

A graph theoretic approach to construct desired cryptographic boolean functions

In this paper, we present four product operations to construct cryptographic boolean functions from smaller ones with predictable Walsh spectrum. A lot of cryptographic properties of boolean functions can be presented by their Walsh spectrum. In our method, we use the product of Cayley graphs to present new boolean functions with desired Walsh spectrum and investigate their non-linearity, algebraic and correlation immunity.

General information

Publication status: Published

MoE publication type: A1 Journal article-refereed

Organisations: Computing Sciences, Research group: Predictive Society and Data Analytics (PSDA), Teacher Training University, University of Applied Sciences Upper Austria, School of Management, Hall in Tyrol, Nankai University

Contributors: Ghorbani, M., Dehmer, M., Taghvayi-Yazdelli, V., Emmert-Streib, F.

Publication date: 1 Jun 2019

Peer-reviewed: Yes

Publication information

Journal: Axioms

Volume: 8

Issue number: 2

Article number: 40

ISSN (Print): 2075-1680

Ratings:

Scopus rating (2019): CiteScore 1.7 SJR 0.314 SNIP 1.249

Original language: English

ASJC Scopus subject areas: Analysis, Algebra and Number Theory, Mathematical Physics, Logic, Geometry and Topology

Keywords: Algebraic immunity, Boolean functions, Cayley graphs, Non-linearity, Walsh spectrum

Electronic versions:

axioms-08-00040-v3

DOIs:

10.3390/axioms8020040

URLs:

<http://urn.fi/URN:NBN:fi:tyy-201906241903>

Source: Scopus

Source ID: 85066846087

Research output: Contribution to journal > Article > Scientific > peer-review

A note on distance-based entropy of dendrimers

This paper introduces a variant of entropy measures based on vertex eccentricity and applies it to all graphs representing the isomers of octane. Taking into account the vertex degree as well (degree-ecc-entropy), we find a good correlation with the acentric factor of octane isomers. In particular, we compute the degree-ecc-entropy for three classes of dendrimer graphs.

General information

Publication status: Published

MoE publication type: A1 Journal article-refereed

Organisations: Computing Sciences, Research group: Computational Medicine and Statistical Learning Laboratory (CMSL), Research group: Predictive Society and Data Analytics (PSDA), Shahid Rajaei Teacher Training University, University of Applied Sciences Upper Austria, Hall in Tyrol, Nankai University, The City College of New York (CUNY)

Contributors: Ghorbani, M., Dehmer, M., Zangi, S., Mowshowitz, A., Emmert-Streib, F.

Publication date: 2019

Peer-reviewed: Yes

Publication information

Journal: Axioms

Volume: 8

Issue number: 3

Article number: 98

ISSN (Print): 2075-1680

Ratings:

Scopus rating (2019): CiteScore 1.7 SJR 0.314 SNIP 1.249

Original language: English

ASJC Scopus subject areas: Analysis, Algebra and Number Theory, Mathematical Physics, Logic, Geometry and Topology

Keywords: Dendrimer, Graph entropy, Vertex eccentricity

Electronic versions:

axioms-08-00098-v2

DOIs:

10.3390/axioms8030098

URLs:

<http://urn.fi/URN:NBN:fi:tuni-201909183381>

Source: Scopus

Source ID: 85071384174

Research output: [Contribution to journal](#) › [Article](#) › [Scientific](#) › [peer-review](#)

Approximate Controllability for Navier–Stokes Equations in 3D Rectangles Under Lions Boundary Conditions

The 3D Navier–Stokes system, under Lions boundary conditions, is proven to be approximately controllable provided a suitable saturating set does exist. An explicit saturating set for 3D rectangles is given.

General information

Publication status: Published

MoE publication type: A1 Journal article-refereed

Organisations: Mathematics, Johann Radon Institute for Computational and Applied Mathematics

Contributors: Phan, D., Rodrigues, S. S.

