BINARY SEQUENCES WITH SPECIFIED CORRELATION PROPERTIES

by

Gerald Seguin

Technical Report No.7103

August 15, 1971

Department of

ELECTRICAL ENGINEERING

UNIVERSITY OF NOTRE DAME, NOTRE DAME, INDIANA

BINARY SEQUENCES WITH SPECIFIED CORRELATION PROPERTIES

by

Gerald Seguin

Technical Report No. 7103

August 15, 1971

Department of Electrical Engineering
University of Notre Dame
Notre Dame, Indiana 46556

This report was submitted to the Graduate School of the University of Notre Dame in partial fulfillment of the requirements for the degree of Doctor of Philosophy

ABSTRACT

For any binary n-tuple the functions E_k and θ_k are defined by $E_k=F_k+F_{n-k}$ and $\theta_k=F_k-F_{n-k}$ where F_k is the usual k-th non-periodic correlation coeficient of a sequence. In Chapter 1 it is shown that these two functions play a dominant role in band-width spreading signal schemes and certain general properties about them are developed. In Chapter 2 a cyclotomic sequence is defined as a sequence $s(x)=s_0+s_1x+\ldots+s_{n-1}x^{n-1}$ which satisfies $s(x)+s(x)^2=x+x^3+x^5+\ldots+x^{n-2}$ modulo $1+x^n$. It is shown that for a given n, such a sequence exists if and only if every cyclotomic coset of integers modulo n contains an even number of odd integers and that in this case there are exactly $2^{\lambda(n)}$ such sequences where $\lambda(n)$ is the number of cyclotomic cosets; and furthermore it is shown that there exists an infinite number of such integers. It is also shown that for cyclotomic sequences $\theta_k\equiv(-1)^kE_{2k}$ where 2k is reduced modulo n.

In Chapter 3 a self-dual sequence is defined as a sequence which satisfies $\theta_k=(-1)^kE_k$. Two methods are given to construct such sequences.

In Chapter 4 a Weakly-Barker sequence is defined as a sequence which satisfies $|F_{n-k}|\leq 1$, for $0< k< (n+1)/2$. It is shown that for these sequences $||E_k|-|\theta_k||\leq 2$, a property not usually satisfied by most commonly encountered sequences. A method is given for the construction of these sequences.

Lastly in Chapter 5 certain results are given about sequences obtained from Arithmetic codes.

CONTENTS

ACKNOWLEDGMENTS

The author would like to thank Prof. James L. Massey for his guidance and encouragement during this research and for the inspiration provided through his teaching, directing and researching.

The author is also grateful for the financial support provided by the National Aeronautics and Space Administration under NASA Grant NGL 15-004-026 in liason with the Goddard Space Flight Center.

Finally the author would like to thank Dr. J.J. Nahas, Dr. R.J. Leake, Dr. J. Uhran and Dr. L. Winslow for being the readers of the dissertation.

CHAPTER 1

BASIC DEFINITIONS AND GENERAL RESULTS

A. THE FUNCTIONS F_k, E_k AND θ_k

Let $\underline{r}=r_0,r_1,\ldots,r_{n-1}$ be a sequence of $+1$'s and -1's, and consider a bandwidth-spreading binary signal scheme[1,2,3] in which the data sequence $\ldots,b_{-1},b_0,b_1,\ldots$ is transmitted as the expanded stream $\ldots,b_{-1}\underline{r},b_0\underline{r},b_1\underline{r},\ldots$ (where $b_i\underline{r}$ denotes the sequence $b_ir_0,b_ir_1,\ldots,b_ir_{n-1}$). We refer to each segment $b_i\underline{r}$ as a baud of the transmitted stream since only one information bit is transmitted in this interval.

Let $\langle\underline{r};\underline{s}\rangle=\sum_0^{n-1} r_is_i$ denote the correlation between any two n-digit sequences of real numbers. A correlation receiver recovers the data digits in the above signal scheme by correlating the received bauds with $\underline{r}$, since

$$\langle b_i\underline{r};\underline{r}\rangle=\sum_{j=0}^{n-1} b_ir_jr_j=nb_i. \tag{1.1}$$

Bandwidth-spreading is used in order to make the correlator sensitive to small(with respect to one baud) shifts of the received signal and thus enable the receiver to acquire and maintain good baud synchronization and/or to reject extraneous delayed versions of the received signal as might be encountered in a multipath environment.

Consider the non-periodic correlation function F_k for the sequence $\underline{r}$ which is defined[4] as

$$F_k=\sum_{j=0}^{n-k-1} r_jr_{j+k} \qquad 0\leqslant k< n$$

$$F_k=0 \qquad k>n \tag{1.2}$$

When the possibility of confusion arises we will write $F_k(\underline{r})$ instead of simply F_k. This correlation function is commonly employed in single pulse synchronization studies[4,5]. When the correlator for the above signal scheme is k bits out of phase with the baud edges, the correlator output is given by

$$\begin{aligned} &< b_{i-1}r_{n-k},\ldots,b_{i-1}r_{n-1},b_i r_0,\ldots,b_i r_{n-k-1};\underline{r} > \\ &\quad = b_{i-1}F_{n-k}+b_i F_k \end{aligned} \tag{1.3}$$

Hence following Massey and Uhran[2] we define

$$\begin{aligned} E_k &= F_k + F_{n-k} \\ \theta_k &= F_k - F_{n-k} \end{aligned} \tag{1.4}$$

which are called the even and the odd correlation functions for $\underline{r}$ respectively to emphasize the facts that $E_{n-k}=E_k$ and $\theta_{n-k}=-\theta_k$. We note that the correlator output will be either $\pm E_k$ or $\pm\theta_k$ depending on the values of b_{i-1} and b_i. For acquiring and maintaining baud synchronization and/or for rejection of extraneous multipath delayed versions of the received signal, it is desirable to minimize the magnitude of the correlator output when the correlator is not in phase with the baud edges. That is, it is desirable to minimize $P=\max(P_E,P_\theta)$ where

$$\begin{aligned} P_E &= \max_{0<k<n} |E_k| = \max_{0<k<n} |F_k+F_{n-k}| \\ P_\theta &= \max_{0<k<n} |\theta_k| = \max_{0<k<n} |F_k-F_{n-k}| \end{aligned} \tag{1.5}$$

are the off-peak maximum magnitudes of the even and the odd correlation coefficients respectively.

We also define the off-peak maximum magnitude P_F of the non-periodic correlation coefficient as

$$P_F = \max_{0 < k < n} |F_k|. \tag{1.6}$$

In the study of sequences it is usually more fruitful to work with sequences over GF(2) instead of sequences of +1's and -1's. If $\underline{r}=(r_0,r_1,\ldots,r_{n-1})$ is a sequence over GF(2), then we shall take by way of convention

$$F_k(\underline{r}) = \sum_{j=0}^{n-k-1} r_j^* r_{j+k}^* \tag{1.7}$$

where $$r_j^* = (-1)^{r_j} \tag{1.8}$$

where r_j is treated as a real number in (1.8).

Lemma 1.1: If $\underline{r}=(r_0,r_1,\ldots,r_{n-1})$ is a sequence over GF(2), then

$$F_k(\underline{r}) = (n-k) - 2d_H(f_{n-k}(\underline{r}), b_{n-k}(\underline{r})) \tag{1.9}$$

where $d_H(\ ,\ )$ is the Hamming metric and $f_j(\underline{r})=(r_0,r_1,\ldots,r_{j-1})$, $b_j(\underline{r})=(r_{n-j},r_{n-j+1},\ldots,r_{n-1})$.

Proof: By (1.7) $F_k(\underline{r}) = \sum_{j=0}^{n-k-1} r_j^* r_{j+k}^*$ where r_j^* is defined by (1.8). Now $r_j^* r_{j+k}^*$ is equal to 1 if $r_j^* = r_{j+k}^*$ and equal to -1 if $r_j^* \neq r_{j+k}^*$. The number of times $r_j^* \neq r_{j+k}^*$ is simply $d_H(f_{n-k}(\underline{r}), b_{n-k}(\underline{r}))$ and the number of times $r_j^* = r_{j+k}^*$ is simply $(n-k) - d_H(f_{n-k}(\underline{r}), b_{n-k}(\underline{r}))$, hence (1.9) follows.

Q.E.D.

From now on we will call a sequence over GF(2) a binary sequence. We define two operators T and N by setting

$$T(r_0,r_1,\ldots,r_{n-1})=(r_{n-1},r_0,r_1,\ldots,r_{n-2})$$
$$N(r_0,r_1,\ldots,r_{n-1})=(\bar{r}_{n-1},r_0,r_1,\ldots,r_{n-2}) \qquad (1.10)$$

where $(r_0,r_1,\ldots,r_{n-1})$ is a binary sequence and $\bar{r}_i$ is the binary complement of r_i. T is the well known cyclic shift operator which is widely used in the study of cyclic codes[6,7]. The operator N was first considered by Massey and Uhran[2] in the study of Sub-Baud codes. For any integer $i>0$ we define T^i and N^i inductively by setting $T^i(\underline{r})=T(T^{i-1}(\underline{r}))$ and $N^i(\underline{r})=N(N^{i-1}(\underline{r}))$. N will be called the compacyclic shift operator. We now express E_k and θ_k in terms of T and N respectively.

Theorem 1.1: If $\underline{r}=(r_0,r_1,\ldots,r_{n-1})$ is a binary sequence, then

$$E_k(\underline{r})=n-2d_H(\underline{r},T^k\underline{r})$$
$$\theta_k(\underline{r})=n-2d_H(\underline{r},N^k\underline{r}). \qquad (1.11)$$

Proof: 1) By equation (1.4) and Lemma 1.1 $E_k(\underline{r})=F_k(\underline{r})+F_{n-k}(\underline{r})$ $=(n-k)-2d_H(f_{n-k}(\underline{r}),b_{n-k}(\underline{r}))+k-2d_H(f_k(\underline{r}),b_k(\underline{r}))=n-2[d_H(f_k(\underline{r}),b_k(\underline{r}))$ $+d_H(f_{n-k}(\underline{r}),b_{n-k}(\underline{r}))]$. Comparing $\underline{r}=(r_0,r_1,..,r_{k-1},r_k,..,r_{n-1})$ and $T^k\underline{r}=(r_{n-k},..,r_{n-1},r_0,r_1,..,r_{n-k-1})$ it is apparent that $d_H(\underline{r},T^k\underline{r})=d_H(f_k(\underline{r}),b_k(\underline{r}))+d_H(f_{n-k}(\underline{r}),b_{n-k}(\underline{r}))$ from which the first part of (1.11) follows.

2) By (1.4) and Lemma 1.1 we have that $\theta_k(\underline{r})=F_k(\underline{r})-F_{n-k}(\underline{r})=$ $(n-k)-2d_H(f_{n-k}(\underline{r}),b_{n-k}(\underline{r}))-k+2d_H(f_k(\underline{r}),b_k(\underline{r}))$. If $\bar{\underline{r}}=(\bar{r}_0,\bar{r}_1,\ldots .,\bar{r}_{n-1})$ denotes the binary complement of $\underline{r}$, then clearly $d_H(f_k(\underline{r}),$ $b_k(\underline{r}))=k-d_H(f_k(\underline{r}),b_k(\bar{\underline{r}}))$ which upon substituting in the above

expression for $\theta_k(\underline{r})$ yields $\theta_k(\underline{r})=(n-k)-2d_H(f_{n-k}(\underline{r}),b_{n-k}(\underline{r}))-k+2k-2d_H(f_k(\underline{r}),b_k(\bar{\underline{r}}))=n-2[d_H(f_k(\underline{r}),b_k(\bar{\underline{r}}))+d_H(f_{n-k}(\underline{r}),b_{n-k}(\underline{r}))]$. Comparing $\underline{r}=(r_0,r_1,..,r_{k-1},r_k,..,r_{n-1})$ and $N^k\underline{r}=(\bar{r}_{n-k},\bar{r}_{n-k+1},..,\bar{r}_{n-1},r_0,r_1,..,r_{n-1})$ we note that $d_H(\underline{r},N^k\underline{r})=d_H(f_k(\underline{r}),b_k(\bar{\underline{r}}))+d_H(f_{n-k}(\underline{r}),b_{n-k}(\underline{r}))$, and so the second part of (1.11) follows.

