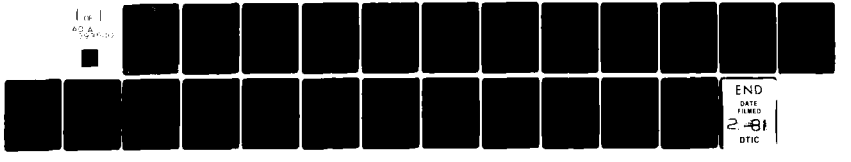
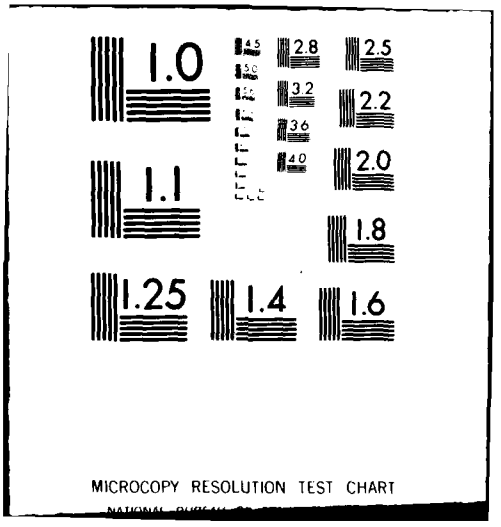
AD-A093 500 PENNSYLVANIA STATE UNIV UNIVERSITY PARK APPLIED RESE--ETC F/G 9/3
MULTICOMPONENT SIGNALS BASED UPON QUADRATIC CONGRUENCES.(U)
OCT 80 E L TITLEBAUM, L H SIBUL N00024-79-C-6043
UNCLASSIFIED ARL/PSU/TM-80-213 NL



END
DATE FILMED
2-81
DTIC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
MICROCOPY RESOLUTION TEST CHART

MULTICOMPONENT SIGNALS BASED UPON QUADRATIC CONGRUENCES

E. L. Titlebaum (University of Rochester)
L. H. Sibul

Technical Memorandum
File No. TM 80-213
October 28, 1980
Contract No. N00024-79-C-6043

Copy No. 18

The Pennsylvania State University
Intercollege Research Programs and Facilities
APPLIED RESEARCH LABORATORY
Post Office Box 30
State College, PA 16801

NAVY DEPARTMENT

NAVAL SEA SYSTEMS COMMAND

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

(14) 1. REPORT NUMBER: ARL/PSU/TM-80-213

2. GOVT ACCESSION NO.: AD-A 350

3. RECIPIENT'S CATALOG NUMBER:

4. TITLE (and Subtitle): MULTICOMPONENT SIGNALS BASED UPON QUADRATIC CONGRUENCES

(9) 5. TYPE OF REPORT & PERIOD COVERED: Final

6. PERFORMING ORG. REPORT NUMBER:

(1) 7. AUTHOR(s): E. L. Titlebaum (University of Rochester)
L. H. Sibul

(15) 8. CONTRACT OR GRANT NUMBER(s): N00024-79-C-6043

9. PERFORMING ORGANIZATION NAME AND ADDRESS:
Applied Research Laboratory
P. O. Box 30
State College, PA. 16801

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS:

(11) 11. CONTROLLING OFFICE NAME AND ADDRESS:
NAVAL SEA SYSTEMS COMMAND (SEA 63R1)
DEPARTMENT OF THE NAVY
WASHINGTON, DC 20360

12. REPORT DATE: October 1980

13. NUMBER OF PAGES: 20 (12) 24

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office):

15. SECURITY CLASS. (of this report): UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE:

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release. Distribution Unlimited.

Per NAVSEA - December 9, 1980

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
S/N, multicomponent, signals, quadratic, congruences

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

High efficiency, multicomponent signals for maximization of signal-to-noise ratio are investigated. Maximization of signal-to-noise ratio in colored noise requires control of volume distribution of the signal ambiguity function and transmission of unity efficiency signals. Signal efficiency is defined as the ratio of average power to the peak power. It is concluded that the signals must be frequency hop pulse trains. Quadratic congruences are chosen to place the components in time-frequency space. The number

()ver)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

391027

(20) Abstract (Continued)

theoretic properties of these signals provide bound on the position and amplitude of the various peaks of the signal ambiguity function. The trade-offs are shown between volume removal, number of component signals, and the time-bandwidth product.

