日本科学哲学会第 51 回年次大会

セキュリティ・プロトコル検証に応用可能である分解不可能な論理結合子について

西牟田 祐樹 (Yuki Nishimuta)
慶應義塾大学

Danos-Regnier (1989)は古典線形論理の枠組みで乗法的線形論理の既存の論理結合子の組み合わせでは定義することが出来ない分解不可能な論理結合子を導入した。このような論理結合子に対する計算論的な解釈は知られていない。その理由として直観主義線形論理上ではこのような分解不可能な論理結合子は存在しないということが挙げられる。それゆえ、命題と証明がそれぞれ型とプログラムに対応するというカリー・ハワード対応を用いて Danos-Regnier の分解不可能な論理結合子に対して計算論的な解釈を得ることは困難である。

本発表では同一律除去則 (Hacking, 1979)あるいはエータ拡張 (eta expansion)に着目して分解不可能な論理結合子を考察する。分解不可能な論理結合子の顕著な特徴はカット除去のメインステップ(正規化,ベータ簡約)は成立するが、同一律除去則が成立しないことである。本発表ではまず自然演繹での連言の導入規則と含意の除去規則を組み合わせた論理結合子 (Naibo and Petrolo,2015, pp.158-159)に対して正規化は成立するが、エータ拡張が成立しないことを示す。そして、そのような論理結合子が分解不可能な論理結合子であることを示す。 次にその新たな論理結合子に制限を課すことにより、セキュリティ・プロトコル検証に応用可能であることを説明する。実際に(Clarke, Jha and Marrero, 1996)で用いられているメッセージの導出規則である導入規則と除去規則はそれぞれこの新たな論理結合子の導入規則と除去規則に対応している。導入規則は暗号化に対応し、除去規則は復号に対応することにより、エータ拡張が成立しないような論理結合子に対する計算論的な解釈が可能であることを説明する。

参考文献

E.M.Clarke, S.Jha and W.Marrero, Using state space exploration and a natural deduction style message derivation engine to verify security protocols, Programming Concepts and Methods PROCOMET ’98, pp. 87-106.

V. Danos and L. Regnier, The structure of multiplicatives, Archives for Mathematical Logic, vol. 28, 1989, pp. 181-203.

J.-Y. Girard, Linear Logic, Theoretical Computer Science, vol. 50, 1987, pp. 1-102.

I.Hacking, What is Logic?, Journal of Philosophy, vol.76 Issue 6, 1979, pp. 285-319.

A. Naibo and M. Petrolo, Are Uniqueness and Deducibility of Identicals the Same ?, Theoria, vol.81, 2015, pp.143-181.