Motivation

1) Multiple Access Spread Spectrum and Cellular Communications Systems:
   Require a family of codes which have ideal auto-ambiguity functions and mutually small cross-ambiguity functions.

2) Multiuser Sonar and Radar Systems:
   Here the focus is on reduction of mutual interference for the individual signals. Virtually the same requirements as above.

3) Channel/Target Measurements
   Choosing pairs of signals which have small sidelobe interaction for the twin processor.

Signal Set Conditions

1) $\chi_{u_i u_i} (\tau, \omega) \equiv 0, \ (\tau, \omega) \neq (0,0), \ \forall \ i$

2) $\chi_{u_i u_j} (\tau, \omega) \equiv 0, \ \forall \ (\tau, \omega), \ i \neq j$
Multiple Access Spread Spectrum CDMA Communications

**Multiple Access System:**
- A large number of users communicate with a receiver simultaneously.
- Each user has access to the entire available bandwidth.

**Requirements:**
- Once the signal is received there must be no ambiguity about the sender and the message it transmits.
- The received signals must have minimum mutual interference.
- Each transmission must occupy as much of the available bandwidth as possible (spread spectrum requirement).
- Transmissions may be either synchronous or asynchronous.
How do two FM waveforms Crosscorrelate?

We have two analytic energy normalized waveforms

\[ f(t) = a(t)e^{j\alpha(t)}, \quad g(t) = b(t)e^{j\beta(t)} \]

We define the *instantaneous frequencies* for these signals as

\[ \omega_f(t) = \frac{d \alpha(t)}{dt} \quad \text{and} \quad \omega_g(t) = \frac{d \beta(t)}{dt} \]

Now draw two time-frequency plane *templates*.

Result for **one** intersection (hit):

\[ R_{fg}(\tau) \sim \sqrt{\text{Area}}, \quad BT \to \infty \]
Multiple Hit Case

We have two analytic energy normalized waveforms with two hits, then we get the complex addition of the two areas.

*In the regions of more than one intersection there is an oscillation between the sum and difference of the areas.
The Signals

A rectangular pulse of length $T$ seconds divided into $N$ equal segments of length $T/N$ seconds:

In which we place one of the (radian) frequencies

$$\omega_k = \omega_0 + y(k)\frac{B}{N}, \quad 1 \leq k \leq N$$

where

- $\omega_0$ = initial frequency
- $B$ = approximate radian bandwidth of signal
- $y(k)$ = placement operator

Thus the 'analytic' normalized waveform is

$$u(t) = \frac{1}{\sqrt{T}} \sum_{k=1}^{N} p(t - kT/N) e^{j(\omega_k t + \theta_k)}$$

with

$$p(t) = \begin{cases} 
1, & 0 \leq t \leq T/N \\
0, & \text{elsewhere}
\end{cases}$$
The Frequency Difference Function and the Associated Hit Matrices

Since correlations occur whenever two signals have the same frequency at the same time we define the **frequency difference function** for two signals \( u_1(t) \) and \( u_2(t) \) with placement operators \( y_1(k) \) and \( y_2(k) \) respectively as

\[
y_1 \Delta y_2(k,t,w; \text{ parameters}) = y_1(k + t) + w - y_2(t)
\]

where \( 1 \leq k \leq N, \) and \( -(N - 1) \leq t,w \leq N - 1 \)

The **hit matrix** for the signal pair is defined as the two dimensional array of the **number of roots** of the frequency difference function plotted as a function of \( (t,w) \). The array is square and of size \( 2N - 1 \).
Types of Frequency Hop Waveforms

a) **Costas Arrays** - These are full codes which have "ideal" autoambiguity functions.

b) **Congruence Codes** - Placement operator is a polynomial over the finite field GF(p), where p is an odd prime number.

\[ y(k) = \left[ a_N k^N + a_{N-1} k^{N-1} + \ldots + a_1 k + a_0 \right] \mod p \]

The codes are named according to N. Thus

N = 1: **Linear Congruence Codes (LC)**

N = 2: **Quadratic Congruence Codes (QC)**

N = 3: **Cubic Congruence Codes (CC)**

\[ \ldots \]

N = p-2: **Hyperbolic Congruence Codes (HC)**

c) **Mersereau-Seay Codes** - A cross between Costas arrays and QC codes, based on Reed-Solomon methods.
Some Number Theory

D. Two integers \( b \) and \( c \) are congruent mod \( p \) if \( b - c \) is divisible by \( p \) which is not zero.

D. We write \( (b \equiv c \mod p) \) and \( c \) is called a residue of \( b \mod p \). The set of all numbers \( c \) which satisfy this is called a residue class.

