Optical Orthogonal Codes: Design, Analysis, and Applications

FAN R. K. CHUNG, JAWAD A. SALEHI, MEMBER, IEEE, AND VICTOR K. WEI, MEMBER, IEEE

Abstract —An optical orthogonal code is a family of (0,1) sequences with good auto- and cross-correlation properties, i.e., the autocorrelation of each sequence exhibits the "thumbtack" shape and the cross correlation between any two sequences remains low throughout. The study of optical orthogonal codes has been motivated by an application in a code-division multiple-access fiber optic channel. The use of optical orthogonal codes enables a large number of asynchronous users to transmit information efficiently and reliably. The thumbtack-shaped autocorrelation facilitates the detection of the desired signal, and low-profiled crosscorrelation reduces interference from unwanted signals. In addition to the wide-band multiple-access system, optical orthogonal codes also find applications in mobile radio, spread-spectrum communications, and radar and sonar signal design. Methodologies in the design and analysis of optical orthogonal codes with tools from projective geometry, the greedy algorithm, iterative constructions, algebraic coding theory, block design, and various other combinatorial disciplines are discussed.

I. Introduction

An optical orthogonal code (OOC) is a family of (0,1) sequences with good auto- and cross-correlation properties, i.e., the autocorrelation of each sequence exhibits the "thumbtack" shape and the cross correlation between any two sequences remains low throughout. Its study has been motivated by an application in a code-division multiple-access fiber optical channel. The use of OOC's enables a large number of asynchronous users to transmit information efficiently and reliably. The lack of a network synchronization requirement enhances the flexibility of the system. The thumbtack shape of the autocorrelation facilitates the detection of the desired signal, and the low cross correlation reduces the interference from unwanted signals in the network. In addition to the optical multiple-access channel, optical orthogonal codes also find applications in mobile radio, frequency-hopping spread-spectrum communications, and radar and sonar signal design. Many more potential applications are being actively explored.

Optical orthogonal codes are closely related to constant-weight error-correcting codes and difference sets. Several existing techniques are applied here to the construction and analysis of OOC's. However, the distinction between the subjects allows us to derive new and interesting results. Optical orthogonal codes are also related to well-correlated binary sequences in the literature. However, the codes considered here consist of truly (0,1) sequences and are intended for "unipolar" environments that have no negative components, while most documented correlation sequences are actually $(+1,-1)$ sequences intended for systems having both positive and negative components. This important distinction produces quite different results.

The rest of the paper is organized into four sections. The definition and the fundamental properties of OOC's are presented in Section II. Several applications are outlined in Section III. In Section IV, we derive theoretical upper and lower bounds on the maximum possible size of OOC's and give several methods for constructing them. Section V contains the concluding remarks of this paper. The performance analysis of an optical multiple-access system employing optical orthogonal codes is presented in the Appendix.

Manuscript received March 17, 1986; revised February 23, 1987. This work was presented at the IEEE International Symposium on Information Theory, Ann Arbor, MI, 1986.

The authors are with Bell Communications Research, 445 South Street, Morristown, NJ 07960-1910.

IEEE Log Number 8928186.

II. Fundamental Properties of Optical Orthogonal Codes

In this section, we give the definition and some fundamental properties of OOC's. An $(n, w, \lambda_a, \lambda_c)$ optical orthogonal code C is a family of (0,1) sequences of length n and weight w which satisfy the following two properties.

1) The Autocorrelation Property:

$$\sum_{t=0}^{n-1} x_t x_{t+\tau} \le \lambda_a$$

for any $x \in C$ and any integer τ, $0<\tau<n$.

2) The Cross-Correlation Property:

$$\sum_{t=0}^{n-1} x_t y_{t+\tau} \le \lambda_c$$

for any $x \neq y \in C$ and any integer τ.

We focus on periodic correlations, i.e., the subscripts are reduced modulo n whenever necessary. In short, the autocorrelation of each sequence in the OOC exhibits the thumbtack shape, and the cross correlation between any two sequences remains low throughout. Since each sequence x has weight w, the autocorrelation equals w when $\tau = 0$. The numbers λ_a and λ_c are called the auto- and cross-correlation constraints. The (0,1) sequences of an optical orthogonal code are called its codewords. The size of an optical orthogonal code, denoted by $|C|$, is the

0018-9448/89/0500-0595$01.00 ©1989 IEEE

number of codewords in it. Throughout this paper, we require $\lambda_a, \lambda_c \leq w$ to avoid triviality.

Cyclic shifts of codewords of an optical orthogonal code do not affect its correlation properties. Let C be an $(n, w, \lambda_a, \lambda_c)$ code and let C' be derived from C by shifting an arbitrary subset of codewords by an arbitrary amount (different codewords may be shifted by different amounts). Then C' is still an $(n, w, \lambda_a, \lambda_c)$ code. We do not make a distinction between codes that can be obtained from each other by cyclic shifts.

It is desirable to have a large OOC. For a given set of values of n, w, λ_a, and λ_c, the largest possible size of an $(n, w, \lambda_a, \lambda_c)$ optical orthogonal code is denoted by $\Phi(n, w, \lambda_a, \lambda_c)$. An optical orthogonal code having the maximum size is said to be optimal. The determination of the exact values of $\Phi(n, w, \lambda_a, \lambda_c)$ and the specific construction of optimal codes are of interest. In Section IV, we present lower and upper bounds to $\Phi(n, w, \lambda_a, \lambda_c)$ and give constructions for several classes of optimal or near-optimal OOC's.

We may also view optical orthogonal codes from a set-theoretical perspective. An $(n, w, \lambda_a, \lambda_c)$ optical orthogonal code $\boldsymbol{C}$ can be alternatively considered as a family of w-sets of integers modulo n, in which each w set corresponds to a codeword and the integers within each w set specify the nonzero bits of the codeword. Then the correlation properties can be reformulated as follows.

1) The Autocorrelation Property:

$$|(a+X)\cap(b+X)| \leq \lambda_a$$

for any $X \in \boldsymbol{C}$ and any $a \not\equiv b (\text{mod } n)$.

2) The Cross-Correlation Property:

$$|(a+X)\cap(b+Y)| \leq \lambda_c$$

for any $X \neq Y \in \boldsymbol{C}$ and any a, b. Note that $a + X = \{a + x: x \in X\}$ and all integers under consideration are taken modulo n. The set-theoretical perspective offers a convenient notation for OOC's when w is much smaller than n.

From now on, a *code* is an optical orthogonal code unless otherwise specified, and we use the shorthand notation of an (n, w, λ) code when $\lambda_a = \lambda_c = \lambda$.

Example: $C = \{1101000\}$ is a $(7,3,1)$ code with one codeword. In set notation, $\boldsymbol{C} = \{\{0,1,3\}\}$ (mod 7).

Example: $C = \{1011000100000\}$ is a $(13,4,1)$ code with one codeword. In set notation, $\boldsymbol{C} = \{\{0,2,3,7\}\}$ (mod 3).

Example: $C = \{1100100000000, 1010000100000\}$ *is a* $(13,3,1)$ code with two codewords. In set notation, $\boldsymbol{C} = \{\{0,1,4\},\{0,2,7\}\}$ (mod 13).

