

# Testing-Based Formal Verification for Software Quality Assurance and Cost Reduction

—ソフトウェア品質保証とコスト削減のためのテストに基づく形式検証—

劉 少英<sup>1</sup>

**概要** : Testing and formal verification are two important techniques for software verification and validation, but they face critical challenges. Testing shows the presence of bugs but never their absence. Formal verification can be used to prove the correctness of programs but is usually difficult and costly to manage incorrect programs. Unfortunately, the very reality in software development is that a newly developed system always contains bugs and cannot be correct in the beginning. How to formally prove the correctness of programs in a cost-effective manner is still a challenge. As a matter of fact, even if a program is proved to be correct, it does not necessarily mean that no bugs are included in the program. In this talk, after briefly discussing the characteristics and challenges of current verification and validation approaches, a new approach, known as testing-based formal verification (TBFV), will be introduced. TBFV results from an appropriate integration of formal specification-based testing and Hoare logic for proving program correctness. It is a rigorous gray-box testing approach that takes both the specification and the program structure into account. The most important benefits of TBFV are that it can significantly reduce the number of tests necessary and be applied automatically to ensure the correctness or high reliability of programs.

---

<sup>1</sup> 広島大学大学院先進理工系科学研究科 教授