Ahrendt, Wolfgang; **Dylla, Maximilian**

A system for compositional verification of asynchronous objects. (English) Zbl 1264.68050

Sci. Comput. Program. 77, No. 12, 1289-1309 (2012).

Summary: We present a semantics, calculus, and system for compositional verification of Creol, an object-oriented modelling language for concurrent distributed applications. The system is an instance of KeY, a framework for object-oriented software verification, which has so far been applied foremost to sequential Java. Building on KeY characteristic concepts, like dynamic logic, sequent calculus, symbolic execution via explicit substitutions, and the taclet rule language, the presented system addresses functional correctness of Creol models featuring local cooperative thread parallelism and global communication via asynchronous method calls. The calculus heavily operates on communication histories specified by the interfaces of Creol units. Two example scenarios demonstrate the usage of the system. This article extends the conference paper of the authors ["A verification system for distributed objects with asynchronous method calls", Lect. Notes Comput. Sci. 5885, 387–406 (2009)] with a denotational semantics of Creol and an assumption-commitment style semantics of the logic.

MSC:

68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)
68N19 Other programming paradigms (object-oriented, sequential, concurrent, automatic, etc.)
68Q55 Semantics in the theory of computing

Keywords:

verification; concurrency; semantics; object-orientation

Software:

ANTLR; ASMKeY; Boogie; Caduceus; Creol; ESC/Java; KeY-C; KeYmaera; KRAKATOA; Why3

Full Text: DOI

References:

[1] Ábrahám, E.; De Boer, F. S.; De Roever, W. -P.; Steffen, M.: An assertion-based proof system for multithreaded Java, Theoretical computer science 331, No. 2–3, 251-290 (2005) · Zbl 1070.68016 · doi:10.1016/j.tcs.2004.09.019

[2] Abrial, J. -R.: The B-book: assigning programs to meanings, (1996) · Zbl 0915.68015

[3] W. Ahrendt, Using KeY, in: Beckert et al. [12], pp. 409–451.

[4] W. Ahrendt, F.S. de Boer, I. Grabe, Abstract object creation in dynamic logic, in: A. Cavalcanti, D. Dams (Eds.), Proc. 16th International Symposium on Formal Methods, FM'09, in: LNCS, Springer, 2009 (in press).

[5] Ahrendt, W.; Dylla, M.: A verification system for distributed objects with asynchronous method calls, Lncs 5885, 387-406 (2009)

[6] Apt, K.; Francez, N.; De Roever, W.: A proof system for communicating sequential processes, ACM transactions on programming languages and systems 2, 359-385 (1980) · Zbl 0468.68023 · doi:10.1145/357103.357110

[7] Jr., H. C. Baker; Hewitt, C.: The incremental garbage collection of processes, SIGPLAN notices 12, No. 8, 55-59 (1977)

[8] Barnett, M.; Chang, B. -Y.E.; Deline, R.; Jacobs, B.; Leino, K. R. M.: Boogie: a modular reusable verifier for object-oriented programs, Lncs 4111, 364-387 (2006)

[9] Barnett, M.; Deline, R.; Fändrich, M.; Leino, K. R. M.; Schulte, W.: Verification of object-oriented programs with invariants, Journal of object technology 3, No. 6, 27-56 (2004)

[10] Barnett, M.; Naumann, D.: Friends need a bit more: maintaining invariants over shared state, Lncs 3125, 54-84 (2004) · Zbl 1106.68338 · doi:10.1007/b98756

[11] M. Baum, Proof Visualization, Studienarbeit, Department of Computer Science, University of Karlsruhe, 2006.

[12] , Lncs 4334 (2007)

[13] Beckert, B.; Klebanov, V.: A dynamic logic for deductive verification of concurrent programs, Conference on software engineering and formal methods (2007)

[14] B. Beckert, V. Klebanov, S. Schlager, Dynamic logic, in: Beckert et al. [12], pp. 69–177. · Zbl 0988.03051

[15] J.C. Blanchette, Verification of assertions in Creol programs, Master's Thesis, University of Oslo, Oslo, Norway, May 2008.

