Dovland, Johan; **Johnsen, Einar Broch**; **Owe, Olaf**

Observable behavior of dynamic systems: component reasoning for concurrent objects. (English) Zbl 1277.68056

Goldin, Dina (ed.) et al., Proceedings of the workshop on the foundations of interactive computation (FinCo 2007), Braga, Portugal, March 31, 2007. Amsterdam: Elsevier. Electronic Notes in Theoretical Computer Science 203, No. 3, 19-34 (2008).

Summary: Current object-oriented approaches to distributed programs may be criticized in several respects. First, method calls are generally synchronous, which leads to much waiting in distributed and unstable networks. Second, the common model of thread concurrency makes reasoning about program behavior very challenging. Models based on concurrent objects communicating by asynchronous method calls, have been proposed to combine object orientation and distribution in a more satisfactory way. In this paper, a high-level language and proof system are developed for such a model, emphasizing simplicity and modularity. In particular, the proof system is used to derive external specifications of observable behavior for objects, encapsulating their state. A simple and compositional proof system is paramount to allow verification of real programs. The proposed proof rules are derived from the Hoare rules of a standard sequential language by a semantic encoding preserving soundness and relative completeness. Thus, the paper demonstrates that these models not only address the first criticism above, but also the second.

For the entire collection see [Zbl 1276.68017].

MSC:

68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)
68N19 Other programming paradigms (object-oriented, sequential, concurrent, automatic, etc.)
68Q85 Models and methods for concurrent and distributed computing (process algebras, bisimulation, transition nets, etc.)

Keywords:

observable behavior; concurrent objects; dynamic systems; interaction histories

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, 2-3, 251-290, (2005) · Zbl 1070.68016

[2] Alpern, B.; Schneider, F.B., Defining liveness, Information processing letters, 21, 4, 181-185, (Oct. 1985)

[3] Apt, K.R., Ten years of Hoare's logic: A survey — part I, ACM transactions on programming languages and systems, 3, 4, 431-483, (Oct. 1981)

[4] Apt, K.R., Ten years of Hoare's logic: A survey — part II: nondeterminism, Theoretical computer science, 28, 1-2, 83-109, (Jan. 1984)

[5] ()

[6] Hansen, P. Brinch, Java's insecure parallelism, ACM SIGPLAN notices, 34, 4, 38-45, (Apr. 1999)

[7] Broy, M., Distributed concurrent object-oriented software, (), 83-96

[8] Broy, M.; Stølen, K., Specification and development of interactive systems, Monographs in computer science, (2001), Springer · Zbl 0981.68115

[9] Cenciarelli, P.; Knapp, A.; Reus, B.; Wirsing, M., An event-based structural operational semantics of multi-threaded Java, (), 157-200

[10] de Boer, F.S., A Hoare logic for dynamic networks of asynchronously communicating deterministic processes, Theoretical computer science, 274, 3-41, (2002) · Zbl 0992.68026

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

[12] Dijkstra, E.W., Guarded commands, nondeterminacy and formal derivation of programs, Communications of the ACM, 18, 8, 453-457, (Aug. 1975)

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

[14] J. Dovland, E.B. Johnsen, and O. Owe. A compositional proof system for dynamic object systems. Research Report 351, Department of Informatics, University of Oslo, Norway, Feb. 2007 · Zbl 1277.68056

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

[16] Huisman, M.; Jacobs, B., Java program verification via a Hoare logic with abrupt termination, (), 284-303

[17] International Telecommunication Union. Open Distributed Processing - Reference Model parts 1-4. Technical report, ISO/IEC, Geneva, July 1995

[18] Johnsen, E.B.; Owe, O., An asynchronous communication model for distributed concurrent objects, Software and systems modeling, 6, 1, 35-58, (Mar. 2007)

[19] Morris, J.M., A general axiom of assigment, (), 25-34

[20] Olderog, E.-R.; Apt, K.R., Fairness in parallel programs: the transformational approach, ACM transactions on programming languages, 10, 3, 420-455, (July 1988)

[21] Poetzsch-Heffter, A.; Müller, P., A programming logic for sequential Java, (), 162-176

[22] Reus, B.; Wirsing, M.; Hennicker, R., A Hoare calculus for verifying Java realizations of OCL-constrained design models, (), 300-317 · Zbl 0977.68858

[23] Soundararajan, N., Axiomatic semantics of communicating sequential processes, ACM transactions on programming languages and systems, 6, 4, 647-662, (Oct. 1984)

[24] Soundararajan, N., A proof technique for parallel programs, Theoretical computer science, 31, 1-2, 13-29, (May 1984)