

A New Recursive Construction for Optical Orthogonal Codes

Wensong Chu, *Member, IEEE*, and Solomon W. Golomb, *Fellow, IEEE*

Abstract—In this correspondence, we present a new recursive construction for $(n, \omega, \lambda_a, \lambda_c)$ optical orthogonal codes. For the case of $\lambda_a = \lambda_c = \lambda$, this recursive construction will enlarge the original family with λ unchanged, and produce a new family of asymptotically optimal codes, if the original family is. We call a code asymptotically optimal, following the definition in [7], if, as n , the length of code goes to infinity, the ratio of the number of codewords to the corresponding Johnson bound approaches unity.

Index Terms—Fiber-optic code-division multiple access, optical orthogonal codes, r -simple matrices.

I. INTRODUCTION

Definition 1: An $(n, \omega, \lambda_a, \lambda_c)$ optical orthogonal code (OOC) \mathcal{C} is a family of $(0, 1)$ sequences of length n and weight ω which satisfy the following two properties.

- 1) The *Autocorrelation Property*:

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

for any $x = \{x_t\}_{t=0}^{n-1} \in \mathcal{C}$ and every integer $\tau, \tau \neq 0 \pmod{n}$. Here \oplus denotes addition mod n .

- 2) The *Cross-Correlation Property*:

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

for any $x = \{x_t\}_{t=0}^{n-1} \in \mathcal{C}, y = \{y_t\}_{t=0}^{n-1} \in \mathcal{C}$ with $x \neq y$ and every integer τ . Here \oplus denotes addition mod n .

If $\lambda_a = \lambda_c = \lambda$, the shorthand notation (n, ω, λ) will be used.

We may also view optical orthogonal codes from a set-theoretical perspective. The following alternative reformulation will be used throughout the rest of this correspondence.

Proposition 1 ([4]): An $(n, \omega, \lambda_a, \lambda_c)$ optical orthogonal code \mathcal{C} is also a family of ω -subsets of Z_n which satisfy the following two properties.

- 1) The *Autocorrelation Property*:

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

for any $X \in \mathcal{C}$ and every $a \not\equiv b \pmod{n}$.

- 2) The *Cross-Correlation Property*:

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

for any $X \in \mathcal{C}$ and $Y \in \mathcal{C}$ with $X \neq Y$ and every $a, b \in Z_n$, where $X + a = \{x \oplus a | x \in X\}$, and \oplus denotes addition mod n .

From Proposition 1, we can derive the following interpretation of the correlation properties as follows.

Manuscript received May 21, 2001; revised July 8, 2003.

W. Chu is with the Department of Computer Science and Engineering, Arizona State University, GWC 206, Tempe, AZ 85287-5406 USA (e-mail: wensong.chu@asu.edu).

S. W. Golomb is with the Communication Sciences Institute, the University of Southern California, Electrical Engineering Systems, EEB 500, Los Angeles, CA 90089 USA (e-mail: milly@mizar.usc.edu).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2003.818387

Theorem 1 ([4]): Let \mathcal{C} be a family of ω -subsets of Z_n . \mathcal{C} is an $(n, \omega, \lambda_a, \lambda_b)$ optical orthogonal code if and only if the following two conditions hold:

- 1) for each $X \in \mathcal{C}$, any nonzero $c \in Z_n$ can be represented as a difference $x - x'$, with $x, x' \in X$ in at most λ_a ways;
- 2) for each pair of $X \in \mathcal{C}$ and $Y \in \mathcal{C}$ with $X \neq Y$, any $c \in Z_n$ can be represented as the difference $x - y$ with $x \in X$ and $y \in Y$, in at most λ_c ways.

It is desired to have a large OOC. For a given set of values of n, ω, λ_a , and λ_c , the largest possible size of an $(n, \omega, \lambda_a, \lambda_c)$ OOC is denoted by $\Phi(n, \omega, \lambda_a, \lambda_c)$.

Definition 2: An $(n, \omega, \lambda_a, \lambda_c)$ code \mathcal{C} is called *optimal* if the number of codewords $|\mathcal{C}| = \Phi(n, \omega, \lambda_a, \lambda_c)$.

Since it is difficult to determine the exact value of $\Phi(n, \omega, \lambda_a, \lambda_c)$ in general, upper bounds for $\Phi(n, \omega, \lambda_a, \lambda_c)$ are of interest. Optical orthogonal codes may also be viewed as constant-weight error-correcting codes in which any two codewords are cyclically distinct. The most general upper bound for $\Phi(n, \omega, \lambda)$ in [4] is therefore derived from the Johnson bound for constant-weight codes, which is as follows.

