https://doi.org/10.1007/s00165-020-00510-7

Formal Aspects of Computing (2020) 32: 149–151

Formal Aspects of Computing

André Platzer: Logical foundations of cyber-physical systems

Springer International Publishing, 2018, XXXI+639 pp, ISBN: 978-3-319-63587-3 (Hardcover, $39.99)

Alexander Knapp[1] and Markus Roggenbach[2]

[1] Institut für Informatik, Augsburg University, Augsburg, Germany
[2] Department of Computer Science, Swansea University, Swansea, UK

Will the cat catch the mouse?

One of the early examples illustrating the challenges in analysing hybrid systems was stated by Maler, Manna, and Pnueli in 1991:

At time $T = 0$, a mouse starts running from a certain position on the floor in a straight line towards a hole in the wall, which is at a distance X_0 from the initial position. The mouse runs at a constant velocity V_m. After a delay of Δ time units, a cat is released at the same initial position and chases the mouse at velocity V_c along the same path. Will the cat catch the mouse or will the mouse find sanctuary while the cat crashes against the wall? [MMP91]

While about 30 years ago this problem was at the forefront of research, Platzer's book now presents a comprehensive textbook for educational purposes that, in a step by step manner, develops a formal method capable of addressing challenges like the above.

Platzer defines his field of study as follows: "Cyber-physical systems combine cyber capabilities with physical capabilities to solve problems that neither part could solve alone." [Pla18, p. 1]. Autonomous driving, unmanned aerial vehicles, robots—all these systems and their control transcend the boundaries of classical computer science and informatics, which focus on digital information only. Besides being distributed and reactive, these cyber-physical systems sport the characteristics of combining discrete states with continuous flows.

Under the term of hybrid systems, combinations of discrete and continuous behaviour have indeed been studied since the mid 1990s building on the success of timed automata, which integrate true real time with discrete states. Research and also text book presentations of the topic have been concentrating on model checking as the underlying verification technique. However, for hybrid systems the model checking approach is inherently limited: the reachability problem is undecidable even for simple classes like linear hybrid systems. In contrast, since his dissertation in 2008, Platzer has studied symbolic techniques to reason on hybrid systems. Now he offers with his book a mature treatment of the subject and its foundations.

Taking a formal method $\mathcal{M}$ as comprising of the three elements, cf. [RCS+20],

Syntax precise description of the form of objects (typically strings or graphs) belonging to $\mathcal{M}$;

Semantics describes the 'meaning' of the syntactic objects of $\mathcal{M}$, in general by a mapping into some mathematical structure; and

Method describes algorithmic ways of transforming syntactic objects of $\mathcal{M}$, in order to gain some insight about them;

Correspondence to: A. Knapp, E-mail: knapp@informatik.uni-augsburg.de; M. Roggenbach, E-mail: m.roggenbach@swansea.ac.uk

the book presents a meticulous, stepwise development of all these three aspects: as syntax a dynamic logic extended to continuous semantics is introduced; the semantic domain is hybrid systems with discrete modes and continuous behaviour according to differential equations in these modes; the method, finally, builds on a sound sequent calculus for the dynamic logic.

The book is organised in four main parts:

- The *first part* studies 'elementary cyber physical systems'. Syntactically, these are modelled as hybrid programs involving discrete control and continuous dynamics. For reasoning, a differential dynamic logic is introduced, accompanied with a sound proof calculus in sequent style. Throughout this part, the bouncing ball provides the master example illustrating the concepts.
- The *second part* on differential equation analysis gives an in-depth treatment of how to describe continuous dynamics with differential equations and their analysis with proof rules. Beyond merely solving ordinary differential equations, the techniques of differential invariants and differential ghosts are carefully developed. Again, the theory is illustrated with variations of the bouncing ball.
- *Part three* takes the environment of cyber-physical systems into account and studies hybrid games. This topic is technically more involved, e.g., it uses ordinal numbers and advanced arguments on fix points. Dancing robots serve as illustrations.
- Finally, *part four* provides a comprehensive collection of techniques to prove the correctness of cyber-physical systems. The underlying question is how to implement a prover for the methods discussed in the previous parts. Here, the focus is on 'taming' real arithmetic.

The book is accompanied with comprehensive resources on a web page and also examples in the proof tool Keymaera X. For each chapter it also contains a number of exercises, though without solutions. The bibliography is comprehensive, it is presented chapter by chapter.

As the title says, the book focuses on foundations and thus is a text for a theoretical course. It provides factual knowledge, namely explanations of concepts used, and procedural knowledge, i.e., how we can go about doing things. Thus, the foundations for cyber physical systems engineering are laid. However, the steps towards problem classification, i.e., grouping problems with similar characteristics, and design methods, i.e., recipes for designing solutions for problems, are still to follow and would ideally be presented in a 2nd volume by the author focusing on applications. Together, this would result in a handbook [GKMR20] for symbolic formal methods in cyber physical systems engineering.

The book is written for educational purposes and addresses an undergraduate student reader. Due to this audience, Platzer recapitulates earlier material quite often, which, for the advanced reader, might appear repetitive in some parts. Also, for the researcher, the book's writing style touches on verbosity. As typical for a text book, alternative approaches are only mentioned occasionally and are neither discussed nor related in detail. A point of criticism might be the lack of research perspectives, which are rarely pointed out; this, again, might be due to the target audience of undergraduate students.

Overall, Platzer's textbook gives an excellent account on symbolic reasoning about cyber-physical systems. With its techniques at hand, the reader can analyse complex cyber-physical systems—and it becomes a trifle to figure out under which circumstances the cat catches the mouse.

Acknowledgements

Open Access funding provided by Projekt DEAL.

References

[GKMR20] Gruner S, Kumar A, Maibaum T, Roggenbach M (2020) On the construction of engineering handbooks—with an illustration from the Railway Safety Domain. Springer, New York

[MMP91] Maler O, Manna Z, Pnueli A (1991) From timed to hybrid systems. In: de Bakker JW, Huizing C, de Roever WP, Rozenberg G (eds) Proceedings of the REX workshop. Real-time: theory in practice, volume 600 of lecture notes in computer science. Springer, New York, pp 447–484

[Pla18] Platzer A (2018) Logical foundations of cyber-physical systems. Springer, New York

[RCS+20] Roggenbach M, Cerone A, Schlingloff B-H, Schneider G, Shaikh SA (2020) Formal methods for software engineering—languages, methods, application domains. Springer, New York

Published online 20 March 2020