A library of Taylor models for PVS automatic proof checker

Francisco Cháves[1] and **Marc Daumas**

Laboratoire de l'Informatique du Parallélisme
École Normale Supérieure de Lyon
UMR 5668 CNRS–ENS de Lyon–INRIA
email: Francisco.Jose.Chaves.Alonso,Marc@ENS-Lyon.Fr, Daumas@ENS-Lyon.Fr

Abstract

Taylor models, see for example [3] and references herein, have recently emerged as a nice and convenient way to reduce decorrelation in interval arithmetic [4, 5, 2]. Taylor models are even more attractive when one solves initial value problems for ODEs as they provide a validated built-in integration operator.

Yet, it is now beyond doubt that programs and libraries contain bugs, no matter how precisely they have been specified and how thoroughly they have been tested [8, 7]. As a consequence, the highest Common Criteria Evaluation Assurance Level, EAL 7[2], has only been awarded so far to products that provide validation using a formal tool, specifically an automatic proof checker in first or higher order logic.

We present here our library of Taylor models in PVS [6]. Working with an automatic proof checker, we had to manage two tasks. The first task was to create a data type and operations on this new type to allow users to define and evaluate expressions using Taylor models. The second task was to provide proofs that each operator is correct and a strategy to recursively analyze compound expressions. Both tasks rely on the recently published library on interval arithmetic for PVS [1]. As many mathematical developments are not yet available in PVS, we also had to develop a library on polynomials and prove a few theorems of analysis.

Our library can be used to derive quickly more or less accurate bounds. For example, the user of a formal tool has to provide a proof that the radical is non negative every time an expression uses a square root operator. Some proofs use intricate analysis but most of them are very simple and interval arithmetic or low degree evaluations with Taylor models can produce appropriate proofs. Our library can also be used to expertly derive computer validated proofs of difficult results through an expert use of Taylor models.

The library will be available freely on the Internet as soon as it is stable. Side

[1] This work is supported by the the *Mathlogaps* (Mathematical Logic and Applications) project, an Early Stage Research Training grant of the European Union.

[2] `http://niap.nist.gov/cc-scheme/`.

developments are integrated as they are produced to NASA Langley PVS libraries[3].

References

[1] Marc Daumas, Guillaume Melquiond, and César Muñoz. Guaranteed proofs using interval arithmetic. In Paolo Montuschi and Eric Schwarz, editors, *Proceedings of the 17th Symposium on Computer Arithmetic*, Cape Cod, Massachusetts, 2005.

[2] Luc Jaulin, Michel Kieffer, Olivier Didrit, and Eric Walter. *Applied interval analysis*. Springer, 2001.

[3] Kyoko Makino and Martin Berz. Taylor models and other validated functional inclusion methods. *International Journal of Pure and Applied Mathematics*, 4(4):379–456, 2003.

[4] Ramon E. Moore. *Interval analysis*. Prentice Hall, 1966.

[5] Arnold Neumaier. *Interval methods for systems of equations*. Cambridge University Press, 1990.

[6] Sam Owre, John M. Rushby, and Natarajan Shankar. PVS: a prototype verification system. In Deepak Kapur, editor, *11th International Conference on Automated Deduction*, pages 748–752, Saratoga, New-York, 1992. Springer-Verlag.

[7] Philip E. Ross. The exterminators. *IEEE Spectrum*, 42(9):36–41, 2005.

[8] John Rushby and Friedrich von Henke. Formal verification of algorithms for critical systems. In *Proceedings of the Conference on Software for Critical Systems*, pages 1–15, New Orleans, Louisiana, 1991.

[3] `http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html`.