Improved Johnson Bounds for Optical Orthogonal Codes with $\lambda > 1$ and Some Optimal Constructions

Reza Omrani
Communication Sciences Inst.
Dept. of Electrical Eng.- Systems
University of Southern California
3740 McClintock Ave.
Los Angeles, CA 90089-2565
Email: omrani@usc.edu

Oscar Moreno$^1$
Gauss Research Lab
University of Puerto Rico
PO Box 23334
San Juan, PR 00931-3334
Email: MORENO@UPPR.PR

P. Vijay Kumar$^2$
Communication Sciences Inst.
Dept. of Electrical Eng.- Systems
University of Southern California
3740 McClintock Ave.
Los Angeles, CA 90089-2565
Email: vijayk@usc.edu

Abstract—Optical orthogonal codes (OOC) are used as spreading sequences for optical CDMA networks. An OOC is a family of constant weight binary codes with a pre-specified maximum correlation parameter (MCP).

Johnson in his 1962 paper introduced three bounds for constant weight codes, that we call bounds A, B, and Hybrid. Subsequently Chung et al. adapted Johnson bound A to generate a bound for OOCs, which has been widely used to prove the optimality of OOCs.

Johnson bound B has been used in a prior work of this paper’s authors to prove the optimality of some OOCs. In this paper we give an improvement of this bound, and based on that prove the optimality of some other constructions which were not known to be optimal.

Using the results from Agrell et al., 2000 paper we also give an improvement of Johnson Hybrid bound for constant weight codes, and then use it to generate a bound for OOCs.

Finally, we introduce a new family of OOCs, based on flats in an affine geometry. While OOCs based on lines and hyperplanes are optimal, we can’t say much about other OOCs resulting from this construction. We will show that the Hybrid bound gives tighter bound than the other two bounds in some regions for this construction.

Recently lot of interest has been shown to find all optimal OOCs with weight 4 and 5 and MCP 1 and 2. Using affine geometry construction, a new family of optimal OOCs with weight 4 and MCP 2 is introduced.

I. INTRODUCTION

Recently there has been an upsurge of interest in applying Code Division Multiple Access (CDMA) techniques to optical networks (OCDMA) [1]. The spreading codes used in an OCDMA system are called optical orthogonal codes (OOC):

An $(n, \omega, \lambda)$ Optical Orthogonal Code (OOC) $C$ where $1 \leq \lambda \leq \omega \leq n$, is a family of $\{0,1\}$-sequences of length $n$ and Hamming weight $\omega$ satisfying:

$$\sum_{k=0}^{n-1} x(k) y(k \oplus \tau) \leq \lambda$$

(1)

whenever either $x \neq y$ or $\tau \neq 0$. We will refer to $\lambda$ as the maximum correlation parameter.

For a given set of values of $n$, $\omega$, and $\lambda$ let $\Phi(n, \omega, \lambda)$, denotes the largest possible cardinality of any $(n, \omega, \lambda)$ OOC code, and $P$ the cardinality of a specific construction.

The OOC constructions in which $P = \Phi(n, \omega, \lambda)$ are called optimal codes. An $(n, \omega, \lambda)$ OOC of size $P$ is said to be asymptotically optimum if $\lim_{n \to \infty} \frac{P}{\Phi(n, \omega, \lambda)} = 1$. Traditionally the following bound is used as an upper bound for OOCs [2]. This bound is based on Johnson upper bound [3][4] on the cardinality of a constant weight binary code which is adapted to yield an upper bound on OOCs:

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

There are many optimal and asymptotically optimal constructions in the literature satisfying this bound with $\lambda = 1$ [2][5][6]. Even there are some constructions with $\lambda = 2$ which satisfy this bound with equality [7]. We have not found any construction with $\lambda > 2$ satisfying this bound in the literature.

