Spreads, arcs, and multiple wavelength codes

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

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

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 \( PG(k,q) \).

AMS 2000 subject classification: 94B27 (05B25,51E99)
Keywords: 2-dimensional optical orthogonal code, multiple weight codes, Singer subgroups

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 \((n,w,\lambda)\)-OOC. The number of codewords is the size of the code. For fixed values of \( n, w, \lambda_a \) and \( \lambda_c \), 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 multlwavelength, multiple-wavelength, wavelength-time hopping, and 2-dimensional OOCs. Here we shall refer to these codes as 2-dimensional OOCs (2D-OOCs).

*The author acknowledges support from the N.S.E.R.C. of Canada
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 \(w\), \(\Lambda\) 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.

- (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 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 2-D OOCs.

**Theorem 1.1** ([11]).

\[
\Phi(\Lambda \times T, w, 0, \lambda_c) \leq J_1(\Lambda \times T, w, 0, \lambda_c) = \left\lfloor \frac{\Lambda}{w} \left\lfloor \frac{T(\Lambda - 1)}{w - 1} \right\rfloor \left\lfloor \frac{T(\Lambda - 2)}{w - 2} \right\rfloor \cdots \left\lfloor \frac{T(\Lambda - \lambda)}{w - \lambda} \right\rfloor \right\rfloor. 
\]

If \(w^2 > \Lambda T \lambda_c\), then

\[
\Phi(\Lambda \times T, w, 0, \lambda_c) \leq J_2(\Lambda \times T, w, 0, \lambda_c) = \min \left( \Lambda, \left\lfloor \frac{\Lambda(w - \lambda_c)}{w^2 - \Lambda T \lambda_c} \right\rfloor \right). 
\]

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” \(\Lambda T\) 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

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

Theorem 3

Theorem 5

Table 1: Known constructions of J-optimal families of AMOPPW codes.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Conditions</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$((q^n + 1) \times \theta(k, q), q^n, q - 1)$</td>
<td>$k \geq 1, n \geq 2$</td>
<td>Theorem 5.3</td>
</tr>
</tbody>
</table>

Definitions

Definition 1.2. An $(n, w, \lambda_a, \lambda_c)$-OOC (resp. $(A \times T, w, \lambda_a, \lambda_c)$-2D-OOC) $C$ is said to be extendable if there exists a binary sequence (resp. matrix) $w \notin C$ such that $C \cup \{w\}$ is an $(n, w, \lambda_a, \lambda_c)$-OOC (resp. $(A \times T, w, \lambda_a, \lambda_c)$-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 $(\Lambda \times \theta, \{w_1, w_2, \ldots, w_n\}, \lambda_a, \lambda_c)$ code we shall denote a 2D-OOC in which codewords are of weight $w_1, w_2, \ldots, w_n$. 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 code words of higher weight while those with lower requirement could be assigned words of lower weight. In the 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

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

(2.1)

Similar counting shows that the number of points of $PG(k, q)$ is given by $\theta(k, q) = \frac{k+1}{q-1} - 1$. 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 $t \leq k$. A $d$-flat $\Pi$ in $PG(k, q)$ is a subspace isomorphic to $PG(d, q)$; if $d = k - 1$, the subspace $\Pi$ 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 $\beta$ be a primitive element of $GF(q^k)$, the points of $\Sigma = PG(k, q)$ can be represented by the field elements $\beta^0, \beta^1, \beta^2, \ldots, \beta^{n-1}$ 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) $(a_0, a_1, \ldots, a_{n-1})$ where $a_i = 1$ if and only if $\beta^i \in A$.

Recall that the non-zero elements of $GF(q^k)$ form a cyclic group under multiplication. Moreover, it is not hard to show that multiplication by $\beta$ induces an automorphism, or collineation, on the associated projective space $PG(k, q)$. Denote by $\phi$ the collineation of $\Sigma$ defined by $\beta^i \mapsto \beta^{i+1}$. The map $\phi$ clearly acts sharply transitively on the points of $\Sigma$.

