Compact Circuits for Efficient Mobius Transform

Subhadeep Banik, Francesco Regazzoni
ALaRI - USI, Lugano, Switzerland

Abstract

Mobius transform is a linear circuit used to compute the evaluations of a Boolean Function over all points on its input domain. The operation is completely involutive in the sense that if the same transform is applied to the vector of evaluations of a Boolean Function, we get back the coefficients in the algebraic expression of the function. The operation is very useful in finding the solution of a system of polynomial equations over GF(2) for obvious reasons. However the operation, although linear, needs exponential number of logic operations (around $n \cdot 2^{n-1}$ bit xors) for an n-variable Boolean Function. As such the only known hardware circuit to efficiently compute the Mobius Transfrom requires silicon area that is exponential in n. For Boolean Functions whose algebraic degree is bound by some parameter d, recursive definitions of the Mobius transform exist that requires only $O(n^d)$ space in software. However converting the mathematical definition of this space-efficient algorithm into a hardware architecture is a non-trivial task, primarily because the recursion calls notionally lead to a depth-first search in a transition graph that require context switches at each recursion call for which straightforward mapping in hardware is difficult.

In this presentation we look to overcome these very challenges in an engineering sense. We propose a space efficient sequential hardware circuit for the Mobius transform that requires only polynomial circuit area (i.e. $O(n^d)$) provided the algebraic degree of the Boolean Function is limited to d. We show that how this circuit can be used as a component to efficiently solve polynomial equations of degree at most d by using fast exhaustive search. We propose three different circuit architectures for this, each of which used the Mobius transform circuit as a core component. We show that asymptotically, all the solutions of a system of m polynomials in n unknowns and algebraic degree d over GF(2) can be found using a circuit of silicon area proportional to $m \cdot n^d$ and physical time proportional to $2 \cdot \log_2(n-d) \cdot 2^{n-d}$.