Digital Waveform Codings For Ocean Acoustic Telemetry

Hyuck M. Kwon, Member, IEEE, and Theodore G. Birdsall, Member, IEEE

(Invited Paper)

Abstract—M-sequence waveform coding with a single long codeword has been considered as the basis for long-range underwater acoustic telemetry, for one user. An m-sequence is a periodic, binary, linear-law maximal-length sequence. If the span of the law in n, the maximal length \( L = 2^n - 1 \). For a given law, a single m-sequence transmits a maximum of \( \log_2(L) \) bits of source information per channel word. To increase the number of bits per word, families of m-sequences and Gold codes are considered, and compared to a single m-sequence. A hypothetical idealized multipath channel with added white Gaussian noise is assumed. Coding using families of m-sequences is recommended because it requires a smaller bit-energy-to-noise ratio than other waveform codes to achieve an equivalent codeword error probability.

I. INTRODUCTION

The telemetry system being developed for the Ocean Acoustic Tomography Program has several unique constraints that differentiate it from most digital communication systems [1]-[3]. The total energy used is important, because the tomography transmitters are buoys powered by batteries. The telemetry is designed for distances of 1-5 Mm, with multipath propagation. Offsetting the severe transmitter and propagation limitations is the uncommonly low data requirement (of the order of hundreds of bits) and the rather long time available to transmit this data (tens of minutes). The high energy necessary for reliable telemetry can be achieved with long symbol durations if the channel can be operated as a coherent channel. Long symbol (or codeword) duration with a low signal-to-noise power ratio, (i.e., long word times (long coherent integration)), and high signal-to-noise (SNR) energy ratio per word, fits well with the recent practice of Ocean Acoustic Tomography experiments [2], [3] and has been used as a cornerstone of the telemetry system. Long multipath spread times of several seconds might be combated by long convolutional codes. The method used in Ocean Acoustic Tomography is to use a sequence period at least as long as the multipath spread, transmit many periods, and segment the processing into nonoverlapping intervals during which the reception on all paths is due to the same codeword. Three concepts are intertwined here: The first is that the multipath spread will cause intersymbol interference unless the transmission is so long, compared to the spread, that the receiver can snip out the offending codeword overlap so that the remaining reception has no intersymbol overlap. The second is that the codeword rate is so low that the transmission consists of many periods of the same sequence. Together, these mean that the signal energy lost by snipping out the overlap is a minor fraction of the total energy, and that coherent addition of the retained periods increases the received signal-to-noise ratio proportional to the number of periods added. The third concept is that decoding performance depends on the signal energy-to-noise spectral density ratio, not the signal-to-noise power ratio, so that periodic transmissions with coherent addition permit the use of low-cost low-power transmitters when abundant integration time is available.

The single period of reception considered in the analysis that follows is the coherent sum of many sequence periods of reception, snipped so that the reception is due to a single codeword. In previous experiments [2], [3] single m-sequences (one periodic, binary, maximal length, linear, sequence) were used. However, the number of bits that can be transmitted per word (or sequence or channel symbol) is \( \log_2 L \). To increase the number of bits per word, more words (symbols) must be added to the system. We therefore seek a large set of possible words; i.e., waveforms. The goal of this paper is to compare three sets of waveform codings: Single m-sequence waveform coding, m-sequence family waveform coding, and Gold-sequence family coding.

Long-range underwater communication channels below 1 kHz are inadequately modeled by an ideal, additive white Gaussian noise channel. Our analysis will use the classical, added white Gaussian noise (AWGN) channel model for the usual reasons: "Gaussian" so that the mathematical descriptions concentrate on first- and second-order statistics, "added" to reflect applications where the noise is not signal induced, and "white" because that is worse than "whitenable" and because we will use independent noise samples to focus on signal features instead of noise features. The propagation model, four equal strength well-separated paths, will be equally simple in order to focus on signal types. Though this hypothetical channel model is not practical, performance comparisons of the three sets of waveform codings may give some useful guidance in the selection of the best waveform coding. Single m-sequence waveform coding is described in Section II, m-sequence family waveform coding in Section III, and Gold-sequence family waveform coding in Section IV. Section V concludes the paper.

II. SINGLE M-SEQUENCE WAVEFORM CODING

We analyze the signals based on a baseband sequence-controlled modulating waveform \( s(t) \) over one period \( L \):

\[
s(t) = \sum_{k=0}^{L-1} g(k) p(t - kT) \quad (1)
\]

where \( g(k) \)'s are real numbers, \( \pm 1 \) representations of a 0, 1 m-sequence, \( p(t) \) is a baseband pulse (or chip) waveform with duration \( T_c \), and \( L \) is the period of the sequence. A simplified block diagram of the single m-sequence code system is shown in Fig. 1. The encoder is a simple shift register generator; each block of \( n \) source information bits is the initial contents of the
shift register. If the \( n \)-bit source word is not all zeros, then the generator output will be the \( m \)-sequence. A zero initial content causes an all-zero output. When the initial bits are \( 00 \cdots 0 \), the output \( m \)-sequence is called "the impulse response of the shift register generator," denoted by \( s(t) \). The generated sequence is always periodic, with period \( L = 2^n - 1 \), and starts with the given initially loaded \( n \) bits. Unless the initial condition is all-zero, the generated sequence is a cyclic shift \( JT_1 \) of the impulse response of the shift register; the generated sequence is \( s(t) - JT_1 \). There are \( 2^n - 1 \) possible shifts (or nonzero codewords). For example, consider the shift register generator with number of stages \( n \) equal to 3 in Fig. 1, and suppose an initial storage of 100. Then the succeeding states in the shift register generator are \( 100, 110, 111, 011, 101, 010, 001, \ldots \), repeated over and over. Usually, we regard the output as coming from the last stage of the register. Then the output sequence is 001101, and is periodic. The biphase sequence bits \( g(k) \) in (1) are then \(-1 - 111 - 11\). This is a maximal length sequence and the shift register generator contains all triples, except the all zero triple.

