情報処理学会論文誌　プログラミング　Vol. 3　No. 3　19 (June 2010)

発表概要

確率様相論理による秘匿性の証明

竹内　泉[†1]　真野　健[†2]

情報を秘匿するプロトコルの中には，確率変数によって秘匿性が保証されるものがある．そのようなプロトコルに対して，公理的体系の中で情報の秘匿性を証明することを目的とする．そのための，確率変数を扱うことのできる公理的な論理体系を設計することを目標とする．確率変数によって情報を秘匿するプロトコルにおいても，確率変数ではない変数は存在する．それはプロトコルの開始以前に値の決まっている変数である．このような変数は確率変数ではなく，非決定性過程によって値の定まる変数と見なさなければならない．本発表で提案する論理体系は命題変数と二階量化と確率様相が登場する量化様相命題論理である．そこでは，二階量化によって束縛される命題変数と確率様相によって束縛される命題変数がある．二階量化によって束縛される命題変数は非決定性過程によって値の決まる変数を表す．確率様相によって束縛される命題変数は確率変数である．意味論は可能世界意味論で与え，その意味論に対し健全な公理系を与える．その公理系は完全かどうかは分からない．公理系は完全であることが望ましいが，健全であって必要な定理が証明できる程度に強力なものであれば，完全でなくても有用である．本発表では例題として暗号学者の会食問題を採り上げ，そのプロトコルの情報の秘匿をこの論理体系によって証明する．

A Proof of Secrecy by Probabilistic Modal Logic

Izumi Takeuti[†1] and Ken Mano[†2]

Some protocols with secret information guarantee the secrecy of information by using probabilistic variables. The purpose of this presentation is to prove the secrecy of such protocols in a axiomatic proof system. This presentation aims at proposing such axiomatic proof system which deals with probabilistic variables. A protocol with probabilistic variables also has non-probabilistic variables whose values are decided before the protocol starts. The values of such variables are regarded to be decided in non-deterministic processes. This presentation proposes a proof system of propositional logic which has propositional variables, probabilistic modality and second order quantification. The proof system has two kind of variables; variables bound by second order quantifiers and variables bound by probabilistic modality. Variables bound by second order quantifiers denote non-deterministic processes, and variables bound by probabilistic modality are probabilistic variables. This presentation gives possible world semantics to our proof system, and gives axiomatisation of the proof system which is sound to the semantics. It is not known whether the axiomatisation is complete or not. Although a complete axiomatisation is preferable, a non-complete axiomatisation is also useful if it is so strong that it proves many important theorems. This presentation picks up dining cryptographer protocol as an example, and show how the proof system proves the secrecy for this protocol.

（平成 22 年 1 月 27 日発表）

†1 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)
†2 NTT コミュニケーション科学基礎研究所
NTT Communication Science Laboratories, NTT Corporation