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

[AD+:09] J.P. Aumasson, I. Dinur, W. Meier, and A. Shamir, "Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium," in proc. O. Dunkelman (ed.), Fast Software Encryption, LNCS, vol. 5665, pp. 1-22, Springer, Heidelberg, 2009.

[BLR:93] M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with Applications to Numerical Problems," *Journal of Computer and System Sciences*, vol. 47, no. 3, pp. 549-595, 1993.

[Bry:86] R. Bryant, "Graph-based Algorithms for Boolean Function Manipulation," IEEE Transactions on Computers, vol. C-35, no. 8, pp. 677-691, 1986.

[Cha:66] G.J. Chaitlin, "On the Length of Programs for Computing Finite Binary Sequences," *Journal of the ACM*, vol. 13, pp. 547-570, 1966.

[CM:04] J. Cannons, P. Moulin, "Design and statistical analysis of a hash-aided image watermarking system," *IEEE Transactions on Image Processing*, vol. 13, no. 10, pp. 1393-1408, Oct. 2004.

[CS:09] T.W. Cusick and P. Stănică, **Cryptographic Boolean Functions and Applications**, Elsevier/Academic Press Pub., 2009, ISBN 978-0-1237-4890-4.

[CT:65] J.W. Cooley and J.W. Tukey, "An Algorithm for the Machine Calculation of Complex Fourier Series," *Math. Computation*, vol. 19, pp. 297-301, 1965.

[DB:50] J. Durbin and G.S. Watson, "Testing for Serial Correlation in Least Squares Regression I," *Biometrika*, vol. 37, no. 3/4, pp. 409-428, 1950.

[DB:51] J. Durbin and G.S. Watson, "Testing for Serial Correlation in Least Squares Regression II," *Biometrika*, vol. 38, no. 1/2, pp. 159-179, 1951.

[Dir:39] P.A.M. Dirac, "A New Notation for Quantum Mechanics," *Proc. of the Cambridge Philosophical Society*, vol. 54, p. 416, 1939.

[DS:08] I. Dinur and A. Shamir, "Cube Attacks on Tweakable Black Box Polynomials," in *Cryptology ePrint Archive*, Report 385, 2008.

[DST+:94] R. Drechsler, A. Sarabi, M. Theobold, B. Becker, and M.A. Perkowski, "Efficient Representation and Manipulation of Switching Functions Based on Ordered Kronecker Functional Decision Diagrams," in proc. *IEEE/ACM Design Automation Conference*, pp. 415-419, 1994.

[EJ+:07] H. Englund, T. Johansson, and M.S. Turan, "A Framework for Chosen IV Statistical Analysis of Stream Ciphers," in proc. K. Srinathan, C.P. Rangan, and M. Yung, (eds.) INDOCRYPT 2007, LNCS, vol. 4859, pp. 268-281, Springer, Heidelberg, 2007.

[Fil:02] E. Filiol, "A New Statistical Testing for Symmetric Ciphers and Hash Functions," In Proc. *4th International Conference on Information and Communications Security* (ICICS '02), R.H. Deng, S. Qing, F. Bao, and J. Zhou (Eds.). Springer-Verlag Pub., London, UK, UK, pp. 342-353, 2002.

[FP:90] B.J. Falkowski and M.A. Perkowski, "A Family of all Essential Radix-2 Addition/Subtraction Multi-polarity Transforms: Algorithms and Interpretations in Boolean Domain," in proc. *IEEE Int. Symp. on Circuits and Systems*, pp. 2913-2916, 1990.

[FP:91] B.J. Falkowski and M.A. Perkowski, "One More Way to Calculate the Generalized Reed-Muller Expansions of Boolean Functions," *International Journal of Electronics*, vol. 71, no. 3, pp. 385-396, 1990.

[FSP:92] B.J. Falkowski, I. Schäfer, and M.A. Perkowski, "Effective Computer Methods for the Calculation of Rademacher-Walsh Spectrum for Completely and Incompletely Specified Boolean Functions," *IEEE Transactions on CAD*, vol. 11, pp. 1207-1226, 1992.

[Gau:66] C.F. Gauss, "Theoria Interpolationis Methodo Nova Tractata," Werke band 3, pp. 265-327, 1866, Göttingen: Königliche Gessellschaft der Wissenschaften.