The multipath channel impulse response \( m(t) \) is modeled as
\[
m(t) = \sum_{k=0}^{P-1} c_k \delta(t - \tau_k T_c) \tag{2}\]
where \( c_k \)'s are the attenuation coefficients (which is, in general, a complex number, but in this paper it is assumed to be 1), \( \tau_k \)'s are considered to be integers for simplicity, \( P \) is the number of multipath, and \( \delta(t) \) is the Dirac delta function. The delays are not multiples of the chip duration \( T_c \), of course. However, in this study we choose example multipaths for which the delays are multiples of \( T_c \), because we presumed this to be a "worst case" and it is obviously a simplified analysis.

The signal component of the received signal \( r(t) \) is \( s(t) - JT_1 \) convolved with \( m(t) \). As the noise is assumed to be white and Gaussian, the optimum receiver is a matched filter, matched to \( s(t) - JT_1 \) convolved with \( m(t) \). This receiver can be realized as two filters in series, one matched to \( s(t) \), the other to \( m(t) \). Finite-interval matched filtering is also called inner-product cross correlation and is denoted here by \( \langle u(t), v(t) \rangle \):
\[
\langle u(t), v(t + lT_c) \rangle = K_1 \int_0^{T-lT_c} u^*(t)v(t + lT_c) dt
= K_2 \sum_{k=1}^{L} u^*(kT_c)v((k + l)T_c) \tag{3}\]
where \( u^*(kT_c) \) is the complex conjugate of \( u(kT_c) \). The \( K \) constants are usually irrelevant, since the ultimate purpose is to determine the index \( l \) that corresponds to the maximum magnitude of the cross correlation. \( K_2 \) is chosen to be \( 1/L \) for what we call a sequence correlator, and 1 for what we call a multipath correlator, respectively. The receiver cross-correlation operations are linear, so we may treat the signal and noise separately. If the estimate of \( m(t) \) derived somehow (for example, by observing the first filter output \( x(t) \) in Fig. 1) is considered to be perfect, the signal part of the output of the second cross correlation \( y_s(t) \) is the Dirac delta function. The delays are \( 0, \ldots, L - 1 \), and the duration of codewords, \( L = 2^n - 1 \), is much greater than the multipath channel spread intervals.

A reasonable decision rule to find the shift index \( l \) is a peak detector across the matched-filter output values. The decoder after the peak detector has a table or algorithm relating the initial bits to the rotation \( J \). For simple computer evaluations, the transmitted signals are set to be \( \pm 1 \) pulses controlled by the generated sequence of length \( L \). The total transmitted signal energy, \( E_s = 1/T_c \int_0^{LT_c} s^*(t)s(t) dt \), is \( L \) per path because \( s(t) \) was normalized to unity power. The total received signal energy \( E_r \) over all multipaths is
\[
E_r = R_m(0) E_s = R_m(0) L. \tag{5}\]

The \( P \) path gains or attenuations are modeled as unit values, \( c_k = 1 \), for all \( k, k = 1, \ldots, P \) because all that is important is that they are the same. Then the output sample \( y(k) \) of the multipath correlator at \( \tau = kT_c \) can be written as
\[
y(k) = R_m(k - J) + n(k) \tag{6}\]
where \( n(k) \) is the noise output sample of the cross correlation with the multipath impulse response at \( \tau = kT_c \). The \( n(k) \)'s are dependent, identically distributed, Gaussian random variables.
with statistics,
\[ E[n(k)] = 0, \]
\[ \sigma_n^2 = \text{Var}[n(k)] = R_m(0) \frac{N_0}{2} \frac{1}{L} \]
where \( N_0 / 2 \) is the two-sided power spectral density of the AWGN.

The received signal-to-noise energy ratio (SNR) is expressed as
\[ \frac{E_b}{N_0} = \frac{R_m(0)}{2} \frac{1}{\sigma_n^2} \]
for each information block of \( n \) bits.

We assume that the information blocks of \( n \) source bits are equiprobable; i.e., the \( L \) codewords \( s(t - T_1), \ldots, s(t - L T_3) \) are equiprobable. This implies that the peak of \( y(t) \) will occur at a shift \( J T_r \), with a uniform probability \( 1/L \). Thus the probability of a codeword being correct is then
\[ \Pr[C] = \Pr\left[C \mid s(t - J T_r) \right] = \Pr[y(J T_r) \geq y(k T_r), \quad \text{all } k \mid s(t - J T_r)] = \int_{-\infty}^{\infty} \phi(\alpha) \prod_{k=1}^{n} \Phi\left( \alpha + \frac{R_m(0) - R_m(k T_r)}{\sigma_n} \right) d\alpha \]
where \( \phi \) and \( \Phi \) are the normal density and distribution functions, respectively. The product terms in this integral are due to the independence assumption on the multipath correlator output.

