CONSTRUCTIONS OF OPTICAL ORTHOGONAL CODES FROM FINITE GEOMETRY

T. L. ALDERSON* AND KEITH E. MELLINGER†

Abstract. The link between finite geometry and various classes of error-correcting codes is well known. Arcs in projective spaces, for instance, have a close tie to linear MDS codes as well as the high-performing low-density parity-check codes. In this article, we demonstrate a connection between arcs and optical orthogonal codes (OOCs), a class of non-linear binary codes used for many modern communication applications. Using arcs and Baer subspaces of finite projective spaces, we construct some infinite classes of OOCs with auto-correlation and cross-correlation both larger than 1.

Key words. optical orthogonal codes, arcs, Baer subplanes

AMS subject classifications. 94B27, 51E20

1. Introduction. 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.

One of the first proposed applications of optical orthogonal codes was to optical code-division multiple access communication systems where binary sequences with strong correlation properties are required [1, 3, 5]. Subsequently, OOCs have found application for multimedia transmissions in fiber-optic LANs [9]. Optical orthogonal codes have also been called cyclically permutable constant weight codes in the construction of protocol sequences for multiuser collision channels without feedback [11].

* Mathematical Sciences, University of New Brunswick, Saint John, NB., Canada (talderso@unb.ca), the author acknowledges support from the N.S.E.R.C. of Canada.

†Department of Mathematics, University of Mary Washington, 1301 College Avenue, Trinkle Hall, Fredericksburg, VA 22401, USA (kmelling@umw.edu), the author acknowledges support by a faculty development grant from the University of Mary Washington

An $(n, w, \lambda_a, \lambda_c)$-OOC with $\lambda_a = \lambda_c$ is denoted (n, w, λ)-OOC. The number of codewords 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 $\Phi(n, w, \lambda)$. An (n, w, λ)-OOC of size $\Phi(n, w, \lambda)$ is said to be *optimal*. From the Johnson bound for constant weight codes it follows that [3]

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

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 (perhaps naive) bound on the size of C by taking $\lambda = max\{\lambda_a, \lambda_c\}$ in (1.1). In [17], Yang and Fuja discuss OOCs with $\lambda_a > \lambda_c$ and the following bound is established.

$$\Phi(n, w, \lambda + m, \lambda) \leq \Phi(n, w, \lambda) \cdot (\lambda + m) \tag{1.2}$$

The codes we construct in Sections 4.1, 4.2, and 5 have $\lambda_a < \lambda_c$. As such the 1.1 seems the only applicable bound. We do however offer some analysis regarding the possible optimality of our codes.

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

$$\lim_{n \to \infty} \frac{M(n, w, \lambda)}{J(n, w, \lambda)} = 1. \tag{1.3}$$

For $\lambda = 1, 2$ optimal OOCs are known to exist (see *e.g.* [3, 4, 13]). There are very limited examples of such optimal OOCs with $\lambda > 2$ (in [12, 13] optimal OOCs consisting of a single codeword are shown to exist). Our constructions were originally motivated by the results in [10] where certain families of conics in $PG(2, q)$ are used to construct $(n, q + 1, 2)$-OOCs that are close to optimal. We build on the ideas in [10] and construct several new classes of OOCs based on arcs in finite projective spaces.

2. Preliminaries. As our work relies heavily on the structure of finite projective spaces, we start with a short overview of the fundamentals of finite projective geometry. We let $PG(k, q)$ represent the finite projective geometry of dimension k and order q. Due to a result of Veblen and Young [16], all finite projective spaces of dimension greater than two are isomorphic up to the order q. The space $PG(k, q)$ can be modeled most 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 $\theta_{k,q} = \frac{q^{k+1}-1}{q-1}$.