Q.E.D.

We remark that T is a linear operator, i.e. if $\underline{r}$, $\underline{s}$ are any two binary sequences of length n and $\underline{r}+\underline{s}=(r_0\oplus s_0,r_1\oplus s_1,...,r_{n-1}\oplus s_{n-1})$ where $\oplus$ denotes modulo 2 sum, then $T(\underline{r}+\underline{s})=T\underline{r}+T\underline{s}$. Note that we need not worry about scalar multiplication since we are working over the trivial field GF(2). On the other hand $N(\underline{r}+\underline{s})\neq N\underline{r}+N\underline{s}$, i.e. N is non-linear.

We also remark that E_k is phase independent, that is $E_k(\underline{r})=E_k(T^i\underline{r})$ for any integer $i\geqslant 0$ and any binary sequence $\underline{r}$. On the other hand θ_k is highly phase dependent. For example if $\underline{r}=(1,1,0,1,0)$, then $\theta_0=5$, $\theta_1=-1$, $\theta_2=1$, $\theta_3=-1$, and $\theta_4=1$, but for $\underline{s}=(0,1,1,0,1)=T\underline{r}$, $\theta_0=5$, $\theta_1=-1$, $\theta_2=-3$, $\theta_3=3$, and $\theta_4=1$. Hence for a given binary sequence there exists at least one phase which minimizes $P_\theta=\max_{0<k<n}|\theta_k|$. There is no known way, excluding an exhaustive search, for finding such an optimum phase.

B. COUNTING COMPACYCLIC CLASSES

In this section we will give a few results about the operator N. With respect to the cyclic shift operator T the cyclic order of a binary n-tuple (i.e. a binary sequence

of length n) $\underline{r}$ is defined as the smallest positive integer d such that $T^d\underline{r}=\underline{r}$[8,9]. It is well known[8,9] that d must divide n, and that conversely for a given d which divides n there exists a binary n-tuple whose cyclic order is d. If $\underline{r}$ is a binary n-tuple, then the cyclic class[9] of $\underline{r}$ is defined as the set consisting of $\underline{r}$ and all distinct cyclic shifts of $\underline{r}$. This induces a partition on the set of all binary n-tuples. If m|n, it is known[6] that there are exactly

$$\frac{1}{m}\sum_{d|m}2^d\mu(m/d) \tag{1.12}$$

cyclic classes of order m where $\mu(\ )$ is the Möbius function(p. 234 of [10]) and is defined for any positive integer k by

$$\mu(k)=\begin{cases} 1 & \text{if } k=1 \\ 0 & \text{if } k \text{ has a repeated prime} \\ (-1)^t & \text{if } k \text{ is the product of } t \text{ distinct primes} \end{cases} \tag{1.13}$$

Analogously we define the compacyclic order of a binary n-tuple $\underline{r}$ as the smallest positive integer d such that $N^d\underline{r}=\underline{r}$. The compacyclic class of $\underline{r}$ is defined as the set consisting of $\underline{r}$ and all its distinct compacyclic shifts.

Theorem 1.2: If $\underline{r}$ is a binary n-tuple and d its compacyclic order, then d|2n but d$\not|$n. Conversely, if d|2n but d$\not|$n, then there exists a binary n-tuple $\underline{r}$ whose compacyclic order is d. In particular d is even.

Proof: Let $\underline{r}$ have compacyclic order d and suppose d|n, then

$\bar{\underline{r}}=N^n\underline{r}=N^{qd}\underline{r}=\underline{r}$ which is absurd, therefore $d\nmid n$. Let $2n=qd+m$, $0\leqslant m< d$, then $N^{qd}\underline{r}=\underline{r}$ implies that $N^{2n-m}\underline{r}=\underline{r}$ which in turn implies that $N^m\underline{r}=\underline{r}$. But since $m< d$, we must have that $m=0$ and so $d\mid 2n$.

Conversely, suppose $d\mid 2n$ but $d\nmid n$, then letting $\underline{w}=(1,0,0,\ldots,0)$ where the number of trailing zeros is $(d/2)-1$, we see that $\underline{r}=\underline{w}\bar{\underline{w}}\underline{w}\bar{\underline{w}}\underline{w}\ldots\bar{\underline{w}}\underline{w}$ (i.e. the concatenation of these) of length n has compacyclic order d.

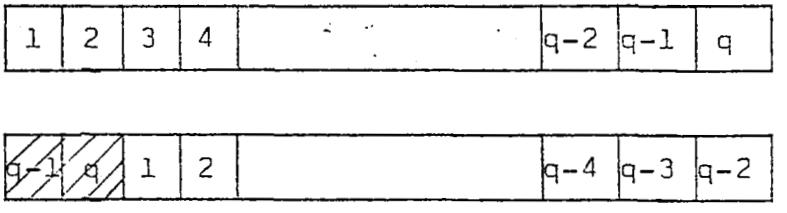
Q.E.D.

Theorem 1.3: If n is odd and $m\mid n$, then the number of binary n-tuples of compacyclic order 2m is

$$\sum_{d\mid m} 2^d\mu(m/d). \tag{1.14}$$

In particular, the number of binary n-tuples of compacyclic order 2m is equal to the number of binary n-tuples of cyclic order m.

Proof: Let $m\mid n$ and suppose $N^{2m}\underline{r}=\underline{r}$, then since $m\mid n$ we can partition the sequence $\underline{r}$ into q blocks of length m where both m and q are odd. Pictorially we have



where the top array represents $\underline{r}$ and the bottom array represents $N^{2m}\underline{r}$ the first two blocks in the bottom array being cross-

hatched to indicate that the coefficients contained in these are the complement of the coefficients contained in the corresponding blocks in the upper array. Now since both these arrays represent one and the same n-tuple, it follows that the coefficients in block 1 are equal to those of block 3 etc. .. up to block q. Similarly the coefficients in block 2 are equal to those of block 4 etc... up to block q-1. But the coefficients of block q-1 are equal to the complement of those in block 1, hence it follows that the first m bits of $\underline{r}$ completely determine $\underline{r}$, since the bits in block i are simply the complement of those in block i-1(the same order being maintained).

We have therefore shown that if $m|n$, then there are exactly 2^m binary n-tuples $\underline{r}$ which satisfy $N^{2m}\underline{r}=\underline{r}$. To obtain the number of binary n-tuples which have compacyclic order 2m we must subtract from 2^m the number of sequences with compacyclic order 2k for every k which divides m but is not equal to it, since these are all accounted for in 2^m. Hence if $\alpha(n,2m)$ denotes the number of binary n-tuples of compacyclic order 2m, then

$$\alpha(n,2m)=2^m-\sum_{\substack{d|m\\ d\neq m}}\alpha(n,2d), \tag{1.15}$$

which can be rewritten as

$$2^m=\sum_{d|m}\alpha(n,2d). \tag{1.16}$$

Applying the Möbius inversion formula(p. 236 of [10]) to

(1.16) we obtain

$$\alpha(n,2m)=\sum_{d|m} 2^d \mu(m/d). \tag{1.17}$$

We remark that this last step cannot be carried out when n is even since (1.16) does not hold for all divisors m of n, because when n is even 2m may divide both 2n and n.

From equations 1.12 and 1.17 it is clear that the number of binary n-tuples of compacyclic order 2m is equal to the number of binary n-tuples of cyclic order m whenever m divides n.

Q.E.D.

We remark that there exists a one to one correspondence between the binary n-tuples of compacyclic order 2m, m|n, and the binary 2n-tuples of cyclic order 2m which are of the form $\underline{r}\bar{\underline{r}}$ (i.e. $\underline{r}$ concatenated with its binary complement $\bar{\underline{r}}$). The one to one correspondence is realized by the mapping $\underline{r} \longrightarrow \underline{r}\bar{\underline{r}}$. Noting that $N_{\underline{r}}\overline{N_{\underline{r}}}=T(\underline{r}\bar{\underline{r}})$, it follows that $\underline{r}$ has compacyclic order 2m if and only if $\underline{r}\bar{\underline{r}}$ has cyclic order 2m. We also have from this correspondence

Theorem 1.4: If $\underline{r}$ is a binary n-tuple, then

$$\theta_k(\underline{r})=\frac{1}{2}E_k(\underline{r}\bar{\underline{r}}),\quad 0 \leqslant k \leqslant n. \tag{1.18}$$

C. DUALIZING SEQUENCES

We define a special binary n-tuple $\underline{z}$ by setting

$$\underline{z}=\begin{cases} 0101\,01\ldots 010 & n \text{ odd} \\ 0101\,01\ldots 101 & n \text{ even.} \end{cases} \tag{1.19}$$

If $\bar{\underline{z}}$ is the binary complement of $\underline{z}$ we have

Lemma 1.2: If $\underline{r}$ is any binary n-tuple, then

$$F_k(\underline{r}+\underline{z})=F_k(\underline{r}+\bar{\underline{z}})=(-1)^k F_k(\underline{r}). \tag{1.20}$$

Proof: 1) n odd. Clearly $f_{n-k}(\underline{z})+b_{n-k}(\underline{z})=(0,0,\ldots,0)$ if n-k is odd and $(1,1,\ldots,1)$ if n-k is even, where both these sequences are n-k digits long. Now $F_k(\underline{r}+\underline{z})=(n-k)-2d_H[f_{n-k}(\underline{r}+\underline{z}), b_{n-k}(\underline{r}+\underline{z})]=(n-k)-2W[f_{n-k}(\underline{r}+\underline{z})+b_{n-k}(\underline{r}+\underline{z})]$ where $W[\ ]$ is the Hamming weight function. We therefore have $F_k(\underline{r}+\underline{z})=(n-k)-2W[f_{n-k}(\underline{r})+b_{n-k}(\underline{r})+f_{n-k}(\underline{z})+b_{n-k}(\underline{z})]=(n-k)-2W[f_{n-k}(\underline{r})+b_{n-k}(\underline{r})]=F_{n-k}(\underline{r})=(-1)^k F_{n-k}(\underline{r})$ if n-k is odd and equal to $(n-k)-2W[f_{n-k}(\underline{r})+b_{n-k}(\underline{r})+(1,1,\ldots,1)]=(n-k)-2[n-k-W[f_{n-k}(\underline{r})+b_{n-k}(\underline{r})]]=-[(n-k)-2W[f_{n-k}(\underline{r})+b_{n-k}(\underline{r})]]=-F_{n-k}(\underline{r})=(-1)^k F_{n-k}(\underline{r})$ if n-k is even. All these arguments hold true for $\bar{\underline{z}}$ also.

2) n even. All the arguments of part 1) hold here except that in this case $f_{n-k}(\underline{z})+b_{n-k}(\underline{z})=(1,1,\ldots,1)$ if n-k is odd and $(0,0,\ldots,0)$ if n-k is even.

Q.E.D.

Theorem 1.5: If n is odd and $\underline{r}$ any binary n-tuple, then

$$\theta_k(\underline{r}+\underline{z})=\theta_k(\underline{r}+\bar{\underline{z}})=(-1)^k E_k(\underline{r}). \tag{1.21}$$

Proof: By Lemma 1.2 we can write $\theta_k(\underline{r}+\underline{z})=F_k(\underline{r}+\underline{z})-F_{n-k}(\underline{r}+\underline{z})=(-1)^k F_k(\underline{r})-(-1)^{n-k}F_{n-k}(\underline{r})=(-1)^k F_k(\underline{r})-(-1)^{n+k}F_{n-k}(\underline{r})=(-1)^k[F_k(\underline{r})-(-1)^n F_{n-k}(\underline{r})]=(-1)^k[F_k(\underline{r})+F_{n-k}(\underline{r})]=(-1)^k E_k(\underline{r})$. The same is true for $\bar{\underline{z}}$. Notice that the second to last step does not hold when n is even.

