Well-Typed Models are Correct Models

Applying State-of-the-Art Advances in Programming Language Theory to Systems-on-a-Chip Designs

Jan de Muijnck-Hughes
University of Glasgow
School of Computing Science
Glasgow, United Kingdom
jan.deMuijnck-Hughes@glasgow.ac.uk

Wim Vanderbauwhede
University of Glasgow
School of Computing Science
Glasgow, United Kingdom
Wim.Vanderbauwhede@glasgow.ac.uk

Reference:
Jan de Muijnck-Hughes and Wim Vanderbauwhede. 2019. Well-Typed Models are Correct Models: Applying State-of-the-Art Advances in Programming Language Theory to Systems-on-a-Chip Designs. In Proceedings of Scottish Seminar on Formal Modelling, Verification, and Synthesis (SFMoVeS 19), Oana Andrei and Michele Sevegnani (Eds.).

Modern Systems-on-a-Chip (SoC) are constructed by composition of IP (Intellectual Property) Cores with the communication between these IP Cores being governed by well described interaction protocols. However, there is a disconnect between the machine readable specification of these protocols and the verification of their implementation in known hardware description languages. Although tools can be written to address such separation of concerns, the tooling is often hand written and used to check hardware designs a posteriori. Further, it is important when connecting components together that only one signal can flow along a channel.

Dependent type-systems present a rich and expressive setting that supports the precises specification of our programs properties to be stated and verified directly in the language's type-system. Such type-systems also support reasoning about a programs substructural properties in the style of substructural typing. We can use these concepts to express model invarients directly within our model's types and provide correctness-by-construction guarantees that our models adhere to external specifications, and are thus well-formed, at design-time using type checking.

In this talk I will present my ongoing work as part of the Border Patrol project to construct a modelling languague for designing Systems-on-a-Chip. Our framework, Cordial, is designed to enrich existing Hardware Description Languages, and development environments, with static design-time mechanisms that reason about the (sub)structural properties of SoC Designs using Dependent, Session, and Quantitative Typing. Cordial's type-system provides guarantees that the interfaces on an IP Core will be well-typed if they adhere to an external specification, and that we can guarantee that components are connected in a safe way by tracking the number of times a port is used within a design and comparing the interconnections ports. With Cordial mismatches between SoC specification and implementation become impossible thereby reducing errors, increasing designer productivity and enhancing safety and security of SoC designs.

Acknowledgments

This work is part of *Border Patrol: Improving Smart Device Security through Type-Aware Systems Design* and has been sponsored by an EPSRC funding call on Trust, Identity, Privacy and Security in the Digital Economy (http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/N028201/1).

SFMoVeS 19, September 09, 2019, Glasgow, UK