Number of pages: 26

Pages: 351-376

Publication date: Jul 2019

Peer-reviewed: Yes

Early online date: 10 Jul 2018

Publication information

Journal: Journal of Dynamical and Control Systems

Volume: 25

Issue number: 3

ISSN (Print): 1079-2724

Ratings:

Scopus rating (2019): CiteScore 2.2 SJR 0.487 SNIP 1.178

Original language: English

ASJC Scopus subject areas: Control and Systems Engineering, Algebra and Number Theory, Numerical Analysis, Control and Optimization

Keywords: Approximate controllability, Navier–Stokes equations, Saturating set

DOIs:

10.1007/s10883-018-9412-0

Source: Scopus

Source ID: 85049619310

Research output: [Contribution to journal](#) › [Article](#) › [Scientific](#) › [peer-review](#)

Constructing Minimal Coverability Sets

This publication addresses two bottlenecks in the construction of minimal coverability sets of Petri nets: the detection of situations where the marking of a place can be converted to ω , and the manipulation of the set A of maximal ω -markings that have been found so far. For the former, a technique is presented that consumes very little time in addition to what maintaining A consumes. It is based on Tarjan's algorithm for detecting maximal strongly connected components of a directed graph. For the latter, a data structure is introduced that resembles BDDs and Covering Sharing Trees, but has additional heuristics designed for the present use. Results from a few experiments are shown. They demonstrate significant savings in running time and varying savings in memory consumption compared to an earlier state-of-the-art technique.

General information

Publication status: Published

MoE publication type: A1 Journal article-refereed

Organisations: Department of Mathematics, Research group: MAT Computer Science and Applied Logics

Contributors: Piipponen, A., Valmari, A.

Number of pages: 22

Pages: 393-414

Publication date: 4 Mar 2016

Peer-reviewed: Yes

Publication information

Journal: Fundamenta Informaticae

Volume: 143

Issue number: 3-4

ISSN (Print): 0169-2968

Ratings:

Scopus rating (2016): CiteScore 1.8 SJR 0.371 SNIP 0.716

Original language: English

ASJC Scopus subject areas: Information Systems, Computational Theory and Mathematics, Theoretical Computer Science, Algebra and Number Theory

Keywords: antichain data structure, coverability set, Tarjan's algorithm

Electronic versions:

Constructing Minimal Coverability Sets

DOIs:

10.3233/FI-2016-1319

URLs:

<http://urn.fi/URN:NBN:fi:tyy-201605274193>

Source: Scopus

Source ID: 84959877143

Research output: Contribution to journal > Article > Scientific > peer-review

On homomorphisms between products of median algebras

Homomorphisms of products of median algebras are studied with particular attention to the case when the codomain is a tree. In particular, we show that all mappings from a product (Formula presented.) of median algebras to a median algebra (Formula presented.) are essentially unary whenever the codomain (Formula presented.) is a tree. In view of this result, we also characterize trees as median algebras and semilattices by relaxing the defining conditions of conservative median algebras.

General information

Publication status: Published

MoE publication type: A1 Journal article-refereed

Organisations: Mathematics, Université de Lorraine, TEI of Epirus

Contributors: Couceiro, M., Foldes, S., Meletiou, G. C.

Number of pages: 9

Pages: 545–553

Publication date: 2017

Peer-reviewed: Yes

Publication information

Journal: Algebra Universalis

Volume: 78

Issue number: 4

ISSN (Print): 0002-5240

Ratings:

Scopus rating (2017): CiteScore 1.1 SJR 0.583 SNIP 1.038

Original language: English

ASJC Scopus subject areas: Algebra and Number Theory

DOIs:

10.1007/s00012-017-0468-6

Source: Scopus

Source ID: 85031922238

Research output: Contribution to journal > Article > Scientific > peer-review

On the spectral and Frobenius norm of a generalized Fibonacci r -circulant matrix

Consider the recursion $g_0 = a$, $g_1 = b$, $g_n = g_{n-1} + g_{n-2}$, $n = 2, 3, \dots$. We compute the Frobenius norm of the r -circulant matrix corresponding to g_0, \dots, g_{n-1} . We also give three lower bounds (with equality conditions) for the spectral norm of this matrix. For this purpose, we present three ways to estimate the spectral norm from below in general.

