FORMAL VERIFICATION OF ARITHMETIC DATAPATHS USING ALGEBRAIC GEOMETRY AND SYMBOLIC COMPUTATION

A tutorial presented at FMCAD 2015
by

Priyank Kalla
Electrical and Computer Engineering, University of Utah, Salt Lake City
kalla@ece.utah.edu, http://www.ece.utah.edu/~kalla

Algebraic geometry is the study of the geometry of solutions to a system of multivariate polynomial equations. Modern algebraic geometry does not explicitly solve the system of equations to enumerate the solutions, but rather reasons about the presence, absence, dimensions or intersection properties of the solution-sets, etc. Abstract and computational algebra is often used for this purpose – particularly the theory and technology of Gröbner bases, which provides a very powerful set of tools to solve many polynomial decision problems. In this talk, I will present a tutorial on how some of these techniques from algebraic geometry and commutative algebra can be used for formal verification of RTL datapaths and arithmetic circuits.

Datapath designs implement arithmetic computations over finite word-length operands, say, over k-bit vectors. These circuits implement functions that are mappings over k-dimensional Boolean spaces $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$. Such functions can also be construed as mappings over: i) finite integer rings of the type $\mathbb{Z}_{2^k} \equiv \mathbb{Z} \pmod{2^k}$, i.e. as functions $f : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_{2^k}$; or ii) as functions over the Galois field of 2^k elements, i.e. $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$. The designs can then be modeled as a system of polynomial functions over $\mathbb{Z}_{2^k}$ or $\mathbb{F}_{2^k}$, and Gröbner basis techniques can be applied for verification by reasoning about the solutions (functions) of the polynomial systems (circuits). Given the arithmetic nature of the designs, such an approach provides a natural *word-level abstraction* which can enable efficient verification.

While Gröbner basis techniques are very powerful, the computation suffers from high complexity. Therefore, the main focus of the tutorial will be on how to overcome this complexity. I will describe:

- How to formulate various verification problems using ideal membership, Nullstellensatz, elimination theory and Gröbner bases;
- How to exploit the number-theoretic properties of finite rings and fields to simplify the problems;
- How to analyze the structure/topology of the given circuits to get more theoretical insights into the corresponding polynomial ideals, and use this information to improve the computation; and
- How to implement the aforementioned concepts using modern symbolic computation algorithms, *e.g. Faugére's* F_4-style reductions, for practical datapath verification.

Arithmetic datapaths are usually custom designed, and they often exhibit some structure or symmetry in the implementations. Gröbner bases can help identify this inherent symmetry. By exploiting this information, efficient symbolic computation algorithms can then be devised for scalable verification.

The verification context will be motivated by applications such as elliptic curve cryptography, error correcting circuits, polynomial signal processing, word-level RTL synthesis, etc. I will provide information on various resources – publications, design benchmarks and the verification tools developed by us – so that interested participants can explore this exciting area of work. I will conclude by describing important unsolved problems in this specific area, and the challenges that need to be overcome to fully exploit the potential of the theory and technology.

BIOGRAPHY

Priyank Kalla received the Bachelors degree in electronics engineering from Sardar Patel University, in 1993, and MS and PhD degrees from the Univ. of Massachusetts Amherst in 1998 and 2002, respectively. Since 2002, he has been a faculty member at the ECE department at the Univ. of Utah. He has also worked at Advanced Micro Devices and the Digital Equipment Corporation (Alpha CAD & Test group). His areas of interest are in Electronic Design Automation and Hardware Verification. He was the chair of the IEEE Technical Committee on Computer-Aided Network Design (CANDE) 2012, and the General Chair of IEEE High-Level Design Validation and Test Workshop (HLDVT) 2009. He is a recipient of the US National Science Foundation Faculty Early Career Development (CAREER) Award, and the ACM Trans. on Design Automation 2009 best paper award.