Optical Orthogonal Codes from Singer Groups

T. L. Alderson *
Mathematical Sciences
University of New Brunswick
Saint John, NB.
E2L 4L5
Canada
tim@combinatorics.ca

Keith E. Mellinger†
Department of Mathematics
University of Mary Washington
Fredericksburg, VA
22401
USA
kmelling@umw.edu

Abstract

We construct some new families of optical orthogonal codes that are asymptotically optimal. In particular, for any prescribed value of λ, we construct infinite families of (n, w, λ)-OOCs that in each case are asymptotically optimal. Our constructions rely on various techniques in finite projective spaces involving normal rational curves and Singer groups. These constructions generalize and improve previous constructions of OOCs, in particular, those from conics [14] and arcs [1].

1 Introduction

There is interest in applying code-division multiple-access (CDMA) techniques to optical networks (OCDMA) and the codes used in an OCDMA system are called *optical orthogonal codes*. An $(n, w, \lambda_a, \lambda_c)$-optical orthogonal code (OOC) is a family of binary sequences (codewords) of length n, and 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 $\sum_{i=1}^{n-1} c_i c_{i+t} \leq \lambda_a$
- (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.

As stated above, an application of optical orthogonal codes is to optical CDMA communication systems where binary codewords with strong correlation properties are required (see [5, 6, 11] for more details). Subsequently, OOCs have been used for multimedia transmissions in networks using fiber-optics [13]. Optical orthogonal codes have also been called cyclically permutable constant weight codes in the construction of protocol sequences for multiuser collision channels without feedback [15]. Mathematically, OOCs have been studied in their own right because of their connection to various problems that arise naturally in combinatorics. For instance, there is a fundamental equivalence between optimal OOCs and maximum cyclic t-difference packings [10].

An $(n, w, \lambda_a, \lambda_c)$-OOC with $\lambda_a = \lambda_c$ is denoted an (n, w, λ)-OOC. The number of codewords is the *size* of the code. For fixed values of n, w, λ_a and λ_c, the largest size of an $(n, w, \lambda_a, \lambda_c)$-OOC

*The author acknowledges support from the N.S.E.R.C. of Canada

†The author acknowledges support by a Jepson Fellowship from the University of Mary Washington and National Security Agency grant #H98230-06-1-0080

is denoted $\Phi(n, w, \lambda_a, \lambda_c)$. An $(n, w, \lambda_a, \lambda_c)$-OOC of size $\Phi(n, w, \lambda_a, \lambda_c)$ is said to be *optimal*. In applications, optimal OOCs facilitate the largest possible number of asynchronous users to transmit information efficiently and reliably. From the Johnson Bound for constant weight codes it follows [6] that

$$\Phi(n, w, \lambda) \leq \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \right\rfloor \cdots \right\rfloor \right\rfloor. \tag{1.1}$$

Much of the literature is restricted to (n, w, λ)-OOCs. 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 (1.1). Alternatively, in [19], Yang and Fuja discuss OOCs with $\lambda_a > \lambda_c$ and a corresponding bound is established. The codes we construct in Sections 3 and 4 both have $\lambda_a = \lambda_c$ and, as such, (1.1) seems the only applicable bound.

We now carefully define the concept of an OOC being asymptotically optimal. Let F be an infinite family of OOCs of varying length n 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 $J(n, w, \lambda)$.

Definition 1.1. The family F is called asymptotically optimal if

$$\lim_{n\to\infty} \frac{M(n, w, \lambda)}{J(n, w, \lambda)} = 1. \tag{1.2}$$

For $\lambda = 1, 2$ there are many constructions of (asymptotically) optimal families of (n, w, λ)-OOCs. For $\lambda > 2$ however, constructive examples seem relatively scarce. In [1, 3, 4, 14], methods of projective geometry are successfully employed to provide asymptotically optimal families of OOCs with $\lambda \geq 2$. In the present work we generalize the previous constructions. In particular, for each prescribed $\lambda \geq 2$ we provide several new asymptotically optimal families of OOCs (Theorems 3.4, 5.2 and Corollaries 4.2, 4.4, 5.3, and 5.6). The codes constructed in Theorem 5.2 have the same or similar parameters to those constructed in [14] yet compare more favorably with the Johnson Bound (JB). For instance, Table 1 shows how the sizes of some of our codes compare to some previously known codes. We remark that the construction given in [14] is a special case of our Corollary 4.2 by taking $k = 3$. We also mention that the construction provided in Corollary 4.4 is a strict improvement to the main results of [1].

Table 1: Comparison of constructions of $(n, 9, \lambda)$-OOCs

n	λ	$\lvert C\rvert$	JB	$\lvert C\rvert/JB$	Reference
585	2	456	673	0.6775631501	[14], Proposition 6
511	2	448	510	0.8784313727	Theorem 5.2 ($k = 3$, $q = 8$)
4681	3	14450752	33845825	0.4269581846	[1], Theorem 9
4681	3	14479433	33845825	0.4278055860	Corollary 4.4 ($k = 4$, $q = 8$)

2 Preliminaries

As our work relies heavily on the structure of finite projective spaces, we start with a short overview of the fundamental concepts needed. We let $PG(k, q)$ represent the finite projective geometry of dimension k and order q. Due to a result of Veblen and Young in the early 1900s, all finite projective spaces of dimension not equal to two are equivalent up to the order. The space $PG(k, q)$ can be modeled easily with the vector space of dimension $k + 1$ over the finite field $GF(q)$. In this model, the one-dimensional subspaces represent the points, two-dimensional subspaces represent lines, etc. Using this model, it is not hard to show by elementary counting that the number of points of $PG(k, q)$ is given by $\theta(k, q) = \frac{q^{k+1}-1}{q-1}$. We will continue to use the symbol $\theta(k, q)$ to represent this number.

