Günther, Henning; **Laarman, Alfons**; **Sokolova, Ana**; **Weissenbacher, Georg**

Dynamic reductions for model checking concurrent software. (English) Zbl 06687360

Bouajjani, Ahmed (ed.) et al., Verification, model checking, and abstract interpretation. 18th international conference, VMCAI 2017, Paris, France, January 15–17, 2017. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 10145, 246-265 (2017)

Summary: Symbolic model checking of parallel programs stands and falls with effective methods of dealing with the explosion of interleavings. We propose a dynamic reduction technique to avoid unnecessary interleavings. By extending Lipton's original work with a notion of bisimilarity, we accommodate dynamic transactions, and thereby reduce dependence on the accuracy of static analysis, which is a severe bottleneck in other reduction techniques.

The combination of symbolic model checking and dynamic reduction techniques has proven to be challenging in the past. Our generic reduction theorem nonetheless enables us to derive an efficient symbolic encoding, which we implemented for IC3 and BMC. The experiments demonstrate the power of dynamic reduction on several case studies and a large set of SVCOMP benchmarks.

For the entire collection see [Zbl 1355.68009].

MSC:

68Q60 Specification and verification (program logics, model checking, etc.)

Cited in **1** Document

Software:

VVT; CTIGAR

Full Text: DOI

References:

[1] Alur, R., Brayton, R.K., Henzinger, T.A., Qadeer, S., Rajamani, S.K.: Partial-order reduction in symbolic state space exploration. In: Grumberg, O. (ed.) CAV 1997. LNCS, vol. 1254, pp. 340–351. Springer, Heidelberg (1997). doi: 10.1007/3-540-63166-6_34 · Zbl 1001.68080 · doi:10.1007/3-540-63166-6$_3$4

[2] Beyer, D.: The software verification competition website. http://sv-comp.sosy-lab.org/2016/

[3] Beyer, D.: Reliable and reproducible competition results with benchexec and witnesses (Report on SV-COMP 2016). In: Chechik, M., Raskin, J.-F. (eds.) TACAS 2016. LNCS, vol. 9636, pp. 887–904. Springer, Heidelberg (2016). doi: 10.1007/978-3-662-49674-9_55· doi:10.1007/978-3-662-49674-9$_5$5

[4] Beyer, D., Cimatti, A., Griggio, A., Erkan Keremoglu, M., Sebastiani, R.: Software model checking via large-block encoding. In: FMCAD, pp. 25–32. IEEE (2009)· doi:10.1109/FMCAD.2009.5351147

[5] Beyer, D., Henzinger, T.A., Théoduloz, G.: Configurable software verification: concretizing the convergence of model checking and program analysis. In: Damm, W., Hermanns, H. (eds.) CAV 2007. LNCS, vol. 4590, pp. 504–518. Springer, Heidelberg (2007). doi: 10.1007/978-3-540-73368-3_51 · Zbl 1135.68466 · doi:10.1007/978-3-540-73368-3$_5$1

[6] Birgmeier, Johannes, Bradley, Aaron, R., Weissenbacher, Georg: Counterexample to induction-guided abstraction-refinement (CTIGAR). In: Biere, Armin, Bloem, Roderick (eds.) CAV 2014. LNCS, vol. 8559, pp. 831–848. Springer, Cham (2014). doi: 10.1007/978-3-319-08867-9_55 · Zbl 06349551 · doi:10.1007/978-3-319-08867-9$_5$5

[7] Bondy, J.A., Murty, U.S.R.: Graph Theory with Applications, vol. 290. Macmillan, London (1976) · Zbl 1226.05083 · doi:10.1007/978-1-349-03521-2

[8] Bradley, A.R.: SAT-based model checking without unrolling. In: Jhala, R., Schmidt, D. (eds.) VMCAI 2011. LNCS, vol. 6538, pp. 70–87. Springer, Heidelberg (2011). doi: 10.1007/978-3-642-18275-4_7 · Zbl 1317.68109 · doi:10.1007/978-3-642-18275-4$_7$

[9] Cimatti, A., Griggio, A., Mover, S., Tonetta, S.: IC3 modulo theories via implicit predicate abstraction. In: Ábrahám, E., Havelund, K. (eds.) TACAS 2014. LNCS, vol. 8413, pp. 46–61. Springer, Heidelberg (2014). doi: 10.1007/978-3-642-54862-8_4 · Zbl 06400453 · doi:10.1007/978-3-642-54862-8$_4$