Q.E.D.

We remark that the transformation $\underline{r} \longrightarrow \underline{r}+\underline{z}$ has been considered by Golomb and Scholtz[11] as one of the Barker preserving transformations.

Example: If $\underline{r}=(1,1,0,1,1)$ then $\underline{r}+\underline{z}=(1,0,0,0,1)$. The even correlation coefficients of $\underline{r}$ are 5,1,1,1,1 and the odd correlation coefficients of $\underline{r}+\underline{z}$ are 5,-1,1-1,1.

Since $\theta_k(\underline{r}+\underline{z})=(-1)^k E_k(\underline{r})$ and $E_k(\underline{r}+\underline{z})=(-1)^k \theta_k(\underline{r})$, then, with respect to the even and odd correlation coefficients, $\underline{r}$ and $\underline{r}+\underline{z}$ are in a sense duals of each other. For this reason we make the following definition

Definition 1.1: If $\underline{r}$ is a binary sequence of odd length n, then $\underline{r}$ will be called self-dual if

$$\theta_k(\underline{r})=(-1)^k E_k(\underline{r}). \qquad (1.21)$$

This type of sequence will be studied in Chapter 3.

It is sometimes more convenient to work with polynomials instead of sequences. We therefore associate with the binary n-tuple $\underline{r}=(r_0,r_1,\ldots,r_{n-1})$ the polynomial $r(x)=r_0+r_1x+\ldots.+r_{n-1}x^{n-1}$ and conversely. This association sets up a one to one correspondence between the set of all binary n-tuples and the set of all binary polynomials of degree n-1 or less. If r(x) and s(x) are any two binary polynomials of degree n-1 or less, then by r(x)+s(x) we mean the polynomial $(r_0 \oplus s_0)+(r_1 \oplus s_1)x+\ldots.+(r_{n-1} \oplus s_{n-1})x^{n-1}$ where $\oplus$ denotes modulo 2 sum. Hence the binary n-tuple corresponding to r(x)+s(x) is simply $\underline{r}+\underline{s}=(r_0 \oplus s_0, r_1 \oplus s_1,\ldots,r_{n-1} \oplus s_{n-1})$. By $F_k[r(x)]$, $E_k[r(x)]$ and $\theta_k[r(x)]$ we will mean $F_k(\underline{r})$, $E_k(\underline{r})$ and $\theta_k(\underline{r})$ respectively. All polynomials

considered in this thesis will be over GF(2). If $z(x)$ is the polynomial corresponding to $\underline{z}$ and $\bar{z}(x)$ the one corresponding to $\bar{\underline{z}}$ we have

Theorem 1.6: If n is odd, then

$$\text{g.c.d.}(1+x^n, z(x)) = \begin{cases} 1+x & \text{if } 4 \mid n-1 \\ 1 & \text{if } 4 \nmid n-1 \end{cases} \tag{1.23}$$

$$\text{g.c.d.}(1+x^n, \bar{z}(x)) = \begin{cases} 1+x & \text{if } 4 \mid n+1 \\ 1 & \text{if } 4 \nmid n+1 \end{cases} \tag{1.24}$$

Proof: Before entering into the proof per se we make the following remarks: 1) If $f(x)=f_0+f_1x+\ldots+f_kx^k$ is any polynomial over GF(2) and $i \geq 0$ then $f(x)^{2^i}=f_0+f_1x^{2^i}+\ldots+f_kx^{k2^i}$ since by the binomial theorem all other coefficients are even hence 0 modulo 2. 2) If s and t are any two positive integers such that g.c.d.$(s,t)=1$, then g.c.d.$(1+x^s,1+x^t)=1+x$. To see this let F be an extension field of GF(2) which contains all the roots of $1+x^s$ and $1+x^t$. Let $\alpha \in F$ be a root of $1+x^s$ and $1+x^t$, then the multiplicative order of α must divide s and t, but since g.c.d.$(s,t)=1$ it follows that $\alpha=1$, hence g.c.d.$(1+x^s,1+x^t)=1+x$. 3) Let t be an integer, $t>0$, then an irreducible factor $g(x)$ of $1+x^t$ over GF(2) is said to have multiplicity s if $g(x)^s \mid 1+x^t$ but $g(x)^{s+1} \nmid 1+x^t$. Now it is well known[12] that over GF(2) all irreducible factors of $1+x^t$, $t>0$, have the same multiplicity and that this multiplicity is 2^k where k is the largest integer such that $2^k \mid t$. With these remarks in mind we proceed to the proof.

$z(x)=x+x^3+x^5+\ldots+x^{n-2}=x(1+x^2+x^4+\ldots+x^{n-3})=x(1+x+x^2+\ldots+x^{(n-3)/2})^2=x(1+x^{n-1})/(1+x)^2$. Hence g.c.d.$(1+x^n,z(x))$=g.c.d.$(1+x^n,$

$x(1+x^{n-1})/(1+x)^2$) and by remark 2) it follows that this is 1 if $(1+x)^3 \nmid 1+x^{n-1}$ and $1+x$ if $(1+x)^3 | 1+x^{n-1}$. Now if $(1+x)^3 | 1+x^{n-1}$, then $1+x$ must have multiplicity at least 4 by remark 3, hence $(1+x)^4 = 1+x^4 | 1+x^{n-1}$ and this can be if and only if $4|n-1$. It therefore follows that $(1+x)^3$ divides $1+x^{n-1}$ if and only if $4|n-1$ from which (1.23) follows.

Equation (1.24) can be established in a perfectly analogous way.

Q.E.D.

D. REVIEW AND PREVIEW

The purpose of this section is to briefly review what has been done in the first three sections and to briefly outline the remainder of the thesis.

In section A a bandwidth-spreading binary signal scheme was described which required a binary n-tuple with small parameter $P=\max(P_E, P_\theta)$. This gives rise to a new problem in the design of sequences. There are methods available for the construction of sequences with small P_E. For example the maximal length sequences[13], the Legendre sequences[17], the twin-prime sequences[17] and the Hall sequences[19] all have $P_E=1$ and are all of odd length. In fact for these sequences $E_k=-1$, $0 < k < n$, or $E_k=1$, $0 < k < n$. By the results of section C we can use the above techniques to construct sequences for which $P_\theta=1$, simply by adding $\underline{z}$ or $\bar{\underline{z}}$ to the sequences obtained by these methods. However the problem of constructing sequences with small P has never been considered before. From the expression for E_k

and θ_k(equation 1.4) it readily follows that

$$P_F \leqslant P \leqslant 2P_F \tag{1.25}$$

Hence if we have a sequence with small P we automatically have a sequence with small P_F. Sequences with small P_F are very important in radar ranging problems[5,20]. However there are no known techniques, similar in nature to those for constructing sequences with small P_E, for constructing sequences with small P_F.

In the following three chapters three classes of sequences will be presented for which E_k and θ_k bear certain relations to each other. More specifically in Chapter 2 we present a class of sequences for which $\theta_k=(-1)^k E_{2k}$ where 2k is reduced modulo n. In particular we have $P=P_E=P_\theta$ for this class. The construction technique for this class gives rise to an interesting problem in Number Theory(see Theorem 2.1). The study of this class of sequences also gave birth to an interesting result(see Theorem 2.6) on the factorization of the polynomial $1+x^n$ over GF(2).

In Chapter 3 we give two methods for constructing sequences which satisfy $\theta_k=(-1)^k E_k$, $0< k< n$. One of these classes (see section B of Chapter 3) seems to be a good source of sequences with small P. In particular it is shown that the Barker sequences[5] of lengths 5 and 13 belong to this latter class.

In Chapter 4 a class of sequences is described which satisfy $\| |E_k| - |\theta_k| \| \leqslant 2$, $0< k< n$.

CHAPTER II

CYCLOTOMIC SEQUENCES

In this chapter we describe a class of sequences which satisfy $\theta_k=(-1)^k E_{2k}$, $0\leq k< n$, and where 2k is reduced modulo n. In particular we have $P_E=P_\theta$ for this class.

Let $r(x)=r_0+r_1x+\ldots+r_{n-1}x^{n-1}$ be a binary polynomial. Then when n is odd, it is well known(p. 54 of [13]) that the even correlation coefficients of $r(x)^2$(reduced modulo $1+x^n$) are a permutation of the even correlation coefficients of r(x). In fact, $E_k[r(x)^2]=E_{2k}[r(x)]$ where 2k is reduced modulo n.

Let n be odd and suppose r(x) has the property that $r(x)+r(x)^2\equiv z(x) \bmod 1+x^n$. Then by the above remarks and Theorem 1.5 it follows that $\theta_k[r(x)]=(-1)^k E_k[r(x)+z(x)]=(-1)^k E_k[r(x)^2]=(-1)^k E_{2k}[r(x)]$ where $r(x)^2$ is reduced modulo $1+x^n$ and 2k is reduced modulo n. The following Theorem tells us when such an r(x) exists.

Theorem 2.1: Let n be odd, then there exists an r(x) such that $r(x)+r(x)^2\equiv z(x) \bmod 1+x^n$ if and only if every cyclotomic coset of integers modulo n contains an even number of odd integers, and in this case there are exactly $2^{\lambda(n)}$ such r(x)'s where $\lambda(n)$ is the number of cyclotomic cosets modulo n.

Proof: In the following arguments all polynomials are reduced modulo $1+x^n$.

Necessity. The cyclotomic coset modulo n of an integer k, $0\leq k< n$, is the set $<k>=\{2^i k \bmod n \mid i=0,1,\ldots.\}$ [13]. The formation of these cosets induces a partition on the set of inte-

gers $\{0,1,2,\ldots,n-1\}$. Note also that since for any integer k, $0<k<n$, $2^i k \bmod(n)=k[2^i \bmod(n)]\bmod(n)$ for any integer $i \geq 0$, then the cyclotomic coset of k is $<k>=k<1>=\{km_i \bmod(n) \mid i=1,2,\ldots,s\}$ where $<1>=\{m_1,m_2,\ldots,m_s\}$ is the cyclotomic coset of 1.

Suppose there exists an r(x) such that $r(x)+r(x)^2=z(x)$. Let k_1 be any odd integer, $0<k_1<n$, then the elements of $<k_1>$ can be arranged as

$$k_1,2k_1,..,2^{i_1-1}k_1,k_2,2k_2,..,2^{i_2-1}k_2,k_3,$$
$$.....,2^{i_{m-1}-1}k_{m-1},k_m,2k_m,..,2^{i_m-1}k_m \qquad (2.1)$$

where $k_1,k_2,\ldots,k_m$ are the only odd integers in the coset(i_j is the smallest positive integer for which $2^{i_j}k_j \geq n$). Since x^{k_1} is a term in z(x), then x^{k_1} must be a term in r(x) or $r(x)^2$. Suppose x^{k_1} is a term in r(x), then since z(x) contains no even powers of x, but x^{2k_1} appears in $r(x)^2$, we must also have the cancelling term x^{2k_1} in r(x). By similar reasoning, r(x) must include $x^{2^2k_1},\ldots,x^{2^{i_1-1}k_1}$ but must not include x^{k_2} since this term will appear in $r(x)^2$ and must not be cancelled since it appears also in z(x). Also we must not have x^{k_m} in r(x), for if x^{k_m} is in r(x), then by the previous argument, we must also have x^{2k_m} etc... in r(x) which shows that x^{k_1} will be in $r(x)^2$ resulting in the undesired cancellation with the similar term in r(x).

