

Title	匿名性プロトコルのOTS/CafeOBJ法に基づく形式化
Author(s)	程, 剣
Citation	
Issue Date	2008-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/4348
Rights	
Description	Supervisor: 緒方 和博, 情報科学研究科, 修士

匿名性プロトコルのOTS/CafeOBJ法に基づく形式化

程 剣 (610058)

2008年2月7日

匿名性プロトコル, 入出力オートマトン, 観測遷移システム, 匿名性シミュレーション関係, OTS/CafeOBJ 法.

本研究の目的は, 観測遷移システムで匿名性プロトコルをモデル化し, CafeOBJ でその仕様を作成する方法を提案することである. また, 匿名性プロトコルの CafeOBJ 仕様に基づく証明譜による匿名性検証の可能性も探る.

匿名性の考え方は, 投票, 寄付, 内部告発など, 実世界のさまざまな場面に現れている. 現在, 匿名性を形式的に記述しその正しさを計算機を使って検証する研究が行われ始めた. しかし, 分散システムが持つ匿名性を厳密に証明する手法は, まだ確立されていない.

ロンドン大学の Steve Schneider らは, FDR (failures-divergences refinement) を用いた有限状態システムのトレース匿名性のモデル検査器による検証方法を提案している. NTT コミュニケーション科学基礎研究所の河辺らは, 匿名性シミュレーションと呼ばれる関係を用いたトレース匿名性の検証方法を提案している. この検証方法では, 入出力オートマトンでプロトコルをモデル化し, モデルを代数仕様言語 Larch で記述し, 定理証明器 LP を用いてプロトコルがトレース匿名性を満たしていることを証明する.

河辺らの論文によると, 入出力オートマトンは, アクションの集合, 状態集合, 初期集合および遷移の集合から構成されている. アクションには, 入力, 出力, 内部の3種類がある. 入力アクションと出力アクションを, 外部アクションと呼ぶ. 河辺らはトレースを定義し, 混乱の原理 (principle of confusion) に基づく匿名性の考え方を導入した. その考え方では, あるシステムのあるユーザ A が, ある (観測可能な) トレースを引き起し, ほかのユーザも同じトレースを引き起すことができれば, そのシステムは匿名であるというものである. 河辺らの方法は, まず入出力オートマトン X および出力アクションの集合族 A に対し, 入出力オートマトン $anonym_A(X)$ を定義する. $anonym_A(X)$ は定義から A に関してトレースを満たすものである. このため $traces(anonym_A(X)) = traces(X)$ であれば, X は A に関してトレース匿名性を満たすことになる. 河辺らは, I/O-オートマトンのトレース匿名性を示すための手法を導入している. この手法は, 匿名シミュレーションと呼ばれる, 状態集合上の2項関係を用いる. 河辺らは, 匿名シミュレーションの存在がトレース匿名性の十分条件であることを証明することによって, 匿名シミュレーションを用いた証明法が妥当なものであることを示した.

本研究は、入出力オートマトンと観測遷移システムの類似性に着目する。匿名性プロトコルを観測遷移システムとしてモデル化し、CafeOBJ でその仕様を作成する方法を提案する。観測遷移システムは、CafeOBJ で抽象機械を記述するための数学モデルの一つである。観測遷移システムでモデル化されたシステムでは、その任意の状態を包含する状態空間 Y の存在を仮定している。システムの任意の状態は、 Y の要素 v として必ず存在している。システムを構成する興味深い値が遷移によってどのように変化するかを、システムの外部から v を観測することで、システムのモデルが作成される。観測遷移システムは、観測の集合 (O)、初期状態の集合 (I) および 条件付遷移規則の集合 (T) から成る。観測の集合 (O) は、外部から v を観測する関数 o の集合である。初期状態の集合 (I) は、状態空間 Y の部分集合である。遷移規則 $t \in T$ は、効果と効力条件の組で定義する。

入出力オートマトンと観測遷移システムの類似点では、入出力オートマトンの状態の集合は観測遷移システムの状態空間 Y に対応している。入出力オートマトンの初期状態の集合は観測遷移システムの初期状態の集合に対応している。また入出力オートマトンのアクションの集合と遷移の集合は観測遷移システムの条件付遷移規則の集合に対応している。入出力オートマトンと観測遷移システムの相違点では、入出力オートマトンのアクションには外部と内部の区別があり、観測遷移システムの遷移には外部と内部の区別がないことがわかった。このため、観測遷移システムの遷移にも外部と内部の区別を与え、観測遷移システムのトレースを定義する必要がある。また、河辺らの匿名性シミュレーションと呼ばれる関係を用いたトレース匿名性の検証方法を参考にして、匿名性プロトコルの CafeOBJ 仕様に基づく証明譜による匿名性検証の可能性についても考察した。証明譜を用いて CafeOBJ で帰納法の検証を行うには、検証者は、証明譜と呼ばれるコードを記述し、それを処理系に実行させる。証明譜では、適切な場合分けの指示とともに基底と帰納段階の各推論を記述し、各証明節を CafeOBJ システムで実行することで、言明が成り立つことをチェックする。

OTS/CafeOBJ 法では、観測遷移システム (OTS: Observational Transition System) としてシステムやプロトコルの数学モデルを作成する。観測遷移システムは、代数仕様言語 CafeOBJ で記述され、観測遷移システムの CafeOBJ 仕様をもとに、システムやプロトコルが望みの性質を満たすことを検証する。匿名性プロトコルの OTS/CafeOBJ 法による仕様記述では、直感的に理解しやすいものとなっており、その可読性も高いものとなっている。記述した仕様は書き換え規則により自動的に状態遷移が行われる。その状態遷移の変化はシーケンスチャートに自然に対応させることができるため、遷移の様子を把握することは容易である。また、OTS/CafeOBJ 法は、ユニークな特徴 (システムやプロトコルの外部から観測可能な値の変化に着目したモデル化や可読性等に優れた証明譜による検証法など) を持つ。そして、本研究では、河辺らの提案方法を参考にして、OTS/CafeOBJ 法のユニークな特徴を活かした、匿名性プロトコルを観測遷移システムとしてモデル化し、CafeOBJ でその仕様を作成する方法を提案した。また匿名性プロトコルの CafeOBJ 仕様に基づく、証明譜による匿名性検証の可能性があることを確認した。