The following facts on OOC's are useful in later sections.

Fact 1: There is another interpretation of the correlation properties. Condition 1') is equivalent to the following: for each $X \in \boldsymbol{C}$, any integer $c \neq 0$ can be represented as the difference $x - x'$, with $x, x' \in X$, in at most λ_a ways. Similarly, 2') is equivalent to the following: for every pair of w-sets $X \neq Y \in \boldsymbol{C}$, any integer $c \neq 0$ can be represented as the difference $x - y$, with $x \in X, y \in Y$, in at most λ_c ways. The proof is straightforward.

Fact 2: An upper bound on the maximum code size $\Phi(n, w, 1)$ can be derived from a distinct difference argument. Let $\boldsymbol{C}$ be an $(n, w, 1)$ code, and let $\Delta(X) = \{x - x': x, x' \in X \text{ and } x \neq x'\}$ (mod n) for $X \in \boldsymbol{C}$. Since an $(n, w, 1)$ code has no repeated differences, $0 \notin \Delta(X)$, $|\Delta(X)| = w(w-1)$ for any $X \in \boldsymbol{C}$, and $\Delta(X) \cap \Delta(Y) = \varnothing$ for any $X \neq Y \in \boldsymbol{C}$. This immediately leads to the upper bound

$$\Phi(n, w, 1) \leq \frac{n-1}{w(w-1)}.$$

Furthermore, when n is even, $n/2 \notin \Delta(X)$ for any $X \in \boldsymbol{C}$; otherwise, $|X \cap (n/2 + X)| \geq 2 > \lambda_a$. Therefore, when n is even, we have the slightly stronger bound

$$\Phi(n, w, 1) \leq \frac{n-2}{w(w-1)}.$$

More bounds are presented in Section IV.

Fact 3: Optical orthogonal codes are related but different from difference sets which are well studied in combinatorics (see Hall [10] or Ryser [17]). An (n, w, λ)-difference set is a w-set of integers modulo n such that every nonzero integer modulo n can be written in exactly λ ways as the difference between two members of the w-set. It consists of a single w-set. An (n, w, λ) OOC is a family of w-sets with additional constraints between the sets. However, the two subjects are closely related. Any (n, w, λ)-difference set gives an (n, w, λ)-OOC with a single codeword. The reverse relation is not true in general.

Fact 4: Optical orthogonal codes are related to but different from other orthogonal codes and well-correlated sequences in the literature (e.g., Barker sequences). The lack of "negative components" in current optical transmission technology dictates a different set of correlation properties. Most well-correlated binary sequences studied in the literature are actually $(+1, -1)$ sequences even if they use the $(0,1)$ notation; this is evidenced by the way of calculating their correlations. They are intended for application in systems with both positive and negative numbers available. The correlation constraint can be made zero. Our study focuses on true $(0,1)$ sequences intended for "unipolar" environments which have no negative components, such as a direction-detection optical system. The minimum feasible correlation constraint is 1. Furthermore, a well-correlated $(+1, -1)$ sequence typically has about the same number of $+1$'s and -1's while a good optical orthogonal code has many more 0's than 1's in each codeword. Each class of sequences can be used in the opposite application but only with inferior results. In the name optical orthogonal codes, we wish to imply a unipolar system (optical) with minimal correlation (orthogonal).

III. Applications

The study of OOC's has been motivated by an application in optical code-division multiple access. As shown in Fig. 1, many users are transmitting information over a

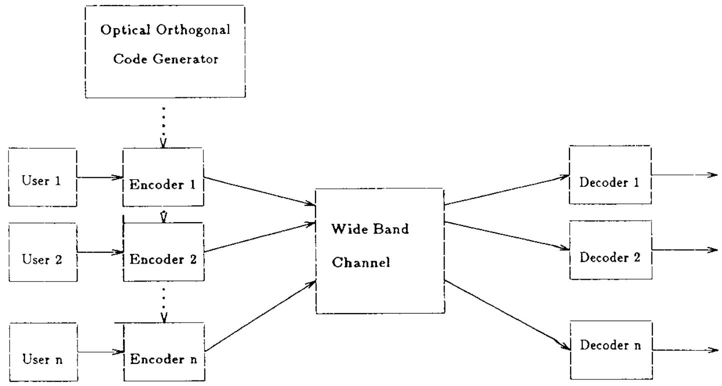

Fig. 1. Code-division multiple-access optical system.

common wide-band optical channel. The objective is to design an efficient system, with available implementation technology, to allow the users to share the common channel. Traditional multiple-access approaches such as frequency division, time division, collision detection, or demand assignment require elaborate network synchronization at high speed (often optical speed), and frequent conversions between the optical domain and the electronic domain. These requirements limit the efficiency of such an optical multiple-access system. However, by employing a code-division multiple-access system with optical orthogonal codes, we are able to simplify greatly the complexity of the system, to implement it with available technology, and to achieve potentially higher transmission efficiency.

Let an $(n, w, 1)$ optical orthogonal code $\boldsymbol{C}$ with M codewords (i.e., w sets) be used. The system can accommodate M transmitters simultaneously. Each transmitter is assigned a w-set from $\boldsymbol{C}$. (Here, we use the set-theoretical notation of OOC's.) At a transmitter, every information bit is encoded into a frame of n optical chips in the following way. (A chip is an optical time slot which can assume one of two values: ON or OFF.) Let the assigned w-set for a particular transmitter be $S = \{s_1, s_2, \cdots, s_w\}$. Assume the information bit is **1**. In the corresponding frame, which consists of n optical chips, photon pulses (i.e., ON signals) are sent at exactly the s_1th, s_2th,$\cdots$, and s_wth chips. In the other $n - w$ chips, no photon pulses (i.e., OFF signals) are sent. In other words, the codeword set is used as the signature sequence of the transmitter. On the other hand, if the information bit is **0**, no photon pulses are sent in the corresponding frame, i.e., all OFF signals are sent.

All M users are allowed to transmit at any time. There is no network synchronization required. At the receiving end, correlation-type decoders are used to separate the transmitted signals. The decoder consists of a bank of M tapped delay-lines, one for each codeword. The delay taps on a particular line exactly match the signature sequence, i.e., the delays between successive taps are equal to $s_2 - s_1, s_3 - s_2, s_4 - s_3, \cdots,$ optical chips, respectively. These tapped delay-lines can be easily implemented with existing optical technology.

Each tapped delay-line effectively calculates the correlation of the received waveform with its signature sequence. Because of the properties of optical orthogonal codes, the correlation between different signature sequences is low. Thus the delay-line output is high only when the intended transmitter's information bit is 1. The transmitted information is extracted by thresholding the correlator output.

This optical code-division multiple-access system can be easily implemented. The tapped delay-line correlator is readily available. Little or no electronic–optical domain conversion is required. There is no synchronization requirement in the network. Although bandwidth expansion is effected by the transmitter, the simplicity and flexibility of the system concept enables us to pump optical pulses at a much faster chip rate than otherwise possible. The overall system throughput efficiency can be much improved.

