

ソフトウェアの形式検証に関する調査と教育

A Survey on the Formal Verification of Software

情報システム部 堀 武司・波 通隆
企画調整部 奥田 篤

■研究の背景

高い信頼性が求められる分野のソフトウェア開発では、ソフトウェアの要求仕様や設計を形式的に記述し、数学的検証技法や検査ツールによって不具合の検証を行う形式手法（Formal Method）と呼ばれる手法が注目されています。しかし、数学的専門知識が必要である事、入手可能な技術情報が少ない事などから、技術導入があまり進んでいないのが現状です。そこで、企業の開発現場への形式手法導入の準備作業として、主要な形式手法に関する調査と技術者教育を行いました。

■研究の要点

1. 現在用いられている主な形式手法と関連する支援ツールの調査
2. 組込み制御分野を対象とした研修教材の開発
3. 開発要員向け教育の試行

The composite image illustrates the research process. On the left, a flowchart titled 'Bメソッドによる開発フロー' (Development Flow using B-method) shows the stages: 要求 (Requirements) -> 仕様検討 (Specification Review) -> 抽象機械 (Abstract Machine) -> 設計検討 (Design Review) -> 詳細化 (Refinement) -> 設計検討 (Design Review) -> 実装 (Implementation) -> コード生成 (Code Generation) -> プログラム (Program). A box labeled 'B検証支援ツール' (B-Verification Support Tools) is connected to the '仕様検討', '設計検討', and '実装' stages, with arrows pointing to '定理証明系による検証' (Verification using theorem provers). In the center, a screenshot of the 'ProB' tool interface shows code and verification results. On the right, a photograph shows a seminar titled 'システム設計検証技術研究会' (System Design Verification Technology Research Meeting) with a presenter and an audience.

■研究の成果

1. 形式手法の一つであるBメソッドとその支援ツールに関して、調査と試用を行いました。また、他の手法（VDM, Z記法など）との比較検討を行いました。
2. 組込み制御分野を想定した研修教材（自動車のドアロック制御など）を開発しました。
3. 企業の開発要員を対象として、手法と支援ツール活用に関する教育を実施しました。その結果、現場技術者にも十分習得可能との結論を得ました。

東海ソフト(株)、サニー技研、(株)ヴィッツ、名古屋市工業研究所
(独)産業技術総合研究、名古屋大学