The Fundamental Theorem of Projective Geometry states that the full automorphism group of $PG(k,q)$ is the group $P\Gamma L(k+1,q)$ of semilinear transformations acting on the underlying vector space. The subgroup $PGL(k+1,q) \cong GL(k+1,q)/Z_0$ (where Z_0 represents the center of the group $GL(k+1,q)$) of projective linear transformations is easily modeled by matrices and will be referred to in some of our discussions. A Singer group is a cyclic group acting sharply transitively on the points and hyperplanes of $PG(k,q)$, and the generator of such a group is known as a Singer cycle. Singer groups are known to exists in projective spaces of any order and dimension.

Another property that will provide some assistance is the principle of duality. For any result about points of $PG(k,q)$, there is always a corresponding result about hyperplanes (subspaces, or *flats*, of dimension $k-1$). More generally, for any result dealing with flats of $PG(k,q)$, replacing each reference to an m-flat, $m < k$, with a reference to a $(k-m-1)$-flat, yields a corresponding *dual* statement that has the same truth value. For instance, a result about a set of points of $PG(k,q)$, no three of which are collinear, could be rewritten dually about a set of hyperplanes of $PG(k,q)$, no three of which meet in a common $(k-2)$-flat.

In [6] Chung, Salehi, and Wei provide a method for constructing $(n,w,1)$-OOCs using lines of the projective geometry $PG(k,q)$. As our methods may be viewed as a generalization of this construction, we describe the technique in detail. The idea makes use of a so-called Singer group that is most easily understood by modeling a finite projective space using a finite field. If we let ω be a primitive element of $GF(q^{k+1})$, the points of $\Sigma = PG(k,q)$ can be represented by the field elements $\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}$ where $n = \frac{q^{k+1}-1}{q-1}$. Hence, in a natural way a point set A of $PG(k,q)$ corresponds to a binary n-tuple (or codeword) $(a_0, a_1, \ldots, a_{n-1})$ where $a_i = 1$ if and only if $\omega^i \in A$.

Recall that the non-zero elements of $GF(q^{k+1})$ form a cyclic group under multiplication. Moreover, it is not hard to show that multiplication by ω induces an automorphism, or collineation, on the associated projective space $PG(k,q)$. Denote by ϕ the collineation of Σ defined by $\omega^i \mapsto \omega^{i+1}$. The map ϕ clearly acts transitively on the points (and dually on the hyperplanes) of Σ. It is important to note that 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 $\Sigma = PG(k,q)$, consider its orbit $\mathcal{O}_\ell$ under ϕ. We say $\mathcal{O}_\ell$ is a *full orbit* if it has size $n = \theta(k,q)$). Let $\mathcal{L}(k,q)$ denote the number of full line orbits. A variety of techniques for determining $\mathcal{L}(k,q)$ exist in the literature (in sections 4,5 of [5] Bird and Keedwell employ methods of design theory, whereas in section 5 of [9], Ebert *et. al.* take a more geometrical approach). If $\mathcal{O}_\ell$ is a full orbit then a representative line and corresponding codeword is chosen. Short orbits are discarded. Let 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 the following is obtained.

Theorem 2.1. *For any prime power q and any positive integer k, there exists a $(\theta(k,q), q+1, 1)$-OOC consisting of $\mathcal{L}(k,q) = \left\lfloor \frac{q^k-1}{q^2-1} \right\rfloor$ codewords.*

Our new constructions of asymptotically optimal OOCs will also rely on orbits of Singer groups. However, we consider the orbits of flats of varying dimension. As such, we let $\begin{bmatrix} k+1 \\ d+1 \end{bmatrix}_q$ denote the number of d-flats in $PG(k,q)$. Elementary counting can be used to show that

$$\begin{bmatrix} k+1 \\ d+1 \end{bmatrix}_q = \frac{(q^{k+1}-1)(q^{k+1}-q)\cdots(q^{k+1}-q^d)}{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)} \approx q^{(k-d)(d+1)}.$$

Moreover, it is well understood that in $PG(k,q)$, not all orbits of d-flats are full orbits (having size $\theta(k,q)$). The number of orbits of d-flats of varying lengths was investigated in [8]. We let $\mathcal{N}_q(d,k)$ be the number of full d-flat orbits in $PG(k,q)$. Hence, using the notation from the construction above, $\mathcal{N}_q(1,k) \equiv \mathcal{L}(k,q)$. The following lemma is a consequence of Theorem 2.1 of [8] and shall prove useful in our new constructions of asymptotically optimal OOCs. Note that the count in Theorem 2.1 is a special case of the following.

Lemma 2.2. *Using the notation above,*

$$\mathcal{N}_q(d,k) = \left\lfloor \frac{1}{\theta(k,q)} \left[\begin{array}{c} k+1 \\ d+1 \end{array} \right]_q \right\rfloor \approx q^{(k-d-1)d}.$$

The final concept from finite projective geometry that we make use of is that of an *arc*. An *m-arc* in $PG(d,q)$ is a collection of $m > d$ points that meets some hyperplane in d points and meets no hyperplane in as many as $d+1$ points. 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. An arc is called *complete* if it is maximal with respect to inclusion. The concept of an arc generalizes naturally. We define an m-arc of *degree* r $(\geq d)$ in $PG(d,q)$ to be a set of m points of $PG(d,q)$ that meets some hyperplane in r points and meets no hyperplane in as many as $r+1$ points. Hence, arcs of degree d are simply arcs. In the plane $PG(2,q)$, for instance, an arc of degree 2 is simply an arc, and an arc of degree 3 (also known as a *cubic arc*) is a set of points such that no 4 points lie on a common line. There is a great deal of literature regarding the connection between arcs and other classes of error-correcting codes including low-density parity-check codes [7] and MDS codes [2].

