Usage of Invariants for Symbolic Verification of Requirements

Short Paper

Alexander Letichevsky[1], Alexander Godlevsky[1], Anton Guba[1], Alexander Kolchin[1], Oleksandr Letychevskyi[1], Vladimir Peschanenko[2]

[1] V.M. Glushkov Institute of Cybernetics, Kiev, Ukraine
let@cyfra.net, godl@iss.org.ua, antonguba@ukr.net, kolchin_av@yahoo.com, lit@iss.org.ua
[2] Kherson State University, Kherson, Ukraine
vladimirius@gmail.com

The main goal of the paper is finding of pre- and post-invariants for transitions between symbolic states in the system that must be verified and use them for verification purposes. Systems are specified by basic protocols [1]. This specification defines a transition system with transitions $s \rightarrow s'$ where s and s' are symbolic states, b is a basic protocol. The main problem of verification is a reachability problem for given properties expressed in specification logic language.

We present double approximation method of verification based on computing invariants. The method is implemented as an iterative algorithm which solves in parallel reachability problem and computes lower and upper approximations of invariants for basic protocols.

Currently there are a lot of significant works devoted to computing invariants, which are considered for loops in programs. Loops are marked explicitly - syntactic constructions like while and others. When we deal with requirement specifications, we do not deal with explicit marked loops, moreover basic protocols provide non-deterministic order. Existing methods usually ignore the conditions of the loops. Invariants formulae, which is obtained as a result, include unreachable states and therefore could be used in verification only in the following way: if a property does not intersect with the invariant formula, then it is unreachable, if intersects, then conclusion cannot be done. Therefore, the problem of modification of existing methods, or to develop a new algorithm that could be applied in practice of requirements verification is actual.

Research of problems of automatic program invariants generation for a variety of data algebras was performed starting from 70-th years in Institute of Cybernetics of NAS of Ukraine. Their main results are presented in [2]. Double approximation method, is the dynamic iterative method of invariants generation and it is based on these results and adapted for requirements verification. The method also can be applied to program verification if a program is considered as a special case of basic protocol specification. The method has been implemented in VRS (Verification of Requirement Specifications) system [3] and IMS (Insertion Modeling System) system [4].

References

[1] A. Letichevsky, J. Kapitonova, V. Volkov, A. Letichevsky Jr., S. Baranov, V. Kotlyarov, T. Weigert. System Specification with Basic Protocols. Cybernetics and System Analyses, vol. 4, 2005, p. 3-21.

[2] Godlevsky A.B., Kapitonova Y.V., Krivoy S.L., Letichevsky A.A. Iterative methods of program analysis. Cybernetics, vol. 2, 1989, . 9-19.

[3] Verification for Requirement Specification (VRS). http://iss.org.uaISS/VRS/tool.htm, last viewed May 2013.

[4] APS and IMS Systems. http://apsystem.org.ua, last viewed May 2013.