Technical Report 1676
September 1994

Waveforms for Reducing Direct Blast Effects and Mutual Interference

R. Ricks

EXECUTIVE SUMMARY

OBJECTIVE

Design active sonar waveforms that are yield tolerance to the direct blast and reduce the potential for mutual target interference.

APPROACH

Divide the transmission into a wavetrain of noncontiguous pulses with nonuniform spacings and determine the appropriate values for that spacing.

RESULTS

The interpulse spacing is described by a code and exhaustive tables of codes are listed for wave-trains of up to a given number of pulses. Search methods are described for finding the codes.

CONCLUSIONS

For bistatic sonars, a region can be defined where echos from targets in the region are affected by the direct blast. The area of the region is proportional to the root of the temporal pulse length. If the pulse is split into a wavetrain of subpulses, the area can be significantly reduced. The area becomes proportional to the root of the subpulse length.

CONTENTS

1.0 WAVEFORMS FOR REDUCING DIRECT BLAST EFFECTS AND MUTUAL INTERFERENCE 1

1.1 INTRODUCTION 1

1.2 AREA OF THE DIRECT BLAST AND MUTUAL INTERFERENCE REGIONS 4

1.3 OPTICAL ORTHOGONAL CODES (OOC'S) 5

1.4 CODES FOR L > 1 7

1.5 EXHAUSTIVE SEARCH 7

1.6 DIFFERENCE SETS AND MULTIPLIERS 10

1.7 NONCIRCULAR OPTICAL ORTHOGONAL CODES 13

1.8 SEARCH FOR NOOC'S 14

1.9 COMPARING CODES 17

1.10 CONCLUSIONS 19

1.11 REFERENCES 19

Figures

1. Direct blast region 1
2. Mutual interference region 2
3. Example of an OOC code 3
4. Circular autocorrelation function for code [1 0 0 0 1 1 0 1 0 0 0 0 0] 3
5. Noncircular autocorrelation function for code [1 0 0 0 1 1 0 1 0 0 0 0 0] 3
6. Direct blast geometry 5
7. NOOC {1, 4, 7, 13, 2, 8, 6, 3, 1} with the most compact noncircular autocorrelation 18
8. The most spread noncircular autocorrelation, Code {2, 6, 18, 22, 7, 5, 16, 4, 10, 1} 18
9. Noncircular autocorrelation of code {4, 5, 13, 10, 6, 8, 3} with three zeroz on each side of the central peak 18

Tables

1. The number of codes found by multiplication 12
2. Minimum-length orthogonal optical codes 13
3. Minimum-length noncircular orthogonal optical codes 17

1.0 WAVEFORMS FOR REDUCING DIRECT BLAST EFFECTS AND MUTUAL INTERFERENCE

1.1 INTRODUCTION

Sonar has been widely used for actively detecting underwater targets. In active sonar, a pulse of sound is transmitted, and the pulse is reflected off the target and back to a receiver where the echo is processed by detecting the presence of the target. In monostatic sonar, the receiver is collocated with the transmitter. However, in bistatic sonar the receiver and transmitter are widely separated. For bistatic sonar, the transmitted pulse impinges directly on the receiver causing the “direct blast.” To prevent saturation, the receiver is “blanked” during the arrival of the direct blast. For some transmitter-target-receiver geometries, particularly where a target is between the transmitter and receiver, the part of the target echo which arrives during the blanking is lost. Though a partial loss of target echo is tolerable, at some level the target echo loss yields unacceptable performance. For a given transmitter-receiver geometry, the locus of target positions that yield this loss forms an ellipse as illustrated in Figure 1. The interior of the ellipse is called the direct blast region. The area of this region is a measure of a systems “blindness” due to the direct blast.

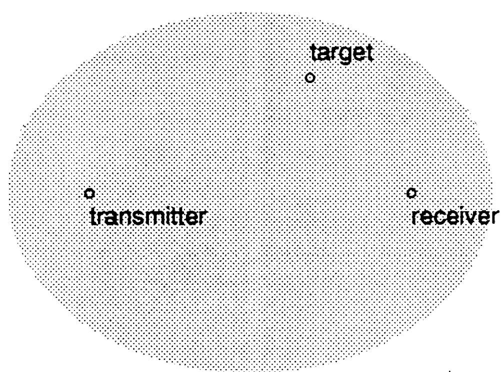

Figure 1. Direct blast region.

Suppose there are one strong and one weak target in a bistatic scenario. The strong target echo may interfere with the weaker target echo. For some level of echo overlap and some disparity in target strength, the two targets cannot be adequately resolved by temporal processing alone. For a given transmitter, strong target, and receiver geometry, the locus of weak target positions that yield this condition forms concentric ellipses as shown in Figure 2. The region between these ellipses is denoted the mutual interference region. The area of this region is a measure of the potential for interference between targets.

The areas of the mutual interference and direct blast regions are functions of the transmit pulse length and can be reduced by shortening the pulse. However, shortening the pulse also reduces the pulse energy. As a result, target echoes become weaker and more difficult to detect.

In this paper, a waveform design is introduced for significantly reducing the direct blast and mutual interference areas by spreading the transmission out into a train of pulses. Each pulse is called a chip. By spreading the transmission, direct blast and mutual interference areas corresponding to a single chip length can be achieved.

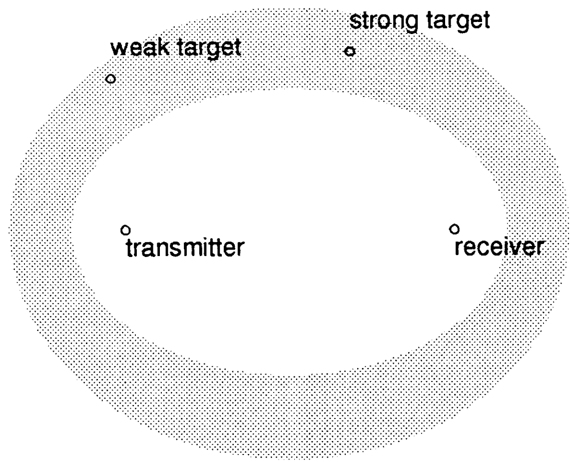

Figure 2. Mutual interference region.

The direct blast and mutual interference properties of the transmission sequence can be measured by the sequence autocorrelation function. The autocorrelation function must have a narrow central lobe two chips in width and be small in magnitude and bounded everywhere else.

If the chips are uniformly spaced, nontrivial target ranges exist such that much of the target echo arrives during the direct blast. In other words, the autocorrelation function has large sidelobes. Therefore uniform spacing of chips is unacceptable.

In the case of the direct blast, it is useless to consider transmission sequences where autocorrelation sidelobes are reduced by mutual cancellation between chips, as such cancellation would fail because of the need for blanking.[1] Therefore, only unipodal sequences (sequences of 0's and 1's) are considered. For such codes the autocorrelation sidelobes are reduced by minimizing temporal overlap.

In [1, 2], a family of unipodal sequences is introduced that have small, bounded autocorrelation sidelobes. Since their application is in optical communications, the sequences are called optical orthogonal codes (OOC). The term optical indicates unipodal sequences as opposed to antipodal sequences (sequences of –1's and 1's). The term orthogonal is qualitative rather than literal.