Subject: Multicomponent Signals Based Upon Quadratic Congruences

References: See Page 18.

ABSTRACT

High efficiency, multicomponent signals for maximization of signal-to-noise ratio are investigated. Maximization of signal-to-noise ratio in colored noise requires control of volume distribution of the signal ambiguity function and transmission of unity efficiency signals. Signal efficiency is defined as the ratio of average power to the peak power. It is concluded that the signals must be frequency hop pulse trains. Quadratic congruences are chosen to place the components in time-frequency space. The number theoretic properties of these signals provide bound on the position and amplitude of the various peaks of the signal ambiguity function. The trade-offs are shown between volume removal, number of component signals, and the time-bandwidth product.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

The problem we are addressing in this report is how we can design signals which have small volume contributions near the origin and in a strip parallel to the time axis of the ambiguity function. Because of the difficulties of direct synthesis of signals from the signal ambiguity function, the usual approach is to select an interesting set of realizable waveforms and investigate the properties of the selected set of waveforms. Here we investigate signals which are composed of several components of the form

$$u(t) = \sum_{K=1}^{N} u_K(t). \tag{1}$$

The rationale is that if we can choose a set $u_K(t)$ whose crossambiguity functions appear in regions of no interest, then this will have the effect of maximizing the signal-to-interference ratio because we minimize the overlap of total ambiguity volume and clutter scattering function.[1] The scattering function of interest is a strip parallel to the time axis.

All practical transmitters operate under peak power constraints. In order that we can transmit the maximum possible amount of energy in available transmission time, we must design signals which have the maximum average power for fixed peak power. In the next section, we define the concept of signal efficiency which will be used to rule out certain classes of multicomponent signals from consideration. The problem here is that although we gain clear regions in the ambiguity plane, we must reduce average power (i.e., signal energy) and, hence, little improvement is realized in the signal to interference ratio when one is partially noise limited.

Finally, we will discuss a set of signals which have 100% efficiency and which can be used to move the ambiguity volume out of the strip of interest. These are the quadratic congruential codes. The quadratic congruential codes are based on ideas that have been used in development

of linear congruential codes.[2] We will use the number theoretic properties of congruences[3] to establish bounds on the ambiguity function in all regions of the time-frequency plane. The results show that as we increase the available time-bandwidth product, we can move more ambiguity volume outside the interference strip and, hence, increase the signal to interference ratio. Bounds on the volume and height distributions of the ambiguity function have been established by Price and Hofstetter.[4] What we have developed in this paper are easily generatable, unity efficiency codes that move the signal ambiguity-function volume away from the strip parallel to the time axis of the ambiguity function (i.e., we eliminate the effects of sources of interference in frequency band around desired frequency). This concept has application to clutter rejection and spread spectrum communication.[5,6]

II. EFFICIENCY

The design of the energy efficient codes has been addressed by Schroeder[7] and Ackroyd.[8,9] We define the signal efficiency as

$$E_f = P_{ave}/P_{peak} \times 100\% \tag{2}$$

for a signal

$$u(t) \neq 0; \quad 0 \leq t \leq T.$$

Thus, we consider time limited signals. We have that

$$P_{ave} = \frac{1}{T} \int_0^T |u(t)|^2 dt \tag{3}$$

and

$$P_{peak} = \max_t |u(t)|^2 = M^2 . \tag{4}$$

We assume the signal, u(t), is energy normalized. Thus,

$$E_u = \int_0^T |u(t)|^2 dt = 1.$$

Hence,

$$P_{ave} = 1/T$$

and

$$E_f = (1/TM^2)\ 100\% . \tag{5}$$

We now consider two classes of signals.

