Discrete Mathematics 311 (2011) 1187–1196

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Spreads, arcs, and multiple wavelength codes

T.L. Alderson [a,*], Keith E. Mellinger [b]

[a] Mathematical Sciences, University of New Brunswick, Saint John, NB, E2L 4L5, Canada
[b] Department of Mathematics, University of Mary Washington, Fredericksburg, VA 22401, USA

ARTICLE INFO

Article history:
Available online 2 July 2010

Keywords:
2-dimensional optical orthogonal code
Multiple weight codes
Singer subgroups

ABSTRACT

We present several new families of multiple wavelength (2-dimensional) optical orthogonal codes (2D-OOCs) with ideal auto-correlation $\lambda_a = 0$ (codes with at most one pulse per wavelength). We also provide a construction which yields multiple weight codes. All of our constructions produce codes that are either optimal with respect to the Johnson bound (J-optimal), or are asymptotically optimal and maximal. The constructions are based on certain pointsets in finite projective spaces of dimension k over $GF(q)$ denoted $PG(k, q)$.

1. Introduction

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 $1 \leq t \leq n-1$, we have $\sum_{i=1}^{n-1} c_i c_{i+t} \leq \lambda_a$,
- (cross-correlation property) for any two distinct codewords c, c' and for any integer $0 \leq t \leq n-1$, we have $\sum_{i=0}^{n-1} c_i c'_{i+t} \leq \lambda_c$,

where each subscript is reduced modulo n.

An $(n, w, \lambda_a, \lambda_c)$-OOC with $\lambda_a = \lambda_c$ is denoted 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 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.

The $(n, w, \lambda_a, \lambda_c)$-OOCs spread the input data bits in the time domain. Technologies such as Wavelength–Division–Multiplexing (WDM) and dense-WDM enable the spreading of codewords over both time and wavelength domains [15] where codewords may be considered as $\Lambda \times T(0, 1)$-matrices. These codes are referred to in the literature as multiwavelength, multiple-wavelength, wavelength-time hopping, and 2-dimensional OOCs. Here we shall refer to these codes as 2-dimensional OOCs (2D-OOCs).

The code length of a conventional one-dimensional OOC (1D-OOC) is always large in order to achieve good bit error rate performance. However, long code sequences will occupy a large bandwidth and reduce the bandwidth utilization. 1D-OOCs also suffer from relatively small cardinality. The 2D-OOCs overcome both of these shortcomings. We denote by $(\Lambda \times T, w, \lambda_a, \lambda_c)$ a 2D-OOC with constant weight w, Λ wavelengths, and time-spreading length T (hence, each codeword is a $\Lambda \times T$ binary matrix). The autocorrelation and cross correlation of a $(\Lambda \times T, w, \lambda_a, \lambda_c)$-2D-OOC have the following properties.

* Corresponding author.
E-mail addresses: tim@unbsj.ca, tim@unb.ca (T.L. Alderson), kmelling@umw.edu (K.E. Mellinger).

0012-365X/$ – see front matter © 2011 Published by Elsevier B.V.
doi:10.1016/j.disc.2010.06.010

Table 1
Known constructions of J-optimal families of AMOPPW codes. (p prime, q a prime power).

Parameters	Conditions	Reference
Codes with $\lambda = 1$		
$(\Lambda \times p, \Lambda, 1)$	$\Lambda \leq p$,	[9]
$\big(\theta(k, q^2) \times (q+1), q+1, 1\big)$	$k \geq 1$	Theorem 3.2
$(\theta(k, q) \times (q-1), q, 1)$	$k \geq 1$	Theorem 3.4
$((2^n+1) \times \theta(k, 2), 2^n, 1)$	$k \geq 1, n \geq 2$	Theorem 5.3, $q = 2$
Codes with $\lambda \geq 2$		
$(\Lambda \times p, \Lambda, \lambda_c)$	$\Lambda \leq p, \lambda_c \geq 1$	[11]
$((q^n+1) \times \theta(k, q), q^n, q-1)$	$k \geq 1, n \geq 2$	Theorem 5.3

- (auto-correlation property) for any codeword $A = (a_{i,j})$ and for any integer $1 \leq t \leq T-1$, we have $\sum_{i=0}^{\Lambda-1} \sum_{j=0}^{T-1} a_{i,j} a_{i,j+t} \leq \lambda_a$,
- (cross-correlation property) for any two distinct codewords $A = (a_{i,j})$, $B = (b_{i,j})$ and for any integer $0 \leq t \leq T-1$, we have $\sum_{i=0}^{\Lambda-1} \sum_{j=0}^{T-1} a_{i,j} b_{i,j+t} \leq \lambda_c$,

where each subscript is reduced modulo T. There are practical considerations to be made with regard to the implementation of these codes. First, in optical code-division multiple-access (OCDMA) applications, performance analysis shows that codes with $\lambda \leq 3$ are most desirable [10]. Such codes are our main focus here. Second, implementation is simplified (and more cost effective) if the codewords involved have at most one "1" per row [8] (or equivalently have $\lambda_a = 0$). Such codes are referred to as At Most One Pulse Per Wavelength (AMOPPW) OOCs, denoted $(\Lambda \times T, w, \lambda_c)$-AMOPPW. All codes constructed in the sequel are of AMOPPW type. Again, it is of interest to construct codes with as large cardinality as possible. From the Johnson Bound for constant weight codes, the following two bounds can be established for 2D-OOCs.

Theorem 1.1 (*[11]*).

$$\begin{aligned}\Phi(\Lambda \times T, w, 0, \lambda_c) &\leq J_1(\Lambda \times T, w, 0, \lambda_c)\\ &= \left\lfloor \frac{\Lambda}{w} \left\lfloor \frac{T(\Lambda-1)}{w-1} \left\lfloor \frac{T(\Lambda-2)}{w-2} \right\lfloor \cdots \left\lfloor \frac{T(\Lambda-\lambda)}{w-\lambda} \right\rfloor \right\rfloor \cdots \right\rfloor .\end{aligned}$$

If $w^2 > \Lambda T \lambda_c$, *then*

$$\begin{aligned}\Phi(\Lambda \times T, w, 0, \lambda_c) &\leq J_2(\Lambda \times T, w, 0, \lambda_c)\\ &= \min\left(\Lambda, \left\lfloor \frac{\Lambda(w-\lambda_c)}{w^2 - \Lambda T \lambda_c} \right\rfloor\right).\end{aligned}$$

Codes meeting either of the bounds above are said to be *J-optimal*. At present, constructions of infinite families of J-optimal AMOPPW codes are relatively scarce, with restrictive parameters. In Sections 3 and 5 we provide new constructions of J-optimal codes. Table 1 will perhaps place our constructions in context.