Let x_t be a unipodal sequence. The circular autocorrelation of x_n is

$$Z_{x,x}(l) = \sum_{n=0}^{\nu-1} x_n x_{n+1 \bmod \nu} \,,\ 0 \le l \le \nu - l \tag{1}$$

and has the symmetry property

$$Z_{x,x}(l) = Z_{x,x}(\nu - l) \,,\ l \ne 0 \,. \tag{2}$$

The noncircular autocorrelation is

$$W_{x,x}(l) = \sum_{n=0}^{\nu-1} x_n x_{n+l} \,,\ -(\nu-1) \le l \le \nu - 1 \tag{3}$$

and has the symetry property

$$W_{x,x}(l) = W_{x,x}(l) \,. \tag{4}$$

1. Mutual cancellation between chips is useful for reducing mutual interference between targets. However, mutual interference can also be reduced using the methods presented here.

The OOC property of having bounded sidelobes is defined with respect to the circular autocorrelation function. Mathematically,

$$Z_{x,x}(l) \leq \lambda \; , \; 1 \leq l \leq \nu - 1 \; . \tag{5}$$

However, unless identical pulse sequences are transmitted back to back, direct blast and mutual interference properties are determined by the noncircular autocorrelation function. Fortunately, for all unipodal codes, the noncircular autocorrelation is bounded by the circular autocorrelation. More specifically,

$$W_{x,x}(l) \leq Z_{x,x}(l) \; , \; 0 \leq l \leq \nu - 1 \; . \tag{6}$$

Consider, for example, the four-chip OOC code, x_n = [1 0 0 0 1 1 0 1 0 0 0 0 0] shown in Figure 3 which has circular and noncircular autocorrelation functions as shown in Figures 4 and 5, respectively. We have taken the liberty of displaying the continuous correlation functions which accurately represent subchip echo overlap.

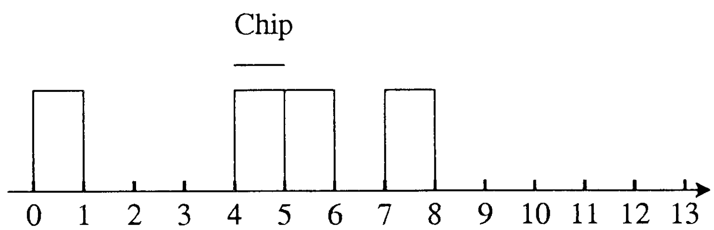

Figure 3. Example of an OOC code.

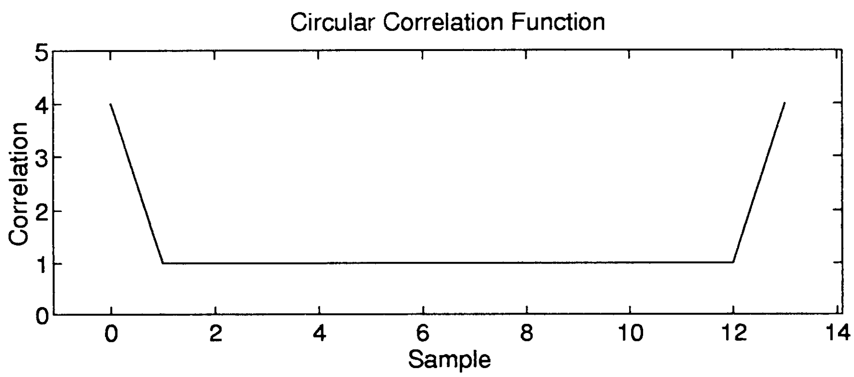

Figure 4. Circular autocorrelation function for code [1 0 0 0 1 1 0 1 0 0 0 0 0].

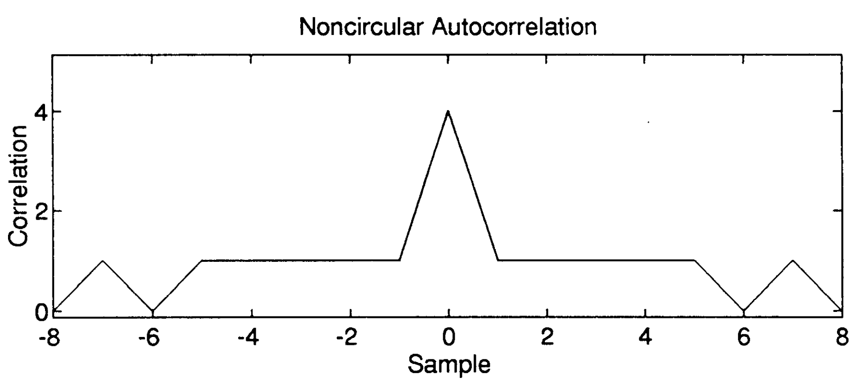

Figure 5. Noncircular autocorrelation function for code [1 0 0 0 1 1 0 1 0 0 0 0 0].

By spreading the transmission, the direct blast and mutual interference regions have been reduced by factors of 2 and 4, respectively. Though the size of the actual direct blast region is related to the length of a single chip, there is a wide region corresponding to 8 chip lengths (compared to 4 chip lengths in the nonspread transmission) in which the direct blast partially overlaps the target echo. However, the overlap is limited to at most one chip. The loss of one chip of target echo is assumed to be tolerable. A design objective is to increase the number of chips to make the one chip loss insigificant.

Similarly, if OOC sequences are used in a mutual interference scenario, there is a wide region in which one chip from a strong target may interfere with one chip from a weaker target. However, the area of mutual interference region where all the chips interfere is substantially reduced.

The remainder of this report is organized as follows. First, the area of the direct blast and mutual interference regions are derived. Then, in Section 3.0, properties of OOC's are discussed. An exhaustive search (Greedy Algorithm) is the only sure way to generate a complete set of codes. Rules are given for accelerating the search. A faster method based on multipliers of difference sets is introduced. This method is limited to minimal length codes. It appears to generate a complete code set, but requires a starting code. In Section 4.0, a new family of codes called noncircular optical orthogonal codes (NOOC) is developed that are defined using the noncircular autocorrelation function. These codes have a higher duty cycle (fraction of time actually transmitting). Finally, criteria for choosing a code as the basis for a waveform design are given in Section 5.0.

1.2 AREA OF THE DIRECT BLAST AND MUTUAL INTERFERENCE REGIONS

In this section, the area of the direct blast and mutual interference regions are derived assuming a single contiguous chip is transmitted. Consider the transmitter-target-receiver geometry shown in Figure 6. The direct transmission travels a distance, D, from the source to the receiver while the target return travels a distance $r = g + h$. The locus of target positions for a given r define an ellipse.

The area of the ellipse is

$$A = \pi ab \tag{7}$$

where a and b are lengths of the major and minor axes, respectively. From geometry, we have

$$a = r/2 \tag{8}$$

$$b = 1/2\sqrt{r^2 - D^2} . \tag{9}$$

But the parameter of interest is

$$\Delta = r - D \tag{10}$$

the difference in the travel distances. Substituting (8) through (10) into (7) yields

$$A(\Delta) = \frac{\pi}{4}(D + \Delta)\sqrt{2\Delta D + \Delta^2} \tag{11}$$

To relate the difference in travel distances to the duration of the transmission, let $\Delta = \beta cT$ where c is the speed of sound and T is the duration of the transmission. The parameter β where $0 \leq \beta \leq 1$ takes into account the acceptable level of target echo loss.