The same arguments hold for k_i $i=1,2,\ldots,m$. Hence if x^{k_i} is a term in r(x), then $x^{k_{i-1}}$ and $x^{k_{i+1}}$ must not be terms in

$r(x)$. Lastly, since x^{k_i} is in $r(x)^2$ if and only if $x^{k_{i-1}}$ is in $r(x)$, then it follows that we must include in $r(x)$ the terms x^{k_1}, $x^{2k_1},\ldots,x^{k_3},x^{2k_3},\ldots$ etc or $x^{k_2},x^{2k_2},\ldots,x^{k_4},x^{2k_4},\ldots$etc, and this can be done successfully if and only if there are an even number of odd integers in $< k_1 >$. This must be true for every cyclotomic coset since every cyclotomic coset(except $< 0 >$) contains an odd integer and all odd powers of x are terms in $z(x)$. Sufficiency. Conversely, suppose that every cyclotomic coset of integers modulo n contains an even number of odd integers, then construct $r(x)$ by including in $r(x)$ $x^{k_1},x^{2k_1},\ldots,x^{k_3},x^{2k_3},$ $\ldots\ldots,x^{k_{m-1}},x^{2k_{m-1}},\ldots$ or $x^{k_2},x^{2k_2},\ldots,x^{k_4},x^{2k_4},\ldots\ldots\ldots,x^{k_m},$ $x^{2k_m},\ldots$ for each coset $< k_1 > \neq 0$. Since x^0 corresponds to $< 0 >$, it may be included or excluded. By the arguments used in the proof of the necessity, this will yield an $r(x)$ which satisfies $r(x)+r(x)^2=z(x)$.

From the above proof we see that in the construction of an $r(x)$ which satisfies $r(x)+r(x)^2=z(x)$ we have exactly two choices for each coset, hence there are exactly $2^{\lambda(n)}$ solutions where $\lambda(n)$ is the number of cyclotomic cosets modulo n.

An alternate way to ascertain that the number of solutions is $2^{\lambda(n)}$ is the following: Let $r(x)$ be such that $r(x)+r(x)^2=$ $z(x)$ and let $e(x)$ be an idempotent[9] in the Algebra of polynomials modulo $1+x^n$ over GF(2), i.e. $e(x)^2=e(x)$. Then $[r(x)+e(x)]+[r(x)+e(x)]^2=r(x)+r(x)^2+e(x)+e(x)^2=z(x)$ and so $s(x)=r(x)+e(x)$ satisfies $s(x)+s(x)^2=z(x)$. Conversely, suppose that $r_1(x)$ and $r_2(x)$ satisfy $r_i(x)+r_i(x)^2=z(x)$, $i=1,2$; then $[r_1(x)+r_2(x)]^2+$

$[r_1(x)+r_2(x)]=r_1(x)+r_1(x)^2+r_2(x)+r_2(x)^2=z(x)+z(x)=0$ which implies that $r_1(x)+r_2(x)$ is an idempotent. We have therefore shown that the set of solutions $\{r(x)|\, r(x)+r(x)^2=z(x)\}$, when it is not empty, forms a coset of the space $\{e(x)|\, e(x)^2=e(x)\}$ of idempotents and this space is known to have dimension $\lambda(n)$ over GF(2) [9].

Q.E.D.

Because of Theorem 2.1 we are led to

Definition 2.1: A binary sequence $\underline{r}$ of odd length n for which $r(x)+r(x)^2=z(x)$ will be called a cyclotomic sequence.

Example: If n=5, then the cyclotomic cosets are {0} and {1,2,4,3}. Hence following the notation used in the proof of Theorem 2.1 we have $k_1=1$ and $k_2=3$. Using the construction technique described there the cyclotomic sequences of length 5 are(in polynomial form) $x+x^2+x^4$, $1+x+x^2+x^4$, x^3 and $1+x^3$.

Suppose n is a prime such that $n\equiv 1 \bmod(4)$ and for which 2 is primitive(i.e. 2 is a primitive element of GF(n)). In this case the cyclotomic cosets are {0} and {1,2,3,...,n-1} and both these cosets contain an even number of odd integers. We therefore have

Theorem 2.2: Cyclotomic sequences of length n exist for all primes n for which 2 is primitive and such that $n\equiv 1 \bmod(4)$.

We single out this subclass by making

Definition 2.2: A cyclotomic sequence of prime length n for which 2 is primitive will be called a primitive cyclotomic sequence.

The following Table lists all primes up to 4649 for which there exists primitive cyclotomic sequences.

TABLE 1

PRIMES LESS THAN 4650 FOR WHICH PRIMITIVE CYCLOTOMIC SEQUENCES EXIST

5, 13, 29, 37, 53, 61,101,149,173,181,197,269,
293,317,349,373,389,421,461,509,541,557,613,653,
661,677,701,709,757,773,797,821,829,853,877,941,
1061,1109,1117,1213,1229,1237,1277,1301,1373,1381,
1453,1493,1549,1621,1637,1669,1693,1733,1741,1861,
1877,1901,1949,1973,1997,2029,2053,2069,2141,2213,
2221,2237,2269,2293,2309,2333,2357,2389,2437,2477,
2549,2557,2621,2677,2693,2789,2797,2837,2861,2909,
2957,3037,3253,3413,3461,3469,3517,3533,3557,3581,
3613,3637,3677,3701,3709,3733,3797,3853,3877,3917,
3989,4013,4021,4093,4133,4157,4229,4253,4261,4349,
4357,4373,4397,4493,4517,4621,4637

Source: A. Cunningham, H.J. Woodall and T.G. Creak, "Proc. of the London Math. Soc.," Vol.21, 1922,pp. 343-358.

By Theorem 2.1, if n is as specified by Theorem 2.2, then there are exactly four primitive cyclotomic sequences of length n. In fact, if $\underline{r}=(r_0,r_1,\ldots,r_{n-1})$ is a primitive cyclotomic sequence then the other three are $\underline{r}_2=(\bar{r}_0,\bar{r}_1,\ldots,\bar{r}_{n-1})$, $\underline{r}_3=(\bar{r}_0,r_1, r_2,\ldots,r_{n-1})$ and $\underline{r}_4=(r_0,\bar{r}_1,\bar{r}_2,\ldots,\bar{r}_{n-1})$ where $\bar{r}_i$ is the binary complement of r_i. It is clear from equation (1.11) that if $\underline{r}$ and $\underline{s}$ are two binary n-tuples differing only in one coordinate, then $|P_E(\underline{r})-P_E(\underline{s})| \leq 4$ and similarly for P_θ and P_F. Hence since

a sequence and its binary complement have exactly the same correlation coeficients(even, odd and finite) then for any two primitive cyclotomic sequences $\underline{r}$ and $\underline{s}$ we have $|P_E(\underline{r})-P_E(\underline{s})| \leq 4$ and similarly for P_θ and P_F. We collect these results as

Theorem 2.3: If $\underline{r}$ and $\underline{s}$ are any two primitive cyclotomic sequences of the same length, then

$$\begin{aligned} |P_E(\underline{r})-P_E(\underline{s})| &\leq 4 \\ |P_\theta(\underline{r})-P_\theta(\underline{s})| &\leq 4 \\ |P_F(\underline{r})-P_F(\underline{s})| &\leq 4 \end{aligned} \qquad (2.2)$$

By (2.2) it follows that for large n all cyclotomic sequences of length n will display a parameter $P=\max(P_E,P_\theta)$ which is approximately the same.

For all n's less than 2358 which satisfy the conditions of Theorem 2.2 the primitive cyclotomic sequence of length n with $r_0=r_1=1$ has been analyzed on the UNIVAC 1107 Computer in the University of Notre Dame Computing Center and the results are contained in Table 2. The Legendre(or quadratic residue) sequences[17] have also been analyzed for comparison's sake and the results of this investigation are given in the Appendix.

Whether or not primitive cyclotomic sequences exist for arbitrarily long lengths is unknown since it is unknown whether or not there exists an infinite number of primes for which 2 is primitive[6]. However the following Theorem shows that there exist cyclotomic sequences of arbitrarily long lengths.

Theorem 2.4: Let $p_1,p_2,\ldots,p_r$ be a set of distinct primes which satisfy

1) $p_i \equiv 1 \bmod(4)$

TABLE 2

THE PARAMETERS P_F, P_E, n/P_F, n/P_E, FOR THAT PRIMITIVE CYCLOTOMIC SEQUENCE OF LENGTH n WHICH STARTS WITH $r_0=r_1=1$, FOR ALL $n< 2358$

n	P_F	n/P_F	P_E	n/P_E	n	P_F	n/P_F	P_E	n/P_E
5	1	5.00	1	5.00	1109	84	13.20	103	10.75
13	4	3.25	5	2.60	1117	101	11.05	113	9.87
29	12	2.42	13	2.23	1213	99	12.26	105	11.55
37	8	4.62	9	4.12	1229	81	15.18	93	13.20
53	16	3.31	17	3.12	1237	82	15.10	107	11.56
61	10	6.10	11	5.55	1277	102	12.50	109	11.70
101	18	5.61	23	4.40	1301	154	8.45	161	8.09
149	26	5.74	31	4.80	1373	120	11.45	127	10.81
173	20	8.65	25	6.92	1381	106	13.01	119	11.61
181	24	7.55	31	5.85	1453	100	14.53	123	11.81
197	26	7.59	35	5.64	1493	131	11.41	133	11.24
269	38	7.08	45	5.98	1549	111	13.93	141	10.97
293	28	10,45	37	7.92	1621	119	13.63	131	12.39
317	41	7.74	53	5.98	1637	142	11.52	149	11.00
349	38	9.19	53	6.59	1669	124	13.45	125	13.33
373	65	5.74	65	5.74	1693	118	14.35	139	12.20
389	52	7.48	53	7.35	1733	126	13.76	139	12.50
421	53	7.95	57	7.40	1741	109	16.00	129	13.50
461	57	8.10	73	6.33	1861	120	15.50	139	13.40
509	55	9.25	57	8.93	1877	110	17.05	135	13.90
541	49	11.05	61	8.89	1901	125	15.21	163	11.68
557	64	8.70	79	7.05	1949	132	14.75	149	13.06
613	64	9.58	65	9.45	1973	120	16.45	143	13.80
653	87	7.51	103	6.35	1997	146	13.68	173	11.52
661	68	9.74	85	7.79	2029	156	13.01	167	12.15
677	98	6.91	103	6.57	2053	152	13.50	161	12.74
701	59	11.90	75	9.35	2069	112	18.50	145	14.29
709	66	10.72	77	9.20	2141	166	12.90	181	11.84
757	84	9.01	91	8.33	2213	132	16.74	161	13.72
773	70	11.01	93	8.32	2221	149	14.91	157	14.17
797	95	8.40	103	7.74	2237	142	15.74	161	13.88
821	87	9.45	91	9.03	2269	131	17.32	169	13.41
829	74	11.20	81	10.22	2293	136	16.85	147	15.60
853	94	9.08	97	8.80	2309	158	14.60	181	12.75
877	64	13.70	79	11.10	2333	156	14.95	173	13.49
941	80	11.79	91	10.35	2357	123	19.15	163	14.45
1061	90	11.80	131	8.11					

2) 2 is primitive modulo p_i.

If $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}>1$, then there exists a cyclotomic sequence of length n.

Proof: 1) Let p be a prime such that $8|p-1$, then by Theorem 95 in Hardy and Wright[10] 2 is a quadratic residue modulo p. That is to say, there exists an integer a such that $a^2\equiv 2 \bmod(p)$, hence $1\equiv a^{p-1}\equiv(a^2)^{(p-1)/2}\equiv 2^{(p-1)/2}\bmod(p)$ from which it follows that 2 is not primitive modulo p. By condition 2 of the Theorem it follows that $(p_i-1)/4$ must be odd for $i=1,2,\ldots,r$.