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. In fact, a well-known result of Segre says that every complete arc of $PG(2,q)$, q odd, is a conic. The $(q+2)$-arcs (hyperovals) exist in $PG(2,q)$ if q is even and they are necessarily complete. Conics are a special case of the so called normal rational curves. A *rational curve* $\mathcal{C}_n$ of order n in $PG(d,q)$ is a set of points

$$\{P(t) = (g_0(t_0,t_1), \ldots, g_d(t_0,t_1)) \,|\, t_0, t_1 \in GF(q)\}$$

where each g_i is a binary form of degree n and the highest common factor of $g_0, g_1, \ldots, g_d$ is 1. The curve $\mathcal{C}_n$ may also be written

$$\{P(t) = (f_0(t), \ldots, f_d(t)) \,|\, t \in GF(q) \cup \{\infty\}\} \tag{2.1}$$

where $f_i(t) = g_i(1,t)$.

Definition 2.3. A normal rational curve (NRC) in $PG(d,q)$, $2 \leq d \leq q-2$ is a rational curve (of order d) projectively equivalent to

$$\{(1,t,\ldots,t^d) \,|\, t \in GF(q)\} \cup \{(0,\ldots,0,1)\}.$$

It is well-known that an NRC is, in fact, a $(q+1)$-arc. 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) $PGL(2,q)$ (see [12] Theorem 27.5.3). It follows that if $\nu(d,q)$ denotes the number of distinct normal rational curves in $PG(d,q)$ then

$$\nu(d,q) = \frac{|PGL(d+1,q)|}{|PGL(2,q)|} = \frac{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)}{(q^2-1)(q^2-q)} \tag{2.2}$$

The following is a well known property of NRCs (see [18]).

Theorem 2.4. *For $2 \leq d \leq q-2$, a $(d+3)$-arc in $PG(d,q)$ is contained in a unique normal rational curve.*

Definition 2.5. Let $\pi = PG(d,q)$. A collection $\mathcal{F}$ of m-arcs (perhaps of varying degrees) in π is said to be a t-family if every pair of distinct members of $\mathcal{F}$ meet in at most t points. By $\mathcal{F}_q^d(m,r,t)$ we denote the maximal size in $PG(d,q)$ of a t-family of m-arcs each having degree at most r $(\geq d)$. If $r = d$ (and consequently all arcs are of degree d) we write $\mathcal{F}_q^d(m,t)$.

Remark 2.6. $\mathcal{F}_q^1(q+1,t) = 1$ for all $t \geq 1$ and in light of Theorem 2.4, $\mathcal{F}_q^d(q+1,d+i) \geq \nu(d,q)$ for all $i \geq 2$.

3 A construction from arcs in d-flats

Our first construction relies on arcs lying in d-flats of a large projective space over sufficiently large order q. Using families of arcs as defined in Definition 2.5, we obtain the following.

Theorem 3.1. *Fix k and d with $k > d \geq 1$. For each prime power $q \geq d$ there exists an $(\theta(k,q), m, d)$-OOC with*

$$|C| = \mathcal{F}_q^d(m,d) \cdot \mathcal{N}_q(d,k)$$

Proof. Let $\Sigma = PG(k,q)$, let ω be a primitive element of $GF(q^{k+1})$ with associated Singer cycle ϕ, and let $N = \mathcal{N}_q(d,k)$. Let $\langle\Pi_1\rangle, \langle\Pi_2\rangle, \ldots, \langle\Pi_N\rangle$ be the full orbits of d-flats in Σ. Within each Π_i, let $\mathcal{F}_i$ be a d-family of m-arcs with $|\mathcal{F}_i| = \mathcal{F}_q^d(m,d)$, $i = 1, 2, \ldots, N$. Let

$$\mathcal{F} = \bigcup_{i=1}^{N} \mathcal{F}_i$$

and identify each member of $\mathcal{F}$ with the corresponding codeword of length $\theta(k,q)$ and weight m.

For the auto-correlation, let $\mathcal{K}$ be a member of $\mathcal{F}$, where say $\mathcal{K}$ is an m-arc in Π_k. For each i, $\mathcal{K} \cap \phi^i(\mathcal{K}) \subset \Pi_k \cap \phi^i(\Pi_k)$. Here, we use $\phi(\mathcal{K})$ to represent the image of $\mathcal{K}$ under the Singer cycle ϕ. Therefore, for all i with $1 \leq i \leq \theta(k,q) - 1$, the number $\left|\mathcal{K} \cap \phi^i(\mathcal{K})\right|$ is bounded above by the maximal intersection of $\mathcal{K}$ with a $(d-1)$-flat contained in Π_k which, by the definition of arc, is d. It follows that $\lambda_a \leq d$.

For the cross-correlation consider two distinct members of $\mathcal{F}$, say $\mathcal{K}$ and $\mathcal{K}'$ where $\mathcal{K}$ and $\mathcal{K}'$ are m-arcs in say Π_s and Π_t respectively (where perhaps $s = t$). We wish to investigate the maximal cardinality:

$$\max_{1 \leq i,j \leq \theta(k,q)} \left\{ |\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}')| \right\}.$$

We have that $\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}') \subseteq \phi^i(\Pi_s) \cap \phi^j(\Pi_t)$. If $s \neq t$ then $\phi^i(\Pi_s)$ and $\phi^j(\Pi_t)$ are in different orbits of d-flats, implying that $\phi^i(\Pi_s) \cap \phi^j(\Pi_t)$ is contained in a $(d-1)$-flat. If $s = t$ but $i \neq j$, then $\phi^i(\Pi_s) \neq \phi^j(\Pi_s)$, implying that $\phi^i(\Pi_s) \cap \phi^j(\Pi_s)$ is still contained in a $(d-1)$-flat. Therefore, by definition of an arc in $PG(d,q)$, $\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}')$ must have cardinality at most d. □

The following appears in [1]; for the sake of completeness we include a proof.

