Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Finite Fields and Their Applications 10 (2004) 405–411

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Optical orthogonal codes obtained from conics on finite projective planes

Nobuko Miyamoto,[a] Hirobumi Mizuno,[b] and Satoshi Shinohara[b,*]

[a] *Department of Information Sciences, Tokyo University of Science, Noda, Chiba 278-8510, Japan*
[b] *Faculty of Informatics, Meisei University, Oume, Tokyo 198-8655, Japan*

Received 27 March 2003; revised 23 September 2003

Communicated by Simeon Ball

Abstract

Optical orthogonal codes can be applied to fiber optical code division multiple access (CDMA) communications. In this paper, we show that optical orthogonal codes with auto- and cross-correlations at most 2 can be obtained from conics on a finite projective plane. In addition, the obtained codes asymptotically attain the upper bound on the number of codewords when the order q of the base field is large enough.

Keywords: Optical orthogonal codes; Conics; Finite projective plane

1. Introduction

An optical orthogonal code (OOC) $(n, w, \lambda_a, \lambda_c)$-OOC is a family C of (0,1)-sequences of length n with constant Hamming-weight w satisfying the following two properties:

- (*auto-correlation property*) for any codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, the inequality $\sum_{i=0}^{n-1} c_i c_{i+t} \leqslant \lambda_a$ holds for any integer $1 \leqslant t \leqslant n-1$, and
- (*cross-correlation property*) for any two distinct codewords $c, c' \in C$, the inequality $\sum_{i=0}^{n-1} c_i c'_{i+t} \leqslant \lambda_c$ holds for any integer $0 \leqslant t \leqslant n-1$,

*Corresponding author. Faculty of Informatics, Meisei University, Oume, Tokyo 198-8655, Japan. Fax: +81-428-25-5184.

E-mail addresses: miyamoto@is.noda.tus.ac.jp (N. Miyamoto), sshinoha@mi.meisei-u.ac.jp (S. Shinohara).

1071-5797/$ - see front matter
doi:10.1016/j.ffa.2003.09.004

where each subscript i of c_i is reduced modulo n. We denote an optical orthogonal code with these parameters, $n, w, \lambda_a, \lambda_c$, by $(n, w, \lambda_a, \lambda_c)$-OOC. When $\lambda_a = \lambda_c = \lambda$, we denote (n, w, λ)-OOC for simplicity. The number of codewords is called the *size* of the optical orthogonal code. We assume $\lambda < w$ because if $\lambda \geqslant w$ then all $(0,1)$-sequences have the above properties of optical orthogonal codes.

From a practical point of view, a code with large size is required. To find best possible codes, we need to determine an upper bound on the size of an optical orthogonal code with given parameters. Let $\Phi(n, w, \lambda)$ be the largest possible size of an (n, w, λ)-OOC. An optical orthogonal code achieving this maximum size is said to be *optimal*. Based on the Johnson bound for constant weight codes, we have the following bound [4]:

$$\Phi(n, w, \lambda) \leqslant \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \cdots \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor. \tag{1}$$

When $\lambda = 2$,

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

Example 1. The following 3 sequences are the codewords of a $(40, 4, 1)$-OOC.

1100000000000000000000000000100000000100

1010000000000000001000000100000000000000

1000010000010000000100000000000000000000

This code is optimal since $\Phi(40, 4, 1) \leqslant \left\lfloor \frac{1}{4} \left\lfloor \frac{40-1}{4-1} \right\rfloor \right\rfloor = 3$.

We often use the notation $\{i\colon c_i = 1\}$ for representing the codeword $(c_0, c_1, \ldots, c_{n-1})$. For example, the three codewords in Example 1 can be rewritten as $\{0, 1, 28, 37\}$, $\{0, 2, 18, 25\}$, and $\{0, 5, 11, 19\}$.

For $\lambda \geqslant 2$, there are only a few methods of construction of optimal optical orthogonal codes. Chung and Kumar [3] constructed optimal $(p^{2m} - 1, p^m + 1, 2)$-OOCs for any prime p by applying logarithmic maps from $\mathrm{GF}(p^{2m})\backslash\{0\}$ to the integers modulo $p^{2m} - 1$. Optimal $(n, 4, 2)$-OOCs were derived from block designs constructed by Bitan and Etzion [2]. Bird and Keedwell [1] showed a construction method of optimal $(n, k, 2)$-OOCs from cyclic Steiner 3-designs with block size k. In this paper, we show that for any prime power q a series of optical orthogonal codes $(q^3 + q^2 + q + 1, q + 1, 2)$-OOCs, can be obtained from conics on a projective plane over a finite field of order q. The method introduced in this paper is a generalization of the method using lines in a projective geometry, which is first given in [4]. In Section 2, we briefly review the construction method from lines. In Section 3, a new

construction method of optical orthogonal codes is described. The optimality of the obtained optical orthogonal codes is discussed in Section 4.

