

発表概要

情報の使用法をその発信者が制限できるプロセス計算

伊 藤 徹[†]

インターネットをはじめとする通信システムにおいて、著作権やセキュリティの問題から情報の使用をその発信元が制限できることが望ましい。本研究では、計算に対して、データ(π 計算の用語では、name, 以降、nameと呼ぶ)を送信する際、送信先におけるそのnameの使用に制限を加えられるようにする方法について、2つのアプローチから考察を行った。1つ目のアプローチは、新しいプリミティブを導入するというものである。初めの試みでは、nameに対して送信回数の最大値を指定できる計算系($1-\pi$)を導入する。次の試みでは、2種類のnameを持つ計算系($2-\pi$)を導入する。この計算系には、従来のnameに加え、送信後の使われ方が制限されたnameが存在する。この2つのnameによって、安全性に関して2つのレベルを持つ通信が表現される。2つ目のアプローチは、プロセスを構成する構文を制限するというものである。制限の仕方は3種類考えられ、その3種類の制限によって、(1)通信によって受け取ったものは送ることができない計算系($\alpha\beta$)、(2)通信によって知った相手からは受信できない計算系($\beta\pi$)、(3)通信によって知った相手には送信できない計算系($\gamma\pi$)が得られる。これらの計算系では、nameを送信したプロセスは受信したプロセスに対してnameを送信側の意図に沿った形でしか使わせないようにできる。なお、 $\alpha\pi$ 、 $\beta\pi$ は、プロセスの構文を制限したにもかかわらず、 π 計算と同等の表現力を有することを証明した。一方、 $\gamma\pi$ の表現力は π 計算とは同等でないと予想される。しかし、まだ証明には至っていない。

Controlling the Usage of Communicated Data in Name-passing Calculi

TETSU ITO[†]

In communication systems such as the Internet, it is desirable that in sending data one can impose some restrictions on how the data should be used from the view points of copyright and security. In this presentation, several new variants of π -calculus are introduced, in which the receiver of a name cannot use it violating the restrictions. Two approaches are presented.

The first one is to add new primitives to π -calculus. In this approach, two calculi are introduced. The first one makes it possible to specify the maximum number of copying names. And the other has a new sort of names in addition to the usual ones. They can't be used in input actions. The second approach is to limit the syntax of processes. There are three ways of limitation. By them, three calculi are obtained: (1) one cannot send received names, (2) one cannot use received names as input channels, (3) one cannot use received names as output channels. The π -calculus is encoded into (1) and (2). It is conjectured, however, not to be the case with (3).

(平成13年1月23日発表)

[†] 京都大学大学院理学研究科数学数理解析専攻
Division of Mathematics and Mathematical Analysis,
Graduate School of Science, Kyoto University