A Construction for Optical Orthogonal Codes with Correlation 1

Samvel Martirosyan and A.J. Han Vinck

University of Essen, Essen, Germany
Ellernstr. 29, 45326, Essen
Institute for Experimental Mathematics
vinck@exp-math.uni-essen.de

Abstract: *We describe a construction of a class of Optical Orthogonal Codes with maximum correlation 1. The construction can be used for constant weight code vectors. The cardinality of the constructed code is larger than known lower bounds.*
keywords: optical orthogonal codes; correlation; construction

1. INTRODUCTION

Optical Orthogonal Codes (OOC) with low correlation between code vectors are used to allow multi user optical communication, see [1, 6]. Optical orthogonal codes have also found applications in mobile radio, frequency-hopping spread spectrum communications, etc. We do not intend to give any characterization of performance in communication systems. In this paper we concentrate on the construction of a specific class of codes defined as follows.

Definition: An (n,w,1)-Optical Orthogonal Code C is a family of binary code vectors of length n and weight w which satisfy the auto-correlation and cross-correlation property

$$\text{Auto-correlation: } \sum_{t=0}^{n-1} x_t x_{t+\tau} \le 1 \quad \tau \ge 1; \text{ subscripts reduced modulo n} \tag{1a}$$

$$\text{Cross-correlation: } \sum_{t=0}^{n-1} x_t y_{t+\tau} \le 1 \quad \tau \ge 0; \text{ subscripts reduced modulo n} \tag{1b}$$

for any $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in C$ and any $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \neq \mathbf{x} \in C$. It is easy to see that cyclic shifts of code words of an OOC do not affect its correlation properties. Hence, there is no need to make a distinction between code words that can be obtained from each other by cyclic shifts.

The problem considered is the construction of codes, with maximum cardinality $\Phi(n,w,1)$. The Johnson upper bound on the number of code vectors in an (n,w,1)–OOC is based on the maximum number of code vectors in a constant weight block code. For the relevant parameters,

$$\Phi(n,w,1) \le \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \right\rfloor \right\rfloor. \tag{2}$$

Several constructions are known for $\lambda = 1$, see Chung, Salehi and Wei [1]. The first interesting problem arises for $w = 3$, which has been solved in [1]. Optimal constructions

are given that meet the Johnson upper bound with equality for $n \neq 2 \bmod 6$. In [5] optimal constructions are given for $n \neq 14$ or 20 modulo 24, all meeting the Johnson bound with equality. Bitan and Etzion [6] show that for $n = 14$ or 20 modulo 24 the Johnson bound can not be met with equality. For $w = 4$ tables for $n < 264$ are given in [6]. There are only a few constructions for $w > 4$ that give optimal codes. Some optimal constructions can be found in [6].

Lower bounds on $\Phi(n,w,1)$ can be found in [1, 3]. In [4] we showed that the lower bound obtained with the so called accelerated Greedy algorithm as given in [1] is incorrect for $\lambda = 1$. We therefore use the lower bound as given in [1] for $n >> w$,

$$\Phi(n,w,1) \geq \frac{2n}{w^2(w-1)^2} + \text{lower order terms} \qquad (3)$$

In section 2 we give a new construction for a class of (n,w,1)-OOCs. We also indicate the cardinality $|C|$ of our class of codes compared with the lower bound (3). We conclude with some specific examples for $w = 3$ up to $w = 12$.

2. CONSTRUCTION

We first give some definitions convenient for our descriptions. Then we describe the construction of the class of codes and conclude this chapter with some properties that follow from the construction.

Let $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ be a binary vector of Hamming weight w. For the vector $\mathbf{x}$ we define its first neighbor set as follows.

Definition: The "first neighbor" set notation for $\mathbf{x}$ is defined as $\mathbf{X}_1 = \{ x_{1,1}, x_{1,2}, \ldots, x_{1,w-1} \}$, where $x_{1,k}$ represents the difference in the position of the k+1-th symbol 1 and the k-th symbol 1 in the vector $\mathbf{x}$, $1 \leq k < w$.

Note that from the first neighbor set we can find the vector $\mathbf{x}$ up to the position of the first nonzero symbol. In the same way, we can define the "i-th neighbor" set.

