Classes of Optical Orthogonal Codes from Arcs in Root Subspaces

T.L. Alderson [1]

Department of Mathematical Sciences, University of New Brunswick, Saint John, New Brunswick, E2L 4L5, Canada

Keith E. Mellinger [*,2]

Department of Mathematics, University of Mary Washington, 1301 College Avenue, Trinkle Hall, Fredericksburg, VA 22401, USA

Abstract

We present new constructions for (n, w, λ) optical orthogonal codes (OOC) using techniques from finite projective geometry. In one case codewords correspond to $(q-1)$-arcs contained in Baer subspaces (and, in general, k^{th}-root subspaces) of a projective space. In the other construction, we use sublines isomorphic to $PG(1, q)$ lying in a projective plane isomorphic to $PG(1, q^k)$, $k > 1$. Our construction yields for each $\lambda > 1$ an infinite family of OOCs which, in many cases, are asymptotically optimal with respect to the Johnson bound.

Key words: optical orthogonal code, arc, normal rational curve
PACS: 94B27, 51E21

1 Introduction

An Optical Orthogonal Code (OOC) is a family of binary sequences with strong auto- and cross-correlation properties. One of the first proposed applications of optical orthogonal codes was to optical code-division multiple access

* corresponding author
Email addresses: talderso@unbsj.ca (T.L. Alderson), kmelling@umw.edu (Keith E. Mellinger).

[1] The author acknowledges support from the NSERC of Canada.
[2] The author acknowledges support by a faculty development grant from the University of Mary Washington

communication systems where binary sequences with strong correlation properties are required [2,4,5]. Subsequently, OOCs have found application for multimedia transmissions in fiber-optic LANs [7]. Optical orthogonal codes have also been called cyclically permutable constant weight codes in the construction of protocol sequences for multiuser collision channels without feedback [10]. In application, good OOCs have the property that each codeword has many more 0's than 1's [4]. The codes constructed here have this property.

An $(n, w, \lambda_a, \lambda_c)$-optical orthogonal code (OOC) is a family of binary sequences (codewords) of length n, with constant hamming weight w satisfying the following two conditions:

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

where each subscript is reduced modulo n.

An $(n, w, \lambda_a, \lambda_c)$-OOC with $\lambda_a = \lambda_c$ is denoted (n, w, λ)-OOC. Any constant weight code of weight w is an (n, w, λ)-OOC if $\lambda \geq w$, hence in all codes considered here we assume $w > \lambda$. The number of codewords in a given OOC is the *size* of the code. For fixed values of n, w, and λ, the largest size of an (n, w, λ)-OOC is denoted $\Phi(n, w, \lambda)$. In general, $\Phi(n, w, \lambda)$ is difficult to compute. In [4] the Johnson bound for constant weight codes (see [6]) is used to derive the following upper bound on $\Phi(n, w, \lambda)$.

$$\Phi(n, w, \lambda) \leq \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \right\rfloor \cdots \right\rfloor \right\rfloor \tag{1}$$

If an (n, w, λ)-OOC meets the bound (1) then the code is said to be *optimal*. If C is an $(n, w, \lambda_a, \lambda_c)$-OOC with $\lambda_a \neq \lambda_c$ then we obtain a bound on the size of C by taking $\lambda = max\{\lambda_a, \lambda_c\}$ in (1).

For $\lambda = 1, 2$ optimal OOCs are known to exist [4,3]. It is still unknown as to whether optimal (n, w, λ)-OOCs exist with $\lambda > 2$. There is much interest in constructing optimal and asymptotically optimal OOCs. The concept of asymptotic optimality was introduced in [8].

Definition 1 *Let F be an infinite family of OOCs with $\lambda_a = \lambda_c$. For any (n, w, λ)-OOC $C \in F$ containing at least one codeword, the number of codewords in C is denoted by $M(n, w, \lambda)$ and the corresponding Johnson bound is*

denoted by $J(n, w, \lambda)$. The code F is called asymptotically optimal if

$$\lim_{n\to\infty} \frac{M(n, w, \lambda)}{J(n, w, \lambda)} = 1 \tag{2}$$

There are many constructions of infinite families of (asymptotically) optimal (n, w, λ)-OOCs where $\lambda = 1$ or 2. However, for $\lambda > 2$ examples seem scarce.