D. The numbers \( \{c_0, c_1, \ldots, c_{p-1}\} \) form a complete residue system mod \( p \) if for every \( b \) there is one and only one \( c_i \) such that

\[
    b \equiv c_i \mod p
\]

D. The numbers \( \{c_0, c_1, \ldots, c_{p-1}\} \) form a minimally complete residue system mod \( p \) if each of the \( c_i \) have the smallest magnitude.

Example with \( p = 5 \).

a) 1, 6, -4, -9, 11 are in the same residue class (for 1).

b) \{10, 6, 7, 3, -1\} and \{0, 1, 2, 3, 4\} are complete residue systems mod 5.

c) \{-2, -1, 0, 1, 2\} is the minimally complete residue system mod 5.
T. If $p$ is a prime number then set of numbers $J_p$ with 

$$J_p = \{0, 1, 2, \ldots, p-1\}$$

form a **finite field**, with **addition** and **multiplication** performed **mod** $p$.

**Consequence of being a field:** Almost everything you think is true is true!

T. The set of numbers $J_p \setminus \{0\}$ is a **group**.

  e.g. $\{1, 2, 3, 4\}$ for $p = 5$.

D. A **primitive root** of a prime $p$ is any number $R$ in the group that generates the group as powers of $R$.

Example: 2 is a primitive root of 5 since 

$$\{2, 4, 8, 16 \ mod \ 5\} = \{2, 4, 3, 1\}$$

T. A polynomial congruence over the prime $p$ of degree $N$ has at most $N$ incongruent solutions. (It can have less!).

*Thus a linear congruence has at most one root, a quadratic congruence has at most two roots, etc.
The Codes and their Properties

a) **Costas Arrays** - These are full codes have which have 'ideal' autoambiguity functions. They have at most one hit for any time and/or frequency shift of the code with respect to itself.

Simplest way to generate a Costas Array is to use the group generated by any primitive root of the prime $p$.

(L. Welch). \{R^k \mod p: 1 \leq k \leq p - 1\}.

**Example:** $p = 19$:

**Cross Properties.** At most two code words can be found which have two hits, for all Doppler. These are obtained using reciprocal roots. e.g. $p = 19$, use $R = 2$ and 10.

**W. Chang** (NUWC;NL) proved that you can have 1 hit with a limited Doppler for a pair of codes.
Time-Frequency Hop Codes

1 -- Welch-Costas Arrays
2 -- Tempel-Costas Arrays
3 -- Linear Congruences
4 -- Quadratic Congruences
5 -- Cubic Congruences
6 -- Quintic Congruences
7 -- Hyperbolic Congruences

Enter your choice --> 1
Welch starting index --> 3

- Welch -- \( N = 7 \) ------
\( (N = 7, R = 3, A = 1) \)
\[ 3 \ 2 \ 6 \ 4 \ 5 \ 1 \]

tickpos := t * tickincrement
else
tickpos := tickincrement;
if adjustlabels and (n > 5) then
begin
Hit Matrix for Welch-Costas Array
\[ y(k) = \{3, 2, 6, 4, 5, 1\} \]

<table>
<thead>
<tr>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shift</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>-1</td>
</tr>
<tr>
<td>-2</td>
</tr>
<tr>
<td>-3</td>
</tr>
<tr>
<td>-4</td>
</tr>
<tr>
<td>-5</td>
</tr>
</tbody>
</table>

Time Lag

Magnitude

Digital Frequency

Time Lag
b) Congruence Codes

1) Linear Congruence Codes.

