Zufferey, Damien; **Wies, Thomas**; **Henzinger, Thomas A.**

Ideal abstractions for well-structured transition systems. (English) Zbl 1326.68205

Kuncak, Viktor (ed.) et al., Verification, model checking, and abstract interpretation. 13th international conference, VMCAI 2012, Philadelphia, PA, USA, January 22–24, 2012. Proceedings. Berlin: Springer (ISBN 978-3-642-27939-3/pbk). Lecture Notes in Computer Science 7148, 445-460 (2012).

Summary: Many infinite state systems can be seen as well-structured transition systems (WSTS), i.e., systems equipped with a well-quasi-ordering on states that is also a simulation relation. WSTS are an attractive target for formal analysis because there exist generic algorithms that decide interesting verification problems for this class. Among the most popular algorithms are acceleration-based forward analyses for computing the covering set. Termination of these algorithms can only be guaranteed for flattable WSTS. Yet, many WSTS of practical interest are not flattable and the question whether any given WSTS is flattable is itself undecidable. We therefore propose an analysis that computes the covering set and captures the essence of acceleration-based algorithms, but sacrifices precision for guaranteed termination. Our analysis is an abstract interpretation whose abstract domain builds on the ideal completion of the well-quasi-ordered state space, and a widening operator that mimics acceleration and controls the loss of precision of the analysis. We present instances of our framework for various classes of WSTS. Our experience with a prototype implementation indicates that, despite the inherent precision loss, our analysis often computes the precise covering set of the analyzed system.

For the entire collection see [Zbl 1236.68007].

MSC:

68Q85 Models and methods for concurrent and distributed computing (process algebras, bisimulation, transition nets, etc.)
68Q60 Specification and verification (program logics, model checking, etc.)

Software:

Lift; PICASSO

Full Text: DOI

References:

[1] Abdulla, P.A., Cerans, K., Jonsson, B., Tsay, Y.-K.: General decidability theorems for infinite-state systems. In: LICS, pp. 313–321 (1996)· doi:10.1109/LICS.1996.561359

[2] Abdulla, P.A., Collomb-Annichini, A., Bouajjani, A., Jonsson, B.: Using forward reachability analysis for verification of lossy channel systems. FMSD˜25(1), 39–65 (2004) · Zbl 1073.68675

[3] Abdulla, P.A., Jonsson, B.: Verifying programs with unreliable channels. In: LICS, pp. 160–170 (1993) · Zbl 0856.68096 · doi:10.1109/LICS.1993.287591

[4] Azzopardi, T.: Generic compute server in Scala using remote actors (2008), http://tiny.cc/yjzva (accessed November 2011)

[5] Bagnara, R., Hill, P.M., Zaffanella, E.: Widening operators for powerset domains. Software Tools for Technology Transfer˜8(4/5), 449–466 (2006) · Zbl 05075103 · doi:10.1007/s10009-005-0215-8

[6] Calcagno, C., Distefano, D., O'Hearn, P.W., Yang, H.: Compositional shape analysis by means of bi-abduction. In: POPL, pp. 289–300 (2009) · Zbl 1315.68085

[7] 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)· doi:10.1145/512950.512973

[8] Cousot, P., Cousot, R.: Systematic design of program analysis frameworks. In: POPL, pp. 269–282. ACM (1979) · Zbl 1323.68356 · doi:10.1145/567752.567778

[9] Cousot, P., Cousot, R.: Abstract interpretation frameworks. Journal of Logic and Computation˜2(4), 511–547 (1992) · Zbl 0783.68073 · doi:10.1093/logcom/2.4.511

[10] Dufourd, C., Finkel, A., Schnoebelen, P.: Reset Nets Between Decidability and Undecidability. In: Larsen, K.G., Skyum, S., Winskel, G. (eds.) ICALP 1998. LNCS, vol.˜1443, pp. 103–115. Springer, Heidelberg (1998) · Zbl 0909.68124 · doi:10.1007/BFb0055044

[11] Engelfriet, J., Gelsema, T.: Multisets and structural congruence of the pi-calculus with replication. Theor. Comput. Sci.˜211(1-2), 311–337 (1999) · Zbl 0912.68125 · doi:10.1016/S0304-3975(97)00179-5

[12] Finkel, A., Goubault-Larrecq, J.: Forward Analysis for WSTS, Part I: Completions. In: STACS. Dagstuhl Sem. Proc., vol.˜09001, pp. 433–444 (2009) · Zbl 1236.68183