It is known that the above bound is not always achievable, for example in [8] we have introduced optimal OOCs, which are not satisfying the above bound. Agrell, Vardy, and Zeger in [9] give some bounds for constant weight codes, which are tighter than the Johnson bounds for constant weight codes [3]. Using these bounds we are going to introduce bounds for OOC which are tighter than the above bound in some regions in Section II.

Essentially we are proposing that the above bound is not very tight for some regions when $\lambda$ is large. On the other hand, in [5] certain asymptotically optimal constructions are give for $\lambda > 1$, therefore the above bound is good in some other regions. This question about how good is the above bound and for what regions it can be improved is the object of the present paper.

Some of our main results in this paper are as follows:

- Improved Johnson Bound B for OOC (See Theorem 2)
- Hybrid Bound for OOC (See Theorem 3)
- Application of Improved Johnson bound B to prove the optimality of an OOC construction from [8] (See

$^1$Work partially supported by NSF CISE Grant No. EIA-0080926
$^2$P. Vijay Kumar is currently on leave of absence from USC at the ECE Department, Indian Institute of Science, Bangalore. This work was supported in part, by the DARPA OCDMA Program under Grant No. N66001-02-1-8939.
Theorem 4)

- A new construction of OOCs (using d-flats of an affine geometry) for which our Hybrid bound gives tighter bound than the other two bounds in some regions (See Theorem 11).
- A new family of optimal \((n, 4, 2)\) OOCs based on 2-flats in an affine geometry (See Theorem 12)

II. NEW BOUNDS ON OOC, AND SOME OPTIMAL CONSTRUCTIONS

A. Constant Weight Codes

Let \(A(n, \omega, \kappa)\) denote the largest possible size of a constant-weight, binary \((0, 1)\) code in which every codeword has Hamming weight equal to \(\omega\) and the real inner product between any two codewords does not exceed \(\lambda\). The paper by Johnson [3] contains three principal bounds, which we shall refer to as Johnson Bounds A, B and C.

Johnson Bound A:

\[
A(n, \omega, \kappa) \leq \left\lfloor \frac{n}{\omega} \left( \frac{n-\omega}{\omega-\lambda} \right) \right\rfloor. \tag{2}
\]

Johnson Bound B: Provided \(\omega^2 > n\lambda\) we have:

\[
A(n, \omega, \kappa) \leq \left\lfloor \frac{n(\omega-\lambda)}{\omega^2-n\lambda} \right\rfloor. \tag{3}
\]

The third Johnson bound may be regarded as a hybrid of bounds A and B. Let \(\ell\), be the smallest integer, \(1 \leq \ell \leq \kappa-1\), such that \((\omega-\ell)^2 > (\ell-\ell)(\lambda-\ell)\). By combining Johnson bounds A and B we arrive at:

Johnson bound C:

\[
A(n, \omega, \lambda) \leq \left\lfloor \frac{n}{\omega} \left( \frac{n-\omega}{\omega-\lambda} \right) \right\rfloor, \tag{5}
\]

with \(h = \left\lfloor \frac{(n-\ell)(\omega-\lambda)}{(\omega-\ell)^2-(\ell-\ell)(\lambda-\ell)} \right\rfloor. \tag{4}
\]

Agrell, Vardy, and Zeger [9] provide the following bound as their Corollary 5:

\[
A(n, \omega, \lambda) \leq \left\lfloor \frac{n(\omega-\lambda)}{\omega^2-n\lambda} \right\rfloor, \tag{5}
\]

\[
A(n, \omega, \lambda) \leq \left\lfloor \frac{n(\omega-\lambda)}{\omega^2-n\lambda} \right\rfloor, \tag{6}
\]

\[
A(n, \omega, \lambda) \leq \left\lfloor \frac{n(\omega-\lambda)}{\omega^2-n\lambda} \right\rfloor, \tag{7}
\]

Remark 1: While the Bounds in [9] are presented differently, the above bounds are exactly equivalent to the bounds in [9].