Theorem 3.2. *In $\pi = PG(d,q)$, $d \geq 2$, there exists a d-family $\mathcal{F}$ of $(q+1)$-arcs where $|\mathcal{F}| = (q^{d+1} - q^2)(q^{d+1} - q^3) \cdots (q^{d+1} - q^d)$.*

Proof. Consider $\pi = PG(d,q)$ as a (Baer) subspace of $\Pi = PG(d,q^2)$. Let $\Pi^* = \Pi \setminus \pi$. Choose a point $P = (\alpha_0, \alpha_1, \ldots, \alpha_d) \in \Pi^*$.

With reference to Equation (2.1), consider the collection of NRCs in Π having polynomial coefficients in $GF(q)$. Denote by X_P the number of such NRCs containing P. Note that any such NRC intersects π in an NRC of π. To determine X_P, we count ordered pairs $(\mathcal{N}, Q)$ where $\mathcal{N}$ is an NRC of Π over $GF(q)$ and Q is a point of $\mathcal{N}$ in Π^*. This gives us the following.

$$\frac{|PGL(d+1,q)|}{|PGL(2,q)|}[(q^2+1) - (q+1)] = \left[\left(\frac{(q^2)^{d+1} - 1}{q^2 - 1}\right) - \left(\frac{(q)^{d+1} - 1}{q - 1}\right)\right] X_P.$$

After some simplification we arrive at

$$X_P = (q^{d+1} - q^2)(q^{d+1} - q^3) \cdots (q^{d+1} - q^d).$$

Let $\mathcal{C}$ be an NRC in Π over $GF(q)$ containing P. Then the point $P^q = (\alpha_0^q, \alpha_1^q, \ldots, \alpha_d^q)$ conjugate to P is also contained in $\mathcal{C}$ (and is also in Π^*). As such, any two of the NRCs counted above have at most d common points in π. Hence, by restricting to the intersection of these NRCs with π we have a d-family of $(q+1)$-arcs in π having size X_P.

□

Corollary 3.3. *If q is a prime power, then in $PG(d,q)$, the maximum size of a d-family of $(q+1)$-arcs, denoted by $\mathcal{F}_q^d(q+1,d)$ satisfies*

$$\mathcal{F}_q^d(q+1,d) \geq (q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d).$$

Theorem 3.4. *Fix k and d with $k > d \geq 2$. For each prime power $q \geq d$ there exists a $(\theta(k,q), q+1, d)$-OOC C with*

$$|C| \geq (q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d)\cdot\left\lfloor \frac{1}{\theta(k,q)}\begin{bmatrix} k+1 \\ d+1 \end{bmatrix}_q \right\rfloor \approx q^{kd-d-1}$$

Proof. Follows from Theorem 3.1, Corollary 3.3 and Lemma 2.2. □

Now fix $k > d \geq 1$ and consider the infinite family of $(\theta(k,q), q+1, d)$-OOCs constructed as in Theorem 3.4. The Johnson Bound for these codes is

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

With reference to Definition 1.1 we see that the codes constructed as in Theorem 3.4 satisfy the following limit:

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

Hence, we obtain the following.

Theorem 3.5. *Each infinite family of OOCs in Theorem 3.4 is asymptotically optimal.*

4 A construction from arcs of higher degree

We now show that for $d > 1$ it is possible to improve the codes constructed above. Again, we rely on families of arcs lying in certain flats of a large projective space with sufficiently large order q. For this construction, however, we vary the dimension of the flats where the arcs lie.

Theorem 4.1. *Fix k and d with $k > d \geq 1$. For each prime power $q \geq d$ and for each $m > d$ there exists a $(\theta(k,q), m, d)$-OOC with*

$$|C| = \sum_{i=1}^{d} \mathcal{F}_q^i(m,d,d)\cdot\mathcal{N}_q(i,k).$$

Proof. Let $\Sigma = PG(k,q)$. For fixed s, $1 \leq s \leq d$, let $N_s = \mathcal{N}_q(s,k)$, the number of full orbits of s-flats in $PG(k,q)$. For each s, $1 \leq s \leq d$ let $\Pi_{s,1}, \Pi_{s,2}, \ldots, \Pi_{s,N_s}$ be s-flats chosen one from each of the full s-flat orbits under ϕ. In each $\Pi_{s,t}$ $1 \leq s \leq d$, $1 \leq t \leq N_s$ let $\mathcal{F}_{s,t}$ be a d-family of m-arcs each of degree at most d with $|\mathcal{F}_{s,t}| = \mathcal{F}_q^s(m,d,d)$.
Let

$$\mathcal{F} = \bigcup_{s,t}\mathcal{F}_{s,t}.$$

Identify each member of $\mathcal{F}$ with the corresponding codeword of length $\theta(k,q)$ and weight m. We claim that the code C comprised of all such codewords is a $(\theta(k,q), m, d)$-OOC. That C is of constant weight m is clear.

The auto-correlation, $\lambda_a = d$:
Let $\mathcal{K}$ be a member of $\mathcal{F}$, say $\mathcal{K} \in \mathcal{F}_{s,t}$ is an m-arc of degree r $(\leq d)$ in the s-flat Π, $1 \leq s \leq d$, and $\langle\Pi\rangle$ is a full orbit under ϕ. It suffices to show

$$|\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K})| \leq d, \text{ for all } i \neq j, 1 \leq i,j \leq \theta(k,q)$$

For any i, j, $i \neq j, 1 \leq i, j \leq \theta(k,q)$, since $\langle \Pi \rangle$ is a full orbit, $\phi^i(\Pi) \neq \phi^j(\Pi)$ which implies that

$$dim\left(\phi^i(\Pi) \cap \phi^j(\Pi)\right) \leq s-1.$$

Therefore, since $\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}) \subset \phi^i(\mathcal{K}) \cap \left(\phi^i(\Pi) \cap \phi^j(\Pi)\right)$ and since $\phi^i(\Pi) \cap \phi^j(\Pi)$ is at most an $(s-1)$-flat, we are computing the maximum size of the intersection of an m-arc of degree r lying in an s-flat with an $(s-1)$-flat. It follows that

$$|\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K})| \leq |\phi^i(\mathcal{K}) \cap \left(\phi^i(\Pi) \cap \phi^j(\Pi)\right)| \leq r$$

by the definition of an arc of degree r. Since $r \leq d$ we have $\lambda_a \leq d$.

