On cutting blocking sets and their codes

Daniele Bartoli  Antonio Cossidente  Giuseppe Marino  Francesco Pavese

Abstract

Let \( PG(r, q) \) be the \( r \)-dimensional projective space over the finite field \( GF(q) \). A set \( \mathcal{X} \) of points of \( PG(r, q) \) is a cutting blocking set if for each hyperplane \( \Pi \) of \( PG(r, q) \) the set \( \Pi \cap \mathcal{X} \) spans \( \Pi \). Cutting blocking sets give rise to saturating sets and minimal linear codes and those having size as small as possible are of particular interest. We observe that from a cutting blocking set obtained in [20], by using a set of pairwise disjoint lines, there arises a minimal linear code whose length grows linearly with respect to its dimension. We also provide two distinct constructions: a cutting blocking set of \( PG(3, q^3) \) of size \( 3(q+1)(q^2+1) \) as a union of three pairwise disjoint \( q \)-order subgeometries and a cutting blocking set of \( PG(5, q) \) of size \( 7(q+1) \) from seven lines of a Desarguesian line spread of \( PG(5, q) \). In both cases the cutting blocking sets obtained are smaller than the known ones. As a byproduct we further improve on the upper bound of the smallest size of certain saturating sets and on the minimum length of a minimal \( q \)-ary linear code having dimension 4 and 6.

Keywords: Cutting blocking sets, minimal codes, saturating sets, covering codes.

1 Introduction

Let \( q = p^h \), where \( p \) is a prime and \( h \) is a positive integer. Let \( PG(r, q) \) be the \( r \)-dimensional projective space over the finite field \( GF(q) \). We will denote by \( (X_1, X_2, \ldots, X_{r+1}) \) the homogeneous projective coordinates of a point of \( PG(r, q) \). A set \( \mathcal{X} \) of points of \( PG(r, q) \) is said to be a \( t \)-fold blocking set if every hyperplane \( \Pi \) of \( PG(r, q) \) meets \( \mathcal{X} \) in at least \( t \) points.

Definition 1.1. A set of points \( \mathcal{X} \subset PG(r, q) \) is a cutting blocking set, if for each hyperplane \( \Pi \) of \( PG(r, q) \), the set \( \Pi \cap \mathcal{X} \) spans \( \Pi \), i.e., \( \Pi \cap \mathcal{X} \) is not contained in any hyperplane of \( \Pi \).

A cutting blocking set is said to be minimal if it is minimal with respect to set theoretical inclusion. If \( \mathcal{X} \) is a cutting blocking set, then any hyperplane \( \Pi \) of \( PG(r, q) \) is spanned by \( \Pi \cap \mathcal{X} \).
and hence $|\Pi \cap \mathcal{X}| \geq r$ and $\mathcal{X}$ is an $r$--fold blocking set. The term cutting blocking set has been coined recently in [9], see also [11, Proposition 3.3], but such a substructure has been investigated earlier by several authors. In [13] a cutting blocking set is referred to as an $r$--fold strong blocking set, whereas in [20] a cutting blocking set is called a generator set. In [13], some pointsets of $\text{PG}(r,q)$, called $\rho$--saturating sets, were studied.

**Definition 1.2.** A set $Y$ of points of $\text{PG}(r,q)$ is said to be $\rho$--saturating if for any point $P \in \text{PG}(r,q)$ there exist $\rho+1$ points of $Y$ spanning a subspace of $\text{PG}(r,q)$ containing $P$, and $\rho$ is the smallest value with such property.

In particular the authors pointed out that, by embedding $\text{PG}(r,q)$ in $\text{PG}(r,q^r)$, a cutting blocking set of $\text{PG}(r,q)$ is an $(r-1)$--saturating set of $\text{PG}(r,q^r)$ [13, Theorem 3.2]. In this context, saturating sets of the smallest size are interesting as extremal objects and $s_q(r,\rho)$ denotes the smallest size of a $\rho$--saturating set of $\text{PG}(r,q)$. For more recent results on $\rho$--saturating sets of $\text{PG}(r,q)$ the reader is referred to [14, 16]. In [20] the authors, by investigating an idea introduced in [23], studied lines of $\text{PG}(r,q)$ that are said to be higgledy--piggledy arrangement.

**Definition 1.3.** Let $L$ be a lineset of $\text{PG}(r,q)$. The lines of $L$ are said to be in higgledy--piggledy arrangement if the set of points covered by the lines of $L$ forms a cutting blocking set.

Of particular interest is to look for the smallest size that a set consisting of lines in hyggledy--piggledy arrangement may have. It is not difficult to show that in $\text{PG}(2,q)$ this number is three and it is known that in $\text{PG}(3,q)$ the smallest set of lines in higgledy--piggledy arrangement has to contain four (pairwise disjoint) lines; see [20]. In $\text{PG}(4,q)$, if $q$ is large enough, it is possible to find a set of six pairwise disjoint lines in higgledy--piggledy arrangement [3, Proposition 12]. More generally, it is known that a set of lines of $\text{PG}(r,q)$ in higgledy--piggledy arrangement has to contain at least $\lceil \frac{r}{2} \rceil + r$ lines, if $q \geq \lfloor \frac{r}{2} \rfloor + r$, and that there is a set of $2r - 1$ pairwise disjoint lines with the required property whenever $q > 2r - 1$; see [20, Theorem 14, Theorem 20, Theorem 24]. It follows that if $q > 2r - 1$, there exists a cutting blocking set in $\text{PG}(r,q)$ of size at most $(2r - 1)(q + 1)$. Thus

$$\frac{r}{e}q + \frac{r - 1}{2} \leq s_q(r, r - 1) \leq (2r - 1)(q + 1),$$

which improves on the known upper bounds for the size of the smallest saturating set. In the previous formula the lower bound arises from [16, Lemma 4.0.1] and $e$ is the Euler's number.

Here we deal with cutting blocking sets. The main achievements of this paper are summarized in the following theorem.

**Main Theorem.** (i) In $\text{PG}(3,q^3)$ there exists a minimal cutting blocking set of size $3(q + 1)(q^2 + 1)$.

(ii) In $\text{PG}(5,q)$ there exists a minimal cutting blocking set of size $7(q + 1)$.