These are the straight lines in the field and are the generalizations to the finite field of Chirp or LFM signals.

\[ y(k) = (ak + b) \mod p, \quad 0 \leq k \leq p - 1, \quad N = p \]

where \( a \) is a family index so that \( 1 \leq a \leq p - 1 \) and \( b \) can be any constant in the field.

Hit Properties:

The frequency difference function between two code words is

\[ y_1 \Delta y_2 (k; \tau, d) = [a_1 (k + \tau) + b_1 + d - a_2 k - b_2] \]

AutoHit Properties: \( a_1 = a_2, \ b_1 = b_2 \) The set of frequency differences are not a function of \( k \) and thus are constant for fixed \( \tau \).

CrossHit Properties: \( a_1 \neq a_2 \) The frequency difference function is itself a linear congruence. Thus two linear congruence codes in \( k \) have have \textbf{at most one hit} in their CAF. These are the best possible codes.
4 -- Quadratic Congruences
5 -- Cubic Congruences
6 -- Quintic Congruences
7 -- Hyperbolic Congruences

Enter your choice --> 3

This program will calculate, & display the N-th Congruence codes for a prime number, N.
Choose a starting prime by selecting the corresponding index below.
After each code hit Return to continue or q and then hit Return to quit or r and a Return to restart.

1--> 3 10--> 31 18--> 67
2--> 5 11--> 37 19--> 71
3--> 7 12--> 41 20--> 73
4--> 11 13--> 43 21--> 79
5--> 13 14--> 47 22--> 83
6--> 17 15--> 53 23--> 89
7--> 19 16--> 59 24--> 97
8--> 23 17--> 61 25--> 101
9--> 29

Linear starting index --> 7

- Linear -- N = 19 ---------------
  \( N=19, A = 1 \)
  0 1 2 3 4 5 6 7 8 9
  10 11 12 13 14 15 16 17 18

  \( N=19, A = 2 \)
  0 2 4 6 8 10 12 14 16 18
  1 3 5 7 9 11 13 15 17
2) **Quadratic Congruence Codes.**

These are the vertical parabolas in the field. They are generated using the general quadratic placement operator

\[ y(k) = [ak^2 + bk + c] \mod p \]

The frequency difference function for two such codes is

\[ y_1 \Delta y_2(k; \tau, d) = \begin{pmatrix} a_1(k+\tau)^2 + b_1(k+\tau) + c_1 + d \\ -a_2k^2 + b_2k + c_2 \end{pmatrix} \]

**AutoHit Properties:** \( a_1 = a_2, \ b_1 = b_2, \ c_1 = c_2 \). Since the quadratic terms in \( k \) cancel we are left with a linear congruence in \( k \) and, thus, a QC code has **at most one hit** in its AAF.

**CrossHit Properties:** \( a_1 \neq a_2 \) The frequency difference function is itself a quadratic congruence. Thus two quadratic congruence codes in \( k \) have have **at most two hits** in their CAF.

*These are the same properties as the Costas Arrays except there are entire families of such codes.*
**Difficulty**: The QC codes are **not full** codes and in fact only have \( (p+1)/2 \) of the available frequencies. Because of this they also have hits on the delay axis which is not the case for full codes. (See examples).

In general a quadratic congruence will have \( (p-1)/2 \) frequencies hit twice, \( (p-1)/2 \) missing frequencies and one frequency with just one value. Thus the QC codes are always about half full.
Enter your choice --> 4

This program will calculate & display the N-th Congruence codes for a prime number, N. Choose a starting prime by selecting the corresponding index below. After each code hit Return to continue or q and then hit Return to quit or r and a Return to restart.

1--> 3  10--> 31  18--> 67
2--> 5  11--> 37  19--> 71
3--> 7  12--> 41  20--> 73
4--> 11  13--> 43  21--> 79
5--> 13  14--> 47  22--> 83
6--> 17  15--> 53  23--> 89
7--> 19  16--> 59  24--> 97
8--> 23  17--> 61  25--> 101
9--> 29

Quad starting index --> 7

Quad -- N = 19

(N =19, R = 1)

0 1 3 6 10 15 2 9 17 7
17 9 2 15 10 6 3 1 0
3) **Cubic Congruence Codes.**

These are the generalizations of cubic functions to the finite field. Their placement operator is

\[ y(k) = \left[ a(k + b)^3 + c \right] \mod p \]

where \( a \) is the family index and \( b \) and \( c \) are arbitrary.

