Static Analysis by Abstract Interpretation of Numerical Programs and Systems, and FLUCTUAT

Eric Goubault

CEA LIST
CEA Saclay, Nanoinnov, 91191 Gif-sur-Yvette CEDEX, France
eric.goubault@cea.fr

This invited lecture is a survey of our work over the last 12 years or so[1], dealing with the precise analysis of numerical programs, essentially control programs such as the ones found in the aerospace, nuclear and automotive industry.

Our approach is now based on a rather generic abstract domain, based on "zonotopes" or "affine forms" [7], but with some specificities. For instance, our zonotopic domain provides a functional abstraction [16,13], i.e. an abstraction of the input-output relationships between values of variables, allowing for test generation and modular verification [21]. Also, our domain deals with the real number and the finite precision (for instance, floating-point or fixed-point) semantics [14,17]. It is used in practice in FLUCTUAT [20,9,4] to prove some functional properties of programs, generate (counter-) examples, identify the discrepancy between the real number and the finite precision semantics and its origin etc.

Our work is building over methods from abstract interpretation of course [8], but also over methods from applied mathematics, most notably from the "guaranteed computations" or "interval" community (affine arithmetic [7] and more general Taylor models for instance), from optimization and game theory, and from control theory (with policy iteration for instance [11] or quadratic invariants, as in [2]). In some ways, this interplay between numerical mathematics and abstract interpretation makes the calculations in the abstract much like a perturbed numerical scheme, which has its own stability and convergence properties, related to the stability and convergence of the concrete numerical scheme we are trying to prove. Similarly, we can think of our finite-precision abstract semantics as some form of a deformation of the semantics in the real numbers, i.e. the proofs we are providing are deformations of proofs in the real numbers.

Many extensions of this zonotopic abstract domain have been designed over the years: constrained affine forms [12], under-approximations [15] and more recently, "imprecise probabilistic" analyzes [5,1], where we consider that inputs of the program under analysis can be given by (non-deterministic) ranges as well as probability or sets of probability distributions.

[1] With a first publication at a previous SAS [18]. Acknowledgments are due to all my colleagues in the MeASI team over these last years and in particular for this talk, Olivier Bouissou, Tristan Legall, Matthieu Martel, Sylvie Putot, Franck Védrine and Sarah Zennou.

F. Logozzo and M. Fähndrich (Eds.): SAS 2013, LNCS 7935, pp. 1–3, 2013.
© Springer-Verlag Berlin Heidelberg 2013

On the application side, we have become interested not only in certifying control software [20], potentially as part of an hybrid system [6] but also in characterizing the algorithmic error [9] (or "method" error) very early on in the software development phase, and not only the implementation error, due to finite-precision arithmetics. Recent applications of our static analyzes include "sensitivity" analysis, uncertainty propagation (in parametric models such as the ones found in robust control, or due to uncertain errors on inputs) and generating correct "optimal" fixed-point formats for programs [22].

Among the future directions of our work are the links with proof theory and program provers and the analysis of scientific computing codes, such as finite element methods for solving partial differential equations. As a matter of fact, proof-theoretic approaches, similar in spirit, have been introduced slightly later (such as [3]) and make it possible, combining it with our work, to make precise the notion of "perturbation of a proof" from real numbers to finite-precision implementations. This latter notion has actually been, implicitely at least, introduced long ago [25,24] for the study of important numerical schemes such as conjugate gradient or Lanczos methods, see [23] for a modern account. This might explain that our interest in embedded systems codes has gradually moved towards more general "cyber-physical systems" and, in parallel, towards scientific computing, which presents a real challenge to static analyzers, both on the numerical, and on the alias analysis part. One of the consequences is that we would then have to integrate our numerical domains in static analyzers dealing with concurrent programs, using our own methods [19,10]. In the realm of parallel computing, the issues concerning floating-point computations are of big concern, since in general, programs do compute a lot more numerical expressions, with even lower control on their order of evaluation, and run on hardware architectures with complicated semantics (GPUs, weak-memory models on multicore systems etc.).

References

1. Adjé, A., Bouissou, O., Goubault-Larrecq, J., Goubault, E., Putot, S.: Analyzing probabilistic programs with partially known distributions. In: VSTTE (2013)
2. Adjé, A., Gaubert, S., Goubault, E.: Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. Logical Methods in Computer Science 8(1) (2012)
3. Boldo, S., Filliâtre, J.C.: Formal Verification of Floating-Point Programs. In: 18th IEEE International Symposium on Computer Arithmetic (June 2007)
4. Bouissou, O., Conquet, E., Cousot, P., Cousot, R., Ghorbal, K., Lesens, D., Putot, S., Turin, M.: Space software validation using abstract interpretation. In: DASIA (2009)
5. Bouissou, O., Goubault, E., Goubault-Larrecq, J., Putot, S.: A generalization of p-boxes to affine arithmetic. Computing 94(2-4), 189–201 (2012)
6. Bouissou, O., Goubault, E., Putot, S., Tekkal, K., Vedrine, F.: HybridFluctuat: A static analyzer of numerical programs within a continuous environment. In: Bouajjani, A., Maler, O. (eds.) CAV 2009. LNCS, vol. 5643, pp. 620–626. Springer, Heidelberg (2009)