2) Since 2 is primitive modulo p_i, then there exists an integer k such that $2^k\equiv -1\bmod(p_i)$ which implies that $2^{2k}\equiv 1\bmod(p_i)$ and this in turn implies that $(p_i-1)|2k$. Since $k< p_i$, we must have that $k=(p_i-1)/2$. We therefore have that $2^{(p_i-1)/2}\equiv -1\bmod(p_i)$ for $i=1,2,\ldots,r$. If $a\equiv b\bmod(p)$, p any prime, then by a simple application of the binomial theorem we obtain $a^p\equiv b^p\bmod(p^2)$ and by induction $a^{p^t}\equiv b^{p^t}\bmod(p^{t+1})$ for any integer $t\geq 0$. Applying this to $2^{(p_i-1)/2}\equiv -1\bmod(p_i)$ we obtain $(2^{(p_i-1)/2})^{p_i^{\alpha_i-1}}\equiv -1\bmod(p_i^{\alpha_i})$ where -1 remains -1 since $p_i^{\alpha_i-1}$ is odd.

Let $\tau=\mathrm{LCM}[(\frac{p_1-1}{2})p_1^{\alpha_1-1},(\frac{p_2-1}{2})p_2^{\alpha_2-1},\ldots,(\frac{p_r-1}{2})p_r^{\alpha_r-1}]$ where LCM stands for least common multiple, then by part 1) of the proof $2|\tau$ but $4\nmid\tau$, which implies that $2\tau/(p_i-1)p_i^{\alpha_i-1}$ is odd for $i=1,2,\ldots,r$. We therefore obtain that $2^\tau\equiv -1\bmod(p_i^{\alpha_i})$ for $i=1,2,\ldots,r$ and consequently $2^\tau\equiv -1\bmod(n)$.

We have therefore shown that -1 belongs to $<1>$

which shows that k and -k belong to the same cyclotomic coset for every integer k, $0 \leq k \leq n$, since $< k > = k < 1 >$. This in turn shows that in each cyclotomic coset (except the trivial coset $< 0 >$) the number of odd integers is equal to the number of even integers because if k is odd(even) then $-k \equiv n-k \bmod(n)$ is even(odd). If we can now show that the order of each cyclotomic coset(except the trivial one) is divisible by 4 we will have completed the proof that each cyclotomic coset contains an even number of odd integers as required by Theorem 2.1.

3) If k is an integer, $0 \leq k \leq n$, then the order of $< k >$ is the smallest positive integer i such that $2^i k \equiv k \bmod(n)$, i.e. such that $n \mid k(2^i-1)$. Since $k \leq n$, then $p_t \mid 2^i-1$ for some t, $1 \leq t \leq r$. But, since 2 is primitive modulo p_i, this implies that $(p_t-1) \mid i$ which in turn implies that $4 \mid i$ since $4 \mid (p_t-1)$.

Q.E.D.

Though Theorem 2.4 produces an infinite number of integers for which cyclotomic sequences exist, yet these do not exhaust all such integers. Consider for example n=17, then the cyclotomic cosets are $< 0 > = \{0\}$, $< 1 > = \{1,2,4,8,16,15,13,9\}$ and $< 3 > = \{3, 6,12,7,14,11,5,10\}$. Since all these cosets contain an even number of odd integers it follows from Theorem 2.1 that there exist cyclotomic sequences of length 17, yet 17 is not of the form specified by Theorem 2.4. A list of all n's up to 269 for which cyclotomic sequences exist is given in Table 3.

The following Theorem gives two necessary conditions for the existence of cyclotomic sequences.

TABLE 3

INTEGERS UP TO 269 FOR WHICH THERE EXIST CYCLOTOMIC SEQUENCES

5, 13, 17*, 25, 29, 37, 41*, 53,61,65, 97*,101,109*,113*,125,137*,145,149,157*, 169,173,181,185,193*,197,205*,229*,241*, 257*,265,269

* Integer not of the form specified by Theorem 2.4.

Theorem 2.5: If n is odd and if there exists a cyclotomic sequence of length n, then $4|n-1$ and n is not divisible by an integer of the form 2^i-1 for $i>1$.

Proof: 1) The weight(i.e. the number of non-zero coeficients) of z(x) is clearly (n-1)/2. Since r(x) and $r(x)^2$ have the same weight, then the weight of $r(x)+r(x)^2$ is even. Hence if there exists an r(x) such that $r(x)+r(x)^2=z(x)$ it follows that (n-1)/2 must be even, i.e. 4 must divide n-1.

2) Suppose $2^i-1|n$ for some $i>1$, then $n=q(2^i-1)$ and the cyclotomic coset of q is $q,2q,\ldots,2^{i-1}q$ which contains only one odd integer(namely q itself). By Theorem 2.1 no cyclotomic sequence of length n exists.

Q.E.D.

The conditions of Theorem 2.5 however are not sufficient. For example the cyclotomic coset of 3 modulo 89 is {3,6,12,24, 48,7,14,28,56,23,46} which contains only 3 odd integers, yet 89 satisfies the conditions of Theorem 2.5.

The problem of finding the irreducible factors of $1+x^n$ over GF(2) is a very important problem in the study of cyclic codes[6,7] and as a method of finding irreducible polynomials over GF(2)[7,18]. Theorem 2.4 affords an interesting Corollary in this direction which we state as

Theorem 2.6: If n is of the form specified by Theorem 2.4, then all the irreducible factors of $1+x^n$ over GF(2) are self-reciprocal and all(except $1+x$) have degree a multiple of 4.

Proof: It is well known[9] that there exists a one to one correspondence between the irreducible factors of $1+x^n$ over GF(2) and the cyclotomic cosets of integers modulo n. In fact if α is a primitive n-th root of unity belonging to some extension field of GF(2) and k an integer, $0 < k < n$, $< k >=\{m_1, m_2, \ldots, m_s\}$ its cyclotomic coset, then $g(x)=\prod_{i=1}^{s} (x-\alpha^{m_i})$ is an irreducible factor of $1+x^n$ of degree s. If n is of the form specified by Theorem 2.4, then m_i and $-m_i$ belong to $< k >$ which implies that if τ is a root of g(x) then so is τ^{-1} which in turn implies that g(x) is self-reciprocal(a polynomial f(x) of degree s is said to be self-reciprocal if $f(x)=x^s f(1/x)$).

Since the order of every cyclotomic coset(except $< 0 >$) is a multiple of 4 it follows by the above correspondence that all the irreducible factors(except $1+x$) have degree a multiple of 4.

Q.E.D.

Examples: 1) The irreducible factors of $1+x^{25}$ over GF(2) are $1+x$, $1+x+x^2+x^3+x^4$ and $1+x^5+x^{10}+x^{15}+x^{20}$.

2) The irreducible factors of $1+x^{65}$ over GF(2) are $1+x$, $1+x+x^2+x^3+x^4$, $1+x+x^2+x^3+.....+x^{12}$, $1+x^4+x^5+x^6+x^7+x^8+x^{12}$, $1+x^2+x^5+x^6+x^7+x^{10}+x^{12}$, $1+x^2+x^3+x^4+x^6+x^8+x^9+x^{10}+x^{12}$ and $1+x+x^3+x^5+x^6+x^7+x^9+x^{11}+x^{12}$. We remark that $1+x^{65}$ contains all the self-reciprocal irreducible polynomials of degrees 1,4 and 12.

A binary cyclic code is said to be reversible[22] if whenever $v(x)=v_0+v_1x+...+v_{n-1}x^{n-1}$ is a code word then so is $x^nv(1/x)$, where n is the length of the code. The following Corollary is immediate.

Corollary: If n is as specified in Theorem 2.4, then all binary cyclic codes of length n are reversible.

CHAPTER III

SELF-DUAL SEQUENCES

In Chapter 1 a self-dual sequence was defined(Def'n 1.1) as a binary n-tuple $\underline{r}$ for which $\theta_k(\underline{r})=(-1)^k E_k(\underline{r})$. The following Theorem characterizes the self-dual sequences in a slightly different manner.

Theorem 3.1: If n is odd and $\underline{r}$ a binary n-tuple, then $\underline{r}$ is self-dual if and only if $F_k(\underline{r})=0$ for all odd k, $0< k< n$.

Proof: 1) Suppose $\underline{r}$ is self-dual, then for odd k, $F_k(\underline{r})-F_{n-k}(\underline{r})$ $=-F_k(\underline{r})-F_{n-k}(\underline{r})$ which implies that $F_k(\underline{r})=0$.
2) Suppose $F_k(\underline{r})=0$ for all odd k, $0< k< n$, then $\theta_k(\underline{r})=F_k(\underline{r})$ $-F_{n-k}(\underline{r})=(-1)^k E_k(\underline{r})$. If k is even, then n-k is odd and so $\theta_k(\underline{r})$ $=F_k(\underline{r})=(-1)^k E_k(\underline{r})$.

Q.E.D.

It is therefore clear that for self-dual sequences $P=P_E=P_\theta=P_F$.

In this chapter we give two methods for the construction of self-dual sequences. The strategy in both of these techniques is to consider an operator H which maps binary n-tuples into binary n-tuples and which leaves the even correlation coefficients invariant, i.e. $E_k(H\underline{r})=E_k(\underline{r})$, and then look for sequences $\underline{r}$ which satisfy $\underline{r}+\underline{z}$(or $\bar{\underline{z}}$)$=H\underline{r}$.

A. THE CYCLIC SHIFT OPERATOR

Let $\underline{r}$ be a binary n-tuple, T the cyclic shift operator defined in Chapter 1, then it is well known(Theorem 5.4 of [13])

that $E_k(T^i\underline{r})=E_k(\underline{r})$, $0\leqslant i< n$. Suppose $\underline{r}$ has the property that $\underline{r}+\underline{z}=T^i\underline{r}$ for some i, $0< i< n$, then by the above remark and Theorem 1.5 if follows that $\theta_k(\underline{r})=(-1)^k E_k(\underline{r}+\underline{z})=(-1)^k E_k(T^i\underline{r})=(-1)^k E_k(\underline{r})$, hence $\underline{r}$ is self-dual. The same of course is true if $\underline{z}$ is replaced by $\bar{\underline{z}}$. Theorem 3.2 will tell us for which values of i and n such an $\underline{r}$ exists. In the proof of Theorem 3.2 we will use polynomials modulo $1+x^n$ instead of binary n-tuples and so we make the following observation: if $r(x)=r_0+r_1x+\ldots+r_{n-1}x^{n-1}$, then $x^ir(x)\equiv(r_{n-i}+r_{n-i+1}x+\ldots+r_{n-1}x^{i-1}+r_0x^i+\ldots+r_{n-i-1}x^{n-1})\bmod 1+x^n$ and so the n-tuple corresponding to $x^ir(x)\bmod 1+x^n$ is simply $T^i\underline{r}$. Hence to find a binary n-tuple $\underline{r}$ such that $\underline{r}+\underline{z}=T^i\underline{r}$ is equivalent to finding a binary polynomial r(x) such that $r(x)+z(x)\equiv x^ir(x)\bmod 1+x^n$.

Theorem 3.2: There exists a binary n-tuple $\underline{r}$ such that $\underline{r}+T^i\underline{r}=\underline{z}(\bar{\underline{z}})$ if and only if $4|n-1(4|n+1)$ and g.c.d.$(n,i)=1$; and in that case, there are exactly two such n-tuples.

Proof: We will prove the Theorem for $\underline{z}$, the proof for $\bar{\underline{z}}$ being perfectly analogous.

Sufficiency. Suppose $4|n-1$ and g.c.d.$(n,i)=1$, then by remark 2 in the proof of Theorem 1.6 we have that g.c.d.$(1+x^n,1+x^i)=1+x$ and since n is odd(which in particular implies that $1+x^n$ has no repeated factors) it follows that g.c.d.$[1+x^n,(1+x^i)/(1+x)]=1$. If g(x) is a polynomial over GF(2) which is relatively prime to $1+x^n$, then there exists polynomials f(x) and h(x) such that $1=f(x)g(x)+h(x)[1+x^n]$ from which it follows that $f(x)g(x)\equiv 1\bmod 1+x^n$(see Theorem 3H in [14]). Hence there exists a poly-

nomial s(x) such that $s(x)[(1+x^i)/(1+x)] \equiv 1 \bmod 1+x^n$ which, upon multiplying both sides by z(x), becomes $[z(x)s(x)/(1+x)](1+x^i) \equiv z(x) \bmod 1+x^n$. Letting $r(x)=z(x)s(x)/(1+x) \bmod 1+x^n$ we have $r(x)(1+x^i) \equiv z(x) \bmod 1+x^n$ from which it follows that $\underline{r}+T^i\underline{r}=\underline{z}$ which is what we wanted to show. We now show that if there is one solution, then there are exactly two.