The paper is organized as follows. In Section 2 we construct a minimal cutting blocking set of $\text{PG}(3,q^3)$ of size $3(q + 1)(q^2 + 1)$ obtained by glueing together three suitable pairwise disjoint
$q$–order subgeometries. In Section 3 we show that there is a set of seven lines of $\text{PG}(5, q)$ in higgledy-piggledy arrangement. There arises a minimal cutting blocking set of $\text{PG}(5, q)$ of size $7(q + 1)$. As a byproduct we obtain the following improvements on the upper bound of the smallest size of a 2–saturating set of $\text{PG}(3, q^9)$ and of a 4–saturating set of $\text{PG}(5, q^5)$:

$$\frac{3}{e} q^3 + 1 \leq s_{q^d}(3, 2) \leq 3(q + 1)(q^2 + 1),$$

$$\frac{5}{e} q + 2 \leq s_{q^d}(5, 4) \leq 7(q + 1).$$

### 1.1 Minimal and covering linear codes

The concepts of cutting blocking set and saturating set are of interest not only from a geometrical point of view, but they also have applications in coding theory. For a vector $u = (u_1, \ldots, u_n) \in \text{GF}(q^n)$, its support is the set $\text{supp}(u) = \{ i \mid u_i \neq 0 \}$ and the Hamming weight $w(u)$ of $u$ is the cardinality of its support. The Hamming distance on $\text{GF}(q^n)$ is defined as $d(u, v) = |\text{supp}(u - v)|$, for every pair of vectors $u, v \in \text{GF}(q)$. A $q$–ary linear code of dimension $k$ and length $n$, or an $[n, k]_q$ code, $C$ is a $k$–dimensional vector subspace of $\text{GF}(q)^n$. The elements of $C$ are called codewords. A generator matrix of $C$ is a matrix whose rows form a basis of $C$ as a vector space over $\text{GF}(q)$. The minimum distance of $C$ is $d = \min\{w(u) \mid u \in C, u \neq 0\}$. Let $u, v \in \text{GF}(q)^n$. The vector $u$ is $\rho$–covered by $v$ if $d(u, v) \leq \rho$. The covering radius of a code $C$ is the smallest integer $\rho$ such that every vector of $\text{GF}(q^n)$ if $\rho$–covered by at least one codeword of $C$. If $d$ or $\rho$ are needed, then $C$ is said to be an $[n, k, d]_q$ code or an $[n, k]_q \rho$ code. The weight distribution of $C$ is the sequence $A_0(C), \ldots, A_n(C)$, where $A_i(C) = |\{u \in C \mid w(u) = i\}|$. For $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \text{GF}(q)^n$, let $u \cdot v = \sum_{i=1}^{n} u_i v_i$ be the Euclidean inner product between $u$ and $v$. For a code $C$, its dual code is $C^\perp = \{v \in \text{GF}(q)^n \mid v \cdot c = 0, \forall c \in C\}$. The dimension of the dual code $C^\perp$ or the codimension of $C$ is $n - k$. Any matrix which is a generator matrix of $C^\perp$ is called a parity check matrix of $C$. If $C$ is a linear $[n, k]_q \rho$ code, with parity check matrix $N$, its covering radius is the smallest $\rho$ such that every $v \in \text{GF}(q)^{n-k}$ can be written as a linear combination of at most $\rho$ columns of $N$. For an introduction to coverings of vector spaces over finite fields and to the concept of code covering radius, see [12].

The representatives of the points of a saturating set of $\text{PG}(r, q)$ can be considered as columns of a parity check matrix of a $q$–ary linear code of codimension $r + 1$. In particular, a $\rho$–saturating set of $\text{PG}(r, q)$ of size $n$ corresponds to a parity check matrix of an $[n, n - (r + 1)]_q (\rho + 1)$ code; see [13] and references therein.

Let $C$ be an $[n, k]_q$ linear code with generator matrix $M$. The code $C$ is called non–degenerate if there is no $i$, with $1 \leq i \leq n$, such that $u_i = 0$, for all $u \in C$. A non–zero codeword $u \in C$ is called minimal if every codeword $u' \in C$, with $\text{supp}(u') \subseteq \text{supp}(u)$ is a multiple of $u$ and $C$ is minimal if all its codewords are minimal. A minimal code $C$ is called reduced if for every $i$, with $1 \leq i \leq n$, the code obtained by deleting the same $i$–th coordinate in each codeword is not minimal.

A projective $[n, r + 1, d]_q$ system $Z$ is a set of $n$ points (counted with multiplicity) of $\text{PG}(r, q)$.
that do not all lie on a hyperplane and such that

\[ d = n - \max\{|H \cap Z| : H \text{ hyperplane of } \text{PG}(r, q)\}. \]

There is a well–known correspondence between non–degenerate \([n, r + 1, d]_q\) linear codes and projective \([n, r + 1, d]_q\) systems. Indeed, the points of \(\text{PG}(r, q)\) represented by the columns of a generator matrix \(M\) of an \([n, r + 1, d]_q\) code form a set of \(n\) points (counted with multiplicity) of \(\text{PG}(r, q)\). Viceversa, the code generated by the matrix having the representatives of the points of a projective \([n, r + 1, d]_q\) system \(Z\) as columns, gives an \([n, r + 1, d]_q\) linear code. Moreover, for any non–zero vector \(u = (u_1, u_2, \ldots, u_{r+1}) \in \text{GF}(q)^{r+1}\), the hyperplane of \(\text{PG}(r, q)\) with equation \(u_1X_1 + u_2X_2 + \cdots + u_{r+1}X_{r+1} = 0\) contains \(|Z| - w\) points of \(Z\) if and only if the codeword \(uM\) has weight \(w\). For more details the reader is referred to [33].

In this setting it has been established a correspondence between \([n, r + 1, d]_q\) minimal linear codes and projective \([n, r + 1, d]_q\) systems that are cutting blocking sets. Furthermore reduced minimal \([n, r + 1, d]_q\) linear codes are equivalent to minimal cutting blocking sets of \(\text{PG}(r, q)\) of size \(n\); see [11, Theorem 3.4] and [32, Theorem 14].

In the context of minimal codes, one of the main issue is to provide explicit constructions of families of minimal codes of short length for a given dimension and in particular to construct minimal codes whose length grows linearly with respect to their dimension; see [11, Problem 2], [2], and [32, Open Problem 24]. In this regard, if \(m(r + 1, q)\) denotes the minimum length of a minimal \(q\)–ary linear code having dimension \(r + 1\), from the construction of \(2r - 1\) pairwise disjoint lines of \(\text{PG}(r, q)\), \(q > 2r - 1\), in hyggledy–piggledy arrangement provided in [20], the following upper bound can be derived:

\[ r(q + 1) \leq m(r + 1, q) \leq (2r - 1)(q + 1). \]

The lower bound in the previous formula follows from [2, Theorem 2.14]. Moreover, from the constructions of cutting blocking sets presented here, we obtain the following improvements:

\[ 3(q^3 + 1) \leq m(4, q^3) \leq 3(q + 1)(q^2 + 1), \quad \text{see Theorem 2.26} \]
\[ 5(q + 1) \leq m(6, q) \leq 7(q + 1), \quad \text{see Proposition 3.16} \]

### 2 Cutting blocking sets from subgeometries

In this section we construct a cutting blocking set of \(\text{PG}(3, q^3)\) of size \(3(q + 1)(q^2 + 1)\) obtained by gluing together three suitable pairwise disjoint \(q\)–order subgeometries.

