

1-1-1995

Periodic complementary binary sequences

Maria Consuelo C Pickle
University of Nevada, Las Vegas

Follow this and additional works at: <https://digitalscholarship.unlv.edu/rtds>

Repository Citation

Pickle, Maria Consuelo C, "Periodic complementary binary sequences" (1995). *UNLV Retrospective Theses & Dissertations*. 470.

<https://digitalscholarship.unlv.edu/rtds/470>

This Thesis is protected by copyright and/or related rights. It has been brought to you by Digital Scholarship@UNLV with permission from the rights-holder(s). You are free to use this Thesis in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/or on the work itself.

This Thesis has been accepted for inclusion in UNLV Retrospective Theses & Dissertations by an authorized administrator of Digital Scholarship@UNLV. For more information, please contact digitalscholarship@unlv.edu.

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
313/761-4700 800/521-0600

PERIODIC COMPLEMENTARY
BINARY SEQUENCES

by

Maria Consuelo C. Pickle

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Science

in

Mathematical Sciences

Department of Mathematical Sciences
University of Nevada, Las Vegas
May 1995

UMI Number: 1374899

UMI Microform 1374899

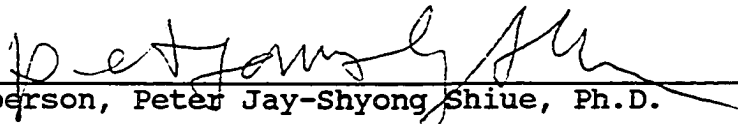
Copyright 1995, by UMI Company. All rights reserved.

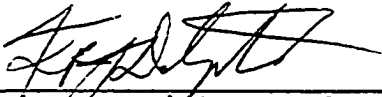
This microform edition is protected against unauthorized
copying under Title 17, United States Code.


UMI


300 North Zeeb Road
Ann Arbor, MI 48103

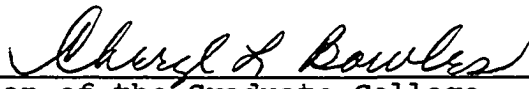
The thesis of Maria Consuelo C. Pickle for the degree of Master of Science in the Mathematical Sciences is approved.


Chairperson, Peter Jay-Shyong Shiue, Ph.D.


Examining Committee Member, Rohan Dalpatadu, Ph.D.


Examining Committee Member, Harold Bowman, Ph.D.


Graduate Faculty Representative,
R. Venkatasubraman, Ph.D.


Interim Dean of the Graduate College,
Cheryl L. Bowles, ED.D.

University of Nevada, Las Vegas,
May 1995

ABSTRACT

Since man devised a way to count, patterns or sequences of numbers have held mathematicians' attention. However, it has only been recently that binary sequences have received so much attention due to their compatibility with computers. For the past 30 years the fields of Electrical Engineering, Computer Engineering and Mathematics have done some extensive research in this area because of its many applications in radar, sonar and the reliability and security of communication systems such as digital communications, faxes, telecommunications and electronic transfers especially in banking and finance. First discussed will be the Perfect Binary Sequence. Then the Golay Complementary Sequence and finally the general case of the Periodic Complementary Binary Sequence or PCBS.

TABLE OF CONTENTS

TITLE	PAGE
ABSTRACT	iii
ACKNOWLEDGEMENTS	v
CHAPTER 1	
Introduction	1
Background	2
CHAPTER 2	
Perfect Binary Sequences	3
CHAPTER 3	
Golay Complementary Sequences	8
CHAPTER 4	
Periodic Complementary Binary Sequences	18
CHAPTER 5	
Conclusion	28
BIBLIOGRAPHY.....	29

ACKNOWLEDGEMENTS

First of all, I would like to thank my parents for all their help and support throughout my life. Next I would like to thank Dr. Peter Shiue, Dr. Rohan Dalpatadu and Mrs. Margie Wells for easing my way through my masters. Especially, Dr. Shiue for providing all of my reference materials and for choosing such an interesting thesis topic that fit so well with my electrical engineering and mathematical background. Last but not least, I would like to thank my husband for standing by me through all these years of college.

CHAPTER 1

INTRODUCTION

This thesis examines binary sequences, specifically Periodic Complementary Binary Sequences or PCBS. By definition a set of binary sequences becomes a set of PCBS, if the sum of the periodic autocorrelation functions of all sequences is a delta function. What we mean by a delta function is that the value of the function when evaluated is always zero except when evaluated at zero.