Hereafter, q shall denote a prime power. In the foundational work of Chung, Salehi, and Wei [4], lines of $PG(d, q)$ are used to construct optimal OOCs with $\lambda = 1$. We briefly describe this method in the next section. In [9], the methods of [4] are applied to certain families of conics in $PG(2, q)$ in order to construct asymptotically optimal OOCs with $\lambda = 2$. In [1] the methods of [9] are generalized, using normal rational curves in $PG(d, q)$ to construct infinite families of asymptotically optimal $\left(\frac{q^{\lambda+2}-1}{q-1}, q+1, \lambda\right)$ OOCs. In the present paper we present some new constructions of OOCs using subspaces of $PG(n, q^k)$. In particular, we look OOCs constructed from sublines isomorphic to $PG(1, q)$ lying in $PG(2, q^k)$ and we look at families of arcs in Baer (and, in general, k^{th}-root) subspaces to construct new infinite families of asymptotically optimal OOCs. We will use the term *Baer subspace* to denote a subspace isomorphic to $PG(n, q)$ lying in $PG(n, q^2)$, and, in general, *root subspace* to denote a subspace isomorphic to $PG(n, q)$ lying in $PG(n, q^k)$.

2 OOCs from lines of $PG(d, q)$

In [4] Chung, Salehi, and Wei provide a method for constructing $(n, w, 1)$-OOCs using lines of the projective geometry $PG(d, q)$. Briefly, let ω be a primitive element of $GF(q^{d+1})$. The points of $\Sigma = PG(d, q)$ can be represented as $\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}$ where $n = \frac{q^{d+1}-1}{q-1}$. Hence, in a natural way a point set A of $PG(d, q)$ corresponds to binary n-tuple (or codeword) $(a_0, a_1, \ldots, a_{n-1})$ where $a_i = 1$ if and only if $\omega^i \in A$.

Denote by ϕ the collineation of Σ defined by $\omega^i \mapsto \omega^{i+1}$, a singer group acting on Σ. The map ϕ acts transitively on the points (and dually on the hyperplanes) of Σ. If A is a point set of Σ corresponding to the codeword $c = (a_0, a_1, \ldots, a_{n-1})$, then ϕ induces a cyclic shift on the coordinates of c.

For each line ℓ of Σ, consider the orbit $\mathcal{O}_\ell$ under ϕ. If $\mathcal{O}_\ell$ is a full orbit (has size n) then a representative line and corresponding codeword is chosen. Short orbits are discarded. Let $\mathcal{L}(d, q)$ represent the cardinality of this set of chosen lines. Two lines of Σ intersect in at most one point and each line contains $q+1$ points. It follows that the codewords satisfy both $\lambda_a \leq 1$ and $\lambda_c \leq 1$ and by

counting the number of full orbits under ϕ the following is obtained.

Theorem 2 *For any prime power q and any positive integer d, there exists an (optimal) $\left(\frac{q^{d+1}-1}{q-1}, q+1, 1\right)$-OOC consisting of $\mathcal{L}(d,q) = \left\lfloor \frac{q^d-1}{q^2-1} \right\rfloor$ codewords.*

3 Codes from sublines of $PG(2, q^k)$

Our goal is to construct some new families of OOCs using techniques similar to those found in Chung, Salehi, and Wei [4]. In the most basic setting, we look at root sublines lying in the projective plane. We start with some basic properties of the geometry of these subspaces of the projective line. Recall that we use the term *root subline* to denote a projective line isomorphic to $PG(1, q)$ lying in $PG(1, q^k)$.

Lemma 3 *In $PG(1, q^k)$ let P be a distinguished point. Then there exist*

$$\frac{\binom{q^k}{2}}{\binom{q}{2}} = q^{k-1}(q^{k-1} + q^{k-2} + \cdots + q + 1)$$

root sublines containing P.

proof: As coordinates of $PG(1, q)$ are uniquely determined by 3 points, we have that three points uniquely determine a root subline. The number of root sublines through P is therefore $\frac{\binom{q^k}{2}}{\binom{q}{2}}$. ■

Let $\pi = PG(2, q^k)$ and let ℓ be a distinguished line of π. Let S be the set of all root sublines of ℓ containing P. Note that two members of S can meet in at most one point other than P (3 points uniquely determine a root subline). By removing P from each member of S we arrive at a collection, say S', of collinear q-sets no two meeting in as many as 2 points. The members of S' will correspond to the codewords in our code.