Let F be an infinite family of 2D-OOCs with varying "length" ΛT and with $\lambda_a = \lambda_c$. For any $(\Lambda \times T, w, \lambda)$-OOC $C \in F$ containing at least one codeword, the number of codewords in C is denoted by $M(\Lambda \times T, w, \lambda)$ and the corresponding Johnson bound is denoted by $J(\Lambda \times T, w, \lambda)$.

The family F is called asymptotically optimal if

$$\lim_{\Lambda T \to \infty} \frac{M(\Lambda \times T, w, \lambda)}{J(\Lambda \times T, w, \lambda)} = 1. \tag{1.1}$$

See [11] for a summary of known asymptotically optimal families of AMOPPW codes. Related to optimality is the concept of code maximality.

Definition 1.2. An $(n, w, \lambda_a, \lambda_c)$-OOC (resp. $(\Lambda \times T, w, \lambda_a, \lambda_c)$-2D-OOC) C is said to be *extendable* if there exists a binary sequence (resp. matrix) $\mathbf{w} \notin C$ such that $C \cup \{\mathbf{w}\}$ is an $(n, w, \lambda_a, \lambda_c)$-OOC (resp. $(\Lambda \times T, w, \lambda_a, \lambda_c)$-2D-OOC). A code which is not extendable is said to be *maximal*.

If a given code C has a cardinality that does not achieve an established upper bound, an exhaustive search could determine whether or not C is maximal. Of course, for codes of reasonable length, exhaustive searches quickly become infeasible. The codes constructed here correspond to pointsets in finite projective spaces and as such we are able in most cases to establish our codes as either optimal or maximal using the techniques of finite geometry. In particular (Sections 4 and 6) we provide infinite families of asymptotically optimal codes that are maximal.

There has been recent interest in constructing 2D-OOCs in which codewords may have different weights (see e.g. [6,12]). By a $(\Lambda \times T, \{w_1, w_2, \ldots, w_n\}, \lambda_a, \lambda_c)$ code we shall denote a 2D-OOC in which codewords are of weight $w_1, w_2, \ldots,$ or w_n.

Such codes have been shown to exhibit good bit error rate performance, and can be used to address certain quality-of service (QoS) requirements. For example, services such as voice-over-IP or video-on-demand have different quality of service (QoS) and bit-rates. Using multiple weight codes, these requirements can be addressed through weight assignment. Signals with higher QoS requirements may be assigned to codewords of higher weight while those with lower requirement could be assigned words of lower weight. In Section 6 we provide constructions for two infinite families of multiple weight codes that are both asymptotically optimal and maximal.

2. Preliminaries

Since our techniques rely heavily on the properties of finite projective and affine spaces, we start with a short overview of the necessary concepts. By $PG(k, q)$ we denote the classical (or Desarguesian) finite projective geometry of dimension k and order q which may be modeled with the affine (vector) space $AG(k + 1, q)$ of dimension $k + 1$ over the finite field $GF(q)$. Under this model, points of $PG(k, q)$ correspond to 1-dimensional subspaces of $AG(k, q)$, projective lines correspond to 2-dimensional subspaces, and so on. Elementary counting can be used to show that the number of d-flats in $PG(k, q)$ is given by the Gaussian coefficient

$$\begin{bmatrix} k+1 \\ d+1 \end{bmatrix}_q = \frac{(q^{k+1}-1)(q^{k+1}-q)\cdots(q^{k+1}-q^d)}{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)}. \tag{2.1}$$

Similar counting shows 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 $\theta(k, q)$ to represent this number. For a point set A in $PG(k, q)$ we shall denote by $\langle A\rangle$ the span of A, so $\langle A\rangle = PG(t, q)$ for some $t \le k$. A *d-flat Π* in $PG(k, q)$ is a subspace isomorphic to $PG(d, q)$; if $d = k - 1$, the subspace Π is called a *hyperplane*. 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.

A *Singer group* of $PG(k, q)$ is a cyclic group of automorphisms acting sharply transitively on the points. The generator of such a group is known as a *Singer cycle*. Singer groups are known to exist in classical projective spaces of any order and dimension and their existence follows from that of primitive elements in a finite field.

In the sequel we make use of a Singer group that is most easily understood by modeling a finite projective space using a finite field. If we let β be a primitive element of $GF(q^{k+1})$, the points of $\Sigma = PG(k, q)$ can be represented by the field elements $\beta^0 = 1, \beta, \beta^2, \dots, \beta^{n-1}$ where $n = \theta(k, q)$. Hence, in a natural way a point set A of $PG(k, q)$ corresponds to a binary n-tuple (or codeword) $(a_0, a_1, \dots, a_{n-1})$ where $a_i = 1$ if and only if $\beta^i \in A$.

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 β induces an automorphism, or collineation, on the associated projective space $PG(k, q)$. Denote by ϕ the collineation of Σ defined by $\beta^i \mapsto \beta^{i+1}$. The map ϕ clearly acts sharply transitively on the points of Σ.

We can construct 2-dimensional codewords by considering orbits under subgroups of G. Let $n = \theta(k, q) = \Lambda \cdot T$ where G is the Singer group of $\Sigma = PG(k, q)$. Since G is cyclic there exists a unique subgroup H of order T (H is the subgroup with generator ϕ^Λ).

Definition 2.1 (*Projective Incidence Matrix*)**.** Let Λ, T be integers such that $n = \theta(k, q) = \Lambda \cdot T$. For an arbitrary pointset S in $\Sigma = PG(k, q)$ we define the $\Lambda \times T$ incidence matrix $A = (a_{i,j})$, $0 \le i \le \Lambda - 1$, $0 \le j \le T - 1$ where $a_{i,j} = 1$ if and only if the point corresponding to $\beta^{i+j\cdot\Lambda}$ is in S.

If A is a pointset of Σ with corresponding $\Lambda \times T$ incidence matrix W of weight w, then ϕ^Λ induces a cyclic shift on the columns of W. For any such set A, consider its orbit $Orb_H(A)$ under the group H generated by ϕ^Λ. The set A has *full H-orbit* if $|Orb_H(A)| = T = \frac{n}{\Lambda}$ and *short H-orbit* otherwise. If A has full H-orbit then a representative member of the orbit and corresponding 2-dimensional codeword is chosen. The collection of all such codewords gives rise to a $(\Lambda \times T, w, \lambda_a, \lambda_c)$-2D-OOC, where

$$\lambda_a = \max_{1\le i<j\le T} \left\{|\phi^{\Lambda\cdot i}(A) \cap \phi^{\Lambda\cdot j}(A)|\right\} \tag{2.2}$$

and

$$\lambda_c = \max_{1\le i,j\le T} \left\{|\phi^{\Lambda\cdot i}(A) \cap \phi^{\Lambda\cdot j}(A')|\right\} \tag{2.3}$$

range over all A, A' with full H-orbit.