Suppose we have two binary n-tuples $\underline{r}_1$ and $\underline{r}_2$ such that $\underline{r}_1+T^i\underline{r}_1=\underline{z}$ and $\underline{r}_2+T^i\underline{r}_2=\underline{z}$, then $(\underline{r}_1+\underline{r}_2)=T^i(\underline{r}_1+\underline{r}_2)$ and since g.c.d.(n,i)=1, this can occur only if $\underline{r}_1=\underline{r}_2$ or $\underline{r}_1=\bar{\underline{r}}_2$.

Necessity. Suppose there exists a polynomial r(x) such that $r(x)+z(x) \equiv x^i r(x) \bmod 1+x^n$, then it follows that $(1+x^i)r(x) \equiv z(x) \bmod 1+x^n$, which in equation form is $(1+x^i)r(x)=z(x)+f(x)(1+x^n)$ for some polynomial f(x). Let g.c.d.(n,i)=d, hence $n=q_1 d$ and $i=q_2 d$ where g.c.d.$(q_1,q_2)=1$. We therefore have $(1+x^{q_1 d})r(x)=z(x)+f(x)(1+x^{q_2 d})$ which implies that $(1+x^d) \mid$ g.c.d.$(z(x),1+x^n)$ which by Theorem 1.6 implies that $4 \mid n-1$ and d=1.

Q.E.D.

If n is an odd integer, then $4 \mid n-1$ or $4 \mid n+1$ (but not both), hence by Theorem 3.2, given an odd integer n, there exists exactly $2\emptyset(n)$ binary n-tuples $\underline{r}$ which satisfy $\underline{r}+T^i\underline{r}=\underline{z}$ (or $\bar{\underline{z}}$) for some i, $0 < i < n$, and $\emptyset(n)$ is the Euler-Phi function of n (see Section 5.5 in [10]). $\emptyset(n)$ is simply the number of integers less than n and prime to it.

Example: When n=3, $2\emptyset(3)=4$ and the solutions to $\underline{r}+T^i\underline{r}=\underline{z}$ are (1,1,0),(0,0,1,),(0,1,1) and (1,0,0).

Definition 3.1: We define the reciprocal operator R by setting

$$R(r_0,r_1,\ldots,r_{n-1})=(r_{n-1},r_{n-2},\ldots,r_0).$$

Lemma 3.1: For any binary n-tuple $\underline{r}$ we have that $RT^i\underline{r}=T^{n-i}R\underline{r}$

Proof: $RT^i\underline{r}=R(r_{n-i},..,r_{n-1},r_0,r_1,..,r_{n-i-1})=(r_{n-i-1},r_{n-i-2},..,r_0,r_{n-1},..,r_{n-i})$. On the other hand $T^{n-i}R\underline{r}=T^{n-i}(r_{n-1},\ldots,r_0)=(r_{n-i-1},r_{n-i-2},..,r_0,r_{n-1},..,r_{n-i})$. Hence it follows that $RT^i\underline{r}=T^{n-i}R\underline{r}$.

Q.E.D.

Theorem 3.3: If $\underline{r}+T^i\underline{r}=\underline{z}(\bar{\underline{z}})$, then $R\underline{r}+T^{n-i}R\underline{r}=\underline{z}(\bar{\underline{z}})$.

Proof: By Lemma 3.1, $R\underline{r}+T^{n-i}R\underline{r}=R\underline{r}+RT^i\underline{r}=R[\underline{r}+T^i\underline{r}]=R\underline{z}=\underline{z}$ and similarly for $\bar{\underline{z}}$.

Q.E.D.

By Theorem 3.3 when finding the solutions $\underline{r}$ of $\underline{r}+T^i\underline{r}=\underline{z}$(or $\bar{\underline{z}}$) we only need consider those i's which are less than or equal to (n-1)/2.

For all n's up to 51 the best sequence(in the sense of minimizing $P=\max(P_E,P_\theta)$) in the above class, i.e. the class $\underline{r}$ $\underline{r}+T^i\underline{r}=\underline{z}$(or $\bar{\underline{z}}$), g.c.d.(n,i)=1 , was found on the IBM 1130 computer of the Engineering College of the University of Notre Dame. The results of this investigation are given in Table 4. Instead of giving a best sequence explicitely the corresponding i, i.e. that i such that $\underline{r}+T^i\underline{r}=\underline{z}$(of $\bar{\underline{z}}$), is given.

TABLE 4

SELF-DUAL SEQUENCES WHICH

SATISFY $\underline{r}+T^i\underline{r}=\underline{z}$ (or $\bar{\underline{z}}$)

n	i	$P=P_F$	n	i	$P=P_F$
3	1	1	29	12	9
5	2	1	31	12	11
7	2	3	33	10	15
9	2	5	35	8	19
11	3	5	37	10	17
13	5	3	39	16	19
15	4	7	41	12	17
17	5	7	43	12	19
19	7	7	45	19	17
21	8	5	47	13	21
23	7	11	49	18	19
25	7	11	51	11	29
27	8	11			

B. THE RECIPROCAL OPERATOR

It is clear that if $\underline{r}$ is a binary n-tuple, n odd, then $E_k(R\underline{r})=E_k(\underline{r})$, i.e. R leaves the even correlation coeficients invariant. Hence if $\underline{r}+\underline{z}=R\underline{r}$ then $\underline{r}$ is self-dual. We note here that we cannot use $\bar{\underline{z}}$ because $z_{\frac{n-1}{2}}=1$ whereas the corresponding coordinate of $\underline{r}+R\underline{r}$ is always zero. We have

Theorem 3.4: If $4|n-1$, then the set $\{\underline{r}|\underline{r}+R\underline{r}=\underline{z}\}$ forms a coset of the space $\{\underline{r}|R\underline{r}=\underline{r}\}$. In particular, the number of binary n-tuples $\underline{r}$ which satisfy $\underline{r}+\underline{z}=R\underline{r}$ is $2^{(n+1)/2}$.

Proof: It is clear that the set of all binary n-tuples forms

a vector space over GF(2)(with the natural operations) of dimension n. Since R is a linear transformation on this space then $V=\{\underline{r}|R\underline{r}=\underline{r}\}$ is a vector subspace. Now $R\underline{r}=\underline{r}$ if and only if $(r_{n-1},\ldots,r_{(n+1)/2})=(r_0,r_1,\ldots,r_{(n-3)/2})$, the middle coordinate being arbitrary, hence the dimension of V over GF(2) is (n+1)/2.

Let $\underline{s}=(0,..,0,0,1,0,1,..,1,0)$ where the number of leading zeros is (n+1)/2. Let $\underline{w}$ belong to V and let $\underline{r}=\underline{s}+\underline{w}$, then $\underline{r}+R\underline{r}=\underline{s}+\underline{w}+R(\underline{s}+\underline{w})=\underline{s}+R\underline{s}+\underline{w}+R\underline{w}=\underline{s}+R\underline{s}=\underline{z}$ and so $\underline{r}$ satisfies $\underline{r}+\underline{z}=R\underline{r}$.

Let $\underline{r}_1,\underline{r}_2$ satisfy $\underline{r}_i+\underline{z}=R\underline{r}_i$ i=1,2, then $(\underline{r}_1+\underline{r}_2)+R(\underline{r}_1+\underline{r}_2)=\underline{z}+\underline{z}=0$ which implies that $(\underline{r}_1+\underline{r}_2)$ belongs to V. Hence $\underline{r}$ satisfies $\underline{r}+\underline{z}=R\underline{r}$ if and only if $\underline{r}$ belongs to $\underline{s}+V$.

Q.E.D.

Corollary: The set $\{\underline{r}|\underline{r}+\underline{z}=R\underline{r}\}$ is closed under R, binary complementation and the map $\underline{r}\longrightarrow\underline{r}+\underline{z}$.

Example: If n=5 the set of $\underline{r}$'s which satisfy $\underline{r}+\underline{z}=R\underline{r}$ is {(0,0,0,1,0),(0,0,1,1,0),(0,1,0,0,0),(0,1,1,0,0),(1,0,0,1,1),(1,0,1,1,1),(1,1,0,0,1),(1,1,1,0,1)}.

A best possible sequence, in the sense of minimizing P, which satisfies $\underline{r}+\underline{z}=R\underline{r}$ has been found for n=5,9,13,17,21,25 and 29. These results are given in Table 5. These results seem to indicate that this class of sequences is a source of good sequences(unfortunately it is large). For example we note from Table 5 that the Barker sequences(sequences which satisfy $|F_k|\leq 1$ for $0<k<n$) of lengths 5 and 13 are in this class.

TABLE 5

SELF-DUAL SEQUENCES WHICH SATISFY

$\underline{r}+\underline{z}=R\underline{r}$

n	Sample Sequence	$P=P_F$
5	10111	1
9	100001011	3
13	1111100110101	1
17	10100100010001111	3
21	111101100001011000101	3
25	1000111000000101011011011	3
29	11100111000000010101001001101	3

Because of the wide attention paid to Barker Sequences we single this out as

Theorem 3.5: The Barker sequences of lengths 5 and 13 satisfy $\underline{r}+\underline{z}=R\underline{r}$.

For the lengths 9,17,21,25 and 29 the sequences given in Table 5 are the best (in the sense of minimizing P) for these lengths since there do not exist Barker Sequences for these lengths[15].

For lengths 33,37 and 41 a sequence in the above class was found for which P=5. These are given below.

n=33, 110110110100000001010100001110001

n=37, 1001101011110010000101110010111110011

n=41, 11011001011011000000010101001110000110001

We remark that these may not be the best for these lengths.

CHAPTER IV

WEAKLY-BARKER SEQUENCES

In Chapter 1 a binary signal scheme was introduced which gave birth to a new problem in the design of sequences, namely the problem of finding sequences having small $P=\max(P_E,P_\theta)$. Hence given n we would like to find an n-tuple $\underline{r}$ which minimizes P. A Barker Sequence[5] is a binary n-tuple $\underline{r}$ such that $|F_{n-k}(r)| \leq 1$, $0 < k < n$. Since $E_k=F_k+F_{n-k}$ and $\theta_k=F_k-F_{n-k}$ it follows that for a Barker Sequence $\underline{r}$, $P_E(\underline{r}) \leq 2$ and $P_\theta(\underline{r}) \leq 2$ from which it follows that $P(\underline{r}) \leq 2$. We can say a little more for since $F_k(\underline{r})=(n-k)-2d_H[f_{n-k}(\underline{r}),b_{n-k}(\underline{r})]$ then $F_k(\underline{r}) \equiv (n-k) \bmod (2)$. If n is odd and k is odd then $2|F_k(\underline{r})$. Hence if $\underline{r}$ is a Barker Sequence of odd length n, then $F_k(\underline{r})=0$ for k odd and $|F_k(\underline{r})|=1$ for even k. Therefore for a Barker Sequence $\underline{r}$ of odd length $P(\underline{r})=1$ and for a Barker sequence $\underline{r}$ of even length $P(\underline{r})=2$. In both cases this is an optimum solution to the above minimization problem. Unfortunately, Barker sequences are known to exist only for n=1,2,3,4,5,7,11 and 13. It is known that if any other Barker sequences exist, they have n even and a perfect square[4,15,16]. Whether any such exist for n greater than 13 and of this form is unknown, but the educated guess seems to be "no".

The tactic in this Chapter is to relax the strict Barker criterion sufficiently to guarantee the existence of many sequences without eliminating all the useful implications which the condition imposes on E and θ. To this end, we define a

Weakly-Barker Sequence(or WB-sequence for short) to be a binary n-tuple $\underline{r}$ such that

$$|F_{n-k}(r)| \leq 1 \quad 0 < k < (n+1)/2 \tag{4.1}$$

The following result shows that this relaxation of the full Barker criterion has indeed greatly widened the number of sequences.

