AFRL-SR-BL-TR-00-

0057

REPORT DOCUMENTATION PAGE

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Feb. 9, 2000	Final (July 1, 1996 - Nov. 30, 1999)

4. TITLE AND SUBTITLE
High Volume Communication Channels
(A mathematical investigation)

5. FUNDING NUMBERS
AFOSR Grant
F49620-96-1-0328

6. AUTHORS

K.T. Arasu

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Department of Mathematics & Statistics
Wright State University
Dayton, OH 45435

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR
110 Duncan Avenue, Suite B115
Bolling AFB, DC 20332-0001

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release,
distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

Time-discrete one and two-dimentional sequences and arrays with perfect autocorrelation functions are studied. Such sequences find applications in signal processing and as aperture functions for electromagnetic and acoustic imaging. Two dimensional perfect arrays are also applicable in 2-D synchronization and time-frequency coding. 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.

14. SUBJECT TERMS
Sequences, arrays, correlation

15. NUMBER OF PAGES
7

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-1
298-102

Final Report on

AFOSR Grant F49620-96-0328
High Volume Communication Channels:
A Mathematical Investigation

for the period covering July, 1996 to November 1999

Principal Investigator: K.T.Arasu,
Department of Mathematics and Statistics,
Wright State University,
Dayton, OH 45435
Phone number: 937 775 3828
Fax Number: 937 775 2081
Email: karasu@math.wright.edu
karasu@desire.wright.edu

1. Objectives:

Time-discrete one and two-dimensional sequences and arrays with perfect autocorrelation functions are studied. Such sequences find applications in signal processing and as aperture functions for electromagnetic and acoustic imaging. Two dimensional perfect arrays are also applicable in 2-D synchronization and time-frequency coding. 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.

2. Status of effort:

Periodic sequences and multidimensional arrays whose entries are either 0, 1, or -1 or the complex fourth roots of unity are studied. These sequences/arrays with low autocorrelation values are useful in reliable synchronization problems. The present final report summarizes a few structure theorems the PI has proved and discusses the contents of papers that came out during this reporting period.

3. Accomplishments:

Periodic sequences with entries plus or minus one all but one of whose autocorrelation coefficients are zero were studied by Wolfmann. Using their equivalence to certain nice

subsets in a cyclic group whose order equals the period of the corresponding sequence (these subsets are called divisible difference sets), we obtain sequences of period 8, 12 and 28. Further structure theorems using the factorization of ideals in a suitable algebraic number field are also proven. The theory developed in this paper [1] could be used for other types of sequences and arrays. This joint work with Ma and Voss has appeared in the Journal of Algebra.

In [2], (a joint work with Ma), we characterize those abelian groups which admit a McFarland difference set of order 81. These difference sets are variations of the well-known Hadamard difference sets, which are equivalent to perfect binary arrays. Our methods do not make use of the widely made assumption known as "self-conjugacy". (This roughly means that the complex conjugation fixes the prime ideal factors of the principal ideal generated by the order of the corresponding difference set). We thus are able to fill two missing entries in Kopilovich's table. (Incidentally Kopilovich is a Ukrainian engineer who is writing up a monograph in this area that connects radar problems and "my" kind of mathematics. Our results will be cited in his book.) This paper [2] has appeared in the Journal Designs, Codes and Cryptography.

A square matrix W of order n with entries from (0, -1, +1) satisfying W Wt = k I_n 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. Using very interesting facts about finite fields, we provide a construction of a family of circulant matrices of weight 33t and weight 25, for each positive integer t. Consequently we fill a missing entry in the CRC handbook (Section on weighing matrices by Craigen). While not a single matrix of order 33 and weight 25 was known before, we actually constructed a circulant one, to the surprise of experts in this field. Our new matrices also give a rise to a new class of orthogonal designs. This paper [3] has appeared in the Journal of Combinatorial Designs.

In [4] Seberry and the P.I. investigate circulant weighing matrices of various weights whose order equal the number of points on a finite projective plane. This is an extremal case and the investigation is very theoretical. We have settled the existence question in orders upto 25. This paper has appeared in the Australasian Journal of Combinatorics.

In [5], (joint work with Balasubramanian and Evans), we point out the connection between quadratic starters in a finite field and a class of nested row-column designs. As a consequence we provide an infinite class of such designs, generalizing a few sporadic examples obtained earlier by others. This paper has appeared in the Journal of Combinatorics and Combinatorial Computing.

The construction of periodic sequences with good correlation properties is very important in signal processing. Many applications require the knowledge of sequences and their correlation functions. In the binary case, sequences with period v can be equivalently described as subsets D of the cyclic group of order v. The distribution of the differences that can be formed with elements from this subset D can be computed from the correlation function of the corresponding sequence. Therefore we obtain the following statement: instead of

looking for sequences with nice correlation functions, we can equivalently look for subsets of cyclic groups with a nice distribution of differences. (Of course the underlying group is in general abelian if we deal with higher dimensional arrays). A difference set is a subset of a group such that the list of differences contains every non-identity element equally often. These difference sets correspond to sequences/arrays whose correlation has just two values. Small variations of this "uniform difference property" correspond to small variations of the "two-value-property" of the sequence. Thus the study of difference sets and their generalizations is important in designing sequences with desirable correlation properties.

