【Grant-in-Aid for Scientific Research(S)】
Integrated Science and Innovative Science (Comprehensive fields)

Title of Project : Development of the Innovative Specification Verification System based on Proof Scores

Kokichi FUTATSUGI
(JAIST, School of Information Science, Professor)

Research Area : Informatics-Software
Keywords : Specification Construction/Verification, Formal Methods, CafeOBJ, Proof Scores

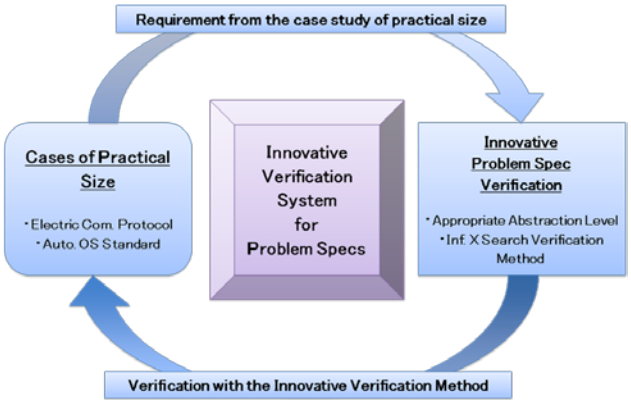
【Purpose and Background of the Research】

Construction of reliable and secure problem specifications (i.e. specifications or models of processes, activities, rules, and/or organizations in problem/application domains) is one of the most important issue in software technology of 21st century. For example, many company or government agencies are currently trying to provide new services on the Internet, and reliable and secure specifications of requirements in problem domains are vital important. In the automotive embedded software area where the shift to electric cars is apparent, it is an urgent issue to prepare fundamentals for the social system where many companies can collaborate flexibly in producing reliable and secure automotive software. Establishment of reliable and secure standards (i.e. problem specifications) for basic automotive software is an inevitable prerequisite for the end.

This research project is aiming at the development of the innovative verification system that can verify reliability and security of problem specifications of practical sizes. The verification system is going to be developed based on the CafeOBJ proof score methodology, which is an original research achievement of Prof. Futatsugi's research group. The developed verification system will be an important foundational contribution to the formal methods in software engineering.

【Research Methods】

To improve the current verification method for making it applicable to problem specifications of practical sizes, the following two are going to be achieved. (1) Construction of specifications in the appropriate abstraction levels. (2) Verification with the seamless combination of inferences and searches. The verification system is going to be developed in parallel with the case studies in the following two domains. (a) Electric commerce protocols. (b) Automotive software standards. With these approaches, the methods for constructions and verifications of problem specifications of practical sizes are going to be clarified. The obtained methods will be embodied into the revised CafeOBJ language system, which will be distributed worldwide through the Internet.



【Expected Research Achievements and Scientific Significance】

(1) The verification system (i.e. a revised CafeOBJ language system) for problem specifications that can be used to construct problem specifications in appropriate abstraction levels and to verify the specifications with the seamless combination of inferences and searches. The system can prove and/or disprove the problem specifications of practical sizes.
(2) The verified formal problem specifications of practical sizes in the domains of electric commerce protocols and of automotive software standards.
(3) The developed verification methods, verification system, and verified problem specifications will be the foundational contributions to the core part of software technology.

【Publications Relevant to the Project】

Kokichi Futatsugi: Fostering Proof Scores in CafeOBJ, Proc. of 12th International Conference on Formal Engineering Methods (ICFEM 2010), LNCS 6447, Springer, pp.1-20, 2010. (invited keynote paper)

【Term of Project】 FY 2011-2015

【Budget Allocation】 134,300 Thousand Yen

【Homepage Address and Other Contact Information】

http://www.ldl.jaist.ac.jp/cafeobj/
futatsugi@jaist.ac.jp