For a monostatic scenario, $D = 0$,

$$A_{db} = \frac{\pi}{4}(\beta cT)^2 . \tag{12}$$

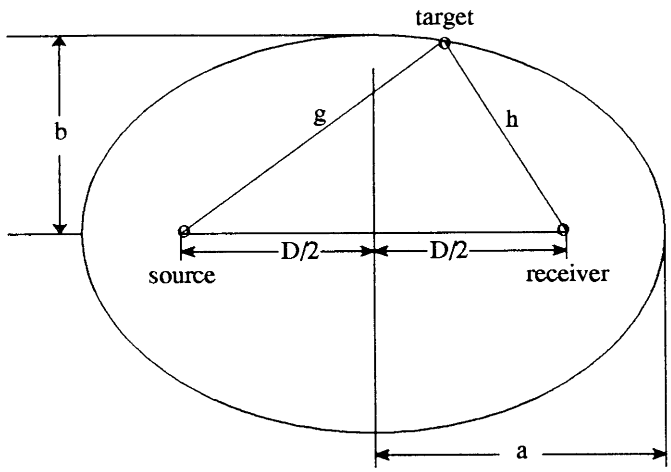

Figure 6. Direct blast geometry.

For a typical bistatic scenario, assuming $\Delta_0 \ll D$ yields

$$A_{ab} \approx \pi(D/2)^{\frac{3}{2}}(\beta cT)^{\frac{1}{2}} \tag{13}$$

and the area of the direct blast region is proportional to the square root of the duration of the transmission as claimed.

Now consider the mutual interference region and ignore the direct blast. The mutual interference region is an elliptic annulus as shown in Figure 2. If Δ_s and Δ_w are differences in the travel distances (compared to the direct path) associated with the strong and weak target, respectively, and $\Delta_d = |\Delta_s - \Delta_w|$, the area of the mutual interference region can be described in terms of $A(\Delta)$ defined in (11) as

$$A_{mi} = A(\Delta_s + \Delta_d) - A(\Delta_s - \Delta_d) \tag{14}$$

Again the difference in path lengths between the strong and weak targets can be related to the transmission duration using $\Delta_d = \gamma cT$ where γ is determined by the level of acceptable overlap and disparity in target strengths.

For the monostatic sonar,

$$A_{mi} \approx \pi\Delta_s\gamma cT\,. \tag{15}$$

Similarly, for the bistatic sonar, if we assume $\Delta_d \ll \Delta_s$ and $\Delta_d + \Delta_s \ll D$,

$$A_{mi} \approx \pi(D/2)^{\frac{3}{2}}\Delta_s^{-\frac{1}{2}}\gamma cT\,. \tag{16}$$

The bottom line is that to substantially reduce direct blast effects and mutual interference, sequences of noncontiguous chips must be considered. The temporal space between chips is described by a code.

1.3 OPTICAL ORTHOGONAL CODES (OOC'S)

An example of an OOC is shown in Figure 3. Because of the need to reduce sidelobes by avoiding temporal correlation, OOC's tend to have few 1's and many 0's. The placement of the 1's is critical. The orthogonality of an OOC is stated as

$$Z_{x,x}(l) \le \lambda \forall\, l \neq 0 \,. \tag{17}$$

Now, consider the code representation. The {1 0 0 0 1 1 0 1 0 0 0 0 0] representation is too lengthy. A more consise representation groups each ‘1’ with the ‘0’s that follow it and describes each group by the number of digits. For example, the four-chip code in Figure 3 is represented by the set {4, 1, 2, 6}. This is the difference representation.

In the literature, OOC’s are grouped into families defined by the parameters ν, the code length (sum of the digits in difference representation); K, the code weight (number of transmit chips, also the number of digits in differential representation); and λ. The code of Figure 3 has a length of 13, a weight of 4, and $\lambda = 1$. Combinatorics is used to determine the existence of codes, and if they exist, the number of codes per family. By our definition, all code variations with the same circular autocorrelation function are considered to be redundant.

Let $\{\tau_i, i=1, \dots K\}$ be the code difference representation where τ_i are integers. If $\tau_1 + \tau_2 = \tau_3$, then the correlation between the τ_3 shifted signal and the original depicted for $\tau_1 = 1$ and $\tau_2 = 2$ by

1101001...
   1101...

is at least 2. This motivates the following definition of an OOC which is useful for testing codes.

Definition 1 *A code is an (ν, K, λ) OOC if and only if*

$$\{\sum_{i=j \bmod \nu}^{j+m} \tau_1 | m = 1, \dots, K-1; j = 1, \dots, K\} \tag{18}$$

is a collection of integers with no member repeated more than λ times.

For a given weight and λ, there is a lower bound, ν_0, on the code length.

Property 1 *The minimum length of an OOC is*

$$\nu_0 = \left\lceil \frac{K(K-1}{\lambda} \right\rceil + 1 \,. \tag{19}$$

Proof. The trivial shift yields a correlation of K. Each of the K chips aligns with every other chip for some shift. Therefore, $\sum_{l=0}^{\nu_0 - 1} Z_{x,x}(l) = K^2$. If only nontrivial shifts are considered, $\sum_{l=0}^{\nu_0 - 1} Z_{x,x}(l) = K(K-1)$. Since each nontrivial shift yields a correlation of λ or less, and there arde $\nu_0 - 1$ distinct nontrivial shifts,

$$K(K-1) \le \lambda(\nu_0 - 1) \tag{20}$$

and Property 1 follows from the requirement that ν_0 be an integer.■

Furthermore, Ryser [4] makes the following Conjecture.

Conjecture 1 *If $K - \lambda$ is a power of a prime number, a minimal length code exists.*

Conjecture 1 has been verified for $K - \lambda \le 1600$.

There are OOC’s longer than the bound. For instance, codes (1, 2, 12, 5, 18, 4, 6), (1, 3, 2, 7, 10, 11, 14), (1, 3, 6, 20, 5, 2, 11), and (1, 4, 2, 19, 9, 3, 10) have a weight of 7 (though 7–1 = 2x3, not a power of a prime) and length 48 (cp. minimum length of 43). No $(\nu, 7, 1)$ codes exist for $\nu < 48$.

One OOC can be generated from another. Simple methods are given here. More complex methods are discussed in Section 3.3.

Property 2 *In difference representation, any cyclic permutation of an OOC is an OOC.*

Note that $Z_{x,x}(l)$ changes with cyclic permutation of x. This correlation has the most compact support region if the largest τ_i is last.

Definition 2 *A reversal of an OOC is a code generated by reversing the integer sequence.*

For example, the reversal of the code {1, 3, 10, 2, 5} is {5, 2, 10, 3, 1}.

Property 3 *The reversal of an OOC is also an OOC.*

Proof. The proof follows directly from Definition 1.■

A code and its reversal, both cyclically permuted such that the last τ is the same, have the same noncircular autocorrelation function and therefore are equivalent and redundant for waveform design. The shift and reversal properties will be used to limit the search space for a complete (exhaustive) code search.