In [6] we provide the present state of the art of abelian difference sets. This article will appear as a chapter in the Encyclopedia of Electrical and Electronics Engineering, to be published by Wiley. In [7] we review some existence and nonexistence results, in an attempt to introduce the algebraic ideas to a reader who is interested in getting into this interesting field. This paper has appeared in the special volume on Algebra to be published by the Indian Academy of Sciences. In [8] we prove a new structure theorem for abelian difference sets. The proof techniques generalize to yield similar theorems for divisible difference sets and partial difference sets. (Incidentally partial difference sets are equivalent to a class of 2-weight codes). As applications, we establish the existence status of two previously open cases of abelian difference sets: (243,121,60) Hadamard difference sets in $Z_9 \times Z_{27}$ and (351,126,45) difference sets in Z_{351}, thereby filling two missing entries in a recent table of Vera Lopez and Sanchez. This paper has been accepted by the Journal of Statistical planning and Inference.

A square matrix W of order n with entries from {0, -1, +1}) satisfying $W W' = k I_n$ is said to be a weighing matrix of order n with weight k. Here W' denotes the transpose of W and I_n denotes the $n \times n$ identity matrix. If the underlying matrix is also circulant, the first row of W defines a perfect ternary sequence of period n. Circulant weighing matrices of order n with weight k are denoted by WC(n,k). Under some conditions, we prove a reduction theorem for these: the existence of WC(n,k) implies that of WC(n/2,k/4). Our proof actually provides a method to recover the larger matrix from the smaller one, thus giving a strategy to construct these objects. As a consequence of our theorem, we settle the previously open existence status of WC(n,k) for the pairs (n,k) = (125,25), (44,36), (64,36), (66,36), (80,36), (72,36), (118,36), (128,36), (136,36), (128,100), (144,100), (152,100), (88,36), (132,36), (160,36), (166,36), (176,36), (198,36), (200,36) and (200,100). These results are contained in [9]. This paper has appeared in the Australasian Journal of Combinatorics.

In [10], we use the notion of multipliers and intersection numbers to settle the existence status of nine open cases in a recent table of Lopez and Sanchez: (5085,124,3) difference set in $Z_3 \times Z_3 \times Z_5 \times Z_{113}$, (1975,141,10) difference sets in $Z_5 \times Z_5 \times Z_{79}$ or Z_{1975}, (1161,145,18) difference sets in $K \times Z_{43}$, where K is any abelian group of order 27, (448,150,50) difference sets in three groups of order 448 and (16513,129,1) difference sets in $Z_7 \times Z_7 \times Z_{337}$. This paper will appear in Combinatorial Mathematics and Combinatorial Computing. 1n [11] we investigate cyclic relative difference sets with classical parameters. The motivation comes from PI's old result in which the 20-year old Waterloo problem was settled. That paper dealt with: which Singer difference sets (equivalently m-sequences with perfect correlation values)

can be lifted to relative difference sets in groups of twice the original order. The present paper studies the affine analog of this problem and answers a question of Pott in his recent monograph affirmatively. Complete characterization is given. A new family of cyclic relative difference sets come out as a by-product. These must give rise to some interesting class of sequences with nice correlation properties, a property we have not studied yet. My guess: the resulting sequences will have complex valued, some n-th roots of unity for a suitable n. This paper has been submitted to the J. Combinatorial Theory (A).

In [12] we show that a circulant Hadamard matrix of order n is equivalent to a relative difference set in the group $Z_4 \times Z_n$ where the forbidden subgroup of order 2 is contained in the Z_4 component. Then we obtain new exponent bounds for the Sylow p-subgroups for odd primes p. These are sufficient to establish the existence status of circulant complex Hadamard matrices for many orders. Using character theory and algebraic number theory, we prove several structure theorems for these.

In [13], we investigate perfect ternary arrays. A perfect ternary array is an r-dimensional array with entries 0, +1 and -1 such that all of its out-of-phase periodic autocorrelation coefficients are zero. Such an array is equivalent to a group developed weighing matrix. These can therefore be considered as elements in the group ring ZG for a suitable abelian group G. Using this approach we investigate these objects, restricting our attention mostly to one- and two-dimensional (so called cyclic and bicyclic) cases.

In [14], we study two dimensional arrays of fourth root of unity, which have perfect periodic autocorrelation properties. A two dimensional perfect array PBA *(s,t)* is a $s \times t$ (1,-1)-array with perfect autocorrelation properties. Recently, a re-examination of the connection between perfect binary arrays and certain combinatorial designs has sparked advances in both areas of study. Yet the only known two dimensional examples (with $s \geq t$) *have* $s=2^a+c+3^b$ *and* $t=2^a3^b$, where c=0 *or 2,* $a \geq 0$, $b \geq 0$ and b=0 unless $2a + c \geq 2$.