Although the motivating application is optical, the same system can also be used in other wide-band code-division multiple-access environments. For more detailed description of the system, see [2]. For other related ideas, see [11], [12].

In this paper, we restrict our attention to periodic correlations. Codes with aperiodic correlation properties are also worth studying. Since periodic correlation is a stronger property, OOC's naturally satisfy aperiodic correlation constraints. However, larger codes can be designed if only aperiodic correlation properties are required. Some may argue that aperiodic correlation sequences are more appropriate for the present application. We do not settle this issue here.

There are several other potential applications of optical orthogonal codes. In spread-spectrum communications, frequency hopping patterns are required to have low correlation. Optical orthogonal codes can be used to generate good hopping patterns. However, there is one more important factor for consideration. Frequency hopping patterns can be depicted as dots in a rectangular checkerboard. Typically, there is exactly one dot per column, representing that only one frequency component is used per time slot. To obtain hopping patterns from OOC's, we write down a codeword into a rectangular box in either rowmajor or column-major form. The number of dots in a column can vary from 0 or 1 to more than 1. This represents a variable number of frequency components in a time slot. However, the auto- and cross-correlation requirements of frequency hopping patterns are preserved. The removal of the one-dot-per-column restriction tends to increase the number of available patterns. This increases the diversity of spread-spectrum systems and is considered desirable. However, the implementation calls for further study.

The same methodology can be used to obtain patterns useful in situations requiring good auto- and cross-correlation properties, such as radar and sonar signal design, Costas arrays, etc. In each situation, a unipolar application environment (which lacks negative components because an energy-type detection method is used) needs binary sequences with good correlation properties. To use an optical orthogonal code, write out codewords into a matrix either column by column or row by row. The resulting matrices will have good correlation properties with respect to any combination of horizontal and vertical shifts. (During the preparation of this paper, another important application of optical orthogonal codes has been exploited by Vecchi and Salehi [23].)

IV. The Design and Analysis of Optical Orthogonal Codes

In this section, we derive general upper and lower bounds on the maximum size of OOC's and present several construction methods. First, general upper bounds on the maximum size of OOC's are given. Next we present iterative methods of constructing codes from existing codes. In Section IV-C the "greedy" algorithm is used to construct codes. The results in Sections IV-B and -C yield general lower bounds for code sizes. In Section IV-D a large class of codes is constructed from finite projective geometries, and many of them are optimal. In Section IV-E more optimal codes are constructed via combinatorial methods. In Section IV-F we discuss the usage of block design and algebraic coding theory for constructing OOC's.

A. Upper Bounds

Upper bounds on the maximum size of an optical orthogonal code $\Phi(n,w,\lambda)$ can be obtained from related results in algebraic coding theory. An error-correcting code is a set of binary n-tuples with a certain structure. Each n-tuple is a codeword, and the number of 1's is its (Hamming) weight. The (Hamming) distance between two n-tuples is the number of bit positions in which they differ. A fundamental problem in algebraic coding theory is to find the largest error-correcting code with length n and distance at least d between every pair of codewords. It is also interesting to consider the same problem in the class of error-correcting codes with constant codeword-weight. Let $A(n,d,w)$ denote the maximum size of an error-correcting code with length n, constant codeword-weight w, and distance d or more between every pair of codewords. The determination of the precise values of $A(n,d,w)$ for general parameters n, d, and w is a difficult problem. Numerous references to results on this topic can be found in Best *et al.* [1], Golay [7], and MacWilliams and Sloane [16]. In particular, the Johnson bound [13], [16] states that

$$A(n,2\delta,w) \le \frac{n(n-1)\cdots(n-w+\delta)}{w(w-1)\cdots\delta}.$$

We will use the Johnson bound and the relationship between $\Phi(n,w,\lambda)$ and $A(n,d,w)$ to derive a general upper bound for $\Phi(n,w,\lambda)$.

Theorem 1: $\Phi(n,w,\lambda) \le (1/n)A(n,2w-2\lambda),w) \le ((n-1)\cdots(n-\lambda)/w(w-1)\cdots(w-\lambda))$.

Proof: For any (n,w,λ) optical orthogonal code C, let C' be the error-correcting code consisting of all cyclic shifts of codewords of C. Since for every codeword of C, its n cyclic shifts are all distinct, we have $|C'|=n|C|$. Every n-tuple in C' has Hamming weight w. Furthermore, for any two members of C', there are at most λ bit positions where they both have a 1. Therefore, C' has minimum distance at least $2w-2\lambda$, and we have

$$|C'| \le A(n,2w-2\lambda,w).$$

Since $|C'|=n|C|$, this implies the theorem.

When $\lambda_a \ne \lambda_c$, we can set $\lambda=\max\{\lambda_a,\lambda_c\}$ and apply the above upper bound. The bound is particularly strong for small values of λ. For large values of λ, other available upper bounds on the size of constant weight codes are contained in MacWilliams and Sloane [16].

The problem of designing codes for the chip and frame synchronous multiple-access optical system is equivalent to the problem of designing constant-weight codes. In the chip-synchronous optical system, we wish to design a large set of (0,1) sequences with constant weight and minimum overlap. It is equivalent to designing a large constant-weight code. However, it may be interesting to design a large set of (0,1) sequences with several (say, two or three) possible weights and minimum overlap for use over the chip-synchronous optical system. This does not correspond to any well-known coding problem.

B. Iterative Construction

Given an $(n,w,\lambda_a,\lambda_c)$ code, we present several methods of constructing another code with different parameters. The first method is trivial.

Method 1: Given an $(n,w,\lambda_a,\lambda_c)$ code C, we can use it as an $(n,w,\lambda'_a,\lambda'_c)$ code with $\lambda'_a \ge \lambda_a$ and $\lambda'_c \ge \lambda_c$.

Method 2: Given an $(n,w,\lambda_a,\lambda_c)$ code C with m codewords, we construct an $(n,2w-2\lambda_c,2\lambda_a+2\lambda_c,w+3\lambda_c)$ code C' with $\binom{m}{2}$ codewords as follows. For every pair of codewords x and y of C, we construct a codeword z of C' as follows. First, let $z'=x \vee y$, where $\vee$ represents the bit-wise OR operation. Since x and y both have weight w and overlap at no more than λ_c bit positions, the weight of z', denoted by wt (z'), is at least $2w-2\lambda_c$. Then let z be derived from z' by changing any wt $(z)-(2w-2\lambda_c)$ bits from 1 to 0. Every codeword z of C' has weight precisely $2w-2\lambda_c$. The autocorrelation of z is at most equal to the autocorrelation of z', which is

$$\begin{aligned}|(x \vee y) \cap (\text{a cyclic shift of } x \vee y)| &\le |x \cap (\text{a cyclic shift of } x)| \\ &\quad + |x \cap (\text{a cyclic shift of } y)| \\ &\quad + |y \cap (\text{a cyclic shift of } x)| \\ &\quad + |y \cap (\text{a cyclic shift of } y)| \\ &\le \lambda_a + \lambda_c + \lambda_c + \lambda_a = 2\lambda_a + 2\lambda_c.\end{aligned}$$

Therefore, C' satisfies the autocorrelation property. Let z_1 and z_2 be two codewords which are derived from $z'_1 = x_1 \vee y_1$ and $z'_2 = x_2 \vee y_2$, where x_1, x_2, y_1, and y_2 are codewords of C with $\{x_1, y_1\} \neq \{x_2, y_2\}$. The cross correlation between z_1 and z_2 is at most the cross correlation between z'_1 and z'_2, which is

$$|(x_1 \vee y_1) \cap (\text{a cyclic shift of } x_2 \vee y_2)| \le \begin{cases} 4\lambda_c, & \text{if } \{x_1, y_1\} \cap \{x_2, y_2\} = \varnothing \\ w + 3\lambda_c, & \text{otherwise} \end{cases}.$$

Since $\lambda_c \le w$, C' satisfies the cross-correlation constraint.