Theorem 2 ([6]) (Johnson Bound):

$$\Phi(n, \omega, \lambda) \leq \left\lfloor \frac{1}{\omega} \left\lfloor \frac{n-1}{\omega-1} \left\lfloor \frac{n-2}{\omega-2} \left[\dots \left[\frac{n-\lambda}{\omega-\lambda} \right] \dots \right] \right] \right] \right\rfloor.$$

Since [4] was published, optical orthogonal codes have attracted a lot of attention in both the information theory area and the combinatorial design field. Coding theory, finite projective geometry, finite fields and combinatorial design theory play major roles in the studies of OOCs. There are many infinite families of OOCs which have been constructed. Among these families, the most interesting ones are optimal OOCs and asymptotically optimal ones. The concept of *asymptotically optimal* was introduced in [7] as follows.

Definition 3: Let \mathcal{F} be an infinite family of OOCs with $\lambda_a = \lambda_c$. For any (n, ω, λ) OOC $\mathcal{C} \in \mathcal{F}$ containing at least one codeword, the number of codewords in \mathcal{C} is denoted by $M_{(n, \omega, \lambda)}$ and the Johnson bound for (n, ω, λ) OOCs is denoted by $J(n, \omega, \lambda)$. \mathcal{F} is called *asymptotically optimal with respect to the Johnson bound* (in this correspondence, asymptotically optimal is always with respect to the Johnson bound), if the following limit exists and approaches 1:

$$\lim_{n \rightarrow \infty} \frac{M_{(n, \omega, \lambda)}}{J(n, \omega, \lambda)} = 1.$$

The close relationships between OOCs and cyclic t -designs have been investigated in [4], [5], [3], [9]. The so-called *cyclic difference packing* or *difference families* is the main method used in the construction of $(n, \omega, 1)$ OOCs and fruitful results have been obtained from it. In this correspondence, we will give a new recursive construction which can be applied to any $(n, \omega, \lambda_a, \lambda_c)$ OOCs and the asymptotic optimum property is preserved.

II. RECURSIVE CONSTRUCTIONS

A. The Basic Construction

In this section, we present some new recursive constructions for optical orthogonal codes. Several recursive constructions have been presented for $(n, \omega, 1)$ OOCs, for example, [5], [9]. But very few recursive constructions are available for OOCs with $\lambda > 1$. In [4], the following constructions were presented.

Theorem 3 ([4]) :

- 1) Given an $(n, \omega, \lambda_a, \lambda_c)$ code \mathcal{C} , then \mathcal{C} is also an $(n, \omega, \lambda'_a, \lambda'_c)$ code for $\lambda'_a \geq \lambda_a$ and $\lambda'_c \geq \lambda_c$.
- 2) Given an $(n, \omega, \lambda_a, \lambda_c)$ code \mathcal{C} with m codewords, there exists an $(n, 2\omega - 2\lambda_c, 2\lambda_a + 2\lambda_c, \omega + 3\lambda_c)$ code \mathcal{C}' with $\binom{m}{2}$ codewords.
- 3) Given an $(n, \omega, \lambda_a, \lambda_c)$ code \mathcal{C} and a positive integer t , there exists a $(tn, t\omega, t\lambda_a, t\lambda_c)$ code \mathcal{C}' with the same number of codewords.

Remark 1: All the constructions of Theorem 3 enlarge the values of λ_a and λ_c . Given an $(n, \omega, \lambda_a, \lambda_c)$ code \mathcal{C} , we hope that recursive constructions will have the following properties.

- 1) The codes resulting from recursive constructions have the values of λ_a and λ_c as small as possible. In particular, the recursive constructions should keep these two values unchanged.
- 2) If \mathcal{C} is optimal, the new code resulting from recursive constructions should be optimal too, or at least “close” to optimal.

In this section, making use of so-called *r-simple* matrices, we present several new recursive constructions which will keep the values of λ_a and λ_c unchanged, and give new codes “close” to optimal if an original code is optimal with $\lambda_a = \lambda_c$. In this correspondence, “close” means asymptotically optimum.

Definition 4: Let G be an Abelian group of size n . Let r be a positive integer. An $s \times t$ matrix $A = (a_{ij})$ over G is called *r-simple*, if the difference of any two column vectors of A contains any element in G at most $r - 1$ times.

In this correspondence, we only make use of *r-simple* matrices over a cyclic group G . In most cases, we take $G = Z_g$.