In this paper, we consider two dimensional arrays with perfect periodic autocorrelation properties whose entries are fourth roots of unity. Here the answer to the existence question appears to be very different. Working with fourth roots of unity allows many odd primes other than 3 to divide the dimensions of two dimensional arrays with perfect autocorrelation. In this paper, we obtain examples of two dimensional perfect quaternary arrays for many small dimensions for which perfect binary arrays are not known. These include *(s,t)=(3, 6), (3, 24), (3, 48), (6, 12), (6, 48), (6, 96), (7, 28), (7, 56), (7, 112), (9, 18), (9,72), (12,24), (12, 96), (14,14), (14, 28), (14, 56), (14, 112), (24, 48), (27, 54), (28, 28), (28, 56), (28, 112), (42, 84), (48, 96), (51, 102), (54, 108), (56, 56), (56, 112), (84, 84), (102, 102)* and *(112, 112).* It is interesting to note that we also obtain $t \times t$ perfect quaternary arrays for some values of t for which there cannot exist perfect binary array (t=14 and 28, for instance).

In [15], we answer a question of Pott on almost perfect sequences. Periodic binary (plus-minus) sequences all but one of whose out-of- phase autocorrelation coefficients are zero

are studied by Wolfmann. Using the equivalence of these almost perfect sequences to certain cyclic divisible difference sets (noted by Bradley and Pott), we settle the existence status of a previously open case of an almost perfect sequence of length 852, thereby answering a question of Pott negatively.

4. Publications:

1. On a class of almost perfect sequences, (with S.L.MA and *N.J.Voss),* J. Algebra. 192, 641-650 (1997).

2. Abelian difference sets without self-conjugacy, (with S.L.Ma), Designs, Codes and Cryptography, 15, 223-230, 1998.

3. New weighing matrices of weight 25, Journal of Combinatorial Designs, 5, 1-5 (1997).

4. Circulant weighing matrices, (With Jennifer Seberry) to appear in Australasian J. Combinatorics.

5. A new family of nested row-column designs, (with Balasubramanian and A.B.Evans), Journal of Combinatorial Mathematics and Combinatorial Computing, 29(1999), 139-144.

6. Theory of difference sets, (with A. Pott), to appear in the Encyclopedia of Electrical and Electronics Engineering, Wiley.

7. On abelian difference sets, (with S.K.Sehgal), In : Algebra: Some recent Advances, Ed. I.B.S.Passi, Indian Academy of Sciences, 1-29 , 1999.

8. A nonexistence result on difference sets, partial difference sets and divisible difference sets, (with S.L.Ma) , to appear in J. Stat. Planning and Inference.

9. A reduction theorem for circulant weighing matrices, Australasian Journal of combinatorics,
   18(1998), 111-114.

10. Nonexistence of some difference sets, (with S.K.Sehgal), J.Comb. Math. and Comb. Computing, (in press).

11. Cyclic relative difference sets with classical parameters, (with J.F. Dillon, K.H. Leung and S.L.Ma), submitted to J. Comb. Theory (A)..

12. On circulant complex Hadamard matrices, (with W. de Launey and S.L.Ma), submitted to Designs, Codes & Cryptography.

13. Perfect ternary arrays (with J.F. Dillon), NATO volume on Difference Sets and Sequences and Correlation Properties, Ed. A.Pott et al, Kluwer, 1999, 1-15.

14. Two dimensional perfect quaternary arrays, (with W. DeLauney), submitted to IEEE trans. Info. Th.

15.Answering a question of Pott on almost perfect sequences (with N.J.Voss), Designs, Codes & Cryptography, 18, 7-10, 1999.

5. Personnel supported

Jeffrey Linthicum, Graduate research assistant

6. Conference Presentations

1. Invited lecture at the third International Conference of Combinatorics and Statistics at Portland, Maine, July 1997

2. Keynote address at the International conference on Combinatorics, May 1997, Hefei, China

3. Invited colloquium at the University of Hong Kong, May 1997

4. Invited colloquium at the Mathematical Institute, Madras, India, June 1997
5. Keynote addresses at the NATO workshop on Difference sets, sequences and their correlation properties, August 1998

6. Invited speaker at the Ohio State University - Denison University meeting, May 1998

7. Colloquium at the National Security Agency, July 1998

8. Invited one-hour lecture at the AMS meeting in Melbourne Australia, July, **1999**.

9. Invited speaker at the Victorian Algebra Conference, Melbourne, July, 1999.

10. Invited talk to the AMS Sectional meeting at UNLV, April, 1999.

11. Colloquium at Sinclair College, May, 1999.

7. Honors

1. I have been invited to write a chapter on Difference sets and its relation to Communication Engineering by Wiley Publishers. This 40 to 50 page article will be one chapter of an encyclopedia they are publishing on Computational Engineering.

2. Invited to give keynote addresses at the NATO workshop in Germany, in August 1998. It was a gathering of well-known engineers and mathematicians working in this area of sequence designing with desirable correlation properties.