AFRL-AFOSR-VA-TR-2015-0257

Algebraic Methods to Design Signals

Krishnasany Arasu
WRIGHT STATE UNIVERSITY

08/27/2015
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTC
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 19-08-2015	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)* June 2012 - May 2015

4. TITLE AND SUBTITLE
ALGEBRAIC METHODS TO DESIGN SIGNALS

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-12-1-0297

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
K.T.Arasu

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Wright State University
3640 Colonel Glenn Highway
Dayton, OH 45435

8. PERFORMING ORGANIZATION REPORT NUMBER

668838

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of
Scientific Resesearch (AFOSR)
875 N Randolph Street RM 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

This report describes progress to date on designing signals using algebraic and combinatorial methods. Mathematical tools from algebraic number theory, representation theory and group theory are employed to investigate the theory of their construction methods leading to new families of these arrays and some generalizations thereof. The major task of this project is to design signals based on small alphabet sets. The relevant research resulted in many papers that have been published based on this effort.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** K.T.Arasu
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	SAR	3	**19b. TELEPHONE NUMBER** *(include area code)* 937-775-3828

FINAL REPORT (Detailed)
To: technicalreports@afosr.af.mil
CC: arje.nachman@us.af.mil
SSNav@afosr.af.mil

Subject: Final Report Statement to Dr. Arje Nachman
Contract/Grant Title: ALGEBRAIC METHODS TO DESIGN SIGNALS
Contract/Grant #: FA9550-12-1-0297
Reporting Period: 1 Jun 2012 – 31 MAY 2015

Accomplishments (200 words max): This research focuses on the discovery of a few very rich classes of sequences all of whose out-of-phase autocorrelation values are very small. We call the constructed sequences perfect sequences and they serve as perfect algebraic/combinatorial objects in designing signals for communication purposes. Sequences and arrays with desirable autocorrelation properties have many applications in spread spectrum communication systems such as a code division multiple access (CDMA) system, which has been adopted as a standard for multiple access methods in mobile radio communication systems.

We continue our mathematical framework based on group algebras, character theory, algebraic number theory, finite geometry, and combinatorics in designing signals as a by-product of new combinatorial designs and the corresponding sequences and arrays with desirable correlation properties. The methods used are very algebraic and number theoretic. Many new families of sequences with low correlation values have been found. The effort resulted in 10 published research papers in refereed journals.

Archival publications (published) during reporting period:

1. Block Weighing Matrices, (with Simone Severini and, Edmund Velten). Cryptography and Communications 5(3): 201-207 (2013).

   In this paper, We define block weighing matrices, as a special type of weighing matrices. Motivated by some questions arising in the context of optical quantum computing, we prove that infinite families of anticirculant block weighing matrices can be obtained from generic weighing matrices

2. Gauss sum factorizations yield perfect sequences, (with John Dillon and Kevin Player), IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 61, NO. 6, JUNE 2015, Pages 3276-3304.

Paper # [2] deals with some new constructions of sequences and arrays whose auto-correlation functions have desirable correlation properties. Of particular interest are the *p*-ary sequences, where *p* is a prime, and the entries of the underlying sequence are *pth* roots of unity. The ternary case has entries that are complex third roots of unity. In the p-ary case, the prefix "perfect" for the underlying sequence (i.e. 1-dimensional array) refers to the case when all the out-of-phase autocorrelations are equal to minus one. The main tools used in our new research are: Stickelberger congruence on Gauss Sums and Hasse-Davenport formulae.

Theorem 1 Let $p = 2$ and $d > 2$ be an integer. Also let r be any integer with $(r, d) = 1$. Assume that d and r of opposite parity. Then $P_{[1, -3, (2^r+1)]}$ is a perfect sequence over $GF(2^d) \setminus \{0\}$.

Theorem 2 Let p be an odd prime. Let d be an integer, $d > 2$. Let r be an integer with $(p^r + 1, p^d - 1) = 2$, or equivalently $d/(r,d)$ is odd. Then $P_{[1, -2, p^r + 1]}$ is a perfect sequence over $GF(p^d) \setminus \{0\}$.

Theorem 3 Let $p = 3$ and $d > 2$ be an integer. Also let r be any integer with $(r, d) = 1$. Then

(i) $P_{[1, -2, \frac{1}{2}(3^r+1)]}$ is a perfect sequence over $GF(3^d) \setminus \{0\}$

(ii) If furthermore d is odd, $P_{[1+(3^d-1)/2, -2, \frac{1}{2}(3^r+1)+(3^d-1)/2]}$ is a perfect sequence over $GF(3^d) \setminus \{0\}$

3. Binary Sequence/Array Pairs via Difference Set Pairs : A Recursive Approach, (with Anika Goyal and Abhishek Puri), To appear in Transactions in Combinatorics, (24 page manuscript) .