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 useful in our constructions. Another property that we rely on is the principle of duality. For any space $S = PG(k,q)$, there is a *dual* space S^* whose points and hyperplanes (subspaces of dimension $k-1$) are respectively the hyperplanes and points of S. For any result about points of S, there is always a corresponding result about hyperplanes of S^*. More generally, for any result dealing with subspaces of S, replacing each reference to a subspace $PG(m,q)$, $m < k$, with a reference to the subspace $PG(k-m-1,q)$ yields a correspond *dual* statement of S^* 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 subspace of dimension $k-2$.

3. OOCs from lines of PG$(\mathbf{k},\mathbf{q})$. In [3] Chung, Salehi, and Wei provide a method for constructing $(n,w,1)$-OOCs using lines of the projective geometry $PG(k,q)$. Briefly, let ω be a primitive element of $GF(q^{k+1})$. The points of $\Sigma = PG(k,q)$ can be represented as $\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}$ where $n = \frac{q^{k+1}-1}{q-1}$. Hence, in a natural way a point set A of $PG(k,q)$ corresponds to 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 cycle 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 entries 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 $\mathcal{L}(k,q)$ 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 3.1. *For any prime power q and any positive integer k, there exists an (optimal) $(\theta_{k,q}, q+1, 1)$-OOC consisting of $\mathcal{L}(k,q) = \left\lfloor \frac{q^k-1}{q^2-1} \right\rfloor$ codewords.*

4. OOCs from arcs in PG(k,q). An *n-arc* in $PG(k,q)$ is a collection of $n > k$ points such that no $k+1$ are incident with a common hyperplane. It follows that if $\mathcal{K}$ is an n-arc in $PG(k,q)$ then no $k+1$ points of $\mathcal{K}$ lie on a hyperplane, no k lie on a $(k-2)$-flat,..., no 3 lie on a line. An n-arc is called *complete* if it is not contained in an $(n+1)$-arc.

For given k and q, let m(k, q) denote the maximum value of n for which an n-arc exists in $PG(k,q)$. Then $m(k,q) = k+2$ for $q \leq k+1$. In homogeneous coordinates, the points (1, 0, . . . , 0), (0, 1, 0, . . . , 0), ... ,(0, . . . , 0, 1), and (1, 1, . . . , 1) constitute such an arc. Hence, for $q \leq k+1$, every point in $PG(k,q)$ is a linear combination of at most k of these $k+2$ points. 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.

When q is even, one can add one additional point to each conic, the so-called *knot* where all of the tangent lines intersect. The resulting $(q+2)$-arc is called a hyperoval and is 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

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

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

$$\{P(t) = P\left(f_0(t), \ldots, f_d(t)\right) \,|\, t \in GF(q) \cup \{\infty\}\,\} \tag{4.1}$$

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

DEFINITION 4.1. *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 the set of points*

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

It is well-known that an NRC is, in fact, a $(q+1)$-arc. When stated in terms of arcs, the *Main Conjecture* (MC) for MDS Codes, always taking $q > k+1$, is the following: $m(k,q) = q+2$ for $k = 2$ and $k = q-2$ both with q even, $q+1$ in all other cases. The main conjecture has its roots in a problem first posed over 50 years ago

by B. Segre. The MC has not been proved in general. It has been verified in many cases. See [6] for a recent survey of results relating to the MC.

DEFINITION 4.2. *Let $\pi = PG(k,q)$. A t-family $\mathcal{F}$ of m-arcs in π is a collection of m-arcs mutually meeting in at most t points.*

THEOREM 4.3. *Let $\mathcal{F}$ be a t-family of m-arcs in $\pi = PG(k,q)$. Let $\mu = max\{k,t\}$. Then there exists a $\left(\frac{q^{k+2}-1}{q-1}, m, k, \mu\right)$-OOC C consisting of $|\mathcal{F}|$ codewords.*