1.4 CODES FOR λ > 1

Before using properties and definitions to search for codes, we show that the search can be shortened by requiring $\lambda = 1$ without losing direct blast tolerance. Let $C = 1 - \lambda/K$ be a measure of tolerance to the direct blast. C is the fraction of the original signal not obscured by the direct blast. Also let $D = K/v$ be the duty cycle. For systems with fixed transmission length, D determines the total transmission energy. The transmission energy is determined by detection range requirements. Thus, D is considered as a given design parameter. Substituting into equation (20) yields

$$D = \frac{1 - c}{1 - \dfrac{C(1-C)}{\lambda}} \,. \tag{21}$$

For $0 < 1 - C \ll 1$ and λ a positive integer

$$1 - C \le D \le (1 - C)/C \,. \tag{22}$$

Thus C is nearly determined by D independent of λ. Hence, $\lambda = 1$ is assumed without loss of generality.

1.5 EXHAUSTIVE SEARCH

There are many methods for constructing OOC's [1, 3]. Yet, there are no fast methods that are guaranteed to find all possible codes. In this section, rules are derived for speeding up the Greedy algorithm (an exhaustive search). The objective is to minimize the search space using the definitions and properties given.

The exhaustive search program is composed of nested "loops" with τ's as the loop indices. A code test is placed inside the innermost loop. The following rules apply.

Rule 1 *Assume $\tau_1 < \tau_i$, i=2, ..., K.*

Due to the shift property, all codes that violate this assumption are cyclic permutations of codes for which it holds.

It is convenient to reference ν to its minimum value and define

$$\varDelta\nu = \nu - \nu_0 . \tag{23}$$

It is also convenient to restate (19) where $\lceil\ \rceil$ is dropped for $\lambda = 1$ as

$$n_0 = K(K-1) + 1 . \tag{24}$$

Rule 2 $\boldsymbol{\tau_1 \le \lfloor \varDelta\nu/2 \rfloor + 1}$ **.**

Proof. For $\tau_1 > 1$, $Z_{x,x}(l) = 0$ for $l = 1, ..., \tau_1 - 1$ and $l = \nu - \tau i + 1, ..., \nu - 1$. Using arguments similar to those used in proving the length property,

$$\sum_{l=1}^{\nu-1} Z_{x,x}(l) = K(K-1) \le \nu - 1 - 2(\tau_i - 1) . \tag{25}$$

Substitution from (24) and (23) yields the desired result.■

Rule 3 $\boldsymbol{\tau_1 \le \lfloor (\varDelta\nu + 1)/K + (K-1)/2 \rfloor}$ **.**

Proof. By definition $\nu = \sum_{i=1}^{K} \tau_i$. When bounds are set on τ_m (loop m), τ_j, $j = 1, ..., m - 1$ are set, but τ_j, $j = m + 1, ..., K$ are not yet determined. Therefore,

$$\tau_i \le \nu - \min\left(\sum_{i=2}^{K} \tau_i\right) \tag{26}$$

and

$$\min\left(\sum_{i=2}^{K} \tau_i\right) = \sum_{i=1}^{K-1} (\tau_1 + i) \tag{27}$$

$$= (K–1)\tau_1 + K(K–1)/2 . \tag{28}$$

Substitution yields (26).■

Rules 2 and 3 are both useful. Rule 2 is tigher for $\varDelta\nu < K - 1$, while Rule 3 is tigher for $\varDelta\nu > K - 1$.

Rule 4 *Assume* $\tau_2 \le \left\lfloor \varDelta\nu/2 - (K-2)\tau_1/2 + (K^2 + 3K - 6)/4 \right\rfloor$.

This is based on the assumption $\tau_2 + 1 \le \tau_K$ which always holds for a code or its reversal. Then

$$\nu \ge \tau_1 + \tau_2 + (\tau_2 + 1) + \sum_{i=3}^{K-1} \tau_i \tag{29}$$

and 4 follows.

Rule 5

$$\boldsymbol{\tau_j \le \varDelta\nu + 1 + [K^2 + (2j-3)K - j(j+1)]/2 - (K - j + 1)\tau_1 - 2\tau_2 - \sum_{i=2}^{j-1} \tau_i \forall j = 3, ..., K - 1} .$$

Proof. Again, the τ_i, i=1, ..., j–1 are set. Therefore,

$$\tau_j \le \nu - \sum_{i=1}^{j-1} \tau_i - \min\left(\sum_{i=j+1}^{K} \tau_i\right) . \tag{30}$$

At this point, the approximation

$$\min\left(\sum_{i=j+1}^{K}\tau_i\right) \le I_j = \sum_{i=1}^{K-j}(\tau_1 + i) \tag{31}$$

$$= (K-j)\tau_1 + (K-j)(K-j+1)/2 \tag{32}$$

is used to remove interdependence between $\min(\sum_{i=j}^{K}\tau_i)$ and τ_i, $i = 1, ..., j-1$. Rule 5 follows.■

The following bound is tighter for $j > K - 1 - \tau_2 + \tau_1$.

Rule 6 $\boldsymbol{\tau_j \le \Delta\nu + [K^2 + (2j-1)K - j(j+1)]/2 - (K-j)\tau_1 - 2\tau_2 - \sum_{i=3}^{j-1}\tau_i \forall j = 3, \ldots, K-1}$ **.**

Proof. This proof is the same as for Rule 5 except that $\tau_2 + 1$ is substituted for min τ_{K-1}.■

Rules 5 and 6 are not tight bounds for some j. To achieve that, a tight bound on the maximum τ is needed. Unfortunately, a provable tight bound has been elusive. Following is the tightest known bound.

Rule 7 $\boldsymbol{\tau_{\max} = \max_K \le \Delta\nu + [K(K-1)]/2}$ **.**

Proof. If a code is shifted so that the largest τ is shifted to the Kth position, the code has $\nu - \tau_{max}$ trailing zeros and an equal number of shifts for which the noncircular autocorrelation may be nonzero. Clearly,

$$\nu - \tau_{\max} \ge \sum_{l=1}^{\nu} W_{x,x}(l) \tag{33}$$

$$\sum_{l=1}^{\nu} W_{x,x}(l) = \sum_{i=1}^{K-1} i \tag{34}$$

$$= K(K-1)/2\,. \tag{35}$$

Substituting from (23) and (24) yields the desired result.■

Though potentially dangerous, fitting a polynomial through the values of τ_{max} from Table 2 gives the following conjecture which is tight.

Conjecture 2 $\tau_{max} \le \left\lfloor (K^2 + K + 6)/6 \right\rfloor$.

This conjecture is not used in the code search, but is, rather, a product of that search.

Finally, τ_K is determined by the previous τ's.

Rule 8 $\tau_K = \nu - \sum_{l=1}^{K-1}\tau_i$.

Besides limits on the loops, conditions (if statements) can be placed between nested loops to implement some conditions of Definition 1. The easiest condition to test is

Rule 9 $\tau_i \neq \tau_j \forall i \neq j$.

These rules greatly reduce the search space. The result is a hybrid between the "Greedy" and "Accelerated Greedy" methods in [1]. This algorithm is capable of searching for minimal and non-minimal length codes. It is an exhaustive search in that it finds a complete code set. It has been used to find codes with weights as large as $K = 8$.