2.1. An affine analogue of the Singer automorphism

A further automorphism of $\Sigma = \mathrm{PG}(k, q)$ shall play a role in our constructions. It may be viewed as an affine analogue of the Singer automorphism. If a hyperplane Π_∞ (at infinity) is removed from $\mathrm{PG}(k, q)$, what remains is $\mathrm{AG}(k, q)$-the k-dimensional affine space. One way to model $\mathrm{AG}(k, q)$ is to view the points as the elements of $\mathrm{GF}(q^k)$. Recall that the set $\mathrm{GF}(q^k)^*$ of non-zero elements of $\mathrm{GF}(q^k)$ forms a cyclic group under multiplication. Take α to be a primitive element (generator) of $\mathrm{GF}(q^k)^*$. Each nonzero affine point corresponds in the natural way to α^j for some j, $0 \le j \le q^k - 2$. Denote by ψ the mapping of $\mathrm{AG}(k, q)$ defined by $\psi(\alpha^j) = \alpha^{j+1}$ and $\psi(0) = 0$. The map ψ is an automorphism of $\mathrm{AG}(k, q)$ and, moreover, ψ admits a natural extension to an automorphism $\hat{\psi}$ of $\mathrm{PG}(k, q)$. Denote by $\hat{G}$ the group generated by $\hat{\psi}$. The fundamental properties of the group $\hat{G}$ central to the constructions here are (for details, see e.g. [4,13].):

1. $\hat{G}$ fixes the point P_0 corresponding to the field element 0, and acts sharply transitively on the $q^k - 1$ nonzero affine points of $\mathrm{PG}(k, q)$.
2. $\hat{G}$ acts cyclically transitively on the points of Π_∞, in particular the subgroup $H = \langle \hat{\psi}^{\theta(k-1,q)} \rangle$ fixes Π_∞ pointwise.

The 2D-OOCs constructed using affine pointsets will therefore consist of codewords of dimension $\Lambda \times T$, where $\Lambda \cdot T = q^k - 1$.

Definition 2.2 (*Affine Incidence Matrix*)**.** Let Λ, T be integers such that $q^k - 1 = \Lambda \cdot T$. For an arbitrary pointset S in $\mathrm{AG}(k, q)$ we define the $\Lambda \times T$ incidence matrix $A = (a_{i,j})$, $0 \le i \le \Lambda - 1$, $0 \le j \le T - 1$ where $a_{i,j} = 1$ if and only if the point corresponding to $\alpha^{i+\Lambda \cdot j}$ is in S.

If A is a set of w nonzero affine points with corresponding $\Lambda \times T$ incidence matrix W of weight w, then $\hat{\psi}^\Lambda$ induces a cyclic shift on the columns of W. For any such set A, consider its orbit $\mathrm{Orb}_{\hat{H}}(A)$ under the group $\hat{H} = \langle \hat{\psi}^\Lambda \rangle$. If A has full $\hat{H}$-orbit then a representative member of the orbit and corresponding 2-dimensional codeword (say W) is chosen. The collection of all such codewords give rise to a $(\Lambda \times T, w, \lambda_a, \lambda_c)$-2D-OOC, where

$$\lambda_a = \max_{1 \le i < j \le T} \left\{ |\hat{\psi}^{\Lambda \cdot i}(A) \cap \hat{\psi}^{\Lambda \cdot j}(A)| \right\} \tag{2.4}$$

and

$$\lambda_c = \max_{1 \le i, j \le T} \left\{ |\hat{\psi}^{\Lambda \cdot i}(A) \cap \hat{\psi}^{\Lambda \cdot j}(A')| \right\} \tag{2.5}$$

range over all A, A' with full $\hat{H}$-orbit.

3. Optimal codes from lines, $\lambda_c = 1$

3.1. Codes from projective lines

Let $\Sigma = \mathrm{PG}(k, q)$, where $G = \langle \phi \rangle$ is the Singer group of Σ. Our work will rely on the following results about orbits of flats.

Theorem 3.1 (*[13,5]*)**.** *In $\Sigma = \mathrm{PG}(k, q)$, there exists a short G-orbit of d-flats if and only if $\gcd(k+1, d+1) \ne 1$. In this case there is precisely one short orbit $\mathcal{S}$; $\mathcal{S}$ partitions the points of Σ (i.e., constitutes a d-spread of Σ); the G-stabilizer of any $\Pi \in \mathcal{S}$ is $\mathrm{Stab}_G(\mathcal{S}) = \left\langle \phi^{\frac{\theta(k,q)}{\theta(d,q)}} \right\rangle$.*

Let $\Sigma = \mathrm{PG}(k, q)$, k odd with Singer group $G = \langle \phi \rangle$. Let $\mathcal{S}$ be the line spread determined (as in Theorem 3.1) by G where say $\mathrm{Stab}_G(\mathcal{S}) = H$. Consider a line $\ell \notin \mathcal{S}$. As ℓ is of full G-orbit, it is also of full H-orbit, that is $|O_H(\ell)| = q + 1$. Moreover, the lines in $O_H(\ell)$ are disjoint (ℓ is incident with precisely $q + 1$ members of $\mathcal{S}$, and H acts sharply transitively on the points of each line of $\mathcal{S}$). It follows that the number of full H-orbits of lines is

$$\frac{\begin{bmatrix} k+1 \\ 2 \end{bmatrix}_q - |\mathcal{S}|}{q+1} = \frac{1}{q+1} \cdot \left[\frac{(q^{k+1}-1)(q^{k+1}-q)}{(q^2-1)(q^2-q)} - \frac{\theta(k,q)}{q+1} \right] = \frac{q \cdot \theta(k,q) \cdot \theta(k-2,q)}{(q+1)^2}. \tag{3.1}$$

For each full H-orbit of lines, select a representative member and corresponding (projective) $\frac{\theta(k,q)}{q+1} \times (q+1)$ incidence matrix (2D-codeword). The collection of all such codewords comprises a $\left(\frac{\theta(k,q)}{q+1} \times (q+1), q+1, \lambda_a, \lambda_c\right)$-2DOOC C. As two lines intersect in at most one point we have (Eq. (2.3)) $\lambda_c = 1$. Moreover, since the lines in any particular full H-orbit