Let ω and ϕ be defined as in Section 2. Let ℓ' be in S'. Recall that a singer group acts regularly on the points and lines of π. Since any two lines of π meet in one point, ℓ' and $\phi^i(\ell')$ meet in at most one point. By associating a codeword (as in Section 2) with each member of S', we have the following.

Theorem 4 *Let q be a prime power and $k \geq 1$. Then there exists an $(q^{2k} + q^k + 1, q, 1)-OOC$ consisting of $q^{k-1}(q^{k-1} + q^{k-2} + \cdots + q + 1)$ codewords.*

The Johnson bound for the codes above is

$$J(q^{2k}+q^k+1,q,1)=\left\lfloor\frac{1}{q}\left\lfloor\frac{q^{2k}+q^k}{q-1}\right\rfloor\right\rfloor.$$

The size of the codes in Theorem 4 is

$$M(q^{2k}+q^k+1,q,1)=q^{k-1}(q^{k-1}+q^{k-2}+\cdots+q+1).$$

As such, taking asymptotics into account, we get the following limit.

$$\lim_{n\to\infty}\frac{M(n,w,\lambda)}{J(n,w,\lambda)}=\lim_{q\to\infty}\frac{q^{2k-2}}{q^{2k-2}}=1 \tag{3}$$

Hence, our codes are asymptotically optimal.

We note that

$$J(q^4+q^2+1,q,1)=\left\lfloor\frac{1}{q}\left\lfloor\frac{q^4+q^2}{q-1}\right\rfloor\right\rfloor\left(=q^2+q+2,\text{ for } q>3\right)$$

It follows that for $q>3$, the OOCs constructed as above using Baer sublines are just 2 words shy of optimal.

4 Arcs and Baer subspaces in $PG(d,q^2)$

The projective space $PG(d,q^2)$ contains subspaces isomorphic to $PG(d,q)$, otherwise known as *Baer subspaces*. For a comprehensive introduction to Baer subspaces see [11]. The coordinates of all points in $PG(d,q)$ are uniquely determined once the coordinates of $d+2$ fundamental points have been chosen. As such, we have the following Lemma.

Lemma 5 *A set of $d+2$ points in general position (i.e. a $(d+2)$-arc) in $PG(d,q^2)$ uniquely determines a Baer subspace.*

Denote by $\mathcal{B}(d,q^2)$ the number of Baer subspaces of $PG(d,q^2)$. Then

$$\mathcal{B}(d,q^2)=\frac{|PGL(d+1,q^2)|}{|PGL(d+1,q)|}=q^{\frac{d(d+1)}{2}}\prod_{i=2}^{d+1}(q^i+1). \tag{4}$$

An *m-arc* in $PG(d,q)$ is a collection of $m > d$ points such that no $d+1$ are incident with a common hyperplane. It follows that if $\mathcal{K}$ is an m-arc in $PG(d,q)$ then no $d+1$ points of $\mathcal{K}$ lie on a hyperplane, no d lie on a $(d-2)$-flat,..., no 3 lie on a line. A point $P \in PG(d,q)$ is an *extending point* of an m-arc $\mathcal{K}$ if $\{P\} \cup \mathcal{K}$ is an $(m+1)$-arc. An arc $\mathcal{K}$ is called *complete* if it is maximal with respect to inclusion (i.e. there are no points extending $\mathcal{K}$).

In $PG(2,q)$, a (non-degenerate) conic is a $(q+1)$-arc and elementary counting shows that this arc is complete when q is odd. The $(q+2)$-arcs (hyperovals) exist in $PG(2,q)$ if q is even and they are necessarily maximal. It is a long standing conjecture that, except for some special cases, the maximum size of an arc in $PG(d,q)$, $d > 2$ is $q+1$. Conics are a special case of the so called normal rational curves.

Definition 6 *A normal rational curve (NRC) in $PG(d,q)$, $2 \leq d \leq q-2$ is a $(q+1)$-arc projectively equivalent to the $(q+1)$-arc $\{(1,t,\ldots,t^d) \,|\, t \in GF(q)\} \cup \{(0,\ldots,0,1)\}$.*

If $\mathcal{C}$ is an NRC in $PG(d,q)$ then the subgroup of $PGL(d+1,q)$ leaving $\mathcal{C}$ fixed is isomorphic to $PGL(2,q)$. It follows that if $\nu(d,q)$ denotes the number of distinct normal rational curves in $PG(d,q)$ then

$$\nu(d,q) = \frac{|PGL(d+1,q)|}{|PGL(2,q)|} = \frac{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)}{(q^2-1)(q^2-q)} \tag{5}$$

The following is a well known property of NRCs (see [12]).