The search for $K = 8$ took 11 hours. The algorithm was implemented in Matlab and run on an Apollo DN3500 workstation. There were 1373 codes that passed the conditions mentioned above and were evaluated using the full test of Definition 1.

1.6 DIFFERENCE SETS AND MULTIPLIERS

Though exhaustive search techniques are guaranteed to find all possible codes, there are faster, possibly less complete code search methods. Before introducing them, the positional OOC representation must be defined. This representation uses a set of integers to denote the position of the pulses in the train. For example, the positional representation of the code in Figure 3 is {0,4,5,7}. The positional representation plus the length of the code is equivalent to the differential representation.

Let the general positional representation be $\{p_i \mid i = 1, ..., K\}$. Then the position property can be stated in a more general form as

Property 4 *The code* $\{p'_i = P_{i+j \bmod \nu} | i = 1, ..., K\}$ *for an arbitrary integer j as a shift of* $\{p_i\}$.

Property 4 is more general than Property 2 because it includes shifts that do not change the interchip spacing. On the other hand, since the interchip spacing is not changed, the noncircular autocorrelation is not changed and these codes are irrelevant.

Let the symbol $\equiv$ be used to denote modulo congruence. For a set Y, let $|Y|$ denote the number of members in the set. Also let $a + X$ for a scalar a and set X be defined as $\{a + p \mid p \in X\}$. Then the autocorrelation property of an OOC can also be stated for the positional representation set X as

$$|(a + X) \bigcap (b + X)| \leq \lambda \tag{36}$$

for $a \neq b \bmod \nu$.

We can consider that a and b shift the sequence. Equality holds in (36) if the code has minimal length. Minimal length codes can be related to the mathematical concept of difference sets.

A difference set is defined as a set X such that any integer $c \neq 0$ can be represented as $p_i - p_j$, with $p_i, p_j \in X$ in exactly λ ways. (Again the p's are the positional representation of the code.) To show that all minimal length codes are based on difference sets, set $c = a - b$ for a and b as defined in Property 5.

There is a faster method of searching for minimal length OOC's based on difference sets and the theory of "multipliers" [4, 5].

Definition 3 *Let (t, ν) – 1 where (,) means the greatest common factor and let s be an arbitrary integer. Then an integer t is a multiplier of the (ν, K, λ) difference set D =* $\{p_1, p_2, ..., p_K\}$ *if there exists an integer s such that E =* $\{tp_1, tp_2, ..., tp_K\}$ *and* $\acute{E} = \{p_1 + s, p_2 + 2, ..., pK + 2\}$ *are the same K-subset of X.*

Addition and multiplication are assumed to be modulo ν unless otherwise stated. If the elements of the positional representation are multiplied by an integer, t, and t does not divide ν, the result is a possibly shifted and/or reversed version of the original code or a new code in the sense of the noncircular autocorrelation. For example, multiplying the code {0, 1, 3, 9} by 2 modulo 13 yields {0, 2, 6, 5}. Subtracting 5 modulo 13 and rearranging elements yields {0, 1, 8, 10} which is a new code with a different noncircular autocorrelation function.

A rigorous statement of this property is based on the following theorem.

Theorem 1 *The congruence $a \equiv n \bmod m$ has a solution if and only if (a, m) | n where z|y indicated x divides evenly into y.*

The set of all $a < m$ such that $(a, m) = 1$ is called the reduced residual system of m. There are $\phi(m)$ elements in the system where $\phi(\bullet)$ is Euler's function.

The following property is a corollary of Theorem 1.

Property 6 *In positional representation, the product of an OOC and any element of the reduced residual system of ν is an OOC.*

Proof. Let $D = \{p_1, p_2, ..., p_K\}$ be an OOC and let t be an element of the reduced residual system of ν. Also let $E = \{tp_1, tp_2, ..., tp_K\}$. Then E is an OOC if and only if $t(p_i - p_j) = n$ for λ different i, j pairs and for all $1 \le n \le \nu - 1$. The most restrictive case is $n = 1$. This case has a solution if and only if $(t(p_i - p_j), \nu) = 1$. But $(t(p_i - p_j), \nu) = 1$ is equivalent to $(p_i - p_j, \nu) = 1$ and $(t, \nu) = 1$. Since $p_i - p_j$ is arbitrary, the earlier condition is always satisfied. Therefore $(t, \nu) = 1$ is necessary and sufficient to guarantee the existence of a solution. The property follows. ■

Multiplication by some elements of the reduced residual system generates redundant codes.

Theorem 2 *Elements t and $\nu - t$ of the reduced residual system produce mutually reversed codes.*

Proof. The numbers, $\nu - t$ and $-t$ are congruent modulu ν. Therefore multiplication by $\nu - t$ modulo ν is congruently equivalent to multiplication by $-t$. Furthermore, multiplication by $-t$ is equivalent of multiplying sequentially by -1 and t. The order is not important. Multiplying by -1 reverses the positional order. ■

Clearly, in the search for OOC's, only multiplying by the integers 2 through $(\nu-1)/2$ need be considered. Some of these integers are multipliers and produce shifted versions of the same code. An interesting question is how many multipliers are in this set of integers.

The most general form of the Multiplier Theorem is the following.

Theorem 3 *Let D be a (ν, K, λ) difference set. Let n be a divisor of $K - \lambda$ and suppose that $(n, \nu) = 1$ and $n > \lambda$. Let t be an integer such that for each prime divisor q of n there is an integer j such that $q^j \equiv t \pmod{\nu}$. Then t is a multiplier of the difference set D.*

If Conjecture 1 is true, q is unique (for each $K - \lambda$).

Let $g = g(q, \nu)$ be the smallest positive integer such that q^g 1 mod ν. Then g is called the order of $q(\bmod \nu)$[7]. Theorem 3 allows the enumeration of OOC's that are found by multiplication.

Theorem 4 *Let $\psi(K)$ be the number of weight K codes (reversals not counted) generated from an initial code by multiplication. Assume q is the only prime divisor of $K - \lambda$ and suppose that $(q, \nu) = 1$ and $q > \lambda$. Then*

$$\psi = \frac{\phi}{2g} . \qquad (37)$$

Proof. The number g is the number of multipliers for a given difference set between 1 and $\nu - 1$. If another code is generated by multiplication by t, then multiplication by tq^i, $i = 0, 1, ..., g - 1$ generates shifts of the same code. Therefore, there are g elements of the reduced residual system that generate each code.

The condition $(q, \nu) = 1$ can be further justified.

Theorem 5 *Let q be a prime divisor of $K - \lambda$. Then $(q,\lambda) = 1$ implies $(q, \nu) = 1$.*

Proof. From the length of an OOC, we know

$$K - \lambda = K^2 - \lambda\nu \tag{38}$$

$$= (K - \lambda)^2 + 2\lambda(K - \lambda) + \lambda(\lambda - \nu)\,. \tag{39}$$

The statement $q \mid K - \lambda$, implies $q \mid \lambda(\lambda - \nu)$. Since by hypothesis $(q, \lambda) = 1$, $q \mid (\lambda - \nu)$ and one concludes that $(q, \nu) = 1$. ■

For $\lambda = 1$, the condition $(q, \nu) = 1$ is always true.