#### 2.1 Clubs and Splashes of \(\text{PG}(1, q^3)\)

Here we consider certain pointsets of \(\text{PG}(1, q^3)\), called clubs and splashes. These sets have been investigated by several authors [5, 6, 7, 8, 18, 21, 28, 30, 31]. Before recalling their definitions and summarizing some of their properties, we mention the following well known results.

**Lemma 2.1** ([15]). In \(\text{PG}(2, q^3)\), let \(\pi_0\) be a \(q\)–order subplane and let \(H\) be the stabilizer of \(\pi_0\) in \(\text{PGL}(3, q^3)\). The group \(H\) has three orbits on the points of \(\text{PG}(2, q^3)\):
• $\pi_0$;

• $\mathcal{O}_2'$ consisting of the $q(q^2 - 1)(q^2 + q + 1)$ points of $\text{PG}(2, q^3)$ lying on exactly one extended subline of $\pi_0$;

• their complement $\mathcal{O}_3'$ of size $q^3(q - 1)(q^2 - 1)$.

The group $H$ has three orbits on the lines of $\text{PG}(2, q^3)$:

• the $q^2 + q + 1$ extended sublines of $\pi_0$;

• $\mathcal{L}_2'$ consisting of the $q(q^2 - 1)(q^2 + q + 1)$ lines of $\text{PG}(2, q^3)$ intersecting $\pi_0$ in one point;

• their complement $\mathcal{L}_3'$ of size $q^3(q - 1)(q^2 - 1)$ formed by lines disjoint from $\pi_0$.

Let $\ell_1 \in \mathcal{L}_2'$, $\ell_2 \in \mathcal{L}_3'$. Let $R_1$ be a point of $\mathcal{O}_2'$, where $r$ is the unique extended subline of $\pi_0$ containing $R_1$, and let $R_2$ be a point of $\mathcal{O}_3'$. In geometric terms, a club of $\text{PG}(1, q^3)$ can be defined in two distinct ways.

i) By extension. By extending the sublines of $\pi_0$ to lines of $\text{PG}(2, q^3)$ and intersecting these with the line $\ell_1$, one obtains a club of $\ell_1$ with head $\ell_1 \cap \pi_0$.

ii) By projection. By projecting the points of $\pi_0$ from $R_1$ onto a line $m$ not containing $R_1$, one obtains a club of $m$ with head $m \cap r$.

A club has the following properties.

• All clubs of $\text{PG}(1, q^3)$ are projectively equivalent.

• A club of $\text{PG}(1, q^3)$ contains $q(q + 1)$ $q$–order sublines.

• Through two non–head points there passes exactly one $q$–order subline and it contains the head point. Two distinct $q$–order sublines of a club have at most a point in common distinct from the head point.

• Let $\mathcal{C}$ be a club with head point $T$. The unique $q$–order subline determined by two non–head points and $T$ is contained in $\mathcal{C}$.

• A $q$–order subline of a club arises either from the sublines of $\pi_0$ through a point of $\pi_0$ or from a subline of $\pi_0$ according as the club is obtained by extension or by projection, respectively.

Similarly, it is possible to define geometrically a splash of $\text{PG}(1, q^3)$ in two equivalent ways.

i) By extension. By extending the sublines of $\pi_0$ to lines of $\text{PG}(2, q^3)$ and intersecting these with the line $\ell_2$, one obtains a splash of $\ell_2$.

ii) By projection. By projecting the points of $\pi_0$ from $R_2$ onto a line $m$ not containing $R_2$, one obtains a splash of $m$.  

5
A splash has the following properties.

- All splashes of $\text{PG}(1, q^3)$ are projectively equivalent.

- A splash of $\text{PG}(1, q^3)$ contains $2(q^2 + q + 1)$ $q$-order sublines divided into two equally sized families, say $\mathcal{F}_1$ and $\mathcal{F}_2$.

- A $q$-order subline of a family arises either from the extended sublines of $\pi_0$ through a point of $\pi_0$ or from a subline of $\pi_0$ according as the splash is obtained by extension or by projection, respectively. A $q$-order subline of the opposite family arises either from the extended sublines of $\pi_0$ of a dual subconic of $\pi_0$ or from a subconic of $\pi_0$ according as the splash is obtained by extension or by projection, respectively.

- Two distinct sublines of the same family meet in one point, whereas sublines of different families have in common 0, 1 or 2 points. Through two points there is exactly one $q$-order subline of each family.

- Let $s$ be a fixed $q$-order subline of $\mathcal{F}_1$. Among the $q$-order sublines of $\mathcal{F}_2$ there are $q + 1$ meeting $s$ in one point, $q(q + 1)/2$ meeting $s$ in two points, and $q(q - 1)/2$ disjoint from $s$.

- The stabilizer of a splash in $\text{PGL}(2, q^3)$ is a group of order $2(q^2 + q + 1)$ and it acts transitively on its $2(q^2 + q + 1)$ $q$-order sublines.

In the remaining part of this subsection we prove further properties regarding splashes of $\text{PG}(1, q^3)$ that will be used in the paper.

Let $r_1$ be the canonical $q$-order subline of $\text{PG}(1, q^3)$ and let $K = \text{PGL}(2, q)$ be the stabilizer of $r_1$ in $\text{PGL}(2, q^3)$. Let $x \in \text{GF}(q^3) \setminus \text{GF}(q)$ and let

$$\mathcal{S}_x = \{(z - z^q, xz^q - x^qz) \mid z \in \text{GF}(q^3) \setminus \{0\}\} = \{(t^q - t, xt - x^qt^q) \mid t \in \text{GF}(q^3) \setminus \{0\}\}.$$

Since the projectivity of $\text{PGL}(2, q^3)$ induced by

$$\begin{pmatrix} x & 1 \\ x^q & 1 \end{pmatrix}$$

maps $\mathcal{S}_x$ to the splash $\{(z, z^q) \mid z \in \text{GF}(q^3) \setminus \{0\}\}$, we have that $\mathcal{S}_x$ is a splash of $\text{PG}(1, q^3)$. The stabilizer of $\mathcal{S}_x$ in $\text{PGL}(2, q^3)$ is generated by

$$\left\{ \begin{pmatrix} \xi x - \xi x^q \\ -x^q(\xi - \xi^q) \\ \xi^q x - \xi^q x^q \end{pmatrix} \mid \xi \in \text{GF}(q^3) \setminus \{0\} \right\} \text{ and } \begin{pmatrix} -1 \\ x + x^q \\ 1 \end{pmatrix}. $$