Remark 2: As it can be seen Equation 5 is exactly the same as Johnson bound B, and Equation 6 is an improvement on the Johnson bound B. By Combining these two bounds, we get the following improvement on Johnson Bound B:

Improved Johnson Bound B: Provided \(\omega^2 > n\lambda\) we have:

\[
A(n, \omega, \lambda) \leq \min(n, \left\lfloor \frac{n(\omega-\lambda)}{\omega^2-n\lambda} \right\rfloor). \tag{8}
\]

Using the idea of the Hybrid Johnson bound and the above improvement of Agrell et. al we are introducing the Improved Hybrid Johnson bound:

**Theorem 1:** Improved Johnson Bound C: Provided \(\ell\), is some integer, \(1 \leq \ell \leq \lambda-1\), such that \((\omega-\ell)^2 > (\ell-\ell)(\lambda-\ell)\)

\[
A(n, w, \lambda) \leq \left\lfloor \frac{n}{w} \left( \frac{n-1}{w-1} \cdots \frac{n-(\ell-1)}{w-(\ell-1)} \right) \right\rfloor \tag{9}
\]

where here \(h\) is:

\[
h = \min(n-\ell, \left\lfloor \frac{(n-\ell)(\omega-\lambda)}{(\omega-\ell)^2-(\ell-\ell)(\lambda-\ell)} \right\rfloor). \tag{10}
\]

Note that, while the formulization of the bound is new, it is not generating new results for constant weight code [10], but it is very useful to generate a new bound for OOCs.

B. Optical Orthogonal Codes

If \(C\) is an \((n, \omega, \lambda)\) OOC, then by including every cyclic shift of each codeword in \(C\) one can construct a constant weight code with parameters \((n, \omega, \lambda)\) of size \(n \mid C\mid\). This observation allows us to translate bounds on constant weight codes to bounds on OOC:

\[
\Phi(n, \omega, \lambda) \leq \left\lfloor \frac{A(n, \omega, \lambda)}{n} \right\rfloor \tag{11}
\]

This bound was first pointed out by Chung, Salehi, and Wei in [2], and is exactly the same bound which is introduced in Introduction.

**Theorem 2:** Improved Johnson Bound B: Provided \(\omega^2 \geq n\lambda\):

\[
\Phi(n, \omega, \lambda) \leq \min(1, \left\lfloor \frac{n(\omega-\lambda)}{\omega^2-n\lambda} \right\rfloor), \quad \omega^2 > n\lambda. \tag{12}
\]

\[
\Phi(n, \omega, \lambda) \leq 1, \quad \omega^2 = n\lambda \tag{13}
\]

**Remark 3:** Equation 13 results from Agrell et. al. Bound of Equation 7.

**Remark 4:** We note that the observation that \(\Phi(n, \omega, \lambda) \leq 1\) for \(\omega^2 > n\lambda\) first appears in [7], while the more general form for the constant weight codes has been proved much later by Agrell, Vardy, and Zeger in [9].

**Theorem 3:** Improved Johnson Bound C:

\[
\Phi(n, w, \lambda) \leq \left\lfloor \frac{n}{w} \left( \frac{n-1}{w-1} \cdots \frac{n-(\ell-1)}{w-(\ell-1)} \right) \right\rfloor \tag{14}
\]

with \(h = \min(n-\ell, \left\lfloor \frac{(n-\ell)(\omega-\lambda)}{(\omega-\ell)^2-(\ell-\ell)(\lambda-\ell)} \right\rfloor). \tag{15}\)

and, where \(\ell\), is any integer, \(1 \leq \ell \leq \lambda-1\), such that \((\omega-\ell)^2 > (\ell-\ell)(\lambda-\ell)\).

The following two OOCs have been introduced by the authors of this paper in [6][8]:

1) **Generalized Bose-Chowla with** \(\lambda = 1\): \(A(q^a-1, q, 1)\) OOC of size \(q^{a-1}-1\).