The number of codes of a given weight are listed in Table 1. Caution is in order. The theory of multipliers is based on difference sets and only pertains to OOC's of minimal length. Furthermore, a code search that uses all elements of the reduced residual system is not guaranteed to find all minimal length codes. So far, no minimal length codes are known for $\lambda = 1$ that could not be found by multiplication. However, [4] gives an example for $\lambda = 6$. Upon testing the two codes in his example, one code generates two other codes, but the other only generates itself.

Table 1. The number of codes found by multiplication.

Weight	Length	q	$\phi(\nu)$	$g(q,\nu)$	Number of Codes
3	7	2	6	3	1
4	13	3	12	3	2
5	21	2	12	6	1
6	31	5	30	3	5
8	57	7	36	3	6
9	73	2	72	9	4
10	91	3	72	6	6
12	133	11	108	3	18
14	183	13	120	3	20
17	273	2	144	12	6
18	307	17	306	3	51
20	381	19	252	3	42

Generating codes by multiplication requires an initial code. That code may be found from the Greedy algorithm. A list of one code for each weight (up to 12) is given in [4, page 132] for $\lambda = 1$. With these codes as starters, Table 2 was generated using the multipliers $t = 1, ..., (\nu - 1)/2$. Reversals were removed for brevity.

Table 2. Minimum-length orthogonal optical codes.

Weight	Length	Code: Differential Representation											
3	7	1	2	4									
4	13	1	2	6	4								
		1	3	2	7								
5	21	1	3	10	2	5							
6	31	1	2	5	4	6	13						
		1	2	7	4	12	5						
		1	3	2	7	8	10						
		1	3	6	2	5	14						
		1	7	3	2	4	14						
7		Minimal length codes do not exist.											
8	57	1	2	10	19	4	7	9	5				
		1	3	5	11	2	12	17	6				
		1	3	8	2	16	7	15	5				
		1	4	2	10	18	3	11	8				
		1	4	22	7	3	6	2	12				
		1	6	12	4	21	3	2	8				
9	73	1	2	4	8	16	5	18	9	10			
		1	4	7	6	3	28	2	8	14			
		1	6	4	24	13	3	2	12	8			
		1	11	8	6	4	3	2	22	16			
10	91	1	2	6	18	22	7	5	16	4	10		
		1	3	9	11	6	8	2	5	28	18		
		1	4	2	20	8	9	23	10	3	11		
		1	4	3	10	2	9	14	16	6	26		
		1	5	4	13	3	8	7	12	2	36		
		1	6	9	11	29	4	8	2	3	18		
11		Minimal length codes do not exist.											
12	133	1	2	9	8	14	4	43	7	6	10	5	24
		1	2	12	31	25	4	9	10	7	11	16	5
		1	2	14	4	37	7	8	27	5	6	13	9
		1	2	14	12	32	19	6	5	4	18	13	7
		1	3	8	9	5	19	23	16	13	2	28	6
		1	3	12	34	21	2	8	9	5	6	7	25
		1	3	23	24	6	22	10	11	18	2	5	8
		1	4	7	3	16	2	6	17	20	9	13	35
		1	4	16	3	15	10	12	14	17	33	2	6
		1	4	19	20	27	3	6	25	7	8	2	11
		1	4	20	3	40	10	9	2	15	16	6	7
		1	5	12	21	29	11	3	16	4	22	2	7
		1	7	13	12	3	11	5	18	4	2	48	9
		1	8	10	5	7	21	4	2	11	3	26	35
		1	14	3	2	4	7	21	8	25	10	12	26
		1	14	10	20	7	6	3	2	17	4	8	41
		1	15	5	3	25	2	7	4	6	12	14	39
		1	22	14	20	5	13	8	3	4	2	10	31

1.7 NONCIRCULAR OPTICAL ORTHOGONAL CODES

Here, a class of codes is introduced that may have a more compact correlation function than OOC's, but have equal direct blast tolerance. It is defined with respect to the noncircular correlation function by

$$W_{x,x}(l) < \lambda \,, \; 1 \le l \le \nu - 1 \,. \tag{40}$$

The definition of an OOC is similar, but uses the circular correlation function. Let a code in this class be called noncircular optical orthogonal code (NOOC). A more formal definition can be based on the τ's of the differential representation.

Definition 4 *A code is an (n, K, λ) NOOC if and only if*

$$\left\{ \sum_{i=j}^{m} \tau_i \middle| 1 \le j \le m \le K \right\} \tag{41}$$

is a collection of integers with no member repeated more than λ times.

Without loss of generality, $\tau_K = 1$ can be assumed since the trailing zeros do not affect the noncircular correlation function.

The shift property does not apply for NOOC's, but a version of the reversal property holds.

Definition 5 *A reversal of an (ν, K, λ) NOOC is a code generated by reversing the first K – 1 integer sequence of the difference representation.*

For example, the reversal of the code {3, 1, 6, 2, 1} is {2, 6, 1, 3, 1}.

Property 7 *The reversal of an NOOC is an NOOC.*

Proof. The proof follows directly from Definition 4. ■

For a given weight and λ, a theoretical lower bound, ν_0, on the code length can be calculated.

Property 8 *The length of a K-weight NOOC is greater than or equal to*

$$\nu_0 = \left\lceil \frac{K(K-1)}{2\lambda} \right\rceil + 1\,. \tag{42}$$

Proof. The trivial shift yields a correlation of K. Each of the K chips aligns with every other chip for some shift. Therefore, $\sum_{l=-(\nu_0-1)}^{\nu_0-1} W_{x,x}(l) = K^2$. If only positive nontrivial shifts are considered, $\sum_{l=-(\nu_0-1)}^{\nu_0-1} W_{x,x}(l) = K(K-1)/2$. Since each nontrivial shift yields a correlation of λ or less, and there are $\nu_0 - 1$ distinct nontrivial shifts,

$$K(K-1)/2 \le \lambda(\nu_0 - 1) \tag{43}$$

and Property 8 follows from the requirement that ν_0 be an integer. ■

Property 8 is highly restrictive.

Property 9 *If λ = 1, codes which meet the theoretical minimal length do not exist for $K \ge 5$.*

Proof. In order to meet the bound, the set $\{\tau_l \mid l = 1, ..., K-1\}$ must be a permutation of the set of integers 1 through $K - 1$. Suppose $\tau j = 1$ and $2 \le j \le K-2$. Then τ_{j-1} and τ_{j+1} must be chosen such that $\tau_{j-1} + 1$ and $\tau_{j+1} + 1$ are not equal and both are greater than $K - 1$. This is a contradiction. Therefore either $\tau_1 = 1$, or $\tau_{K-1} = 1$ and the former is assumed without loss of generality due to Property 7. Then $\tau_2 = K - 1$ so that $\tau_1 + \tau_2$ does not equal any of the τ's. Similarly, $\tau_3 = 2$, but here the sequence stops. If $\tau_4 = K - 2$ then $\tau_1 + \tau_2 = \tau_3 + \tau_4$. There is no acceptable value for τ_4 unless $K = 4$ in which case $\tau_4 = 1$ and the code is finished. ■

1.8 SEARCH FOR NOOC'S

Again the search begins by asking if there is an advantage in direct blast tolerance for a given duty cycle using codes with $\lambda > 1$. An answer can only be implied. A proof would require an attainable theoretical minimum length for all λ and the weight of interest.

