**Signal Designs via Combinatorial Designs**

This report describes progress to date on designing signals using combinatorial designs. We shall regard signal design problems as “The Correlation Problem”. The Correlation Problem is to design sequences with specified lengths with entries chosen from a specified finite set so that all non-trivial periodic autocorrelations lie in a prescribed restrictive set. Mathematical tools from algebraic number theory, representation theory and group theory are employed to investigate the theory of their existence leading to new families of these arrays and some generalizations thereof. The major task of this project is to design signals based on complex roots of unity. The relevant research resulted in many papers that have been published based on this effort.

**14. ABSTRACT**

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
<th>17. LIMITATION OF ABSTRACT</th>
<th>18. NUMBER OF PAGES</th>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT</td>
<td>b. ABSTRACT</td>
<td>c. THIS PAGE</td>
<td>K.T.Arasu</td>
</tr>
<tr>
<td>SAR</td>
<td>SAR</td>
<td>SAR</td>
<td>K.T.Arasu</td>
</tr>
</tbody>
</table>
I. OBJECTIVES:

We continue our mathematical frame work 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 proposed are very algebraic and number theoretic. Many new families of sequences with low correlation values are found.

The Correlation Problem actually covers a broad fundamental combinatorial problem with deep mathematical content. Specific solutions to the Correlation Problem have practical diverse applications in communications, experimental design, laboratory instrumentation and manufacturing. As technology changes so too will the instances of the Correlation Problem which need solving. It is therefore important to develop better mathematical techniques for attacking the problem.

II. STATUS OF EFFORT:

This report describes progress to date on designing signals using combinatorial designs. We shall regard signal design problems as “The Correlation Problem”. The Correlation Problem is to design sequences with specified lengths with entries chosen from a specified finite set so that all non-trivial periodic autocorrelations lie in a prescribed restrictive set. Usually the autocorrelations are computed using a quadratic form.

Mathematical tools from algebraic number theory, representation theory and group theory are employed to investigate the theory of their existence leading to new families of these arrays and some
generalizations thereof. Using their relationship with so-called circulant weighing matrices, structural theorems on these latter objects are proved, thereby answering their existence status in many open cases. The major task of this project is to design signals based on complex roots of unity. The relevant research is in progress.

Periodic sequences and multidimensional arrays whose entries are either 0, 1 and -1 or the complex roots of unity are studied. These sequences/arrays with low autocorrelation values are useful in reliable synchronization problems. Some new constructions of a class of such sequences have been obtained. A few structure theorems for these mathematical objects have also been proved. Another joint work with my student Alexander Gutman has resulted in classifying the existence status of periodic ternary sequences (i.e. with entries 0, 1 and -1) all of whose out-of-phase autocorrelations are zero.

III. ACCOMPLISHMENTS:

A square matrix W of order n with entries from \{0, -1, +1\} satisfying \(W W^t = k \text{In}\) is said to be a weighing matrix of order n with weight k. If the underlying matrix is also circulant, we therefore get a perfect ternary sequence of period n.

In [1], we employ theoretical and computational techniques to construct new weighing matrices constructed from two circulants. In particular, we construct \(W(148; 144)\), \(W(152; 144)\), \(W(156; 144)\) which are listed as open in the second edition of the Handbook of Combinatorial Designs. In addition, we obtain infinite families of weighing matrices constructed from two circulants, such as \(W(68 + 2k; 52)\) and \(W(108 + 2k; 64)\) for all \(k > 0\), based on ternary complementary pairs. We also fill a missing entry in Strassler's table with answer 'YES', by constructing a circulant weighing matrix of order 142 with weight 100.

In [2], we give an overview of perfect binary sequences of even length. We give a theoretical explanation for the existence of a perfect binary sequence of length 14. We show that no balanced perfect binary sequence of length 14 can exist. Both results have been checked earlier by computer. Our results provide some new ideas using which one can construct several classes of binary sequences with desirable correlation properties.

In [3], Gutman and the P.I. investigate circulant weighing matrices of various weights. We have settled the existence question in orders upto 200. This paper fills many missing entries in a table of Strassler on Circulant Weighing Matrices.