(a) Single FM Signal

These are signals that have only one frequency component at one time. They may have many frequency components but these components must appear in different time slots. We may characterize these signals with a rectangular envelope as

$$u(t) = \frac{1}{\sqrt{T}} e^{j\theta(t)}, \quad 0 \leq t \leq T. \tag{6}$$

Thus, $M = \frac{1}{\sqrt{T}}$ and the efficiency is

$$E_{ff} = \frac{1}{T\left(\frac{1}{\sqrt{T}}\right)^2} \times 100 = \underline{\underline{100\%}} .$$

(b) Multiple FM Signals

At first consideration, these signals appear to have many desirable properties. They do not have the pedestal behavior that many of the single FM signals possess, such as SQFM and VCHIRP. They have reduced volume in the strip since each FM component can be designed so that their crossambiguity functions appear outside the strip of interest. However, they have a diminished efficiency. Consider

$$u(t) = \sum_{K=1}^{N} a_K e^{j\theta_K(t)}, \quad 0 \leq t \leq T. \tag{7}$$

If we assume for simplicity that the signal is energy normalized, each component of the signal has the same energy, and the frequency components are far removed from one another then

$$E_u = NTa^2 = 1$$

and

$$a = 1/\sqrt{NT} \ . \tag{8}$$

Hence, the maximum value for the signal is at most

$$M = Na = \sqrt{N/T} \ . \tag{9}$$

This occurs when all cosines go through their peak value at the same time. Thus, we have

$$E_{ff} = \frac{1}{T} \times \frac{1}{N/T} \times 100 = \frac{100}{N}\% \tag{10}$$

so that we reduce efficiency inversely and the number of components we have in the signal.

Computer results have shown that for N = 2, with two CHIRP signals spaced apart, we do indeed see a reduced volume in the strip by a factor of about 2. However, since we must reduce signal energy by about the same factor, virtually no gain in SNR is achieved under noise limited conditions. Thus, to prevent possible loss in SIR, the efficiency of signal must be 100%.

III. MULTICOMPONENT-DISJOINT TIME SIGNALS

It is clear from the previous discussion that any multiple component signal we consider must also have a 100% efficiency. Thus, we conclude that the component must be disjoint in both time and frequency in order to achieve this end.

In this section we shall show that, if the components are widely spaced in time and frequency, we can move the volume away from the origin and we will discuss how much of the volume is involved. In the next section, we present a new class of signal which provides our greatest hope of achieving maximum SIR.

We first consider two components and then generalize the results to N signal. Exact placement of the components in time-frequency space will be discussed in the next section.

For two components, we have

$$v(t) = u_1(t) + u_2(t). \tag{11}$$

The ambiguity function is

$$\begin{aligned} A_{vv} &= Au_1 + u_2,\ u_1 + u_2 \\ &= Au_1u_1 + Au_1u_2 + Au_2u_1 + Au_2u_2. \end{aligned} \tag{12}$$

Taking the magnitude squared, we have

$$|A_{vv}|^2 = |(Au_1u_1 + Au_2u_2) + (Au_1u_2 + Au_2u_1)|^2$$

$$= \underbrace{|Au_1u_1 + Au_2u_2|^2}_{A} + \underbrace{|Au_1u_2 + Au_2u_1|^2}_{B}$$

$$+ \underbrace{2\mathrm{Re}\left\{ (Au_1u_1 + Au_2u_2)(Au_1u_2 + Au_2u_1)^* \right\}}_{C}. \qquad (13)$$

We discuss the various terms in Equation (13) labelled A, B and C.

First, we observe that since the signals are widely spaced, the peaks in the cross term and the auto term appear in totally different regions of the time-frequency plane. Hence, C is very small and can be ignored. By the same argument, B can be shown to be

$$B = |Au_1u_2|^2 + |Au_2u_1|^2.$$

Thus, the total is

$$|A_{vv}|^2 = |Au_1u_1 + Au_2u_2|^2 + |Au_1u_2|^2 + |Au_2u_1|^2. \qquad (14)$$

Also, we know that

$$\int_{-\infty}^{\infty}\int |Au_1u_2(\tau,\phi)|^2 d\tau d\phi = Eu_1Eu_2. \qquad (15)$$

Suppose for simplicity that each component has the same energy. Thus,

$$Eu_1 = Eu_2 = 1/2 \text{ and } E_v = 1.$$

Since the total volume is unity and the volume under each cross term in (14) is 1/4, we have moved half of the volume away from the main lobe and placed it at the peak of the two cross terms.