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 $\phi^\Lambda$).

**Definition 2.1** (Projective Incidence Matrix). Let $\Lambda, T$ 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 $A = (a_{i,j})$, $0 \leq i \leq \Lambda - 1$, $0 \leq j \leq T - 1$ where $a_{i,j} = 1$ if and only if the point corresponding to $\beta^i$ is in $S$.

If $A$ is a pointset of $\Sigma$ with corresponding $\Lambda \times T$ incidence matrix $W$ of weight $w$, then $\phi^\Lambda$ induces a cyclic shift on the columns of $W$. For any such set $A$, consider its orbit $\text{Orb}_H(A)$ under the group $H$ generated by $\phi^\Lambda$. The set $A$ has full $H$-orbit if $|\text{Orb}_H(A)| = T = \frac{n}{\Lambda}$ 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

$$\lambda_a = \max_{1 \leq i < j \leq T} \{|\phi^{\Lambda+1}(A) \cap \phi^{\Lambda+2}(A)|\}$$  \hspace{5cm} (2.2)

and

$$\lambda_c = \max_{1 \leq i < j \leq T} \{|\phi^{\Lambda+1}(A) \cap \phi^{\Lambda+2}(A')|\}$$  \hspace{5cm} (2.3)

ranging over all $A, A'$ with full $H$-orbit.

### 2.1 An affine analogue of the Singer automorphism

A further automorphism of $\Sigma = PG(k, q)$ shall play a role in our constructions. It may be viewed as an affine analogue of the Singer automorphism. If a hyperplane $\Pi_{\infty}$ (at infinity) is removed from $PG(k, q)$, what remains is $AG(k, q)$-the $k$-dimensional affine space. One way to model $AG(k, q)$ is to view the points as the elements of $GF(q^k)$. Recall that the set $GF(q^k)^*$ of non-zero elements of $GF(q^k)$ forms a cyclic group under multiplication. Take $\alpha$ to be a primitive element (generator) of $GF(q^k)^*$. Each nonzero affine point corresponds in the natural way to $\alpha^j$ for some $j$, $0 \leq j \leq q^k - 2$. Denote by $\psi$ the mapping of $AG(k, q)$ defined by $\psi(\alpha^j) = \alpha^{j+1}$ and $\psi(0) = 0$. The map $\psi$ is an automorphism of $AG(k, q)$ and, moreover, $\psi$ admits a natural extension to an automorphism $\hat{\psi}$ of $PG(k, q)$. 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 $PG(k, q)$.

2. $\hat{G}$ acts cyclically transitively on the points of $\Pi_\infty$, in particular the subgroup $H = \langle \theta(k-1,q) \rangle$ fixes $\Pi_\infty$ 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 $\Lambda, T$ be integers such that $q^k - 1 = \Lambda \cdot T$. For an arbitrary pointset $S$ in $AG(k, q)$ we define the $\Lambda \times T$ incidence matrix $A = (a_{i,j})$, $0 \leq i \leq \Lambda - 1$, $0 \leq j \leq T - 1$ where $a_{i,j} = 1$ if and only if the point corresponding to $a^{i + \Lambda j}$ 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 $\psi^A$ induces a cyclic shift on the columns of $W$. For any such set $A$, consider its orbit $\text{Orb}_{\hat{H}}(A)$ under the group $\hat{H} = \langle \psi^A \rangle$. 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 $(\Lambda \times T, w, \lambda_a, \lambda_c)$-2DOOC, where

$$\lambda_a = \max_{1 \leq i < j \leq T} \left\{ |\psi^A \cap \psi^A (A)| \right\}$$  (2.4)

and

$$\lambda_c = \max_{1 \leq i < j \leq T} \left\{ |\psi^A \cap \psi^A (A')| \right\}$$  (2.5)