2. Known construction method from lines

Let $\mathrm{GF}(q)$ be a finite field of order q. By using lines in a projective geometry $\mathrm{PG}(d,q)$, we have an $(n,w,1)$-OOC, where n is the number of points in $\mathrm{PG}(d,q)$ and w is the number of points on a line.

Let ω be a primitive element of a finite field $\mathrm{GF}(q^{d+1})$ of order q^{d+1}. The points in a projective geometry $\mathrm{PG}(d,q)$ of dimension d over $\mathrm{GF}(q)$ can be represented as the powers of ω, that is, $\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}$, where $n = \frac{q^{d+1}-1}{q-1}$ is the number of points in $\mathrm{PG}(d,q)$. Let ϕ be the collineation defined as $\omega^i \mapsto \omega^{i+1}$. For a line l in $\mathrm{PG}(d,q)$, the set of exponents of the points on the line l, $\{i\colon\ \omega^i \in l\}$, can be regarded as the set notation of a codeword of an optical orthogonal code, since two distinct lines have at most one point in common. A line must be chosen as a representative from each orbit under ϕ since the map ϕ induces a cyclic shift for a codeword. If a line belongs to a short orbit, then the line should be omitted since otherwise the auto-correlation of the corresponding codeword is equal to the weight w.

Theorem 2 (Bird and Keedwell [1]). *For any prime power q and any positive integer d, there exists a $\left(\frac{q^{d+1}-1}{q-1}, q+1, 1\right)$-OOC consisting of $\left\lfloor \frac{q^d-1}{q^2-1} \right\rfloor$ codewords, where $\lfloor a \rfloor$ is the largest integer not greater than a.*

By using the above method, we have an example as follows.

Example 3. Let ω be a primitive element of $\mathrm{GF}(3^4)$ satisfying $\omega^4 + \omega^3 - 1 = 0$. The following four lines are representatives of the four orbits.

$$\hat{l_1} = \{1, \omega, \omega^{28}, \omega^{37}\}$$

$$\hat{l_2} = \{1, \omega^2, \omega^{18}, \omega^{25}\}$$

$$\hat{l_3} = \{1, \omega^5, \omega^{11}, \omega^{19}\}$$

$$\hat{l_0} = \{1, \omega^{10}, \omega^{20}, \omega^{30}\}$$

By regarding the exponents of points on each line, we have four sets each of which represents the positions of non-zero elements in the corresponding codeword. The first three lines are representatives of full orbits, and the last one is in a short

orbit. Hence we obtain three codewords of an optimal OOC, which is shown in Example 1.

3. New construction method of optical orthogonal codes with $\lambda = 2$

The correlation between two codewords obtained by the method shown in the previous section can be considered as the number of points in the intersection of two lines. The auto-correlation is the largest number of points in the intersection of two lines in the same orbit, and the cross-correlation is the largest number of points in the intersection of two lines from distinct orbits. Since the number of common points of distinct two lines is at most one, optical orthogonal codes with $\lambda \geqslant 2$ cannot be directly obtained by applying the method in the previous section.

In this section non-singular plane curves of degree 2, called conics, are used for constructing optical orthogonal codes with $\lambda = 2$. By the same manner as the method using lines, we consider the exponents of the points on a conic as the 1's position in a codeword. Hence the auto- and cross-correlation can be regarded as the number of points in the intersection between two conics respectively. In general, two conics have at most 4 common points in a three-dimensional projective space $\mathrm{PG}(3,q)$. It can be shown that the number of points in the intersection of two conics is at most 2 in $\mathrm{PG}(3,q)$ when the conics are from a particular set of conics on a projective plane.

Lemma 4. *Let $\mathscr{C}$ be a set of conics on a projective plane $\mathrm{PG}(2,q)$ each pair of which has at most two common points. Then there exists a $(q^3+q^2+q+1, q+1, 2)$-OOC consisting of $\#\mathscr{C}+q$ codewords, where $\#\mathscr{C}$ is the number of conics in $\mathscr{C}$.*