If a single sequence is a delta function then this is called a perfect binary sequence. If two sequences of length n added together equals a delta function then it is called a Golay Complementary Sequence. Perfect Binary Sequences and Golay Complementary Sequences have already been investigated while the general case has not. The main focus of this research thesis will be the general case which has many applications in communications. Namely, it can address several problems pertaining to radar, sonar and time-position synchronization leading to finding two-dimensional patterns of +1 (dots) and -1

(blanks), for which the autocorrelation function such as the ambiguity function of radar analysis, has minimum out-of-phase values and thus greater accuracy. Also discussed are the properties and certain unique qualities inherent to these types of sequences which can be utilized in communication systems as well as certain criteria to help find these sequences.

BACKGROUND

The usefulness of Periodic Complementary Binary Sequences (PCBS) stems from the fact that physical phenomena can often be represented by correlation functions. However, whatever the medium, be it wavelengths or frequencies, the basic model remains the same. The PCBS separate or filter out the background "noise" from the signals wanted. Golay first used such sequences to separate light into its spectrum hence the title of his paper "Multislit Spectrometry" [5]. Since then it has been used to facilitate and enhance radar, sonar and laser imaging. It is also in use in cryptography systems such as wire transfers and faxes.

CHAPTER 2

PERFECT BINARY SEQUENCES

First let us clearly define what we mean by binary sequences. We assume that all sequences are taken from $F_2 = \{+1, -1\}$.

DEFINITION:

If a sequence G of length n , where each element g_i is taken from $F_2 = \{+1, -1\}$, then the periodic autocorrelation function is defined as

$$P_g(i) = \sum_{j=1}^{n-1} g_i g_{i+j} \quad \text{for all } i, j = 0, 1, 2, \dots, n-1$$

where the second subscript is actually chosen from the complete set of residue(mod n) or $0 \leq c \leq n-1$,
 $(i + j) \equiv c \pmod{n}$.

The clarification of this definition is shown clearly in the following example.

EXAMPLE 1

Let $T = \{ 1, -1, 1, -1 \}$, Then

$$\begin{aligned}
 P(0) &= \begin{matrix} t & t & & & \\ & 1 & 1 & & \\ t & & 2 & 2 & \\ & & & 3 & 3 \\ & & & & 4 & 4 \end{matrix} \\
 &= (1)(1) + (1)(1) + (1)(1) + (1)(1) \\
 &= 4 \quad \text{and}
 \end{aligned}$$

$$\begin{aligned}
 P(1) &= \begin{matrix} t & t & & & \\ & 1 & 2 & & \\ t & & 2 & 3 & \\ & & & 3 & 4 \\ & & & & 4 & 1 \end{matrix} \\
 &= (1)(-1) + (-1)(1) + (1)(-1) + (-1)(1) \\
 &= -4 \quad \text{and}
 \end{aligned}$$

$$\begin{aligned}
 P(2) &= \begin{matrix} t & t & & & \\ & 1 & 3 & & \\ t & & 2 & 4 & \\ & & & 3 & 1 \\ & & & & 4 & 2 \end{matrix} \\
 &= (1)(1) + (-1)(-1) + (1)(1) + (-1)(-1) \\
 &= 4 \quad \text{and}
 \end{aligned}$$

$$\begin{aligned}
 P(3) &= \begin{matrix} t & t & & & \\ & 1 & 4 & & \\ t & & 2 & 1 & \\ & & & 3 & 2 \\ & & & & 4 & 3 \end{matrix} \\
 &= (1)(-1) + (-1)(1) + (1)(-1) + (-1)(1) \\
 &= -4
 \end{aligned}$$

Thus the values of $P(i)$ are found.

However, we have an easier method to find

$P(i)$. For any given binary sequence

$S = \{ s_1, s_2, \dots, s_n \}$ of length n , first arrange

the elements of the sequence S' as the first row of a square circulant matrix we now call S . Second find

T
 SS and the first row of this matrix are the
 corresponding values of $P_s(0), P_s(1), \dots, P_s(n-1)$.

From now on this "matrix" method will be used to find
 the individual $P_s(i)$'s.

However there are certain types of sequences
 of particular interest. The first type is called a
 Perfect Binary Sequence (Storer and Turyn, [9]).