Equation (11) shows clearly that the performance depends on the peak correlation value \( R_m(0) \) and the off-peak correlation values \( R_m(k T_r) \), but not on the times \( k T_r \) at which these values occur.

A channel is defined to be a uniformly spaced multipath channel if its autocorrelation has a triangular shape. For example, if the multipath channel \( m(t) \) is \( \delta(t) + \delta(t - 2 T_r) + \delta(t - 4 T_r) + \delta(t - 6 T_r) \), then the autocorrelation \( R_m(t) \) is \( 4 \delta(t) + 3 \delta(t + 2 T_r) + 2 \delta(t + 4 T_r) + \delta(t + 6 T_r) \). A channel is defined to be a sparsely spaced multipath channel if its autocorrelation has three levels; i.e., one big spike at the origin, equal off peaks, and zero otherwise. The peak of the autocorrelation of a sparsely spaced multipath channel is “dominant” compared to the other off-peak values. If the multipath channel \( m(t) \) is \( \delta(t) + \delta(t - T_r) + \delta(t - 3 T_r) + \delta(t - 7 T_r) \), then the autocorrelation \( R_m(t) \) is \( 4 \delta(t) + \delta(t + T_r) + \delta(t + 2 T_r) + \delta(t + 4 T_r) + \delta(t + 6 T_r) + \delta(t + 7 T_r) \).

In this study, a four-path sparsely spaced multipath channel was chosen, with all paths of unit strength. Four paths were chosen for two reasons—one physical, one mathematical. The physical reason is that in deep ocean propagation paths typically arrive in sets of four, the paths differing depending on whether the rays left the source at angle above or below the horizontal and whether the rays were received at angles above or below. These four are generally of nearly equal amplitude. The mathematical reason is that four is the smallest number that has more than two interarrival times; i.e., the “simplest complicated”

---

III. M-SEQUENCE FAMILY WAVEFORM CODING

Let \( N \) denote the number of essentially different \( m \)-sequences\(^1\) which an \( n \)-stage shift-register generator can generate by all possible different feedback connections. Then we know, \( N = \phi(2^n - 1)/n \) [4], where \( \phi(L) \) is the Euler phi function; i.e., the number of positive integers less than \( L \) and relatively prime to \( L \), including 1. Since each essentially different \( m \)-sequence has \( L = 2^n - 1 \) cyclic rotations and each cyclic shift

\(^1\)“Essentially different”: means that any cyclic shift of an essentially different sequence is not the same as any cyclic shift of another essentially different sequence. It is equivalent to saying, “the sequences have different linear laws.”
can be a codeword, we can encode $\log_2 NL$ source bits at a
time. The encoder decides which essentially different $m$-se-
quencies shift register generator should be chosen, then puts $n$
bits into the chosen shift register generator as its initial condi-
tion. So the first $\log_2 N$ bits indicate the sequence index $I$, and
the next $n$ bits tell the rotation $J$. (The all-zero $n$ tuple is
excluded.)

The receiver is pictured as $N$ cross correlators; and each
calculates the cross-correlation function of the received signal
$(r(t))$ and its standard $m$-sequence $(s_i(t))$, for $i = 1, 2, \ldots, N$.

Suppose that the transmission was $s_I(t - JT_c)$, which is a
baseband sequence-controlled phase-modulated signal from the
$I$th generator with $JT_c$ rotation, and that $m(t)$ is the multipath
impulse response. Let $x_i(t)$ be the output from the $ith$ correla-
tor. Then the sample output at $t = \tau T_c$ is

$$x_i(\tau) = s_I(\tau) + n_i(\tau)$$

$$s_I(\tau) = \langle s_I(t - JT_c) \rangle = \frac{1}{L} \int_{L \tau = L T_c}^0 (s_I(t - JT_c) \otimes m(t))s_I(t - \tau T_c) \, dt$$

and

$$n_i(\tau) = \langle n_i(t) \rangle = \int_{L \tau = L T_c}^0 n_i(t) \otimes s_I(t - \tau T_c) \, dt,$$

where $x(t) \otimes y(t)$ is the convolution of $x(t)$ and $y(t)$, and
$n_i(t)$ is the input white Gaussian noise whose samples are
$N(0, N_0/2)$. Although we often think integrals and actual digital
signal-processing computers use many samples per chip, the
performance comparisons sought in this paper correctly calcu-
lated by using one sample per chip. The output noise samples
$n_i(k)$ are i.i.d. with $N(0, N_0/2L)$ when the modulation ang-
le was chosen so that the sequence rotations are orthogonal (see
Appendix A).

It is shown in Appendix B that the time average of $s_I(t)$
over the sequence length) is independent of the pair $(i, I)$. For
the correlator that is matched to the transmitted sequence, $i = I$,
the total activity of $s_I(t)$ is concentrated at multipath delays
$JT_c (J + \tau T_c) \ldots (J + \tau p_{N - 1} T_c)$. Hence the signal com-
ponent $s_I(t)$ of the matched correlator output $x_i(t)$ is the $JT_c$
shift of the multipath channel $m(t)$ multiplied by $L$ (see Fig. 3,
where $I = 1$). However, if the correlator is unmatched ($i \neq I$),
the same amount of total activity is distributed over the whole
period.