Theorem 4: (The Basic Construction): Let \mathcal{C} be an $(n, \omega, \lambda_a, \lambda_c)$ OOC. If there exists an $\omega \times N$ *r-simple* matrix over Z_g , then there exists an $(ng, \omega, \lambda_a, \max\{\lambda_a, \lambda_c, r - 1\})$ OOC \mathcal{C}' with $|\mathcal{C}'| = N|\mathcal{C}|$, where $|\mathcal{C}'|$ and $|\mathcal{C}|$ denote the number of codewords in the new and original codes, respectively.

Proof: Let $\mathcal{C} = \{C_i | 1 \leq i \leq |\mathcal{C}|\}$ be the family of codewords with the parameters $(n, \omega, \lambda_a, \lambda_c)$, where $C_i = \{b_{i1}, b_{i2}, \dots, b_{i\omega}\}$ with $b_{ij} \in Z_n$ and $1 \leq i \leq |\mathcal{C}|$, $1 \leq j \leq \omega$. Here we use set-theoretical notation.

Let $D = (d_{ij})$ with $1 \leq i \leq \omega$ and $1 \leq j \leq N$ be the *r-simple* matrix over Z_g .

Let $C_i = \{b_{i1}, b_{i2}, \dots, b_{i\omega}\}$ be a codeword from \mathcal{C} . Construct the following N new codewords as follows:

$$F_{il} = \{b_{ij} + nd_{jl} | 1 \leq j \leq \omega\}$$

where $1 \leq l \leq N$ and the addition is taken in Z_{ng} .

Let $\mathcal{C}' = \{F_{il} | 1 \leq i \leq |\mathcal{C}|, 1 \leq l \leq N\}$. Then \mathcal{C}' is the desired $(ng, \omega, \lambda_a, \max\{\lambda_a, \lambda_c, r - 1\})$ OOC. To prove the claim, we need to check the autocorrelation and cross-correlation properties.

For any codeword $C_i \in \mathcal{C}$, any integer $c \neq 0$ in Z_n can be represented as $x - x'$ with $x, x' \in C_i$ in at most λ_a ways. Now, for any codeword F_{il} in \mathcal{C}' , any difference $b_{ij_1} + nd_{j_1l} - b_{ij_2} - nd_{j_2l}$ can occur at most λ_a times, as this difference is congruent to $b_{ij_1} - b_{ij_2}$ modulo n , which occurs at most λ_a times.

To check the cross-correlation property, we need to verify two cases.

- Case 1) First we check the cross-correlation between $F_{i_1l_1}$ and $F_{i_2l_2}$ with $i_1 \neq i_2$. This means that these two codewords are constructed based on different codewords in \mathcal{C} .

Suppose we have these two codewords as follows:

$$\begin{aligned} F_{i_1l_1} &= \{b_{i_1j} + nd_{j_1l_1} | 1 \leq j \leq \omega\} \\ F_{i_2l_2} &= \{b_{i_2j} + nd_{j_2l_2} | 1 \leq j \leq \omega\}. \end{aligned}$$

Notice that any difference

$$\begin{aligned} (b_{i_1j_1} + nd_{j_1l_1}) - (b_{i_2j_2} + nd_{j_2l_2}) \\ = b_{i_1j_1} - b_{i_2j_2} \pmod{n}. \end{aligned}$$

Thus, it can occur at most λ_c times in Z_{ng} , as it cannot occur more than λ_c times in Z_n .

- Case 2) The cross-correlation value between $F_{i_1l_1}$ and $F_{i_2l_2}$ possibly becomes larger than λ_c , when these are constructed based on a same codeword in \mathcal{C} .

Suppose these two codewords are as follows:

$$\begin{aligned} F_{i_1l_1} &= \{b_{ij} + nd_{j_1l_1} | 1 \leq j \leq \omega\} \\ F_{i_2l_2} &= \{b_{ij} + nd_{j_2l_2} | 1 \leq j \leq \omega\}. \end{aligned}$$

Consider any difference $(b_{ij_1} + nd_{j_1l_1}) - (b_{ij_2} + nd_{j_2l_2})$ between them. If $j_1 \neq j_2$, then the same argument indicates that such a difference cannot occur more than λ_a times. If $j_1 = j_2$, then the difference

$$(b_{ij_1} + nd_{j_1l_1}) - (b_{ij_2} + nd_{j_2l_2}) = n(d_{j_1l_1} - d_{j_2l_2}).$$

With the help of the assumption that the difference matrix D is *r-simple*, we know that such a difference cannot occur more than $r - 1$ times. Combining all the cases, the value of the cross-correlation between $F_{i_1l_1}$ and $F_{i_2l_2}$ is no more than $\max\{\lambda_a, \lambda_c, r - 1\}$.

