Optical Orthogonal Codes with Unequal Auto- and Cross-Correlation Constraints

Guu-Chang Yang , Member , IEEE
And
Thomas E. Fuja , Member ,IEEE

IEEE Transactions on Information Theory
Vol.41 No.1 Page:96~106
January 1995

NCTU Dep. of Communication Engineering
Reporter: Chi-Kai Liang u8625038

1

OOC (optical orthogonal code) is a collection of binary sequences with good auto- and cross-correlation properties ; they were defined by Salehi and others as a means of obtaining CDMA on optical network.

Before 1995,all work on OOC's have assumed that the constraint placed on the auto-correlation and that placed on the cross-correlation are the same.

In this paper we consider codes for which the two constraint are not equal !

Goal：

Develop bounds on the size of such OOC's and demonstrate construction techniques for building them.

The results demonstrate that a significant increase in the code size is possible by letting the auto-correlation constraint **exceed** the cross-correlation constraint.

These results suggest that for a given performance requirement the optimal OOC may be one with *unequal constraint*.

2

Definitions and past work：

An (n,w, λ_a,λ_c) optical orthogonal code C is a collection of binary n-tuples,each of Hamming weight w：

- Autocorrelation: for any x =[χ_0,…,χ_{n-1}]∈ C and any integer τ ,0< τ <n

$$\sum_{t=0}^{n-1} \chi_t \chi_{t\oplus\tau} \le \lambda_a$$

- Cross-correlation: for any x=[χ_0,…,χ_{n-1}]∈ C and any integer τ ,0< τ <n and any y=[y_0,…,y_{n-1}]∈ C such that x≠y ,any integer τ

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

3

Alternate Definition：

- Autocorrelation：for any x∈ C , $d^a_{\min}(x) \ge 2w-2\lambda_a$,where $d^a_{\min}(x)$ is min. distance between x and its cyclic shifts

  ----i.e. $d^a_{\min}(x) \equiv \min\{d_H(x, D^\tau x): \tau = 1,2,\ldots,n-1\}$

- Cross-correlation： for any x∈ C ,and for any y∈ C , $d^a_{\min}(x,y) \ge 2w-2\lambda_c$ where

  $$d^a_{\min}(x,y) \equiv \min\{d_H(x, D^\tau y): \tau = 1,2,\ldots,n-1\}$$

Partition the binary n-tuples into “clouds”,where every cloud consists cyclic shift of the same n-tuples. Then constructing an OOC consists of picking at most one n-tuples from every cloud under two constraints;

The first constraint specifies the min. Hamming distance ‘*within*’ a cloud;

The second specifies the min. Hamming distance ‘*between*’ clouds.

4

IF two constraints are equal---i.e. $\lambda_a = \lambda_c = \lambda$ ----then an OOC,represents a constant-weight cyclic error-correcting code with min. distance 2w-2 λ .

- Consider $\lambda_a \neq \lambda_c$:

  The auto-correlation constraint guarantees that each signature sequences is unlike cyclic shifts of itself,and this property enables the receiver to obtain "synchronization".

  The cross-correlation constraint guarantees that each signature sequences is unlike cyclic shifts of the other signature sequences .and this property enables the receiver to estimate its message in the presence of interference from other users.

  So,the auto-correlation constraint contributes only to synchronization,while the other signature sequences affects both synchronization and operation.

  Taking these as our performance criteria,we see why "asymmetric" OOC's

  ---i.e.codes with $\lambda_a \neq \lambda_c$ ----might be preferable to "symmetric" codes.

  ---If we compare (for instance) an $(n, w+m, \lambda+m, \lambda)$ OOC with either an (n, w, λ, λ) code or an $(n, w+m, \lambda+m, \lambda+m)$ code,we see the asymmetric code is more robust.