2) **Generalized Bose-Chowla with** \(\lambda = q^{a-2}\): \(A(q^a-1, q^{a-1}, q^{a-2})\) OOC of size 1.
The first OOC can be shown to be optimal using the traditional Johnson Bound A [6]. The second construction is proved to be optimal in [8] for \( q = 2 \) using Johnson bound B. IN following we use one of our new bounds to prove the optimality of the second construction above:

**Theorem 4:** \((q^a - 1, q^{a-1}, q^{a-2})\) generalized Bose-Chowla OOC construction is an optimal construction for every \( q \) a power of a prime.

**Proof:** Using the Improve Johnson bound B of Equation 12 this fact can be proved. ■

III. CODE CONSTRUCTION

A. Preliminaries

In this section we need to use some properties of affine geometries. In following we are going to introduce the necessary concepts:

The points of \( EG(a, q) \), the affine geometry of dimension \( a \) over \( GF(q) \), consist of all elements of \( GF(q^a) \). Let \( \xi_0, \xi_1, \ldots, \xi_d \) be \( d+1 \) linearly independent elements of \( GF(q^a) \). The \( d \) points of the form:

\[
\xi_0 + v_1 \xi_1 + v_2 \xi_2 + \cdots + v_d \xi_d
\]

with \( v_i \in GF(q) \) for \( 1 \leq i \leq d \), constitute a \( d \)-flat in \( EG(a, q) \) passing through the point \( \xi_0 \). If we set \( \xi_0 = 0 \), we will end up with a \( d \)-flat passing through origin. Moreover each \( d \)-flat can be shown as a subset of size \( q^d \) of the set \( \{-\infty, 0, 1, \ldots, q^a - 2\} \) using the mapping \( \log_{x_\beta} \) when \( \beta \) is a primitive element of \( GF(q^a) \) over \( GF(q) \). A \( d \)-flat, for \( d = 1 \) is called a line, and for \( d = a - 1 \) is called a hyperplane. Any two \( d \)-flats with \( d < a - 1 \) neither are intersecting, or their intersection is an \( i \)-flat with \( i \leq (d - 1) \). Any two hyperplanes \((a - 1)\)-flats either are not intersecting, or their intersection is an \((a - 2)\)-flat.

To count the number of \( d \)-flats in an \( EG(a, q) \), we need to use the Gaussian coefficients [4][13].

**Lemma 5:** The number of \( d \)-dimensional subspaces of an \( a \)-dimensional vector space over \( GF(q) \) is defined as Gaussian coefficient, and is shown as \([ a \atop d ]_q \). Can be computed as follows [13]:

\[
[a \atop d]_q = \frac{(q^a - 1)(q^{a-1} - 1) \cdots (q^{a-d+1} - 1)}{(q^d - 1)(q^{d-1} - 1) \cdots (q - 1)}
\]

It is a well-known fact that the \( d \)-flats of an affine geometry are blocks of a balanced Incomplete Block Design (BIBD) [13]. Using the properties of these designs we can find the number of \( d \)-flats in an \( EG(a, q) \).

**Lemma 6:** The number of \( d \)-flats in an \( EG(a, q) \) is equal to \( q^{a-d} [a \atop d]_q \), and the number of \( d \)-flats passing through any specific point in the geometry is equal to \([ a \atop d ]_q \) [13].

To use affine geometry to construct OOCs, we need to study the properties of a cyclic shifted version of a \( d \)-flat in \( EG(q^a, a) \):

**Lemma 7:** Let \( \{c_1, c_2, \ldots, c_{q^a}\} \) with all \( c_i \)'s \( \in \{-\infty, 0, 1, \ldots, q^a - 2\} \) represent the points on a \( d \)-flat, then the set \( \{c_1 + i, c_2 + i, \ldots, c_{q^a} + i\} \mod (q^a - 1) \), for any given integer \( i \) also defines some \( d \)-flat, which we call a cyclic shifted version of the original \( d \)-flat.