[13] Finkel, A., Goubault-Larrecq, J.: Forward Analysis for WSTS, Part˜II: Complete WSTS. In: Albers, S., Marchetti-Spaccamela, A., Matias, Y., Nikoletseas, S., Thomas, W. (eds.) ICALP 2009, Part II. LNCS, vol.˜5556, pp. 188–199. Springer, Heidelberg (2009) · Zbl 1248.68352 · doi:10.1007/978-3-642-02930-1$_1$6

[14] Finkel, A., Schnoebelen, P.: Well-structured transition systems everywhere! Theor. Comput. Sci.˜256(1-2), 63–92 (2001) · Zbl 0973.68170 · doi:10.1016/S0304-3975(00)00102-X

[15] Ganty, P., Raskin, J.-F., Van Begin, L.: A Complete Abstract Interpretation Framework for Coverability Properties of WSTS. In: Emerson, E.A., Namjoshi, K.S. (eds.) VMCAI 2006. LNCS, vol.˜3855, pp. 49–64. Springer, Heidelberg (2005) · Zbl 1176.68119 · doi:10.1007/11609773$_4$

[16] Geeraerts, G., Raskin, J.-F., Van Begin, L.: Expand, Enlarge and Check: New algorithms for the coverability problem of WSTS. J. Comput. Syst. Sci.˜72(1), 180–203 (2006) · Zbl 1105.68084 · doi:10.1016/j.jcss.2005.09.001

[17] Goubault-Larrecq, J.: On noetherian spaces. In: LICS, pp. 453–462. IEEE Computer Society (2007)· doi:10.1109/LICS.2007.34

[18] Haller, P., Odersky, M.: Scala actors: Unifying thread-based and event-based programming. Theor. Comput. Sci.˜410(2-3), 202–220 (2009) · Zbl 1162.68396 · doi:10.1016/j.tcs.2008.09.019

[19] Joshi, S., König, B.: Applying the Graph Minor Theorem to the Verification of Graph Transformation Systems. In: Gupta, A., Malik, S. (eds.) CAV 2008. LNCS, vol.˜5123, pp. 214–226. Springer, Heidelberg (2008) · Zbl 1155.68410 · doi:10.1007/978-3-540-70545-1$_2$1

[20] Karp, R.M., Miller, R.E.: Parallel program schemata. J. Comput. Syst. Sci.˜3(2), 147–195 (1969) · Zbl 0198.32603 · doi:10.1016/S0022-0000(69)80011-5

[21] Lift. Lift web framework, http://liftweb.net/

[22] Meyer, R.: On boundedness in depth in the pi-calculus. In: IFIP TCS. IFIP, vol.˜273, pp. 477–489. Springer, Boston (2008)

[23] Milner, E.C.: Basic wqo- and bqo-theory. Graphs and order (1985) · Zbl 0573.06002

[24] Milner, R.: The polyadic pi-calculus: A tutorial. In: Logic and Algebra of Specification. Computer and Systems Sciences. Springer, Heidelberg (1993)

[25] Petri, C.A., Reisig, W.: Scholarpedia˜3(4), 6477 (2008), http://www.scholarpedia.org/article/Petri_net

[26] Rival, X., Mauborgne, L.: The trace partitioning abstract domain. ACM Trans. Program. Lang. Syst.˜29(5) (2007) · Zbl 05459396 · doi:10.1145/1275497.1275501

[27] Schnoebelen, P.: Revisiting Ackermann-Hardness for Lossy Counter Machines and Reset Petri Nets. In: Hliněný, P., Kučera, A. (eds.) MFCS 2010. LNCS, vol.˜6281, pp. 616–628. Springer, Heidelberg (2010) · Zbl 1287.68059 · doi:10.1007/978-3-642-15155-2$_5$4

[28] Wies, T., Zufferey, D., Henzinger, T.A.: Forward Analysis of Depth-Bounded Processes. In: Ong, L. (ed.) FOSSACS 2010. LNCS, vol.˜6014, pp. 94–108. Springer, Heidelberg (2010) · Zbl 1284.68419 · doi:10.1007/978-3-642-12032-9$_8$

[29] Zufferey, D., Wies, T.: Picasso Analyzer, http://ist.ac.at/˜zufferey/picasso/

[30] Zufferey, D., Wies, T., Henzinger, T.A.: On ideal abstractions for well-structured transition systems. Technical Report IST-2011-10, IST Austria (November 2011) · Zbl 1326.68205