In Fig. 4 a relative frequency of the unmatched cross-correla-
tion values $s_{i}^{\parallel}(\tau)$ for Gold sequences (studied in Section IV) is
shown. The shape is similar to the familiar bell shape. This is
also true for the unmatched cross correlations $s_{i}^{\parallel}(\tau)$ for the
$m$-sequence case. Hence we model the unmatched-determin-
istic-signal component $s_{i}^{\parallel}(\tau)$ as i.i.d. Gaussian with mean zero
and variance $u$ for a simple and approximate analysis, where

$$u = \frac{1}{L} \sum_{\tau = 0}^{L - 1} \left| s_{i}^{\parallel}(\tau) \right|^2 - \left( \frac{1}{L} \sum_{\tau = 0}^{L - 1} s_{i}^{\parallel}(\tau) \right)^2. \quad (15)$$

This modeling is better as $L$ increases.
Let \( v \) denote the variance of the noise component process. Then,

\[
v = \text{Var} \left[ n_i(t) \right] = \frac{N_0}{2} \frac{1}{L}, \quad \text{any } i.
\]

(16)

Our goal is to evaluate an optimal receiver that decodes \( I \) and \( J \) jointly. As usual, we assume that the source blocks are equiprobable. This problem is patterned after an "\( M \)-alternative forced choice problem" in detection theory [5], [6]; i.e., finding which signal was sent if one signal out of \( M \) orthogonal equiprobable signals is present, with \( M = NL \). Let \( H_{ij} \) be the hypothesis that the transmitted signal is from code \( i \) with rotation \( j \), and \( H_0 \) be the noise alone hypothesis. That is,

\[
H_{1, j}: x_i(j) = \sum_{k=0}^{P-1} c_k \delta(j - J - \tau_k) + n_i(j),
\]

\[
n_i(j) \sim N(0, v), \quad j = 0, \ldots, L - 1 \tag{17}
\]

\[
H_{i, j}: x_i(j) \sim N(0, u + v), \quad i \neq 1,
\]

\[
i = 1, \ldots, N, \quad j = 0, \ldots, L - 1 \tag{18}
\]

\[
H_0: x_i(j) \sim N(0, u), \quad \text{i.i.d.},
\]

\[
i = 1, \ldots, N, \quad j = 0, \ldots, L - 1 \tag{19}
\]

A simple thing to do is, instead of trying to test the hypothesis \( H_{1,j} \) against all the rest of them, is to calculate the log likelihood ratio for every \( H_{1,j} \) versus the \( H_0 \) hypothesis, and then pick the biggest among them. The details are shown in Appendix C. The optimal decision rule is choosing a pair \((I, J)\) for which \( T(x \mid I, J) \) is the biggest among \( T(x \mid i, j) \) for all pairs \((i, j)\), \( i = 1, \ldots, N, \quad j = 0, \ldots, L - 1 \), where \( T(\ ) \) is monotone with the log likelihood ratio and is

\[
T(x \mid I, J) = \frac{1}{v} \sum_{k=0}^{P-1} c_k x_i((J + \tau_k) T_c) - \frac{1}{2} \frac{u}{u + v} \sum_{k=0}^{L-1} x_i^2(k T_c) \tag{20}
\]

where \( x \) is the total observation vector of dimension \( NL \), \( v \) is the noise variance, and \( u \) is the apparent signal cross-correlation variance.

This can be interpreted logically as choosing the decoding that has the right balance between matching the known multipath impulse response and yet has low overall output energy. The filter matched to the multipath channel \( m(t) \) in Fig. 1 seems to have disappeared in Fig. 3. The matched filter to \( m(t) \) is incorporated in the final decision box, choosing \( T(x \mid I, J) \) at which \( T(x \mid I, J) \) is maximum, through the first term of (20). A receiver equivalent to the one in Fig. 3 can be built; one filter matched to the multipath channel \( m(t) \) followed by \( N \) sequence filters \( s_i(t) \) (instead of \( N \) sequence filters and each followed by \( m(t) \)), because \( m(t) \) is common to all the sequence filters. In this paper we use the receiver of Fig. 3, because we can update the estimate of multipath channel by observing the output of the sequence correlator matched to the transmitted sequence. As mentioned earlier, the output of the correlator matched to the transmitted sequence is a time-shift version of the multipath channel.

For computer evaluation we chose the transmitted sequence as ±1 pulses, as was done in the single \( m \)-sequence waveform coding. The total received SNR is

\[
\frac{E_x}{N_0} = \frac{R_{m}(0)}{2} \frac{1}{v} \tag{21}
\]

since the transmitted signal energy is \( E_x = L \) per path, the total received signal energy is \( E_x = R_{m}(0)L \) over all multipaths, and \( v = N_0/2L \). Thus the bit energy SNR is

\[
\frac{E_b}{N_0} = \frac{1}{\log_2(NL)} \frac{E_x}{N_0} \tag{22}
\]

as each codeword carries \( \log_2 NL \) bits.