If $z \in \text{GF}(q)$ or $z = x + a$, where $a \in \text{GF}(q)$, then $(z - z^q, xz^q - x^qz)$ is a point of $r_1$. Hence $r_1$ is a $q$-order subline of $\mathcal{S}_x$. Let $\mathcal{F}_1$ denote the family of $q$-order sublines of $\mathcal{S}_x$ containing $r_1$ and let $\mathcal{F}_2$ be the opposite family. Thus

$$\mathcal{F}_1 = \{r_\xi : \xi \in \text{GF}(q^3) \setminus \{0\}\}, \quad \mathcal{F}_2 = \{r'_\xi : \xi \in \text{GF}(q^3) \setminus \{0\}\},$$

where

$$r_\xi = \{((\xi(x + a) - \xi^q(x^q + a), x\xi(x^q + a) - x^q\xi(x + a)) \mid a \in \text{GF}(q)\} \cup \{(\xi - \xi^q, x\xi^q - x^q\xi)\},$$

$$r'_\xi = \{((\xi^q(x^q + a) - \xi(x + a), x\xi(x + a) - x^q\xi(x^q + a)) \mid a \in \text{GF}(q)\} \cup \{(\xi^q - \xi, x\xi - x^q\xi)\}.$$
Lemma 2.2. Let $r'_\xi$ be a $q$-order subline of $\mathcal{F}_2$ such that $|r'_\xi \cap r_1| = i$, $0 \leq i \leq 2$. Then there is a subgroup of $K$ if order $q + 1 - i$ fixing $r'_\xi$.

Proof. Let $r'_\xi \in \mathcal{F}_2$ such that $|r'_\xi \cap r_1| = 1$.

- If $r'_\xi \cap r_1 = \{(0, 1)\}$, then $\xi \in \text{GF}(q)$ and $r'_\xi = r'_1$, where

  $$r'_1 = \{R_a = (1, -a - x - x^q) \mid a \in \text{GF}(q)\} \cup \{R = (0, 1)\}.$$  

Consider the subgroup $\{\gamma_c : c \in \text{GF}(q)\}$ of $K$ of order $q$ fixing $R$, where $\gamma_c$ is induced by the matrix

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix},$$

for some $c \in \text{GF}(q)$. Then $\gamma_c(R_a) = R_{a - c}$ and $\gamma_c$ fixes $r'_1$.

- If $r'_\xi \cap r_1 = \{(1, b)\}$, for a fixed $b \in \text{GF}(q)$, then $\xi = \frac{1}{x + b}$ and

  $$r'_\xi = r'_{(x+b)^{-2}} = \{R_a \mid a \in \text{GF}(q)\} \cup \{R = (x + x^q + 2b, b^2 - x^{q+1})\},$$

where

$$R_a = (x^{q+1} + a(x + x^q) + 2ab - b^2, (2b - a)x^{q+1} + b^2(x + x^q) + ab^2).$$

Consider the subgroup $\{\gamma_c : c \in \text{GF}(q)\}$ of $K$ of order $q$ fixing $R_b$, where $\gamma_c$ is induced by the matrix

$$\begin{pmatrix} 1 - bc & c \\ -b^2c & 1 + bc \end{pmatrix},$$

for some $c \in \text{GF}(q)$. Let $\gamma_c \neq id$, i.e., $c \neq 0$. Then $\gamma_c(R) = R_{bc^{-1}}$ and, for $a \neq b$, we have that $\gamma_c(R_a)$ equals $R$ or $R_{a-bc(a-b)}^{-1}$, according as $c = (a - b)^{-1}$ or $c \neq (a - b)^{-1}$. Hence $\gamma_c$ fixes $r'_{(x+b)^{-2}}$.

Suppose that $r'_\xi$ is such that $|r'_\xi \cap r_1| = 2$.

- If $r'_\xi \cap r_1 = \{(0, 1), (1, b)\}$, for a fixed $b \in \text{GF}(q)$, then $\xi = (x + b)^{-1}$ and $r'_\xi = r'_{(x+b)^{-1}}$, where

  $$r'_{(x+b)^{-1}} = \{R_a = (a - b, x^{q+1} + b(x + x^q) + ab) \mid a \in \text{GF}(q)\} \cup \{R = (1, b)\}.$$  

Let $\Gamma$ be the subgroup of $K$ of order $q - 1$ fixing both $R$ and $R_b$ induced by the subgroup of $\text{GL}(2, q)$ given by

$$\left\{ \begin{pmatrix} c & 0 \\ (c - d)b & d \end{pmatrix} : c, d \in \text{GF}(q), cd \neq 0 \right\}.$$  

A member of $\Gamma$, say $\gamma_c$, is induced by the following matrix

$$\begin{pmatrix} 1 & 0 \\ (1 - c)b & c \end{pmatrix},$$

for some $c \in \text{GF}(q) \setminus \{0\}$. Then $\gamma_c(R_a) = R_{a-bc}^{-1}$ and $\gamma_c$ fixes $r'_{(x+b)^{-1}}$.  

7
• If \( r'_c \cap r_1 = \{(1, b_1), (1, b_2)\} \), for two fixed elements \( b_1, b_2 \in \text{GF}(q) \), then \( \xi = \frac{1}{(x+b_1)(x+b_2)} \).

In this case the subline \( r'_c = r'_{(x+b_1^{-1})(x+b_2)^{-1}} \) turns out to be

\[
\{ R_a \mid a \in \text{GF}(q) \} \cup \{ R = (x + x^q + b_1 + b_2, b_1 b_2 - x^{q+1}) \},
\]

where

\[
R_a = (x^{q+1} + a(x + x^q) + a(b_1 + b_2) - b_1 b_2, (b_1 + b_2 - a)x^{q+1} + b_1 b_2(x + x^q + a)).
\]

Let \( \Gamma \) be the subgroup of \( K \) of order \( q-1 \) fixing both \( R_{b_1} \) and \( R_{b_2} \) induced by the subgroup of \( \text{GL}(2, q) \) given by

\[
\left\{ \begin{pmatrix} c & d \\ -db_1 b_2 & c + d(b_1 + b_2) \end{pmatrix} : c, d \in \text{GF}(q), (c + b_1 d)(c + b_2 d) \neq 0 \right\}.
\]

A non-trivial projectivity of \( \Gamma \), say \( \gamma_c \), is induced by the following matrix

\[
\begin{pmatrix} c & 1 \\ -b_1 b_2 & c + b_1 + b_2 \end{pmatrix},
\]

for some \( c \in \text{GF}(q) \setminus \{-b_1, -b_2\} \). Then \( \gamma_c(R) = R_{-c} \) and \( \gamma_c(R_a) \) equals \( R \) or \( R_{\frac{ac + b_1 b_2}{b_1 + b_2 - a}} \), according as \( c = a - b_1 - b_2 \) or \( c \neq a - b_1 - b_2 \). Hence \( \gamma_c \) fixes \( r'_{(x+b_1)^{-1}(x+b_2)^{-1}} \).