Theorem 7 *A $(d+3)$-arc in $PG(d,q)$ is contained in a unique normal rational curve.*

Definition 8 *Let $\pi = PG(d,q)$. A t-family $\mathcal{F}$ of m-arcs in π is a collection of m-arcs mutually meeting in at most t points.*

Lemma 9 *Let $\pi = PG(d,q)$, $d \geq 2$. Then the number of NRCs containing two fixed points of π is $q^{\frac{d^2+d-2}{2}} \prod_{i=1}^{d-1}(q^i-1)$.*

proof: In $\pi = PG(d,q)$ fix two points P and Q. Denote by X_d the number of NRCs containing P and Q. By counting ordered triples $(\mathcal{N}, P_1, P_2)$ where $\mathcal{N}$ is a NRC in π and P_1 and P_2 are distinct points of $\mathcal{N}$ we get

$$\frac{|PGL(d+1,q)|}{|PGL(2,q)|}(q+1)(q) = \left(\frac{q^{d+1}-1}{q-1}\right)\left(\frac{q^{d+1}-1}{q-1}-1\right)X_d \tag{6}$$

which gives

$$X_d = (q^{d+1} - q^2)(q^{d+1} - q^3) \cdots (q^{d+1} - q^d) = q^{\frac{d^2+d-2}{2}} \prod_{i=1}^{d-1} (q^i - 1). \tag{7}$$

■

Corollary 10 *In $\pi = PG(d, q)$, $d \geq 2$, there exists a d-family $\mathcal{F}$ of $(q-1)$-arcs where $|\mathcal{F}| = q^{\frac{d^2+d-2}{2}} \prod_{i=1}^{d-1}(q^i - 1)$*

proof: Two NRCs in π intersect in at most $d + 2$ points. Hence, removing P and Q from each of the X_d NRCs constructed in Lemma 9 we arrive at a d-family $\mathcal{F}$ of $(q-1)$-arcs. ■

Lemma 11 *Let $\Pi = PG(d, q^2)$. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be distinct Baer subspaces of Π both containing the point P. Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be arcs in $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively, both having P as an extending point. Then $|\mathcal{K}_1 \cap \mathcal{K}_2| \leq d$.*

proof: Let $\mathcal{K} = \mathcal{K}_1 \cap \mathcal{K}_2$. By assumption, $\mathcal{K}' = \mathcal{K} \cup \{P\}$ is an arc contained in both $\mathcal{B}_1$ and $\mathcal{B}_2$. If $|\mathcal{K}| \geq d + 1$ then $|\mathcal{K}'| \geq d + 2$ whence $\mathcal{B}_1$ and $\mathcal{B}_2$ coincide (Lemma 5), a contradiction. ■

Lemma 12 *Let $\Pi = PG(d, q^2)$. The number of Baer subspaces through a fixed point is*

$$q^{\frac{d(d+1)}{2}} \prod_{i=1}^{d} (q^i + 1).$$

proof: Choose a point $P \in \Pi$ and denote by Y_P the number of Baer subspaces containing P. By counting ordered pairs $(\mathcal{B}, Q)$ where $\mathcal{B}$ is a Baer subspace of Π and Q is a point in $\mathcal{B}$ we get

$$\mathcal{B}(d, q^2) \cdot |PG(d, q)| = |PG(d, q^2)| \cdot Y_P$$

from which we get

$$Y_P = \frac{\mathcal{B}(d, q^2)(q+1)}{q^{d+1} + 1} = q^{\frac{d(d+1)}{2}} \prod_{i=1}^{d} (q^i + 1). \tag{8}$$

■

Theorem 13 *Let $\Pi = PG(d, q^2)$. Then Π contains a d-family $\mathcal{F}$ of $(q-1)$-*

arcs where

$$|\mathcal{F}| = q^{d^2+d-2}\left(q^d+1\right)\prod_{i=1}^{d-1}(q^{2i}-1)$$

proof: Fix a point $P \in \Pi$ and consider the set A of all Baer subspaces containing P. Within each Baer subspace $\mathcal{B} \in A$ we construct a d-family of $(q-1)$-arcs as follows. Choose a point $Q \in \mathcal{B}$, $Q \neq P$. By considering the collection of NRCs containing both P and Q we construct (as in Lemma 9 and Corollary 10) a d-family of $(q-1)$-arcs having size

$$q^{\frac{d^2+d-2}{2}}\prod_{i=1}^{d-1}(q^i-1) \tag{9}$$

Denote this family $\mathcal{F}(\mathcal{B})$. Note that both P and Q are extending points of each member of $\mathcal{F}(\mathcal{B})$. Define the collection $\mathcal{F}$, of $(q-1)$-arcs as

$$\mathcal{F} = \bigcup_{\mathcal{B}\in A}\{\mathcal{F}(\mathcal{B})\} \tag{10}$$