In Paper # [3], binary array pairs with optimal/ideal correlation values and their algebraic counterparts difference set pairs" (DSPs) in abelian groups are studied. In addition to generalizing known 1-dimensional (sequences) examples, we provide four new recursive constructions, unifying previously obtained ones. Any further advancements in the construction of binary sequences/arrays with optimal/ideal correlation values (equivalently cyclic/abelian difference sets) would give rise to richer classes of DSPs (and hence binary perfect array pairs). Discrete signals arising from DSPs find applications in cryptography, CDMA systems, radar and wireless communications.

4. Xiuping Peng, Chengqian Xu, Arasu, K.T., New Families of Binary Sequence Pairs With Two-Level and Three-Level Correlation. IEEE Transactions Information Theory, Volume: 58, Issue: 11, Nov 2012, Page(s): 6968 – 6978

In this popular paper (which has been downloaded over 200 times), we provide constructions for new binary sequence pairs with optimal correlation values.

5. K.T. Arasu, Pradeep Bansal, Cody Watson, Partially balanced incomplete block designs with two associate classes. Journal of Statistical Planning and Inference, Volume 143, Issue 5, May 2013, Pages 983–991

In this paper, we provide constructions of cyclic 2-class partially balanced incomplete block designs using cyclotomy in finite fields. Our results give theoretical explanations of the two sporadic examples given by Agrawal. THESE DESIGNS HAVE IMMEDIATE CONNECTIONS TO WHAT WE CALL AS ALMOST DIFFERENCE SETS IN THE PROPOSAL AND ARE USED IN COMMUNICATION ENGINEERING.

6. K.T.Arasu and Keli Parker, Multilevel Hadamard Matrices, Bulletin of Kerala Mathematics Association, 9, (2012), pp.343-372.

   In this paper, we investigate Multilevel Hadamard Matrices (MHMs) which have been examined by Trihn, Fan, and Gabidulin for constructions of multilevel zero-correlation zone sequences, which in turn have useful application in quasi-synchronous code division multiple access (CDMA) systems. We provide several observations regarding Adams' construction, and give new constructions for other orders of MHMs

7. K.T.Arasu and S.L.Ma, "Nonexistence of CW(110,100)", Designs, Codes and Cryptography, p. 273-278, vol. 62, (2012).

In this paper, we use character theoretic methods to settle the existence status of a circulant weighing matrix (equivalently perfect ternary sequence) of order 110 with weight 100. This fills a missing entry in recent tables.

8. K.T.Arasu and Jeff Hollon (2013). Group developed weighing matrices. *AUSTRALASIAN JOURNAL OF COMBINATORICS*. 55, 205-233.

   In this paper, we discuss group developed weighing matrices, which could be viewed as higher dimensional analogs of perfect sequences used in signal designs. A weighing matrix is a square matrix whose entries are 1, 0 or -1 and has the property that the matrix times its transpose is some integer multiple of the identity matrix. We examine the case where these matrices are said to be developed by an abelian group.

9. K.T.Arasu, Kyle Bayes and Ali Nabavi . Circulant weighing matrices of weight 81. **Transactions on Combinatorics** ISSN (print): 2251-8657, ISSN (on-line): 2251-8665, Vol. 4 No. 3 (2015), pp. 43-52.

In this paper, we settle the existence question of two previously open weighing matrices (equivalently, perfect ternary sequences) of weight 81. We apply two very different methods to do so; for one, we use almost purely counting methods, while for the other, we use algebraic ideas.

10.K.T.Arasu, Ankita Bakshi, Deeksha Sheokand "Constructions of Punctured Difference Set Pairs and their corresponding Punctured Binary Array Pairs" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 61, NO. 4, APRIL 2015**,** Pages 2191-2199.

In paper # 10, we present some construction methods for Punctured Binary Array/Sequence Pairs (PBAPs/PBSPs) with ideal/optimal correlation constant using their algebraic counterparts “Punctured Difference Set Pairs ”(PDSPs) in abelian groups. In addition, we provide new construction techniques of PBAPs/PBSPs via geometry and also by using the embeddable sequence pairs of smaller lengths to obtain larger ones. PBAPs/PBSPs find a plethora of applications in radar systems, engineering fields.