DEFINITION :

Let $P = \{ p_1, p_2, p_3, \dots, p_n \}$ be a sequence of

length n from F_2 . If the periodic autocorrelation

function

$$P_p(i) = \begin{cases} n & \text{if } i = 0 \\ 0 & \text{if } i \neq 0, \end{cases}$$

then P is called a perfect binary sequence.

EXAMPLE 2

Let $T_a = \{ -1, -1, -1, 1 \}$ be a sequence of length 4.

We then form the square circulant matrix C using the
 elements of T_a as the first row. So

$$C = \begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix} \quad \text{Then,}$$

$$\begin{aligned}
 CC^T &= \begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix} \begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix} \\
 &= \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}
 \end{aligned}$$

Thus T_a is a Perfect Binary Sequence.

Recall that we are only concerned with the first row as each entry corresponds to a particular $P_t(i)$.

EXAMPLE 3

Let $T_b = \{1, 1, 1, -1\}$ be a sequence of length 4. Again form the square circulant matrix D using the elements of T_b as the first row. So

$$D = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix} \quad \text{Then,}$$

$$\begin{aligned}
 DD^T &= \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix} \\
 &= \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}
 \end{aligned}$$

Thus T_b is Perfect Binary Sequence.

Notice that they are symmetric which leaves us the possibility that if another perfect binary sequence exists, let us call it T_c , is $-T_c$ also a perfect binary sequence.

Unfortunately only the sequences shown in examples 2 and 3 have been found so far as exhibiting these traits and no other perfect binary sequence has been found other than the two given above (Storer And Turyn, [9]). It remains open whether any more such sequences exist and if so are there any criteria in which to find them.

CHAPTER 3

GOLAY COMPLEMENTARY SEQUENCES

Since perfect binary sequences are so few, the next logical step would be two sequences, that when added together fit the periodic autocorrelation function definition. This was proposed by Marcel Golay [5], in his article "Multislit Spectrometry". He used the two sequences to separate light into its individual spectrum of colors. Recall each color has its own particular wavelength and the sequences act like a filter letting pass only certain wavelengths.

DEFINITION:

$$\text{Let } X = \left\{ \begin{array}{l} A = \{ a_1, a_2, \dots, a_n \}, \\ B = \{ b_1, b_2, \dots, b_n \} \end{array} \right\}$$

be two sequences from F_2 both of length n . Then

$$\begin{aligned} P_X(i) &= P_A(i) + P_B(i) \\ &= \sum_{i=1}^{n-1} a_i a_{i+j} + \sum_{i=1}^{n-1} b_i b_{i+j} \end{aligned}$$

where $j = 0, 1, 2, \dots, n-1$

If the periodic autocorrelation function

$$P_X(i) = \begin{cases} 2n & \text{if } i = 0 \\ 0 & \text{if } i \neq 0, \end{cases}$$

then X is called a Golay Complementary Sequence.

Here again the "matrix" method can be used to find $P_X(i)$. In this case, A is the square circulant matrix constructed using the first sequence A' as the first row of the matrix, B is the second square circulant matrix constructed using the second sequence B' as the first row of the matrix and

$$AA^T + BB^T = 2nI_n$$

holds for the Golay Complementary Sequence.

EXAMPLE 4

Let $X = \{ A'_1 = \{ 1, 1 \}, B'_1 = \{ 1, -1 \} \}$ Then

$$\begin{aligned} A_1 A_1^T &= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \quad \text{and} \end{aligned}$$

$$\begin{aligned} B_1 B_1^T &= \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix} \quad \text{and} \end{aligned}$$

$$\begin{aligned}
 \begin{matrix} & T & & T \\ A & A & + & B & B \\ 1 & 1 & & 1 & 1 \end{matrix} &= \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix} \\
 &= (2)(2) I_2
 \end{aligned}$$

Thus X is a Golay Complementary Sequence.

EXAMPLE 5

$$\text{Let } X = \left. \begin{array}{l} A'_2 = \{ 1, -1, -1, 1, -1, 1, -1, -1, -1, 1 \} \\ B'_2 = \{ 1, -1, -1, -1, -1, -1, -1, 1, 1, -1 \} \end{array} \right\}$$

Then X can be easily verified as a Golay Complementary Sequence.

The computations for finding such sequences are very lengthy even with the aid of computers. Fortunately for us, there are several criteria to help us find Golay Complementary Sequences.