**Proof:** If \( \xi_0, \xi_1, \ldots, \xi_d \) are linearly independent points generating the d-flat:

\[
\forall c_j, \exists v_{1j}, \ldots, v_{dj} \in GF(q) : \beta^{c_j} = \xi_0 + \sum_{k=1}^{d} v_{kj} \xi_k
\]

\[
\Rightarrow \beta^{c_j+i} = \beta^{c_j} \beta^i = \xi_0 \beta^i + \sum_{k=1}^{d} v_{kj} \xi_k \beta^i
\]

All we need is to show that \( \xi_0 \beta^i, \ldots, \xi_d \beta^i \) are linearly independent, which is obvious.

If we start with a \( d \)-flat and start cyclically shift it by one unit, the \( d \)-flat is called cyclic if at some point we return to the original \( d \)-flat. The smallest number of shifts to return to the original \( d \)-flat is called the cycle of the \( d \)-flat.

**Theorem 8:** In \( EG(a, q) \), every \( d \)-flat is cyclic, and the cycle of any \( d \)-flat not passing through origin, is equal to \( q^a - 1 \).

**Proof:** Take the integers \( C = \{c_1, c_2, \ldots, c_{q^a}\} \) represent the points on a \( d \)-flat. Since \( c_i + (q^a - 1) = c_i \mod (q^a - 1) \), obviously every \( d \)-flat is cyclic. If we assume that the cycle of \( C \) is equal to \( g \), then \( g = g \mod (q^a - 1) \), then obviously \((q^a - 1) \). Let’s assume \( g < (q^a - 1) \). Let’s add all the elements of \( C \) and \( + g \mod (q^a - 1) \):

\[
\sum_{i=1}^{q^a} c_i = \sum_{i=1}^{q^a} (c_i + g) = \sum_{i=1}^{q^a} c_i + q^a g \mod (q^a - 1)
\]

\[
\Rightarrow q^a g = 0 \mod (q^a - 1) \Rightarrow (q^a - 1)|q^a g \Rightarrow \frac{q^a - 1}{g} | q^a
\]

Since we assume \( g < (q^a - 1) \), then \( \frac{q^a - 1}{g} \) is an integer greater than 1, which means that there is a common factor greater than 1 between \( q^a - 1 \) and \( q^a - 1 \). If \( g = (q^a - 1) \), we are done. Note that the above argument is not true when the \( d \)-flat is passing through origin. That is because, when the \( d \)-flat is passing through origin one of the \( c_i \)'s is equal to \( -\infty \), and \( -\infty + g = -\infty \).

The above theorem which was originally stated in [12], is the key property of affine geometries we use to construct OOCs.

B. Previous Works

In [14] it is proved that the following two constructions correspond to lines and hyperplanes of an affine geometry:

**Theorem 9:** Take \( a \) a primitive element of \( GF(q^a) \) over \( GF(q) \). For any vector \( \ell_i = (\ell_{i0}, \ldots, \ell_{i-1}, \ell_i) = 1 \) with all \( \ell_j \in GF(q) \) and \( i < a - 1 \), define \( P_{\ell_i}(x) = \ell_i x^{i+1} + \ell_{i-1} x^i + \cdots + \ell_0 x \). Each of these polynomials is generating one codeword of the code. The codeword corresponding to the \( P_{\ell_i}(x) \) has a 1 precisely in the coordinates corresponding to \( [\log_{x_\beta} P_{\ell_i}(x) + v] \) for any \( v \in GF(q) \), where \( \beta \) is any primitive element of \( GF(q^a) \) over \( GF(q) \).

The above construction gives us an \( (n = q^a - 1, \omega = q, \lambda = 1) \) OOC with \( q^{a-2} + q^{a-3} + \cdots + 1 \) codewords, for any \( q \) which is a power of a prime[6].