The co-authors are two young undergraduate juniors (majoring in Computer Engineering) from India who spent 10 weeks as summer interns with the PI and produced this phenominal paper. This paper got accepted by IEEE within 5 months with no revisions !! (even the reviewer's comments were very good.) Our novel way of looking at that problem (in addition to the unified approach) would stimulate further research.

Changes in research objectives, if any: None

Change in AFOSR program manager, if any: Dr. Arje Nachman

Extensions granted or milestones slipped, if any: None

Include any new discoveries, inventions, or patent disclosures during this reporting period (if none, report none): None

1.

1. Report Type

Final Report

Primary Contact E-mail
Contact email if there is a problem with the report.

k.arasu@wright.edu

Primary Contact Phone Number
Contact phone number if there is a problem with the report

937-775-2785

Organization / Institution name

Wright State University

Grant/Contract Title
The full title of the funded effort.

ALGEBRAIC METHODS TO DESIGN SIGNALS

Grant/Contract Number
AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-12-1-0297

Principal Investigator Name
The full name of the principal investigator on the grant or contract.

K.T.Arasu

Program Manager
The AFOSR Program Manager currently assigned to the award

Dr. Arje Nachman

Reporting Period Start Date

06/01/2012

Reporting Period End Date

05/31/2015

Abstract

This research focuses on the discovery of a few very rich classes of sequences all of whose out-of-phase autocorrelation values are very small. We call the constructed sequences perfect sequences and they serve as perfect algebraic/combinatorial objects in designing signals for communication purposes. Sequences and arrays with desirable autocorrelation properties have many applications in spread spectrum communication systems such as a code division multiple access (CDMA) system, which has been adopted as a standard for multiple access methods in mobile radio communication systems.

We used mathematical framework based on group algebras, character theory, algebraic number theory, finite geometry, and combinatorics in designing signals as a by-product of new combinatorial designs and the corresponding sequences and arrays with desirable correlation properties. The methods used are very algebraic and number theoretic. Many new families of sequences with low correlation values have been found. The effort resulted in 10 published research papers in refereed journals.

Distribution Statement
This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement

If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF The maximum file size for an SF298 is 50MB.

AFOSR2015-sf298.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

FINAL REPORT (Detailed).pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

1. Block Weighing Matrices, (with Simone Severini and, Edmund Velten). Cryptography and Communications 5(3): 201-207 (2013).
2. Gauss sum factorizations yield perfect sequences, (with John Dillon and Kevin Player), IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 61, NO. 6, JUNE 2015, Pages 3276-3304.
3. Binary Sequence/Array Pairs via Difference Set Pairs : A Recursive Approach, (with Anika Goyal and Abhishek Puri), To appear in Transactions in Combinatorics, (24 page manuscript) .

4. Xiuping Peng, Chengqian Xu, Arasu, K.T., New Families of Binary Sequence Pairs With Two-Level and Three-Level Correlation. IEEE Transactions Information Theory, Volume: 58, Issue: 11, Nov 2012, Page(s): 6968 – 6978
5. K.T. Arasu, Pradeep Bansal, Cody Watson, Partially balanced incomplete block designs with two associate classes. Journal of Statistical Planning and Inference, Volume 143, Issue 5, May 2013, Pages 983–991
6. K.T.Arasu and Keli Parker, Multilevel Hadamard Matrices, Bulletin of Kerala Mathematics Association, 9, (2012), pp.343-372.
7. K.T.Arasu and S.L.Ma, "Nonexistence of CW(110,100)", Designs, Codes and Cryptography, p. 273-278, vol. 62, (2012).
8. K.T.Arasu and Jeff Hollon (2013). Group developed weighing matrices. AUSTRALASIAN JOURNAL OF COMBINATORICS. 55, 205-233.
9. K.T.Arasu, Kyle Bayes and Ali Nabavi . Circulant weighing matrices of weight 81. Transactions on Combinatorics ISSN (print): 2251-8657, ISSN (on-line): 2251-8665, Vol. 4 No. 3 (2015), pp. 43-52.
10. K.T.Arasu, Ankita Bakshi, Deeksha Sheokand "Constructions of Punctured Difference Set Pairs and their corresponding Punctured Binary Array Pairs"
IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 61, NO. 4, APRIL 2015, Pages 2191-2199.

Changes in research objectives (if any):

None

Change in AFOSR Program Manager, if any:

Dr. Arje Nachman

Extensions granted or milestones slipped, if any:

None

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

Aug 19, 2015 21:24:19 Success: Email Sent to: k.arasu@wright.edu