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

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

### 3.1 Codes from projective lines

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

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

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

$$\frac{\binom{k+1}{2}}{q+1} - |S| = \frac{1}{q+1} \left[ \frac{(q^k+1 - 1)(q^k+1 - q)}{(q^2 - 1)(q^2 - q)} - \frac{\theta(k,q)}{q+1} \right] = \frac{q \cdot \theta(k,q) \cdot \theta(k-2,q)}{(q+1)^2}$$  (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 $(\frac{\theta(k,q)}{q+1} \times (q+1), q+1, \lambda_a, \lambda_c)$-2DOOC C. As two lines intersect in at most one point we have (Equation (2.3)) $\lambda_a = 1$. Moreover, since the lines in any particular full $H$-orbit $O_H(\ell)$ are disjoint, we have (Equation 2.2 $\lambda_a = 0$. Hence, C is a $(\frac{\theta(k,q)}{q+1} \times (q+1), q+1, 1)$-AMOPPW code. From the bound (Theorem 1.1) we have

$$\Phi \left( \frac{\theta(k,q)}{q+1} \times (q+1), q+1, 0, 1 \right) \leq \frac{\theta(k,q)}{q+1} \left. \frac{(q+1)(\theta(k,q) - 1)}{q} \right|$$  (3.2)
Comparing (3.1) and (3.2) we see that $C$ is in fact optimal. Noting that $\frac{\theta(k,q)}{q+1} = \theta(\frac{k-1}{2}, q^2)$, we have shown the following.

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

### 3.2 Codes from affine lines

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

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

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

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

(3.3)

For each full $\hat{H}$-orbit, select a representative line $\ell$ 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 $\ell$ used in the construction meets $\Pi_{\infty}$ 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 $P_{\infty}$ is fixed under the action of $H$, the orbit $O_H(\ell)$ is comprised of $|H| = q-1$ lines, each incident with $P_{\infty}$ (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

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

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, 2, 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 $PG(2,q)$ is a collection of $m > 2$ points that meets no line in as many as 3 points. A line $\ell$ is said to be external, tangent, or secant to an arc $K$ in the case that it is incident with precisely 0, 1, or 2 points of $K$ respectively. An $m$-arc is complete if it is not contained in an $(m+1)$-arc. 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 B. 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.
If \( C \) is a conic in \( PG(2, q) \), then the subgroup of \( PGL(3, q) \) leaving \( C \) fixed is (isomorphic to) \( PGL(2, q) \) (see [7] Theorem 27.5.3). It follows that the number of distinct conics in \( PG(2, q) \) is given by

\[
\frac{|PGL(3, q)|}{|PGL(2, q)|} = \frac{(q^3 - 1)(q^3 - q)(q^3 - q^2)}{(q^2 - 1)(q^2 - q)} = q^5 - q^2
\] (4.1)

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

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

A collection \( \mathcal{F} \) of \( m \)-arcs in \( \pi = PG(2, q) \) is said to be a \( t \)-family if every pair of distinct members of \( \mathcal{F} \) meet in at most \( t \) points. Hence, from (4.1) the collection of all conics in \( \pi \) 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 \( \pi = PG(2, q) \) there exists a 2-family, \( \mathcal{F} \), of conics in \( \pi \) such that:

1. \( |\mathcal{F}| = q^3 - q^2 \).
2. There exists a particular line \( \ell \), 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 \( \Sigma = PG(3, q) \) and let \( G = \langle \phi \rangle \) be the associated Singer group. Consider the action of \( G \) on the lines of \( \Sigma \) and let \( \mathcal{S} \) be the spread of \( \Sigma \) determined by \( G \) as in Theorem 3.1. In particular, the subgroup \( H = \langle \phi^{q^2+1} \rangle \) 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 \( \pi_i \) be any plane containing \( \ell_i \). Since the \( \ell_i \)'s are mutually skew, it follows that the \( \pi_i \)'s are distinct. On each \( \pi_i \), let \( \mathcal{F}_i \) be a 2-family of conics (as in Theorem 4.2), each having \( \ell_i \) 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 Equation 3.1, there are precisely \( q(q^2 + 1) \) codewords of type \( B \).