*note that they are not a general cubic.

T. (Maric) The Cubic Congruence Codes are full for primes satisfying the condition that \( p = 3m + 2 \). (about 50% of the primes).

**AutoHit Properties:** \( a_1 = a_2, \) etc. Since the cubic terms in \( k \) cancel we are left with a quadratic congruence in \( k \) and, thus, a QC code has **at most two hits** in its AAF.

**CrossHit Properties:** \( a_1 \neq a_2. \) The frequency difference function is itself a cubic congruence. Thus two cubic congruence codes in \( k \) have have **at most three hits** in their CAF.
The Ambiguity Function Bound

a) Linear Congruence Crossambiguity, Quadratic Congruence Autoambiguity and Costas Array Autoambiguity bound

In both of these cases the set of frequency differences is a complete residue system. The ambiguity functions are determined by the set of frequency differences below.

If $s_k(t)$ is the $k$'th subpulse with correlation

$$C_{kl}(\tau) = \int_{-\infty}^{\infty} s_k(t + \tau)s^*_l(t)dt$$

It can be shown that

$$|C_{kl}(\tau)| = \begin{cases} \frac{1}{N} - \frac{|\tau|}{T} & , \ k = 1 \\ \frac{2N}{BT|y_k - y_l|} & , \ k \neq 1 \end{cases}$$
Design Tradeoffs

The Ambiguity Bound

\[ A_A(N) = \frac{1}{N} + \frac{8N}{BT} \left( 1 + \ln M \right) \]

becomes, for large BT product

\[ A_A(N) = \frac{1}{N} , \quad \text{as } BT \to \infty \]

However if we constrain the BT product then we have a minimum in the curve. \( A_A(N) \) can be differentiated and we can solve for BT yielding

\[ (BT)_{opt} = 8N^2 \left( 1 + \frac{N}{2M} + \ln M \right) \]

and substituting back into the bound yields

\[ A_A(N)_{min} = \frac{1}{N} \left( 1 + \frac{1 + \ln M}{1 + \frac{N}{2M} + \ln M} \right) \]

which goes to zero as \( 2/N \) as \( N \to \infty \).
Ambiguity Function Bound

$$A_A(N) = \frac{1}{N} + \frac{8N}{BT}(1 + \ln M)$$

where \hspace{1em} M = \left\lfloor \frac{N - 1}{2} \right\rfloor

Plot of \(A_A(N)\) vs \(N\) for a family of \(BT\) values
Nyquist Choice of BT Product

Costas as well as others require that

\[ BT = 2\pi N^2 \]

yields

\[ A_A(N) = \frac{1}{N} + \frac{4}{\pi N}(1 + \ln M) \]

which asymptotically is

\[ A_A(N) = \frac{4}{\pi N} \ln N, \quad N \to \infty \]

and generates peaks larger than \( 2/N \).
Multiple Hit Ambiguity Bounds

In any situation which has \( q \) hits the bound may be calculated to be

\[
A(N) = \frac{q}{N} + \frac{8qN}{BT} \left[ 1 + \ln \left( 1 + \frac{N+1}{2q} \right) \right]
\]

which again has a minimum at \((BT)_{opt}\) and which becomes asymptotically

\[
A(N) = \frac{2q}{N}, \quad N \to \infty
\]

For QC Cross- and CC Auto-ambiguity Functions \( q = 2 \).
For CC Crossambiguity Functions \( q = 3 \)
Welch-Costas Array \( y(k) = \{3,2,6,4,5,1\} \)
Welch-Costas Array $y(k) = (3, 2, 6, 4, 5, 1)$
4) Hyperbolic Congruence Codes.

These are the generalizations of hyperbolic functions to the finite field. Their placement operator is given by

\[ y(k) = \frac{a}{k} \mod p, \quad 1 \leq a, k \leq N = p - 1 \]

where \( a \) is the family index.