$O_H(\ell)$ are disjoint, we have (Eq. (2.2)) $\lambda_a = 0$. Hence, C is a $\left(\frac{\theta(k,q)}{q+1} \times (q+1), q+1, 1\right)$-AMOPPW code. From the bound (Theorem 1.1) we have

$$\Phi\left(\frac{\theta(k,q)}{q+1} \times (q+1), q+1, 0, 1\right) \leq \left\lfloor \frac{\frac{\theta(k,q)}{q+1}}{q+1} \left\lfloor \frac{(q+1)\left(\frac{\theta(k,q)}{q+1} - 1\right)}{q} \right\rfloor \right\rfloor. \tag{3.2}$$

Comparing (3.1) and (3.2) we see that C is in fact optimal. Noting that $\frac{\theta(k,q)}{q+1} = \theta\left(\frac{k-1}{2}, q^2\right)$, we have shown the following.

Theorem 3.2. *Let q be a prime power and let $t \geq 1$. There exists a J-optimal $\left(\theta(t, q^2) \times (q+1), q+1, 1\right)$-AMOPPW code.*

3.2. Codes from affine lines

Let $\Sigma = \mathrm{PG}(k, q)$ where $E = \Sigma \setminus \Pi_\infty$ is the associated affine space $\mathrm{AG}(k, q)$. Let $\hat{G} = \langle \hat{\psi} \rangle$ be the map as described in Section 2.1 based on the primitive element α of $\mathrm{GF}(q^k)^*$. Our affine analog of Theorem 3.1 follows from Theorem 8 of [13].

Theorem 3.3 (*[13]*)**.** *A d-flat Π in $\mathrm{PG}(k, q)$ is of full $\hat{G}$-orbit if and only if the origin $P_0 \notin \Pi$ and Π is not a subset of Π_∞.*

From Theorem 3.3 it follows that each point of Π_∞ is incident with precisely $q^{k-1} - 1$ lines of full $\hat{G}$-orbit. Let $H = \langle \hat{\psi}^{\theta(k-1,q)} \rangle$ be the unique subgroup of order $q - 1$. Note that H fixes each point of Π_∞. Clearly, any line with full $\hat{G}$-orbit is also of full H-orbit. The number of full $\hat{H}$-orbits of lines is therefore at least

$$\frac{\theta(k-1, q) \cdot (q^{k-1} - 1)}{q - 1} = \theta(k-1, q) \cdot \theta(k-2, q). \tag{3.3}$$

For each full $\hat{H}$-orbit, select a representative line ℓ and corresponding (affine) $\Lambda \times T = \theta(k-1, q) \times (q-1)$ incidence matrix W (corresponding to the points of $\ell' = \ell \cap E$). A $(\Lambda \times T, w, \lambda_a, \lambda_c)$-2D-OOC C results.

Each representative line ℓ used in the construction meets Π_∞ in precisely one point, say $\ell \cap \Pi_\infty = P_\infty$, so codewords are of weight q. As two lines meet in at most one point we get $\lambda_c = 1$. Moreover, since P_∞ is fixed under the action of $\hat{H}$, the orbit $O_{\hat{H}}(\ell)$ is comprised of $|H| = q - 1$ lines, each incident with P_∞ (in particular, no two meet in an affine point). Therefore, we have $\lambda_a = 0$ and C is a $(\theta(k-1, q) \times (q-1), q, 1)$-AMOPPW code where $|C|$ is given by (3.3).

From Theorem 1.1 we have

$$\Phi(\theta(k-1, q) \times (q-1), q, 1) \leq \left\lfloor \frac{\theta(k-1, q)}{q} \left\lfloor \frac{q^k - 2}{q - 1} \right\rfloor \right\rfloor = \lfloor \theta(k-1, q) \cdot \theta(k-2, q) \rfloor = |C|.$$

We have shown the following.

Theorem 3.4. *For q a prime power and for each t there exists a J-optimal $(\theta(t, q) \times (q-1), q, 1)$-AMOPPW code.*

4. Codes from arcs, $\lambda_c = 2$

In the next construction, families of asymptotically optimal codes are obtained. Our construction relies on the use of *arcs* in finite projective spaces. The idea of using arcs to construct OOCs was used extensively in [1–3]. While the codes we are about to construct are not optimal, they are asymptotically optimal and maximal.

We start by recalling a few additional concepts from finite geometry. An *m-arc* in $\mathrm{PG}(2, q)$ is a collection of $m > 2$ points that meets no line in as many as 3 points. A line ℓ is said to be external, tangent, or secant to an arc $\mathcal{K}$ in the case that it is incident with precisely 0, 1, or 2 points of $\mathcal{K}$ respectively. An *m-arc* is complete if it is not contained in an $(m+1)$-arc. In $\mathrm{PG}(2, q)$ 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 *B.* Segre says that every complete arc of $\mathrm{PG}(2, q)$, q odd, is a conic. The $(q+2)$-arcs (hyperovals) exist in $\mathrm{PG}(2, q)$ if q is even and they are necessarily complete.

If $\mathcal{C}$ is a conic in $\mathrm{PG}(2, q)$, then the subgroup of $\mathrm{PGL}(3, q)$ leaving $\mathcal{C}$ fixed is (isomorphic to) $\mathrm{PGL}(2, q)$ (see [7, Theorem 27.5.3]). It follows that the number of distinct conics in $\mathrm{PG}(2, q)$ is given by

$$\frac{|\mathrm{PGL}(3, q)|}{|\mathrm{PGL}(2, q)|} = \frac{(q^3-1)(q^3-q)(q^3-q^2)}{(q^2-1)(q^2-q)} = q^5 - q^2. \tag{4.1}$$

The following is a well known property of conics (see [14]).

Theorem 4.1. *A 5-arc in $\mathrm{PG}(2, q)$ is contained in a unique conic.*

A collection $\mathcal{F}$ of m-arcs in $\pi = \mathrm{PG}(2, q)$ is said to be a t-family if every pair of distinct members of $\mathcal{F}$ meet in at most t points. Hence, from Theorem 4.1 the collection of all conics in π forms a 4-family. Central to our construction is a particular 2-family of arcs, the existence of which follows from Theorem 8 in [1].