261
TABLE I

(31, 2d, 2d−1) OOCs Based on d-flats of an EG(5, 2) Affine Geometry

<table>
<thead>
<tr>
<th>d = 1</th>
<th>d = 2</th>
<th>d = 3</th>
<th>d = 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>{4, 10}</td>
<td>{4, 10, 17, 30}</td>
<td>{4, 7, 10, 17, 22, 26, 28, 30}</td>
<td>{4, 7, 9, 10}</td>
</tr>
<tr>
<td>{17, 30}</td>
<td>{4, 7, 10, 22}</td>
<td>{4, 9, 10, 16, 17, 21, 25, 30}</td>
<td>{13, 14, 15, 16}</td>
</tr>
<tr>
<td>{7, 22}</td>
<td>{4, 10, 26, 28}</td>
<td>{4, 10, 13, 14}</td>
<td>25, 26, 28, 30</td>
</tr>
<tr>
<td>{26, 28}</td>
<td>{4, 10, 21, 25}</td>
<td>{3, 17, 29, 30}</td>
<td>{2, 5, 13, 14}</td>
</tr>
<tr>
<td>{21, 25}</td>
<td>{4, 9, 10, 16}</td>
<td>{6, 17, 27, 30}</td>
<td>{3, 15, 24, 29}</td>
</tr>
<tr>
<td>{9, 16}</td>
<td>{4, 10, 13, 14}</td>
<td>{8, 17, 20, 30}</td>
<td>{9, 7, 16, 21, 22, 25, 26, 28}</td>
</tr>
<tr>
<td>{13, 14}</td>
<td>{4, 10, 15, 24}</td>
<td>{1, 17, 18, 30}</td>
<td>{7, 13, 14, 15, 22, 24, 26, 28}</td>
</tr>
<tr>
<td>{15, 24}</td>
<td>{4, 6, 10, 27}</td>
<td>{7, 15, 22, 24}</td>
<td>{3, 6, 7, 22, 26, 27, 28, 29}</td>
</tr>
<tr>
<td>{3, 29}</td>
<td>{4, 8, 10, 20}</td>
<td>{3, 7, 22, 29}</td>
<td>{7, 8, 12, 20, 22, 23, 26, 28}</td>
</tr>
<tr>
<td>{6, 27}</td>
<td>{4, 10, 12, 23}</td>
<td>{6, 7, 22, 27}</td>
<td>{2, 5, 7, 11, 19, 22, 26, 28}</td>
</tr>
<tr>
<td>{8, 20}</td>
<td>{2, 4, 5, 10}</td>
<td>{2, 5, 7, 22}</td>
<td>{8, 9, 12, 16, 20, 21, 23, 25}</td>
</tr>
<tr>
<td>{12, 23}</td>
<td>{4, 10, 11, 19}</td>
<td>{7, 11, 19, 22}</td>
<td>{3, 6, 13, 14, 15, 24, 27, 29}</td>
</tr>
<tr>
<td>{2, 5}</td>
<td>{1, 4, 10, 18}</td>
<td>{21, 25, 26, 28}</td>
<td>{2, 5, 11, 13, 14, 15, 19, 24}</td>
</tr>
<tr>
<td>{11, 19}</td>
<td>{7, 17, 22, 30}</td>
<td>{9, 16, 26, 28}</td>
<td>{2, 3, 5, 6, 11, 19, 27, 29}</td>
</tr>
<tr>
<td>{1, 18}</td>
<td>{17, 26, 28, 30}</td>
<td>{6, 26, 27, 28}</td>
<td>{2, 5, 8, 11, 12, 19, 20, 23}</td>
</tr>
</tbody>
</table>

Each set is a codeword. The codeword corresponding to each set has 1 precisely in the coordinates corresponding to the numbers in the set.

It is proved in [14] that each codeword in the above construction is a representative of every full cyclic orbit of lines of $EG(a, q)$ not passing through origin.