General information

Publication status: Published

MoE publication type: A1 Journal article-refereed

Organisations: Mathematics, Lulea University of Technology

Contributors: Merikoski, J. K., Haukkanen, P., Mattila, M., Tossavainen, T.

Number of pages: 14

Pages: 23-36
Publication date: 1 Jan 2018
Peer-reviewed: Yes

Publication information

Journal: Special Matrices
Volume: 6
Issue number: 1
ISSN (Print): 2300-7451
Ratings:

Scopus rating (2018): CiteScore 0.7 SJR 0.408 SNIP 1.044

Original language: English

ASJC Scopus subject areas: Algebra and Number Theory, Geometry and Topology

Keywords: Euclidean norm, Frobenius norm, generalized Fibonacci numbers, r-circulant matrix, spectral norm

Electronic versions:

spma-2018-0003

DOIs:

10.1515/spma-2018-0003

URLs:

<http://urn.fi/URN:NBN:fi:ty-201803131371>

Source: Scopus

Source ID: 85042290997

Research output: Contribution to journal › Article › Scientific › peer-review

Toward measuring network aesthetics based on symmetry

In this exploratory paper, we discuss quantitative graph-theoretical measures of network aesthetics. Related work in this area has typically focused on geometrical features (e.g., line crossings or edge bendiness) of drawings or visual representations of graphs which purportedly affect an observer's perception. Here we take a very different approach, abandoning reliance on geometrical properties, and apply information-theoretic measures to abstract graphs and networks directly (rather than to their visual representations) as a means of capturing classical appreciation of structural symmetry. Examples are used solely to motivate the approach to measurement, and to elucidate our symmetry-based mathematical theory of network aesthetics.

General information

Publication status: Published

MoE publication type: A1 Journal article-refereed

Organisations: Faculty of Biomedical Sciences and Engineering, Research group: Computational Medicine and Statistical Learning Laboratory (CMSL), Research group: Predictive Society and Data Analytics (PSDA), Nankai University, Institute for Bioinformatics and Translational Research, The City College of New York (CUNY)

Contributors: Chen, Z., Dehmer, M., Emmert-Streib, F., Mowshowitz, A., Shi, Y.

Publication date: 1 Jun 2017

Peer-reviewed: Yes

Publication information

Journal: Axioms
Volume: 6
Issue number: 2
Article number: 12
ISSN (Print): 2075-1680
Ratings:

Scopus rating (2017): CiteScore 1.8 SNIP 0.514

Original language: English

ASJC Scopus subject areas: Algebra and Number Theory, Analysis, Geometry and Topology, Logic, Mathematical Physics

Keywords: Aesthetical theory, Aesthetics, Entropy, Network aesthetics, Networks

Electronic versions:

axioms-06-00012-v2

DOIs:

10.3390/axioms6020012

URLs:

<http://urn.fi/URN:NBN:fi:ty-201710091991>

Source: Scopus

Source ID: 85029485798

Research output: Contribution to journal › Article › Scientific › peer-review

Application and theory of Petri nets and other models of concurrency: Special issue of selected papers from Petri Nets 2015

General information

Publication status: Published

MoE publication type: B1 Article in a scientific magazine

Organisations: Department of Mathematics, Research group: MAT Computer Science and Applied Logics

Contributors: Devillers, R., Valmari, A., Penczek, W.

Pages: v-vi

Publication date: 13 Sep 2016

Peer-reviewed: No

Publication information

Journal: Fundamenta Informaticae

Volume: 146

Issue number: 1

ISSN (Print): 0169-2968

Ratings:

Scopus rating (2016): CiteScore 1.8 SJR 0.371 SNIP 0.716

Original language: English

ASJC Scopus subject areas: Theoretical Computer Science, Algebra and Number Theory, Information Systems, Computational Theory and Mathematics

DOIs:

10.3233/FI-2016-1373

Source: Scopus

Source ID: 84988662462

Research output: Contribution to journal › Editorial › Scientific