The cross-correlation, $\lambda_c = d$:
Let $\mathcal{K} \neq \mathcal{K}' \in \mathcal{F}$ where $\mathcal{K} \in \mathcal{F}_{s,t}$ is an m-arc of degree $r \leq d$ in the s-flat Π, $\langle \Pi \rangle$ a full orbit and $\mathcal{K}' \in \mathcal{F}_{s',t'}$ is an m-arc of degree $r' \leq d$ in the s'-flat Π', $\langle \Pi' \rangle$ a full orbit. It suffices to show

$$|\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}')| \leq d, \text{ for all } i, j, \ 1 \leq i, j \leq \theta(k,q).$$

For any $i, j, \ 1 \leq i, j \leq \theta(k,q)$, either $s = s'$ or, without loss of generality, $s' < s$. If $s' < s$ then $dim(\phi^i(\Pi) \cap \phi^j(\Pi')) \leq s' < s$ and therefore (as in the first part of the proof)

$$|\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}')| \leq r \leq d.$$

If $s = s'$ we consider two cases:
Case 1: $\Pi = \Pi'$. In this case $\Pi, \Pi' \in \mathcal{F}_{s,t}$. Therefore if $i = j$, then (by definition of a d-family) $|\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}')| \leq d$. If $i \neq j$ then $dim\left(\phi^i(\Pi) \cap \phi^j(\Pi)\right) \leq s-1$ whence

$$|\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}')| \leq r \leq d.$$

Case 2: $\Pi \neq \Pi'$. In this case $\langle \Pi \rangle \neq \langle \Pi' \rangle$, so $\phi^i(\Pi) \neq \phi^j(\Pi')$ and again $dim\left(\phi^i(\Pi) \cap \phi^j(\Pi)\right) \leq s-1$ whence

$$|\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}')| \leq r \leq d.$$

It follows that $\lambda_c \leq d$.

□

If we use the 2-family of arcs (in this case, conics) in the plane as in Theorem 3.2, and embed into the ambient space $PG(k,q)$, we obtain the following asymptotically optimal class of OOCs.

Corollary 4.2. *For $k > 2$ and for each prime power $q \geq 2$ there exists a $(\theta(k,q), q+1, 2)$-OOC C with*

$$|C| = (q^3-q^2)\cdot\mathcal{N}_q(2,k)+\mathcal{N}_q(1,k) = (q^3-q^2)\cdot\left\lfloor \frac{1}{\theta(k,q)} \begin{bmatrix} k+1 \\ 3 \end{bmatrix}_q \right\rfloor + \left\lfloor \frac{1}{\theta(k,q)} \begin{bmatrix} k+1 \\ 2 \end{bmatrix}_q \right\rfloor. \quad (4.1)$$

Remark 4.3. For $k = 3$ above, we get the main result of [14].

Table 2 compares some of the classes of codes constructed as in Corollary 4.2 with the number of codes given by the Johnson Bound.

Teaming the result of Theorem 4.1 with the construction in Theorem 3.2 for large families of arcs we can improve upon the codes constructed as in Theorem 3.4. That is, codes of the same parameters and of larger size result. Indeed, fix d, let our ambient space be $PG(k,q)$, $k > d$, and consider the full Singer orbits of flats of dimension d or less. For our first class of codewords, we take a d-family of arcs in a representative d-flat from each full d-flat orbit. As in Corollary 3.3 we have

$$\mathcal{F}_q^d(q+1, d, d) \geq (q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d).$$

For our second class of codewords, we look at the $(d-1)$-flats. In the construction outlined in Theorem 4.1 a d-family of arcs of degree d in a representative $(d-1)$-flat from each full orbit is

Table 2: Values of $\frac{M(n,w,\lambda)}{J(n,w,\lambda)}$, $n=\theta(k,q)$, $w=q+1$, $\lambda=2$

q	$k=3$	$k=4$	$k=5$
7	0.6404255318	0.6330472103	0.6318161869
11	0.7546353523	0.7521739130	0.7519103045
121	0.9754142500	0.9754115290	0.9754115020
343	0.9912792665	0.9912791440	0.9912791434
1721	0.9982578413	0.9982575034	0.9982578401

used. For such families, a general construction yielding a family of significant size appears difficult. However, a $(d-1)$-family of arcs in $PG(d-1,q)$ is easily constructed (as in Theorem 3.2) and may be considered (perhaps rather trivially) as a d-family of arcs of degree at most d. That is,

$$\mathcal{F}_q^{d-1}(q+1,d,d) \geq \mathcal{F}_q^{d-1}(q+1,d-1,d-1) \geq (q^d-q^2)(q^d-q^3)\cdots(q^d-q^{d-1}).$$

For subsequent classes of codewords, we consider in turn the $(d-i)$-flats, for each $i \geq 2$. By Theorem 2.4 the collection of all NRCs in a $(d-i)$-flat $i \geq 2$ is a $(d-i+2)$-family of arcs (of degree $(d-i)$). Hence again we arrive at an ostensibly loose lower bound:

$$\mathcal{F}_q^{d-i}(q+1,d,d) \geq \nu(d-i,q) \text{ for each } i \geq 2.$$

Putting all of these classes of codewords together establishes the following.

