

Z 规格说明的推理与验证

赵正旭¹, 温晋杰², 赵卫华²

(1. 石家庄铁道大学 石家庄 050043) ; (2. 石家庄铁道大学 信息科学与技术学院 石家庄 050043)

摘要: Z 规格说明具有非形式规约不可比拟的严谨性、清晰性。这种描述对于系统内对象的状态描述、行为描述是非常有用的原始参照物。但是, 形式化描述不可避免的可能会含有错误或者是矛盾, 这些问题在后期必定会导致前期的形式化设计不能付诸实践。因此, 有必要做一些形式化的推理与验证来确保 Z 规约的实施。形式化推理是基于 Z 规格说明对一个操作模式求其前置条件, 即求一个操作成功执行的必要条件, 然后对比客观条件是否满足必要条件; 形式化验证是一个操作模式求其后置条件, 从集合的角度出发验证一个操作成功执行之后所导致的状态量变化是否与操作模式描述一致。

关键词: Z 规格说明; 推理; 验证; 形式化; 条件

The Reasoning and Verifying of Z Specification

ZHAO Zheng-xu¹, WEN Jin-jie², ZHAO Wei-hua²

(1.Shijiazhuang Tiedao University,Shijiazhuang,050043,China) ; (2.School of Information Science and Technology ,Shijiazhuang Tiedao University, Shijiazhuang, 050043,China)

Abstract: Compared with the informal specification, Z notion has incomparable rigor and clarity. The notion is an original reference for the state description and behavior description of objects in the system. However, Z notion may inevitably contains errors or contradictions, these problems will lead to the early formal design cannot be put into practice in the later. Therefore, it is necessary to do some formal reasoning and validation to ensure the implementation of Z notion. Formal reasoning is based on Z specification for an operator schema of its pre-condition, that is to infer the necessary conditions for the successful execution of an operation and calculates whether the objective conditions meet the necessary specifications; Formal verification is an operation mode for its post condition, from a set perspective the verification of whether the change of the state variables caused by a successful operation is consistent with the description of the operator schema.

Keywords: Z specification; Reasoning; Verification; Formalization; Conditions

在软件研发的过程中, 面对需求越来越多变, 系统越来越复杂的现状, 软件需求规格说明书在软件生命周期中占有举足轻重的地位, 是所有软件研发参与人员的一个可靠参照物。如何确保撰写的规格说明具有客户所要求的性质? 如何确保参照该规格说明编写出的软件与规格说明书所描述的相吻合? 如何保证研发人员编写出的程序的可靠性、功能性、效率性等各项质量指标呢^[1]? 形式化推理是验证软件正确性的重要方法之一, 它通过严格的数学方法来评价一个程序是否达到了需求规格说明书所描述的功能, 也就是说, 对于一组允许输入的信息 X, 严格的证明程序能否正确执行以及能否得到正确的输出信息 Z。程序正确性证明的研究早在 20 世纪 50 年代就为图灵等人所注意。一份合格的 Z 规格说明需要清晰准确的描述“做什么”, 还必须要保证参照该规格说明编写出的软件与规格说明书所描述的各项特性相匹配。2014 年在新加坡举行的第 19 届形式化方法国际研讨会

上, 有两个来自中国的团队进行了汇报, 恰巧他们汇报的题目都与玉兔月球车相关, 一个与月球软着陆控制器相关, 另一个与玉兔月球车控制系统相关。其中用形式化方法验证玉兔控制系统切实体现了形式化方法的强大与复杂^[2,3]。2015 年国外一个技术团队利用形式化方法验证 Java 中一些排序算法的正确性, 在验证 Timsort 排序算法时发现了 Bug。利用自动生成的测试用例集很难生成一个可以触发该 Bug 的 Array, 所以, 通过形式化推理来证明程序的正确性的时候发现了这个错误^[4]。

1. Z 语言概述

Z 语言是一种用“数学文字”或“数学符号”来描述计算机系统的规范化语言, 它不但能应用于计算机硬件系统, 而且也特别适用于计算机软件系统。Z 语言描述“做什么”

基金项目: 河北省高等学校高层次人才科学研究项目 (GCC2014010);

作者简介: 赵正旭(1960—), 男, 教授, 长江学者, 博士生导师, 主要研究领域: 虚拟现实, 数据组织; 温晋杰(1990—), 男, 石家庄铁道大学, 硕士研究生, 电子邮件: 474600137@qq.com, 研究方向: 形式化软件工程; 赵卫华 (1961—), 女, 副教授, 主要研究领域: 信息组织;