Let \( \mathcal{C} \) be the collection of all projective \((q^2+1) \times (q + 1)\) incidence matrices (codewords) of type \( A \) or \( B \). That \( \mathcal{C} \) has constant weight \( q + 1 \) is clear, so \( \mathcal{C} \) 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 \( C_1 \) and \( C_2 \). Let \( \pi_a \) and \( \pi_b \) be the planes of \( \Sigma \) containing \( C_1 \) and \( C_2 \) respectively. If \( \pi_a = \pi_b \), then \( C_1 \) and \( C_2 \) are members of a common 2-family and therefore share at most 2 points. Otherwise \( \pi_a \) and \( \pi_b \) meet in a line; in which case (since a line meets a conic in at most two points) \( |C_1 \cap C_2| \leq 2 \). 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 $(q^2 + 1 \times q + 1, q + 1, 2)$-AMOPPW code, $C$ with $|C| = (q^2 + 1)(q^3 - q^2 + q)$.

4.1.1 Optimaly

From the bound (Theorem 1.1) we have

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

**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 $\Sigma$. To maintain the cross-correlation of 2, $S$ must meet each line of $\Sigma$ 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 $\pi$ with our set $S$. Clearly, $\pi$ contains some spread line, $\ell$. 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 $\pi$ in at most 3 points. In particular, if $S$ meets $\pi$ in three points, then the points necessarily form a triangle, with precisely one point incident with $\ell$. Thus, by counting co-planar pairs $(\tau, \ell)$, where $\tau$ is a triangle (of points) in $S$ and $\ell$ is a spread line we obtain

\[
\frac{q + 1}{3} \leq (q + 1) \left\lfloor \frac{q}{2} \right\rfloor
\]

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

4.2 A generalization to higher dimensions

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

We first note that every plane $\pi$ will have full orbit under $H$. Indeed, if $\pi$ contains a line of $S$ then $Stab_H(\pi)$ is an automorphism of $\pi$ fixing a line of $\pi$, and dually, must fix a point. Since $G$ acts sharply transitively on the points of $\Sigma$, $\pi$ must have a trivial stabilizer. If $\pi$ contains no line of $S$ then $\pi$ is incident with precisely $\theta(2, q)$ members of $S$. For each $\ell \in S$, $H$ acts sharply transitively on the points of $\ell$. Consequently, the orbit $Orb_H(\pi)$ 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, $\gamma$, and a 2-family $F$ conics on $\gamma$ composed of $q^3 - q^2$ members. Note that if $\gamma$ contains a line $\ell$ of $S$ then (as in the three dimensional case) $F$ is chosen in such a way that $\ell$ is external to each member of $F$. 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 $(\theta \left(\frac{k-1}{2}, q^2\right) \times (q + 1), q + 1, 2)$-AMOPPW code, $C$ (Note: $\frac{\theta(k, q)}{q+1} = \theta \left(\frac{k-1}{2}, q^2\right)$). With reference to equations 2.1 and 3.1 we have

\[
|C| = \frac{1}{q + 1} \left[\frac{k + 1}{3}\right] q^3 - q^2 + \frac{q \cdot \theta(k, q) \cdot \theta(k - 2, q)}{(q + 1)^2} \approx q^{3k-4}. \tag{4.2}
\]

From the bound (Theorem 1.1) we have

\[
\Phi(C) \leq \left[\frac{\theta \left(\frac{k-1}{2}, q^2\right)}{q + 1}\right] \left(\frac{q + 1)(\theta \left(\frac{k-1}{2}, q^2\right) - 1)}{q} \left(\frac{q + 1)(\theta \left(\frac{k-1}{2}, q^2\right) - 2)}{q - 1}\right)^{(q + 1)(\theta \left(\frac{k-1}{2}, q^2\right) - 2)} \right]
\]

\[
\approx q^{3k-4}.
\]
Consequently, we have:

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

## 5 Codes with $\lambda_c \geq 1$

Here we shall provide a construction for $((q^2 + 1) \times (q + 1), q^2, q - 1)$-AMOPPW codes. Let $\Sigma = PG(3, q)$ with Singer group $\langle \phi \rangle$. By Theorem 3.1, there exists a short $G$-orbit of lines, $S = \{\ell_1, \ell_2, \ldots, \ell_{q^2 + 1}\}$. 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 $\ell$ of $\Sigma$ is contained in precisely $q + 1$ planes, forming the fan of planes on $\ell$. For each $i = 1, 2, \ldots, q^2 + 1$, let $P_i$ be the fan of planes on $\ell_i$. Each plane of $\Sigma$ is of full $H$-orbit. It follows that $H$ acts sharply transitively on the members of $P_i$ for each $i = 1, 2, \ldots, q^2 + 1$.

Let $P_i \in P_i$ and let $P_i^* = P_i \setminus \{\ell_i\}, i = 1, 2, \ldots, q^2 + 1$. The collection of incidence matrices corresponding to the $P_i^*$’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 $P_i^*$ 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 points sets $P_i^*$ and $P_i^*$ respectively. A dimension argument shows $P_i$ and $P_i$ meet precisely in a line, say $P_1 \cap P_2 = \ell$. Since $\ell$ is incident with both $\ell_1$ and $\ell_2$ it follows that $|P_i^* \cap P_i^*| = q - 1$. A similar argument shows $|\sigma^t (P_i^*) \cap \sigma^t (P_i^*)| = q - 1$ for any $s, t$. From the equation (2.3) we have $\lambda_c = q - 1$. We have shown the following.

**Theorem 5.1.** For $q$ a prime power, there exists a $((q^2 + 1) \times (q + 1), q^2, q - 1)$-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

$$\Phi(\Lambda \times T, w, 0, \lambda_c) \leq \min \left( \Lambda, \left\lfloor \frac{\Lambda(w - \lambda_c)}{w^2 - \Lambda T \lambda_c} \right\rfloor \right)$$

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

$$= q^2 + 1$$

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 $\Sigma = PG(2n + 1, q)$, $n \geq 1$. Let $G$ be the Singer group of $\Sigma$, $H = \langle \sigma \rangle$ be the unique subgroup of $G$ having order $\theta(n, q)$. Let $\Pi = \Pi_1, \Pi_2, \ldots, \Pi_{q^{n+1} + 1}$ be the $n$-spread of $\Sigma$ fixed by $H$ as in the Theorem 3.1. For each $i = 1, 2, \ldots, q^{n+1} + 1$, let $P_i$ be the fan of $(n + 1)$-flats on $\Pi_i$, let $\Omega_i$ be a representative member of $P_i$, and let $\Omega_i^* = \Omega_i \setminus \Pi_i$. Note that $H$ acts sharply transitively on the members of $P_i$ for each $i$.

The collection of incidence matrices corresponding to the $\Omega_i$’s shall comprise a $(q^{n+1} + 1) \times \theta(n, q), q^{n+1}, q - 1)$-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 $\Omega_i^*$. 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
\(\Omega_1\) is of full \(H\) orbit. Observe that if \(|\Omega_1 \cap \Pi_j| > 1\) then \(\Omega_1\) and \(\Pi_j\) share (at least) a line. Every line in \(\Omega_1\) intersects \(\Pi_1\) nontrivially, so

\[|\Omega_1 \cap \Pi_j| > 1 \quad \text{To } \Pi_1 \cap \Pi_j \neq \emptyset \quad \text{To } \Pi_1 = \Pi_j.\]

By the Pigeonhole Principle it follows that if \(1 \neq j\) then \(\Omega_1\) meets \(\Pi_j\) precisely in a point. That \(\Omega_1\) has full \(H\)-orbit then follows from the fact that \(H\) acts sharply transitively on the points of each \(\Pi_j\) (Theorem 3.1).