Proof. Consider $\pi = PG(k,q)$ as embedded in $\Sigma = PG(k+1,q)$ and let ω be a primitive element of $GF(q^{k+2})$. Let C be t-family of m-arcs π. Identify each arc in C with the corresponding codeword of length $\frac{q^{k+2}-1}{q-1}$ and weight m. As in Section 3, let $\phi : \omega^i \mapsto \omega^{i+1}$ be a singer group acting on Σ. Let $\mathcal{K}$ be an arc in C. The auto-correlation λ_a is the maximum number of points in the intersection of $\phi^i(\mathcal{K})$ and $\phi^j(\mathcal{K})$ where $i \neq j$. Since ϕ is a collineation of Σ, $\phi^i(\mathcal{K}) \cap \phi^j(\mathcal{K}) \subset \phi^i(\pi) \cap \phi^j(\pi)$. As ϕ acts regularly on the hyperplanes of Σ, $\phi^i(\pi) \neq \phi^j(\pi)$ and $\phi^i(\pi) \cap \phi^j(\pi)$ is necessarily a $(k-1)$-flat. It follows that λ_a is bounded above by the maximum intersection of an arc in $PG(k,q)$ and a $(k-1)$-flat, hence $\lambda_a \leq k$. Now let $\mathcal{K}$ and $\mathcal{K}'$ be distinct arcs in C. The cross-correlation λ_c is the maximum number of points in the intersection of $\phi^i(\mathcal{K})$ and $\phi^j(\mathcal{K}')$. If $i \neq j$ then, as above, this number is at most k. However if $i = j$ then $\phi^i(\mathcal{K})$ and $\phi^j(\mathcal{K}')$ are in a common hyperplane of Σ and can therefore share as many as t points. It follows that $\lambda_c = max\{k,t\}$. □

Using the notation of the previous proof, a line of Σ intersects any member of $\mathcal{F}$ in at most 2 points. Hence, adding the $\mathcal{L}(k,q)$ codewords from Theorem 3.1 to C will not violate either correlation requirement. However, each line gives a codeword of weight $q+1$ whereas the weight of C is m. This poses no problem if $m \leq q+1$. Moreover, if $m \leq q+1$ the points of each of the $\mathcal{L}(k,q)$ lines may arbitrarily subdivided into $\lfloor \frac{q+1}{m} \rfloor$ disjoint subsets (or more generally, into subsets mutually intersecting in at most k points) of size m. Each of the resulting $\lfloor \frac{q+1}{m} \rfloor \cdot \mathcal{L}(k,q)$ subsets then corresponds to a codeword of C. This gives the following.

COROLLARY 4.4. *Let $\mathcal{F}$ be a t-family of m-arcs, $m \leq q+1$ in $\pi = PG(k,q)$. Let $\mu = max\{k,t\}$. Then there exists a $\left(\frac{q^{k+2}-1}{q-1}, m, k, \mu\right)$-OOC consisting of $|\mathcal{F}| + \lfloor \frac{q+1}{m} \rfloor \cdot \mathcal{L}(k,q)$ codewords.*

4.1. An $(\mathbf{n}, \mathbf{w}, \lambda, \lambda+\mathbf{2})$ construction using Normal Rational Curves. The following is a well known property of NRCs (see e.g. [15]).

THEOREM 4.5. *A $(d+3)$-arc in $PG(d,q)$ is contained in a unique normal rational curve.*

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 [7] Theorem 27.5.3]) . It follows that if $\nu(d,q)$ denotes the number of distinct normal rational curves in $PG(d,q)$ then

$$\nu(d,q) = \frac{|PGL(d+1,q)|}{|PGL(2,q)|} = \frac{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)}{(q^2-1)(q^2-q)} \tag{4.2}$$

THEOREM 4.6. *For any prime power q and for each $k \geq 2$ there exists a $\left(\frac{q^{k+2}-1}{q-1}, q+1, k, k+2\right)$-OOC consisting of $\nu(k,q)+\mathcal{L}(k,q) \approx q^{k^2+2k-3}$ codewords.*

Proof. This follows immediately from Corollary 4.4 and Theorem 4.5. □

REMARK 4.6.1.