Theorem 4.2. *In $\pi = \mathrm{PG}(2, q)$ there exists a 2-family, $\mathcal{F}$, of conics in π such that:*
1. $|\mathcal{F}| = q^3 - q^2$.
2. *There exists a particular line ℓ, external to each member of $\mathcal{F}$.*

4.1. Code construction

Here we shall provide a construction for a $(q^2 + 1 \times q + 1, q + 1, 2)$-AMOPPW code, C. Each codeword shall be one of two types, A or B. Those of type A shall correspond to conics, and those of type B shall correspond to lines. The codewords of type A may be described as follows.

Let $\Sigma = \mathrm{PG}(3, q)$ and let $G = \langle \phi \rangle$ be the associated Singer group. Consider the action of G on the lines of Σ and let $\mathcal{S}$ be the spread of Σ determined by G as in Theorem 3.1. In particular, the subgroup $H = \left\langle \phi^{q^2+1} \right\rangle$ acts sharply transitively on the points of each line $\ell \in \mathcal{S}$. Let $\mathcal{S} = \{\ell_1, \ell_2, \ldots, \ell_{q^2+1}\}$ and for each $i = 1, 2, \ldots, q^2 + 1$ let π_i be any plane containing ℓ_i. Since the ℓ_is are mutually skew, it follows that the π_is are distinct. On each π_i, let $\mathcal{F}_i$ be a 2-family of conics (as in Theorem 4.2), each having ℓ_i as an external line. Note that any such conic necessarily meets each spread line in at most one point. Each of the $(q^2 + 1)(q^3 - q^2)$ conics constructed in this manner shall give rise to a projective $(q^2 + 1) \times (q + 1)$ incidence matrix. The collection of all such matrices shall be the codewords of type A.

The codewords of type B shall be the collection of projective $(q^2 + 1) \times (q + 1)$ incidence matrices corresponding to representative lines, chosen one from each full H-orbit of lines. As in Eq. (3.1), there are precisely $q(q^2 + 1)$ codewords of type B.

Let C be the collection of all projective $(q^2 + 1) \times (q + 1)$ incidence matrices (codewords) of type A or B. That C has constant weight $q + 1$ is clear, so C is a $(q^2 + 1 \times q + 1, q + 1, \lambda_a, \lambda_c)$-2D-OOC.

We claim $\lambda_a = 0$. For codewords of type A, this follows from the fact that each of the conics used in the construction meets each spread line in at most one point. For codewords of type B the result follows from Section 3.1.

Next, we claim $\lambda_c = 2$. Let w_1 and w_2 be distinct codewords (or cyclic column shifts of codewords). We consider cases.

Case 1: w_1 and w_2 are both of type A. In this case, let w_1 and w_2 correspond to the conics $\mathcal{C}_1$ and $\mathcal{C}_2$. Let π_a and π_b be the planes of Σ containing $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. If $\pi_a = \pi_b$, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are members of a common 2-family and therefore share at most 2 points. Otherwise π_a and π_b meet in a line; in which case (since a line meets a conic in at most two points) $|\mathcal{C}_1 \cap \mathcal{C}_2| \le 2$. So two type A codewords satisfy $\lambda_c = 2$.

Case 2: w_1 and w_2 are both of type B. From the results of Section 3.1, two such codewords satisfy $\lambda_c = 1$.

Case 3: w_1 is of type A and w_2 is of type B. In this case w_1 corresponds to a conic and w_2 corresponds to a line. Since a line meets a conic in at most two points, the result follows.

We have shown the following.

Theorem 4.3. *Let q be a prime power. Then there exists a $\left(q^2 + 1 \times q + 1, q + 1, 2\right)$-AMOPPW code, C with $|C| = (q^2+1)(q^3 - q^2 + q)$.*

4.1.1. Optimality

From the bound (Theorem 1.1) we have

$$\Phi\left(q^2 + 1 \times q + 1, q + 1, 2\right) \le \left\lfloor \frac{q^2 + 1}{q + 1} \left\lfloor \frac{(q + 1)q^2}{q} \left\lfloor \frac{(q + 1)(q^2 - 1)}{q - 1} \right\rfloor \right\rfloor \right\rfloor$$
$$= (q^2 + 1)(q^3 + 2q^2 + q).$$

Theorem 4.4. *The family of codes constructed in Theorem 4.3 is asymptotically optimal, and for $q > 4$, each code is maximal.*

Proof. That the codes are asymptotically optimal is clear. We only need to show that our codes are maximal. To see this, consider the possibility of a new codeword W being added to our codes. This codeword necessarily corresponds to a set S of points of Σ. To maintain the cross-correlation of 2, S must meet each line of Σ in at most 2 points, and to maintain auto-correlation $\lambda_a = 0$, S must meet each spread line in at most 1 point.

Now consider the intersection of a plane π with our set S. Clearly, π contains some spread line, ℓ. A quick count shows that the 2-family of conics described in the construction of the codes covers every triangle of points in $\pi \setminus \{\ell\}$. In order to maintain a cross-correlation of 2, S must therefore meet π in at most 3 points. In particular, if S meets π in three points, then the points necessarily form a triangle, with precisely one point incident with ℓ. Thus, by counting co-planar pairs (τ, ℓ), where τ is a triangle (of points) in S and ℓ is a spread line we obtain

$$\binom{q + 1}{3} \le (q + 1) \left\lfloor \frac{q}{2} \right\rfloor.$$

This inequality is false for $q > 4$. Consequently, the codes are maximal for $q > 4$. $\square$

4.2. A generalization to higher dimensions

The construction above can be mimicked in higher dimensional ambient spaces $\Sigma = \mathrm{PG}(k, q)$, $k > 3$ odd. Let G be the Singer group of Σ, H the unique subgroup of order $q+1$, and $\mathcal{S}$ the line spread fixed by H.

We first note that every plane π will have full orbit under H. Indeed, if π contains a line of $\mathcal{S}$ then $\mathrm{Stab}_H(\pi)$ is an automorphism of π fixing a line of π, and dually, must fix a point. Since G acts sharply transitively on the points of Σ, π must have a trivial stabilizer. If π contains no line of $\mathcal{S}$ then π is incident with precisely $\theta(2, q)$ members of $\mathcal{S}$. For each $\ell \in \mathcal{S}$, H acts sharply transitively on the points of ℓ. Consequently, the orbit $\mathrm{Orb}_H(\pi)$ consists of $q+1$ mutually disjoint planes.

Codewords shall again be of two types, A, and B. Codewords of type A shall correspond to certain conics as follows. For each full H-orbit of planes, select a representative member, γ, and a 2-family $\mathcal{F}$ conics on γ composed of $q^3 - q^2$ members. Note that if γ contains a line ℓ of $\mathcal{S}$ then (as in the three dimensional case) $\mathcal{F}$ is chosen in such a way that ℓ is external to each member of $\mathcal{F}$. The collection of all such conics shall comprise the codewords of type A.