To show that \(\lambda_c = q - 1\), let \(w_1\) and \(w_2\) be codewords corresponding to \(\Omega_1^1\) and \(\Omega_1^2\) respectively. A dimension argument shows that \(\Omega_1\) and \(\Omega_2\) meet in at least a line. Moreover, since \(\Pi_1\) and \(\Pi_2\) are disjoint, it follows that \(\Omega_1\) and \(\Omega_2\) meet in at most a line. So \(\Omega_1 \cap \Omega_2 = \ell\) for some line \(\ell\). Since \(\ell\) must be incident with both \(\Pi_1\) and \(\Pi_2\) it follows that \(|\Omega_1^1 \cap \Omega_1^2| = q - 1\). A similar argument shows that for any \(i, j\), \(|\sigma^i(\Omega_1)\) and \(\sigma^j(\Omega_2)| = q - 1\). From the equation (2.3) we have \(\lambda_c = q - 1\). We have shown the following.

**Theorem 5.3.** For \(q\) a prime power, there exists a \(((q^{n+1} + 1) \times \theta(n, q), q^{n+1}, q - 1)\)-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

\[\Phi(\Lambda \times T, w, 0, \lambda_c) \leq \min\left(\Lambda, \frac{|\Lambda(w - \lambda_c)|}{w^2 - \Lambda T \lambda_c}\right) = q^{n+1} + 1\]

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 \(\ell_\infty\) be a line of \(\Pi = PG(2, q)\) 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 \(\bar{G} = \langle \Psi \rangle\) be the affine analogue of the Singer map. Let \(\hat{H} = \langle \sigma \rangle\) be the unique subgroup of \(\bar{G}\) having order \(q - 1\).

Consider the collection of all conics passing through the point \(P_0\). By counting ordered pairs \((P, \Gamma)\) where \(P\) is a point of \(\Pi\) and \(\Gamma\) is a conic containing \(P\), we see that there are \(q^3 - q^2\) such conics. For each conic in the collection, remove the point \(P_0\), and remove any infinite points (points on \(\ell_\infty\)). We are left with a collection \(C\) 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 \(C\) meet in at most three points.

We claim that each member of \(C\) is of full \(\hat{H}\) orbit. Clearly, \(\hat{H}\) fixes \(P_0\), and fixes \(\ell_\infty\) point-wise. So, given a line \(\ell\) incident with \(P_0\), \(\hat{H}\) fixes both \(P_0\) and the infinite point \(\ell \cap \ell_\infty\) of \(\ell\), and acts sharply transitively on the \(q - 1\) non-zero affine points of \(\ell\). 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 \(C\) has this property it follows that all members of \(C\) 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.

<table>
<thead>
<tr>
<th>Word Weight</th>
<th>Number of codewords</th>
</tr>
</thead>
<tbody>
<tr>
<td>( q )</td>
<td>( \frac{q^3 + q + 2}{2} )</td>
</tr>
<tr>
<td>( q - 1 )</td>
<td>( q^2 + q )</td>
</tr>
<tr>
<td>( q - 2 )</td>
<td>( \frac{q^3 - q}{2} )</td>
</tr>
</tbody>
</table>

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 \( \Pi^* \). 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 \( \Pi, P_0, \ell_\infty, G, \) and \( \hat{H} \), be as defined above. Let \( P_1 \) be a point of \( \ell_\infty \) and consider the collection of all conics containing both \( P_0 \) and \( P_1 \). By counting ordered triples \( (P, Q, \Gamma) \) where \( P \) and \( Q \) are points and \( \Gamma \) 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 \( \ell \) 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 \( \ell \) 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.
<table>
<thead>
<tr>
<th>Word Weight</th>
<th>Number of codewords</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q + 1$</td>
<td>1</td>
</tr>
<tr>
<td>$q$</td>
<td>$q$</td>
</tr>
<tr>
<td>$q - 1$</td>
<td>$q$</td>
</tr>
<tr>
<td>$q - 2$</td>
<td>$q^2 - q$</td>
</tr>
</tbody>
</table>

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 $\pi^*$ 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 $q > 7$, each of the codes is maximal.

**Theorem 6.4.** The family of codes constructed in Theorem 6.3 is asymptotically optimal. For $q > 6$, each code in the family is maximal.

### References