5

Definition and preliminary results：

Define $\Phi(n, w, \lambda_a, \lambda_c)$ to be the cardinality of an optimal OOC with the given parameters,

$$\Phi(n, w, \lambda_a, \lambda_c) \equiv \max\{|C|: C \text{ is an } (n, w, \lambda_a, \lambda_c) \text{ OOC}\}$$

Let $x=[x_0, x_1, \ldots . x_{n-1}]$ be a binary n-tuple of weight w ; assume $x_{j0} = x_{j1} = \ldots = x_{jw-1} = 1$ The adjacent relative delay vector associates with x is denoted

$$t_x = [t_1, t_2, \ldots . t_{w-1}]$$

and is defined by

$$t_i = \begin{cases} j_{i+1} - j_i & , for\ i = 0,1,\ldots, w-2 \\ n + j_0 - j_{w-1} & \end{cases}$$

EX: x = [1001100010000] ,then $t_x = [t_0, t_1, t_2, t_3] = [3,1,4,5]$

6

For any $x \in \{0,1\}^n$ and any integer $\lambda(1 \le \lambda \le w-1)$ let $M_{x,\lambda}$ be the set of integer λ-tuples given by

$$M_{x,\lambda} = \{[\sum_{k_0=0}^{i_0} t_{j \cup k_0}, \sum_{k_1=i_0+1}^{i_1} t_{j \cup k_1}, \sum_{k_2=i_1+1}^{i_2} t_{j \cup k_2}, \cdots\cdots, \sum_{k_{\lambda-1}=i_{\lambda-2}+1}^{i_{\lambda-1}} t_{j \cup k_{\lambda-1}},]:$$

$$0 \le i_0 < i_1 < \ldots < i_{\lambda-1} \le w-2 \ , \ j = 0,1,\ldots\ldots,w-1\}$$

Lemma1：let $x=[x_0,x_1,\ldots,x_{n-1}]$ be a binary n-tuples.Then the inequality

$$\sum_{t=0}^{n-1} \chi_t \chi_{t \oplus \tau} \le \lambda$$

holds for $1 \le \tau \le n-1$ if and only if no component of Rx appears more than times.

Lemma2：let $x=[x_0,x_1,\ldots,x_{n-1}]$ and $y=[y_0,y_1,\ldots,y_{n-1}]$ be binary n-tuples. Then the inequality $\sum_{t=0}^{n-1} \chi_t y_{t \oplus \tau} \le \lambda$

holds for all $0 \le \tau \le n-1$ if and only if $M_{x,\lambda}$ and $M_{y,\lambda}$ are disjoint.

Lemma3：let $x=[x_0,x_1,\ldots,x_{n-1}]$ be binary n-tuples. Then the inequality

$\sum_{t=0}^{n-1} x_t x_{t \oplus \tau} \le \lambda$ holds for all $\tau = 0,1,\ldots\ldots,n-1$ if and only if $|M_{x,\lambda}| = w$.

- Upper bound ：

  Theorem1:Johnson bound for constant weight error-correcting codes

$$\Phi(n,w,\lambda,\lambda) \le \frac{(n-1)(n-\lambda)\ldots(n-\lambda)}{w(w-1)\ldots\ldots(w-\lambda)}$$

Lemma4：Let $x \in C$,where C is an (n,w, λ +m, λ) OOC (m>0 is an integer)

Then $|M_{x,\lambda}| \geq \frac{w\left\lfloor \frac{w-1}{\lambda} \right\rfloor}{\lambda+m}$

Theorem2：let m be a nonnegative integer.Then

$$\Phi(n,w,\lambda+m,\lambda) \leq \frac{(n-1)(n-2)\ldots(n-\lambda)(\lambda+m)}{w(w-1)(w-2)\ldots(w-\lambda)}$$

- Lower Bound：

  Theorem3：

$$\Phi(n,w,\lambda_a,\lambda_c) \geq \frac{\left\lfloor \frac{n}{w} \right\rfloor A}{B}$$

9

Asymptotic Bounds：

Lemma5: let λ c be a positive integer,and let p and q be a nonnegative constant such that $p>(\lambda_C+q)/(\lambda_c+1)$ .Then

$\lim_{n\to\infty} \Phi(n,\lceil \alpha n^p \rceil,\lceil \beta n^q \rceil,\lambda_c) = 0$ for any positive real α and β .

