Case Studies for First-Order Temporal Logic*

M.Carmen Fernández Gago, Michael Fisher, Clare Dixon,
Boris Konev, Ullrich Hustadt and Frank Wolter
Logic and Computation Group
Department of Computer Science,
University of Liverpool,
L69 7ZF, United Kingdom
Email: {mcarmen,michael,clare,konev,ullrich,frank}@csc.liv.ac.uk

Discrete linear temporal logic has been widely used in Computer Science and Artificial Intelligence, in particular, for the formal specification and verification of concurrent and distributed systems [MP92, Pnu77]. Although it is well known that *first-order* temporal logic is a powerful tool for these fields, its use has been avoided. The main reason is that this logic is not even semi-decidable. However, recent work [HWZ00] has shown that a fragment of first-order temporal logic, called the *monodic* fragment is complete. This has led to the development of proof techniques for this fragment. Thus, the main aim of this project (carried out by King's College, London and the University of Liverpool) is to develop, implement and apply verification methods for this fragment of first-order temporal logic. So far, a tableaux-based procedure for the monodic fragment has been presented in [KLWZ03] and a clausal resolution-based method for the same fragment has been defined in [DF01, DFK03] and been proved complete. In [KDD$^+$03] this resolution method has been refined for the case of expanding domains in order to make it more suitable for implementation. The latter techniques are based upon the resolution method for temporal logic defined in [FDP01].

First-order temporal logic is an extension of classical first-order logic with the addition of operators that deal with a linear and discrete model of time (isomorphic to $\mathbb{N}$). These temporal operators are $\Box$ (' always in the future'), $\bigcirc$ ('at the next moment in time'), $\Diamond$ ('sometime in the future'), $\mathcal{U}$ (until) and $\mathcal{W}$ (unless or weak until). The language also contains the usual features of a first-order language, (predicate symbols, variables, constants, quantifiers, boolean operators), the main being restricition that it is monodic, i.e. formulae containing a temporal operator contain at most one free variable.

TeMP [HKRV04] is an automatic theorem prover for the monodic fragment of first-order logic. The prover is based on *fine-grained resolution* [KDD$^+$03]. Monodic formulae are translated into a normal form preserving satisfiability, called *Divided Separated Normal Form* (DSNF). Then, the resolution calculus is applied. It consists of *fine-grained step resolution* (or resolution beteween states) and *fine-grained eventuality resolution* rule (or resolution over states).

TeMP is an extension of the propositional temporal prover TRP++ [HK03, HK02], where TRP++ is an implementation of the temporal resolution method described in [FDP01] for PTL (Propositional Temporal Logic).

In the future we intend to use TeMP in order to verify propeties of case studies that fall into the monodic first-order temporal logic category. Currently, we are investigating the possibility of translating into the monodic fragment of first-order

*This work was partially supported by EPSRC grant GR/R45376/01.

temporal logic, some security protocols. These security protocols have been specified using temporal logics of knowledge and verified (by hand) [DFGFvdH03] using a method developed for this logic based upon resolution. We also intend to verify properties of security protocols specified in temporal logics of knowledge and beliefs and other suitable examples.

References

[DF01] A. Degtyarev and M. Fisher. Towards First-Order Temporal Resolution. In *Proceedings of KI, the 24th German Conference on Artifical Intelligence*, volume 2174 of *LNCS*, pages 18–32. Springer, 2001.

[DFGFvdH03] C. Dixon, M.C. Fernández-Gago, M. Fisher, and W. van der Hoek. Using Temporal Logics of Knowledge in the Formal Verification of Security Protocols. Technical Report 03-022, ULCS, http://www.csc.liv.ac.uk/research, 2003.

[DFK03] A. Degtyarev, M. Fisher, and B. Konev. Monodic Temporal Resolution. In *Automated Deduction CADE-19*, LNAI. Springer, 2003.

[FDP01] M. Fisher, C. Dixon, and M. Peim. Clausal Temporal Resolution. In *Transactions on Computational Logic 2(1)*, January 2001.

[HK02] U. Hustadt and B. Konev. TRP++: A Temporal Resolution Prover. In *Proceedings of the Third International Workshop on the Implemetation of Logics*, October 2002.

[HK03] U. Hustadt and Boris Konev. Trp++ 2.0: A temporal resolution prover. In F. Baader, editor, *Automated Deduction—CADE-19*, volume 2741 of *LNAI*, pages 274–278. Springer, 2003.

[HKRV04] U. Hustadt, B. Konev, A. Riazanov, and A. Voronkov. TeMP: A Temporal Monodic Prover. Technical Report 04-004, ULCS, http://www.csc.liv.ac.uk/research, 2004.

[HWZ00] I. Hodkinson, F. Wolter, and M. Zakharyaschev. Decidable fragments of First-Order Temporal Logic. *Annals of Pure and Applied Logic*, 106:85–134, 2000.

[KDD+03] B. Konev, A. Degtyarev, C. Dixon, M. Fisher, and U. Hustadt. Towards the Implementation of First-Order Temporal Resolution: the Expanding Domain Case. In *Proceedings of the 10th International Symposium on Temporal Representation and Reasoning (TIME-ICTL)*, IEEE Comouter Society Press, 2003.

[KLWZ03] R. Kontchakov, C. Lutz, F. Wolter, and M. Zakharyaschev. Temporalising tableaux. *Studia Logica*, 76(1):91–134, 2003.

[MP92] Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Specification.* Springer-Verlag, New York, 1992.

[Pnu77] A. Pnueli. The Temporal Logic of Programs. In *Proceedings of the 18th Symposium on the Foundations of Computer Science*, Providence, November 1977.