Din, Crystal Chang; **Dovland, Johan**; **Johnsen, Einar Broch**; **Owe, Olaf**

Observable behavior of distributed systems: component reasoning for concurrent objects.

(English) Zbl 1247.68184
J. Log. Algebr. Program. 81, No. 3, 227-256 (2012).

Summary: Distributed and concurrent object-oriented systems are difficult to analyze due to the complexity of their concurrency, communication, and synchronization mechanisms. Rather than performing analysis at the level of code in, e.g., Java or C++, we consider the analysis of such systems at the level of an abstract, executable modeling language. This language, based on concurrent objects communicating by asynchronous method calls, avoids some difficulties of mainstream object-oriented programming languages related to compositionality and aliasing. To facilitate system analysis, compositional verification systems are needed, which allow components to be analyzed independently of their environment. In this paper, a proof system for partial correctness reasoning is established based on communication histories and class invariants. A particular feature of our approach is that the alphabets of different objects are completely disjoint. Compared to related work, this allows the formulation of a much simpler Hoare-style proof system and reduces reasoning complexity by significantly simplifying formulas in terms of the number of needed quantifiers. The soundness and relative completeness of this proof system are shown using a transformational approach from a sequential language with a non-deterministic assignment operator.

MSC:

68Q85 Models and methods for concurrent and distributed computing (process algebras, bisimulation, transition nets, etc.)
68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)
68M14 Distributed systems
03B70 Logic in computer science

Keywords:

distributed systems; object-orientation; compositional reasoning; Hoare logic; concurrent objects

Software:

JCobox; ABS; Java Jr

Full Text: DOI

References:

[1] Ábrahám, E.; Grabe, I.; Grüner, A.; Steffen, M., Behavioral interface description of an object-oriented language with futures and promises, J. logic algebr. programming, 78, 7, 491-518, (2009) · Zbl 1187.68130

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

[3] W. Ahrendt, M. Dylla, A system for compositional verification of asynchronous objects, Sci. Comput. Programming, in press. doi:10.1016/j.scico.2010.08.003. Available from: <http://www.sciencedirect.com/science/article/B6V17-50TRX0X-1/2/80b594aa8b2596602fdbd0d · Zbl 1264.68050

[4] Alpern, B.; Schneider, F.B., Defining liveness, Inform. process. lett., 21, 4, 181-185, (1985) · Zbl 0575.68030

[5] Apt, K.R., Ten years of hoare's logic: a survey – part I, ACM trans. program. lang. syst., 3, 4, 431-483, (1981) · Zbl 0471.68006

[6] Apt, K.R., Ten years of hoare's logic: a survey – part II: nondeterminism, Theoret. comput. sci., 28, 1-2, 83-109, (1984) · Zbl 0523.68015

[7] ()

[8] Broy, M.; Stølen, K., Specification and development of interactive systems, Monographs in computer science, (2001), Springer-Verlag

[9] Dahl, O.-J., Can program proving be made practical?, (), 57-114

[10] Dahl, O.-J., Verifiable programming, International series in computer science, (1992), Prentice Hall New York, NY

[11] Dahl, O.-J., Object-oriented specifications, (), 561-576

[12] O.-J. Dahl, O. Owe, Formal Methods and the RM-ODP, Research Report 261, Department of Informatics, University of Oslo, Norway, May 1998.

[13] de Boer, F.S., A Hoare logic for dynamic networks of asynchronously communicating deterministic processes, Theoret. comput. sci., 274, 3-41, (2002) · Zbl 0992.68026

[14] de Boer, F.S.; Pierik, C., How to cook a complete Hoare logic for your pet OO language, (), 111-133 · Zbl 1104.68428

[15] de Boer, F.S.; Clarke, D.; Johnsen, E.B., A complete guide to the future, (), 316-330

[16] C.C. Din, J. Dovland, E.B. Johnsen, O. Owe, Observable behavior of distributed systems: component reasoning for concurrent objects, Research Report 401, Department of Informatics, University of Oslo, Norway, October 2010. · Zbl 1247.68184

[17] Dovland, J.; Johnsen, E.B.; Owe, O., Verification of concurrent objects with asynchronous method calls, (), 141-150

[18] Dovland, J.; Johnsen, E.B.; Owe, O., Observable behavior of dynamic systems: component reasoning for concurrent objects, Electron. notes theor. comput. sci., 203, 3, 19-34, (2008) · Zbl 1277.68056

[19] Dovland, J.; Johnsen, E.B.; Owe, O.; Steffen, M., Lazy behavioral subtyping, J. logic algebr. programming, 79, 7, 578-607, (2010) · Zbl 1204.68072

[20] Johnsen, E.B.; Hähnle, R.; Schäfer, J.; Schlatte, R.; Steffen, M., ABS: A core language for abstract behavioral specification, (), 142-164

[21] Hoare, C.A.R., Communicating sequential processes, International series in computer science, (1985), Prentice Hall · Zbl 0637.68007

[22] International Telecommunication Union, Open Distributed Processing - Reference Model Parts 1-4, Tech. Rep., ISO/IEC, Geneva, July 1995.

[23] Jeffrey, A.S.A.; Java, J. Rathke, Fully abstract trace semantics for a core Java language, (), 423-438 · Zbl 1108.68349

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

[25] Johnsen, E.B.; Owe, O., An asynchronous communication model for distributed concurrent objects, Software syst. model., 6, 1, 35-58, (2007)

[26] Olderog, E.-R.; Apt, K.R., Fairness in parallel programs: the transformational approach, ACM trans. program. lang., 10, 3, 420-455, (1988)

[27] C. Pierik, F.S. d. Boer, A Syntax-Directed Hoare Logic for Object-Oriented Programming Concepts, Tech. Rep. UU-CS-2003-010, Department of Information and Computing Sciences, Utrecht University, 2003. · Zbl 1253.68087

[28] Schäfer, J.; Poetzsch-Heffter, A., Jcobox: generalizing active objects to concurrent components, (), 275-299

[29] Soundararajan, N., Axiomatic semantics of communicating sequential processes, ACM trans. program. lang. syst., 6, 4, 647-662, (1984) · Zbl 0542.68013

[30] Soundararajan, N., A proof technique for parallel programs, Theoret. comput. sci., 31, 1-2, 13-29, (1984) · Zbl 0543.68010