1. *Let $M(\frac{q^{k+2}-1}{q-1}, q+1, k, k+2)$ denote the size of the codes constructed in Theorem 4.6. We compare the size of our codes to other codes with similar correlation parameters in order to obtain some insight on the optimality of our codes. On the one hand (as one might expect), we have*

$$M\left(\frac{q^{k+2}-1}{q-1}, q+1, k, k+2\right) < J\left(\frac{q^{k+2}-1}{q-1}, q+1, k+2\right) \approx q^{k^2+2k-1}$$

while on the other hand,

$$M\left(\frac{q^{k+2}-1}{q-1}, q+1, k, k+2\right) > J\left(\frac{q^{k+2}-1}{q-1}, q+1, k+1\right) \approx q^{k^2+k-1}$$

Also, from the bound of Yang and Fuja (1.2) it follows that if $q^k > \frac{k+2}{q^4}$ then

$$M\left(\frac{q^{k+2}-1}{q-1}, q+1, k, k+2\right) > \Phi\left(\frac{q^{k+2}-1}{q-1}, q+1, k+2, k+1\right).$$

Thus, we have a strong indication that the codes constructed in Theorem 4.6 are quite robust. Moreover, we see that for the code parameters specific to the theorem and for q sufficiently large

$$\Phi(n, w, \lambda+1, \lambda) < \Phi(n, w, \lambda-1, \lambda+1).$$

2. *Let C be an $\left(\frac{q^{k+2}-1}{q-1}, q+1, k, k+2\right)$-OOC constructed as in the theorem and let $\Sigma = PG(k+1,q)$. Let c_1, $c_2 \in C$ be two codewords. By the construction it follows that there is at most one cyclic shift of c_2, say c_2' for which the cross correlation of c_1 and c_2' is greater than k (this will only occur if the NRCs $\mathcal{C}_1$ and $\mathcal{C}_2$ corresponding respectively to c_1 and c_2' are contained in a common hyperplane of Σ and intersect in more than k points).*

4.2. An $(\mathbf{n}, \mathbf{w}, \lambda)$ construction from m-arcs. In [10], Miyamoto, Mizuno, and Shinohara prove the existence of an asymptotically optimal family of $(n, w, 2)$-OOCs. Their proof utilizes a clever construction of a large 2-family of $(q+1)$-arcs in $PG(2, q)$. The construction relies heavily on the fact that the $(q+1)$-arcs concerned are conics (i.e. NRCs). In what follows we provide a construction for large families of arcs in $PG(k, q)$, $k \geq 2$. For $k = 2$ the corresponding OOCs form an asymptotically optimal family. Also, for $k = 2$ our code parameters match those of [10] for q even (see Corollary 4.10). Our construction is quite general in that it holds for arbitrary arcs, that is to say we do not rely on any correspondence between the arcs involved and algebraic curves. As such, our construction holds for arcs of size larger than $q+1$ in $PG(d, q)$ (which necessarily do not correspond to NRCs).

THEOREM 4.7. *Let $\pi = PG(k, q)$. If π contains an m-arc, then π contains a $(k+1)$-family $\mathcal{F}$ of m-arcs where $|F| = q^{k+1} - q^k$. Moreover, there exists a point P incident with each member of $\mathcal{F}$. Consequently, there exists a k-family consisting of $q^{k+1} - q^k$ distinct $(m-1)$-arcs.*