THEOREM 1 (Andres And Stanton, [1])

EXISTENCE CONDITION FOR SPECIAL CASE OF GOLAY COMPLEMENTARY SEQUENCE

If there exists a Golay Complementary Sequence of length n, then n is the sum of two squares and n is even.

PROOF

Given the Golay Complementary Sequence

$$A' = \{ a_1, a_2, \dots, a_n \}, B' = \{ b_1, b_2, \dots, b_n \}.$$

Let length $n = 2L$ and let us rewrite each pair of the Golay Complementary Sequence as

$$P_a(i) + P_b(i) = P_x(i) = 4L$$

since every pair of sums are zero except for when

$i = 0$. For this case $P_a(0) = P_b(0) = n = 2L$.

Next, sum up all the individual pairs. Thus

$$\sum_{i=0}^{n-1} [P_a(i) + P_b(i)] = 4L$$

But by definition this is the summation of $a_i a_{i+j}$

and the $b_i b_{i+j}$. So this can be written as

$$\sum_{i,j=0}^{n-1} a_i a_{i+j} + \sum_{i,j=0}^{n-1} b_i b_{i+j} = 4L$$

where the $i+j$'s are actually the residue (mod n).

Now let us separate $P_a(0)$ and $P_b(0)$ from the others.

So
$$\sum_i a_i^2 + \sum_{i,j} a_i a_j + \sum_i b_i^2 + \sum_{i,j} b_i b_j = 4L \quad (1)$$

Recall though that only $a_i a_i$ and $b_i b_i$ have values other

than zero. Thus

$$\sum_{i,j} a_i a_j + \sum_{i,j} b_i b_j = 0 \quad (2)$$

and clearly twice this summation is still zero.

Next substitute twice (2) into (1) and we have

$$\sum_i a_i^2 + 2 \sum_{i,j} a_i a_j + \sum_i b_i^2 + 2 \sum_{i,j} b_i b_j = 4L$$

So
$$\left(\sum_i a_i \right)^2 + \left(\sum_i b_i \right)^2 = 4L$$

or
$$\frac{\left(\sum_i a_i \right)^2}{2} + \frac{\left(\sum_i b_i \right)^2}{2} = 2L$$

Recall a result from Number Theory that in order for this to be true and that the length is an integer then the length of both sequences are even. Now let the summation of sequence A = 2X and the summation of sequence B = 2Y. Hence,

$$(2X)^2 + (2Y)^2 = 4X^2 + 4Y^2 = 4L$$

This implies that $L = X^2 + Y^2$. In other words the length is the sum of two squares. ■

Here the existence theorem is proven for the special case of $m = 2$.

NOTE 1: Unfortunately Theorem 1: "Existence Condition for Special case of the Golay Complementary Sequence" is not sufficient to ensure the existence of a Golay Complementary Sequence. In other words even if the length n is the sum of two squares and n is even, this does not necessarily mean that a Golay Complementary Sequence exists for that particular length.

EXAMPLE 6
(Andres and Stanton [1])

Through the aid of computers and the method of eliminating all possibilities it has been shown that no Golay Complementary Sequence exists for the length

of $n = 34$. Clearly, $34 = 5^2 + 3^2$ is even and the sum of two squares.

NOTE 2: Clearly, the Golay Complementary Sequence as a set is closed under the operation of multiplication. This fact will be used later on as part of the proof of Theorem 2.

EXAMPLE 7

We found Golay Complementary Sequences for the following lengths:

$$n = 2 = 1^2 + 1^2$$

$$n = 4 = 2^2 + 0^2$$

$$n = 10 = 3^2 + 1^2$$

See examples 2 through 5.

NOTE 3: Notice that 0^2 can be used as part of the sum.

Using the existence condition, for lengths from 0 to 50, this greatly reduces the possible lengths for Golay Complementary Sequences to 2, 4, 8, 10, 16, 18, 20, 26, 32, 34, 36, 40, 50. Now let us see if we can narrow this down even further.

THEOREM 2

(Seberry And Yamada [7], Andres and Stanton [1])

There exists Golay Complementary Sequence of lengths 2, 10 and 26, then there are Golay Sequences

of length $2^a 10^b 26^c$ where a, b, c are integers.