Lemma6：let λ a and λ c be positive integers ,and let p be a positive constant such that

$p <$ m in $\{\lambda_a/(2\lambda_a+3), \lambda_c/(2\lambda_a+3)\}$

then $\lim_{n\to\infty} \Phi(n,\lfloor \alpha n^p \rfloor,\lambda_a,\lambda_c) = \infty$ for any positive real α

Lemma7：let p,q and r be constant , 0 < p, q, r < 1

Then if p < ½

$$\lim_{n\to\infty} \Phi(n,\lfloor \alpha n^p \rfloor,\lfloor \beta n^q \rfloor,\lfloor r n^r \rfloor) = \infty$$

For any positive α, β, γ .

10

Definition：Given an encoder f: $\{0,1\}^k \to \{0,1\}^n$,the separation vector associated with the encoder is an integer k-tuples $s=[s_0, s_1, \ldots, s_{k-1}]$ defined by

$$s_i = \min\{d(f(x), f(y)): x, y \in \{0,1\}^k \text{ and } x_i \neq y_i\}$$

Theorem4：Let α and β be positive,even integers .Then there exits a weight-w $(n, k_1 + k_2)$ error control code with separation vector

$$s = [\underbrace{\alpha, \alpha, \ldots, \alpha}_{k_2}, \underbrace{\beta, \ldots, \beta, \beta}_{k_1}]$$

where $k_2 = \lfloor \log_2 M(n, w, w-(\beta/2), w-(\alpha/2)) \rfloor$

$k_1 = \lfloor \log_2 n \rfloor$

- Constructing an (n , w , 2 , 1) OOC

  Here,we present two techniques for constructing (n,w,2,1) OOC.

  Both are derived from previously published methods for constructing a bounded incomplete block design(BIBD).

  A BIBD is structure equivalent to an (n,w,1,1) OOC.

  The techniques loosen the autocorrelation constraint to two.
- Construction I

  In the case w=5:

  (n,5,2,1) OOC:Let n be a prime number such that n=12t+1 for integer t ;

  $\alpha^q = \alpha^{3t} - 1$ *and* $\alpha^r = 2$,where q and r are integers that are nonzero modulo-3 and are distinct modulo-3.

  The ith codeword x_i contains a “1” in position

  $0, \alpha^{3i}, \alpha^{3t+3i}, \alpha^{6t+3i}, \alpha^{9t+3i}$ and “0” everywhere else.This holds for i =0,1,…t-1

- Construction II:

  An (n,5,2,1) OOC:Let n be a prime number such that n=12t+1 for an integer t. Let α be a primitive element of the field GF(n) such that ,for some integer $y \in \{1,2,\ldots,6t-1\}$,all of the following are nonzero and distinct modulo-6. $y, \log_\alpha[\alpha^y - 1], \log_\alpha[\alpha^{6t} - 1], \log_\alpha[\alpha^y(\alpha^{6t} - 1)]$ .then we can construct an (n,5,2,1) OOC from the blocks

$$\{[0, \alpha^{6i}, \alpha^{y+6i}, \alpha^{6t+6i}, \alpha^{6t+6i+y}] : i = 0,1,\ldots,t-1\}$$

From construct I and Theorem2:

$$\Phi(37,5,2,1) \le (36*2)/(5*4) = 3.6 \Rightarrow optimal$$

From construct II and Theorem2:

$$\Phi(41,4,2,1) \le 2*40/12 = 6.66 \Rightarrow not\ sure\ optimal$$

It is possible to construct an (n,w+1,2,1) code with either 2(n-1)/(w+1)(w+1) codewords (for even w+1) or 2(n-1)/w(w+2) codewords (for odd w+1);but Theorem1 tell us it is impossible to construct an (n,w,1,1) code more than (n-1)/w (w-1) codewords.

Therefore,for w≥6 the (n,w+1,2,1) codes offer better performance and more codewords than (n,w,1,1) code.

Ex: It is possible to construct a (1801,9,2,1) OOC with 45 codewords
But construct an (1801,8,1,1) code the Johnson bound tell us it is impossible to have more than 32 codewords.

- Summary

  Unlike previous work in this area,the author considered the possibility that the auto- and cross-correlation constraint *might not be identical* ; indeed,the bounds and the constructions suggest that it may sometimes be preferable to use such *"asymmetric"*

  OOC's.

  Among the constructions presented,we note that the (n,w,2,1)codes are near-optimal; their caridinality is 2(n-1)/w*w and have demonstrated that it is impossible to get more than 2(n-1)/w(w-1).