The code length obeys the inequality

$$\nu \geq \frac{K(K-1)}{2\lambda} + 1 \,. \tag{44}$$

Let C and D, the direct blast tolerance and duty cycle, be defined as before. Substitution into (44) yields

$$D \leq \frac{2(1-C)}{1 - \frac{(1-C}{\lambda}(2C-1)} \approx 2(1-C) \,. \tag{45}$$

Again, there appears to be no advantage for $\lambda > 1$. A comparison of (45) and (22) suggests that some NOOC's have a higher duty cycle than minimal length OOC's for the same direct blast tolerance.

All OOC's arde NOOC's, but the converse is not true. High duty cycle NOOC's can be generated either by a sequence of operations on OOC's or by the Greedy algorithm (exhaustive search). Generating NOOC's from OOC's does not always yield the minimal length codes, but it is much faster than an exhaustive search. To motivate the concept, suppose the largest τ of an OOC is shifted to the Kth position and the superfluous trailing zeros dropped. For example, the nine-weight codes {1, 4, 7, 6, 3, 28, 2, 8, 14} is shifted to {2, 8, 14, 1, 4, 7, 6, 3, 28}, and truncated to the NOOC {2, 8, 14, 1, 4, 7, 6, 3, 1}. Now let this be stated in a more general form.

Property 910 *A high duty cycle (ν', K, λ) NOOC can be generated from an (ν, K + m, λ) OOC, for an arbitrary j, by removing the m consecutive τ's, namely, τ_{j+1}, ..., $\tau_{j+m \bmod K}$, setting τ_j = 1 and shifting it to the Kth position. The OOC and j are chosen to maximize $\sum_{i=j}^{j+m} \tau_i$.*

The value of ν' depends on the OOC and the τ's removed.

There is no guarantee that minimal length NOOC's may be found from OOC's and there are no other known procedures for finding NOOC's except through exhaustive search. Therefore, the following rules are derived from the NOOC properties to minimize the search space. The structure of the search is the same as that given for OOC's, but the rules are different and estimating the minimum length is part of the search. Since the shift property does not hold, τ_1 is not necessarily the smallest τ.

Assuming $\lambda = 1$ gives the theoretical minimum length of an NOOC as

$$\nu_o = K(K-1)/2 + 1 \,. \tag{46}$$

It is convenient to express ν as

$$\nu = \nu_o + \delta\nu \,. \tag{47}$$

There is a tighter limit on τ_1 than on the other τ's.

Rule 10 *$\tau_1 \leq \delta\nu/2 + K - 2$can be assumed without loss of generality.*

Proof. This is based on the assumption $\tau_1 + 1 \leq \tau_{K-1}$. This holds for either a code or its reversal. From the definition of ν,

$$\tau_1 \leq \nu - \min\left(\sum_{i=2}^{K} \tau_i\right) \tag{48}$$

and

$$\min\left(\sum_{i=2}^{K}\tau_i\right) = \tau_K + \min\tau_{K-1} + \sum_{i=1}^{K-3} i \tag{49}$$

$$-\ 1 + (\tau_1 + 1) + (K-3)(K-2)/2 \tag{50}$$

using $\tau_K = 1$. Substituting this, (46) and (47) into (48) yields the result. ■

As for OOC's, there are two limits for the general τ_j.

Rule 11 $\boldsymbol{\tau_j \le \delta\nu + j(2K - j - 1)/2 - \sum_{i=1}^{j-1}\tau_i \forall j = 2, \ldots, K-1}$ **.**

Proof. Since τ_i, i = 1, ..., j – 1 are predetermined

$$\tau_j \le \nu - \sum_{i=1}^{j-1}\tau_i - \min\left(\sum_{i=j+1}^{K-1}\tau_i\right) - 1 \tag{51}$$

and

$$\min\left(\sum_{i=j+1}^{K-1}\tau_i\right) = \sum_{i=1}^{K-j-1} i \tag{52}$$

The results follows. ■

For $j \ge K - \tau_1 - 2$ the following bound is tighter.

Rule 12 $\boldsymbol{\tau_j \le \delta\nu - 1 + (j+1)(2K - j - 2)/2 - 2\tau_1 - \sum_{i=2}^{j-1}\tau_i \forall j = 2, \ldots, K-2}$ **.**

Proof. This proof is similar to that of Rule 11 except $\tau 2K$–1 $\ge \tau_1 + 1$ is assumed. ■

There is also a limit on the largest τ. This limit is much tighter than the limit for OOC's.

Rule 13 $\boldsymbol{\tau_{\max} = \delta\nu + K - 1}$ **.**

Proof. This rule is an extension of Rule 11 to $j = 1$. ■

Then τ_{K-1} is predetermined.

Rule 14 $\boldsymbol{\tau_{K-1} = \nu - 1 - \sum_{i=1}^{K-2}\tau_i}$ **.**

Proof. As for OOC's, conditions from Definition 4 in the form of "if" statements can be placed between loops. The simplest condition to implement is the following.

Rule 15 $\boldsymbol{\tau_i \ne \tau_j, \forall i \ne j, i,j \in [0, K-1]}$ **.**

In our algorithm, all the conditions of Definition 4 are implemented in such "if" statements and there is no need to test a code inside the inner-most loop. Table 3 was generated using this algorithm.

It gives a complete list of codes of minimal length through $K = 9$. Note that minimal length NOOC's are significantly shorter than minimal length OOC's.

Table 3. Minimum-length noncircular orthogonal optical codes.

Weight	Length	Code								
3	4	1	2	1						
4	7	1	3	2	1					
5	12	1	3	5	2	1				
		2	5	1	3	1				
6	18	1	3	6	2	5	1			
		1	3	6	5	2	1			
		1	7	3	2	4	1			
		1	7	4	2	3	1			
7	26	1	3	6	8	5	2	1		
		1	6	4	9	3	2	1		
		1	10	5	3	4	2	1		
		2	1	7	6	5	4	1		
		2	5	6	8	1	3	1		
8	35	1	3	5	6	7	10	2	1	
9	45	1	4	7	13	2	8	6	3	1

1.9 COMPARING CODES

Within the realm of OOC's and NOOC's, there are several approaches to choosing codes from Tables 2 and 3 to construct a waveform design. For the OOC's, besides the codes listed, any cyclic shift of a code is another code with different autocorrelation properties.

To determine the appropriate code weight, consider the following. Compared to a contiguous pulse, the direct blast area is reduced by a factor of $\sqrt{K}$ for bistatic sonars or a factor of K^2 for monostatic sonars. The mutual interference is reduced by a factor of K.

However, as K increases, the duty cycle diminishes by roughly a factor of $1/K$. Using Conjecture 2 to estimate τ_{max} gives a duty cycle of

$$\frac{6K}{5K^2 - 7K + 1}$$

which still falls off as $1/K$.

The largest duty cycle of a given weight is achieved with a minimum length NOOC. The code that maximizes the duty cycle also yields the most compact noncircular autocorrelation. The noncircular autocorrelation for the NOOC {1, 4, 7, 13, 2, 8, 6, 3, 1} is shown in Figure 7. Since the theoretical minimal length is not achievable, the correlation function does not have a solid pedestal. Rather the pedestal is solid in the middle and full of holes or nulls on the outsides.