[10] Cohen, E., Lamport, L.: Reduction in TLA. In: Sangiorgi, D., Simone, R. (eds.) CONCUR 1998. LNCS, vol. 1466, pp. 317–331. Springer, Heidelberg (1998). doi: 10.1007/BFb0055631· doi:10.1007/BFb0055631

[11] Dimitrov, D., et al.: Commutativity race detection. ACM SIGPLAN Not. 49(6), 305–315 (2014)· doi:10.1145/2666356.2594322

[12] Doeppner Jr., T.W.: Parallel program correctness through refinement. In: POPL, pp. 155–169. ACM (1977)· doi:10.1145/512950.512965

[13] Dwyer, M.B., Robby, J.H., Ranganath, V.P.: Exploiting object escape, locking information in partial-order reductions for concurrent object-oriented programs. FMSD 25(2–3), 199–240 (2004) · Zbl 1090.68020

[14] Elmas, T., Qadeer, S., Tasiran, S.: A calculus of atomic actions. In: POPL, pp. 2–15. ACM (2009) · Zbl 1315.68087 · doi:10.1145/1594834.1480885

[15] Flanagan, C., Godefroid, P.: Dynamic partial-order reduction for model checking software. In: POPL, vol. 40, no. 1, pp. 110–121. ACM (2005) · Zbl 1369.68135 · doi:10.1145/1040305.1040315

[16] Flanagan, C., Qadeer, S.: Transactions for software model checking. ENTCS 89(3), 518–539 (2003). Software Model Checking · Zbl 1271.68086

[17] Flanagan, C., Qadeer, S.: A type and effect system for atomicity. In: PLDI, pp. 338–349. ACM (2003)· doi:10.1145/781131.781169

[18] Günther, H., Laarman, A., Sokolova, A., Weissenbacher, G.: Dynamic reductions for model checking concurrent software (2016). https://arxiv.org/abs/1611.09318 · Zbl 06687360

[19] Godefroid, P. (ed.): Partial-Order Methods for the Verification of Concurrent Systems. LNCS, vol. 1032. Springer, Heidelberg (1996) · Zbl 1293.68005

[20] Gribomont, E.P.: Atomicity refinement and trace reduction theorems. In: Alur, R., Henzinger, T.A. (eds.) CAV 1996. LNCS, vol. 1102, pp. 311–322. Springer, Heidelberg (1996). doi: 10.1007/3-540-61474-5_79· doi:10.1007/3-540-61474-5$_7$9

[21] Grumberg, O., Lerda, F., Strichman, O., Theobald, M.: Proof-guided under approximation-widening for multi-process systems. In: POPL, pp. 122–131. ACM (2005) · Zbl 1369.68259

[22] Gueta, G., Flanagan, C., Yahav, E., Sagiv, M.: Cartesian partial-order reduction. In: Bošnački, D., Edelkamp, S. (eds.) SPIN 2007. LNCS, vol. 4595, pp. 95–112. Springer, Heidelberg (2007). doi: 10.1007/978-3-540-73370-6_8 · Zbl 05492028 · doi:10.1007/978-3-540-73370-6$_8$

[23] Günther, H.: The Vienna verification tool website. http://vvt.forsyte.at/ . Accessed 21 Nov 2016

[24] Günther, H., Laarman, A., Weissenbacher, G.: Vienna verification tool: IC3 for parallel software. In: Chechik, M., Raskin, J.-F. (eds.) TACAS 2016. LNCS, vol. 9636, pp. 954–957. Springer, Heidelberg (2016). doi: 10.1007/978-3-662-49674-9_69· doi:10.1007/978-3-662-49674-9$_6$9

[25] Günther, H., Weissenbacher, G.: Incremental bounded software model checking. In: SPIN, pp. 40–47. ACM (2014)· doi:10.1145/2632362.2632374

[26] Henzinger, T.A., Jhala, R., Majumdar, R., Sutre, G.: Lazy abstraction. In: POPL, pp. 58–70. ACM (2002) · Zbl 1323.68374 · doi:10.1145/503272.503279

[27] Kahlon, V., Gupta, A., Sinha, N.: Symbolic model checking of concurrent programs using partial orders and on-the-fly transactions. In: Ball, T., Jones, R.B. (eds.) CAV 2006. LNCS, vol. 4144, pp. 286–299. Springer, Heidelberg (2006). doi: 10.1007/11817963_28 · Zbl 1188.68190 · doi:10.1007/11817963$_2$8