Proof. Let ω be a primitive element of a finite field $\mathrm{GF}(q^4)$ and $\phi : \omega^i \mapsto \omega^{i+1}$. Any point in $\mathrm{PG}(3,q)$ is represented as the power of ω. Since the number of points on any conic is $q+1$ and ϕ is an automorphism on the points in $\mathrm{PG}(3,q)$, the weight of codewords is $q+1$. The length of codewords is the number of points in $\mathrm{PG}(3,q)$, that is, q^3+q^2+q+1. Let $\mathscr{P}$ be a projective plane in $\mathrm{PG}(3,q)$. We can assume that all the conics in $\mathscr{C}$ are on $\mathscr{P}$. For a point set X, let $\phi(X) = \{\phi(x)\colon x \in X\}$. Two distinct conics C and C' in $\mathscr{C}$ can be regarded as the intersection of C with $\mathscr{P}$, and of C' with $\mathscr{P}$, respectively. The cross-correlation is the largest number of the points in the intersection between $C \cap \mathscr{P}$ and $\phi^i(C' \cap \mathscr{P})$ for $i = 0, 1, \ldots, n-1$. When $i = 0$ this number is less than or equal to 2 from assumption. For $i = 1, \ldots, n-1$, we have

$$(C \cap \mathscr{P}) \cap (\phi^i(C' \cap \mathscr{P})) = C \cap \mathscr{P} \cap \phi^i(C') \cap \phi^i(\mathscr{P})$$

$$\subseteq C \cap (\mathscr{P} \cap \phi^i(\mathscr{P})).$$

Since ϕ is a collineation, $\phi^i(\mathscr{P})$ is also a plane. Moreover, $\mathscr{P} \neq \phi^i(\mathscr{P})$ for $i = 1, \ldots, n-1$. Hence $C \cap (\mathscr{P} \cap \phi^i(\mathscr{P}))$ is the set of points in the intersection between a conic and a line, and the number is no more than 2. Similarly, it can be said that the auto-correlation is less than or equal to 2 since it is the number of points in the intersection between a conic and a line. In addition, the $\left\lfloor \frac{q^3-1}{q^2-1} \right\rfloor = q$ codewords obtained from lines in Theorem 2 can be added to the above codewords from conics since the number of points on any line is equal to $q+1$ and since the number of points in the intersection between a line and a conic is not more than 2. □

In Lemma 4, a set of conics each pair of which meet at most two points is required to obtain an optimal orthogonal code.

Lemma 5. *Let P be a point on $\mathrm{PG}(2, q^2)$ but not on $\mathrm{PG}(2, q)$, and let $\mathscr{C}$ be the set of conics over $\mathrm{GF}(q)$ passing through the point P. Any pair of two distinct conics in $\mathscr{C}$ have at most two common points, and the number of conics in $\mathscr{C}$ is $q^3 - q^2$.*

Proof. Put $P = (\alpha, \beta, \gamma)$ and a conic C passing through P is defined by the equation $f(x, y, z) = 0$ over $\mathrm{GF}(q)$. Then the point $P^q = (\alpha^q, \beta^q, \gamma^q)$ is a point on C since $f(\alpha^q, \beta^q, \gamma^q) = (f(\alpha, \beta, \gamma))^q = 0$. Since any conic in $\mathscr{C}$ passes through the two points P and P^q, any pair of two distinct conics have at most two common points in $\mathrm{PG}(2, q)$. The number of conics in $\mathscr{C}$ can be calculated as follows [5]. Let $\{P_s, P_t, P_u\}$ be three non-collinear points on $\mathrm{PG}(2, q)$ each of which is not on the line passing through P and P^q. Since no three points in $\{P_s, P_t, P_u, P, P^q\}$ are collinear, there exists a unique conic C defined over $\mathrm{GF}(q^2)$ passing through these five points. Moreover, the intersection of the conic C with $\mathrm{PG}(2, q)$ is also a conic in $\mathrm{PG}(2, q)$. The number of triples $\{P_s, P_t, P_u\}$ is $q^2(q^2-1)(q^2-q)$, and the number of triples which determine the same conic is $(q+1)q(q-1)$. Hence, the number of conics in $\mathscr{C}$ is $\frac{q^2(q^2-1)(q^2-q)}{(q+1)q(q-1)} = q^3 - q^2$. □

From Lemmas 4 and 5 we have a series of optical orthogonal code with $\lambda = 2$.