Corollary 4.4. *For $k > d \geq 3$ and for each prime power $q \geq d$ there exists a $(\theta(k,q), q+1, d)$-OOC C consisting of*

$$\begin{aligned}&\mathcal{N}_q(d,k)\cdot\prod_{i=2}^{d}(q^{d+1}-q^i)+\mathcal{N}_q(d-1,k)\cdot\prod_{i=2}^{d-1}(q^d-q^i)+\sum_{i=1}^{d-2}\big(\nu(i,q)\cdot\mathcal{N}_q(i,k)\big)\\ &=\left\lfloor\frac{1}{\theta(k,q)}\begin{bmatrix}k+1\\ d+1\end{bmatrix}_q\right\rfloor\prod_{i=2}^{d}(q^{d+1}-q^i)+\left\lfloor\frac{1}{\theta(k,q)}\begin{bmatrix}k+1\\ d\end{bmatrix}_q\right\rfloor\prod_{i=2}^{d-1}(q^d-q^i)+\sum_{i=1}^{d-2}\left(\nu(i,q)\cdot\left\lfloor\begin{bmatrix}k+1\\ i+1\end{bmatrix}_q\right\rfloor\right).\end{aligned} \tag{4.2}$$

codewords.

Remark 4.5. Taking $k=d+1$ in the above yields codes of the same parameters as those constructed in [1]. Moreover, the size of the codes constructed in [1] correspond to the first and last terms in the expansion (4.2). Consequently, for $\lambda > 2$ we obtain a strict improvement to the main construction of (n,w,λ)-OOCs in [1].

Tables 3 and 4 compare some of the classes of codes constructed as in Corollary 4.4 with the number of codes given by the Johnson Bound.

Table 3: Values of $\frac{M(n,w,\lambda)}{J(n,w,\lambda)}$, $n=\theta(k,q)$, $w=q+1$, $\lambda=3$

q	$k=4$	$k=5$	$k=6$
7	0.3723672313	0.3778141740	0.3788019688
11	0.5503002252	0.5542495934	0.5546309684
121	0.9512311850	0.9512954758	0.9512960102
343	0.9826092131	0.9826175386	0.9826175623
1721	0.9965177060	0.9965180418	0.9965180423

Table 4: Values of $\frac{M(n,w,\lambda)}{J(n,w,\lambda)}$, $n = \theta(k,q)$, $w = q+1$, $\lambda = 5$

q	$k=6$	$k=7$	$k=8$
7	0.0663583530	0.0677297426	0.0679268867
11	0.2100588301	0.2118051740	0.2119642548
121	0.8822149212	0.8822751817	0.8822756800
343	0.9570511656	0.9570593005	0.9570593242
1721	0.9913154765	0.9913158107	0.9913158117

5 Affine constructions

For our final construction, we will work in the finite affine space $AG(k,q)$. Our basic technique follows the work of [16] where the authors use d-flats of $AG(k,q)$ to construct some OOCs, some of which are optimal. One way to model $AG(d,k)$ is to simply start in the projective space $PG(d,k)$ and delete any hyperplane Σ. The remaining points form the points of $AG(d,k)$ and the flats of $AG(d,q)$ are simply the flats of $PG(d,k)$ with any points of Σ deleted.

It is well-known that $AG(d,q)$ does not admit a Singer group in the same fashion as $PG(d,q)$. However, we can still apply the same general techniques as above. One way to model $AG(k,q)$ is with a k-dimensional vector space over $GF(q)$. In this model, the vectors represent the affine points. The finite field $GF(q^k)$ is one example of such a vector space. As the non-zero field elements of $GF(q^k)$ form a cyclic group under multiplication, we can obtain a similar group (to that of a Singer group of $PG(d,q)$) by simply removing the point corresponding to the zero element of $GF(q^k)$. Briefly, let $\Sigma = AG(k,q)$ and denote by 0 the zero vector in Σ. Take α to be a primitive element of $GF(q^k)$. Just as in the projective case, each nonzero vector in Σ corresponds in the natural way to α^j for some j, $0 \le j \le q^{k-2}$. Denote by $\hat{\phi}$ the (Singer-like) mapping of Σ defined by $\hat{\phi}(\alpha^j) = \alpha^{j+1}$ and $\hat{\phi}(0) = 0$. Hence, for all of our constructions below, our code lengths will be of the form $q^k - 1$ where the coordinates of the codewords correspond to the non-zero elements of the finite field $GF(q^k)$ (see e.g. [17]). Just as in the previous sections, we will make use of certain families of arcs lying in $AG(k,q)$.

Definition 5.1. Let $\pi = AG(d,q)$. A collection $\mathcal{F}$ of m-arcs (perhaps of varying degrees) in π is said to be a t-family if every pair of distinct members of $\mathcal{F}$ meet in at most t points. By $\mathcal{E}_q^d(m,r,t)$ we denote maximal size in $AG(d,q)$ of a t-family of m-arcs each having degree at most $r\,(\ge d)$. If $r = d$ (and consequently all arcs are of degree d) we write $\mathcal{E}_q^d(m,t)$.

Consider the space $AG(k,q)$ with the origin removed, and consider the d-flats that do not contain the origin as a point. We wish to count the number of full orbits of these d-flats under the action of the group described above on the points of $AG(d,q)$ minus the origin. We let $\mathcal{M}_q(d,k)$ be the number of such full d-flat orbits in $AG(k,q)$. It follows from Theorem 8 of [17] that

$$\mathcal{M}_q(d,k) = \frac{q^{k-d}-1}{q^d-1} \cdot \begin{bmatrix} k \\ d \end{bmatrix}_q = \frac{(q^{k-1}-1)(q^{k-2}-1)\cdots(q^{k-d}-1)}{(q^d-1)(q^{d-1}-1)\cdots(q-1)}.$$

Theorem 5.2. *For each prime power $q \ge 2$ there exists a $(q^k-1, q+1, 2)$-OOC C with*

$$|C| = (q^3-q^2)M_q(2,k).$$

Proof. Our technique is exactly as in Theorem 3.1. We consider a family of $(q+1)$-arcs lying in a plane π of $AG(k,q)$ not containing the origin. We only need to show that the 2-family of $(q+1)$-arcs of $PG(2,q)$ constructed in Theorem 3.2 can still be constructed in $AG(2,q)$.