Consider now an N-component signal.

$$v(t) = \sum_{K=1}^{N} u_K(t) \tag{16}$$

Each component will have $Eu_K = 1/N$. By the same argument, we have that

$$|A_{vv}|^2 \cong |Au_1u_1 + \ldots + Au_Nu_N|^2$$

$$+ \sum_{\substack{j,K=1 \\ K \neq j}}^{N} |Au_ju_K|^2, \tag{17}$$

the second term of which has N^2-N terms.

Since the signals are assumed widely separated and if the cross terms do not overlap, we have that the second term has volume.

$$V_{sec} = (N^2-N)\left(\frac{1}{N^2}\right) = 1 - 1/N \tag{18}$$

and, hence, we have moved all but 1/N of the volume away from the origin. The difficulty here is that if the volume is still in the strip or if the cross terms overlap, we have lost much of the gain for our present application. For example, the cross terms may themselves pile up considerable volume although away from the main lobe, yet in the strip. In the next section, we will discuss a placement in T-W space which assures that these problems do not occur. We shall use a guard-band in frequency to account for the problem of zero-time cross terms.

IV. QUADRATIC CONGRUENCE PLACEMENT

In this section, we discuss a method of placing the signal components in time-frequency space which assures that we will have the maximum SIR with 100% efficiency. The notion of efficiency requires that we consider essentially pulse-train like signals, each of which possesses a different spectral component.

The fundamental notion that we require is as follows: the degree to which two signal components correlate with one another, if they occupy the same time slot, is determined by their proximity in frequency. If they occupy the same spectral location, they will maximally correlate. As they separate, their correlation decreases inversely as the frequency difference between them.

This concept was used to develop a set of codes which have mutually small crosscorrelation properties for all shifts in time and frequency axis.[2] These are the linear congruence codes. The difficulty here is that we are not interested in a set of codes but only one placement. Further, the autocorrelation properties of these codes were such that significant side lobe could appear within the strip of interest (i.e., for zero Doppler).

We shall first require that a guard-band be placed between the top of a low component and the bottom of the next component up. This assures that for the present application we have minimum strip volume. We call this guard-band G Hz. Each component will be separated by at least G Hz from all others. Now we call the spectral centroid of each component f_K, so that the set $\{f_K\}$ is what we must choose in order to define the signal. The individual components themselves may be chosen to suit the desired behavior at and around the main lobe; whereas, the set $\{f_K\}$ determines how large and where are the side lobes of the signal. Since most of the volume (see Equation 18) occurs in the side lobes, this is the cricial choice.

We shall first demonstrate a poor choice of centroid set. Suppose we take, as our set, a linearly increasing frequency $f_K = f_0 + K\Delta f$

$K = 0,\ldots,N-1$. This is shown in Figure 1 for $N = 5$.

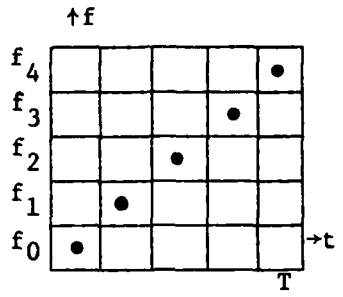


Figure 1. Linear Congruential Code for $N = 5$.

There are two problems with such a signal. First, if we shift the signal one slot horizontally and one slot vertically, then 4 dots overlap one another. Similarly, if we shift two slots in both directions, then 3 dots overlap. This accounts for the ridge behavior that CHIRP signals possess in their ambiguity functions. Secondly, if we shift horizontally one slot, then all but one of the dots are the same distance apart. This accounts for the poor side lobe structure that CHIRP signals have in their auto-correlation function.