Proof. We work with the dual. Let $\mathcal{K} = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ be a dual m-arc in π. Consider π as embedded in $\Sigma = PG(k+1, q)$ and let $\Sigma^* = \Sigma \backslash \pi$ be the associated affine space. Let σ be any hyperplane of Σ on λ_m other than π. For each point $P \in \Sigma^* \setminus \sigma$ denote by ϕ_P the projection map taking π to σ through P. Each such ϕ_P fixes λ_m and carries $\mathcal{K}$ to a dual arc $\phi_P(\mathcal{K})$ in σ (containing λ_m). Let $S = \{\phi_P(\mathcal{K}) | P \in \Sigma^* \setminus \sigma\}$ be the set of $q^{k+1} - q^k$ dual m-arcs in σ obtained by projection. *We claim that apart from λ_m no two dual arcs S share as many as $k+1$ common members.* Let $\lambda \neq \lambda_m$ be a member of $\phi_P(\mathcal{K})$ and let $\psi = \lambda \cap \lambda_m$. Other than λ_m there is precisely one member of $\mathcal{K}$, say λ' containing ψ (at most two members of $\mathcal{K}$ are incident with a given $(k-2)$-flat). So $\langle P, \lambda \rangle = \langle P, \lambda' \rangle = \langle \lambda, \lambda' \rangle$. It follows that if $\lambda \in \phi_Q(\mathcal{K})$ with $P \neq Q$ then the line $\langle P, Q \rangle$ intersects π in a point of λ'. Hence, if $\phi_P(\mathcal{K})$ and $\phi_Q(\mathcal{K})$ have $k+1$ common members other than λ_m, then the point at which the line $\langle P, Q \rangle$ intersects π will be incident with $k+1$ members of $\mathcal{K}$, a contradiction. Hence, S is a $(k+1)$-family of m-arcs where $|S| = q^{k+1} - q^k$. By removing λ_m from each member of S we obtain the k-family of dual $(m-1)$-arcs as required. □

Restricting to $k = 2$ we can give explicit coordinates for constructing the $q^3 - q^2$ conics of the projective plane described in Theorem 4.7. These coordinates are derived directly from the projection construction when q is odd. Let (x, y, z) represent the homogeneous coordinates for a projective point of π. Then, for fixed $a, b, c \in GF(q)$, $c \neq 0$, let $C_{a,b,c} = \{(1, a - cx^2, b - cx) : x \in GF(q)\} \cup \{(0, 1, 0)\}$. One can easily show

that $C_{a,b,c}$ defines a conic of π. Varying a, b and c gives a family of $q^3 - q^2$ conics that have the desired intersection property, and that meet in the point $(0, 1, 0)$. As $c \neq 0$, we have exactly $q^3 - q^2$ conics of this form. These coordinates generate a similar set when q is even.

LEMMA 4.8. *If there exists an m-arc in $PG(k, q)$, then there exists a $(\theta_{k+1,q}, m-1, k)$-OOC C where*

$$|C| = \begin{cases} q^{k+1} - q^k + \lfloor \frac{q+1}{m-1} \rfloor \cdot \mathcal{L}(k+1, q) & m \leq q+2 \\ q^{k+1} - q^k & \text{otherwise.} \end{cases}$$

Proof. Follows immediately from Theorem 4.7 and Corollary 4.4. □

An NRC in $PG(d, q)$ is a $(q+1)$-arc and $(q+2)$-arcs are known to exist in $PG(2, 2^t)$. This gives us the following two corollaries.

COROLLARY 4.9. *For q a prime power and $k \geq 2$ there exists a $(\theta_{k+1,q}, q, k)$-OOC consisting of $q^{k+1} - q^k + \mathcal{L}(k, q)$ codewords.*

Proof. Normal rational curves provide $(q+1)$-arcs in $PG(k, q)$, $k \geq 2$. The result follows from Lemma 4.8. □

Thus, for each $k \geq 2$ we have (via Corollary 4.9) an infinite family of OOCs. Moreover, for $k = 2$ it is easily verified that the family is asymptotically optimal. When $k = 2$ and q is even the fact that hyperovals exist in $PG(2, q)$ gives the following corollary yielding codes with parameters matching those of Miyamoto and Mizuno [10].

COROLLARY 4.10. *For $q = 2^t$ there exists a $\left(\frac{q^4-1}{q-1}, q+1, 2\right)$-OOC consisting of $q^3 - q^2 + q$ codewords.*

4.3. An $(\mathbf{n}, \mathbf{w}, \lambda)$ Construction from (k+1)-arcs in PG(k,q). As observed above, $k+2$ arcs exist in $PG(k, q)$ for every k. Denote by $\mathcal{N}(k+1, q)$ the family of all $(k+1)$-arcs in $PG(k, q)$. As $\mathcal{N}(k+1, q)$ is a k-family of arcs in $PG(k, q)$, Theorem 4.3 gives the following.