T. (Maric) The Hyperbolic Congruence Codes are full codes.

\[ y_1 \Delta y_2 (k, t, w; a) = \frac{a_1}{k + t} + w + \frac{a_2}{k} \]

**AutoHit Properties:** \( a_1 = a_2 \), etc. The denominator in the frequency difference function is never zero and the numerator is a quadratic congruence in \( k \) and, thus, has **at most two hits** in its AAF.

**CrossHit Properties:** \( a_1 \neq a_2 \). The numerator of the frequency difference function is also a quadratic congruence. Thus two hyperbolic congruence codes in \( k \) have have **at most two hits** in their CAF.
Example: \( p = 11 \) thus \( N = 10 \) (code length), \( a = 1 \) and 3

\[
\begin{array}{c|c|c|c|c|c|c|c|c|c|c|}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
\hline
1 & & & & & & & & & \\
2 & & & & & & & & & \\
3 & & & & & & & & & \\
4 & & & & & & & & & \\
5 & & & & & & & & & \\
6 & & & & & & & & & \\
7 & & & & & & & & & \\
8 & & & & & & & & & \\
9 & & & & & & & & & \\
10 & & & & & & & & & \\
\end{array}
\]

\[
\begin{array}{c|c|c|c|c|c|c|c|c|c|c|}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
\hline
1 & & & & & & & & & \\
2 & & & & & & & & & \\
3 & & & & & & & & & \\
4 & & & & & & & & & \\
5 & & & & & & & & & \\
6 & & & & & & & & & \\
7 & & & & & & & & & \\
8 & & & & & & & & & \\
9 & & & & & & & & & \\
10 & & & & & & & & & \\
\end{array}
\]

\( a = 1 \) \hspace{1cm} \( a = 3 \)
Figure 2 Auto-hit arrays of the codes shown in figure 3.6.1.
Figure 3 Cross-hit array of the codes shown in figure 3.6.1.

The auto- and cross-ambiguity functions of the codes are shown in figures 3.6.4 and 3.6.5.
Old Method for Scattering Function Estimation:

We again assume the all of the Target and Channel models are of the form

\[ y(t) = \sum_{k=1}^{N} a_k u(t - \tau_k) e^{j\omega_k t} \]

In which \{a_k\} represent the various amplitudes, \{\tau_k\} are the time delays and \{\omega_k\} are the Doppler shifts.

They are assumed to be random variables. The signal \( u(t) \) is the transmitted signal.

The received signal in the presence of noise is then

\[ r(t) = y(t) + n(t) \]

The usual method (Ziomek, Van Trees, etc) then is to pose a detection problem using the following receiver structure:
where $\mathcal{I}$ is then compared to a threshold to detect the presence or absence of the model. The noise is assumed to be white Gaussian noise with PSD

$$S_n(\omega) = N_0, \quad \forall \omega$$

In order to evaluate this test we extract $E[I]$ which evaluates to

$$E[I] = \int_{-\infty}^{\infty} S(t, \sigma) \left| \chi_{uu}(\tau - t, \omega - \sigma) \right|^2 dt d\sigma + N_0$$

If we are attempting to measure $S(t, \sigma)$ then we must find a signal $u(t)$ whose autoambiguity function is an "ideal thumbtack" or delta function.

**Result:** An autoambiguity function must have both a peak and a pedestal.

*The pedestal usually causes the sidelobes in the AAF.*
We assume that the two received signals are of the form

\[ r_1(t) = y_1(t) + n_1(t) \]

and

\[ r_2(t) = y_2(t) + n_2(t) \]

with the two model outputs being given by

\[ y_k(t) = \sum_{i=1}^{N} a_i u_k (t - \tau_i) e^{j \omega t}, \quad k = 1, 2 \]

and we have two different signals \( u_1(t) \) and \( u_2(t) \).

We are assuming that the two noise components are statistically independent and the channel and/or target have the same model for the two different looks provided by the two signals.
New Method for Scattering Function Estimation

In order to remove the pedestal from consideration we want to determine a new method which does not involve the magnitude squared of an autoambiguity function and thus is not tied to a detection problem.

