Verification, Testing and Statistics

Sriram K. Rajamani

Microsoft Research India
sriram@microsoft.com

Formal verification is the holy grail of software validation. Practical applications of verification run into two major challenges. The first challenge is in writing detailed specifications, and the second challenge is in scaling verification algorithms to large software. In this talk, we present possible approaches to address these problems:

- We propose using statistical techniques to raise the level of abstraction, and automate the tedium in writing detailed specifications. We present our experience with the Merlin project [4], where we have used probabilistic inference to infer specifications for secure information flow, and discovered several vulnerabilities in web applications.
- We propose combining testing with verification to help scalability, an reducing false errors. We present our experience with the Yogi project [1,2,3,5], where we have built a verifier that combines static analysis with testing to find bugs and verify properties of low-level systems code.

Acknowledgment. We thank our collaborators Anindya Banerjee, Nels Beckman, Bhargav Gulavani, Patrice Godefroid, Tom Henzinger, Yamini Kannan, Ben Livshits, Aditya Nori, Rob Simmons, Sai Tetali and Aditya Thakur.

References

1. Beckman, N.E., Nori, A.V., Rajamani, S.K., Simmons, R.J.: Proofs from tests. In: ISSTA 2008: International Symposium on Software Testing and Analysis, pp. 3–14. ACM Press, New York (2008)
2. Godefroid, P., Nori, A.V., Rajamani, S.K., Tetali, S.: Compositional May-Must Program Analysis: Unleashing The Power of Alternation. Microsoft Research Technical Report MSR-TR-2009-2, Microsoft Research (2009)
3. Gulavani, B.S., Henzinger, T.A., Kannan, Y., Nori, A.V., Rajamani, S.K.: SYNERGY: A new algorithm for property checking. In: FSE 2006: Foundations of Software Engineering, pp. 117–127. ACM Press, New York (2006)
4. Livshits, B., Nori, A.V., Rajamani, S.K., Banerjee, A.: Merlin: Specification Inference for Explicit Information Flow Problems. To appear in PLDI 2009: Programming Language Design and Implementation. ACM Press, New York (2009)
5. Nori, A.V., Rajamani, S.K., Tetali, S., Thakur, A.V.: The Yogi Project: Software Property Checking via Static Analysis and Testing. In: TACAS 2009: Tools and Algorithms for Constuction and Analysis of Systems. LNCS, vol. 5509, pp. 178–181. Springer, Heidelberg (2009)

M. Leucker and C. Morgan (Eds.): ICTAC 2009, LNCS 5684, p. 79, 2009.