PROOF

Since the proof of this theorem is actually composed of several papers it has been omitted here. For the proof of this theorem see "Golay Sequences" by T. H. Andres and R. G. Stanton [1] and "Hadamard Matrices, Sequences and Block Designs, Contemporary Design Theory : A Collection Of Surveys, by J. Seberry and M. Yamada [7]. ■

Although there are no conceptual proofs yet we have been able to eliminate some lengths for Golay Complementary Sequences through the use of computers. Computational methods were used in such a way that all the possibilities for the sequences were exhausted through the use of a program. The results of the computations show that there are no Golay Complementary Sequences for the following lengths mentioned in Remark 1 below.

REMARK 1:
(Andres and Stanton, [1])

If there exists Golay Complementary Sequences of length n , then the length of n is not 34, 36, and 50.

Consequently, using Remark 1 and Theorem 2 the only lengths possible for Golay Complementary Sequences of lengths less than 50 are 2, 4, 8, 10, 16, 20, 26, 32, and 40. For examples of these lengths see Arasu and Xiang [2].

THEOREM 3

(Eliahou, Kervaine And Saffari [4], Lin, Selfridge And Shiue [6])

If n is the length of a pair of Golay Sequences, then every prime factor congruent to 3 mod 4 has an even exponent.

PROOF

If there exists a Golay Complementary Sequence, then the length $2n$ is the sum of two squares (Existence

Condition: Theorem 1). So $2n = t_0^2 + t_1^2$ or

$$n = \frac{\begin{pmatrix} t_0 + t_1 \\ 0 \quad 1 \end{pmatrix}^2}{2} + \frac{\begin{pmatrix} t_0 - t_1 \\ 0 \quad 1 \end{pmatrix}^2}{2} .$$

Since $t_0^2 + t_1^2$ is even, t_0 and t_1 are both even or odd.

Thus $\frac{t_0 + t_1}{2}$ and $\frac{t_0 - t_1}{2}$ are integers.

To complete the proof we need a corollary from Number Theory. Recall that a positive integer n is representable as the sum of two squares if and only if each of its prime factors of the form $4k + 3$ occurs to an even power (Elementary Number Theory by D. Burton, page 307). ■

The proof above is from Lin, Selfridge and Shiue [6]. Notice how elegant it is in its simplicity and understandability. The proof found in Eliahou, Kervaine and Saffari [4] is rather lengthy and depends upon a lemma that must be proven first.

CHAPTER 4

PERIODIC COMPLEMENTARY BINARY SEQUENCES

The next step would be to consider the general case of more than two sequences of the same length.
DEFINITION:

$$\text{Let } Y = \left\{ \begin{array}{l} Z_1 = \{ b_{11}, b_{12}, \dots, b_{1n} \}, \\ Z_2 = \{ b_{21}, b_{22}, \dots, b_{2n} \}, \dots, \\ Z_m = \{ b_{m1}, b_{m2}, \dots, b_{mn} \} \end{array} \right\}$$

be m sequences all of length n from F_2 . Then

$$P_y(i) = P_{z_1}(i) + P_{z_2}(i) + \dots + P_{z_m}(i)$$

$$= \sum_{i=1}^n \sum_{j=1}^n b_{ij} b_{i+k, j+k}$$

where $k = 0, 1, \dots, n-1$

If the periodic autocorrelation function

$$P_y(i) = \begin{cases} nm & \text{if } i = 0 \\ 0 & \text{if } i \neq 0, \end{cases}$$

then $P_y(i)$ is called a Periodic Complementary Binary Sequence or denoted PCBS (Bomer & Antweiler, [3]).

Let z_i be the first row of the circulant matrix Z_i for the set of sequences of $P(i)$ then the definition of the PCBS from the previous page is equivalent to

$$\sum_{i=0}^{m-1} Z_i Z_i^T = nmI_n$$

This equivalent equation [6] will be used to simplify the proofs discussed in the following theorems. Also to simplify the notation of these sequences we will

use the abbreviation $PCBS_m^n(a_i)$ or $PCBS_m^n$ where n is

the length of each sequence and m is the number of sequences in the particular discussion. Using this notation Perfect Binary Sequences are denoted as

$PCBS_1^n(a_i)$ and Golay Complementary Sequences are

denoted as $PCBS_2^n(a_i)$.

EXAMPLE 8

Clearly any Golay Complementary Sequence is also a Periodic Complementary Binary Sequence for $m = 2$.