[28] Kahlon, V., Wang, C., Gupta, A.: Monotonic partial order reduction: an optimal symbolic partial order reduction technique. In: Bouajjani, A., Maler, O. (eds.) CAV 2009. LNCS, vol. 5643, pp. 398–413. Springer, Heidelberg (2009). doi: 10.1007/978-3-642-02658-4_31 · Zbl 1242.68166 · doi:10.1007/978-3-642-02658-4$_3$1

[29] Kurshan, R., Levin, V., Minea, M., Peled, D., Yenigün, H.: Static partial order reduction. In: Steffen, B. (ed.) TACAS 1998. LNCS, vol. 1384, pp. 345–357. Springer, Heidelberg (1998). doi: 10.1007/BFb0054182· doi:10.1007/BFb0054182

[30] Laarman, A.W., van de Pol, J.C., Weber, M.: Boosting multi-core reachability performance with shared hash tables. In: FMCAD, pp. 247–255. IEEE-CS (2010)

[31] Lamport, L., Schneider, F.B.: Pretending atomicity. Technical report, Cornell University (1989)

[32] Lipton, R.J.: Reduction: a method of proving properties of parallel programs. Commun. ACM 18(12), 717–721 (1975) · Zbl 0316.68015 · doi:10.1145/361227.361234

[33] McMillan, K.L.: Lazy abstraction with interpolants. In: Ball, T., Jones, R.B. (eds.) CAV 2006. LNCS, vol. 4144, pp. 123–136. Springer, Heidelberg (2006). doi: 10.1007/11817963_14 · Zbl 1188.68196 · doi:10.1007/11817963$_1$4

[34] Milner, R.: Communication and Concurrency. Prentice Hall, New York (1989) · Zbl 0683.68008

[35] Nalumasu, R., Gopalakrishnan, G.: An efficient partial order reduction algorithm with an alternative proviso implementation. FMSD 20(3), 231–247 (2002) · Zbl 1017.68069

[36] Papadimitriou, C.: The Theory of Database Concurrency Control. Principles of Computer Science Series. Computer Science Press, San Jose (1986) · Zbl 0609.68073

[37] Park, D.: Concurrency and automata on infinite sequences. In: Deussen, P. (ed.) GI-TCS 1981. LNCS, vol. 104, pp. 167–183. Springer, Berlin, Heidelberg (1981). doi: 10.1007/BFb0017309· doi:10.1007/BFb0017309

[38] Peled, D.: All from one, one for all: on model checking using representatives. In: Courcoubetis, C. (ed.) CAV 1993. LNCS, vol. 697, pp. 409–423. Springer, Heidelberg (1993). doi: 10.1007/3-540-56922-7_34· doi:10.1007/3-540-56922-7$_3$4

[39] Popeea, C., Rybalchenko, A., Wilhelm, A.: Reduction for compositional verification of multi-threaded programs. In: FMCAD, pp. 187–194. IEEE (2014)· doi:10.1109/FMCAD.2014.6987612

[40] Stoller, S.D., Cohen, E.: Optimistic synchronization-based state-space reduction. In: Garavel, H., Hatcliff, J. (eds.) TACAS 2003. LNCS, vol. 2619, pp. 489–504. Springer, Heidelberg (2003). doi: 10.1007/3-540-36577-X_36 · Zbl 1031.68085 · doi:10.1007/3-540-36577-X$_3$6

[41] Valmari, A.: Eliminating redundant interleavings during concurrent program verification. In: Odijk, E., Rem, M., Syre, J.-C. (eds.) PARLE 1989. LNCS, vol. 366, pp. 89–103. Springer, Heidelberg (1989). doi: 10.1007/3-540-51285-3_35· doi:10.1007/3-540-51285-3$_3$5

[42] Valmari, A.: Stubborn sets for reduced state space generation. In: Rozenberg, G. (ed.) ICATPN 1989. LNCS, vol. 483, pp. 491–515. Springer, Heidelberg (1991). doi: 10.1007/3-540-53863-1_36· doi:10.1007/3-540-53863-1$_3$6

[43] Wang, C., Yang, Z., Kahlon, V., Gupta, A.: Peephole partial order reduction. In: Ramakrishnan, C.R., Rehof, J. (eds.)

TACAS 2008. LNCS, vol. 4963, pp. 382–396. Springer, Heidelberg (2008). doi: 10.1007/978-3-540-78800-3_29 · Zbl 1134.68421 · doi:10.1007/978-3-540-78800-3$_2$9