From Lemma 11 it follows that $\mathcal{F}$ is a d-family of arcs. Using (9) and Lemma 12 we then have

$$\begin{aligned}|\mathcal{F}| &= \left(q^{\frac{d^2+d-2}{2}}\prod_{i=1}^{d-1}(q^{\,i}-1)\right)\left(q^{\frac{d(d+1)}{2}}\prod_{i=1}^{d}(q^{\,i}+1)\right)\\ &= q^{d^2+d-1}\left(q^{\,d}+1\right)\prod_{i=1}^{d-1}(q^{2i}-1).\end{aligned}$$

■

5 OOCs in $PG(d, q^2)$

Let $\Pi = PG(d, q^2)$, $d > 1$. Let $\mathcal{F}$ be a d-family of $(q-1)$-arcs constructed as in Theorem 13. Consider Π as embedded in $\Sigma = PG(d+1, q^2)$. Let ω be a primitive element of $GF(q^{2d+4})$. Identify each arc in $\mathcal{F}$ (considered as a point set in Σ) with the corresponding codeword of length $\frac{q^{2d+4}-1}{q^2-1}$ and weight $q-1$. As before, let $\phi : \omega^i \mapsto \omega^{i+1}$ be a singer group acting on Σ. Let $\mathcal{K}$ be an arc in $\mathcal{F}$. Then we have

$$\lambda_a = \max\left|\{\mathcal{K} \cap \phi^i(\mathcal{K}) | 1 \leq i \leq n-1\}\right|.$$

As $\mathcal{K} \cap \phi^i(\mathcal{K}) \subset \Pi \cap \phi^i(\Pi)$ (a hyperplane of Π), and an arc in Π intersects a hyperplane in at most d points, we get $\lambda_a \leq d$. Similarly,

$$\lambda_c = \max|\{\mathcal{K} \cap \phi^i(\mathcal{K}')|\mathcal{K} \neq \mathcal{K}' \in \mathcal{F}, 0 \leq i \leq n-1\}|$$

If $i \neq 0$ then (as above) this number is at most d. If $i = 0$ then $\mathcal{K}$ and $\phi^i(\mathcal{K}')$ are in Π and can therefore share as many as d points so $\lambda_c = d$.

Denote by L the collection of $\mathcal{L}(d+1, q^2)$ lines of Π having full orbit (as in Theorem 2). Two lines of Σ intersect in at most one point and a line intersects an arc in at most two points. It follows that if $\ell \in L$ and $S_1, S_2 \subseteq \ell$ are sets of size $q-1$ intersecting in at most 2 points then the codewords corresponding to S_1 and S_2 may be added to C. Any two Baer sublines of ℓ intersect in at most 2 points. Therefore, by arbitrarily removing 2 points from each Baer subline of ℓ we may construct $\mathcal{B}(1, q^2)$ new codewords that may be added to C. Thus, we have the following.

Theorem 14 *For $\lambda = d > 1$ and q a prime power, there exists a $\left(\frac{q^{2(d+2)}-1}{q^2-1}, q-1, d\right)$-OOC C where*

$$|C| = q^{d^2+d-1}\left(q^d+1\right)\prod_{i=1}^{d-1}(q^{2i}-1) + \mathcal{B}(1,q^2)\mathcal{L}(d+1,q^2)$$

5.1 Optimality

Fix $\lambda = d > 1$ and consider the infinite family of (n, w, d)-OOCs constructed as for Theorem 14. The Johnson bound for these codes is

$$J(n,w,d) = \left\lfloor \frac{1}{q-1}\left\lfloor \frac{\frac{q^{2d+4}-1}{q^2-1}-1}{q-2}\left\lfloor \frac{\frac{q^{2d+4}-2}{q^2-1}-2}{q-3}\left\lfloor \cdots \left\lfloor \frac{\frac{q^{2d+4}-d}{q^2-1}-d}{q-1-d}\right\rfloor\right\rfloor\right\rfloor\right\rfloor .$$