Suppose the approach is to spread the autocorrelation as uniformly as possible. This corresponds to choosing the code where the largest τ in the code is the smallest. Nulls can even be placed around the main peak. A null can be created on the side of the central peak by putting the 1 last as in the ten-weight OOC {2, 6, 18, 22, 7, 5, 16, 4, 10, 1}. This noncircular autocorrelation is shown in Figure 8.

The null on each side of the central peak can be increased by selecting OOC's of greater than minimum length within the bounds of Rules 3 and 2. If the τ_1 = n (assuming τ_1 is the smallest τ), then there are $n - 1$ zeros around the central peak. If τ_1 is shifted to last, there are n zeros around the central peak. The noncircular autocorrelation of the 7-weight 49-length code {4, 5, 13, 10, 6, 8, 3} has three zeros on each side of the central peak as shown in Figure 9.

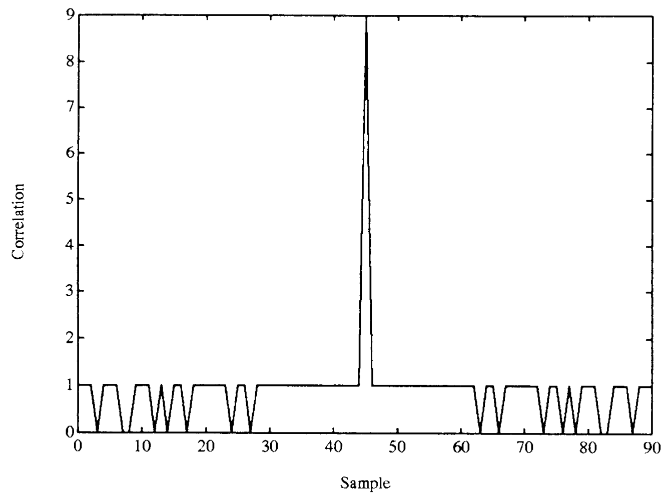

Figure 7. NOOC {1, 4, 7, 13, 2, 8, 6, 3, 1} with the most compact noncircular autocorrelation.

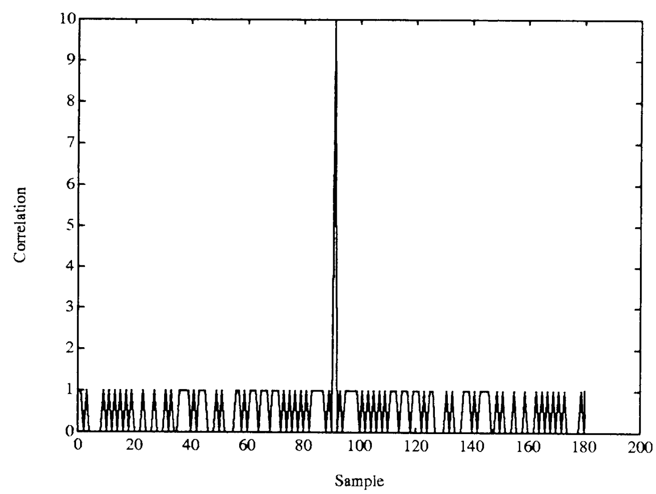

Figure 8. The most spread noncircular autocorrelation, Code {2, 6, 18, 22, 7, 5, 16, 4, 10, 1}.

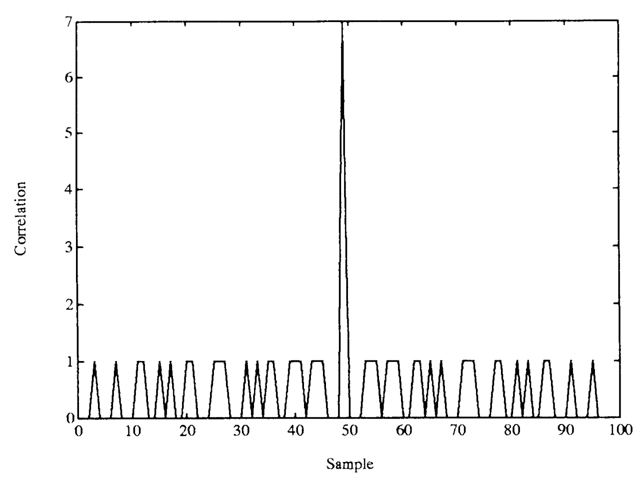

Figure 9. Noncircular autocorrelation of code {4, 5, 13, 10, 6, 8, 3} with three zeroz on each side of the central peak.

In yet another approach, codes are chosen that have good post detection pulse compression properties. This is important because OOC's and NOOC's can be long enough to overresolve targets in Doppler. Combinations of coherent and incoherent summing across chips are used to achieve a reasonable Doppler resolution. The OOC {4, 8, 2, 3, 17, 1, 6, 8, 11, 29} can be divided into possibly overlapping groups having comparable lengths (and therefore comparable Doppler resolution). For instance, chips can be combined (coherently processed) in groups of three or four. One such grouping is chips 1, 2, 3, 4; 4, 5, 6; 6, 7, 8; 8, 9, 10. This yields a maximum and minimum integration time of 22 and 15 chips, respectively. In this grouping the chips are overlapped. Grouping the pulses (especially with overlap) reduces the improvements in direct blast and mutual interference tolerance. Another grouping into sets of two is chips 1 and 3, 2 and 4, 5 and 6, 7 and 9, 8 and 10. This gives a maximum and minimum integration time of 21 and 11 chips, respectively.

1.10 CONCLUSIONS

This concludes our discussion of codes. Two nonstandard waveform types composed of disjoined chips were introduced to significantly reduce mutual interference and the effects of the direct blast. Orthogonal Optical Codes (OOC's) were previously introduced in the literature, but Non-circular Orthogonal Optical Codes (NOOC's) are new.

Properties of both codes and methods of generating them have been discussed. Since NOOC's are new, their properties are not fully known. In particular, an attainable minimum code length is not known. An exhaustive list of minimum length codes was given assuming minimal cross correlation ($\lambda = 1$).

Criteria for determining the best code for a given application have been discussed. None of these arguments are irrefutably conclusive. Therefore, a full set of codes are given as a pallet from which to construct future waveforms.

1.11 REFERENCES

1. Chung, F. R. K. and J. A. Salehi, "Optical Orthogonal Codes: Design, Analysis, and Applications," *IEEE Transactions on Information Theory*, vol. 35, no. 3, May 1989.

2. Salehi, J. A., "Code Division Multiple-Access Techniques in Optical Fiber Networks—Part I: Fundamental Principles," *IEEE Transactions on Communications*, vol. 37, no. 8, August 1989.

3. Chung, H. and P. V. Kumar, "Optical Orthogonal Codes–New Bounds and an Optimal Construction," *IEEE Transactions on Information Theory*, vol. 36, no. 4, July 1990.

4. Ryser, H. J., *Combinatorial Mathematics*, Wiley and Sons, 1963.

5. Hall, M., Jr., *Combinatorial Theory,* Blaisdell, 1967.

6. Andrews, G. E., *Number Theory,* W. B. Saunders Co., 1971.

7. Hua, L. K., *Introduction to Number Theory*, Springer-Verlag, 1982.