Let $\Pi = PG(2,q^2)$ and let $\pi \cong PG(2,q)$ be the natural Baer subplane of Π consisting of the set of points whose homogeneous coordinates lie in the subfield $GF(q)$ of the field $GF(q^2)$. Let P be any point of $\Pi \setminus \pi$. As in Theorem 3.2, there are q^3-q^2 arcs of Π, the family $\mathcal{F}$, that meet the Baer

subplane π in a sub-arc of size $q+1$. We refer to these sub-arcs as $GF(q)$-arcs. Now, consider the line PP^q, that is, the line joining P with is conjugate point P^q. It's a simple consequence of the classical theory that this line meets the subplane π in a Baer subline. Since the points P and P^q both lie on each of the arcs of $\mathcal{F}$, it follows that no other points of the line PP^q lie on any of the $GF(q)$-arcs. Hence, if we remove the Baer subline of PP^q lying in π from the Baer subplane π, we are left with an isomorphic copy of $AG(2,q)$ containing a set of q^3-q^2 arcs, pairwise meeting in at most two points.

We now embed the affine plane $AG(2,q)$ in $AG(k,q)$ and associate with each arc of the family a codeword. The results on auto and cross correlation now follow as in Theorem 3.1. □

We can increase the number of codewords in the code above by adding the lines of $AG(2,q)$ as additional codewords. In $AG(2,q)$, however, lines contain q points. Hence, in order to keep our codewords of constant weight, we start by removing one point (randomly) from each arc of the family $\mathcal{F}$. Using these q-arcs together with the lines of $AG(2,q)$ gives us the following.

Corollary 5.3. *For $k>2$ and for each prime power $q\geq 2$ there exists a $(q^k-1,q,2)$-OOC C with*

$$|C| = (q^3-q^2)\mathcal{M}_q(2,k)+\mathcal{M}_q(1,k).$$

Just as with the projective case, the construction above generalizes naturally. The proof of the following is entire similar to that of Theorem 4.1.

Theorem 5.4. *Fix k and d with $k>d\geq 1$. For each prime power $q\geq d$ and for each $m>d$ there exists a (q^k-1,m,d)-OOC C with*

$$|C| = \sum_{i=1}^{d}\mathcal{E}_q^i(m,d,d)\cdot\mathcal{M}_q(i,k).$$

We now establish some lower bounds on $\mathcal{E}_q^i(m,d,d)$, $i\leq d$.

Lemma 5.5. *In $AG(d,q)$, $d\geq 2$, there exists a d-family $\mathcal{F}_0$ of $(q-d+3)$-arcs with $|\mathcal{F}_0| = (q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d)$.*

Proof. As in Theorem 5.2, consider $\pi = PG(d,q)$ as a (Baer) subspace of $\Pi = PG(d,q^2)$ and choose a point P of Π outside of π. As discussed in Theorem 3.2, there are $(q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d)$ NRCs (the family $\mathcal{F}$) passing through P and meeting π in a sub-arc, and this collection of $(q+1)$-arcs forms a d-family of $GF(q)$-arcs in π. The line PP^q of Π meets π in a Baer subline l_0. Now consider *any* $(d-1)$-flat, say π_0, of π that contains the line l_0. The hyperplane π_0 extends to a hyperplane of the entire space Π that contains the points P and P^q. By the definition of arc, any of the arcs in our family $\mathcal{F}$ meet this $(d-1)$-flat of Π in at most d points, two of which are P and P^q. Hence, if we delete the hyperplane π_0 from π, we delete at most $d-2$ points from any arc of the family $\mathcal{F}$. This gives us a family of arcs we call $\mathcal{F}_0$. For any arc of $\mathcal{F}$ not meeting π_0 in $d-2$ points, we (randomly) remove points so that each arc of $\mathcal{F}_0$ has size $(q+1)-(d-2) = q-d+3$. Hence, every member of $\mathcal{F}_0$ is a $(q-d+3)$-arc. □

From Lemma 5.5 we have

$$\mathcal{E}_q^d(q-d+3,d,d)\geq (q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d).$$

Moreover, an analysis similar to that preceding Corollary 4.4 yields

$$\mathcal{E}_q^{d-1}(q-d+3,d,d)\geq \mathcal{E}_q^{d-1}(q-d+3,d-1,d-1)\geq (q^d-q^2)(q^d-q^3)\cdots(q^d-q^{d-1}),$$

and

$$\mathcal{E}_q^{d-i}(q-d+3,d,d)\geq \nu(d-i,q) \text{ for each } i\geq 2$$

which, with Theorem 5.4, establishes the following.

Corollary 5.6. *For $k > d \geq 3$ and for each prime power $q \geq d$ there exists a $(q^k-1, q-d+3, d)$-OOC C with*

$$|C| \quad = \quad \mathcal{M}_q(d,k) \cdot \prod_{i=2}^{d}(q^{d+1}-q^i) + \mathcal{M}_q(d-1,k) \cdot \prod_{i=2}^{d-1}(q^d-q^i) + \sum_{i=1}^{d-2}\big(\nu(i,q) \cdot \mathcal{M}_q(i,k)\big).$$

As discussed before Corollary 4.4, we can potentially increase the number of codewords by using arcs of higher degree. In particular, if there exists a t-family $\mathcal{F}$ of m-arcs of degree r in $PG(d,q)$, then there would exist a t-family $\mathcal{F}_0$ of $(m-r)$-arcs of degree r in $AG(d,q)$. Such a family $\mathcal{F}_0$ could potentially be larger than the family described in Lemma 5.5 which would lead to larger codes. In addition, notice in the constructions above that we were forced to remove some points from our arcs for the sole purpose of maintaining a constant codeword weight. Avoiding this might improve the parameters of our codes.

Tables 5, 6, and 7 compare some of the classes of codes constructed as in Corollary 5.6 with the number of codes given by the Johnson Bound. Of particular note are the codes for $\lambda = 2$ (Table 5) whose ratio with the Johnson bound is extremely close to 1.