Theorem 4.1: There exist WB-sequences of length n for every n.

Proof: The proof follows by noting that $\underline{r}$=(1,0,1,0,..,1,0,0,.....,0), where the number of trailing zeros is (n-1)/2 for odd n and (n/2)+1 for n even, is always a WB-sequence(Unfortunately, this particular sequence has poor E and θ functions for large n).

Q.E.D.

That the relaxation of the Barker condition has not completely destroyed its utility with respect to describing E and θ follows from the following Theorem which states essentially that for WB-sequences either the even and odd correlation functions are both good or they are both bad.

Theorem 4.2: For a WB-sequence,

$$||E_k| - |\theta_k|| \leq 2, \quad 0 < k < n. \tag{4.2}$$

Proof: From (1.4) we have that

$$\begin{aligned} E_k - \theta_k &= 2F_{n-k} \\ E_k + \theta_k &= 2F_k \end{aligned} \qquad 0 < k < n \tag{4.3}$$

But (4.3) with the definition of a WB-sequence shows that

$$|E_k-\theta_k| \leq 2 \quad 0< k< (n+1)/2$$
$$|E_k+\theta_k| \leq 2 \quad [(n-1)/2]< k< n. \tag{4.4}$$

But (4.4) in turn implies (4.2).

Q.E.D.

The fact that for a WB-sequence both the even and the odd correlation functions are of the same quality is a feature not charactheristic of most commonly encountered sequences. For instance, PN-sequences[13] have optimal even correlation coefficients(in fact $E_k=-1$ for $0< k< n$) but can have fairly poor odd correlation coefficients, i.e. there may be values of k for which θ_k is quite large. For example, the PN-sequence 100001101 010010001011111011001l of length 31 has $\theta_{18}=13$.

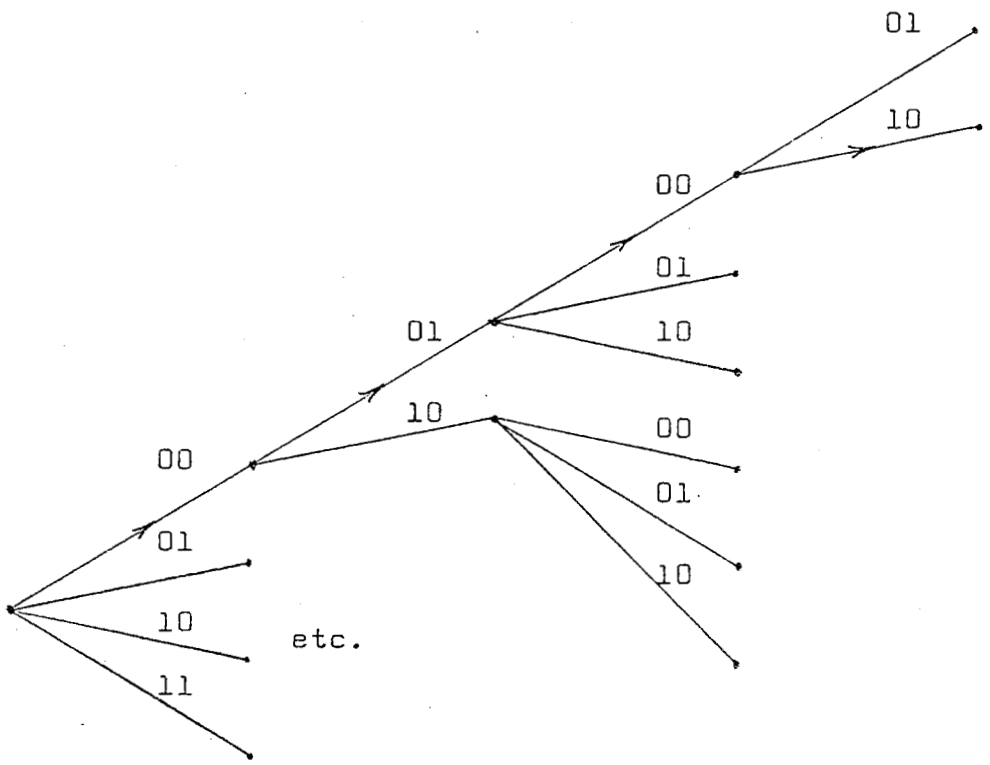
For any given length n, the set of all WB-sequences can be generated as follows. First pick r_0 and r_{n-1} arbitrarily. Hence there are four starting points for the construction. Next, choose r_1 and r_{n-2} in such a way that $|F_{n-2}| \leq 1$. Recall that F_{n-i} is a function of $r_0,r_1,\ldots,r_{i-1},r_{n-i},r_{n-i+1},\ldots,r_{n-1}$, hence can be computed. On the k^{th} step choose r_{k-1} and r_{n-k} such that $|F_{n-k}| \leq 1$. If n is odd , then the last step in the algorithm will consist in choosing $r_{(n-1)/2}$ such that $|F_{(n-1)/2}| \leq 1$. If we only consider the construction of WB-sequences of even length, then the above algorithm generates a tree in which each branch is labelled with a binary 2-tuple, namely (r_{k-1},r_{n-k}). All the paths of length k starting from the first node will give all the WB-sequences of length 2k. In the construction of this tree a path will terminate when it is no longer possible to choose r_{k-1} and r_{n-k} in such a way that $|F_{n-k}| \leq 1$. See figure

1 for an example.

FIGURE 1.

PARTIAL TREE FOR THE GENERATION OF

WB-SEQUENCES OF LENGTH 8



Following the path with arrow heads we obtain the WB-sequence 00010010 of length 8. The above algorithm was implemented on the UNIVAC 1107 computer in the University of Notre Dame Computing Center, and all the WB-sequences were generated for lengths 13, 14,16,18,19,20,21,22,25,27,31 and 32. In Table 6 a sample of the best WB-sequences(in the sense of minimizing P) obtained is given for each of the above mentioned lengths. In Table 7 all the best WB-sequences of length 31 are given. It is interesting to note that the smallest value of P_g obtainable with PN-sequences of length 31 is 7. Hence the WB-sequences given in Table 7 are strictly better than the best PN-sequences(in the sense of minimi-

zing P).

TABLE 6

SAMPLE OF BEST WB-SEQUENCE OF VARIOUS LENGTHS

n	P_E	P_θ	Number of Sequences	Sample Sequence
13	1	1	4	1111100110101
14	2	4	54	11100011101101
16	4	2	8	0000110010010101
18	2	2	8	010110100000110011
19	5	3	8	1010101001111110011
20	4	4	64	00111100100010010101
21	5	5	72	010110100100000110011
22	2	4	8	0110010101100011111111
25	5	5	40	1010101001100111111001111
27	5	5	24	101010100101100001111110011
31	5	5	12	0000110000110111011101010010101
32	4	6	16	11100011111101000100010101101101

TABLE 7

BEST WB-SEQUENCES OF LENGTH 31

0000110000110111011101010010101
1111001111001000100010101101010
0101100101100010001000000111111
1010011010011101110111111000000
0000001111110111011100101100101
1111110000001000100011010011010
0101011010100010001001111001111
1010100101011101110110000110000
0000000111100100111001011010101
1111111000011011000110100101010
0101010010110001101100001111111
1010101101001110010011110000000

CHAPTER V

SEQUENCES OBTAINED FROM AN-CODES

There exists very few methods of obtaining sequences with desirable correlation properties. The only real success obtained in this area has been the construction of binary two-level autocorrelation sequences(i.e. binary sequences for which $E_0=n$ and $E_k=m$, $0< k< n$, and m an integer, $-n< m< n$)[13] The success obtained here can be mainly attributed to the fact that the construction of binary two-level autocorrelation sequences has a perfect analog in Mathematics, namely the construction of special difference sets[17,19]. As has been pointed out before, there are no construction techniques available for the construction of sequences with a prescribed value of $P_F=\max_{0< k<n}|F_k|$.

This Chapter is mainly a compendum of results obtained about sequences derived from Arithmetic Codes, more specifically from cyclic AN-codes. These results seem to indicate that this is a source of good correlation sequences and hopefully more work will be done in this area.

For any positive integer A the AN-code generated by A is the set of integers AN for $0\leqslant N< B$ where B is a specified integer which determines the number of integers in the code[21]. With each integer(or code point) in an AN-code we associate a code word as follows: Let the largest code point A(B-1) in the AN-code require n places for its radix two form, then we associate with each code point in the AN-code its n-place radix

two form which is called the corresponding code word and n the length of the code. For example if A=3 and B=4 then the AN-code is $\{0,3,6,9\}$ and the corresponding set of code words is {0000, 0011,0110,1001} where the rightmost digit in the radix two form corresponds to 2^0. An AN-code is said to be cyclic if the corresponding set of code words is closed under the cyclic-shift operator T. In the study of cyclic AN-codes the convention is adopted that a cyclic AN-code of length n is not to contain the integer corresponding to the all 1 code word. With this convention it is known(see Theorem 3.1 of [21]) that an AN-code with B code points is cyclic if and only if $AB=2^n-1$. For example if A=3 and B=5 then the AN-code is $\{0,3,6,9,12\}$ and the corresponding set of code words is {0000,0011,0110,1001,1100} which is clearly closed under T. Given an odd integer A the convention is adopted that $B=(2^n-1)/A$ where n is chosen such that $A|2^n-1$, but $A\not|2^i-1$, for any i, $0< i< n$. This particular n is called the exponent of 2 modulo A and denoted by e(A)(e(A) is therefore the length of the cyclic AN-code generated by A). Sequences obtained from two classes of cyclic AN-codes have been analyzed, namely the Mandelbaum-Barrows cyclic AN-codes and the modified Mandelbaum-Barrows cyclic AN-codes. In the first case the sequence analyzed was taken to be the first half of the code word corresponding to A(the reason for this is given in section A) and in the second case the sequence was taken as the code word corresponding to A.

A. MANDELBAUM-BARROWS

We state Theorem 3.7 of [21] even though it uses terms

which have not been defined here. The definitions can be found in [21].

Theorem 5.1(Mandelbaum-Barrows): If B is any prime such that 2 is primitive in GF(B), then $A=(2^{B-1}-1)/B$ generates an equidistant cyclic AN-code of length n=B-1 and minimum distance $D_{min}=int[(B+1)/3]$.

The codes given by the above Theorem are the Mandelbaum-Barrows cyclic AN-codes. It has been observed in this work that the code words of the Mandelbaum-Barrows code are all of the form $\underline{r}\bar{\underline{r}}$ where $\underline{r}$ is an n/2-tuple. This follows directly from the fact that the set of non-zero code-words for these codes forms a single cyclic class which is closed under complementation and the only way this can be is that the code words be of the form suggested above. We collect this as

Theorem 5.2: The non-zero code words corresponding to the Mandelbaum-Barrows cyclic AN-codes are all of the form $\underline{r}\bar{\underline{r}}$, where $\underline{r}$ is an n/2-tuple and n is the length of the code.

Because of Theorem 1.4 we have used for our sequence the first half of the code word corresponding to A. The results of this investigation are given in Table 8.

B. MODIFIED MANDELBAUM-BARROWS AN-CODES

The main result about the Modified Mandelbaum-Barrows cyclic AN-codes is contained in Corollary 3.3 of [21] which we state as

Theorem 5.3: If B is a prime such that $R_B(-2)=B-2$ is primitive in GF(B) but 2 is not primitive, then $A=[2^{(B-1)/2}-1]/B$

generates an equidistant cyclic AN-code of length n=(B-1)/2 and minimum distance $D_{min}=(1/2)int[(B+1)/3]$.