The same four-path, equal-strength sparsely spaced multipath channel as in the single \( m \)-sequence code discussion is evaluated: \( R_{m}(0) = 4 \) and \( n = 7 \). Its performance is shown in Fig. 5; three curves are shown; the upper and lower bounds are taken from [7] and the middle curve is the result of simulation.

IV. GOLD SEQUENCE FAMILY WAVEFORM CODING

Gold [8] showed that for every \( m \)-sequence of 0's and 1's, say \( a(k) \), there was another with the same period \( L \), say \( b(k) \), such that the set containing these two and the sum (modulo 2) of \( a(k) \) and all rotations of \( b(k) \) had minimum maximum cross correlation. This set has \( L + 2 = 2^n + 1 \) essentially different sequences; each sequence has \( L = 2^n - 1 \) distinct rotations, so all together the number of possible codewords is \( (L + 2)L = 2^{2n} - 1 \). We call this set of codewords a Gold sequence family.

A possible source encoder would map the source data into blocks of \( 2n \) binary digits (except for the all-zero \( 2n \)-tuple). Two simple shift register generators, one for the \( a(k) \) law and
one for the $b(k)$ law, would each be initialized with $n$ of the source encoded bits.

The following performance evaluation considers the multipath impulse response as known. The signal component of the reception is the convolution of the transmitted sequence and multipath impulse response; the matched-filters receiver matches to each possibly different sequence convolved with the multipath impulse response. The receiver outputs due to the signal component of the reception are the (circular) cross correlations of the actual codeword and each of the distinctly different sequences, convolved with the autocorrelation of the multipath impulse response. Since the receiver is linear, signal and noise may be treated separately, so the evaluation models the noise as scaled-noise added to the final outputs.

Assume that the transmitted sequence was from the Zth code with the Jth rotation, denoted by $s_J((k - J)T_c)$. Let $R_J(t)$ be the output of the cross correlation against an estimated multipath after the Jth code sequence correlator. To decode the information block of $2n$ bits transmitted correctly, the value $R_J((\tau - J)T_c) + n_J(\tau T_c)$ at $\tau = J$ should be greater than all the wrong values. The probability that the codeword is correct is

$$\Pr[C \mid s_J(t - J T_c)] = \int_{-\infty}^{\infty} \phi(\alpha) \prod_{i=1}^{L+2} \prod_{j=1}^{j} \Phi\left(\frac{\alpha + R_J(0) - R_J(j T_c)}{\sigma_n}\right) d\alpha \quad (23)$$

where $\sigma_n^2 = R_m(0)N_0/2L$ is the variance of the noise out of the multipath correlator.

There are $2^{2n} - 2$ cross-correlation values $R_J(j T_c)$ corresponding to mismatches in (23). Each of these appears many times in the product terms at the integrand of (23). An approximation formula for a high power of the normal distribution function $\Phi(x)$ is given in [9]; it is called Tippet’s rule. For convenience, we rewrite it here:

$$\Phi^\ast(x) = \exp\left[-\exp\{a(u)(x-u)\}\right] \quad (24)$$

where $u$ satisfies $\Phi(-u) = 1/\alpha$, for integer $\alpha$. For the computer evaluations, the transmitted signals were $\pm 1$ Gold sequences of length, $L = 127$. The same four-path sparsely spaced equal-strength multipath was chosen with, $R_m(0) = 4$. Each source block is $2n = 14$ b. Bit energy SNR is

$$E_b/N_0 = \frac{1}{2n} \frac{1}{N_0} \frac{1}{4n} \frac{R_2(0)}{\sigma_n^2}. \quad (25)$$

The integrand of (23) has $2^{2n} - 1$ factors in the double product, 16,383 for the numerical example. Four approaches were taken to cope with this large number of factors:

(i) Tippet’s rule was used for any factor which appeared more than 200 times.

(ii) The $R_J(j T_c)$ were ordered in descending order and searched for the largest that occurred at least 200 times; all smaller cross-correlation values were set equal to this largest and Tippet’s rule used for the corresponding factor; this yields an upper bound.

(iii) The $R_J(j T_c)$ were ordered in ascending order and searched for the smallest that occurred at least 200 times; all larger cross-correlation values were set equal to this smallest and Tippet’s rule used for the corresponding factor; this yields a lower bound.

(iv) Random Variable Method: all $R_J(J T_c)$ except $R_J(J T_c)$ were replaced with i.i.d. random values drawn from a random number generator with a Gaussian distribution whose mean and variance were the mean and variance of the distribution shown in Fig. 4. (Fig. 4 is a histogram of all the normalized cross-correlation values between sequences in a Gold code family of 127 digits.)

These four approximations to (23) are shown in Fig. 6. The authors consider Curve I to be the best approximation. The upper bound Curve II is much closer to Curve I than the lower bound Curve III. That means that the most influential cross-correlation values are near the correct cross-correlation value. The random variable approximation Curve IV for the sparsely spaced multipath channel is close to Curve I for a low SNR. The discrepancy between them increases as the SNR increases.

V. CONCLUSION

Three block waveform codings with the same block length were evaluated for a hypothetical multipath channel and a single user. The block length was $L = 127$, and the channel was a four-path, equal-strength sparsely spread channel. Fig. 7 presents our best evaluations of the codes’ performances. At $10^{-5}$ codeword error probability, the $m$-sequence family coding requires $E_b/N_0$ of 5.1 dB, the Gold-sequence family coding requires $E_b/N_0$ of 6.8 dB, and the single $m$-sequence coding requires $E_b/N_0$ of 7.7 dB. The Gold-sequence family and $m$-sequence family difference is 1.5-1.7 dB at all error levels investigated.