Thus, we have proved the Basic Construction according to Theorem 1. \square

In fact, we can do a little bit better than the Basic Construction by adding more codewords into the new code under some circumstances.

Corollary 1: In addition to the conditions in the Basic Construction, if furthermore there exists a $(g, \omega, \lambda_a, \lambda_c)$ OOC with t codewords, then there exists an $(ng, \omega, \lambda_a, \max\{\lambda_a, \lambda_c, r - 1\})$ OOC with t more codewords than in the Basic Construction.

Proof: Let $\mathcal{H} = \{H_1, H_2, \dots, H_t\}$ be the $(g, \omega, \lambda_a, \lambda_c)$ OOC. For any $H_i = \{h_{i1}, h_{i2}, \dots, h_{i\omega}\}$, construct a new codeword as

$$nH_i = \{nh_{i1}, nh_{i2}, \dots, nh_{i\omega}\} \pmod{ng}.$$

Adding these t new codewords into \mathcal{C}' , we get a code with t more codewords.

To verify that this is the desired code, we only need to check the cross-correlation between nH_i and any codeword F_{jl} constructed by the Basic Construction. Let $nH_i = \{nh_{i1}, nh_{i2}, \dots, nh_{i\omega}\}$ and $F_{jl} = \{b_{j1}, b_{j2}, \dots, b_{j\omega}\}$. Suppose that two differences between nH_i and F_{jl} are equal, say $nh_{i1} - b_{j1} = nh_{i2} - b_{j2}$. It implies that $j_1 = j_2$ and $i_1 = i_2$. So any difference between nH_i and F_{jl} cannot occur more than once. \square

B. *r-Simple Matrices*

To make use of the Basic Construction, we need to construct some *r-simple* matrices. Here, we present a construction based on finite fields.

Lemma 1: Let p be a prime and $f(x)$ be a polynomial in $\text{GF}(p)[x]$. Define a $p \times p$ array $D = (d_{ij})$ with $d_{ij} = ij + f(i)$, $0 \leq i, j \leq p - 1$. Then D is a 2-simple matrix over Z_p .

Proof: Suppose $0 \leq j_1 \neq j_2 \leq p-1$. We need to show that the multiset $\{d_{ij_1} - d_{ij_2} | 0 \leq i \leq p-1\}$ contains every element in $\text{GF}(p)$ no more than once, i.e., exactly once in this case

$$d_{ij_1} - d_{ij_2} = ij_1 + f(i) - ij_2 - f(i) = (j_1 - j_2)i.$$

Notice that $j_1 \neq j_2$ implies that $\{(j_1 - j_2)i | 0 \leq i \leq p-1\}$ contains each element of Z_p exactly once. \square

Now we are ready to give a construction of a $p \times p^{r-1}$ r -simple matrix over Z_p for any prime p , with $r \geq 3$. We start from $r = 3$, as $r = 2$ can be obtained from Lemma 1.

Theorem 5: Let $3 \leq r \leq p$ be an integer, and p be an odd prime. Let

$$\mathcal{F} = \left\{ f(x) = \sum_{i=2}^{r-1} a_i x^i \mid a_i \in \text{GF}(p), 2 \leq i \leq r-1 \right\}$$

be a family of p^{r-2} polynomials over $\text{GF}(p)$. Define $D_{f(x)} = (d_{ij}^{f(x)})$ with $d_{ij}^{f(x)} = ij + f(i)$, ($1 \leq i, j \leq p$), for any $f(x) \in \mathcal{F}$. Then

$$\mathcal{D} = (D_{f(x)} \mid f(x) \in \mathcal{F})$$

is an r -simple matrix over Z_p , where \mathcal{D} is a $p \times p^{r-1}$ array consisting of all $D_{f(x)}$'s with $f(x) \in \mathcal{F}$.

Proof: Notice that $|\mathcal{F}| = p^{r-2}$. So \mathcal{D} is a $p \times p^{r-1}$ matrix. To prove the conclusion, we only need to show it is r -simple.