Example 9

The following is an example of PCBS $\begin{matrix} 8 \\ 3 \end{matrix}$.

$$\text{Let } X = \left\{ \begin{array}{l} \{-1, 1, -1, 1, 1, 1, 1, 1\} \\ \{-1, -1, 1, -1, 1, 1, 1, 1\} \\ \{-1, -1, 1, 1, -1, 1, 1, 1\} \end{array} \right\}$$

Now let us discuss some criteria to aid us in finding such sequences.

THEOREM 4 EXISTENCE CONDITION
(Arasu and Xiang [2], Lin, Selfridge And Shiue [6])

If there is a Periodic Complementary Binary Sequence of m sequences all of length n , then nm is a sum of m squares.

PROOF

Recall that we can think of these individual sequences as circulant matrices Z_i , where $i = 0, 1, 2, \dots, m-1$.

$$\sum_{i=0}^{m-1} Z_i Z_i^T = nmI_n$$

$$\sum$$

which is equivalent to

$$\sum_{i=1}^{m-1} \cancel{\circ} z_i z_i^{(k)} = \begin{cases} nm & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases}$$

for $k = 0, 1, \dots, m-1$

$$\text{Let } r_i = \sum_{j=0}^{n-1} z_i(j) \quad \text{for } i = 0, 1, \dots, m-1$$

The circulant matrix property gives us

$$Z_i J = r_i J \quad \text{and}$$

$$Z_i^T J = r_i J$$

where J is a matrix of order n whose elements are composed entirely of +1's. This gives us

$$\left(\sum_{i=0}^{m-1} \begin{matrix} Z_i & Z_i^T \\ i & i \end{matrix} \right) J = \begin{matrix} (nmI) \\ n \end{matrix} J$$

In other words,

$$\sum_{i=0}^{m-1} \begin{matrix} 2 \\ (r_i J) \\ i \end{matrix} = nmJ$$

which leads to

$$\left[\sum_{i=0}^{m-1} \begin{matrix} (r_i)^2 \\ i \end{matrix} \right] J = (nm)J$$

But recall that J is composed entirely of +1's thus

$$\sum_{i=0}^{m-1} r_i^2 = nm$$

In other words nm is the sum of m squares. ■

The proof for the special case of $m = 2$ (Golay Complementary Sequences Section 4) is from Andres and Stanton [1]. Arasu and Xiang [2] also provide proofs for the special cases of $m = 2$ and $m = 3$. As shown in the Andres and Stanton proof, these proofs are long and complicated. A much simpler generalized proof is found in Lin, Selfridge and Shiue [6] shown above.

EXAMPLE 10

From example 9 of a Periodic Complementary Binary Sequence, we have $n = 8$ and $m = 3$. So

$$mn = 24 = 4^2 + 2^2 + 2^2$$

thus 24 is a sum of 3 squares.

EXAMPLE 11

Also from the earlier example 5 of a Golay Complementary Sequence of length 10.

$$nm = (10)(2) = 4^2 + 2^2$$

So 20 is the sum of 2 squares.

COROLLARY 1 (Shiue, [8])

If there is a Periodic Complementary Binary Sequence of m sequences of length n where n is an odd integer, then nm is a sum of m nonzero integer squares.

PROOF

$$\text{Let } r_i = \sum_{j=0}^n z_i(j) \text{ where } i = 0, 1, \dots, m-1$$

By the definition of r_i , it is an odd integer when n

is an odd integer. ■

THEOREM 5 (Lin, Selfridge And Shiue [6])

There is no PCBS $_3^n$ (a $_i$) with $n = 4^h (8r + 5)$, $h \geq 0$, $r \geq 0$.

PROOF

It is well known that for any $h \geq 0$ and $t \geq 0$,

$4^h (8t + 7)$ is not the sum of three integer squares.

Thus if $n = 4^h (8r + 5)$, and

$$3n = 4^h (24r + 15) = 4^h [8(3r + 1) + 7] \text{ and}$$

$3n$ is not the sum of three integral squares. By

Theorem 4 there is no such PCBS $_3^n$ (a $_i$). ■

THEOREM 6 (Shiue, [8])

If there exists PCBS $_m^n$ $_1$, PCBS $_m^n$ $_2$, ..., and PCBS $_m^n$ $_t$,

then there exists PCBS $_m^n$ where $m = m_1 + m_2 + \dots + m_t$.