APPENDIX A

In this appendix we will show how to choose the phase for the $m$-sequence-controlled waveform so that the discrete-time autocorrelation of the $m$-sequence-controlled waveform $R(\tau)$ is zero...
The first three terms are constants, so $R_{12}(\tau)$ takes on only two values:

$$
R_{12}(\tau) = \begin{cases} 
  \frac{L + 1}{2L} a^*c + \frac{L - 1}{2L} b^*d, & \text{if } \tau = 0 \mod L \\
  \frac{L + 1}{4L} (a + b)^*(c + d) - \frac{1}{L} b^*d, & \text{if } \tau \neq 0 \mod L.
\end{cases}
$$

(A6)

If $s_1(k)$ represents the transmitter's version of the sequence and $s_2(k)$ represents the receiver's processing of the signal, it is obvious that the receiver can adjust $c$ and $d$ to yield a zero cross correlation when $\tau \neq 0$. This is desirable in multipath situations so that strong paths do not obscure weak paths due to "time-sidelobes"; i.e., nonzero cross correlation for $\tau \neq 0$.

The autocorrelation of $s_1(k)$ may be deduced by setting, $c = a$, $d = b$, yielding:

$$
R_{11}(\tau) = \begin{cases} 
  \frac{L + 1}{2L} |a|^2 + \frac{L - 1}{2L} |b|^2, & \text{if } \tau = 0 \mod L \\
  \frac{L + 1}{4L} |a + b|^2 - \frac{1}{L} |b|^2, & \text{if } \tau \neq 0 \mod L.
\end{cases}
$$

(A7)

Of particular interest is the "biphase signal," $a = 1$, $b = -1$, for which

$$
R_{11}(\tau) = \begin{cases} 
  1, & \text{if } \tau = 0 \mod L \\
  -\frac{1}{L}, & \text{if } \tau \neq 0 \mod L.
\end{cases}
$$

(A8)

and the "general biphase signal," $a = e^{i\theta}$, $b = e^{-i\theta}$, for which

$$
R_{11}(\tau) = \begin{cases} 
  1, & \text{if } \tau = 0 \mod L \\
  \frac{L + 1}{L} \cos^2 \theta - \frac{1}{L}, & \text{if } \tau \neq 0 \mod L.
\end{cases}
$$

(A9)

If $\theta = \tan^{-1}(\sqrt{L})$, then the $\tau \neq 0$ autocorrelation is zero. This is known as the "period matched angle" [2], [10]. The single $m$-sequence waveform code with the period matched angle is an orthogonal code with codewords (or rotations in time).

APPENDIX B

We will show that the time average and total power of the signal component $s_1(\tau)$ at the sequence cross correlators in (13) are independent of the pair $(i, J)$.

We assume that rotation index $J$ is equal to zero without loss of generality, since $s_{1,j}(\tau - J)$ is periodic. The $m$-sequence-controlled baseband modulating waveform $s_J(t)$ is

$$
C_{s_J}(t) = \sum_{k=0}^{L-1} a_k(k) e^{i\theta_k(k)} p(t - kT_c) 
$$

(B1)

where $p(t)$ is a complex-valued baseband pulse with duration $T_c$, $a_k(k)$, and $\theta_k(k)$ are selected in some manner by the $L$ chip $m$-sequence. $T_c$ is the duration of one $m$-sequence chip.

For convenience, let’s use the following notation:

$$
\psi_k(k) = a_k(k) e^{i\theta_k(k)} = g_1(k) + b
$$

where $a$ and $b$ are complex numbers, and $g_1(k)$ is a real linear maximal sequence based on $\pm 1$ representation from the $i$th
simple shift-register generator. If the sequence chip is a logical one, 
\[ w_I(k) = b + a \]  
while if the sequence chip is a logical zero, 
\[ w_I(k) = b - a. \]  

The \( i \)th cross-correlator output, due to the \( i \)th sequence transmitted, is 
\[ s_{iI}(\tau) = \frac{1}{L} \left( w_I(k) \odot m(k), w_I(k + \tau) \right) \]
\[ = \sum_{n=0}^{P-1} c_n \sum_{k=0}^{L-1} w_I(k - \tau_n) w_I^*(k + \tau) \]

where \( a(k) \odot b(k) \) is the convolution of \( a(k) \) and \( b(k) \), and \( w^* \) is the complex conjugate of \( w \). The time average of \( s_{iI}(\tau) \) over one period \( L \), denoted by \( E[I_s_{iI}] \), is 
\[ E[I_s_{iI}] = \frac{L}{L - 1} \sum_{\tau=0}^{L-1} s_{iI}(\tau) \]
\[ = \sum_{n=0}^{P-1} c_n \sum_{k=0}^{L-1} w_I(k - \tau_n) \left[ \sum_{\tau=0}^{L-1} w_I^*(k + \tau) \right]. \]

However, the bracketed factor in (B6) is constant, since \( w_I \) has a period \( L \). The bracket factor is 
\[ \sum_{\tau=0}^{L-1} w_I^*(k + \tau) = Lb^* + a^*, \quad \text{for all } i \]

since there are \((L + 1)/2\) ones and \((L - 1)/2\) negative ones in any \( m \)-sequences \( s(k) \) of period \( L \). Similarly, the second summation factor in (B6) is equal to \((Lb + a)\). Hence 
\[ E[I_s_{iI}] = \frac{(Lb + a)^2}{L^2} \sum_{n=0}^{P-1} c_n \]

for any \( m \)-sequence pairs \((i, I)\), including the \( i = I \) pair.