Definition: The "i-th neighbor" set notation for $\mathbf{x}$ is defined as $\mathbf{X}_i = \{ x_{i,1}\, x_{i,2}, \ldots, x_{i,w-i} \}$; $1 \leq i < w$, where $x_{i,j}$ represents the difference in the position of the j+i-th symbol 1 and the j-th symbol 1 in the vector $\mathbf{x}$.

Example: Let $n = 7$ and $w = 4$. The vector $\mathbf{x} = (1\ 1\ 1\ 0\ 1\ 0\ 0)$ has a first neighbor set $\mathbf{X}_1 = \{1,1,2\}$, second neighbor set $\mathbf{X}_2 = \{2,3\}$ and third neighbor set $\mathbf{X}_3 = \{4\}$.

Let $\Delta\mathbf{X}$ denote the set with $w(w-1)/2$ elements of the form

$$\Delta\mathbf{X} = \{ \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_{w-1} \} = \{ x_{1,1}, x_{1,2}, \cdots, x_{1,w-1}, x_{2,1}, x_{2,2}, \cdots, x_{2,w-2}, \cdots, x_{w-1,1} \}$$

and

$$\Delta C = \bigcup_{\mathbf{x} \in C} \Delta\, \mathbf{X}$$

Proposition. A code C of length n and constant weight w is a (n,w,1)-OOC if and only if

1. all elements of ΔC are different
2. $u + v \neq n$ for $u, v \in \Delta C$.

Proof. The proof follows from the definition for OOCs, since there are no intervals between any two different ones that are equal. □

We now give a description of a construction of a set ΔC based on an initial code vector x^0 of length n^0 and weight w. Then we will use this set to define an OOC of length n.
Let

1. $\mathbf{x^0}$ be a code vector of length n^0 and weight w. The code vector $\mathbf{x^0}$ has the auto-correlation property as given in (1a).
2. m be an integer such that $x^0_{w-1,1} \leq m < n^0$.
3. let the code $C = \{\mathbf{x^r}\}$, $r = 0,1,\cdots,K$; $K \in N$, be a set of code vectors of weight w for which

$$\Delta C = \bigcup_{r=0}^{K} \Delta \mathbf{X^r}\ ; \tag{4a}$$

$$\mathbf{X^r}_i = \{ x^0_{i,1} + irm,\ x^0_{i,2} + irm,\ldots,\ x^0_{i,w-i} + irm\},\ 1 \leq i < w; \tag{4b}$$

$$n = (w-1)Km + n^0. \tag{4c}$$

We may add the following condition to (4): for any pair $\{ u \in \mathbf{X^0}_i,\ v \in \mathbf{X^0}_j\}$; $1 \leq i, j < w$;

1. either $u + v \neq n^0$ modulo m (5a)

or

2. for those pairs (i, j), $(i+j) \geq w$, for which $u + v = n^0$ modulo m (5b)
   $u + irm + v + jsm \neq n = (w-1)Km+n^0$; $0 \leq r, s \leq K$

Theorem. The code C as defined by (4) and (5) is a $((w-1)Km + n^0, w, 1)$-OOC.
Proof: We prove that the two conditions from the proposition are satisfied:
i) All elements of ΔC are different. This follows from the fact that the elements of $\Delta \mathbf{X^0}$ are all different;
ii) If for any two elements $\{ u \in \mathbf{X^0}_i,\ v \in \mathbf{X^0}_j\}$, $u + v \neq n^0$ modulo m, it immediately follows that $u + irm + v + jsm \neq n = (w-1)Km+n^0$. Hence, the second condition of the proposition has to be checked for those values of u and v for which $u + v = n^0$ modulo m. Let $u' = u + irm$ and $v' = v + jsm$, where $u, v \in \Delta \mathbf{X^0}$ and $1 \leq i, j < w$; $0 \leq r, s \leq K$. Since $u + v < n^0 + m$, and $u + v \neq n^0$, the possible solutions might have the form $u + v = n^0 - t\,m$, where $1 \leq t$. Hence, $u + irm + v + jsm = n^0 - t\,m + irm + jsm < n^0 - t\,m + wKm \leq (w-1)Km+n^0$ for $(i + j) < w$. The condition (5b) thus has to be fulfilled for those pairs (i, j) for which $i + j \geq w$. □

Example: The following set ΔC defines a $(n=6K+9, 3, 1)$-OOC with K+1 code vectors, $m = 3$ and $n^0 = 9$.