Method 3: Given an $(n, w, \lambda_a, \lambda_c)$ code C, we can construct a $(tn, tw, tw, t\lambda_c)$ code C' with the same number of codewords in the following way. For each codeword x of C construct a codeword z of C' by concatenating t copies of x. (Here, the codeword x is considered as a binary n-tuple.) Each codeword of C' has length tn and weight tw. The autocorrelation can be no larger than tw, and it is easy to verify that codewords of C' satisfy the cross-correlation constraint $t\lambda_c$.

C. The Greedy Algorithm and General Lower Bounds

The "greedy" algorithm is useful in many combinatorial and computational problems. Here we use it to construct optical orthogonal codes with general parameters. Two lower bounds on the performance of the algorithm are given. Each is sharper than the other in a particular range of code parameters. In practice, the algorithm may yield better codes than the lower bounds suggest. Furthermore, there are potential methods to improve the basic algorithm.

The Greedy Algorithm for Constructing $(n, w, \lambda_a, \lambda_c)$ Codes: Originally, the code is empty. In $\binom{n}{w}$ steps, the algorithm examines all the binary n-tuples of weight w, one at a time. If an n-tuple satisfies the autocorrelation property and satisfies the cross-correlation property with every codeword already included, it is added to the code; otherwise, it is discarded.

The algorithm can be implemented in computation time of order $\binom{n}{w}|C|w^2$ and storage space of order $|C|n$. Two lower bounds on the sizes of the OOC's generated by the greedy algorithm are given below.

Theorem 2:

$$\Phi(n, w, \lambda_a, \lambda_c) \ge \frac{\binom{n}{w} - \frac{n-1}{2}\binom{w}{\lambda_a+1}\binom{n}{w-\lambda_a-1}}{n \cdot \sum_{i=\lambda_c+1}^{\min\{n-w, w\}} \binom{n-w}{w-i}\binom{w}{i}}.$$

Proof: In the first part, we show that there are at most $\frac{1}{2}(n-1)\binom{w}{\lambda_a+1}\binom{n}{w-\lambda_a-1}$ n-tuples violating the autocorrelation property. In the second part, we show that, given any n-tuple, there are at most

$$n \sum_{i=\lambda_c+1}^{\min\{n-w, w\}} \binom{n-w}{w-i}\binom{w}{i}$$

n-tuples (counting itself) which violate the cross-correlation property with respect to it. These two facts imply the theorem.

Part I: We overcount the conflicting n-tuples by the following method. Let y be an n-tuple which has 1's in bit positions $s_1, s_2, \cdots, s_w$. By Fact 2 of Section II, if y violates the autocorrelation property, then there exists a number δ, $1 \le \delta \le (n-1)/2$ (if $\delta > (n-1)/2$, take $n - \delta$) that can be represented in $\lambda_a + 1$ or more ways as the difference $s_i - s_j$. There are at most $(n-1)/2$ choices of δ, at most $\binom{w}{\lambda_a+1}$ ways to choose the pairs, and at most $\binom{n}{w-\lambda_a-1}$ ways to choose the remaining bit positions. The upper bound then follows easily.

Part II: Given an n-tuple x, there are $\sum_{i=\lambda_c+1}^{\min\{n-w, w\}}\binom{n-w}{w-i}\binom{w}{i}$ n-tuples which overlap more than λ_c bit positions with it. Each such n-tuple has at most n cyclic shifts, all of which violate the cross-correlation property with respect to x. These are all the n-tuples which violate the cross-correlation property with respect to x.

Combining the arguments of parts I and II, we complete the proof.

When $n \gg w$ and $\lambda_c \gg w^2/n$, we have

$$\Phi(n, w, \lambda_a, \lambda_c) \ge \frac{n^{\lambda_c}}{\frac{w!}{(w-\lambda_c-1)!}\binom{w}{\lambda_c+1}} + (\text{lower order terms})$$

where the lower order terms are asymptotically negligible.

In situations where the greedy algorithm is considered too slow, the following "accelerated greedy algorithm" can be used. The code found is likely to be smaller, but the speed is dramatically improved.

The Accelerated Greedy Algorithm: This algorithm is best visualized via the set-theoretical perspective. It attempts to include a new codeword as a w set by adding one element at a time. The algorithm consists of two nested loops; the outer loop attempts to include a new codeword at each iteration, and the inner loop tries to add one element at a time to the codeword at hand. We begin with the empty code and stop when the inner loop fails to find a suitable element for inclusion.

Assume $m-1$ w-sets have been included in the code and $w-1$ elements have been included in the w-set under consideration. For each number x, $0 \le x < n$, the algorithm calculates the number of ways x can be expressed as $x = a + b - c$, where $a, b, c, a \ne c$, are elements in the incomplete codeword-set at hand. If there are less than λ_a ways, then x can be included without violating the autocorrelation property. For each existing codeword S_i (as a w set), $1 \le i \le m-1$, and each x, $0 \le x < n$, the algorithm also calculates the number of ways x can be expressed as $x = a + b - c$, where a is in the incomplete w set at hand, and $b \ne c$ are elements in S_i. If there are fewer than λ_c ways, then x can be included without violating the cross-correlation property with respect to S_i. There are $(w-1)^2(w-2)$ expressions $a+b-c$ with $a, b, c, a \ne c$ in the codeword at hand; and there are $(m-1)w(w-1)^2$ expressions with a in the current codeword and $b \ne c$ in an existing codeword. Therefore, an element can always be included to make the current codeword complete if

$$\frac{(m-1)w(w-1)^2}{\lambda_c} + \frac{(w-1)^2(w-2)}{\lambda_a} + w - 1 < n.$$

From this, we have the following lower bound.

Theorem 3:

$$\Phi(n, w, \lambda_a, \lambda_c) \ge \frac{\lambda_c(n-w+1) - (\lambda_c/\lambda_a)(w-1)^2(w-2)}{w(w-1)^2}.$$

The accelerated greedy algorithm can be implemented in computation time $O(|C|^2 w^4)$ and storage space $O(n)$. It is considerably faster than the basic greedy algorithm for a wide range of parameter values. The accelerated algorithm is expected to perform better than the bound in Theorem 3 because the worst case considerations in the derivation are unlikely to occur in practice.

