Eigenanalysis of the matrix representations of vectorial Boolean functions

BRANDON DRAVIE

2nd July 2014

Introduction

- Matrix representations of vectorial Boolean functions

Introduction

- Matrix representations of vectorial Boolean functions
- Spectral analysis by oriented graph theory

Introduction

- Matrix representations of vectorial Boolean functions
- Spectral analysis by oriented graph theory
- Better understanding of vectorial Boolean functions and application for the design of Self-Synchronizing Stream Ciphers

Plan

Plan

Plan

Plan

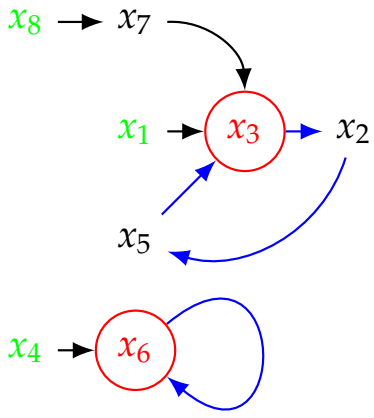
Plan

Perspective

- Diagonalization of the adjacency matrix

Perspective

- Diagonalization of the adjacency matrix



The number of leaves is equal to the number of junctions

Perspective

- Diagonalization of the adjacency matrix
- Graph containing cycles of length prime number

References I


C. Carlet, *Boolean models and methods in mathematics, computer science, and engineering*, ch. Boolean Functions for Cryptography and Error-Correcting Codes, in [Cra10], 2010.


_____, *Boolean models and methods in mathematics, computer science, and engineering*, ch. Vectorial Boolean Functions for Cryptography, in [Cra10], 2010.


C. Carlet and P. Guillot, *A new representation of boolean functions*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, eds.), Lecture Notes in Computer Science, vol. 1719, Springer Berlin / Heidelberg, 1999, 10.1007/3-540-46796-3_10, pp. 731–731.


Y. Crama, *Boolean models and methods in mathematics, computer science, and engineering*, Cambridge Press, 2010.


J. Daemen, R. Govaerts, and J. Vandewalle, *Correlation matrices*, Fast Software Encryption : Second International Workshop, LNCS 1008, Springer-Verlag, 1994, pp. 275–285.


C. Godsil and G. Royle, *Algebraic graph theory*, Springer, 2001.


P. Guillot, *Fonctions courbes binaires et transformation de möbius*, Ph.D. thesis, 1999.


J. Parriaux, *Control, synchronization and encryption*, Ph.D. thesis, Université de Lorraine, 2012.

References II


Jeremy Parriaux, Philippe Guillot, and Gilles Millérioux, *Synchronization of boolean dynamical systems : a spectral characterization*, In proceedings of the 6th Conference on Sequences and their applications, SETA 2010, 2010, p. 14.


_____, *A spectral approach for characterizing the self-synchronization of stream ciphers*, In proceedings of the Symmetric Key Encryption Workshop, SKEW 2011, 2011, p. 14.