Codewords of type B shall correspond to full H-orbits of lines, just as in the three dimensional case. In this manner we arrive at an $\left(\theta\left(\frac{k-1}{2}, q^2\right) \times (q+1), q+1, 2\right)$-AMOPPW code, C. (Note: $\frac{\theta(k,q)}{q+1} = \theta\left(\frac{k-1}{2}, q^2\right)$.) With reference to Eqs. (2.1) and (3.1) we have

$$|C| = \frac{1}{q+1}\begin{bmatrix} k+1 \\ 3 \end{bmatrix}_q (q^3 - q^2) + \frac{q \cdot \theta(k, q) \cdot \theta(k-2, q)}{(q+1)^2} \approx q^{3k-4}. \tag{4.2}$$

From the bound (Theorem 1.1) we have

$$\Phi(C) \le \left\lfloor \frac{\theta\left(\frac{k-1}{2}, q^2\right)}{q+1} \left\lfloor \frac{(q+1)\left(\theta\left(\frac{k-1}{2}, q^2\right) - 1\right)}{q} \left\lfloor \frac{(q+1)\left(\theta\left(\frac{k-1}{2}, q^2\right) - 2\right)}{q-1} \right\rfloor \right\rfloor \right\rfloor$$
$$\approx q^{3k-4}.$$

Consequently, we have:

Theorem 4.5. *For each $t \ge 1$, there exists an asymptotically optimal family of $\left(\theta\left(t, q^2\right) \times (q+1), q+1, 2\right)$-AMOPPW codes.*

5. Codes from planes, $\lambda_c \ge 1$

Here we shall provide a construction for $((q^2+1) \times (q+1), q^2, q-1)$-AMOPPW codes. Let $\Sigma = \mathrm{PG}(3, q)$ with Singer group $\langle \phi \rangle$. By Theorem 3.1, there exists a short G-orbit of lines, $\mathcal{S} = \{\ell_1, \ell_2, \ldots, \ell_{q^2+1}\}$. Let $\sigma = \phi^{q^2+1}$ and let $H = \langle \sigma \rangle$ be the unique subgroup of G having order $q+1$.

Note that each line ℓ of Σ is contained in precisely $q+1$ planes, forming the *fan of planes on* ℓ. For each $i = 1, 2, \ldots, q^2+1$, let $\mathcal{P}_i$ be the fan of planes on ℓ_i. Each plane of Σ is of full G orbit, and is therefore of full H-orbit. It follows that H acts sharply transitively on the members of $\mathcal{P}_i$ for each $i = 1, 2, \ldots, q^2+1$.

Let $\Pi_i \in \mathcal{P}_i$, and let $\Pi_i^* = \Pi_i \setminus \{\ell_i\}$, $i = 1, 2, \ldots, q^2+1$. The collection of incidence matrices corresponding to the Π_i^*'s shall comprise a $((q^2+1) \times (q+1), q^2, q-1)$-AMOPPW code, C. That C is of constant weight $w = q^2$ is clear.

First note that $\lambda_a = 0$. This follows from the fact that each Π_i^* meets each spread line in at most one point.

We now argue that $\lambda_c = q-1$. Let w_1 and w_2 be codewords of C. With no loss of generality, we may assume that w_1 and w_2 correspond to the pointsets Π_1^* and Π_2^* respectively. A dimension argument shows Π_1 and Π_2 meet precisely in a line, say $\Pi_1 \cap \Pi_2 = \ell$. Since ℓ is incident with both ℓ_1 and ℓ_2 it follows that $|\Pi_1^* \cap \Pi_j^*| = q-1$. A similar argument shows $|\sigma^s\left(\Pi_1^*\right) \cap \sigma^t\left(\Pi_2^*\right)| = q-1$ for any s, t. From the Eq. (2.3) we have $\lambda_c = q-1$. We have shown the following.

Theorem 5.1. *For q a prime power, there exists a $\left((q^2+1) \times (q+1), q^2, q-1\right)$-AMOPPW code with $|C| = q^2+1$.*

Note that the second bound of Theorem 1.1 applies to this class of codes since $w^2 = q^4 > \Lambda \cdot T \cdot \lambda_c = q^4 - 1$. As such

$$\begin{aligned}\Phi(\Lambda \times T, w, 0, \lambda_c) &\le \min\left(\Lambda, \left\lfloor \frac{\Lambda(w-\lambda_c)}{w^2 - \Lambda T \lambda_c} \right\rfloor\right) \\ &= \min\left(q^2+1, \left\lfloor \frac{(q^2+1)(q^2-(q^2-1))}{q^4-(q^4-1)} \right\rfloor\right) \\ &= q^2+1\end{aligned}$$

and we have that our codes are indeed optimal.

Theorem 5.2. *The codes constructed in Theorem 5.1 are J-optimal.*

5.1. A generalization to higher dimensions

The construction above can be generalized to higher dimensions. Let $\Sigma = \mathrm{PG}(2n+1, q)$, $n \geq 1$. Let G be the Singer group of Σ, $H = \langle\sigma\rangle$ be the unique subgroup of G having order $\theta(n, q)$. Let $\mathcal{S} = \Pi_1, \Pi_2, \ldots, \Pi_{q^{n+1}+1}$ be the n-spread of Σ fixed by H as in Theorem 3.1. For each $i = 1, 2, \ldots, q^{n+1} + 1$, let $\mathcal{P}_i$ be the fan of $(n + 1)$-flats on Π_i, let Ω_i be a representative member of $\mathcal{P}_i$, and let $\Omega_i^* = \Omega_i \setminus \Pi_i$. Note that H acts sharply transitively on the members of $\mathcal{P}_i$ for each i.

The collection of incidence matrices corresponding to the Ω_i^*s shall comprise a $\left((q^{n+1} + 1) \times \theta(n, q), q^{n+1}, q - 1\right)$-AMOPPW code, C. That C is of constant weight $w = q^n$ is clear.

