

---

**発表概要**

---

## 定理証明システム Coq 上での Pre Logical Relation を用いた詳細化の正しさの証明

永山友和<sup>†</sup> 佐藤雅彦<sup>†</sup> 亀山幸義<sup>†</sup>

仕様からプログラムを開発する際、抽象的な仕様を具体的なプログラムへ変換することが行われている。抽象的な仕様には、用いるプログラミング言語では与えられていないデータ構造が含まれている可能性があり、具体的なプログラムとは、それらのデータ構造が実現されたプログラムである。このような変換のことを“詳細化”と呼ぶ。Honsell は、Pre Logical Relation を用いる、詳細化の正しさの証明技法を提案した。本研究では、定理証明システム Coq を用いて彼らの技法を形式化した。このことより、計算機上でプログラムの詳細化の正しさを厳密に証明することができる。

### Proof Method of Correctness of Refinement with Pre-Logical Relation on Coq

TOMOKAZU NAGAYAMA,<sup>†</sup> MASAHICO SATO<sup>†</sup>  
and YUKIYOSHI KAMEYAMA<sup>†</sup>

In developing programs from specifications, we transform abstract programs (specifications) into concrete programs. Abstract programs may have data, which are not available in our programming languages. In concrete programs, these data are represented by data which are provided. We call these transformation *data refinement*. Honsell suggest proof method of data refinement which use pre-logical relation. In this paper, we formalize their method with Coq. As a result, we can strictly prove the correctness of data refinement on computer.

(平成 13 年 1 月 23 日発表)

---

<sup>†</sup> 京都大学大学院情報学研究科  
Graduate School of Informatics, Kyoto University