A Method of Path Feasibility Judgment Based on Symbolic Execution and Range Analysis

Ya-Wen Wang¹ ², Ying Xing¹ ³ and Xu-Zhou Zhang¹

¹State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China
²State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China
³Liaoning Technical University, Huludao, China

wangyawan@bupt.edu.cn, lovelyjamie@yeah.net, laomao22311@126.com

Abstract

In program testing, the accurate information of path feasibility can improve the efficiency of static analysis. The dynamic judgment method of path feasibility needs to execute program, and the results usually not sound. On the basis of symbolic execution, this paper proposes a new static judgment method, which simultaneously computes two interval sets of each symbolic variable: possible value set and necessary value set. According to these range information, we can easily give the definite judgment of a path: feasible, infeasible or uncertain. Experiment shows that the method is appropriate and efficient in case of the weakly relevant input.

Keywords: path feasibility, symbolic execution, interval computation, static analysis

1. Introduction

The problem of path feasibility judgment, which is an important part of structure testing, has been studied since 1970s. The accurate information about path feasibility can improve the efficiency of static program analysis. Moreover, it is beneficial for testers to detect infeasible paths in early times, because generating test data for infeasible paths will consume a great deal of human and material resources in the subsequent dynamic testing stage.

Weyuker [1] has proved that it is an unsolvable problem to determine whether a program path is feasible or not. According to the study progress on path feasibility, there are three main strategies.

1) To select feasible paths based on fewer decision nodes, since the fewer predicates means the smaller probability of infeasible paths [2].

2) To judge infeasible paths dynamically. That is to say, to evaluate whether one path is feasible by the effort when generating test cases for the path [3-4].

3) To judge infeasible paths statically by analyzing the satisfaction of path conditions or the effect of branch correlation [5-6].

However, because of the uncertainty of the checking results, the first two methods are just suitable for most of the program paths. Although the static method cannot determine the feasibility of all the paths definitely, its checking result is sound, which presents the path feasibility accurately, and it is much useful for the program testing.

In this paper, we propose a new judging method based on symbolic execution and static range analysis, which uses the extended interval arithmetic. As one of the static methods, it can accurately identify not only part of infeasible paths, but also part of the feasible paths, and this is the main contribution of this paper.

The remainder of this paper is organized as follows. Section 2 defines the possible value set and necessary value set of a variable in the condition expression and gives the
result is sound. If the result tells that one path is feasible or infeasible, it is true with the fact. Of course, limited by the approximation of interval arithmetic, the method is effective for the functions with weakly relevant input, and there may exist quite many paths identified uncertain. Our next work is to improve the precision of interval computation with complex expressions and operators. By this way, a significant accuracy enhancement of path feasibility identification will be achieved.

Acknowledgement

This paper is supported by the National Natural Science Foundation of China (No. 61202080), the National Grand Fundamental Research 863 Program of China (No. 2012AA011201), the Key Project of the National Natural Science Foundation of China (No. 91318301) and the Open Funding of State Key Laboratory of Computer Architecture (CARCH201201).

References