Mathematical Problems of Computer Science 21, 2000, 97–100.

A Construction for the $(n, 4, 2)$ Optical Orthogonal Codes

Sosina S. Martirosyan

Institute for Informatics and Automation Problems of NAS RA and YSU

Abstract

An optical orthogonal code is a constant weight block code with good autocorrelation and cross correlation properties. In this article we consider Optical Orthogonal Codes (OOC) when the maximal correlation equals two.It is given a new construction method for $(n, 4, 2) - OOC$.

Definitions

An (n, ϖ, λ) optical orthogonal code C is a family of binary sequences of length n and weight ϖ which satisfy the autocorrelation property:

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

for any $x \in C$ and any integer $0 < \tau < n$, and the crosscorrelation property:

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

for any $x \neq y \in C$ and any integer $0 \leq \tau < n$ (where the subscripts are to be taken modulo n) [1].

Whereas several optimal constructions for $\lambda = 1$ known, only a few are known for $\lambda = 2$. For $\varpi = 4$ and $\lambda = 2$ the correlation properties are automatically satisfied, so all that is important is the set of sequences with full cyclic order.

The case $\varpi = 4$ and $\lambda = 2$ is the first non-trivial case. Bitan and Etzion in [3] give a method for constructing optimal$(n, 4, 2)$ –codes with the use of Steiner quadruple systems. In this article we will give a new construction method of $(n, 4, 2)$ –OOC for any length n, the cardinality of which is $|C| = O(n^2)$.

For the case $\varpi = 4$ and $\lambda = 2$ the cardinality of known OOC [2] derived by using a greedy algorithm is equal to $n^2/96$.

Our codes cardinality is equal to $|C| = \begin{cases} \dfrac{n^2 - 2n + 1}{36}, & \text{when } n \text{ is even,} \\ \dfrac{n^2 - 2n + 1}{36}, & \text{when } n \text{ is odd.} \end{cases}$

The Johnson upper bound is equal $\dfrac{n^2 - 3n + 9}{24}$.

Let $U = (u_1, u_2, ..., u_n)$ be a binary n-tuple of Hamming weight ω , where $u_i \in [0, 1]$.

For convenience , we use the set notation of U , i.e.$U = \{u_{V1}, v_2, ..., v_n\}$, where v_l denotes the slot distance between lth "1" and $l + 1$th "1" for $l = 1, 2, ..., \varpi - 1$, and v_ϖ denotes n minus the slot distance between ϖth "1" and 1st "1".

Head	Head	Head
entry	entry	entry
entry	entry	entry
entry	entry	entry

Table 1:

Definition 1 *For any $U = (u_1, u_2, ..., u_n)$ binary n-tuple of Hamming weight ϖ, let set $\acute{U} = \{a_1, a_2, ..., a_\varpi\}_n$ where a_l denotes the slot distance between the lth "1" and $(l+2)$th "1", $l = 1, , ..., \varpi - 2$, and $a_{\varpi-1}$denotes n minus the slot distance between $\varpi - 1$th "1" and 1st "1", and a_ϖ denotes n minus the slot distance between ϖth "1" and 2nd "1".*

For any U the set $\acute{U}$ we will call second neighbors' set of U.
The binary n-tuples of Hamming weight 4,
$C = \{U_{i,j}\}_n$ $j = 1, 2, ..., \left\lceil\frac{S_n}{2}\right\rceil, i = 1, 2, ..., S_n - 2j + 2,$
where $U_{ij} = \{i, S_n - i - j + 2, i + 2j - 1, 2S_n - i - j + 3\}_n$.
The cardinality of the code C is: $|C| = \sum_{j=1}^{S_n/2} S_n - 2j + 2,$

$$|C| = \begin{cases} \dfrac{n^2 - 2n - 8}{36}, & \text{when } n \text{ is even,} \\ \dfrac{n^2 - 2n + 1}{36}, & \text{when } n \text{ is odd.} \end{cases}$$