The method used in the Construction of Theorem 9 can be modified to construct a new class of OOC with $\lambda \geq 2$ [8]:

**Theorem 10:** Let $F_q^\alpha$, be a finite field with $q^\alpha$ elements, with $\alpha$ and $\beta$ primitive elements of $F_q^\alpha$ over $F_q$. Now construct a single codeword of length $q^\alpha - 1$ which has 1 precisely in the coordinates corresponding to $log_2(\alpha^{a-1} + \ell_2 a^{a-2} + \cdots + \ell_1 a + \ell_0)$ for all $\ell_i \in F_q$. This gives rise to an OOC with parameters $(q^\alpha - 1, q^{\alpha-1}, q^{\alpha-2})$ of size $\Phi = 1$ [8].

It is proved in [14] that the codeword in the above construction is the representative of full cyclic orbit of hyperplanes of $EG(a, q)$ not passing through origin.

Note that the constructions of Theorems 9 and 10, correspond to the two OOCs introduced at the end of Section II-B, and are both optimal constructions.

**C. General Construction**

Using the theorems of this section, we are now ready to give one of our main results:

**Theorem 11:** In an $EG(a, q)$ affine geometry, by picking one member out of each full cyclic orbit of $d$-flats, not passing through the origin as the codewords of an OOC, we can construct a $(q^d - 1, q^d, q^{d-1})$ OOC of size:

$$(q^a - 1)(q^{a-1} - 1)\cdots(q^d - 1).$$

**Proof:** Every element of the set of all $d$-flats not passing through the origin, is a member of some full cyclic orbit of $d$-flats by Theorem 8. It is obvious that any two distinct orbits are disjoint. So the cyclic orbits of $d$-flats not passing through the origin partition the set of $d$-flats not passing through the origin. In addition it is known that any two $d$-flats can intersect maximally in a $(d - 1)$-flat. So any two $d$-flats can have maximally $q^{d-1}$ points in common.

Choosing only one member out of each orbit guarantees that any two different cyclic shifts of the same codeword can have maximally $q^{d-1}$ points in common. In addition two different cyclic shifts of two distinct codewords, are members of two different orbits, and can have maximally $q^{d-1}$ points in common. So the chosen codewords satisfy Equation 1. So they are making an OOC.

By Lemma 6, total number of $d$-flats in an $EG(a, q)$ is equal to $q^{a-d} \binom{a}{d} q$. In addition we know that $\binom{a}{d}_q$ of these $d$-flats, are passing through the origin. So there are totally $(q^{a-d} - 1) \binom{a}{d}_q$ $d$-flats not passing through the origin. On the other hand, each full orbit consists of $q^a - 1$ $d$-flats, so there are $\frac{q^a - 1}{q^{a-d} - 1} \binom{a}{d}_q$ codewords in the OOC:

$${\text{OOC Size}} = \frac{q^{a-d} - 1}{q^a - 1} \binom{a}{d}_q$$

$$= \frac{q^{a-d} - 1}{q^a - 1} \frac{(q^a - 1)(q^{a-1} - 1)\cdots(q^{a-d+1} - 1)}{(q^a - 1)(q^{a-1} - 1)\cdots(q - 1)}$$

$$= \frac{(q^a - 1)\cdots(q^{a-d} - 1)}{(q - 1)(q^d - 1)}.$$

It is obvious that the constructions of Theorems 9 and 10 are special cases of the above construction for $d = 1$, and $d = a - 1$ respectively.

**Example 1:** An $EG(5, 2)$ affine geometry consists of 32 points. The points of $EG(5, 2)$ consists of all members of $GF(2^5)$. $x^5 + x^2 + 1$ is a primitive polynomial generating $GF(2^5)$. Assuming $a$ to be a zero of the primitive polynomial, the points of $EG(2, 5)$ can be shown as $\{0, \alpha^0, \alpha^1, \cdots, \alpha^{q^a-2}\}$. Equivalently we can show these points with integers $\{-\infty, 0, 1, \cdots, q^a - 2\}$.

