FORMAL VERIFICATION OF GALOIS FIELD ARITHMETIC CIRCUITS USING COMPUTER ALGEBRA TECHNIQUES

PRIYANK KALLA

Associate Professor, ECE Dept., Univ. of Utah

ABSTRACT

With the spread of Internet and mobile devices, transferring information safely and securely has become more important than ever. Galois fields have many applications in such domains, such as in elliptic curve cryptography, error correcting codes, signal processing, VLSI testing, etc. In most applications, e.g. cryptography, the field-size and the data-path size of the circuits can be very large, requiring (semi-) custom design and specialized architectures for greater performance. Formal verification of such applications is imperative. However, due to their large size and high complexity, formal verification of such circuits is beyond the capabilities of contemporary verification techniques. In this talk, I will describe our work on formal verification of Galois field circuits using computer-algebra based approaches -- notably, Groebner bases theory and technology over Galois fields.

While Groebner bases theory can be a very powerful symbolic reasoning tool, the computation suffers from very high complexity -- doubly exponential in the input data. Therefore, the focus of our work is on attempting to overcome this complexity. In the talk, I will describe: i) how to formulate various verification problems using Nullstellensatz and Groebner bases; ii) how to exploit polynomial function theory over Galois fields within a Groebner basis context for verification; iii) how to analyze the given circuit information to get more theoretical insights into the polynomial ideals, and use this information to overcome Groebner basis complexity; iv) how to employ modern F4-style polynomial reduction techniques to further improve the decision procedures. I will present the results that we have achieved so far, and conclude the talk with some discussion on future work and challenges.

BIOGRAPHY

Priyank Kalla received the Bachelors degree in electronics engineering from Sardar Patel University in 1993, and MS and PhD degrees from Univ. of Massachusetts in 1998 and 2002, respectively. Since 2002, he has been a faculty member at the ECE department at the Univ. of Utah, where he is now an Associate Professor. In between his graduate studies, he has also worked at AMD and DEC-Alpha CAD group. His areas of interest are in Electronic Design Automation and Design Verification -- with a special focus on verification of finite-precision arithmetic using computer-algebra techniques. He was the chair of 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 NSF Faculty Early Career Development (CAREER) Award and the ACM Trans. on Design Automation 2009 best paper award.

Email: kalla@ece.utah.edu; Web: http://www.ece.utah.edu/~kalla