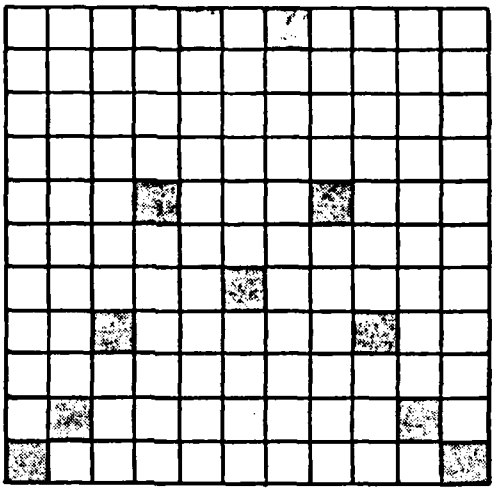
What we desire is a signal that has no more than one overlap for every shift and a nonconstant difference for horizontal shifts. To this end, we now consider a quadratic of the form.

$$y_{K+1} = [y_K + (K+1)]\text{Mod}(N),$$

$$0 \leq K \leq N-1 \tag{19}$$

In what follows, we shall assume that N is the prime number. We also assume that y_0 is zero. However, the actual frequency will be f_0, the lowest spectral centroid. Figures 2 and 3 show several examples of the arrays generated for several values of N. Two of these are prime; whereas, the third is not. Notice the symmetry with respect to the center for all of these arrays. This may first appear to preclude the use of these sets. However, we get around this by only using the first (or second) half of the arrays.

N = 11



N = 13

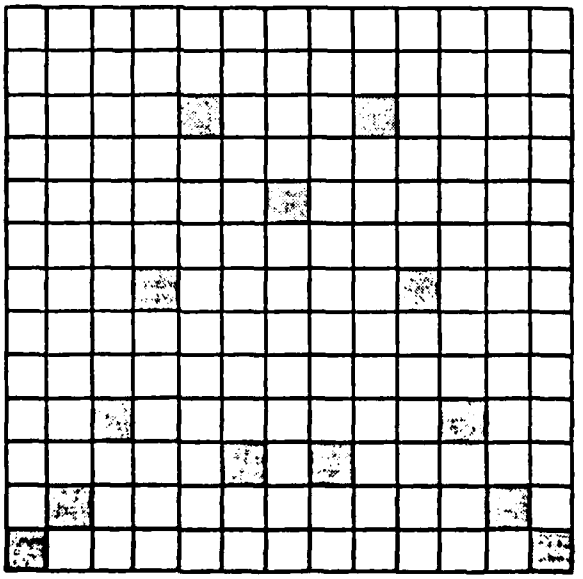


Figure 2. Quadratic Congruential Codes for N = 11 and N = 13.

We shall now present the properties of the quadratic congruences defined in Equation (19), leaving the proofs for the Appendix. We will then apply these results to establish the results for the ambiguity function.

prop. 1) $$y(K) = \left[\frac{K(K+1)}{2}\right] \text{Mod}(N) \qquad 0 \leq K \leq N-1$$

prop. 2) Symmetry: for any N, odd

$$y(N-K-1) = [y(K)] \text{ Mod}(N) \qquad 0 \leq K \leq N-1$$

prop. 3) Horizontal Shift:

$$y(K+m) = [y(K) + Km + y(m)] \text{ Mod}(N) \qquad 0 \leq K,m \leq N-1$$

prop. 4) Difference with Horizontal and Vertical Shift:

$$Z(K,m,\ell) \triangleq y(K+m) - y(K) + \ell$$

$$= [y(m) + Km + \ell] \text{Mod}(N) \qquad 0 \leq K,m,\ell \leq N-1$$

Property one establishes a closed form for generating the arrays without the recursive formula. It shows why we call these quadratic congruences. The formula is quadratic in K. Property two is the symmetry property we observed previously. Property four is the main result. We observe that for any (m,ℓ) with $m \neq 0$, the difference, 2, is a linear congruence. Thus, for N prime the differences must go through a complete residue sequence, Mod N. Thus, we know the minimum distance (in frequency) for the entire time-frequency plane. For the $m = 0$ case, all the shifts are ℓ units apart. This is another reason for the guard-band. The property for horizontal shifts of the CHIRP-like signals switches axes and now is valid for strict Doppler shifts with no time shift.