The size of the codes in Theorem 14 is

$$M(n,w,d) = q^{d^2+d-1}\left(q^d+1\right)\prod_{i=1}^{d-1}(q^{2i}-1) + (q^3+q)\left\lfloor \frac{q^{2d+2}-1}{q^4-1}\right\rfloor .$$

As such we get the following limit.

$$\lim_{n\to\infty}\frac{M(n,w,d)}{J(n,w,d)} = \lim_{q\to\infty}\frac{q^{2d^2+d-1}}{q^{2d^2+d-1}} = 1 \tag{11}$$

Hence (Definition 1) we get the following Theorem.

Theorem 15 *For each $\lambda > 1$, the corresponding infinite family of OOCs in Theorem 14 is asymptotically optimal.*

Table 1 shows the comparison of the size of some of the codes constructed above with with the Johnson bound.

Table 1
Comparison of the codes constructed in Section 5 with the Johnson bound.

q	$\frac{M(n,w,\lambda)}{J(n,w,\lambda)}, \lambda = 2$	$\frac{M(n,w,\lambda)}{J(n,w,\lambda)}, \lambda = 3$	$\frac{M(n,w,\lambda)}{J(n,w,\lambda)}, \lambda = 4$
7	.33574	.13841	.03864
27	.79039	.67148	.54636
64	.90847	.85128	.78458
121	.95103	.91947	.88141
343	.98258	.97111	.95694
961	.99377	.98963	.98448

6 Generalizations to $PG(d, q^k)$

For k a positive integer, let $\Sigma = PG(d, q^k)$. The projective space Σ contains k^{th}-root subspaces isomorphic to $PG(d, q)$, which we refer to as *root subspaces*. Once again, as the coordinates of $PG(d, q)$ are uniquely determined by $d + 2$ fundamental points we have the following Lemma.

Lemma 16 *A set of $d + 2$ points in general position (i.e. a $(d + 2)$-arc) in $\Sigma = PG(d, q^k)$ uniquely determines a root subspace.*

Denote by $\mathcal{B}(d, q^m)$ the number of root subspaces of $PG(d, q^k)$. Then

$$\mathcal{B}(d, q^k) = \frac{\left|PGL(d+1, q^k)\right|}{|PGL(d+1, q)|} = \frac{(q^{k(d+1)} - 1)(q^{k(d+1)} - q^k) \cdots (q^{k(d+1)} - q^{kd}) \cdot (q-1)}{(q^{d+1} - 1)(q^{d+1} - q) \cdots (q^{d+1} - q^d) \cdot (q^k - 1)}. \quad (12)$$

The proof of the following is entirely similar to that of Lemma 11.

Lemma 17 *Let $\Pi = PG(d, q^m)$ and fix $P \in \Pi$. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be distinct root subspaces of Π containing P. Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be arcs in $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively, both having P as an extending point. Then $|\mathcal{K}_1 \cap \mathcal{K}_2| \leq d$.*

Lemma 18 *Let $\Pi = PG(d, q^k)$ and fix a point P in Π. The number of root*

subspaces of Π *containing* P *is*

$$\frac{\left(q^{k(d+1)}-q^k\right)\left(q^{k(d+1)}-q^{2k}\right)\cdots\left(q^{k(d+1)}-q^{kd}\right)}{\left(q^{d+1}-q\right)\left(q^{d+1}-q^2\right)\cdots\left(q^{d+1}-q^d\right)}. \tag{13}$$

proof: Choose a point $P \in \Pi$ and denote by Z_P the number of subspaces isomorphic to $PG(d,q)$ containing P. By counting ordered pairs $(\mathcal{B}, Q)$ where $\mathcal{B}$ is a subspace and Q is a point in $\mathcal{B}$ we get

$$\mathcal{B}(d,q^k)\cdot|PG(d,q)| = |PG(d,q^k)|\cdot Z_P.$$

Substituting equation (12), we get

$$Z_P = \mathcal{B}(d,q^k)\frac{q^{d+1}-1}{q-1}\frac{q^k-1}{q^{k(d+1)}-1} = \frac{(q^{k(d+1)}-q^k)(q^{k(d+1)}-q^{2k})\cdots(q^{k(d+1)}-q^{kd})}{(q^{d+1}-q)(q^{d+1}-q^2)\cdots(q^{d+1}-q^d)}. \tag{14}$$