Assume that \( r'_c \) is such that \( |r'_c \cap r_1| = 0 \). Let \( s_1, s_2 \) be elements of \( \text{GF}(q) \) such that the polynomial \( f(X) = X^2 + s_1 X + s_2 \) is irreducible over \( \text{GF}(q) \). This means that there exists \( u \in \text{GF}(q^2) \setminus \text{GF}(q) \) such that \( f(u) = f(u^q) = 0 \) and hence \( u^{q+1} = s_2, u + u^q = -s_1 \). In this case \( \xi = \frac{1}{(x+u)(x+u^q)} \) and

\[
r'_c = r'_{(x+u)^{-1}(x+u^q)^{-1}} = r'_{\frac{1}{(x+u)(x+u^q)}} = \{ R_a \mid a \in \text{GF}(q) \} \cup \{ R = (x + x^q - s_1, s_2 - x^{q+1}) \},
\]

where

\[
R_a = (x^{q+1} + a(x + x^q) - as_1 - s_2, -(s_1 + a)x^{q+1} + s_2(x + x^q + a)).
\]

Let \( \Gamma \) be the subgroup of \( K \) of order \( q+1 \) induced by the subgroup of \( \text{GL}(2, q) \) given by

\[
\left\{ \begin{pmatrix} c & d \\ -s_2 d & c - s_1 d \end{pmatrix} : c, d \in \text{GF}(q), (c, d) \neq (0, 0) \right\}.
\]

A non-trivial projectivity of \( \Gamma \), say \( \gamma_c \), is induced by the following matrix

\[
\begin{pmatrix} c & 1 \\ -s_2 & c - s_1 \end{pmatrix},
\]

for some \( c \in \text{GF}(q) \). Then \( \gamma_c(R) = R_{-c} \) and \( \gamma_c(R_a) \) equals \( R \) or \( R_{\frac{ac + s_1}{u - s_1}} \), according as \( c = a + s_1 \) or \( c \neq a + s_1 \). Hence \( \gamma_c \) fixes \( r'_{(x+u)^{-1}(x+u^q)^{-1}} \).

Lemma 2.3. No non-trivial projectivity of \( K \) fixes \( S_x \).
Proof. Let $\gamma$ be the projectivity of $K$ associated with the matrix
\[
\begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix} \in \text{GL}(2, q).
\]
Then
\[
\gamma(t^q - t, xt - x^q t^q) = -\left( (bx^q - a)t^q - (bx - a)t, \frac{c - dx^q}{bx - a}(bx - a)t - \frac{c - dx}{bx^q - a}(bx^q - a)t^q \right).
\]
Hence $\gamma(S_x) = S_{\frac{c - dx}{bx - a}}$. Hence $S_x \neq \gamma(S_x)$ unless $b = c = 0$ and $a = d$, i.e., $\gamma$ is the identity. 

**Proposition 2.4.** Let $S$ be a splash of $\text{PG}(1, q^3)$ and let $s, s'$ be two $q$–order sublines of $S$ such that $|s \cap s'| = 1$. Then $s'$ belongs to the opposite family of $s$ if and only if $s'$ is stabilized by a subgroup of order $q$ of $\text{Stab}_{\text{PGL}(2, q^3)}(s)$.

**Proof.** Since $\text{PGL}(2, q^3)$ is transitive on its splashes and the stabilizer of $S$ in $\text{PGL}(2, q^3)$ is transitive on its $q$–order sublines, we may assume w.l.o.g. that $S = S_x$ and that $s = r_1$. If $s'$ belongs to the opposite family of $s$, then, from Lemma 2.2, we have that there exists a subgroup of order $q$ of $\text{Stab}_{\text{PGL}(2, q^3)}(s)$ fixing $s'$. Viceversa, if $s'$ belongs to the same family as $s$, we claim that no non–trivial element of $\text{Stab}_{\text{PGL}(2, q^3)}(s)$ fixes $s'$. Assume on the contrary that there exists such a projectivity $\gamma$. Then from Lemma 2.3 we have that $S \neq \gamma(S)$, where $s, s'$ are two $q$–order sublines of both $S$ and $\gamma(S)$, contradicting [S Theorem 5.2].

**Theorem 2.5.** There are $q^3 - q$ splashes of $\text{PG}(1, q^3)$ through a $q$–order subline.

**Proof.** Let $s$ be a $q$–order subline. In $\text{PG}(1, q^3)$, there are $(q - 1)(q + 1)^2(q^2 + 1)$ $q$–order sublines intersecting $s$ in exactly one point. Let $B$ denote the set of such sublines. It can be easily checked that a subgroup of order $q$ of $\text{Stab}_{\text{PGL}(2, q^3)}(s)$ acts on points of $\text{PG}(1, q^3)$ by fixing a point $P$ of $s$ and by forming $q^2$ orbits of size $q$. Moreover, each of these orbits of size $q$ together with $P$ gives rise to a $q$–order subline of $\text{PG}(1, q^3)$. Therefore there is a subset $B'$ of $B$ consisting of $(q^2 - 1)(q + 1)$ $q$–order sublines that are stabilized by a subgroup of order $q$ of $\text{Stab}_{\text{PGL}(2, q^3)}(s)$.

Let us count in two ways the couples $(Z, s')$, where $Z$ is a splash of $\text{PG}(1, q^3)$ containing $s$ and $s'$ is a further $q$–order subline of $Z$ belonging to the same family of $s$. From Proposition 2.4, $s'$ belongs necessarily to $B \setminus B'$. Hence $s'$ can be chosen in $q^2(q + 1)(q^2 - 1)$ ways, and from [S Theorem 5.2], a splash containing $s$ and a further $q$–order subline $s'$ belonging to the same family of $s$ is uniquely determined. Hence on the one hand the number of these couples equals $q^2(q + 1)(q^2 - 1)$. On the other hand, if $z$ denotes the number of splashes of $\text{PG}(1, q^3)$ containing $s$, we have that the number of these couples equals $z(q^2 + q)$. Therefore $z = q^3 - q$, as required.

We are ready to prove the main result of this subsection.

**Theorem 2.6.** Let $S_1, S_2$ be two distinct splashes of $\text{PG}(1, q^3)$ having a $q$–order subline $s$ in common. Then $S_1, S_2$ share a $q$–order subline belonging to the opposite family of $s$. 