We now show that $\lambda_a = 0$. Let the codeword w_1 correspond to the pointset Ω_1^*. For any k we have $\Pi_1 \subseteq \Omega_1 \cap \sigma^k(\Omega_1)$. Consequently, the proof will follow as in the case $n = 1$ if we can show that Ω_1 is of full H orbit. Observe that if $|\Omega_1 \cap \Pi_j| > 1$ then Ω_1 and Π_j share (at least) a line. Every line in Ω_1 intersects Π_1 nontrivially, so

$$|\Omega_1 \cap \Pi_j| > 1 \Rightarrow \Pi_1 \cap \Pi_j \neq \emptyset \Rightarrow \Pi_1 = \Pi_j.$$

By the Pigeonhole Principle it follows that if $1 \neq j$ then Ω_1 meets Π_j precisely in a point. That Ω_1 has full H-orbit then follows from the fact that H acts sharply transitively on the points of each Π_j (Theorem 3.1).

To show that $\lambda_c = q - 1$, let w_1 and w_2 be codewords corresponding to Ω_1^* and Ω_2^* respectively. A dimension argument shows that Ω_1 and Ω_2 meet in at least a line. Moreover, since Π_1 and Π_2 are disjoint, it follows that Ω_1 and Ω_2 meet in at most a line. So $\Omega_1 \cap \Omega_2 = \ell$ for some line ℓ. Since ℓ must be incident with both Π_1 and Π_2 it follows that $|\Omega_1^* \cap \Omega_2^*| = q - 1$. A similar argument shows that for any i, j, $|\sigma^i\left(\Omega_1^*\right) \cap \sigma^j\left(\Omega_2^*\right)| = q - 1$. From Eq. (2.3) we have $\lambda_c = q - 1$. We have shown the following.

Theorem 5.3. *For q a prime power, there exists a $\left((q^{n+1} + 1) \times \theta(n, q), q^{n+1}, q - 1\right)$-AMOPPW code with $|C| = q^{n+1} + 1$.*

As in Theorem 5.2, our generalized construction will again lead to codes that are J-optimal. The second bound of Theorem 1.1 applies to this class of codes as well since in this case $w^2 = (q^{n+1})^2 > \Lambda \cdot T \cdot \lambda_c = (q^{n+1}+1)\left(\frac{q^{n+1}-1}{q-1}\right)(q-1) = (q^{n+1})^2 - 1$. As such

$$\begin{aligned}\Phi(\Lambda \times T, w, 0, \lambda_c) &\leq \min\left(\Lambda, \left\lfloor \frac{\Lambda(w - \lambda_c)}{w^2 - \Lambda T \lambda_c} \right\rfloor\right) \\ &= q^{n+1} + 1\end{aligned}$$

and we have that our codes are indeed optimal.

Theorem 5.4. *The codes constructed in Theorem 5.3 are J-optimal.*

6. Multiple weight constructions

6.1. Codes with $\lambda_c = 3$

Here we shall provide a construction for multiple weight $((q + 1) \times (q - 1), \{q, q - 1, q - 2\}, 3)$-AMOPPW codes. Let ℓ_∞ be a line of $\Pi = \mathrm{PG}(2, q)$ and let $\Pi^* = \Pi \setminus \ell_\infty$ be the associated affine plane. To avoid degenerate cases, we shall assume $q > 5$. As in Section 2.1 denote by P_0 the affine point corresponding to the origin, and let $\hat{G} = \langle\Psi\rangle$ be the affine analogue of the Singer map. Let $\hat{H} = \langle\sigma\rangle$ be the unique subgroup of $\hat{G}$ having order $q - 1$.

Consider the collection of all conics passing through the point P_0. By counting ordered pairs (P, Γ) where P is a point of Π and Γ is a conic containing P, we see that there are $q^4 - q^2$ such conics. For each conic in the collection, remove the point P_0, and remove any infinite points (points on ℓ_∞). We are left with a collection $\mathcal{C}$ of arcs having size q, $q - 1$, or $q - 2$ depending on whether the original conic contained 0, 1, or 2 infinite points respectively. Moreover (Theorem 4.1) any two members of $\mathcal{C}$ meet in at most three points.

We claim that each member of $\mathcal{C}$ is of full $\hat{H}$ orbit. Clearly, $\hat{H}$ fixes P_0, and fixes ℓ_∞ point-wise. So, given a line ℓ incident with P_0, $\hat{H}$ fixes both P_0 and the infinite point $\ell \cap \ell_\infty$ of ℓ, and acts sharply transitively on the $q - 1$ non-zero affine points of ℓ. Hence, any affine point set not containing P_0 and meeting each line through P_0 in at most one point will have full $\hat{H}$ orbit. As each member of $\mathcal{C}$ has this property it follows that all members of $\mathcal{C}$ are of full $\hat{H}$ orbit. Select a representative member from each one of the $q^3 + q^2$ full $\hat{H}$-orbits, and include the corresponding $(q + 1) \times (q - 1)$ incidence matrix in the code. As any two arcs used in the construction may meet in at most three points, the resulting codewords satisfy $\lambda_c = 3$.

Note that as in Section 3.2, there are $q + 1$ full $\hat{H}$-orbits of affine lines. As any line meets an arc in at most two points we may include the corresponding codewords in our code. Simple counting allows us to enumerate the number of codewords of each weight as given in the following table.

Word weight	Number of codewords
q	$\frac{q^3+q+2}{2}$
$q-1$	q^2+q
$q-2$	$\frac{q^3-q}{2}$

That each codeword satisfies $\lambda_a = 0$ follows from the fact that corresponding pointsets meet each line through P_0 in at most one point. Thus, we have the following.

Theorem 6.1. *For each prime power $q > 5$, there exists an $((q+1) \times (q-1), \{q, q-1, q-2\}, 3)$-AMOPPW code consisting of q^3+q^2+q+1 codewords.*

6.1.1. Optimality

We may compare the size of the codes obtained in Theorem 6.1 with the bound of Theorem 1.1, by assuming constant weight $q-2$. In this manner we see that the codes form an asymptotically optimal family. Moreover, each of the codes are maximal. Indeed, let C be a code constructed as in the theorem and suppose that a codeword W may be added to C. The codeword W corresponds to a set S of nonzero points in Π^*. From the auto-correlation property, it follows that S meets each line through P_0 in at most one point. Also, from the cross correlation property, S meets all other lines in at most three points. By assumption, $|S| \geq q-2 > 3$, so S contains three points which form a quadrangle with P_0. Any such quadrangle may be extended to a conic through P_0. Consequently, W will have at least three common coordinates with (a cyclic shift of) some codeword of C. This contradiction gives us the following.