$\mathbf{X^0}_1$; $\mathbf{X^0}_2$	=	1	2	3
$\mathbf{X^1}_1$; $\mathbf{X^1}_2$	=	4	5	9
...		...		
$\mathbf{X^K}_1$; $\mathbf{X^K}_2$	=	3K+1	3K+2	6K+3

This OOC is optimal since for n = 6K+9, the bound (2) gives $\Phi(n,w,1) \le K+1$.
Example: Let w = 4 and $\Delta\mathbf{X}^0 = \{ \mathbf{X}^0_1, \mathbf{X}^0_2, \mathbf{X}^0_3 \} = \{ x_{1,1}, x_{1,2}, x_{1,3}, x_{2,1}, x_{2,2}, x_{3,1} \} = \{1, 3, 2, 4, 5, 6 \}$. For m = 6 and $n^0 = 18$, we have to check the sum of elements for which i + j = 6. According to the definition of the code, these elements have the form u = 6 + 3rm and v = 6 + 3sm. The length n = 18K + 18. Hence, adding two elements gives as a sum u + v = 12 + 18(r + s) and thus, we have a (18K+18,4,1)-OOC:
Example: Let w = 5 and $\Delta\mathbf{X}^0 = \{ \mathbf{X}^0_1, \mathbf{X}^0_2, \mathbf{X}^0_3, \mathbf{X}^0_4 \} = \{ x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, x_{2,1}, x_{2,2}, x_{2,3}, x_{3,1}, x_{3,2}, x_{4,1} \} = \{ 3, 1, 5, 2, 4, 6, 7, 9, 8, 11 \}$. For m = 11 and $n^0 = 21$ there are no numbers for which i + j > 4 and u + v = 21 modulo 11. Thus we have defined a (44K + 21,5,1)-OOC.

Corollary 1. For any vector $\mathbf{x}^0$ of weight w and length n^0 with the auto-correlation property (1a), there exists an m such that (5) is satisfied.
Proof: For any pair $\{ u \in \mathbf{X}^0_i, v \in \mathbf{X}^0_j \}$; $1 \le i, j < w$; $(i+j) \ge w$

$$\min_{i+j \ge w} \left\{ (u+v) > \min_{i+j \ge w} \{1+2+\cdots+i+1+2+\cdots+j\} \right\} \ge$$

$$\ge \min_{i+j=w} \left\{ \frac{i(i+1)}{2} + \frac{j(j+1)}{2} \right\} = \begin{cases} \frac{w(w+2)}{4}, & \text{if } w \text{ is even} \\ \frac{(w+1)^2}{4}, & \text{if } w \text{ is odd} \end{cases}.$$

We choose m according to the following rule, $m \ge x_{w-1,1}$, and thus

$$n^0 - \frac{w(w+2)}{4} \le m \le n^0 \quad \text{for w is even,}$$

$$n^0 - \frac{(w+1)^2}{4} \le m \le n^0 \quad \text{for w is odd.}$$

Then, $u + v = n^0$ modulo n can only have one solution: $u + v = n^0$, which contradicts the assumption on X^0. □

The corollary shows that we can find an OOC for any w. However, to find efficient codes we have to use the smallest possible value for m, which is $m \ge x_{w-1,1}$, see also Table 1.

Corollary 2. The number of code vectors for the OOC as constructed according to the theorem satisfies

$$|C| = K+1 \ge \frac{2n}{w^2(w-1)^2} + \text{lower order terms}$$

for $m < w^2(w-1)/2$.

Proof. From $n = (w-1)Km+n^0$ it follows that

$$K+1=\frac{n-n^0+m(w-1)}{m(w-1)}>\frac{2n}{w^2(w-1)^2}+\frac{-n^0+m(w-1)}{m(w-1)}.$$ □

Corollary 3. If there exists a (n, w,1) difference set, then there exists an m < w(w-1) that satisfies (5).