Since the differences go through a complete residue class, there can be only one intersection of the two frequency patterns. If we were extending the patterns (Mod N), there would be exactly one crossing. Note that for horizontal shifts this always occurs on the opposite side from the center (see Figures 2 and 3), as long as N is a prime number.

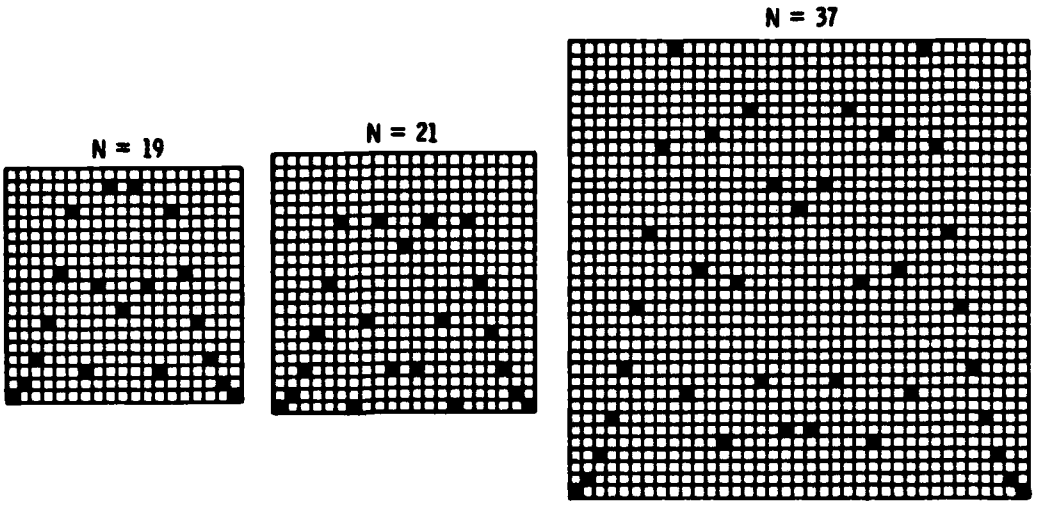


Figure 3. Quadratic Congruential Codes for N = 19 (Prime), N = 21 (Non-Prime) and N = 37 (Prime).

V. BOUNDS ON THE AMBIGUITY FUNCTION

We have established the number theoretic properties for the set of frequency differences. In light of these results and the results for linear congruences, we can place upper bounds on the height of the ambiguity function for the quadratic congruence signals.

Let us assume that the component signals are themselves cosines at the frequencies $\{f_K\}$ and that the total bandwidth is F (= NG). The actual components may be SQFM, CHIRPS or anything else for that matter. The choice of signals only affects the main lobe behavior and the shape of the non main lobes, but not their position and amplitude.

Under this assumption, we observe that two frequencies, f_m and f_n, which overlap for T_1 seconds have maximum crosscorrelation

$$C_{mn} = \begin{cases} N/\pi T_1 |m-n| F, & m \neq n \\ 1/N, & m = n \end{cases} \tag{20}$$

We are also assuming that each element of the set $\{f_K\}$ is one of the frequencies

$$\{f_0 + KG \; ; \; 0 \leq K \leq N-1\}.$$

We are simply assuming that the components are the same distance apart.