Theorem 6.2. *The family of codes constructed in Theorem 6.1 is asymptotically optimal. Each code in the family is maximal.*

6.2. Codes with $\lambda_c = 2$

Employing techniques similar to the construction above we may obtain $((q+1) \times (q-1), \{q+1, q, q-1, q-2\}, 2)$-AMOPPW codes. To avoid degenerate cases, we shall assume $q > 4$. Let Π, P_0, ℓ_∞, $\hat{G}$, and $\hat{H}$, be as defined above. Let P_1 be a point of ℓ_∞ and consider the collection of all conics containing both P_0 and P_1. By counting ordered triples (P, Q, Γ) where P and Q are points and Γ is a conic containing both P and Q, we see that there are $q^3 - q^2$ such conics. For each conic in the collection, remove the point P_0 and any infinite points. We are left with a collection $\mathcal{C}$ of arcs having size $q-1$, or $q-2$ depending on whether the original conic contained 1, or 2 infinite points respectively. Moreover (Theorem 4.1) any two members of $\mathcal{C}$ meet in at most two points.

Each line through P_0 meets any given member of $\mathcal{C}$ in at most one point. It follows that each member of $\mathcal{C}$ is of full $\hat{H}$ orbit. Selecting a representative from each full orbit yields q^2-q codewords satisfying $\lambda_c = 2$. As above we may also include a codeword of weight q for each of the full $\hat{H}$-orbits of lines, but we make one slight change. One of the full line orbits corresponds to a pencil of $(q-1)$ lines through P_1. To the representative line ℓ of this orbit we add one further point $Q \neq P_0, P_1$, chosen arbitrarily from the line $\langle P_0, P_1\rangle$. The resulting set of $q+1$ points meets each line through P_0 in at most one point and is therefore of full $\hat{H}$ orbit. Each line other than ℓ meets $\ell \cup \{Q\}$ in at most 2 points. The line $\langle P_0, P_1\rangle$ is disjoint from each member of $\mathcal{C}$, thus $\ell \cup \{Q\}$ meets each member of $\mathcal{C}$ in at most two points. The resulting code consists of q^2+q+1 codewords with weight distribution as described in the table below.

Word weight	Number of codewords
$q+1$	1
q	q
$q-1$	q
$q-2$	q^2-q

That each codeword satisfies $\lambda_a = 0$ follows from the fact that corresponding pointsets meet each line through P_0 in at most one point. Thus, we have the following.

Theorem 6.3. *For each prime power $q > 4$, there exists an $((q+1) \times (q-1), \{q+1, q, q-1, q-2\}, 2)$-AMOPPW code consisting of q^2+q+1 codewords.*

6.2.1. Optimality

Comparing the size of the codes obtained in Theorem 6.3 with the bound of Theorem 1.1 (by assuming constant weight $q-2$) shows them to be asymptotically optimal (The size of the code exceeds the bound assuming constant weight $q+1$ or q). An argument similar to that used in the previous construction shows that any set of 6 points in π^* having full $\hat{H}$ orbit and satisfying $\lambda_a = 0$ necessarily contains three points which in turn form a 5-arc with P_0 and P_1. Any 5-arc uniquely determines a conic. Consequently, for $q \geq 7$, each of the codes is maximal.

Theorem 6.4. *The family of codes constructed in Theorem 6.3 is asymptotically optimal. For $q \geq 7$, each code in the family is maximal.*

7. Conclusion

As noted in the introduction, constructions of infinite families of J-optimal AMOPPW codes are relatively scarce, and our work provides new constructions of such J-optimal codes. Moreover, we construct infinite families of asymptotically optimal codes that are maximal. Finally, our work provides a method for constructing multiple weight codes. Table 1 provides a nice summary of our constructions. It is clear that the use of finite geometry has the potential to provide robust methods for constructing various classes of codes with strong correlation properties.

Acknowledgement

The first author acknowledges support from the N.S.E.R.C. of Canada Mathematical Sciences.

References

[1] T.L. Alderson, Optical orthogonal codes and arcs in PG(d, q), Finite Fields Appl. 13 (4) (2007) 762–768.
[2] T.L. Alderson, Keith E. Mellinger, Optical orthogonal codes from Singer groups, in: Advances in Coding Theory and Cryptology, in: Coding Theory and Cryptology, vol. 3, World Scientific, Hackensack, NJ, 2007, pp. 51–70.
[3] T.L. Alderson, Keith E. Mellinger, Classes of optical orthogonal codes from arcs in root subspaces, Discrete Math. 308 (7) (2008) 1093–1101.
[4] R.C. Bose, An affine analogue of Singer's theorem, J. Indian Math. Soc. (NS) 6 (1942) 1–15.
[5] Keldon Drudge, On the orbits of Singer groups and their subgroups, Electron. J. Combin. 9 (1) (2002) Research Paper 15, 10 pp (electronic).
[6] F.-R. Gu, J. Wu, Construction and performance analysis of variable-weight optical orthogonal codes for asynchronous optical CDMA systems, J. Lightwave Technol. 23 (2005) 740–748.
[7] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, in: Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991, Oxford Science Publications.
[8] E. Jugl, K. Iversen, New Combinatorial Ber Bounds for Families of (0, 1)-matrix Codes, Vol. 3, 1997, pp. 1543–1547.
[9] W.C. Kwong, Guu-Chang Yang, Extended carrier-hopping prime codes for wavelength-time optical code-division multiple access, IEEE Trans. Commun. 52 (7) (2004) 1084–1091.
[10] S. Mashhadi, J.A. Salehi, Code-division multiple-access techniques in optical fiber networks—part III: optical AND logic gate receiver structure with generalized optical orthogonal codes, IEEE Trans. Commun. 54 (8) (2006) 1457–1468.
[11] R. Omrani, P. Vijay Kumar, Improved constructions and bounds for 2-d optical orthogonal codes, in: ISIT 2005, Proc. Int. Symp. Inf. Theory, September 2005, pp. 127–131.
[12] Yong-Chun Piao, Jinwoo Choe, Wonjin Sung, Dong-Joon Shin, Construction of scalable 2-D multi-weight optical orthogonal codes for optical CDMA networks, IEICE Trans. Commun. E91-B (12) (2008) 3990–3993.
[13] C. Radhakrishna Rao, Cyclical generation of linear subspaces in finite geometries, in: Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, NC, 1967), Univ. North Carolina Press, Chapel Hill, NC, 1969, pp. 515–535.
[14] Joseph A. Thas, Projective geometry over a finite field, in: Handbook of Incidence Geometry, North-Holland, Amsterdam, 1995, pp. 295–347.
[15] Guu-Chang Yang, W.C. Kwong, Performance comparison of multiwavelength CDMA and WDMA + CDMA for fiber-optic networks, IEEE Trans. Commun. 45 (11) (1997) 1426–1434.