Based on the above lemma, $D_{f(x)}$ is 2-simple, so we only need to look at any pair of columns from $D_{f(x)}$ and $D_{g(x)}$ with $f(x) - g(x) \neq 0$ over $\text{GF}(p)[x]$. Take the j_1 th column from $D_{f(x)}$ and the j_2 th from $D_{g(x)}$ and consider the difference between their i th elements

$$\begin{aligned} d_{ij_1}^f - d_{ij_2}^g &= ij_1 + f(i) - ij_2 - g(i) \\ &= i(j_1 - j_2) + f(i) - g(i). \end{aligned}$$

Note that $2 \leq \deg(f(x) - g(x)) \leq r-1$. So for all $c \in \text{GF}(p)$, the equation

$$c = d_{ij_1}^f - d_{ij_2}^g = i(j_1 - j_2) + f(i) - g(i)$$

has no more than $r-1$ solutions. \square

Combining Theorem 5 and Lemma 1, we have the following result.

Corollary 2: For any prime p and integer r with $2 \leq r \leq p$, there exists a $p \times p^{r-1}$ r -simple matrix over Z_p .

Example 1: Let $p = 3$ and $r = 3$. There exists a 3-simple matrix over Z_3 as follows:

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

To get r -simple matrices with other dimensions, we need the following product constructions.

Theorem 6 (Product Construction): Let $A = (a_{ij})$ be an $m \times n$ r -simple matrix over Z_s and $B = (b_{ij})$ be an $m \times k$ r -simple matrix over Z_t . Then there exists an $m \times nk$ r -simple matrix over Z_{st} .

Proof: For any column of A , say the i th column $\alpha_i = (a_{1i}, a_{2i}, \dots, a_{mi})^T$, construct the following $m \times k$ matrix:

$$H_i = \begin{pmatrix} a_{1i} + sb_{11} & a_{1i} + sb_{12} & \cdots & a_{1i} + sb_{1k} \\ a_{2i} + sb_{21} & a_{2i} + sb_{22} & \cdots & a_{2i} + sb_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{mi} + sb_{m1} & a_{mi} + sb_{m2} & \cdots & a_{mi} + sb_{mk} \end{pmatrix}.$$

We claim that

$$H = (H_1, H_2, \dots, H_n)$$

is the desired r -simple matrix.

To prove the claim, we notice the following two facts.

- 1) $\forall i$, H_i is an r -simple matrix over Z_{st} , as it is noticed that the difference of any two columns of H_i is s times the difference of corresponding two columns of matrix B and the r -simplicity of B guarantees the r -simplicity of H_i .
- 2) Now we take two columns from H_i and H_j with $i \neq j$, respectively. The difference vector of these two columns after modulo s operations is equal to the difference of the i th column and j th column. Then r -simplicity of A guarantees that there are at most $r-1$ repeated values in the difference vector.

Combining these two facts, we have proved our claim. \square

The r -simple matrices can be viewed as a generalization of another well-studied type of combinatorial matrices, so-called *difference matrices*. We have found that r -simple matrices have other applications in sequence designs for communications. For a detailed treatment of basic properties, bounds, relationships with difference matrices and orthogonal arrays, constructions and applications, refer to [2].

C. Asymptotically Optimal Recursive Constructions

Now we present a new recursive construction based on the Basic Construction and the product construction for r -simple matrices, for all the OOCs with $\lambda_a = \lambda_c = \lambda$.

Theorem 7: (Construction A): Suppose there exists an (n, ω, λ) OOC with T codewords. Let p be a prime not less than ω . Then there exists an (np, ω, λ) OOC with Tp^λ codewords.

Proof: By Theorem 5 and its corollary, there exists a $p \times p^\lambda$ $(\lambda+1)$ -simple matrix \mathcal{D} over Z_p . Take the first ω rows of \mathcal{D} . Then we have an $\omega \times p^\lambda$ $(\lambda+1)$ -simple matrix over Z_p . Thus, the conclusion follows from the Basic Construction. \square

Corollary 3: Suppose there exists an (n, ω, λ) OOC with T codewords. Let $m = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ be a positive integer, where the p_i 's with $1 \leq i \leq t$ are primes not less than ω . Then there exists an (mn, ω, λ) OOC with Tm^λ codewords.

Proof: Apply Construction A to the (n, ω, λ) OOC several times with appropriate $(\lambda+1)$ -simple matrices. Or we can first construct an $\omega \times m^\lambda$ $(\lambda+1)$ -simple matrix over Z_m via the product construction for r -simple matrices, then apply the Basic Construction to get the desired OOC. \square