Property four shows that for the region away from the zero time slot, the frequency difference goes through a complete residue class. Thus, we may bound the height of the ambiguity function with A_1 where

$$A_1 = \frac{1}{N} + \frac{4N}{\pi FT}\left[1 + \ell n\left(\frac{N-1}{2}\right)\right] \tag{21}$$

This result is proven in the linear congruence coding paper.[2] In the zero time slot, where the frequency differences are all the same, we

bound the ambiguity function with A_2 where

$$A_2 = \frac{2N^2}{\pi FT} \tag{22}$$

Note that A_2 is somewhat higher than A_1 since an N^2 appears in the numerator. The 1/N term in A_1 comes from the fact that there will be exactly one overlap (Mod N); for the nonperiodic case there will be at most one overlap. In the light of property two, if we were to only use the first half of the frequencies, we can drop this term and bound the zero Doppler strip which includes the autocorrelation function by

$$A_1(1/2) = \frac{4N}{\pi FT}\left[1 + \ell n\left(\frac{N-1}{2}\right)\right] \tag{23}$$

This result is valid away from the main lobe ($m \neq 0$).

Now we can see the trade-offs between removed volume, number of slots, and time-bandwidth product. Thus, as we push more volume outside this strip by increasing N, then we must increase FT in order to lower the amplitude of the ambiguity function. Thus, we have established the trade-offs between strip volume and peak amplitudes. The peaks away from the main lobe and off the zero Doppler and zero-time strips are governed by A_1 which has an additional 1/N term in the bound. Thus, these peaks will be slightly higher (depending upon N). Finally, the worst case occurs in the zero time slot (where the removed volume is going), indicating the amplitude is increasing as N^2.

VI. CONCLUSIONS AND FURTHER WORK

In this report, we have established the concept of efficiency and shown that multicomponent signals can be used in clutter limited conditions only if the components occur in disjoint time slots. We have defined a new class of signals which provides a mechanism for removing volume from a strip about the zero Doppler axis and also placing bounds on the actual heights of the ambiguity function. The trade-offs between volume removed and ambiguity amplitude have been established for this class as well.

What remains is to choose the size of the guard-band and the various component signals. The guard-band is chosen by the strip size we wish to clear. This is determined by clutter data. The component signals are chosen to improve main lobe behavior of the ambiguity function of the multicomponent signal.

We are presently investigating the role of the component signals and the shapes of the ambiguity functions for various component signal choices.

VII. ACKNOWLEDGMENTS

This work has been supported by Dr. E. G. Liszka, NAVSEA Code 63R-1, and Dr. C. L. Ackerman, Laboratory Block Principal. Interchange of ideas with Dr. Dennis W. Ricker and Mr. John R. Sacha have contributed to the development of basic concepts of this paper.

REFERENCES

(1) H. L. Van Trees, Detection, Estimation, and Modulation Theory, Part III, New York, NY: John Wiley, 1971, ch. 13, pp. 444-537.

(2) E. L. Titlebaum, "Time-Frequency Hop Coding Based Upon the Theory of Linear Congruences." To be published.

(3) H. Griffen, Elementary Theory of Numbers, New York, NY, McGraw-Hill, 1954.

(4) R. Price and E. M. Hofstetter, "Bounds on the Volume and Height Distributions of the Ambiguity Functions," IEEE Trans. Inform. Theory, Vol. IT-11, pp. 207-214, April 1965.

(5) L. H. Sibul and E. L. Titlebaum, "Signal Design for Detection of Targets in Clutter," Accepted for publication in Proc. IEEE.

(6) R. F. Ormondroyd and M. S. Shipton, "The Feasibility of Using Spread-Spectrum Communication Systems for the Land Mobile Service on a Noninterference Basis with Other Users," The Radio and Electronic Engineer, Vol. 50, pp. 407-418, August 1980.

(7) M. R. Schroeder, "Synthesis of Low-Peak-Factor Signals and Binary Sequences with Low Autocorrelation," IEEE Trans. Information Theory, Vol. IT-16, pp. 85-89, January 1970.

(8) M. H. Ackroyd, "The Design of Huffman Sequences," IEEE Trans. Aerospace and Electronic Systems, Vol. AES-6, pp. 790-796, November 1970.

(9) M. H. Ackroyd, "Synthesis of Efficient Huffman Sequences," IEEE Trans. Aerospace and Electronic Systems, Vol. AES-8, pp. 2-8, January 1972.