PROOF

If there exists

$PCBS_{m, i_1}^n(z_1)$, $PCBS_{m, i_2}^n(z_2)$, ..., and $PCBS_{m, i_t}^n(z_t)$, then

we have

$$\sum_{i=0}^{m-1} Z_{i, i_1}^1 Z_{i, i_1}^{1T} = nm I_{1, n}, \quad \sum_{i=0}^{m-1} Z_{i, i_2}^2 Z_{i, i_2}^{2T} = nm I_{2, n},$$

$$\dots, \text{ and } \sum_{i=0}^{m-1} Z_{i, i_t}^t Z_{i, i_t}^{tT} = nm I_{t, n}.$$

Thus we have

$$\sum_{i=0}^{m-1} Z_{i, i_1}^1 Z_{i, i_1}^{1T} + \dots + \sum_{i=0}^{m-1} Z_{i, i_t}^t Z_{i, i_t}^{tT} = nm I_n \quad \blacksquare$$

EXAMPLE 12

(Bomer and Antweiler [3])

We already know that $PCBS_{4, 48}^{48}$ and $PCBS_{6, 48}^{48}$ exist. By

Theorem 6 we now conjecture that $PCBS_{10, 48}^{48}$ also exists.

The actual sequences have not been found yet.

COROLLARY 2 (Shiue, [8])

If there exists a $PCBS_{m}^n$, then $PCBS_{mq}^n$ also exists

for any integer of q greater than or equal to two.

PROOF

Given a $PCBS_{m}^n$ recall that $m = m_1 + m_2 + \dots + m_t$

(Theorem 6). Now let $v = m_1 = m_2 = \dots = m_t$.

The factor v appears q times and by theorem 6

$PCBS_{mq}^n$ also exists which gives us Corollary 2. ■

SOME RESULTS FROM COROLLARY 2.

RESULT 1

There exists $PCBS_{2m}^2$ for any integer $m \geq 2$.

PROOF

We already know that $PCBS_{2,2}^2$ exists (see example 4).

Applying Corollary 2 gives us Result 1. ■

RESULT 2

There exists $PCBS_{q,1}^4$ for any integer $q \geq 2$.

PROOF

Similarly we know that the perfect binary sequence

exists for $PCBS_{1,1}^4$ (see example 2 and 3). By applying

Corollary 2 we get Result 2. ■

CHAPTER 5

CONCLUSION

The area of PCBS is relatively young compared to other fields of study. As a final note a short discussion of how PCBS can be utilized in practice follows. Basically it acts like a filter letting pass only the signal waves or frequencies that the scientists want thus reducing the amount of noise or interference and hence giving a "clearer picture" in terms of sonar and radar. As far as faxes and bank transfers it keeps the original transmission as intact as possible.

BIBLIOGRAPHY

- [1] T. H. Andres and R. G. Stanton, "Golay Sequences", Lecture Notes In Mathematics, Springer - Verlag, 622, (1977), p. 44 - 54.
- [2] K. T. Arasu and Qing Xiang, "On The Existence Of Periodic Complementary Binary Sequences, Design, Codes and Cryptograph", 2 (1992), p. 257 - 262.
- [3] L. Bomer and M. Antweiler, "Periodic Complementary Binary Sequences", IEEE Transform Information Theory, Vol. 35, (1990), p. 1487 - 1494.
- [4] S. Eliahou, M. Kervaine, and B. Saffari, "A New Restriction On The Lengths Of Golay Complementary Sequences", Journal Comb. Theory, A55, (1990), P. 49 - 59.
- [5] M. J. E. Golay, "Multislit Spectrometry", Journal Of The Optical Society Of America, Vol. 39, (1949), p. 437 - 444.
- [6] Cantain Lin, J. L. Selfridge, and Peter Jau-Shyong, "A Note On Periodic Complementary Binary Sequences" , To Appear in The Journal of Comb. Math and Comb. Computing.
- [7] J. Seberry and M. Yamada, "Hadamard Matrices, Sequences and Block Designs", Contemporary Design Theory : A Collection Of Surveys, John Wiley, (1992) , p. 466 - 487.
- [8] Peter Jau-Shyong Shiue, "On Periodic Complementary Binary Sequences", (1995), Preprint.
- [9] J. Storer and R. Turyn, "On Binary Sequences", Proc. Amer. Math. Soc., 12, (1961), p.394 - 399.