Modeling and Formal Verification of a Telecom System Block using MDGs

M. Hasan Zobair and Sofiène Tahar
Electrical & Computer Engineering Department, Concordia University
Montreal, Quebec, Canada
Email: {mh_zobai, tahar}@ece.concordia.ca

Abstract. *In this paper, we investigate the ability of the MDG (Multiway Decision Graph) tools to carry out the verification of an industrial Telecom System Block (TSB), commercialized by PMC-Sierra Inc. For the formal verification, we adopted a hierarchical proof methodology to handle the complexity of the design. We then carried out MDG based equivalence checking as well as model checking. To measure the performance of the MDG verification, we also conducted the verification of the same TSB with Cadence FormalCheck.*

1. Introduction

Simulation-based methods are currently used by the industrial community for system-level verification, since they can handle the entire design at a time. When a simulation trace exposes a design error, a verifier analyses the trace and rectifies the design for only one specific behavior of the system. Therefore, one cannot confirm that no other trace exposes the error. This handicap is the reason why new methods are needed for the economical and reliable verification of digital systems. Formal verification [3] has paved a path, showing the utility of finding bugs early in the design cycle. FSM-based automatic verification techniques have proven to be successful for real industrial design. However, since it requires the design to be described at the boolean level, they often fail to verify a large-scale design because of the *state space explosion* problem [3] caused by the large datapath.

In this work, we present a methodology for the formal verification of a real industrial design using Multiway Decision Graphs (MDG) [1]. The design we considered is a Telecom System Block (TSB) — **R**eceive **A**utomatic Protection Switch Control, **S**ynchronization Status Extraction and Bit **E**rror Rate Monitor (RASE), a commercial product of PMC-Sierra, Inc.[4]. The main aspect of this work is to illustrate the ability to carry out the verification process of a large industrial design using MDGs. Until recently, the Fairisle ATM (Asynchronous Transfer Mode) switch fabric [5] was the largest design verified by MDGs. This design has 4200 equivalent gates implemented in Xilinx FPGAs. In comparison, our investigated design has 11400 equivalent gates [3].

2. Modelling and Verification of the TSB

The RASE TSB processes a portion of the SONET (Synchronous Optical Network) line overhead of a received data stream. The TSB consists of three types of components: Transport overhead extraction and manipulation, Bit Error Rate Monitoring (BERM) and Interrupt Server (see Figure 1). The transport overhead extraction and manipulation functions are implemented by three sub-modules (transport overhead bytes extractor, automatic protection switch control and synchronization status filtering). In this paper, we describe a hierarchical approach to model the TSB behavior at different levels of the design hierarchy which in turn enables the verification process to be done at different levels. For MDG-based verification we translated the original VHDL models into very similar models using the Prolog-style MDG-HDL. To handle the complexity of the design, we adopted a module abstraction technique for the RTL model.

Based on the hierarchy of the design, we followed a hierarchical approach for the equivalence checking of the RASE TSB. We first verified that the RTL implementation of each module complies with the specification of its behavioral model, given as Abstract State Machine (ASM) in MDG. Thanks to the data abstraction features in MDG, we also succeeded to verify the full RTL implementation of the RASE TSB against its top level specification, give in terms of ASMs. Besides equivalence checking, we furthermore applied property checking to ascertain that both the specification and the implementation of the TSB satisfy some specific characteristics of the system. The verification of the properties was carried out by using the model checking facility of the MDG tools.

One of the motivations of this work was to compare the model checking of the *RASE TSB* using MDG model checker with an existing commercial model checking tool, here, Cadence FormalCheck [2]. While performing the property checking on the top level model of the design using FormalCheck, the verification of some of the datapath oriented properties did not terminate. As the MDG-based approach allows the abstract representation of data while the control information is extracted from the datapath using cross-operators, all of these properties could be verified in MDG. Our experimental result shows that FormalCheck is more efficient in verifying FSM-based design, i.e., concrete data, than the MDG tools (see Table 1).

