Li, Bin; Tang, Zhenhao; Zhai, Juan; Zhao, Jianhua

Summary: This paper presents an approach to prove that a concrete program correctly implements its corresponding abstract program. Here, an abstract program uses some abstract data types such as set, list and map, and abstract operations upon those data types. A concrete program uses the types in the C-like language. The approach presented in the paper requires to specify correspondences between the abstract program and the concrete program, including correspondences between program points and correspondences between variables. Based on the correspondences, the verification task can be divided into small subtasks that can be easily and mostly automatically verified.

MSC:
68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)
68Q60 Specification and verification (program logics, model checking, etc.)
68Q65 Abstract data types; algebraic specification

Keywords:
program verification; consistency; abstract program; refinement; decomposition

Full Text: DOI