We consider the following receiver structure which is based upon the possibility of obtaining two looks at the object, either target or channel.
In order to evaluate this new method we form $E[l_1 l_2^*]$ and since the noise components are independent we obtain

$$E[l_1 l_2^*] = \int_{-\infty}^{\infty} S(t,\sigma) \chi_{11}^*(t - \tau,\sigma - \omega) \chi_{22}(t - \tau,\sigma - \omega) dt d\sigma$$

Observations:

1) There is no noise term in this expression.

2) The signals ambiguity functions appear as products of two auto-ambiguity functions for the two signals.

3) If we can find a pair of signals which have the property that the product of their auto ambiguity functions is a single spike, we can measure $S(t,\sigma)$. 
Hit Array Approach to Finding Signal Pairs:
Suppose we have two LFM signals in the form of two Linear Congruence Codes for $N = 5$, one of which has slope 1 and the other has slope -1. Then the two codes are shown below.

$$u_1 = \{5, 4, 3, 2, 1\} \text{ and } u_2 = \{1, 2, 3, 4, 5\}$$

Thus and "up chirp" and a "down chirp" should have close to the desired property.
Considerations:

1) The volume under an auto-ambiguity function is always 1.0. This the **Radar Uncertainty Principle**.

The volume under the product is \( \leq 1.0 \). Consider the integral of the product

\[
\frac{1}{2\pi} \int_{-\infty}^{\infty} \chi_{11}(\tau,\omega) \chi_{22}^*(\tau,\omega) d\tau d\omega = \left| (u_1, u_2) \right|^2
\]

which can be any value in the interval \([0, 1.0]\).

2) If the volume under the central spike is small then in the presence of noise we might suffer degradation.

3) Quadrature modulation techniques can be used if there is no doppler in the problem, since a Doppler shift will destroy carrier synchronization. There are circumstances in which this is valid.
Twin Processor Implementation

\[ r(t) = u(t) + n(t) \]

\[
\begin{array}{c}
\text{MF for } u_1 \\
u_1^*(T-t) \quad \text{Delay} \\
L_1 \\
A = L_1^* L_2^* \\
2 \text{Re} \{ \} \\
\Sigma \\
\end{array}
\]

\[
\begin{array}{c}
\text{MF for } u_2 \\
u_2^*(T-t) \quad (\cdot)^* \\
L_2^* \\
\end{array}
\]

Matched Filter for \( u(t) \)

\[ u^*(2T - t) = u_1^*(2T - t) + u_2^*(T - t) \]

If \( \chi_{u_1 u_2}(\tau, \omega) \equiv 0, \quad \forall (\tau, \omega) \) then

\[ \hat{L} = \left| L_1 \right|^2 + 2 \text{Re} \{ L_1 L_2^* \} + \left| L_2 \right|^2 = L \]
Discrete Target/Channel Model Simulation:

In this experiment we construct a three reflector target or multipath model and simulate the matched filter output slices. The result is the convolution of the model with the signal ambiguity function.

We keep this target configuration constant while we vary the following:

1) transmitted signal
2) processing configuration
3) noise level (later)

General Form:

\[ y(t) = \sum_{k=1}^{N} a_k u(t - \tau_k) e^{j\omega_k t} \]

In which \( \{a_k\} \) represent the various amplitudes, \( \{\tau_k\} \) are the time delays and \( \{\omega_k\} \) are the doppler shifts.
Simulation Data

The data for the pictures are as follows:

Signal:

\[ N = 400 \text{ samples}, \  \pm (\omega_2 - \omega_1) = \pm 1.0, \]

thus \( TW = 400 \) radians.

Welch - Costas array, Primitive root = 2

Targets:

In the picture the targets are always at

\[ (\tau, \omega) = (0, 0), (50, -25), (100, 0) \]

Doppler slices = \( 2 \ (60) + 1 = 121 \)

Note: To limit picture to one page the first 150 points removed.
Ambiguity page

\[ N = 10, B \times T = 400.00 \]

Code - 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 Root - 2 Mult. - 1 - Welch Costas (n-p-1)
N = 10, BxT = 400.00
Code = 7, 5, 2, 3, 10, 4, 6, 9, 8, 1 Root = 7 Mult. = 1 - Welch Costas (n-p-1)
N = 10, BxT = 400.00
Code = 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 Root = 2 Mult. = 1 - Wallen COSTAS