D. Projective Geometry

Here, we present a method of constructing optical orthogonal codes from finite projective geometries. First, we demonstrate the method by constructing $(n, w, 1)$ codes. The case $\lambda_a, \lambda_c > 1$ will be discussed later.

Projective geometry is an interesting subject in combinatorics with a rich literature. Due to limited space, we cannot hope to give an adequate account here. In the following, we will only attempt a brief survey of the results most closely related to our study. Researchers interested in more details are encouraged to consult standard textbooks such as Carmichael [4], Hall [10], or Ryser [17].

A finite vector space $V(d+1, q)$ consists of $(d+1)$-dimensional vectors with coordinates from the finite field $GF(q)$, where q is a prime power. Points in the projective geometry $PG(d, q)$ correspond to lines through the origin in $V(d+1, q)$. s-spaces in $PG(d, q)$ correspond to $(s+1)$-dimensional subspaces through the origin in $V(d+1, q)$.

In $V(d+1, q)$ there are q vectors on a line, and hence $q-1$ nonzero vectors are on a line through the origin. Two lines through the origin do not share any nonzero vectors. There are $q^{d+1}-1$ nonzero vectors in all. Therefore, there are $(q^{d+1}-1)/(q-1)$ distinct lines through the origin in $V(d+1, q)$. Also, there are $q^2 - 1$ nonzero vectors on a plane through the origin. They can be partitioned into $q+1$ lines consisting of $q-1$ vectors each. Thus there are $q+1$ points on a line in $PG(d, q)$. Similarly, we can show that there are $(q^{d+1}-1)/(q-1)$ points in $PG(d, q)$.

In the finite projective geometry $PG(d, q)$, any two lines intersect at no more than one point. We will use lines in projective geometry as codewords in optical orthogonal codes. Two codewords will intersect at no more than one point, as desired. What remains is to implement a cyclic shift on the points of the geometry which preserves lines. This can be done by taking a discrete logarithm.

A vector β in the space $V(d+1, q)$ has $d+1$ coordinates with values from the finite field $GF(q)$, or alternatively, it can be regarded as an element β of the extension field $GF(q^{d+1})$. Let α be a primitive element of $GF(q^{d+1})$. Then the nonzero elements of $GF(q^{d+1})$ are the 0th through the $(q^{d+1}-2)$th power of α. If $\alpha^e = \beta$, then the discrete logarithm $\log_\alpha \beta = e$. Therefore, the discrete logarithm establishes a one-to-one correspondence between the nonzero vectors in $V(d+1, q)$ and the integers $\{0, 1, \cdots, q^{d+1}-2\}$. The nonzero vectors on a line through the origin are the ith, $(i+n)$th, $\cdots$, $(i+(q-2)n)$th powers of the primitive element for some i, where $n = (q^{d+1}-1)/(q-1)$ is the size of $PG(d, q)$. For an arbitrary point p in $PG(d, q)$, let $\log p$ denote the discrete logarithm of any vector on the line corresponding to p in $V(d+1, q)$ modulo n. Then $\log(\cdot)$ is a one-to-one mapping between the points of the projective geometry $PG(d, q)$ and the integers modulo n. Each line in the projective geometry corresponds to a subset of integers modulo n.

Furthermore, let the cyclic shift of a line L in $PG(d, q)$ be the set of points $\{p: \log p = 1 + \log p' \pmod n$ for some point p' on $L\}$. Then the cyclic shift of a line is still a line in $PG(d, q)$ (a well-known fact in projective geometry). An orbit is a set of lines in $PG(d, q)$ that are cyclic shifts of each other. The number of lines in an orbit is its *size*, which is necessarily a divisor of n. An orbit is *full* if its size is n; otherwise, it is *incomplete*.

Now we are ready to construct $(n, w, 1)$ optical orthogonal codes from the projective geometry $PG(d, q)$, with $n = (q^{d+1}-1)/(q-1)$ and $w = q+1$. Assume there are m full orbits in $PG(d, q)$. Take one representative line from each full orbit and map each line into a set of integers modulo n under $\log(\cdot)$. The m resulting w sets form an OOC with the described parameters and desired correlation properties. Two lines intersect at no more than one point, and therefore two different shifts of a codeword set intersect at most once, and arbitrary shifts of two codeword sets intersect at most once. Incomplete orbits are discarded.

Example: In GF(2^3), we have

$$\alpha^0 = (0,0,1)$$
$$\alpha^1 = (0,1,0)$$
$$\alpha^2 = (1,0,0)$$
$$\alpha^3 = (0,1,1)$$
$$\alpha^4 = (1,1,0)$$
$$\alpha^5 = (1,1,1)$$
$$\alpha^6 = (1,0,1)$$

and $0 = (0,0,0)$. Therefore, the lines in PG(2,2) are mapped to

$$a = \{0,1,3\}$$
$$b = \{0,2,6\}$$
$$c = \{0,5,4\}$$
$$d = \{1,4,2\}$$
$$e = \{1,5,6\}$$
$$f = \{2,5,3\}$$
$$g = \{3,6,4\}.$$

The vectors 0, α^0, α^1, and α^3 form a 2-space in GF(2^3). They (except 0) contribute to the line a in PG(2,2). Other lines are derived similarly. Note that the cyclic shift of any line is also a line. There is only one orbit containing all seven lines. Picking any line to be the representative, we have a (7,3,1) code with only one codeword.

The parameters of some codes constructed in a similar way are listed in Table I. The codewords (as w-sets) of a (341,5,1) code with 17 codewords generated from PG(4,4) are listed in Table II. By Theorem 1, this code is optimal.

TABLE I
$(n, w, 1)$-CODES FROM PROJECTIVE GEOMETRY PG(d, q)

w	n	$\lvert C\rvert$	d	q
3	31	5	4	2
3	63	10	5	2
3	127	21	6	2
3	255	42	7	2
3	511	85	8	2
3	1023	170	9	2
3	2047	341	10	2
3	4095	682	11	2
4	40	3	3	3
4	121	10	4	3
4	364	30	5	3
4	1093	91	6	3
4	3280	273	7	3
5	85	4	3	4
5	341	17	4	4
5	1365	68	5	4
5	5461	273	6	4
6	156	5	3	5
6	631	21	4	5
6	3156	105	5	5

TABLE II
CODEWORD SETS OF AN OPTIMAL (341,5,1)-CODE

S_1	0	1	85	21	5
S_2	0	2	170	10	42
S_3	0	3	111	104	53
S_4	0	6	222	106	208
S_5	0	9	268	151	105
S_6	0	11	45	76	198
S_7	0	12	103	75	212
S_8	0	13	305	227	43
S_9	0	15	107	146	164
S_{10}	0	17	264	203	165
S_{11}	0	19	88	267	220
S_{12}	0	22	90	55	152
S_{13}	0	23	293	252	118
S_{14}	0	24	206	83	150
S_{15}	0	25	54	169	221
S_{16}	0	26	269	86	113
S_{17}	0	37	147	217	81

The number of lines in the projective geometry PG(d, q) is

$$\frac{(q^{d+1}-1)(q^{d+1}-q)}{(q^2-1)(q^2-q)} = (q^d-1)n/(q^2-1)$$
$$= n(n-1)/w(w-1).$$

When d is even, then q^2-1 divides q^d-1 without remainder. Furthermore, all orbits are in fact full (shown in Brickell and Wei [3]), and the resulting OOC's are optimal according to Theorem 1. When d is odd, q^2-1 does not divide q^d-1, and at least one incomplete orbit exists. It is shown in Brickell and Wei [3] that there is precisely one incomplete orbit; all other orbits are full. There are $n/(q+1)$ lines in the incomplete orbit, and one of them is $\{0, n/(q+1), 2n/(q+1), \cdots, qn/(q+1)\}$. Only q possible differences exist between pairs of elements of the same line in the incomplete orbit. The number of complete orbits is $(q^d-q)/(q^2-1)$. Therefore, the resulting OOC is also optimal because $\lfloor (n-1)/w(w-1)\rfloor = (q^d-q)/(q^2-1)$. This meets the upper bound in Theorem 1.