Example 2: The following code is a $(63, 9, 2)$ optimal OOC from [3]:

$$\begin{aligned} &\{1 \quad 5 \quad 8 \quad 18 \quad 28 \quad 31 \quad 35 \quad 40 \quad 59\} \\ &\{2 \quad 7 \quad 10 \quad 16 \quad 17 \quad 36 \quad 55 \quad 56 \quad 62\} \\ &\{3 \quad 11 \quad 24 \quad 25 \quad 27 \quad 29 \quad 30 \quad 43 \quad 51\} \\ &\{4 \quad 9 \quad 14 \quad 20 \quad 32 \quad 34 \quad 47 \quad 49 \quad 61\} \\ &\{6 \quad 22 \quad 23 \quad 39 \quad 48 \quad 50 \quad 54 \quad 58 \quad 60\} \\ &\{12 \quad 15 \quad 33 \quad 37 \quad 44 \quad 45 \quad 46 \quad 53 \quad 57\} \end{aligned}$$

By Construction A, we can construct a $(63 \times 11, 9, 2)$ OOC with $6 \times 121 = 726$ codewords, if we take a 9×121 3-simple matrix over Z_{11} . The Johnson bound for $\Phi(63 \times 11, 9, 2)$ is 948.

This recursive construction satisfies the first requirement in Remark 1. Unfortunately, in general it does not give any new optimal OOCs, even if the original one is. It is possible to get optimal OOCs

under some circumstances with $\lambda = 1$. We will discuss this in a later section. However, it does preserve the asymptotic optimum property.

Theorem 8: Let \mathcal{F} be an infinite family of asymptotically optimal OOCs with respect to the Johnson bound. Then there exists an infinite family \mathcal{F}^* of asymptotically optimal OOCs with the property that for any (n, ω, λ) OOC $\mathcal{C} \in \mathcal{F}$ with T codewords, and for any positive integer m of which all prime factors are not less than ω , there exists an (mn, ω, λ) OOC $\mathcal{C}^* \in \mathcal{F}^*$ with Tm^λ codewords.

Proof: The existence of the family \mathcal{F}^* follows from Corollary 3. We only need to show \mathcal{F}^* is asymptotically optimal with respect to the Johnson bound. Notice that

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{Tm^\lambda}{J(mn, \omega, \lambda)} &= \lim_{n \rightarrow \infty} \frac{m^\lambda T J(n, \omega, \lambda)}{J(mn, \omega, \lambda) J(n, \omega, \lambda)} \\ &= \lim_{n \rightarrow \infty} \frac{m^\lambda J(n, \omega, \lambda)}{J(mn, \omega, \lambda)} \lim_{n \rightarrow \infty} \frac{T}{J(n, \omega, \lambda)} \\ &= 1. \end{aligned}$$

Thus, the conclusion follows from the definition of asymptotically optimal OOCs. \square

III. SOME FAMILIES OF ASYMPTOTICALLY OPTIMAL OPTICAL ORTHOGONAL CODES

In this section, we will apply Construction A to some known families of asymptotically optimal OOCs. In the first subsection, the case of $\lambda = 1$ is treated; the second subsection is devoted to the case of $\lambda > 1$; the last subsection contains some further discussions on the Basic Construction and Construction A.

A. OOCs With $\lambda = 1$

The $(n, \omega, 1)$ OOCs have been most extensively studied in recent decades. Many infinite families of optimal OOCs have been constructed, in particular for small values of ω . Here, we only want to show one example of them, due to Singer [8], under the name of *cyclic difference sets*.

Theorem 9 ([8]): For any prime power q , there exists an optimal $(q^2 + q + 1, q + 1, 1)$ OOC.

Remark 2: Strictly speaking, for any prime power q , the $(q^2 + q + 1, q + 1, 1)$ OOC is a $(q^2 + q + 1, q + 1, 1, 0)$ OOC, as it has only one codeword.

Applying Construction A, the following corollary follows.

Theorem 10: For any prime power q , there exists an $(m(q^2 + q + 1), q + 1, 1)$ OOC, where m is a positive integer whose prime divisors are greater than q . This family is asymptotically optimal as $q \rightarrow \infty$.

In fact, for some special values of m , we can obtain optimal OOCs which were first presented in [1].

Corollary 4 ([1]):

$$\phi(m(q^2 + q + 1), q + 1, 1) = m, \quad \text{if } q < m < q^2 + q + 1$$

where m is a positive integer with prime divisors greater than q .

Furthermore, if we apply the corollary of the Basic Construction (Corollary 1), we can get another optimal family of OOCs under certain circumstances.

Corollary 5: Let q be any prime power. If all prime divisors of $q^2 + q + 1$ are bigger than q , then there exists an optimal $((q^2 + q + 1)^t, q + 1, 1)$ OOC for every positive integer t .