[16] R. Bubel, The Schorr-Waite-Algorithm, in: Beckert et al. [12], pp. 569–587.

[17] R. Bubel, R. Hähnle, Pattern-driven formal specification, in: Beckert et al. [12], pp. 295–315.

[18] Dahl, O. -J.: Can program proving be made practical?, LES fondements de la programmaion, No. December, 57-114 (1977)

[19] M.A.D. Darab, Towards a GUI for program verification with KeY, Master's Thesis, Chalmers University of Technology, Gothenburg, Sweden, January 2010.

[20] De Boer, F. S.; Clarke, D.; Johnsen, E. B.: A complete guide to the future, Lncs 4421, 316-330 (March 2007)

[21] De Boer, F. S.; Grabe, I.; Jaghoori, M. M.; Stam, A.; Yi, W.: Modeling and analysis of thread-pools in an industrial communication platform, Lecture notes in computer science 5885, 367-386 (2009)

[22] De Roever, W. -P.; De Boer, F.; Hannemann, U.; Hooman, J.; Lakhnech, Y.; Poel, M.; Zwiers, J.: Concurrency verification: introduction to compositional and noncompositional methods, Cambridge tracts in theoretical computer science 54 (November 2001) · Zbl 1009.68020

[23] Deboer, F. S.: A Hoare logic for dynamic networks of asychronously communicating deterministic processes, Theoretical computer science 274, No. 1–2, 3-41 (2002) · Zbl 0992.68026 · doi:10.1016/S0304-3975(00)00304-2

[24] J. Dovland, E.B. Johnsen, O. Owe, A Hoare logic for concurrent objects with asynchronous method calls, Technical Report 315, Department of Informatics, University of Oslo, 2006.

[25] J. Dovland, E.B. Johnsen, O. Owe, A compositional proof system for dynamic object systems, Technical Report 351, Department of Informatics, University of Oslo, 2008.

[26] Dovland, J.; Johnsen, E. B.; Owe, O.: Observable behavior of dynamic systems: component reasoning for concurrent objects, Electronic notes in theoretical computer science 203, No. 3, 19-34 (2008) · Zbl 1277.68056

[27] M. Dylla, A verification system for the distributed object-oriented language Creol, Master's Thesis, Chalmers University of Technology, Gothenburg, Sweden, June 2009.

[28] Engel, C.; Hähnle, R.: Generating unit tests from formal proofs, Lncs 4454 (2007) · Zbl 1196.68046

[29] Fidge, C. J.: Timestamps in message-passing systems that preserve the partial ordering, Australian computer science communications 10, 55-66 (1988)

[30] Filliâtre, J. -C.; Marché, C.: The why/krakatoa/caduceus platform for deductive program verification, Lncs 4590 (2007)

[31] Flanagan, C.; Leino, K. R. M.; Lillibridge, M.; Nelson, G.; Saxe, J. B.; Stata, R.: Extended static checking for Java, , 234-245 (2002)

[32] M. Giese, First-order logic, in: Beckert et al. [12], pp. 21–68.

[33] Harel, D.; Kozen, D.; Tiuryn, J.: Dynamic logic, (2000) · Zbl 0976.68108

[34] Hoare, C. A. R.: An axiomatic basis for computer programming, Communications of the ACM 12, No. 10, 576-580 (1969) · Zbl 0179.23105 · doi:10.1145/363235.363259

[35] Hoare, C. A. R.: Communicating sequential processes, (1985) · Zbl 0637.68007

[36] J. Hooman, W.-P. de Roever, P. Pandya, Q. Xu, P. Zhou, H. Schepers, A compositional approach to concurrency and its applications, Unfinished manuscript. Available online at http://www.informatik.uni-kiel.de/inf/deRoever/books/, April 2003.