7. Comba, J.L.D., Stolfi, J.: Affine arithmetic and its applications to computer graphics. In: Proceedings of SIBGRAPI (1993)
8. Cousot, P., Cousot, R.: Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: POPL, pp. 238–252 (1977)
9. Delmas, D., Goubault, E., Putot, S., Souyris, J., Tekkal, K., Védrine, F.: Towards an industrial use of FLUCTUAT on safety-critical avionics software. In: Alpuente, M., Cook, B., Joubert, C. (eds.) FMICS 2009. LNCS, vol. 5825, pp. 53–69. Springer, Heidelberg (2009)
10. Fajstrup, L., Goubault, É., Haucourt, E., Mimram, S., Raussen, M.: Trace spaces: An efficient new technique for state-space reduction. In: Seidl, H. (ed.) ESOP 2012. LNCS, vol. 7211, pp. 274–294. Springer, Heidelberg (2012)
11. Gawlitza, T.M., Seidl, H., Adjé, A., Gaubert, S., Goubault, E.: Abstract interpretation meets convex optimization. J. Symb. Comput. 47(12), 1416–1446 (2012)
12. Ghorbal, K., Goubault, E., Putot, S.: A logical product approach to zonotope intersection. In: Touili, T., Cook, B., Jackson, P. (eds.) CAV 2010. LNCS, vol. 6174, pp. 212–226. Springer, Heidelberg (2010)
13. Goubault, E., Gall, T.L., Putot, S.: An accurate join for zonotopes, preserving affine input/output relations. In: Proceedings of NSAD 2012, 4th Workshop on Numerical and Symbolic Abstract Domains. ENTCS, vol. 287, pp. 65–76 (2012)
14. Goubault, É., Putot, S.: Static analysis of numerical algorithms. In: Yi, K. (ed.) SAS 2006. LNCS, vol. 4134, pp. 18–34. Springer, Heidelberg (2006)
15. Goubault, E., Putot, S.: Under-approximations of computations in real numbers based on generalized affine arithmetic. In: Riis Nielson, H., Filé, G. (eds.) SAS 2007. LNCS, vol. 4634, pp. 137–152. Springer, Heidelberg (2007)
16. Goubault, E., Putot, S.: A zonotopic framework for functional abstractions. CoRR abs/0910.1763 (2009), `http://arxiv.org/abs/0910.1763`
17. Goubault, E., Putot, S.: Static analysis of finite precision computations. In: Jhala, R., Schmidt, D. (eds.) VMCAI 2011. LNCS, vol. 6538, pp. 232–247. Springer, Heidelberg (2011)
18. Goubault, É.: Static analyses of the precision of floating-point operations. In: Cousot, P. (ed.) SAS 2001. LNCS, vol. 2126, pp. 234–259. Springer, Heidelberg (2001)
19. Goubault, E., Haucourt, E.: A practical application of geometric semantics to static analysis of concurrent programs. In: Abadi, M., de Alfaro, L. (eds.) CONCUR 2005. LNCS, vol. 3653, pp. 503–517. Springer, Heidelberg (2005)
20. Goubault, E., Putot, S., Baufreton, P., Gassino, J.: Static analysis of the accuracy in control systems: Principles and experiments. In: Leue, S., Merino, P. (eds.) FMICS 2007. LNCS, vol. 4916, pp. 3–20. Springer, Heidelberg (2008)
21. Goubault, E., Putot, S., Védrine, F.: Modular static analysis with zonotopes. In: Miné, A., Schmidt, D. (eds.) SAS 2012. LNCS, vol. 7460, pp. 24–40. Springer, Heidelberg (2012)
22. Menard, D., Rocher, R., Sentieys, O., Simon, N., Didier, L.S., Hilaire, T., Lopez, B., Goubault, E., Putot, S., Védrine, F., Najahi, A., Revy, G., Fangain, L., Samoyeau, C., Lemonnier, F., Clienti, C.: Design of fixed-point embedded systems (defis) french anr project. In: DASIP, pp. 1–2 (2012)
23. Meurant, G.: The Lanczos and Conjugate Gradient Algorithms: From Theory to Finite Precision Computations (Software, Environments, and Tools). SIAM (2006)
24. Paige, C.C.: The computation of eigenvalues and eigenvectors of very large sparse matrices. Ph.D. thesis (1971)
25. Wilkinson, J.H.: The algebraic eigenvalue problem. Oxford University Press (1965)