THEOREM 4.11. *For q a prime power and $k \geq 1$ there exists a $(\theta_{k+1,q}, k+1, k)$-OOC consisting of $|\mathcal{N}(k+1, q)|$ codewords.*

COROLLARY 4.12. *For q a prime power and $1 \leq k \leq q$ there exists a $(\theta_{k+1,q}, k+1, k)$-OOC consisting of $|\mathcal{N}(k+1, q)| + \left\lfloor \frac{q+1}{k+1} \right\rfloor \cdot \mathcal{L}(k, q)$ codewords.*

Observe that the Johnson bound:

$$J(\theta_{k+1,q}, k+1, k) = \frac{(\theta_{k+1,q} - 1)(\theta_{k+1,q} - 2) \cdots (\theta_{k+1,q} - k)}{(k+1)!} \approx \frac{q^{(k+1)k}}{(k+1)!} \tag{4.3}$$

By counting ordered $(k+2)$-tuples $(P_1, P_2, \ldots, P_{k+1}, \mathcal{K})$ where $\mathcal{K}$ is a $(k+1)$-arc in $PG(k, q)$ and $P_1, P_2, \ldots, P_{k+1}$ are the points in $\mathcal{K}$ we get:

$$|\mathcal{N}(k+1,q)| = \frac{\theta_{k,q}\,(\theta_{k,q}-1)\,(\theta_{k,q}-\theta_{1,q})\,(\theta_{k,q}-\theta_{2,q})\cdots(\theta_{k,q}-\theta_{k-1,q})}{(k+1)!} \approx \frac{q^{k(k+1)}}{(k+1)!} \tag{4.4}$$

It follows that the family of codes constructed as in Theorem 4.11 and Corollary 4.12 are asymptotically optimal.

5. An $(\mathbf{n}, \mathbf{w}, \lambda, \lambda+\mathbf{1})$ construction from arcs in $\mathbf{PG(k, q^2)}$. Since $GF(q)$ is a subfield of $GF(q^n)$ for $n > 1$, the projective space $PG(k,q)$ is naturally embedded in $PG(k,q^n)$ once the coordinate system is fixed. In particular, any $PG(k,q)$ embedded in $PG(k,q^2)$ is called a *Baer subspace* (BSS) of $PG(k,q^2)$ (for an introduction to Baer subspaces see [2] or [14]). A *frame* of a k-dimensional projective space is a set of $k+2$ points of which any $k+1$ points are a basis, that is, a $(k+2)$-arc. It is well known that a Baer subspace of $PG(k,q^2)$ is uniquely determined by a frame. Denote by $\mathcal{B}(k,q^2)$ the number of Baer subspaces of $PG(k,q^2)$. Then by counting ordered $(k+2)$-tuples or otherwise (see e.g. [14]) we have

$$\mathcal{B}(k,q^2) = q^{\frac{k(k+1)}{2}} \prod_{i=2}^{k+1} (q^i + 1) \approx q^{k^2+2k}. \tag{5.1}$$

THEOREM 5.1. *If $\Pi = PG(k,q)$ contains a $(k+1)$-family $\mathcal{F}$ of m-arcs, then there exists a $(k+1)$-family S of m-arcs in $\Sigma = PG(k,q^2)$, where $|S| = \mathcal{B}(k,q^2)\cdot|\mathcal{F}|$.*

Proof. Let Π_i, $1 \le i \le \mathcal{B}(k,q^2)$ denote the baer subspaces of Σ. By assumption, for each j, $1 \le j \le \mathcal{B}(k,q^2)$, there exists a $(k+1)$-family $\mathcal{F}_j$ of m-arcs in Π_j with $|\mathcal{F}_j| = |\mathcal{F}|$. Let

$$S = \bigcup_{j=1}^{\mathcal{B}(k,q^2)} \mathcal{F}_j.$$

As a Baer subspace is uniquely determined by a frame, two distinct BSSs cannot share a $(k+2)$-arc. It follows that S is a $(k+1)$-family of m-arcs with $|S| = \mathcal{B}(k,q^2)\cdot|\mathcal{F}|$. □