In [4], we develop a new method for proving the nonexistence of a certain class of circulant weighing matrices. Using this method we prove the nonexistence of two open cases, namely \(CW(154; 36)\) and \(CW(170; 64)\).

In [5], we prove the non-existence of \(CW(110; 100)\) using algebraic methods. This case has been previously open. Our methods are very ad hoc and we hope that the ideas we present can be extended further to study other cases. The parameter pair \(110; 100\) is particularly interesting since its order n is just one short of 111 and the case \(CW(111;100)\) (even the \(W(111; 100)\) without the "circulant" requirement) would give rise to a projective plane of order 10 which has been shown not to exist.
In [6], we shall discuss perfect sequences and perfect arrays (binary, ternary, quaternary, p-ary for any prime p) and certain variations of them. Binary perfect sequences and their variations have applications in various areas such as signal processing, synchronizing and distance measuring radars. This survey discusses their p-ary analogs, other variations and related matters. Many new results are also presented.

Paper [7] 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 p<sup>th</sup> 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. In this paper, we give the outline of some new construction methods for these interesting combinatorial objects; the ideas reported here basically forming a summary of results obtained jointly with John Dillon and Kevin Player. Our joint paper (nearing its final stage of preparation) will contain detailed proofs of the new results mentioned in this article. The main tools used in our new research are: Stickelberger congruence on Gauss Sums and Hasse-Davenport formulae.

In [8], we provide an overview of the known families of perfect binary sequences of period 2 (mod 4). We present previously unknown examples of balanced perfect binary sequences of period 38 and 50, due to computer results.

The following almost difference sets due to Arasu and Little readily give the optimal binary sequences having autocorrelation values {2,-2}:

\[ D=\{0,1,4,5,6,7,10,12,13,20,22,24,25,26,28,31,33,34,35\} \text{ is a } (38,19,9,28) - \text{almost difference set in } \mathbb{Z}_{38}. \]

\[ D=\{0,1,2,4,5,8,9,10,12,15,16,17,18,19,22,24,26,28,29,31,34,35,37,39,40\} \text{ is a } (50,25,12,37) - \text{almost difference set in } \mathbb{Z}_{50}. \]

We give the corresponding balanced optimal binary sequences below:

Length 38: ++-+-+-++-+-+-+-+-+-+-+-+

Length 50: +++++-+-+-+-+-+-+-+-+

The above two examples are balanced – in the sense, the number of 1's and -1's in the sequence is the same.

In [9], we investigate antenna arrays and combinatorial designs. Radar systems, satellite and ground communications, sensors and biomedical applications often make use of antenna arrays for 3-D scanning with a suitable beam pattern shape in the whole angular region. Use of planar arrays to accomplish this typically results in expensive solutions, if one requires high resolutions and therefore large apertures. Thinning techniques attempt to reduce the number of required elements without sacrificing the radiation properties of the original structures. This important area of research that deals with the designing of thinned planar arrays has spanned over five decades. Use of combinatorial structures like difference sets and their variations in the thinning techniques has been flourishing. Recent activity in the area of difference sets and almost difference sets has rekindled the interest in the
antenna community. In this paper, we also report some recent developments in the mathematical arena (difference sets, etc.) – with the hope that antenna researchers can take advantage of the progress made by their peers from the combinatorics community. It is fitting to note that signal design problems studied in this effort are related to the difference sets and their variations, thus this tangential development of relating developed notions in the antenna area is intriguing and may pave a way to elaborate on these in the next proposal and future efforts in collaboration with AFOSR.

In [10], we discuss group developed weighing matrices, which could be viewed as higher dimensional analogs of perfect sequences used in signal designs. These are also of practical importance as these could be employed in problems mentioned in the previous paragraph. 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. Through a combination of extending previous results and by giving explicit constructions we will answer the question of existence for 318 such matrices of order and weight both below 100. At the end we are left with 98 open cases out of a possible 1022. Further, some of the new results provide insight into the existence of matrices with larger weights and orders.