Table 5: Values of $\frac{M(n,w,\lambda)}{J(n,w,\lambda)}$, $n = q^k - 1$, $w = q + 1$, $\lambda = 2$

q	$k=3$	$k=4$	$k=5$
7	0.8621700881	0.9804586940	0.9972032137
11	0.9104589917	0.9918766332	0.9992610944
121	0.9917366568	0.9999317079	0.9999994356
343	0.9970845975	0.9999915002	0.9999999753
1721	0.9994189427	0.9999996625	0.9999999997

Table 6: Values of $\frac{M(n,w,\lambda)}{J(n,w,\lambda)}$, $n = q^k - 1$, $w = q$, $\lambda = 3$

q	$k=4$	$k=5$	$k=6$
7	0.2960072911	0.3428831335	0.3497386757
11	0.4885791465	0.5365032592	0.5409140118
121	0.9432368020	0.9510961860	0.9511611465
343	0.9797276160	0.9825922863	0.9826006382
1721	0.9959379975	0.9965170310	0.9965173675

Table 7: Values of $\frac{M(n,w,\lambda)}{J(n,w,\lambda)}$, $n = q^k - 1$, $w = q - 2$, $\lambda = 5$

q	$k=6$	$k=7$	$k=8$
8	0.0023607860	0.0026977534	0.0027405412
11	0.0307547138	0.0338295282	0.0341113883
121	0.7894584074	0.7960372276	0.7960916016
343	0.9210483659	0.9237414898	0.9237493411
1721	0.9838383895	0.9844103884	0.9844107212

Note: Our code construction for the tables above involves d-families of $(q-d+3)$-arcs. To avoid trivial arcs we considered only values of q for which $q - d + 3 > d$.

6 Conclusion

We have exhibited a very general construction of optical orthogonal codes that gives rise to a robust class of asymptotically optimal codes. Our codes generalize and improve the prior constructions involving conics [14] and arcs [1] by expanding the families of intersecting arcs and by working in higher dimensional projective spaces. One next step might be to consider subgeometries $PG(k, q)$ embedded in $PG(k, q^n)$ and use large families of arcs in these subgeometries to find other classes of OOCs whose size approaches that given by the Johnson Bound.

In the last section of [16] the authors discuss the possibility of OOCs with different weight classes. In the constructions of Section 5, points were arbitrarily removed from certain arcs for the sole purpose of maintaining a constant codeword weight. Hence, the methods of Section 5 provide a construction for large non-constant weight codes with strong auto and cross correlations properties. The investigation into bounds on the size of such OOCs with different weight classes seems an interesting problem as well.

References

[1] T.L. Alderson. Optical orthogonal codes and arcs in $PG(d, q)$. *Finite Fields Appl.(in press)*.

[2] T.L. Alderson, A. A. Bruen, and R. Silverman. Maximum distance separable codes and arcs in projective spaces. *J. Combin. Theory Ser. A (in press)*.

[3] T.L. Alderson and Keith E. Mellinger. Constructions of optical orthogonal codes from finite geometry. submitted.

[4] T.L. Alderson and Keith E. Mellinger. Optical orthogonal codes from arcs in root subspaces. to appear.

[5] C. M. Bird and A. D. Keedwell. Design and applications of optical orthogonal codes—a survey. *Bull. Inst. Combin. Appl.*, 11:21–44, 1994.

[6] Fan R. K. Chung, Jawad A. Salehi, and Victor K. Wei. Optical orthogonal codes: design, analysis, and applications. *IEEE Trans. Inform. Theory*, 35(3):595–604, 1989.

[7] Sean V. Droms, Keith E. Mellinger, and Chris Meyer. LDPC codes generated by conics in the classical projective plane. *Des. Codes Cryptogr.*, 40(3):343–356, 2006.

[8] Keldon Drudge. On the orbits of Singer groups and their subgroups. *Electron. J. Combin.*, 9(1):Research Paper 15, 10 pp. (electronic), 2002.

[9] G. L. Ebert, K. Metsch, and T. Szönyi. Caps embedded in Grassmannians. *Geom. Dedicata*, 70(2):181–196, 1998.

[10] Ryoh Fuji-Hara and Ying Miao. Optical orthogonal codes: their bounds and new optimal constructions. *IEEE Trans. Inform. Theory*, 46(7):2396–2406, 2000.

[11] Timothy J. Healy. Coding and decoding for code division multiple user communication systems. *IEEE Trans. Comm.*, 33(4):310–316, 1985.

[12] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[13] S. V Maric, O. Moreno, and C. Corrada. Multimedia transmission in fiber-optic lans using optical cdma. *J. Lightwave Technol.*, 14:2149–2153, 1996.

[14] Nobuko Miyamoto, Hirobumi Mizuno, and Satoshi Shinohara. Optical orthogonal codes obtained from conics on finite projective planes. *Finite Fields Appl.*, 10(3):405–411, 2004.

[15] Q. A Nguyen, László Györfi, and James L. Massey. Constructions of binary constant-weight cyclic codes and cyclically permutable codes. *IEEE Trans. Inform. Theory*, 38(3):940–949, 1992.

[16] R. Omrani, O. Moreno, and P.V. Kumar. Improved Johnson bounds for optical orthogonal codes with $\lambda > 1$ and some optimal constructions. *Proc. Int. Symposium on Information Theory*, pages 259–263, 2005.

[17] C. Radhakrishna Rao. Cyclical generation of linear subspaces in finite geometries. In *Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967)*, pages 515–535. Univ. North Carolina Press, Chapel Hill, N.C., 1969.

[18] Joseph A. Thas. Projective geometry over a finite field. In *Handbook of incidence geometry*, pages 295–347. North-Holland, Amsterdam, 1995.

[19] Guu-chang Yang and Thomas E. Fuja. Optical orthogonal codes with unequal auto- and cross-correlation constraints. *IEEE Transactions on Information Theory*, 41(1):96–106, 1995.