9
Proof. We may assume w.l.o.g. that $S_1 = S_x$, where $x$ is a fixed element of $GF(q^3) \setminus GF(q)$ and that $s = r_1$. Let $s'$ be a $q$-order subline of $S_x$ belonging to the opposite family of $s$. From Lemma 2.2 there is a subgroup $\Gamma_{s'}$ of $K$ of order $q + 1 - i$ fixing $s'$, where $|s \cap s'| = i$. Note that from Lemma 2.3 a non-trivial element $\gamma$ of $\Gamma_{s'}$ maps $S_x$ to a splash of PG$(1,q^3)$ distinct from $S_x$. Hence $\gamma(S_x)$ will share with $S_x$ both $s$ and $s'$. In particular $|S_x^{\Gamma_{s'}}| = q + 1 - i$. Moreover if $s', s''$ are two distinct $q$-order sublines of $S_x$ belonging to the opposite family of $s$, then $S_x^{\Gamma_{s'}} \cap S_x^{\Gamma_{s''}} = \{S_x\}$, otherwise if $S \in S_x^{\Gamma_{s'}} \cap S_x^{\Gamma_{s''}}$ and $S \neq S_x$, then $S$ would contain $s, s'$ and $s''$ and hence would share with $S_x$ at least $3q - 2$ points, contradicting [28, Theorem 23]. Since $s'$ can be chosen in $q + 1, q(q + 1)/2$ or $q(q - 1)/2$ ways according as $|s \cap s'|$ equals 1, 2 or 0, we have that there are $(q - 1) \cdot (q + 1) + (q - 2) \cdot q(q + 1)/2 + q \cdot q(q - 1)/2 = q^3 - q - 1$ splashes of PG$(1,q^3)$ distinct from $S_x$ such that each of them shares with $S_x$ the $q$-order subline $s$ and a further $q$-order subline belonging to the opposite family of $s$. The result now follows from Theorem 2.3. \qed

2.2 On the number of points covered by a special lineset of PG$(2,q^3)$

In PG$(2,q^3)$, with the same notation used in Lemma 2.1, let $\pi_0$ be a $q$-order subplane and let $\ell$ be a line of $L'_3$. The line $\ell$ contains $q^2 + q + 1$ points of $O'_2$ and $q^3 - q^2 - q$ points of $O'_3$. Moreover $\ell \cap O'_2$ is a splash $S$ of $\ell$ obtained by extending the $q^2 + q + 1$ sublines of $\pi_0$. Let $F_1$ be the family of $q$-order sublines of $S$ arising from the extended sublines of $\pi_0$ of certain dual subconics of $\pi_0$ and let $F_2$ be the family of $q$-order sublines of $S$ arising from the extended sublines of $\pi_0$ through a point of $\pi_0$. Let $s$ be a fixed element of $F_1$ and let $D$ be the set of extended sublines of the dual subconic of $\pi_0$ which gives rise to $s$. Then $D$ consists of $q + 1$ extended sublines of $\pi_0$ such that through a point of PG$(2,q^3)$ there pass at most 2 lines of $D$ and through a point of $s$ there is exactly one line of $D$. Moreover two distinct lines of $D$ meet in a point of $\pi_0$. There are other $q^2(q + 1)$ lines of PG$(2,q^3)$ having at least a point in common with both $s$ and $\pi_0$. Let $E$ denote the set of such lines. In particular a line of $E$ has exactly one point in common with both $s$ and $\pi_0$, i.e., $E \subset L'_2$. Through a point of $s$ there are $q^2$ lines of $E$ and through a point of $\pi_0$ there are $q + 1, q$ or $q - 1$ lines of $E$, according as there pass 0, 1 or 2 lines of $D$, respectively. A line of $D$ contains $q + 1$ points of $\pi_0$ and $q^3 - q$ points of $O'_2$, whereas a line of $E$ contains one point of $\pi_0$, $q^2$ points of $O'_2$ and $q^3 - q^2$ points of $O'_3$. The main aim of this subsection is to bound the number of points of PG$(2,q^3)$ lying on at least a line of $E$. The following result [7, Lemma 5.6] will be useful.

Lemma 2.7 ([7]). Let $r_1, r_2$ be lines of PG$(2,q^3)$ and $b$ be a $q$-order subline of $r_2$ disjoint from $r_1$. Then each $q$-order subline of $r_1$, disjoint from $r_2$, is the projection of $b$ from exactly one point not on $r_1 \cup r_2$.

Lemma 2.8. Through a point on a line of $D$ and not lying on $\pi_0 \cup s$, there passes at most one line of $E$.

Proof. Assume by contradiction that there is a point $P$ on a line $r \in D$, with $P \notin \pi_0 \cup s$, such that there are two lines of $E$, say $t_1, t_2$, passing through $P$. Let $T_i = t_i \cap \pi_0$, $i = 1, 2$. The line
$t$ obtained by joining $T_1$ and $T_2$ is an extended subline of $\pi_0$. Let $R = t \cap r$. Let $\mathcal{C}_i$ be the set $t_i \cap (\mathcal{O}_2' \cup \pi_0)$. Since $|t_i \cap \pi_0| = 1$, it follows that $\mathcal{C}_i$ is a club of $t_i$ with head point $T_i$, $i = 1, 2$. In particular $\mathcal{C}_i$ is obtained by extending the sublines of $\pi_0$. Let $Q_i = t_i \cap s$ and let $m_i$ be the unique line of $\mathcal{D}$ through $Q_i$, $i = 1, 2$. Note that the club $\mathcal{C}_i$ contains a unique $q$–order subline passing through $T_i, P, Q_i$, $i = 1, 2$. Since every $q$–order subline of $\mathcal{C}_i$ arises from the extended sublines through a point of $\pi_0$, we have that the lines $t, m_i, r$ form a pencil and $R = t \cap r \cap m_i$, $i = 1, 2$. It follows that $m_1, m_2$ and $r$ are three lines of $\mathcal{D}$ through the point $R \in \pi_0$, contradicting the fact that through a point of $\text{PG}(2, q^3)$ there pass at most two lines of $\mathcal{D}$.

**Lemma 2.9.** Through a point of $\mathcal{O}_2'$ not lying on a line of $\mathcal{D}$, there pass at most three lines of $\mathcal{E}$.

**Proof.** Let $P$ be a point of $\mathcal{O}_2'$, let $r$ be the extended subline of $\pi_0$ containing $P$ and let $R = r \cap \ell$. Since $P$ does not lie on a line of $\mathcal{D}$, we have that $r \notin \mathcal{D}$ and hence $R \notin s$. By projecting $\pi_0$ from $P$ onto $\ell$ we get a club $\mathcal{C}$ of $\ell$ with head point $R$. Since $R \notin s$, the $q$–order subline $s$ is not contained in $\mathcal{C}$. From [23] Theorem 8, we have that $|s \cap \mathcal{C}| \leq 3$. This means that there are at most three lines of $\mathcal{E}$ passing through the point $P$.

**Proposition 2.10.** Let $A, B$ be two distinct points of $s$. There are at most $(q - 1)(q^2 - q + 1)$ points of $\mathcal{O}_2'$, not lying on a line of $\mathcal{D}$, and contained in two lines of $\mathcal{E}$ passing through $A$ and $B$.