■

Theorem 19 *Let* $\Pi = PG(d,q^k)$. *Then* Π *contains a* d*-family* $\mathcal{F}$ *of* $(q-1)$*-arcs where*

$$|\mathcal{F}| = \frac{\left(q^{k(d+1)}-q^k\right)\left(q^{k(d+1)}-q^{2k}\right)\cdots\left(q^{k(d+1)}-q^{kd}\right)}{\left(q^{d+1}-q\right)}$$

proof: Fix a point $P \in \Pi$ and consider the set A of all root subspaces of Π containing P. Within each member of A we construct a d-family of $(q-1)$-arcs as follows. Choose a point $Q \in \mathcal{B}$, $Q \neq P$. By considering the collection of all NRCs containing P and Q we may construct (as in Lemma 9 and Corollary 10 a d-family of $(q-1)$-arcs having size

$$\left(q^{d+1}-q^2\right)\left(q^{d+1}-q^3\right)\cdots\left(q^{d+1}-q^d\right) \tag{15}$$

Denote this family by $\mathcal{F}(\mathcal{B})$. Note that both P and Q are extending points of each member of $\mathcal{F}(\mathcal{B})$. Define the collection $\mathcal{F}$, of $(q-1)$-arcs as

$$\mathcal{F} = \bigcup_{\mathcal{B}\in A}\{\mathcal{F}(\mathcal{B})\} \tag{16}$$

From Lemma 17 it follows that $\mathcal{F}$ is a d-family. Using (15) and Lemma 18 we arrive at the following.

$$|\mathcal{F}| = Z_P\cdot\left(q^{d+1}-q^2\right)\left(q^{d+1}-q^3\right)\cdots\left(q^{d+1}-q^d\right)$$

$$= \frac{\left(q^{k(d+1)} - q^k\right)\left(q^{k(d+1)} - q^{2k}\right)\cdots\left(q^{k(d+1)} - q^{kd}\right)}{(q^{d+1} - q)}$$

■

Let $\Pi = PG(d, q^k)$, $k, d > 1$. As in Section 5, consider Π as embedded in $\Sigma = PG(d+1, q^2)$ and identify each arc in $\mathcal{F}$ with the naturally corresponding codeword (of length $\frac{q^{k(d+2)}-1}{q^k-1}$ and weight $q-1$). Denote by L the collection of $\mathcal{L}(d+1, q^k)$ lines of Π having full orbit (as in Theorem 2). If $\ell \in L$ then any two root sublines of ℓ intersect in at most 2 points. Therefore, by arbitrarily removing 2 points from each root subline of ℓ we may construct $\mathcal{B}(1, q^k)$ new codewords that may be added to C. Thus, we have the following.

Theorem 20 *For $\lambda = d > 1$, k a positive integer, and q a prime power, there exists a $\left(\frac{q^{k(d+2)}-1}{q^k-1}, q-1, d\right)$-OOC C where*

$$|C| = \frac{\left(q^{k(d+1)} - q^k\right)\left(q^{k(d+1)} - q^{2k}\right)\cdots\left(q^{k(d+1)} - q^{kd}\right)}{(q^{d+1} - q)} + \mathcal{B}(1, q^k) \cdot \mathcal{L}(d+1, q^k).$$

6.1 Optimality

Fix $\lambda = d > 1$ and $k \geq 2$ and consider the infinite family of (n, w, d)-OOCs constructed as for Theorem 20. The Johnson bound for these codes is

$$J(n, w, d) = \left\lfloor \frac{1}{q-1} \left\lfloor \frac{\frac{q^{k(d+2)}-1}{q^k-1} - 1}{q-2} \left\lfloor \frac{\frac{q^{k(d+2)}-1}{q^k-1} - 2}{q-3} \left\lfloor \cdots \left\lfloor \frac{\frac{q^{k(d+2)}-1}{q^k-1} - d}{q-1-d} \right\rfloor \right\rfloor \right\rfloor \right\rfloor .$$

The size of the codes in Theorem 14 is

$$M(n, w, d) = \frac{\left(q^{k(d+1)} - q^k\right)\left(q^{k(d+1)} - q^{2k}\right)\cdots\left(q^{k(d+1)} - q^{kd}\right)}{(q^{d+1} - q)} + \mathcal{B}(1, q^k) \cdot \mathcal{L}(d+1, q^k).$$

As such we get the following limit.

$$\lim_{n\to\infty} \frac{M(n, w, d)}{J(n, w, d)} = \lim_{q\to\infty} \frac{q^{k(d^2+d)-d-1}}{q^{k(d^2+d)-d-1}} = 1 \tag{17}$$

Hence (Definition 1) we get the following Theorem.