THEOREM 5.2. *In $PG(k,q)$ there exists a $(k+1)$-family $\mathcal{F}$ of q-arcs where*

$$|F| = q^{k-1} \cdot \prod_{i=1}^{k-1} (q^{k+1} - q^i)$$

Proof. Denote by X_P the number of NRCs through an arbitrary fixed point $P \in \Sigma = PG(k,q)$. By counting ordered pairs $(\mathcal{C}, Q)$ where $\mathcal{C}$ is a NRC in Σ and Q is

a point of $\mathcal{C}$ we get

$$\nu(k,q)(q+1) = \left(\frac{q^{k+1}-1}{q-1}\right) \cdot X_P,$$

which gives

$$X_P = q^{k-1} \cdot \prod_{i=1}^{k-1} (q^{k+1} - q^i).$$

Hence, removing P from each of the X_P NRCs through P yields a $(k+1)$-family $\mathcal{F}$ of q-arcs. □

COROLLARY 5.3. *For $k > 1$ and $q > k$ a prime power, there exists a $(\frac{q^{k+2}-1}{q-1}, q, k, k+1)$-OOC consisting of*

$$\mathcal{B}(k,q^2) \cdot X_P + \mathcal{L}(k,q^2) \cdot \mathcal{B}(1,q^2) =$$

$$q^{\frac{k^2+3k-2}{2}} \left(q^{k+1}+1\right) \prod_{i=1}^{k-1} \left[\left(q^{k+1}-q^i\right)\left(q^{i+1}+1\right)\right] + \left\lfloor \frac{q^{2(k+1)}-1}{q^4-1} \right\rfloor (q^3+q^2) \approx q^{2k^2+3k-2}$$

codewords.

Proof. Fix $k > 1$ and $q > k$ and let $\Sigma = PG(k+1, q^2)$. From Theorem 5.1 and Theorem 4.3 there exists a $(\frac{q^{k+2}-1}{q-1}, q, k, k+1)$-OOC C consisting of $\mathcal{B}(k,q^2) \cdot X_P$ codewords. Let ℓ be one of the $\mathcal{L}(k+1,q^2)$ lines in Σ with full orbit. As a frame uniquely determines a Baer subspace, it follows that any two Baer sublines of ℓ intersect in at most two points. Thus, as in Corollary 4.4 we may add $\mathcal{L}(k,q^2) \cdot \mathcal{B}(1,q^2)$ codewords to C. This gives a code of size $\mathcal{B}(k,q^2) \cdot X_P + \mathcal{L}(k,q^2) \cdot \mathcal{B}(1,q^2)$. □

REMARK 5.3.1. *Let $M(n,w,k,k+1)$ be the size of the codes constructed as in the Theorem. Note that $J(n,w,k+1) \approx q^{2k^2+3k}$ and $J(n,w,k) \approx q^{2k^2+2k}$ so though the codes constructed in the Corollary are not asymptotically optimal with respect to the Johnson bound, they appear to be of a competitive size. We also point out that from Equation 1.2 it follows that $M(n,w,k,k+1) > \Phi(n,w,k+1,k)$ for $k > 2$.*

COROLLARY 5.4. *For q a prime power there exists an $(\frac{q^8-1}{q^2-1}, q+1, 2, 3)$-OOC consisting of $\mathcal{B}(2,q^2) \cdot (q^3-q^2) + \mathcal{L}(3,q^2) \cdot \mathcal{B}(1,q^2)$ codewords. For $q = 2^t$ there exists an $(\frac{q^8-1}{q^2-1}, q+2, 2, 3)$-OOC consisting of $\mathcal{B}(2,q^2) \cdot (q^3-q^2) = q^3(q^2+1)(q^3+1)(q^3-q^2)$ (in this case, we cannot include the lines).*