Theorem 4:

$$\Phi(n, w, 1) = \left\lfloor \frac{n-1}{w(w-1)} \right\rfloor$$

for $n = (q^{d+1}-1)/(q-1)$ and $w = q+1$, where q is a prime power. Such optimal optical orthogonal codes can be constructed by using a projective geometry.

So far, we have demonstrated how to construct optimal (n, w, λ) codes with $\lambda = 1$ from a projective geometry. We have used certain lines in the projective geometry as codeword w sets. Since any two lines intersect at no more than one point in the projective geometry, the resulting codes satisfy the autocorrelation constraint $\lambda_a = 1$ and the cross-correlation constraint $\lambda_c = 1$. We can also use s spaces in projective geometry, where $s > 1$, to construct codes with $\lambda > 1$.

An s space consists of $(q^{s+1}-1)/(q-1)$ points, and the intersection of two s spaces is at most $(s-1)$ space, which consists of $(q^s-1)/(q-1)$ points. The cyclic shift of an s

space is also an s space. We now generalize the definition of an *orbit* to be a set of s spaces that are cyclic shifts of each other. The size of an orbit necessarily divides n. Construct an (n, w, λ) code with $n=(q^{d+1}-1)/(q-1)$, $w=(q^{s+1}-1)/(q-1)$, and $\lambda=(q^{s}-1)/(q-1)$ from the projective geometry $PG(d,q)$ as follows. Take one representative from each orbit with n members. The discrete logarithm of the points in each representative s space forms a codeword. The codewords form an (n, w, λ) code with the prescribed parameters. That the codewords satisfy the auto- and cross-correlation properties can be easily verified.

E. Combinatorial Methods

Optical orthogonal codes can be constructed by various combinatorial methods. For the case of $\lambda=1$, the problem of constructing OOC's is equivalent to the problem of packing difference sets as illustrated in Fact 3 of Section II. For the case of $w=3$ and $\lambda=1$, we can obtain optimal codes for all $n \not\equiv 2 \pmod 6$.

Theorem 5:

$$\Phi(n,3,1)=\left\lfloor \frac{n-1}{6} \right\rfloor \text{ if } n \neq 2 \pmod 6.$$

We construct optimal $(n,3,1)$ codes satisfying Theorem 5 with codeword sets of the form $S_i=\{0,i,a_i\} \bmod n$. First, assuming $n=6t+1$, we construct t codeword sets of the form $S_i=\{0,i,t+i,x_i\}$, where the x_i are specified in four cases, depending on the value t modulo 4. With few exceptions, $0<x_i<2t-i$, so that $\Delta(S_i)=\pm i, \pm(t+x_i), \pm(t+i+x_i)$ has one member between zero and t and two members between t and $3t$. This regular structure facilitates the construction and validation of the codes.

Case 1: $t=4k$, $k \geq 2$,

$$x_i=\begin{cases} 2k-j, & i=2j, \quad 1 \leq j \leq 2k-1 \\ 6k-1-j, & i=2j+1, \quad 1 \leq j \leq k-2 \\ 6k-j, & i=2j+1, \quad k \leq j \leq 2k-1 \\ 2k, & i=4k \\ 4k, & i=2k-1 \\ 7k-1, & i=1 \end{cases}.$$

Case 2: $t=4k+1$, $k \geq 2$,

$$x_i=\begin{cases} 2k+1-j, & i=2j, \quad 1 \leq j \leq 2k \\ 6k+1-j, & i=2j+1, \quad 1 \leq j \leq k-2 \\ 6k+2-j, & i=2j+1, \quad k \leq j \leq 2k-1 \\ 2k+1, & i=4k+1 \\ 4k+2, & i=2k+1 \\ 7k+1, & i=1 \end{cases}.$$

Case 3: $t=4k+2$, $k \geq 2$,

$$x_i=\begin{cases} 2k+1-j, & i=2j, \quad 1 \leq j \leq 2k \\ 6k+3-j, & i=2j+1, \quad 1 \leq j \leq k-1 \\ 6k+2-j, & i=2j+1, \quad k+1 \leq j \leq 2k \\ 2k+1, & i=4k+2 \\ 6k+4, & i=2k+1 \\ 4k+2, & i=1 \end{cases}.$$

Case 4: $t=4k+3$, $k \geq 2$,

$$x_i=\begin{cases} 2k+2-j, & i=2j, \quad 1 \leq j \leq k+1 \\ 6k+5-j, & i=2j+1, \quad 1 \leq j \leq k-1 \\ 6k+4-j, & i=2j+1, \quad k+1 \leq j \leq 2k \\ 2k+2, & i=4k+3 \\ 6k+6, & i=2k+1 \\ 5k+4, & i=1 \end{cases}.$$

For small values of t, some optimal $(n,3,1)$ codes are given in Table III.

TABLE III
SOME OPTIMAL $(n,3,1)$-CODES

n	Optimal $(n,3,1)$-codes
7	{0,1,3}
13	{0,1,4}, {0,2,7}
19	{0,1,5}, {0,2,8}, {0,3,10}
25	{0,1,6}, {0,2,9}, {0,3,11}, {0,4,13}
31	{0,1,7}, {0,2,11}, {0,3,15}, {0,4,14}, {0,5,13}
37	{0,1,11}, {0,2,9}, {0,3,17}, {0,4,12}, {0,5,18}, {0,6,12}
43	{0,1,19}, {0,2,22}, {0,3,15}, {0,4,13}, {0,5,16}, {0,6,14}, {0,7,17}

To prove that these codes are optimal $(n,3,1)$ codes, we can verify that $\Delta(S_i) \cap \Delta(S_j)=\varnothing$ for every pair of codeword sets S_i and S_j, $i \neq j$. Note $\Delta(S_i)=\{\pm i, \pm(t+x_i), \pm(t+i+x_i)\}$. Since both x_i and $i+x_i$ assume values between 1 and $2t$ (with only one exception), it is straightforward to verify that $\Delta(S_i) \cap \Delta(S_j)=\varnothing$. By the same technique, we can also show that the same sets form optimal $(n,3,1)$ codes even if $n \not\equiv 1 \pmod 6$, provided that $n \not\equiv 2 \pmod 6$. The details are omitted.