Now let’s prove that the total energy of \( s_{iI}(\tau) \) over one period \( L \) is independent of the pair \((i, I)\). Since the mean is constant, this is equivalent to showing that a time-averaged variance, denoted by \( \text{Var}[s_{iI}] \), is independent of \( i \).

\[ \text{Var}[s_{iI}] = \frac{1}{L} \sum_{\tau=0}^{L-1} \{ s_{iI}(\tau) - E[I_s_{iI}] \}^2 \]
\[ = \frac{1}{L} \sum_{\tau=0}^{L-1} s_{iI}(\tau)s_{iI}^*(\tau) - E[I_s_{iI}]^2 \]
\[ = \frac{1}{L} \sum_{\tau=0}^{L-1} s_{iI}(\tau)s_{iI}^*(\tau) - E[I_s_{iI}]^2 \]
\[ = \frac{1}{L} \sum_{\tau=0}^{L-1} w_I^*(m - \tau_n) w_I^*(n - \tau_n) \times \sum_{\tau=0}^{L-1} w_I^*(m + \tau) w_I(n + \tau) - E[I_s_{iI}]^2. \]

However, for any \( i \), if \( m \) is equal to \( n \), 
\[ \sum_{\tau=0}^{L-1} w_I^*(m + \tau) w_I(n + \tau) = \left( \sum_{\tau=0}^{L-1} |w_I(m + \tau)|^2 \right) \]
\[ = \frac{L + 1}{2} |b + a|^2 + \frac{L - 1}{2} |b - a|^2 \]
\[ = \frac{L + 1}{2} (bb^* + aa^* + ba^* + b*a) \]
\[ + \frac{L - 1}{2} (bb^* + aa^* - ba^* - b*a) \]
\[ = L(bb^* + aa^*) + ba^* + b*a. \]

while, if \( m \) is not equal to \( n \), 
\[ \sum_{\tau=0}^{L-1} w_I^*(m + \tau) w_I(n + \tau) \]
\[ = \frac{L + 1}{4} |b + a|^2 + \frac{L - 1}{4} |b - a|^2 \]
\[ = \frac{L + 1}{4} ((bb^* + aa^*) + ba^* + b*a) \]
\[ + (bb^* - aa^* - ba^* + ab^*) \]
\[ + (bb^* - aa^* + ba^* - ab^*) \]
\[ = L(bb^* + \frac{1}{4} (4aa^* + 4ba^* + 4b*a)) \]
\[ = Lbb^* - a^* + ba^* + b*a. \]

since any \( m \)-sequence modulated sequence has a two-level autocorrelation function. Since the sum of (B10) is the only factor in (B9) that depends on \( i \), \( \text{Var}[s_{iI}] \) is independent of \( i \). To finish the proof we need to show the independence of \( I \). We are free to let \( i = I \). Hence 
\[ \text{Var}[s_{iI}] = \frac{1}{L} \sum_{\tau=0}^{L-1} |s_{iI}(\tau)|^2 - E[I_s_{iI}]^2. \]

Now that it has been shown that the variance depends only on the autocorrelation of the transmission and that all these sequences have the same autocorrelation function, the variance will obviously be independent of \( I \). Therefore \( \text{Var}[s_{iI}] \) is independent of the pair \((i, I)\).

**APPENDIX C**

This appendix develops the test statistic \( T(x | I, J) \) that was used to make the decision that the \( m \)-sequence used was the \( I \)th and the rotation was \( J \), as the decoding for the \( m \)-sequence
family code. The test statistic is defined by
\[ T(x | I, J) = \frac{1}{v} \sum_{k=0}^{P-1} c_k x_k(J + r_k T_c) \]

As background we consider first the simple detection theory problem of deciding whether a real one-dimensional observation \( y \) was more likely to result from a normal distribution with mean \( m \) and variance \( v \), or from a normal distribution with zero mean and variance \( u + v \). The likelihood ratio is
\[ l(y) = \frac{1}{\sqrt{2\pi u + v}} e^{-\frac{(y-m)^2}{2(u+v)}}. \quad (C1) \]

After simple manipulation the logarithm of the likelihood ratio is
\[ \ln l(y) = \frac{my}{v} - \frac{uy^2}{2(u+v)} - \frac{m^2}{2u} + \frac{1}{2} \ln \left( \frac{u + v}{v} \right). \quad (C2) \]

We next consider \( x_z = (x_z(T_c), x_z(2T_c), \ldots, x_z(LT_c)) \), the \( L \) point output of the finite interval matched filter, matched to the \( I \)th \( m \)-sequence of the \( m \)-sequence family. The noise model is one of independent input samples, the rotations of any \( m \)-sequence with period-matched bi-phase modulation are orthogonal, and the multipath impulse response is known. If the transmission was indeed the \( I \)th \( m \)-sequence, the samples of \( x_z \) are independent with the same variance, say \( v \); furthermore, if the coded rotation was \( J \), then the mean of the component \( x_z((J + r_p)T_c) \) is the \( p \)th path gain \( c_p \).