Proof: We will prove this by induction. It is true for $t = 1$. Suppose there exists an optimal $((q^2 + q + 1)^t, q + 1, 1)$ OOC \mathcal{C} . Counting the codewords of \mathcal{C} , we have the following:

$$|\mathcal{C}| = \frac{(q^2 + q + 1)^t - 1}{q(q + 1)} = \sum_{i=0}^{t-1} (q^2 + q + 1)^i.$$

According to the factorization of $q^2 + q + 1$, we can apply Construction A to \mathcal{C} several times, with the appropriate 2-simple matrices, and get a new OOC, \mathcal{C}' . Noticing that there exists an optimal $(q^2 + q + 1, q + 1, 1)$ OOC, we can further make use of Corollary 1 and add one more codeword to \mathcal{C}' . Finally

$$|\mathcal{C}'| = |\mathcal{C}|(q^2 + q + 1) + 1 = \frac{(q^2 + q + 1)^{t+1} - 1}{q(q + 1)}.$$

It is easy to see that $|\mathcal{C}'|$ is equal to the Johnson bound for $((q^2 + q + 1)^{t+1}, q + 1, 1)$ OOCs, so it is an optimal OOC. \square

B. Optical Orthogonal Codes With $\lambda > 1$

In this subsection, we will review some known families of asymptotically optimal (n, ω, λ) optical orthogonal codes with $\lambda > 1$ and extend them by Construction A.

The first infinite family of optimal OOCs with $\lambda = 2$ came from an elegant construction in [3].

Theorem 11 ([3]): Let p be a prime, and m an integer ≥ 1 . Then there exists an optimal $(p^{2m} - 1, p^m + 1, 2)$ OOC with $p^m - 2$ codewords.

Corollary 6: Let p be a prime, m be an integer ≥ 1 , and t be any integer all of whose prime divisors exceed p^m . Then there exists a $(t(p^{2m} - 1), p^m + 1, 2)$ OOC with $t^2(p^m - 2)$ codewords. This family is asymptotically optimal as $p \rightarrow \infty$.

In [7], three families of asymptotically optimal OOCs were presented.

Theorem 12 ([7]):

- 1) Let p be any prime number, m any divisor of $p - 1$, and t any integer, $1 \leq T \leq M$. Then there exists a (pm, m, t) OOC with

$$\frac{1}{pm} \left(\sum_{d|(p-1)} \mu(d) (p^{\lceil (t+1)/d \rceil} - 1) \right)$$

codewords. This family is asymptotically optimal as $m \rightarrow \infty$.

- 2) Let p be any prime number and α, t be natural numbers, $\alpha \geq 2$, $1 \leq t < p - t$. Then there exists a $(p(p^\alpha - 1), p - t, t)$ OOC with $p^{\alpha-1}(p^{t\alpha-1} - 1)/(p^\alpha - 1)$ codewords. This family is asymptotically optimal as $p \rightarrow \infty$ and t is fixed.
- 3) Let $q = p^s$ where $s \geq 1$ and p is any prime number. Let m and $q + 1$ be relatively prime, and t be any integer with $1 \leq t \leq m/2$. Then there exists a $((q + 1)m, m, 2t)$ OOC with $M/m(q + 1)$ codewords, where M is defined as follows:

$$M = \begin{cases} q^{2t+1} - q, & t = 1, 2, 3, 4, 5, 6 \\ \geq q^{2t+1} - \frac{1}{7}q^{2t-6}, & t \geq 7. \end{cases}$$

Furthermore, this family is asymptotically optimal as $m \rightarrow \infty$ and t is fixed.

Based on Construction A, we can construct three new families of asymptotically optimal OOCs. The three new families are much larger than the original ones and are asymptotically optimal with respect to the Johnson bound. We omit the details here.

C. Discussion

With the Basic Construction and Construction A, it is no longer difficult to get some families of OOCs. The following is an example.

Theorem 13: Let q be any prime power, n any positive integer, and m any positive integer whose prime divisors are not less than $\frac{q^n-1}{q-1}$. Then there exists an

$$\left(m \frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1} \right).$$

OOC with $m^{(q^{n-1}-1)/(q-1)}$ codewords.

Proof: For any prime power q , there exists a

$$\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1} \right)$$

OOC with one codeword ([8]). The conclusion then follows from Construction A. \square

If we apply the Basic Construction directly, we can get some families of OOCs with $\lambda_a \neq \lambda_c$. Here is another example.

Example 3: Let q be any prime power, and let m be any positive integer whose prime divisors are bigger than q . Then there exists an $(m(q^2+q+1), q+1, 1, 2)$ OOC with m^2 codewords.