Using this affine geometry, and construction of Theorem 11 we can construct the following OOCs, which are shown in Table I:

1) OOC based on lines: A $(31, 2, 1)$ OOC of size 15. This is an optimal OOC. The codewords of this OOC which are shown in Table I, are constructed using Theorem 9.
2) OOC based on 2-flats: A \((31, 4, 2)\) OOC of size 35. This OOC is optimal using Johnson bound A of Equation 11.

3) OOC based on 3-flats: A \((31, 8, 4)\) OOC of size 15. As it can be seen this construction is not optimal based on any bounds in Section II-B.

4) OOC based on hyperplanes: A \((31, 16, 8)\) OOC of size 1. This is an optimal OOC, and its codeword which is shown in Table I, is constructed using Theorem 10.

As it can be observed from the above example, while we can prove the optimality of OOCs based on lines and hyperplanes, we can’t say much about the optimality of the constructions in Theorem 11 in general.

In addition, there is no general method to generate the codewords of the OOCs from Theorem 11, except for \(d = 1 \text{ and } d = a - 1\), which are discussed in Theorems 9 and 10. To generate the codewords of the OOC for \(d \notin \{1, a - 1\}\), we should first generate all the \(d\)-flats, and then choose one representative from each full orbit to orbits, and then choose one representative from each full orbit not passing through origin. This algorithm is not as fast as an explicit construction to generate the codewords (like Theorem 9 and 10), but still it is much faster than brute force search algorithms to find OOCs.

Example 2: Let’s find the upper bound on the size of a \((63, 16, 8)\) OOC:

1) Johnson bound \(A : \Phi(63, 16, 8) \leq 28270\).

2) Improved Johnson bound \(B : \Phi(6, 16, 8) \leq 28270\).

3) Improved Johnson bound \(C : \Phi(63, 16, 8) \leq 12919\).

As it can be seen that Improved Johnson bound C is generating a tighter bound. If we use the construction of Theorem 11 to generate the OOC, we will end up with an OOC of size 31, which is far from either bounds.

D. An Specific Optimal Construction

Recently, design theorists have shown a lot of interest in finding OOCs with weight 4, and 5. There are some works in the literature on \((n, 4, 2)\) OOCs [15][16][17][18].

Using the construction of Theorem 11, we can construct a family of optimal \((n, 4, 2)\) OOCs:

**Theorem 12:** Using the construction of Theorem 11, for \(q = 2\) and \(d = 2\), a family of optimal OOCs with parameters \((2^a - 1, 4, 2)\) and size \([2a - 1][2a - 2] - 1\) can be constructed.

**Proof:** The only thing we need to prove is the optimality of the construction. By applying Johnson bound A to the parameters of the OOC we can prove its optimality:

\[
\Phi(2^a - 1, 4, 2) \leq \left[ \frac{4(2^a - 1)(2^{a - 1} - 1)}{3a - 1} \right] = \left[ \frac{4}{3a - 1} \right].
\]

Note that \(3a = (2a - 1)(2a - 2) - 1\) for all \(a\).

E. Multi-weight OOC

Constructing OOCs, with different weight classes is a new nice problem involving OOCs which has application in OCDMA networks. As we show a variation of Theorem 11 can be used to generate such classes.

It can be shown that an \(-\text{flat and a } j\)-flat in an \((a, q)\) affine geometry, either are not intersecting, or they intersect in a \(k\)-flat, with \(k < \min(i, j)\).

Now instead of having an OOC based only on \(d\)-flats, we can construct an OOC, which is a combination of \(d_1, d_2, \ldots, d_t\), flats, with the consideration that for \(d_i < d_j\), none of the representatives in \(d_i\)-flats should lie on the orbits of \(d_j\)-flats in the OOC. Such an OOC has length \(q^a - 1\), and weight classes \(q^a, q^a, \ldots, q^a\).

The most interesting property of this OOC is that each weight class \(q^a\) has \(\lambda = q^{a-1}\). This means that the smaller weights are not experiencing extra interference due to higher weights.

REFERENCES