**Proof.** Let $A$ and $B$ be two points of $s$, such that there are two lines of $\mathcal{E}$, say $\ell_A$ and $\ell_B$, where $A \in \ell_A, B \in \ell_B, \ell_A \cap \ell_B = P \in \mathcal{O}_2'$ and $P$ does not lie on a line of $\mathcal{D}$. Note that there is a unique $q$–order subline $s'$ of $\mathcal{S}$ distinct from $s$ and containing $A$ and $B$. In particular $s'$ belongs to the opposite family of $s$. Let $r_P, r_A$ and $r_B$ be the extended sublines of $\pi_0$ containing $A, B$ and $P$, respectively. Then $r_A, r_B \in \mathcal{D}$ and $r_P \notin \mathcal{D}$. Let $T = r_A \cap r_B \in \pi_0$, $T_A = \ell_A \cap \pi_0$, $T_B = \ell_B \cap \pi_0$ and let $m$ be the extended subline of $\pi_0$ passing through $T_A$ and $T_B$. Thus by projecting $m \cap \pi_0$ from $P$ onto $\ell$ the subline $s'$ is obtained. Furthermore an extended subline of $\pi_0$ through $T$ meets $\mathcal{S}$ in a point of $s'$.

We claim that $T \notin r_P$. Assume by contradiction that $T \in r_P$. If $T \notin m$, then by projecting the $q$–order subline $m \cap \pi_0$ from $T$ onto $\ell$ we get $s'$. On the other hand $s'$ is also obtained by projecting $m \cap \pi_0$ from $P$ onto $\ell$, where $P \neq T$, contradicting Lemma 2.7. Hence $T \in m$ and $m \cap \ell = R \in s'$. Since $P$ projects $m \cap \pi_0$ onto $s'$, we infer that the line joining $R$ with $P$ meets $\pi_0$ in a point of $m$. It follows that $P \in m = \langle T_A, T_B \rangle$ and $\ell_A = \langle T_A, P \rangle = \langle T_B, P \rangle = \ell_B$, a contradiction.

We deduce that $T \notin r_P$ and $r_P \cap \ell \in \mathcal{S} \setminus (s \cup s')$. By projecting $\pi_0$ from $A$ onto $r_P$ we get a club $\mathcal{C}_A$ of $r_P$ with head point $T_1 = r_A \cap r_P$. Similarly, by projecting $\pi_0$ from $B$ onto $r_P$ we get a club $\mathcal{C}_B$ of $r_P$ with head point $T_2 = r_B \cap r_P$. Since $T \notin r_P$, it follows that $T_1 \neq T_2$. Also $r_P \cap \pi_0$ is a $q$–order subline of both $\mathcal{C}_A, \mathcal{C}_B$ and $P \in \mathcal{C}_A \cap \mathcal{C}_B$. Hence $|\mathcal{C}_A \cap \mathcal{C}_B| \geq q + 2$. We want to show that $r_P$ contains $q - 1$ points of $\mathcal{O}_2'$ contained in two lines of $\mathcal{E}$ passing through $A$ and $B$. To this end it is enough to prove that $|\mathcal{C}_A \cap \mathcal{C}_B| = 2q$. Let $\bar{r}$ be the $q$–order subline of $r_P$ determined by $T_1, T_2, P$. Then $\bar{r}$ is a $q$–order subline of both $\mathcal{C}_A$ and $\mathcal{C}_B$. Since $\bar{r} \cap (r_P \cap \pi_0) = \{T_1, T_2\}$, we have that $|\mathcal{C}_A \cap \mathcal{C}_B| \geq 2q$. On the other hand if $Z$ were a point of $(\mathcal{C}_A \cap \mathcal{C}_B) \setminus (\bar{r} \cup (r_P \cap \pi_0))$, then the
unique q-order subline of \( r_P \) determined by \( Z, T_1, T_2 \) would lie in \( C_A \cap C_B \) and \( |C_A \cap C_B| \geq 3q - 2 \), contradicting \[28\] Theorem 23. Therefore \( |C_A \cap C_B| = 2q \).

We have seen that if there exists a point \( P \in O'_2 \) not lying on a line of \( D \) and contained in two lines of \( E \) passing through \( A \) and \( B \), then \( r_P \cap \ell \in S \setminus (s \cup s') \) and \( r_P \) contains \( q - 1 \) points with such a property. Since \( |S \setminus (s \cup s')| = q^2 - q + 1 \), the result follows.

**Proposition 2.11.** Let \( q > 2 \). There is a set \( I \) consisting of \( q^2 \) points of \( O'_3 \) such that through a point of \( I \) there are \( q + 1 \) lines of \( E \).

**Proof.** Let \( r \) be an extended subline of \( \pi_0 \) with \( r \notin D \). Then \( \bar{r} = r \cap \pi_0 \) is a q-order subline. From Lemma \[2.7\], there is a unique point \( R \) of \( PG(2, q^3) \) with \( R \notin r \cup \ell \) such that the q-order subline \( s \) is obtained by projecting \( \bar{r} \) from \( R \) onto \( \ell \). If \( R \) were in \( \pi_0 \), then every extended subline of \( \pi_0 \) passing through \( R \) would lie in \( D \), contradicting the fact that through a point of \( \pi_0 \) there pass at most two lines of \( D \). If \( R \) were in \( O'_2 \), then either \( R \) would lie on a line of \( D \), contradicting Lemma \[2.8\] or \( R \) would not lie on a line of \( D \), contradicting Lemma \[2.9\] whenever \( q > 2 \).

**Corollary 2.12.** If through a point of \( O'_3 \setminus I \) there pass three lines of \( E \), then the points in common between these three lines and \( \pi_0 \) are not collinear.

**Proof.** Assume that there is a point \( P \in O'_3 \) such that through \( P \) there are three lines of \( E \), say \( t_1, t_2, t_3 \), and that the three points \( T_i = t_i \cap \pi_0 \), \( 1 \leq i \leq 3 \), are collinear. Let \( Q_i = t_i \cap \ell \) and note that \( Q_i \in s \), \( 1 \leq i \leq 3 \). Then the q-order subline of \( \pi_0 \) containing \( T_1, T_2, T_3 \) is projected from \( P \) onto the unique q-order subline of \( \ell \) containing \( Q_1, Q_2, Q_3 \), namely \( s \). The extended subline \( r \) containing \( T_1, T_2, T_3 \) cannot belong to \( D \). Otherwise let \( R = r \cap \ell \) and the line joining \( P \) and \( R \) meets \( \pi \) in a point of \( r \cap \pi_0 \), i.e., \( P \in r \), a contradiction. It follows that \( P \in I \).