The class of the code vectors for fixed j, $j = 1, 2, ..., \left\lceil\frac{S_n}{2}\right\rceil$ we will denote by

$$L_j : L_j = \{U_{i,j}\}_n,\ i = 1, 2, ..., S_n - 2j + 2$$

Example: $n = 10, \varpi = 4$.
$S_{10} = 2, j = 1, i = 1, 2,$
$U_{11} = (1101010000)_{n=10}, U_{11} = \{1, 2, 2, 5\}_{n=10}, U'_{11} = \{3, 4, 7, 6\}_{n=10},$
$U_{21} = (1011001000)_{n=10}, U_{11} = \{2, 1, 3, 4\}_{n=10}, U'_{21} = \{3, 4, 7, 6\}_{n=10}.$

1 : Bounds on OOC for $(n = 3k + 1, 4, 2)$

n	*New OOC's*	*UB*
7	1	1
10	2	3
13	4	4
16	6	8
19	9	12
22	12	17
25	16	22
28	20	29
31	30	35

Proposition 1 : For fixed j, $j = 1, 2, ..., \left\lceil\frac{S_n}{2}\right\rceil$, all vectors of the class $L_j : L_j = \{U_{i,j}\}_n$, have the same second neighbors' set, which is the following:
$U'_{ij} = \{S_n - j + 2, S_n + j + 1, 2S_n + j + 2, 2S_n - j + 3\}_n$ for $i = 1, 2, ..., S_n - 2j + 2$.
Note that for fixed n and $j, j = 1, 2, ..., \left\lceil\frac{S_n}{2}\right\rceil$ all these $S_n - j + 2, S_n + j + 1, 2S_n + j + 2, 2S_n - j + 3$ for numbers are different.

Proposition 2 : For any two vectors $U_1 \in L_j$ and $U_2 \in L_k$, where $j \neq k$, $k, j = 1, 2, ..., \left\lceil \frac{S_n}{2} \right\rceil$ the sets U_1' and U_2' disjoint.

Theorem: Let C be a family of U_{ij} binary n-tuples of Hamming weight 4,
$C = \{U_{i,j}\}_n$ $j = 1, 2, ..., \left\lceil \frac{S_n}{2} \right\rceil, i = 1, 2, ..., S_n - 2j + 2$
where $U_{ij} = \{i, S_n - i - j + 2, i + 2j - 1, 2S_n - i - j + 3\}_n$
The family C is $(n, 4, 2) - OOC$

Proof: Suppose to the contrary $\lambda \geq 3$.

The proof for the autocorrelation:

$\triangleright$ Note that for any vector $U \in C$ there are two shifts U^1, U^2 the set notations of which have one of the following forms:

*Case*1) $U^1 = \{r_1, r_2, r_3, r_4\}_n$ and $U^2 = \{r_1', r_2', r_3, r_4\}_n$, where $r_1 + r_2 = r_1' + r_2'$

From proposition 1 it follows that the *Case*1) occur only if $U^1 = U^2$ (as $r_1 + r_2 = r_1' + r_2'$).

*Case*2) $U^1 = \{r_1, r_2, r_3, r_4\}_n$ and $U^2 = \{r_1', r_2', r_3', r_4\}_n$, where $r_1 + r_2 = r_1'$ and $r_2' + r_3' = r_3$

1. Let $r_1' = r_3$ .So $r_1 + r_2 = r_2' + r_3'$ and as the second neighbors' set doesn't contains the same number twice(see *proposition*1 it follows that $r_4 = r_1' = r_3$.From the other side $r_4 + r_1' + r_3 = n$. So

$r_4 = r_3 = \frac{n}{3}$. But this is a contradiction, because it follows from construction of C that for any $U \in C$ only one element of the set U can be equal to $\frac{n}{3}$.

2.Let $r_1' \neq r_3$ .As U^1, U^2 are different shifts of the same vector U ,then the set U^1 must contain an element which is equal to r_1',it can be only r_4(as $r_1 + r_2 = r_1'$ and $r_2' + r_3' = r_3$. So $r_4 = r_3$, because the set U^2 must contain an element which is equal to r_3 and it can be again only r_4.