Proof: For any prime power q , there exists a $(q^2+q+1, q+1, 1, 0)$ OOC with one codeword. According to the factorization of m , apply corresponding 3-simple matrices. By the Basic Construction, the desired code is obtained. \square

The above examples show that it is easy to get some families of OOCs. However, none of the above examples is optimal or asymptotically optimal.

IV. CONCLUSION

In this correspondence, we presented a new recursive construction (The Basic Construction) for OOCs. From the Basic Construction, we obtained Construction A for (n, ω, λ) OOCs. With Construction A, we extended some known families of asymptotically optimal OOCs, and the resulting new families are much larger than the original ones and are still asymptotically optimal.

A major question about the Basic Construction is how far it is from obtaining new optimal OOCs if the original families are. In fact, it is really possible to get some optimal families if we modify the Basic Construction under certain circumstances. We are currently preparing another paper to deal with this issue.

Furthermore, with the Basic Construction in hand, we need to find additional direct constructions of optimal or asymptotically optimal OOCs. This is a subject for future work.

ACKNOWLEDGMENT

The first author would like to thank Dr. Habong Chung for his helpful discussions and suggestions in the early stages of this correspondence. Both authors also wish to thank the referees for valuable suggestions.

REFERENCES

- [1] C. Zhi, F. Pingzhi, and J. Fan, "Disjoint difference sets, difference triangle sets and related codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 518–522, Mar. 1992.
- [2] W. Chu, "Optical Orthogonal Codes and Cyclic t -designs," Ph.D. dissertation, Univ. So. Calif., Los Angeles, 2002.
- [3] H. Chung and P. V. Kumar, "Optical orthogonal codes—New bounds and an optimal construction," *IEEE Trans. Inform. Theory*, vol. 36, pp. 866–873, July 1990.

- [4] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis and applications," *IEEE Trans. Inform. Theory*, vol. 35, pp. 595–604, May 1989.
- [5] R. Fuji-Hara and Y. Miao, "Optical orthogonal codes: Their bounds and new optimal constructions," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2396–2406, Nov. 2000.
- [6] S. M. Johnson, "A new upper bound for error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, Apr. 1962.
- [7] O. Moreno, Z. Zhang, and P. V. Kumar, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 448–455, Mar. 1995.
- [8] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *AMS Trans.*, vol. 43, pp. 377–385, 1938.
- [9] J. Yin, "Some combinatorial constructions for optical orthogonal codes," *Discr. Math.*, vol. 185, pp. 201–219, 1998.

Capacity and Decoding Rules for the Poisson Arbitrarily Varying Channel

Shraga I. Bross, *Member, IEEE*, and
Shlomo Shamai (Shitz), *Fellow, IEEE*

Abstract—The single-user and two-user (multiple-access) Poisson arbitrarily varying channel (AVC) with input and state (peak and average-power) constraints, but unlimited in bandwidth, are considered. For both cases, the deterministic and random code capacity with the average probability of error criterion is obtained. In the single-user case, Wyner's [21] decoder attains the deterministic-code capacity whereas for the two-user case, a "nearest neighbor" decoder that belongs to the class of β -decoders introduced in [8] is shown to attain the deterministic-code capacity region as claimed.

Index Terms—Arbitrarily varying channel (AVC), deterministic-code capacity, Poisson channels.

I. INTRODUCTION

The discrete memoryless arbitrarily varying channel (AVC) models a communication scenario in which a channel parameter may vary with time without memory in an arbitrary and unknown manner during the transmission of a codeword. In this correspondence, it is assumed that the sequence of channel states is selected arbitrarily subject to a constraint—the state average-power constraint, and possibly depending on the codebook (as the state generator is assumed to be cognizant of the code) but independently of the codeword actually sent.

AVC's capacity depends on whether or not random codes are permitted, and whether the average or the maximum probability of error criterion is used. The random coding capacity admits a simple characterization as a min-max of mutual information, unfortunately random codes are not always implementable.

Unless stated otherwise, the term capacity will hereafter always refer to the capacity for *deterministic codes* and the *average probability of error criterion* (random-code capacity is the same under both criteria only in the single-user case). In the absence of state constraints,

Manuscript received September 21, 2000; revised November 6, 2002. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Washington, DC, June 2001.

The authors are with the Department of Electrical Engineering, Technion—Israel Institute of Technology, Haifa 32000, Israel (e-mail: shraga@ee.technion.ac.il; sshlomo@ee.technion.ac.il).

Communicated by P. Narayan, Associate Editor for Shannon Theory. Digital Object Identifier 10.1109/TIT.2003.818385