Proposition 6. *Let q be a prime power. Then there exists a $(q^3 + q^2 + q + 1, q + 1, 2)$-OOC consisting of $q^3 - q^2 + q$ codewords.*

Example 7. Let ω be a primitive element of $\mathrm{GF}(3^2)$ satisfying $\omega^2 = \omega + 1$. Any conic over $\mathrm{GF}(3)$ passing through the point $(1, \omega, 0)$ also passes through the point $(1, \omega^3, 0)$. We have the following 18 conics passing through these two points. The right-hand of each polynomial is the corresponding codeword.

$$
\begin{array}{ll}
x^2+xy+2y^2+xz+2yz=0 & \{3,24,26,30\}\\
x^2+xy+2y^2+2xz+2yz=0 & \{3,9,19,30\}\\
x^2+xy+2y^2+2xz+yz+2z^2=0 & \{9,17,24,30\}\\
x^2+xy+2y^2+z^2=0 & \{24,30,35,39\}\\
x^2+xy+2y^2+2z^2=0 & \{9,17,19,26\}\\
x^2+xy+2y^2+yz=0 & \{3,9,24,39\}\\
x^2+xy+2y^2+yz+2z^2=0 & \{19,26,30,35\}\\
x^2+xy+2y^2+2yz=0 & \{3,17,30,35\}\\
x^2+xy+2y^2+2yz+2z^2=0 & \{19,24,26,39\}\\
x^2+xy+2y^2+xz=0 & \{3,9,26,35\}\\
x^2+xy+2y^2+xz+z^2=0 & \{17,19,30,39\}\\
x^2+xy+2y^2+xz+yz=0 & \{3,17,26,39\}\\
x^2+xy+2y^2+xz+yz+z^2=0 & \{9,19,24,35\}\\
x^2+xy+2y^2+2xz+2yz+z^2=0 & \{17,24,26,35\}\\
x^2+xy+2y^2+xz+2yz+2z^2=0 & \{9,17,35,39\}\\
x^2+xy+2y^2+2xz=0 & \{3,17,19,24\}\\
x^2+xy+2y^2+2xz+z^2=0 & \{9,26,30,39\}\\
x^2+xy+2y^2+2xz+yz=0 & \{3,19,35,39\}
\end{array}
$$

In addition, the three codewords obtained in Example 1 are

$$\{0,1,28,37\},\ \{0,2,18,25\},\quad \text{and}\quad \{0,5,11,19\}.$$

Then the set of these 21 codewords forms a $(40,4,2)$-OOC.

4. Optimality of the obtained code

Table 1 shows the comparison between the parameters of optical orthogonal codes obtained from Proposition 6 with their sizes (A) and the upper bound from the Johnson bound (B). It seems to be that the number of codewords obtained from Proposition 6 asymptotically attains the upper bound. In fact, the upper bound Φ of the number of codewords in $(q^3+q^2+q+1,q+1,2)$-OOCs satisfies, from inequality (1),

$$\Phi \leqslant \left\lfloor \frac{1}{q+1}\left\lfloor \frac{q^3+q^2+q}{q}\left\lfloor \frac{q^3+q^2+q-1}{q-1}\right\rfloor\right\rfloor\right\rfloor$$

$$= q^3+2q^2+4q+1 \quad (\text{when } q>3).$$

Table 1
$(n, w, 2)$-OOCs obtained from Proposition 6 for some prime power q

q	n	w	# codewords (A)	Johnson bound (B)	(A)/(B)
3	40	4	21	61	0.344262
4	85	5	52	113	0.460177
5	156	6	105	196	0.535714
7	400	8	301	470	0.640426
8	585	9	456	673	0.677563
9	820	10	657	928	0.707974
11	1464	12	1221	1618	0.754635
13	2380	14	2041	2588	0.78864
16	4369	17	3856	4673	0.825166

The ratio of this number with the number of codewords obtained from Proposition 6 is asymptotically equal to 1 as $q \to \infty$.

Corollary 8. *The optical orthogonal codes obtained from Proposition* 6 *are asymptotically optimal.*

Acknowledgments

The authors thank Professor Gary Ebert, University of Delaware, for his valuable comments and suggestions on the number of conics in Lemma 5. They are also grateful to the referees for helpful comments. This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research of Japan, under Contract 13740081 and 14540100.

References

[1] C.M. Bird, A.D. Keedwell, Design and applications of optical orthogonal codes—a survey, Bull. ICA 11 (1994) 21–44.
[2] S. Bitan, T. Etzion, The last packing number of quadruples and cyclic SQS, Des. Codes Cryptogr. 3 (1993) 283–313.
[3] H. Chung, P.V. Kumar, Optical orthogonal codes: new bounds and an optimal construction, IEEE Trans. Inform. Theory 36 (4) (1990) 866–873.
[4] F.R.K. Chung, J.A. Salehi, V.K. Wei, Optical orthogonal codes: design, analysis, and applications, IEEE Trans. Inform. Theory 36 (1989) 595–604.
[5] Private communication with Professor Gary Ebert, University of Delaware, USA, at the Workshop "Designs, Codes, Graphs and their Links II" in Kyoto, Japan, Summer 2001.