On the Computation of Reed-Muller Spectra for Cryptography and Switching Theory Applications

Mitchell A. Thornton
Darwin Deason Institute for Cyber Security
Southern Methodist University
Dallas, Texas, USA

D. Michael Miller
Department of Computer Science
University of Victoria
Victoria, BC

Abstract—We survey a variety of methods that allow for the Reed-Muller spectrum, also known as the Algebraic Normal Form (ANF), to be computed for functions of a large number of variables. Some of the methods are previously known while others may be new to the research community interested in switching algebras. The techniques described here include decision-diagram based methods, the Möbius transform, and methods to extract the spectra directly from a netlist representation without first formulating a switching function model. It is shown that the Möbius transform can be employed using input data in the form of cube lists and black box responses as an alternative to truth table data as is the usual methodology. One outcome of this survey is that practitioners will be enabled to choose the most appropriate method for computation of the spectrum/ANF based upon the initial form of the native function representation.

Keywords—Reed-Muller spectra, Algebraic Normal Form, fast transform, BDD, FDD, cryptographic primitive analysis

REFERENCES


[References continued...]

[MF:65] D. Michael Miller
Department of Computer Science
University of Victoria
Victoria, BC