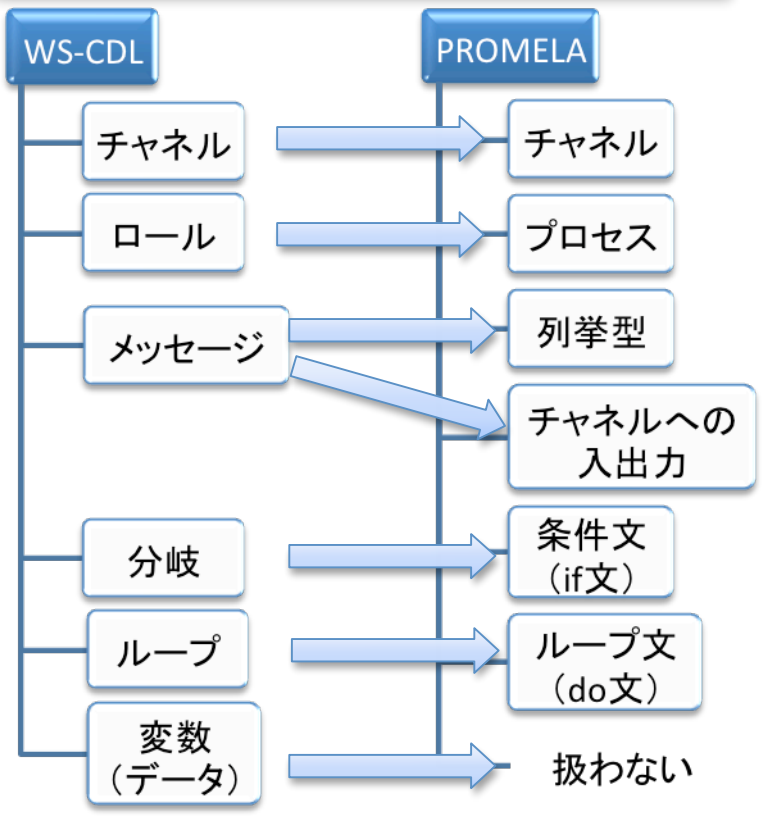
プロトコル合成
部品化した各プロトコルを合成記述の指定によって合成
→ 目的のプロトコルを作成



問題
- 合成記述の指定が間違えている
- 複数の合成間で干渉が起きる

→ 意図しないプロトコルが出来上がる

変換ルール



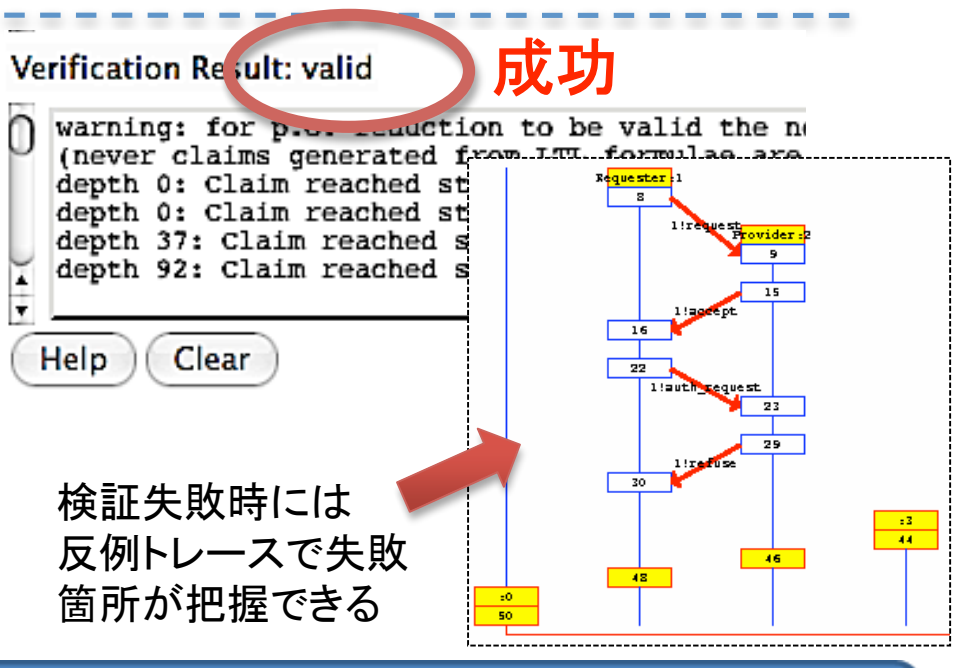
性質・制約の検証

SPINは時相論理を検証する事が可能

→ 協調プロトコルが保持する時間的性質を時相論理で表現，検証が可能になる．

例：　Login処理の後に必ずLogout処理がある．

[](p || q) && []<>p
　p : c_auth_accept == c_logout_accept
　q : c_auth_accept == c_logout_accept+1



検証失敗時には反例トレースで失敗箇所が把握できる

NII 国立情報学研究所 National Institute of Informatics
トップエスイー　～サイエンスによる知的ものづくり教育プログラム～
文部科学省 振興調整費産学融合先端ソフトウェア技術者養成拠点の形成