Deriving Canonical Polynomial Representations from Circuits using Gröbner Bases

T. Pruss[1], P. Kalla[1], and F. Enescu[2]

[1] Electrical & Computer Engineering
University of Utah, USA
[2] Mathematics & Statistics
Georgia State University, USA

Abstract. A combinational circuit with k-inputs and k-outputs implements a Boolean function $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$, where $\mathbb{B} = \{0, 1\}$. The same function can also be construed as a mapping $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$, where $\mathbb{F}_{2^k}$ denotes a Galois field of 2^k elements. Every function over $\mathbb{F}_{2^k}$ is a polynomial function — i.e. there exists a unique, minimal, canonical polynomial $\mathcal{F}$ that describes f. This paper describes a method to derive the canonical (word-level) polynomial representation for the circuit $Y = \mathcal{F}(A)$ over $\mathbb{F}_{2^k}$, such that A is the input bit-vector and Y the output. We show that this can be achieved by computing a Gröbner basis of a set of polynomials derived from the circuit, using an elimination term order. Computing a Gröbner basis using elimination orders is, however, practically infeasible for large circuits. We subsequently show that a large circuit can be partitioned into sub-circuits with arbitrary input-output bit-widths and polynomials can be derived for these sub-circuits over $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$. Finally, a hierarchical approach is proposed for polynomial interpolation from circuits. We demonstrate the application of our approach to verification of Galois-field multiplier circuits, which are generally hard to verify using contemporary automatic verification tools.