“Easy” Parameterized Verification of Cross Clock-Domain Protocols

Geoffrey Brown

Indiana University
Department of Computer Science

Lee Pike

Galois Connections, Inc.

We will present recent work that exploited the bounded model checker and ICS decision procedures of SAL to develop fully parameterized proofs of two types of protocols designed to cross synchronous boundaries: a simple data synchronization circuit and two serial communication protocols – 8N1 used in UARTs and biphase mark. [2, 1, 3] The proofs are parameterized by expressing temporal constraints as a system of linear equations. The proofs are ”easy” in requiring few proof steps. For example, our biphase mark proof required stating 5 invariants, whereas a published proof using PVS required 37; our proof required 5 steps, whereas the PVS proof required more than 4000. [7] Our proofs are quick to check – a few minutes computing time, while one published proof of biphase mark required five hours. Our proofs also seem to be successful in identifying potential bugs. In the case of 8N1, we identified a timing constraint error in a published application note. In the case of the data synchronization circuit, we identified a timing constraint that had not been described in published proofs based upon finite state models.

In the submitted work, we utilized a multiphase model for the circuit building blocks (e.g. flip-flops) with separate “settle” and “stable” phases as well as a “metastable” phase for those flip-flops for which the timing constraints were not met. The timing constraints under which the models were verified related to these phases. For example, the timing constraints for verification of the synchronization constraint relate the phases of the two time domains (a transmitter T and a receiver R)

```
RSETTLE  : { x : TIME | 0 < x};
TSETTLE  : { x : TIME | 0 < x};
TPERIOD  : { x : TIME | TSETTLE < x
                    AND RSETTLE < x};
RPERIOD  : { x : TIME | RSETTLE < x
                    AND TSETTLE < x};
```

In the case of the synchronizer circuit, a key timing constraint limits the settling time of state holding elements in one domain to less than the full period of the second domain. The protocol is not correct unless this constraint is met. Previous proofs of this circuit did not capture the impact of metastability and hence this timing constraint [4, 5].

While the work we have submitted for publication solves the immediate problem – verification of multi-clock domain systems under parameterized timing constraints – the technique utilized is somewhat unsatisfying in that the timing model is tightly bound to the circuit description. We are currently developing models in which issues related to timing and non-digital effects such as metastability are captured in separate constraint processes that execute in parallel with timing and metastability free models. This work is inspired by a recent paper by Seshia et. al. describing the use of ”Generalized Relative Timing.” [6] The goal of these improvements is to develop a verification style that enables proof by refinement. We will report on the state of these improvements.

References

[1] G. Brown. Verification of a data synchronization circuit for all time. Submitted to "International Conference on Asynchronous Circuits and Systems 2006, 2005.

[2] G. Brown and L. Pike. Easy parameterized verification of biphase mark and 8n1 decoders. Submiited to "Conference on Tools and Algorithms for the Construction and Analysis of Systems – ETAPS 2006", 2005.

[3] L. de Moura. SAL: tutorial. Technical report, SRI International, 2004.

[4] T. Kapschitz and R. Ginosar. Formal verification of synchronizers. In *CHARME 2005 – to appear*, 2005.

[5] T. Kapschitz, R. Ginosar, and R. Newton. Verifying synchronization in multi-clock domain SoC. In *DVCon 2004*, 2004.

[6] S. Seshia, R. E. Bryant, and K. S. Stevens. Modeling and verifying circuits using generalized relative timing. In *11th Symposium on Asynchronous Circuits and Systems*, 2005.

[7] F. W. Vaandrager and A. L. de Groot. Analysis of a biphase mark protocol with uppaal and pvs. Technical Report NIII-R0455, Nijmegen Institute for Computing and Information Science, 2004.