This is a contradiction.$\triangleleft$

The proof for the cross correlation:

$\triangleright$ Note that after some shifts set notations for any two vectors $U_1, U_2 \in C$ will have one of the following forms:

*Case*1) $U_1 = \{r_1, r_2, r_3, r_4\}_n$ and $U_2 = \{r_1', r_2', r_3, r_4\}_n$, where $r_1 + r_2 = r_1' + r_2'$

*Case*2) $U_1 = \{r_1, r_2, r_3, r_4\}_n$ and $U_2 = \{r_1', r_2', r_3', r_4\}_n$, where $r_1 + r_2 = r_1'$ and $r_2' + r_3' = r_3$

1) Let $U_1, U_2 \in L_j$, $j = 1, 2, ..., \left\lceil \frac{S_n}{2} \right\rceil$ (U_1 and U_2belongs to the same class.)

*Case*1) : As U_1, U_2 have the same second neighbours" set and that set includes every element only once .(see proposition 1) and $r_1 + r_2 = r_1' + r_2'$ we will have: $r_2 + r_3 = r_2' + r_3' \Longrightarrow r_2 = r_2'$ and $r_4 + r_1 = r_4' + r_1' \Longrightarrow r_1 = r_1'$.So $U_1 = U_2$, which is a contradiction.

*Case*2) Note that for fixed $j, j = 1, 2, ..., \left\lceil \frac{S_n}{2} \right\rceil$ this sets

$\{i, S_n - i - j + 2, i + 2j - 1, 2S_n - i - j + 3\}_n$

$\{S_n - j + 2, S_n + j + 1, 2S_n + j + 2, 2S_n - j + 3\}_n$ for $i = 1, 2, ..., S_n - 2j + 2$, can have an intersection only if $i = S_n - 3j + 3$, or $i = S_n - 2j + 2$.

For $1 < j \leq \left\lceil \frac{S_n}{2} \right\rceil$ the set notation of U_1, U_2 can be only the following:

$U_1 = \{S_n - 3j + 3, 2j - 1, S_n - j + 2, S_n + 2j\}_n$, when $i = S_n - 3j + 3$,

$U_2 = \{S_n - 2j + 2, j, S_n + 1, S_n + j + 1\}_n$, when $i = S_n - 2j + 2$

And this sets are disjoint (as $1 < j \leq \left\lceil \frac{S_n}{2} \right\rceil$) This is a contradiction, because for *case*2) we have that $r_4 \in U_1$ and $r_4 \in U_2$.

2) Let $U_1 \in L_j$ and $U_2 \in L_k$; $k < j$; $k, j = 1, 2, ..., \left\lceil \frac{S_n}{2} \right\rceil$ (U_1 and U_2 belong to the different classes.)

It follows from Proposition 1 that *case*1) can't occur.

*case*2) Note that for $k < j; i_1, i_2 = 1, 2, ...S_n - 2j + 2$, these sets:

$U_1 = U_{i_1 j} = \{i_1, S_n - i_1 - j + 2, i_1 + 2j - 1, 2S_n - i_1 - j + 3\}_n$;
$U_2' = U_{i_2 k}' = \{S_n - k + 2, S_n + k + 1, 2S_n + k + 2, 2S_n - k + 3\}_n$;
can have an intersection only if $S_n - k + 2 = i_1 + 2j - 1; i_1 = S_n - k - 2j + 3$.

From the other side for *case*2) we will have that

1) $2S_n - i_2 - k + 3 = S_n - i_1 - j + 2$ or

2) $2S_n - i_1 - j + 3 = i_2 + 2k - 1$.

But for $i_1 = S_n - k - 2j + 3$ the equations 1) and 2) are note correct.

Thus *case*2) can't occur.$\triangleleft$

References

[1] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical Orthogonal codes: design, analysis and applications," IEEE Trans. Inf. Theory, vol. 35, pp. 595–604, May 1989.

[2] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes',' IEEE Trans. Inf. Theory, vol. 36, pp.1334–1380, Nov. 1990.

[3] S. Bitan and T. Etzion, "Constructions for optimal constant weight cyclically permutable codes and difference families", IEEE Trans. Inf. Theory, vol. 41, pp.77–87, Jan. 1995.