Paper [11] deals with sequence pairs. Two sequences of which in-phase and out-phase crosscorrelation functions are respectively two unequal constants is called as a sequence pair with two-level autocorrelation function. Such sequence pairs are considered as the extension of usual sequences with ideal autocorrelation functions. The binary sequence pair with two-level autocorrelation function has an equivalent relationship with the difference set pair, as a new concept of combinatorial mathematics, which means that the difference set pair can be used in the research of the sequence pair with two-level autocorrelation functions as a kind of important tool. In this paper, four infinite families of difference set pairs are constructed, accordingly deriving corresponding binary sequence pairs. The correlation and spectrum property of the sequence pairs with two-level autocorrelation functions is presented. In addition, a new class of binary sequence pair sets with zero correlation zone applying in quasi-synchronous code multiple division address is constructed by interleaving perfect binary sequence pairs and Hadamard matrix.

Paper [12] discusses Hadamard matrices. Square matrices with entries plus or minus one, all of whose distinct pairs of rows are orthogonal possess some very interesting optimal properties. We shall refer to these as “Hadamard” matrices. They have a variety of applications in several disciplines. In this survey article, we provide the state of the art of their existence problem, primarily focusing on a subclass which admits a group action. It must be noted that P. Kesava Menon has made significant and fundamental contributions to this area of research. We shall also mention certain variations of this theme which are of theoretical and practical interest.

We are also in the process of building up new algebraic machinery which would help us construct several classes of perfect sequences whose entries are complex roots of unity. The major paper (62 page preprint is undergoing some revisions and improvements).

IV. PUBLICATIONS:

10. K.T. Arasu and Jeff Hollon, Group weighing matrices, Submitted to Discrete Mathematics

V. CONFERENCE PRESENTATIONS

1. Menon-Hadamard difference sets, Two plenary talks at the international conference in Number theory – the instructional portion of it), University of Calicut, India, August 2009.
2. Perfect sequence constructions, (one hour invited talk at the international conference in Number theory), University of Calicut, August 2009.
3. Perfect sequence constructions, Loyola University, Chicago, September 2009.
4. Perfect sequence constructions, Florida Atlantic University, December 2009.
8. Invited colloquium at Anna University, Chennai, India, August 2010. Title: Applicability of Classical Mathematics in Contemporary World.
17. Lecture series (8 lectures for a total of 10 hours) at Cochin University of Science and Technology, December 2010. Title: From combinatorial design theory to sequences and arrays with desirable autocorrelation properties.
18. Invited colloquium at University of Slovenia, June 2010. Title: Perfect Sequence Constructions.
20. Invited lectures on “Algebraic methods in the construction of sequences with desirable correlation properties”, Cybersecurity Research Center at St Joseph’s College, Irinjalakuda, Kerala, India, June 2011. (Total of 4 lectures)
25. Invited colloquium at University of Central Florida, June 9, 2011. Title: Perfect Sequence constructions motivated by engineering applications.
26. Invited seminar at University of Central Florida, December 23, 2011. Title: Pseudorandom Sequences,
27. Invited seminar at University of Missouri at St Louis, December 30, 2011. Title: Perfect Sequence Constructions.

VI. HONORS:

1. Two plenary talks at the international conference in Number theory – the instructional portion of it), University of Calicut, India, August 2009.
2. Invited speaker to deliver 3 lectures at the NATO Advanced Study Institute (ASI) "Information Security and Related Combinatorics", held in Croatia, May 31 - June 11, 2010.
3. Group weighing matrices, 45-minute long invited talk at the satellite conference on Combinatorics and Graph Theory in conjunction with the International Congress of Mathematicians, India, August 2010.
4. Perfect Sequence constructions motivated by communication engineering applications,: Invited plenary 1-hour talk at the second international conference on ADVANCED COMPUTING AND COMMUNICATION TECHNOLOGIES FOR HIGH PERFORMANCE APPLICATIONS, Cochin, India, December 2010.

6. Entropy and Hadamard Matrices, Invited 1-hour lecture on workshop on queuing theory, Anna University, Chennai, India, November 2010.