TABLE 8

SEQUENCES OBTAINED FROM MANDELBAUM-BARROWS CYCLIC AN-CODES

n	A	Sequence	P_F	P_E	P_θ
12	315	110111	2	2	2
18	13,797	101001111	3	3	3
28	9,256,395	11010011101111	3	6	4
36	1,857,283,155	1100101000100111111	6	6	6
52	84,973,577,874,915	11000111101101010011011111	5	6	6
66	1,101,298,153,654,301,589	10101001110011011101101110110100 00111111	11	13	11

The results obtained with sequences obtained from the Modified Mandelbaum-Barrows cyclic AN-codes are given in Table 9

TABLE 9

SEQUENCES OBTAINED FROM MODIFIED MANDELBAUM-BARROWS CYCLIC AN-CODES

n	A	Sequence	P_F	P_E	P_θ
11	89	10011010000	2	3	3
23	178,481	10001100100111010100000	5	7	9
35	483,939,977	10010001011010100001101100111 000000	7	11	9
39	6,958,934,353	10001010100101110001001101111 0011000000	11	13	9
51	11,862,134,113,449	10010101001000100101001001111 011100100110101000000	10	11	15

CHAPTER VI

CONCLUSIONS

In Chapter 1 a bandwidth-spreading binary signal scheme was introduced which required a binary n-tuple with small parameter $P=\max(P_E,P_\theta)$ where $P_E=\max_{0<k<n}|F_k+F_{n-k}|$ and $P_\theta=\max_{0<k<n}|F_k-F_{n-k}|$. This gave birth to a new problem in the design of sequences.

A <u>sub-baud code</u>[2] of length n is a set $V=\{\underline{r}_1,\underline{r}_2,\ldots,\underline{r}_M\}$ of M binary n-tuples where no two r_i's belong to the same cyclic class nor to the same compacyclic class. With V we associate the parameters $P_E(V)=\max_{1\leq i\leq M} P_E(\underline{r}_i)$, $P_\theta(V)=\max_{1\leq i\leq M} P_\theta(\underline{r}_i)$, $P_{EC}(V)=\max[\max_{i\neq j}\max_{0\leq k<n}|n-2d_H(\underline{r}_i,T^k\underline{r}_j)|]$ and $P_{\theta C}(V)=\max[\max_{i\neq j}\max_{0\leq k<n}|n-2d_H(r_i,N^k r_j)|]$. Given an n and M then the problem is to construct a V of order M which minimizes $P(V)=\max[P_E(V),P_\theta(V),P_{EC}(V),P_{\theta C}(V)]$. When M=1 we define $P_{EC}(V)=0$ and $P_{\theta C}(V)=0$ in which case $P(V)=\max[P_E(V),P_\theta(V)]$. Hence the problem described in Chapter 1 is but the degenerate case of this more interesting and correspondingly more difficult problem.

In Chapter 2 a class of sequences was described for which $F_k-F_{n-k}=(-1)^k(F_{2k}+F_{2(n-k)})$ or equivalently $\theta_k=(-1)^k E_{2k}$ where 2k and 2(n-k) are reduced modulo n. For this class $P=P_E=P_\theta$. The construction of these sequences gave rise to an interesting problem in Number Theory, namely that of characterizing the integers n for which all cyclotomic cosets contain an even number of odd integers. This problem was only partly solved there.

In Chapter 3 a class of sequences was described for which $\theta_k=(-1)^k E_k$. Two methods were described to generate such sequences. The class given in section B of Chapter 3 looks promising as a source of good sequences and perhaps deserves more study. It should be pointed out that there exist other operators which leave the even correlation coefficients invariant but that T and R were chosen because they could be handled analytically and because the corresponding sequences could easily be generated. It is however possible that other operators may yield better sequences.

In Chapter 4 the Weakly-Barker sequences were introduced for which $\|E_k|-|\theta_k\| \leq 2$ a property not usually possessed by most encountered sequences. Unfortunately not much more seems to be possible here.

Lastly in Chapter 5 certain computer results were given about sequences obtained from AN-codes. Though no analytical results have been obtained here it is hoped that the results presented will stimulate some research in this area.

In Table 11 of the Appendix we have collected some results about the best sequences(in the sense of minimizing P) found during this work.

APPENDICES

TABLE 10

P_F FOR THE ZERO PHASE AND THE [(N+1)/4]-TH PHASE OF THE LEGENDRE SEQUENCES

n	Zero Phase		(n+1)/4* Phase		n	Zero-Phase		(n+1)/4 phase	
	P_F	n/P_F	P_F	n/P_F		P_F	n/P_F	P_F	n/P_F
3	2	1.50	1	3.00	367	29	12.65	16	22.94
7	3	2.33	1	7.00	379	29	13.07	14	27.07
11	4	2.75	3	3.67	383	30	12.76	19	20.16
19	6	3.17	3	6.33	419	34	12.32	16	26.18
23	6	3.83	3	7.66	431	40	10.77	20	21.55
31	7	4.43	4	7.75	439	34	12.91	19	23.11
43	8	5.37	5	8.60	443	34	13.03	16	27.69
47	10	4.70	4	11.75	463	36	12.86	16	28.94
59	12	4.92	5	11.80	467	35	13.34	16	29.19
67	10	6.70	6	11.17	479	37	12.94	20	23.95
71	12	5.92	6	11.83	487	36	13.52	19	25.63
79	13	6.08	7	11.28	491	38	12.92	19	25.84
83	15	5.53	8	10.37	499	39	12.79	21	23.76
103	14	7.36	10	10.30	503	36	13.97	18	27.94
107	14	7.64	8	13.37	523	41	12.76	20	26.15
127	19	6.68	10	12.70	547	41	13.34	23	23.78
131	18	7.28	8	16.37	563	40	14.07	18	31.27
139	18	7.72	9	15.44	571	45	12.69	22	25.95
151	21	7.19	9	16.77	587	47	12.49	23	25.52
163	19	8.58	10	16.30	599	41	14.60	23	26.04
167	20	8.35	11	15.18	607	41	14.80	19	31.94
179	23	7.78	11	16.27	619	41	15.09	21	29.48
191	20	9.55	13	14.69	631	42	15.02	21	30.05
199	19	10.47	11	18.09	643	44	14.61	22	29.23
211	22	9.59	13	16.23	647	43	15.04	24	26.96
223	22	10.14	12	18.58	659	44	14.97	25	26.36
227	25	9.08	13	17.46	683	39	17.51	23	29.67
239	20	11.95	14	17.07	691	46	15.02	23	30.04
251	28	8.96	15	16.73	719	48	14.98	28	25.67
263	28	9.39	13	20.23	727	41	17.73	25	29.08
271	23	11.78	15	18.06	739	49	15.08	25	29.56
283	29	9.76	14	20.21	743	47	15.80	25	29.72
307	27	11.37	15	20.47	751	50	15.02	26	28.88
311	27	11.52	15	20.73	787	48	16.39	27	29.15
331	29	11.41	15	22.07	811	49	16.55	25	32.44
347	30	11.57	17	20.41	823	45	18.29	26	31.65
359	29	12.38	16	22.44	827	55	15.04	25	33.08

* By the (n+1)/4 phase is meant the sequence $T^{(n+1)/4}\,\underline{r}$ where $\underline{r}$ is the zero phase

TABLE 11

THE BEST FOUND SEQUENCES IN THE

SENSE OF MINIMIZING P

Length	P	P_E	P_g	P_F	Sample Sequence	Type
3	1	1	1	1	110	Barker
4	2	0	2	1	1101	Barker
5	1	1	1	1	10111	Barker
7	1	1	1	1	1110010	Barker
9	3	3	3	3	100001011	RSD[1]
11	1	1	1	1	11100010010	Barker
13	1	1	1	1	1111100110101	Barker
14	4	2	4	3	11100011101101	WB[2]
16	4	4	2	3	0000110010010101	WB
17	3	3	3	3	10100100010001111	RSD
18	2	2	2	2	010110100000110011	WB
19	5	5	3	4	1010101001111110011	WB
20	4	4	4	4	00111100100010010101	WB
21	3	3	3	3	111101100001011000101	RSD
22	4	2	4	3	0110010101100011111111	WB
23	5	1	5	3	0100001111101011001100101	Legendre[3]
25	3	3	3	3	1000111000000101011011011	RSD
27	5	5	5	5	1010101001011000011111100011	WB
29	3	3	3	3	11100111000000001010100100101	RSD
31	5	5	5	5	0000110000110111011101010010101	WB
32	6	4	6	5	11100011111110100010001010111011	WB

1. Self-dual sequence from Table 5
2. Weakly-Barker sequence
3. The (n+1)/4 phase of the Legendre sequence

REFERENCES

[1] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing", IEEE Trans. on Inf. Theo., Vol.IT-13, No.4, Oct.1967, pp.619-621.

[2] J.L. Massey and J.J. Uhran, "Sub-Baud Coding and Cyclic Codes", presented at the IEEE Int. Symposium on Information Theory, Noordwijk, The Netherlands, June 1970.

[3] G. Seguin, "Binary Sequences With a Relaxed Barker Criterion", Proceedings of the National Electronics Conference, Vol.26, 1970, pp.456-457.

[4] R. Turyn, "Sequences With Small Correlation", Error-Correcting Codes(edited by H.B. Mann), John Wiley and Sons, 1968, pp.195-228.

[5] R.H. Barker, "Group Synchronization of Binary Digital Systems", in Communication Theory, edited by W. Jackson, New-York, Academic Press, Inc.,1953, pp.273-287.

[6] W.W. Peterson, Error-Correcting Codes , M.I.T. Press, Cambridge, Mass., 1961.

[7] E.R. Berlekamp, Algebraic Coding Theory, McGraw Hill, New-York, 1968.

[8] S.W. Golomb, B. Gordon and L.R. Welch, "Comma-Free Codes", Canadian Journal of Mathematics, Vol.10, 1958, pp.202-209.

[9] Jessie Mac Williams, "The Structure and Properties of Binary Cyclic Alphabets", Bell System Technical Journal, Vol.44, 1964, pp.303-333.

[10] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers , Oxford at the Clarendon Press, 1938.

[11] S.W. Golomb and R.A. Scholtz, "Generalized Barker Sequences", IEEE Trans. on Inf. The., Vol.IT-11, Num.4, 1965, pp.533-537.

[12] A.A. Albert, Fundamental Concepts of Higher Algebra, The Univ. of Chicago Press, Chicago, Ill., 1956.

[13] S.W. Golomb, Shift Register Sequences, Holden-Day, Inc., San Francisco, Calif., 1967.

[14] I.N. Herstein, Topics in Algebra, Blaisdell Pub. Co., New-York, N.Y., 1964.

[15] J. Storer and R. Turyn, "On Binary Sequences", Proc. of The Amer. Math. Soc. Vol.12, 1961, pp.394-399.

[16] Iu. Poliak and R.V. Moshetov, Scientific Transactions of The Radio-Engineering and Institute of the Acad. Sci. US SR 1; pp.124-159.

[17] Leonard D. Baumert, "Codes With Special Correlation", Digital Communications with Space Applications, edited by S.W. Golomb, Prentice-Hall, Englewood Cliffs, N.J., 1964.

[18] Paul E. Allard, "Some Results on the Factorization of $1+x^{2^q-1}$ over GF(2) in Regard to Error Correcting Codes", Master's Thesis, Dept. of Elect. Engrg., University of Ottawa, Ottawa, Ont., Canada.

[19] Marshall Hall Jr., "A Survey of Difference Sets", Proc. of the Amer. Math. Soc., Vol.7, 1956, pp.975-986.

[20] J.R. Caprio, "On Optimum Radar Ranging Codes", Tech. Rep. No.95, Elect. Engrg. Research Lab., Cornell University, Ithaca, New-York, 1966.

[21] J.L. Massey and O. Garcia, "Error-Correcting Codes in Computer Arithmetic", to appear in Advances in Information System Science, Vol.4(Edited by J. Tou), Plenum Press, New-York, 1971.

[22] J.L. Massey, "Reversible Codes", Information and Control, Vol.7, No.3, Sept. 1964, pp. 369-380