[37] Jacobs, B.; Leino, K. R. M.; Piessens, F.; Schulte, W.: Safe concurrency for aggregate objects with invariants, , 137-147 (2005)

[38] Johnsen, E. B.; Blanchette, J. C.; Kyas, M.; Owe, O.: Intra-object versus inter-object: concurrency and reasoning in creol, Electronic notes in theoretical computer science 243, 89-103 (2009)

[39] Johnsen, E. B.; Owe, O.: A compositional formalism for object viewpoints, Proceedings of the 5th international conference on formal methods for open object-based distributed systems, 45-60 (March 2002) · Zbl 1056.68103

[40] Johnsen, E. B.; Owe, O.: An asynchronous communication model for distributed concurrent objects, , 188-197 (September 2004)

[41] Johnsen, E. B.; Owe, O.: Object-oriented specification and open distributed systems, Lncs 2635, 137-164 (2004) · Zbl 1278.68067

[42] Johnsen, E. B.; Owe, O.: An asynchronous communication model for distributed concurrent objects, Software and systems modeling 6, No. 1, 35-58 (2007)

[43] Johnsen, E. B.; Owe, O.; Yu, I. C.: Creol: a type-safe object-oriented model for distributed concurrent systems, Theoretical computer science 365, No. 1–2 (2006) · Zbl 1118.68031 · doi:10.1016/j.tcs.2006.07.031

[44] C.B. Jones, Development Methods for Computer Programs Including a Notion of Interference, Ph.D. Thesis, Oxford University, UK, 1981.

[45] Liskov, B.; Shrira, L.: Promises: linguistic support for efficient asynchronous procedure calls in distributed systems, , 260-267 (1988)

[46] Milner, R.: A calculus for communicating systems, Lncs 92 (1980) · Zbl 0452.68027

[47] Milner, R.: Communicating and mobile systems: the pi calculus, (1999) · Zbl 0942.68002

[48] Misra, J.; Chandy, K.: Proofs of networks and processes, IEEE transactions on software engineering 7, No. 7, 417-426 (1981)

· Zbl 0468.68030

[49] W. Mostowski, The Demoney case study, in: Beckert et al. [12], pp. 533–568.

[50] Mostowski, W.: Fully verified Java card API reference implementation, Ceur ws 259 (July 2007)

[51] Mürk, O.; Larsson, D.; Hähnle, R.: Key-C: a tool for verification of C programs, Lncs 4603, 385-390 (2007)

[52] S. Nanchen, H. Schmid, P.H. Schmitt, R. Stärk, The ASMKeY theorem prover, Technical Report 436, ETH Zürich, 2004.

[53] Owicki, S. S.; Gries, D.: An axiomatic proof technique for parallel programs, Acta informatica 6, 319-340 (1976) · Zbl 0312.68011 · doi:10.1007/BF00268134

[54] Parr, T.: The definitive ANTLR reference: building domain-specific languages, (2007)

[55] Platzer, A.; Quesel, J. -D.: Keymaera: a hybrid theorem prover for hybrid systems, Lncs 5195, 171-178 (2008) · Zbl 1165.68469 · doi:10.1007/978-3-540-71070-7_15

[56] P. Rümmer, Construction of proofs, in: Beckert et al. [12], pp. 179–242.

[57] Schmitt, P. H.; Tonin, I.: Verifying the mondex case study, Proc. 5. IEEE int. Conf. on software engineering and formal methods, 47-56 (2007)

[58] Soundararajan, N.: Axiomatic semantics of communicating sequential processes, ACM transactions on programming languages and systems 6, No. 4, 647-662 (1984) · Zbl 0542.68013 · doi:10.1145/1780.1805

[59] Zwiers, J.: Compositionality, concurrency and partial correctness, Lncs 321 (1989) · Zbl 0674.68011