As a null hypothesis we artificially consider i.i.d. Gaussian samples with zero mean and per-sample variance \( u + v \), where \( u \) is the average mean-square sample output if there were no noise. The added variance \( u \) is the average cross correlation between the \( I \)th \( m \)-sequence and the other \( m \)-sequence with the given multipath impulse response. Although we know the details of all these cross correlations, this artificial null hypothesis ignores that knowledge and replaces it with a simple Gaussian i.i.d. model. We believe the "Gaussian" part of the additional variance is a reasonably accurate description of \( m \)-sequence cross-correlation values when all \( m \)-sequences are lumped together; modeling the detailed deterministic cross-correlation structure with an i.i.d. random process will certainly lead to a nonoptimum decision algorithm whose performance is a lower bound on the performance of the optimum decision algorithm.

This null hypothesis certainly leads to a much simpler decision algorithm, than one that utilizes all the details of the actual sequence cross correlations. Under this i.i.d. null hypothesis, one needs only to calculate the likelihood ratio of each sequence matched-filter output conditional to each codeword and pick the codeword corresponding to the largest likelihood ratio. Stated a bit more accurately, pick \((I, J)\) that maximizes \( l(x_z | I, J) \) or maximizes any function that is monotone-increasing with \( l(x_z | I, J) \).

The logarithm of the likelihood ratio of i.i.d. components is the sum of the component log likelihood ratios. Let’s consider the four terms in \((C2)\) one at a time, moving from the one-dimensional \( y \) to the \( L \)-dimensional \( x_z \):

1st term:
\[ \frac{my}{v} - \frac{1}{v} \sum_{p=0}^{P-1} c_p x_z((J + r_p)T_c) \quad (C3) \]

because the matched-filter output, matched to the correct sequence, has an output proportional to the path impulse response, rotated by the coded rotation \( J \). The sum is over all paths.

2nd term:
\[ -\frac{uy^2}{2(u+v)} \rightarrow -\frac{u}{u + v} - \frac{1}{2} \sum_{k=1}^{L} |x_z(kT_c)|^2. \quad (C4) \]

The sum is over all chips, a "time sum."

3rd term:
\[ -\frac{m^2}{2v} - \frac{1}{2} \sum_{p=0}^{P-1} c_p^2 \quad (C5) \]

This term is a path sum and its value is independent of \( I \) and \( J \), so that it does not effect the decision process or its performance.

4th term:
\[ -\frac{1}{2} \ln \left( \frac{u + v}{v} \right) \rightarrow -\frac{L}{2} \ln \left( \frac{u + v}{v} \right). \quad (C6) \]

This term is a time sum and its value is independent of \( I \) and \( J \), so that it does not effect the decision process or its performance.

The sum of the first and second terms, multiplied by \( v \) for simplicity, is
\[ v \ln l(x_z | I, J) = \sum_{p=0}^{P-1} c_p x_z((J + r_p)T_c) - \frac{u}{2(u+v)} \sum_{k=1}^{L} |x_z(kT_c)|^2 + \text{constant}. \quad (C7) \]

Dropping the unknown constant yields the test statistic \( vT(x | I, J) \) used in Section III.

**REFERENCES**


[10] K. Metzger, Jr., "Signal processing equipment and techniques
Hyuck M. Kwon (S'82-M'84) was born in Korea on May 9, 1953. He received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 1978 and 1980, respectively, and the Ph.D. degree in computer, information, and control engineering from the University of Michigan, Ann Arbor, in 1984.

While at Michigan, he worked as a Research Assistant in the Cooley Electronics Laboratory, where he evaluated the performance of digital coding schemes for the underwater acoustic multipath channel. From 1985 to 1989 he was with the University of Wisconsin, Milwaukee, as an Assistant Professor in the Electrical Engineering and Computer Science Department, where he performed research and taught several graduate courses in the communications system area. Since 1989 he has been with the Lockheed Engineering and Sciences Company, Houston, TX, as a Principal Engineer, where he is responsible for analysis of the Space Station Freedom and Space Shuttle communication systems, and for analysis of Lunar–Mars laser communications systems. In addition, he served as a Consultant for J. S. Lee Associates, Inc., where, in 1985, he analyzed the performance of spread-spectrum communications systems and, in 1987, was involved in analyzing the narrowband, digital, FM Radio spread-spectrum communications systems. His current interests include analysis of satellite communication systems, multiple access communications networks, bandwidth and power-efficient coded modulation, optical laser communications, and neural networks.

Theodore G. Birdsall (M'57) received the M.S. degree in mathematics and the Ph.D. degree in communications sciences.

He is a Professor in the Electrical Engineering and Computer Science Department of the University of Michigan, Ann Arbor. He has worked in engineering research since 1951 and has taught as a member of the Electrical Engineering faculty since 1966. His primary interest is in extraction of information from noisy signals, ranging from signal detection theory, psychophysical measurements, radar, sonar, analog and digital communication, and associated signal processing. Since 1960 most of his research has been in underwater acoustic propagation at long ranges and its applications.