Proof. $(q+1)$-arcs (conics) exist in $PG(2,q)$ and if q is even then $(q+2)$-arcs (hyperovals) exist. Appealing to Theorems 4.7 and 5.1 the first result follows from Theorem 4.3 and the second from Corollary 4.4. □

5.1. Codes from Baer Subspaces. One last consideration for constructing larger weight codes is to use Baer subspaces of $PG(k, q^2)$ themselves to correspond the codewords. The correlation numbers, in this case, are functions of q (for $k > 1$) which is probably not desirable. We provide the example nonetheless. Regarding the maximal intersection of two BSSs we have the following result (see [8], Theorem 1.3).

THEOREM 5.5. *Let B_1 and B_2 be two Baer subspaces of $PG(k, q^2)$. Then*

$$|B_1 \cap B_2| \leq \theta_{k-1,q} + 1$$

This gives us the following.

THEOREM 5.6. *For q a prime power there exists a $\left(\theta_{k+1,q^2}, \theta_{k,q}, \theta_{k-1,q}, \theta_{k-1,q} + 1\right)$-OOC consisting of $\mathcal{B}(k, q^2)$ codewords.*

Proof. As in the previous sections, embed $\Pi = PG(k, q^2)$ into $\Sigma = PG(k + 1, q^2)$ and consider the set of all BSSs in Π. Proceed with a construction as in Theorem 4.3 with BSSs in place of arcs. The auto-correlation, λ_a, is bounded above by the maximum intersection of two Baer subspaces lying in different hyperplanes of Σ. As two such hyperplanes meet in a $(k-1)$-flat of Σ, this intersection is bounded by $\theta_{k-1,q}$. For the cross-correlation λ_c, we need to consider the intersection of two BSSs lying in the same hyperplane of Σ, by Theorem 5.5 we have $\lambda_c \leq \theta_{k-1,q} + 1$. □

6. Conclusion. We have exhibited several classes of optical orthogonal codes generated by the same basic ideas in finite projective spaces. Our codes are derived from a nice geometric construction of sets of objects with small intersections sizes. Our hope was to find more examples of (asymptotically) optimal codes. Perhaps more research into the packing of various geometric objects into projective spaces, subject to a small intersection condition, may lead to further examples of optimal OOCs. We have exhibited constructions of code families wherein the auto-correlation is smaller than the cross-correlation. Perhaps these constructions will serve to motivate new investigations of upper bounds on $\Phi(n, w, \lambda_a, \lambda_c)$ with $\lambda_a < \lambda_c$.

REFERENCES

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

[2] Rey Casse. *Projective Geometry, An Introduction.* Oxford University Press, USA, first edition, 2006.

[3] 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.

[4] Habong Chung and P. Vijay Kumar. Optical orthogonal codes—new bounds and an optimal construction. *IEEE Trans. Inform. Theory*, 36(4):866–873, 1990.

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

[6] J. W. P. Hirschfeld. The number of points on a curve, and applications. Arcs and curves: the legacy of Beniamino Segre. *Rend. Mat. Appl. (7)*, 26(1):13–28, 2006.

[7] 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.

[8] Izabella Jagos, György Kiss, and Attila Pór. On the intersection of Baer subgeometries of $\mathrm{PG}(n, q^2)$. *Acta Sci. Math. (Szeged)*, 69(1-2):419–429, 2003.

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

[10] 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.

[11] 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.

[12] R. Omrani, O. Moreno, and P.V. Kumar. Optimum optical orthogonal codes with $\lambda > 1$. *Proc. Int. Symposium on Information Theory*, page 366, 2004.

[13] 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.

[14] Marta Sved. Baer subspaces in the n-dimensional projective space. In *Combinatorial mathematics, X (Adelaide, 1982)*, volume 1036 of *Lecture Notes in Math.*, pages 375–391. Springer, Berlin, 1983.

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

[16] Oswald Veblen and John Wesley Young. *Projective geometry. Vol. 1*. Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[17] 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.