Theorem 21 *For each $\lambda > 1$, and each positive integer k, the corresponding infinite family of OOCs in Theorem 20 is asymptotically optimal.*

Tables 2 and 3 show the comparison of the size of some of the codes constructed above with with the Johnson bound. Note that in each table, column 1 corresponds to the codes constructed in Section 5.

Table 2
Comparison of some $(n, w, 2)$-OOCs constructed in Section 6 with the Johnson bound.

q	$\frac{M(n,w,2)}{J(n,w,2)}, k=2$	$\frac{M(n,w,2)}{J(n,w,2)}, k=3$	$\frac{M(n,w,2)}{J(n,w,2)}, k=4$
7	.33574	.35403	.35670
27	.79039	.79353	.79365
64	.90847	.90912	.90913
121	.95103	.91522	.95123
343	.98258	.98261	.98261
961	.99377	.99377	.99377

Table 3
Comparison of some $(n, w, 3)$-OOCs constructed in Section 6 with the Johnson bound.

q	$\frac{M(n,w,3)}{J(n,w,3)}, k=2$	$\frac{M(n,w,3)}{J(n,w,3)}, k=3$	$\frac{M(n,w,3)}{J(n,w,3)}, k=4$
7	.13841	.14863	.15038
27	.67148	.67504	.67517
64	.85128	.85210	.85211
121	.91947	.91972	.91972
343	.97111	.97114	.97114
961	.98963	.98963	.98963

7 Conclusion

We have shown that geometric objects such as Baer subspaces, k^{th}-root subspaces, and normal rational curves can be utilized in various ways as a robust method for generating large classes of optical orthogonal codes. Moreover, many of the classes of codes have optimal properties that make them ideal for implementation. It would be interesting to see how other geometric objects in projective spaces, like quadratic or Hermitian surfaces for instance, might be used in the construction of new codes with desirable correlation properties.

References

[1] Alderson, T. L., Optical Orthogonal Codes and Arcs in $PG(d, q)$, Finite Fields Appl., (to appear).

[2] Bird, C. M. and Keedwell, A. D., Design and applications of optical orthogonal codes—a survey, Bull. Inst. Combin. Appl., 11 (1994) 1183-1287.

[3] Chung, Habong and Kumar, P. Vijay, Optical orthogonal codes—new bounds and an optimal construction, IEEE Trans. Inform. Theory, 36 (1990) no. 4, 866-873.

[4] Chung, Fan R. K. and Salehi, Jawad A. and Wei, Victor K., Optical orthogonal codes: design, analysis, and applications, IEEE Trans. Inform. Theory, 35 (1989) 595-604.

[5] Healy, Timothy J., Coding and decoding for code division multiple user communication systems, IEEE Trans. Comm., 33 (1985) no. 4, 310-316.

[6] Johnson, Selmer M., A new upper bound for error-correcting codes, IRE Trans., IT-8 (1962),203–207.

[7] Maric S. V, Moreno O., and Corrada,C., Multimedia transmission in fiber-optic LANs using optical CDMA, J. Lightwave Technol., 14 (1996) 2149-2153.

[8] Moreno, Oscar and Zhang, Zhen and Kumar, P. Vijay and Zinoviev, Victor A., New constructions of optimal cyclically permutable constant weight codes, IEEE Trans. Inform. Theory, 41 (1995) no. 2, 448-455.

[9] Miyamoto, Nobuko and Mizuno, Hirobumi and Shinohara, Satoshi, Optical orthogonal codes obtained from conics on finite projective planes, Finite Fields Appl., 10, no. 3 (2004) 405-411.

[10] Nguyen Q. A and Györfi, László and Massey, James L., Constructions of binary constant-weight cyclic codes and cyclically permutable codes, IEEE Trans. Inform. Theory, 38, no. 3 (1992) 940-949.

[11] Svéd, M., Baer Subspaces in the N Dimensional Projective Space, Combinatorial Mathematics X, Lec. Notes in Math., 1036, Springer-Verlag (1983) 375-391.

[12] Thas, Joseph A., Projective geometry over a finite field, Handbook of incidence geometry, North-Holland, Amsterdam (1995) 295–347.