3. Conclusions

We demonstrated that the Multiway Decision Graphs tools have the capability to verify a moderate size industrial Telecom hardware design. The experimental results showed that in some cases, the MDG model checker was more efficient due to the ability with MDGs to use abstract state variables and uninterpreted function symbols rather than simply a Boolean modeling as in FormalCheck.The experimental results also suggest that a hybrid MDG-FormalCheck model checking approach can be applied to improve the efficiency of formal verification in an industrial setting.

References

[1] F. Corella, Z. Zhou, X. Song, M. Langevin and E. Cerny, "Multiway Decision Graphs for Automated Hardware Verification", *Formal Methods in System Design*, Vol. 10, pp. 7-46, February 1997

[2] Cadence Design Systems, Inc., *Formal Verification Using Affirma FormalCheck*; Manual, Version 2.3, August 1999.

[3] C. Kern and M. Greenstreet, "Formal Verification in Hardware Design: A Survey," *ACM Transactions on Design Automation of E. Systems*, Vol. 4, pp. 123-193, April 1999.

[4] PMC-Sierra Inc., *Receive APS, Synchronization Status and BERM Telecom System Block Engineering Document*; Issue 4, January 29, 1998.

[5] S. Tahar, X. Song, E. Cerny, Z. Zhou, M. Langevin and O. Ait- Mohamed, "Modeling and Verification of the Fairisle ATM Switch Fabric using MDGs", *IEEE Transactions on CAD of Integrated Circuits and Systems*, Vol. 18, No. 7, pp. 956-972, July 1999.

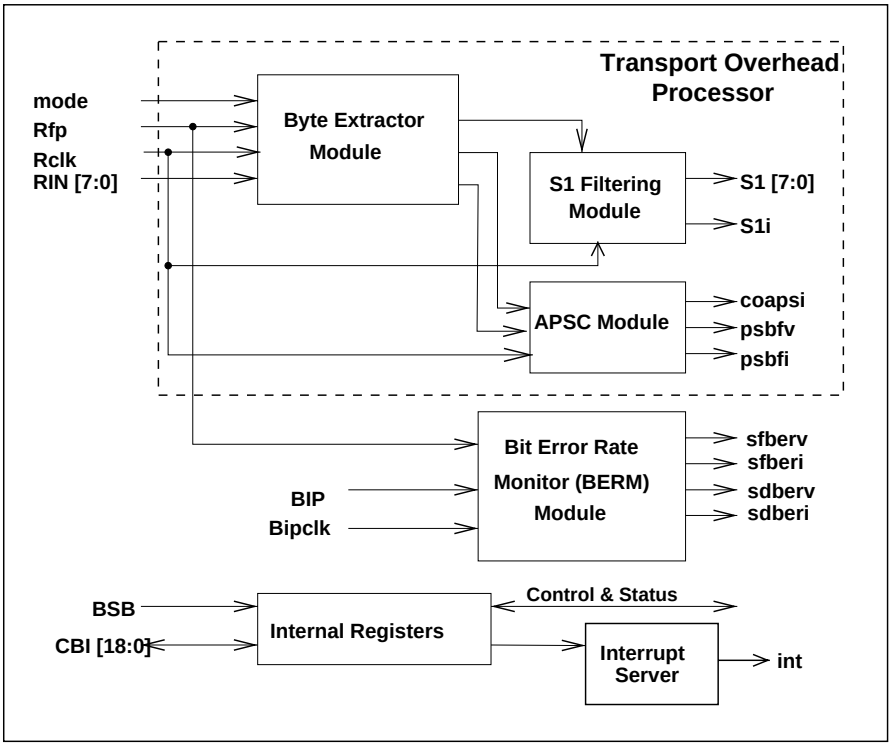

Figure 1. The RASE telecom system block

Table 1: Model checking on the RASE TSB using MDG and FormalCheck

Property	MDG model checker			FormalCheck model checker		
	Time (in Sec.)	Memory (in MB)	State variable	Time (in Sec.)	Memory (in MB)	State variable
Property 1	82.47	15.60	57	60	16.08	54
Property 6	81.65	15.80	55	10	11.75	28
Property 7	82.54	15.86	57	*	*	*
Property 8	64.30	15.72	57	*	*	*
Property 9	78.06	16.65	55	*	*	*

Note: In Table 1, the notation '*' means that the related property checking did not terminate during verification.