October 28, 1980
ELT:LHS:cac

APPENDIX

Quadratic Congruences

(1) We define $y(K)$ by

$$y(K+1) = [y(K) + (K+1)] \text{ Mod } N$$

$$y(0) = 0, \quad 0 \leq K \leq N \quad 1, \quad N \text{ prime}$$

*use ≡ as "is congruent to, Mod N"

(2) T. $y(K) \equiv \left[\frac{K(K+1)}{2}\right]$ is a solution to (1)

P. Consider $y(K+1) \equiv \left[\frac{(K+1)(K+2)}{2}\right]$

$$\equiv \left[\frac{K(K+1)}{2}\right] + \cancel{2}\,\frac{(K+1)}{\cancel{2}} \quad \text{Q.E.D.}$$

(3) T. For N odd $y(K) \equiv y(N-1-K)$ (symmetry about center point)

P. $y(N-1-K) \equiv \left[\frac{(N-1-K)(N-1-K+1)}{2}\right]$

$$\equiv \left[\frac{(N-1-K)(N-K)}{2}\right]$$

expanding $$\equiv \left[\frac{N(N-1)}{2} - \frac{(2N+1)}{2} + \frac{K^2}{2}\right]$$

$$\equiv \left[\underset{A}{\frac{N(N-1)}{2}} - \underset{B}{NK} + \underset{C}{\frac{K(K-1)}{2}}\right]$$

However, $A \equiv 0$, $B \equiv 0$. Thus, since $C \equiv y(K)$
$y(N-1-K) \equiv y(K)$

(4) Translation in K

T. $y(K+m) \equiv y(K) + Km + y(m)$

P. $$y(K+m) \equiv \frac{(K+m)(K+m+1)}{2} \equiv \left[\frac{K(K+1+m)}{2} + \frac{m(K+m+1)}{2}\right]$$

$$\equiv \left[\frac{K(K+1)}{2} + \frac{Km}{2} + \frac{m(m+1)}{2} + \frac{Km}{2}\right]$$

$$\equiv \left[\frac{K(K+1)}{2} + Km + \frac{m(m+1)}{2}\right] \text{ Q.E.D.}$$

(5) Corr. Add $\ell - y(K)$ to both sides

$$Z(K,m,\ell) \triangleq y(K+m) + \ell - y(K) \equiv y(m) + Km + \ell$$

Thus, for fixed translations (m,ℓ), $m \neq 0$, $Z(K,m,\ell)$ is a <u>linear congruence in K</u>. Hence, Z goes through a complete residue sequence as $0 \leq K \leq N-1$. For $m = 0$, $Z(K,\ell) \equiv \ell$.

Distribution List -- TM 80-213

NAVSEA, Dr. E. G. Liszka, SEA 63R1, Copy No. 1
NAVSEA, Mr. D. C. Houser, SEA 63R14, Copy No. 2
NAVSEA, Mr. C. D. Smith, SEA 63R, Copy No. 3
NAVSEA, Mr. J. P. Jenkins, SEA 63X42, Copy No. 4
NAVSEA, Capt. R. M. Wellborn, PMS 406, Copy No. 5
NAVSEA, Mr. J. D. Antinucci, PMS 406B, Copy No. 6
NAVSEA, Mr. T. E. Douglas, PMS 406E1, Copy No. 7
NAVSEA, Code SEA-9961, Library, Copies No. 8 and 9
NCSC, Dr. David Skinner, Code 790, Copy No. 10
OUSDR&D/Naval Warfare, Dr. E. J. McKinney, Copy No. 11
NUSC/NPT, Dr. J. R. Short, Code 363, Copy No. 12
ARL/UT, Mr. J. Willman, Copy No. 13
Marine Physical Laboratory, Dr. W. S. Hodgkiss, Copy No. 14
University of Rochester, Dr. E. L. Titlebaum, Copy No. 15
University of Rochester, Dr. S. Shapiro, Copy No. 16
ORINCOM Corp., 3366 N.Torrey Pines Ct., Suite 320, La Jolla, CA 92037,
Dr. R. A. Altes, Copy No. 17
DTIC, Copies No. 18 through 29