F. Block Designs and Algebraic Coding Theory

Another general approach to constructing optimal orthogonal codes is to use a $t-(v,b,\lambda,k,\lambda)$ block design. A $t-(v,b,r,k,\lambda)$ design consists of v objects and b blocks (sets) of these objects, with each object contained in r blocks, each block containing k objects, and each pair of objects contained in λ blocks.

For any such block design, we can use some of the b blocks as codeword sets, each of which has weight k. However, the properties of block design do not immediately imply the intersection of two blocks is small in general. It only guarantees each t subset appears in exactly λ blocks. Due to the "balanced" structure of the design, some block designs have good intersection properties. We can select a collection of blocks from a design and test if the autocorrelation property and cross-correlation property are satisfied for prescribed constraints λ_a and λ_c. If they pass the test, then we have an optical orthogonal code. For the case of $\lambda=1$, the definition of block design implies the intersection of two blocks is at most 1. The codewords in the OOC's will be chosen as the blocks whose cyclic shifts are also blocks. Block designs that are invariant under a cyclic shift are preferred but not required. The relation of block design to OOC's will be explored in an upcoming paper.

As illustrated in Section IV-A, OOC's are equivalent to a special kind of constant-weight codes. Given an (n, w, λ)

optical orthogonal code with m codewords, we can derive an error-correcting code with constant codeword-weight in which each orbit formed by codewords that are cyclic shifts of each other has size n. The sizes of optical orthogonal codes and constant-weight codes are related by

$$n\Phi(n,w,\lambda) \le A(n,2w-2\lambda,w).$$

To construct an (n,w,λ) optical orthogonal code, we examine an $(n,2w-2\lambda,w)$ constant-weight code. Only those codewords whose cyclic shift is also a codeword will be selected. A good $(n,2w-2\lambda,w)$ constant-weight code will then yield a good (n,w,λ) optical orthogonal code. Cyclic constant-weight codes are preferred but not required. The interplay between OOC's and constant-weight codes will also be studied in an upcoming paper.

V. Summary

In this paper we introduced the notion of optical orthogonal codes and addressed their application to a variety of areas in communications. Furthermore, we displayed the rich and fruitful interconnection between optical orthogonal codes and other research areas in combinatorics and algebraic coding theory. This opens up many new and interesting directions for future research.

Acknowledgment

The authors wish to thank Ernie F. Brickell for many helpful discussions. Ernie has constructed another class of optimal $(n,3,1)$ codes similar to that contained in Section IV-E independently. Thanks are also due to Chuck Brackett for illuminating suggestions and to Steve Cheng for organizing the Bell Communications Research Exchange Network Division Open House in which one author's (Salehi) talk, "Code-division multiple access techniques in optical fiber networks," motivated this collaborative work. Interesting discussions with J. Hui, M. O'Connor, and M. Kerner are also acknowledged. Kerner, O'Connor, and Salehi [14] have been working on the problem of computer generation of codes for the multiple-access optical system. The authors also wish to thank the referees for their helpful suggestions.

Appendix

In this Appendix, we give a brief analysis of the performance of a code-division multiple-access optical system which uses optical orthogonal codes. The results presented here are preliminary. They are included to enhance the reader's understanding of the setting of the optical multiple-access system and the advantages of optical orthogonal codes. For a more detailed analysis, the readers are referred to the papers by Salehi and Brackett [2], [22], [23], [25].

Assume that m users are using codewords from an $(n,w,1)$ optical orthogonal code to transmit information over a code-division multiple-access optical channel such as the one shown in Fig. 1. There is no frame synchronization among the users. For the first half of this Appendix, we assume chip synchronism. In the second half, we deal with the chip asynchronous case. The received signal is fed into a tapped delay line for the extraction of information.

We consider two types of detectors. Due to multiple overlapping transmissions, a tap may sense more than one pulse. The two types of detectors differ in their treatment of this situation. In the soft-limiting detector, the contribution of a tap equals the number of pulses it senses. If there are θ or more pulses, it outputs a 1. In the hard-limiting detector, the contribution of a tap is one when it senses one or more pulses and zero otherwise. The detector outputs a 1 when θ or more taps contribute, and a 0 otherwise. The difference between the two types of detectors is best illustrated when a small number of taps on a single delay line are sensing a large number of pulses. The soft-limiting detector will effect a 1 detection, while the hard-limiting type will not. For both types of detectors the number θ is called the *detection threshold*, or just the threshold. In what follows, we analyze the probability P_e of falsely detecting a 0 as a 1 for both types of detector. We assume that no random noise is present in the system. Note that the false detection of a 1 as a 0 is not possible because, when a 1 is transmitted, the threshold is necessarily exceeded and a 1 detection is effected (provided $0 < w$).

Soft-Limiting Detector, Chip Synchronous

If the information bit is 1, it can never be mistaken for a 0. If the information bit is 0, it may be mistaken for a 1 if interfering transmissions from other users are present in the system. We now analyze the probability of this occurring.

Consider the detector for user 1. A pulse from another user sensed by detector 1 is called a hit. A false detection occurs when there are θ or more hits while user 1 is sending 0. The cross-correlation property ensures that each fortuitous user contributes at most 1 hit, and it does so with probability w^2/n independently. Therefore,

$$\begin{aligned}P_e &= \frac{1}{2}\sum_{i=\theta}^{m-1} \Pr\{i \text{ other users are sending } 1\}\\ &\quad\cdot \Pr\{\text{false detection}|i \text{ other users are sending } 1\}\\ &= \sum_{i=\theta}^{m-1} 2^{-m}\binom{m-1}{i}\cdot\sum_{j=\theta}^{i}\binom{i}{j}\left(\frac{w^2}{n}\right)^{j}\left(1-\frac{w^2}{n}\right)^{i-j}.\end{aligned}$$

Algebraic manipulation gives the following alternative formula:

$$P_e = \left(\frac{1}{2}\right)\sum_{i=\theta}^{m-1}\binom{m-1}{i}\left(\frac{w^2}{2n}\right)^{i}\left(1-\frac{w^2}{2n}\right)^{m-1-i}.$$

Hard-Limiting Detector, Chip Synchronous

Assume that user 1 is sending 0, and exactly i other users are sending 1; consider the detector for user 1. A false detection occurs if and only if at least θ active users are contributing hits to different taps on the same delay line. There are $\binom{i}{\theta}$ combinations of θ contributing "hitters," there are $\binom{w}{\theta}$ combinations of θ taps to sense the hits, and there are $\theta!$ pairings between the hitters and the taps. Furthermore, the probability that an active user contributes to a particular tap is w/n. Therefore, the false detection probability is upper-bounded by

$$\begin{aligned}P_e &= \left(\frac{1}{2}\right)\sum_{i=\theta}^{m-1} \Pr\{i \text{ other users are sending } 1\}\\ &\quad\cdot \Pr\{\text{false detection}|i \text{ other users are sending } 1\}\\ &\le \sum_{i=\theta}^{m-1} 2^{-m}\binom{m-1}{i}\binom{i}{\theta}\binom{w}{\theta}\theta!\left(\frac{w}{n}\right)^{\theta}.\end{aligned}$$

Remark on Chip Asynchronous Case

If there is no chip synchronization among the users, the error probability is even lower because the taps are likely to sense only partial pulses contributed by other users, and it becomes harder to reach the detection threshold and to trigger a false detection.

