# Deductive Verification of Cache Coherence Protocols*

[ABSTRACT]

Michael Fisher and Alexei Lisitsa

Department of Computer Science, University of Liverpool, Liverpool L69 7ZF, U.K.
{M.Fisher,A.Lisitsa}@csc.liv.ac.uk

Local cache techniques[Han93] are important in shared-memory multiprocessor systems because they allows the reduction of both memory access latency and network traffic. In such techniques, each processor has its own fast memory cache, holding local copies of main memory blocks. While reducing the access time this approach poses the problem of cache consistency, whereby one has to ensure that the copies of the *same* memory block in the caches of *different* processors are consistent. Such data consistency can be provided by *cache coherence protocols*, which typically operate as follows: every processor is equipped with a finite state control, which *reacts* to the *read* and *write* requests. Abstracting from the low-level implementation details of read, write and synchronization primitives, one may consider cache coherence protocols as families of identical finite state machines together with a primitive form of communication: if one automaton makes a transition (an action) $a$, then it is required that all other automata simultaneosly make a complementary transition (reaction) $\bar{a}$. Correctness at that level of abstraction can be expressed in terms of co-occurrences some states in which, for example, the processors are allowed the change the content of their cache copies.

The paper [PD97] gives a good survey of verification methods used to prove correctness of cache coherence protocols. If the number of processors is fixed, verification can be carried out by traditional model checking methods [CGP00].

More challenging is the problem of verification of cache coherence protocols for *every* possible number of processors (termed "parameterized cache coherence protocols"). In [Del, Del03] *parameterized model checking* based on constraint technology has been applied and it has been shown to be a method that is complete for a class of protocols and correctness conditions.

We suggest here an alternative route for the verification of parametrized cache coherence protocols:

- by first translating into monodic first-order temporal specifications [DF01, BDFL02] and
- then applying temporal theorem proving [Fis91, FDP01, DF01, BDFL02].

In order to achieve this, we provide a faithful translation from the finite state model of cache protocols [PD95] to monodic temporal specifications [DF01, BDFL02] and demonstrate two proof methods suitable for the proof of correctness of cache coherence protocols. The applicability of these methods is illustrated by the examples of cache coherence protocols from [Del].

* This work was supported by EPSRC, through research grant GR/M46631.

Both theoretical and practical aspects need to be understood better. Theoretically, we would like to have a method that is provably complete for a class of specifications. From the practical viewpoint we intend to adapt and optimize our implementation of the resolution based proof method [LB02] in order to verify all cache coherence protocols from [Del] in pure automatic way. That would provide us with an answer to the question of whether our methods can compete with those based on reduction to arithmetical constraints [Del].

## References


[BDFL02] J. Brotherston, A. Degtyarev, M. Fisher and A. Lisitsa, Searching for Invariants using Temporal Resolution, in Proceeding of 9th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR), Tbilisi, Georgia, 2002, LNAI 2514, Springer, pp 86–101

[CGP00] E. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, Dec. 1999.

[DF01] A. Degtyarev and M. Fisher. Towards first-order temporal resolution. In *Proccedings of KI-2001*, volume 2174 of *LNAI*, 2001.

[Del] G. Delzanno. Automatic verification of parametrized cache coherence protocols. At Web page http://www.disi.unige.it/person/DelzannoG/protocol.html, 27pp.

[Del03] G. Delzanno. Constraint-based Verification of Parametrized Cache Coherence Protocols. to appear in Formal Methods in System Design.

[FDP01] M. Fisher, C. Dixon, and M. Peim. Clausal temporal resolution. *ACM Transactions on Computation Logic*, 2(1), January 2001.

[Fis91] M. Fisher. A resolution method for temporal logic. In *Proc. Twelfth International Joint Conference on Artificial Intelligence (IJCAI)*. Morgan Kaufman, 1991.

[Fis97] M. Fisher. A normal form for temporal logics and its applications in theorem-proving and execution. *Journal of Logic and Computation*, 7(4), 1997.

[Han93] J. Handy. The Cache memory Book. ACademic Press, 1993.

[HWZ00] I. Hodkinson, F. Wolter, and M. Zakharyaschev. Fragments of first-order temporal logics. *Annals of Pure and Applied logic*, 106:85–134, 2000.

[LB02] A. Lisitsa, J. Brotherston, Implementing Invariant search via Temporal resolution, in Proceeding of 2nd Workshop on the Implementation of logics, Tbilisi, Georgia, 2002.

[PD95] F. Pong, M. Dubois. A new approach for the Verfication of Cache Coherence Protocols. IEEE Transactions on Parallel and Disributed Systems 6(8), 1995.

[PD97] F. Pong, M. Dubois. Verification techniques for cache coherence protocols. ACM Computing Surevyes 29(1): 82–126,1997.