Proof. If there exists a (n^0, w, 1) difference set, then there exists a vector $\mathbf{x}^0$ of length n^0 = w(w-1) + 1. The proof then follows from corollary 1. □

4. EVALUATION

The general construction of codes for λ = 1 according to corollary 2 give codes that exceed the known lower bound (3). However, for small values of w better codes can be found when using the construction as given in corollary 3. From n = (w-1)Km+n^0 it follows that starting with a difference set of length n^0 = w(w-1) + 1 gives codes with cardinality

$$K+1 \geq \frac{n}{w(w-1)^2} + \text{lower order terms.} \qquad (6)$$

One can observe that the lower bound (6) is a factor of w higher than the bound as given in (3). The problem with (6) is that we used the existence of difference sets for any w. For λ = 1 it is conjectured that there is a difference set with w elements iff w-1 is a prime power. This conjecture has been verified for cyclic difference sets with w < 3600. The following table gives examples of OOCs for several values of w.

TABLE 1

w	n^0	m	n	$\mathbf{X}^0_1 = \{ x_{1,1}, x_{1,2}, \ldots, x_{1,w-1} \}$
3	9	3	6K+9	1 2
4	18	6	18K+18	1 3 2
5	21	11	44K+21	3 1 5 2
6	31	17	85K+31	1 3 6 2 5
7	49	25	150K+49	3 1 8 6 5 2
8	57	35	245K+57	7 3 6 2 12 1 4
9	73	45	360K+73	3 6 7 4 1 14 8 2
10	91	55	495K+91	2 12 7 8 3 13 4 5 1
11	133	76	760K+133	2 4 18 5 11 3 12 13 7 1
12	133	85	935K+133	2 4 18 5 11 3 12 13 7 1 9

Several codes given in Table 1 are constructed using corollary 3. However, there are also some exceptions like w = 4, where we found a low value for m = 6.

As mentioned in the introduction, several constructions are known for λ = 1, see Chung, Salehi and Wei [1]. For w = 3 the problem has been solved. For w = 4 tables for n < 264 are given in [6]. From this table one can see that the given constructions meet the Johnson bound with equality. However, for the codes found by computer search no code cardinality is given. There are only a few constructions for w > 4 that give optimal codes. Some optimal constructions can be found in [1] and [6]. The construction given in [1], gives codes with parameters w = q+1

and $n = (q^{d+1}-1)/(q-1)$, where q has to be a prime power. In [4], a table with optimal codes of cardinality less than 50 is given for $w = 5$ using the results from [1] and [6].
We do not claim optimality of our new construction, but show that codes can constructed with a simple combinatorial method that are better than a lower bound as given in [1]. We furthermore show that when using difference sets (when they exist) as starting points we can improve the construction with a factor of w.

5. CONCLUSION

We give a new and simple combinatorial construction for OOCs, with correlation $\lambda = 1$. Construction rules are given such that codes can be found with a number of code vectors exceeding a known lower bound.

ACKNOWLEDGEMENT

We thank the anonymous reviewers for their constructive comments.

REFERENCES

[1] F.R.K. Chung, J.A. Salehi and V.K. Wei, "Optical Orthogonal Codes: design, analysis and applications," IEEE Trans. on Inf. Theory, Vol. 35, pp. 595-604, May 1989.
[2] R. Fuji-Hara and Y. Miao, "Optical Orthogonal Codes: their bounds and new optimal constructions," IEEE Trans. on Information Theory, Vol. 46, No. 7, pp. 2396-2406, 2000.
[3] G.C. Yang and T.E. Fuja, "Optical Orthogonal Codes with Unequal Auto- and Cross-correlation Constraints," IEEE Trans. on Inf. Theory, Vol. 41, pp. 96.106, Jan 1995.
[4] M. Stam and A.J. Han Vinck, "On Optical Orthogonal Codes," WIC Symposium on Information Theory in the Benelux, pp. 185-191, 1998.
[5] E.F. Brickell and V.K. Wei, "Optical Orthogonal Codes and difference Families," in Proc. Southeastern Conf. on Combinatorics Graph Theory and Algorithms, 1987.
[6] S. Bitan and T. Etzion, "Construction for Optimal Constant Weight Cyclically Permutable Codes and Difference Families," IEEE Trans. on Information Theory, vol. 41, pp. 77-87, Jan 1995.