[Gol:10] O. Goldreich, **A Primer on Pseudorandom Generators**, American Mathematical Society, Providence, RI, 2010, ISBN 978-0-8218-5192-0.

[Gol:82] S.W. Golomb, **Shift Register Sequences**, Aegean Park Press, 1982.

[Goo:58] I.J. Good, "The Interaction Algorithm and Practical Fourier Analysis," Journal of the Royal Statistical Society, Series B 20 (2), pp. 361-372, 1958, Addendum, ibid. 22(2), pp. 373-375, 1960.

[HT:16] D.K. Houngninou and M.A. Thornton, "Implementation of Switching Circuit Models as Transfer Functions," in proc. *IEEE Int. Symp. on Circuits and Systems* (ISCAS), pp. 2167-2170, May 22-25, 2016.

[Kol:65] A. Kolmogorov, "Three Approaches to the Concept of 'The Amount of Information'," *Problems of Information Transmission*, vol. 1/1, 1965.

[KS:07] T. Kaufman and M. Sudan, "Algebraic Property Testing: The Role of Invariance," 2007.

[Mau:92] U. Maurer, "A Universal Statistical Test for Random Bit Generators," *Journal of Cryptology*, vol. 5, no. 2, pp. 89-105, 1992.

[McC:86] P.J. McCarthy, **Introduction to Arithmetical Functions**, Springer-Verlag, New York, 1985, ISBN 0-367-96262-X.

[MZ:60] S.J. Mason and H.J. Zimmerman, **Electronic Circuits, Signals, and Systems**, Wiley Publishers, New York, 1960.

[NIST:15] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)," FIPS PUB 180-4, August 2015.

[OS:98] D. Olejár and M. Stanek, "On Cryptographic Properties of Random Boolean Functions," *Journal of Universal Computer Science*, vol. 4, no. 8, pp. 705-717, 1998.

[OSW:82] J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent-Function Sequences," *IEEE Transactions on Information Theory*, vol. IT-28, no. 6, pp. 858-864, November 1982.

[PS:13] C. Posthoof, and B. Steinbach, **Logic Functions and Equations: Binary Models for Computer Science**, Springer Science & Business Media, 2013.

[Ru:10] A. Ruhkin, *et. al*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *Special Publication 800-22*, *Revision 1a*, National Institute of Standards and Technology (NIST), April 2010.

[Sha:48] C.E. Shannon, "A Mathematical Theory of Communication," *Bell Sys. Tech. Jour.*, vol. 27, pp. 623-656, 1948.

[Sol:64] R.J. Solomonoff, "A Formal Theory of Inductive Inference," *Information and Control*, vol. 7/1, pp. 1-22, 1964.

[SP:10] B. Steinbach and C. Posthoff. "Boolean Differential Calculus".In: *Progress in Applications of Boolean Functions*. Ed. by T. Sasao and J. Butler, Morgan & Claypool Publishers, pp. 55–78, 2010.

[SP:13] B. Steinbach, and C. Posthoff, **Boolean Differential Equations**, Morgan & Claypool Publishers, 2013, ISBN: 9781627052412.

[TDM:01] M.A. Thornton, R. Drechsler, and D.M. Miller, **Spectral Techniques in VLSI CAD**, Kluwer Academic Publishers, Boston, Massachusetts, July 2001, ISBN 0-7923-7433-9.

[Tho:14] M.A. Thornton, **Modeling Digital Switching Circuits with Linear Algebra**, Morgan & Claypool Pub., San Rafael, California, April 2014, ISBN 9781627052337.

[Tho:15] M.A. Thornton, "Simulation and Implication using a Transfer Function Model for Switching Logic," *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3580-3590, December 2015.

[TT:16] M.A Thornton and M.A. Thornton, "Boolean Function Spectra and Circuit Probabilities," Chap. 4, Section 4.1, in **Problems and New Solutions in the Boolean Domain**, Cambridge Scholars Publishing, Cambridge, UK, Bernd Steinbach, ed., January 2016, ISBN 13-978-1-4438-8947-6.

[WM:07] R. Ward and T. Molteno, "Table of Linear Feedback Shift Registers," *Tech. Report*, Dept. of Physics, Univ. of Otago, Dunedin, New Zealand, October 26, 2007.