For simplicity of analysis, we assume rectangular pulses that are 50 percent as wide as the duration of a chip (i.e., a 50 percent duty cycle). (A complete analysis is included in [2].) We also assume the height of the pulses is two, so that each pulse has unit area, which corresponds to one unit of energy. Each tap is a device which integrates the photon energy present in a window whose width is half a chip duration. In the soft-limiting detector, the detection of a 1 is effected when the total photon energy integrated by the w taps reaches θ. In the hard-limiting detector, a 1 is detected when the energy integrated by θ or more taps reaches unity. Then the cross-correlation property of optical orthogonal codes implies that, at any given time, a fortuitous user can contribute at most one partial or complete pulse to detector 1. Let $f(x)$ denote the probability density function for a fortuitous user to contribute a pulse intensity x to the detector. Then f contains a delta function at $x=0$, and for the remaining range:

$$f(x) = \Pr\{\text{detector 1 sensing a pulse intensity } x \mid \text{fortuitous user}\}$$

$$= \frac{2w^2}{n}(1-x), \qquad 0 < x \leq 1.$$

The probability of a fortuitous user contributing 0 pulse intensity is $1 - w^2/n$ (i.e., $f(\mathbf{0}) = (1 - w^2/n)\delta(0)$).

Soft-Limiting Detector, Chip Asynchronous

Assume user 1 is sending 0 and exactly i other users are sending 1. Let $x_1, x_2, \cdots, x_i$, $0 \leq x_i \leq 1$, denote the pulse intensity contributed by the i active users. Then a false detection results if and only if $x_1 + x_2 + \cdots + x_i \geq \theta$. Therefore, the false detection probability in this situation is given by the integral

$$P_e = \sum_{i=\theta}^{m-1} 2^{-m}\binom{m-1}{i} \int \cdots \int_{x_1 + \cdots + x_i \geq \theta} \left(\frac{2w^2}{n}\right)^i (1-x_1) \times \cdots (1-x_i)\, dx_1 \cdots dx_i.$$

Hard-Limiting Detector, Chip Asynchronous

For the hard-limiting detector, a 1 detection is effected when θ or more taps sense ≥ 1 pulse intensity. Again, we assume pulses have a 50-percent duty cycle. The correlation properties of OOC's dictate that each fortuitous user can contribute a partial or complete pulse to at most one tap. Therefore, it takes at least two users to trigger one tap, and at least 2θ users to trigger a false detection. Given that user 1 is sending 0 and that exactly i other users are sending 1, there are $\binom{i}{2\theta}\binom{2\theta}{\theta}$ combinations of two groups of θ users each to cause a false detection. There are $\binom{w}{\theta}$ combinations of θ taps to sense the fortuitous pulses, and there are $(\theta!)^2$ ways of matching two "culprit" users (one from each group) to each tap. For any particular tap, the probability of a user contributing a nonzero pulse intensity is w/n. So the probability of two fortuitous users triggering a particular tap is upper-bounded by $(w/n)^2$. Combining all these arguments, error probability is upper-bounded by

$$P_e \leq \sum_{i=2\theta}^{m-1} 2^{-m}\binom{m-1}{i}\binom{i}{2\theta}\binom{2\theta}{\theta}\binom{w}{\theta}(\theta!)^2\left(\frac{w}{n}\right)^{2\theta}.$$

References

[1] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, "Bounds for binary codes of length less than 25," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 81–93, 1978.

[2] J. A. Salehi and C. A. Brackett, "Code division multiple access techniques in optical fiber networks," *IEEE Trans. Commun.*, 1989.

[3] E. F. Brickell and V. Wei, "Optical orthogonal codes and difference families," in preparation.

[4] R. D. Carmichael, *Introduction to the Theory of Groups in Finite Order*. New York: Dover, 1937.

[5] J. P. Costas, "medium constraints on sonar design and performance," in *EASCON Conv. Rec.*, 1975, pp. 68A–68L.

[6] ——, "Time-frequency allocation techniques for active sonar," Generic Electric Tech. Inform. Series, R70EMH13, Syracuse, NY, Feb. 1970.

[7] M. J. E. Golay, "Notes on digital coding," *Proc. IEEE*, vol. 37, p. 657, 1949.

[8] S. W. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 600–604, 1982.

[9] R. L. Graham and F. J. MacWilliams, "On the number of information symbols in difference-set cyclic codes," *Bell Syst. Tech. J.*, vol. 45, pp. 1057–1070, 1966.

[10] M. Hall, Jr., *Combinatorial Theory*, 2nd ed. New York: Wiley, 1986.

[11] T. J. Healy, "Coding and decoding for code division multiple user communication systems," *IEEE Trans. Commun.*, vol. COM-33, pp. 310–316, 1985.

[12] J. Y. Hui, "Pattern code modulation and optical decoding—a novel code-division multiplexing technique for multifiber network," *IEEE J. Sel. Areas Commun.*, vol. SAC-3, pp. 916–927, 1985.

[13] S. M. Johnson, "A new upper bound for error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, 1962.

[14] M. Kerner, M. G. O'Connor, and J. A. Salehi, "Generation and application of multiple access codes for optical fiber systems," presented at SIAM Conf. on Linear Systems, 1986.

[15] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983.

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[17] H. J. Ryser, *Combinatorial Mathematics*. MAA Publication, 1963.

[18] A. A. Shaar and P. A. Davies, "A survey of one-coincidence sequences for frequency-hopping spread-spectrum systems," *Proc. Inst. Elec. Eng., pt. F, Commun. Radar Signal Process.*, vol. 131, pp. 721–724, 1984.

[19] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, 3 vols. Computer Science Press, 1985.

[20] U. Timor, "Multitone frequency-hopped MFSK system for mobile radio," *Bell Syst. Tech. J.*, vol. 61, pp. 3007–3017, 1982.

[21] J. P. Robinson and A. J. Bernstein, "A class of binary recurrent codes with limited error propagation," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 106–113, 1967.

[22] J. A. Salehi and C. A. Brackett, "Fundamental principles of fiber optics code division multiple access (FO-CDMA)," in *Proc. IEEE Int. Conf. Communications*, Seattle, WA, 1987 pp. 1601–1609.

[23] J. A. Salehi and C. A. Brackett, "Principles and applications of nonlinear optical elements in fiber optics code division multiple access networks (FO-CDMA)," in *Proc. IEEE Military Communications Conf.*, McLean, VA, 1987, pp. 848–855.

[24] M. P. Vecchi and J. A. Salehi, "Neuromorphic networks based on sparse optical orthogonal codes," *Neural Information Processing Systems — Natural and Synthetic*, Amer. Inst. Physics, pp. 814–823, 1988.

[25] J. A. Salehi, "Emerging Optical Code-Division Multiple Access Communications Systems," *IEEE Network*, vol. 3, no. 2, pp. 31–39, Mar. 1989.