**Proposition 2.13.** Through a point of \( O'_3 \) not lying in \( I \), there pass at most three lines of \( E \).

**Proof.** Let \( P \) be a point of \( O'_3 \setminus I \). By projecting \( \pi_0 \) from \( P \) onto \( \ell \), we get a splash \( S' \) of \( \ell \). If \( S = S' \), then there are \( q + 1 \) lines of \( PG(2, q^3) \) passing through \( P \) and meeting both \( s \) and \( \pi_0 \) at least one point and hence \( P \in I \), which is not the case. Hence \( S \neq S' \). Assume by contradiction that there are at least four lines of \( E \) through the point \( P \). Then \( |s \cap S'| \geq 4 \). By \[28\] Theorem 8], it follows that \( s \) is a q-order subline of \( S' \) as well. Since \( S \) and \( S' \) have in common \( s \), from Theorem \[2.6\] we have that \( S \) and \( S' \) have a further q-order subline \( s' \) in common and \( s' \) belongs to the opposite family of \( s \). From Corollary \[2.12\] if we consider \( s \) as a q-order subline of \( S' \), then \( s \) is obtained by projecting the points of a subconic of \( \pi_0 \) from \( P \) onto \( \ell \). Hence, when \( s' \) is considered as a q-order subline of \( S' \), it is obtained by projecting a subline \( \bar{r} \) of \( \pi_0 \) from \( P \) onto \( \ell \). Similarly, since \( s \), as a q-order subline of \( S \), arises from the extended sublines of a dual subconic of \( \pi_0 \), we have that when \( s' \) is considered as a q-order subline of \( S \), it is obtained by extending the sublines of \( \pi_0 \) through a point \( T \) of \( \pi_0 \). Let \( r \) be the line of \( PG(2, q^3) \) such that \( r \cap \pi_0 = \bar{r} \) and let \( R = r \cap \ell \). If \( T \) were on \( r \), then \( R \) would belong to \( s' \) and the line \( m \) joining \( R \) with \( P \) would meet \( \pi_0 \) at a point of \( \bar{r} \). Hence \( m = r \) and \( P \in O'_2 \), a contradiction. Therefore \( T \notin r \) and in particular \( T \notin \bar{r} \). It follows that \( s' \) is obtained by projecting \( \bar{r} \) from \( T \) onto \( \ell \).
On the other hand, the number of these couples turns out to be 2 (Proposition 2.15). Therefore we have that 2 does not lie on a line of $\mathcal{D}$.

The results achieved in Lemma 2.8, Lemma 2.9, Proposition 2.11 and Proposition 2.13 can be summarized in the following theorem.

**Theorem 2.14.** Through a point of $\text{PG}(2, q^3)$, $q > 2$, not lying in $\pi_0 \cup s$, there pass 0, 1, 2, 3 or $q + 1$ lines of $\mathcal{E}$. In the last case, we get the $q^2$ points of $\mathcal{I} \subset \mathcal{O}_3'$.

Let $z_i$ denote the number of points $P \in \mathcal{O}_3'$ such that there are $i$ lines of $\mathcal{E}$ through $P$, $i = 2, 3, q + 1$ and let $z'_j$ be the number of points $P \in \mathcal{O}_3^\prime \setminus s$ such that there are $j$ lines of $\mathcal{E}$ through $P$, $j = 2, 3$. We have that $z_{q+1} = q^2$. Let us count in two ways the pairs $(r, r')$, where $r, r' \in \mathcal{E}$ and $r \cap r' \in (\mathcal{O}_2' \cup \mathcal{O}_3') \setminus s$. For a fixed $r \in \mathcal{E}$, let $R = r \cap \pi_0$. There are $q^3 - q + i$ lines of $\mathcal{E}$ intersecting $r$ in a point of $(\mathcal{O}_2' \cup \mathcal{O}_3') \setminus s$ according as through the point $R$ there pass $i$ lines of $\mathcal{D}$, $i = 0, 1, 2$. There are $q + 1$ points of $\pi_0$ incident with one line of $\mathcal{D}$, $q(q + 1)/2$ points of $\pi_0$ incident with 2 lines of $\mathcal{D}$ and $q(q - 1)/2$ points of $\pi_0$ on no line of $\mathcal{D}$. Hence on the one hand the number of these couples equals

$$\frac{q(q - 1)}{2} \cdot (q + 1) \cdot (q^3 - q) + \frac{q(q + 1)}{2} \cdot (q - 1) \cdot (q^3 - q + 2) + q \cdot (q + 1) \cdot (q^3 - q + 1).$$

On the other hand, the number of these couples turns out to be $2(z_2 + z'_2) + 6(z_3 + z'_3) + q^2q(q + 1)$. Comparing these two quantities, we have that

$$z_2 + z'_2 + 3(z_3 + z'_3) = \frac{q^2(q + 1)(q^3 - 2q + 1)}{2}. \tag{2.1}$$

Analogously, let us count in two ways the pairs $(r, r')$, where $r, r' \in \mathcal{E}$ and $r \cap r' \in \mathcal{O}_2' \setminus s$. Let $r, r' \in \mathcal{E}$, with $r \neq r'$ and let $P = r \cap r'$. First note that from Lemma 2.8 if $P \in \mathcal{O}_2' \setminus s$, then $P$ does not lie on a line of $\mathcal{D}$. Moreover from Proposition 2.10 for two fixed points $A, B \in s$, there are at most $(q - 1)(q^2 - q + 1)$ points $P \in \mathcal{O}_2' \setminus s$ such that $r \cap s = A$, $r' \cap s = B$ and $r \cap r' = P$. Therefore we have that $2z'_2 + 6z'_3 \leq (q - 1)(q^2 - q + 1) \cdot q(q + 1)$, that is

$$z'_2 + 3z'_3 \leq \frac{(q^3 - q)(q^2 - q + 1)}{2}. \tag{2.2}$$

**Proposition 2.15.** If $q \geq 5$, then $z_2 + 2z_3 > q^5 - 2q^3$.

**Proof.** Taking into account (2.1) and (2.2), we have that $z_2 + 2z_3 \geq (q^3 - q)(q^3 - 1)/2$. On the other hand, from Corollary 2.12 we have that the value $z_3$ cannot exceed the number of triangles of $\pi_0$, that is $q^3(q + 1)(q^2 + q + 1)/6$. Hence

$$z_2 + 2z_3 \geq \frac{(q^3 - q)(q^3 - 1)}{2} - z_3 \geq \frac{(q^3 - q)(q^3 - 1)}{2} - \frac{q^3(q + 1)(q^2 + q + 1)}{6} = \frac{2q^6 - 2q^5 - 5q^4 - 4q^3 + 3q}{6} > q^5 - 2q^3,$$

whenever $q \geq 5$. \qed
2.3 Cutting blocking sets of \( \text{PG}(3, q^3) \) as union of three \( q \)-order subgeometries

Let \( \text{PG}(3, q^3) \) be the three-dimensional projective space over \( \text{GF}(q^3) \).

**Lemma 2.16.** A plane of \( \text{PG}(3, q^3) \) shares with a \( q \)-order subgeometry of \( \text{PG}(3, q^3) \) either one point or \( q + 1 \) points of a \( q \)-order subline or \( q^2 + q + 1 \) points of a \( q \)-order subplane.

**Proof.** Let \( \Sigma \) be a \( q \)-order subgeometry of \( \text{PG}(3, q^3) \), let \( P \) be a point of \( \Sigma \) and let \( \pi \) be a plane of \( \text{PG}(3, q^3) \) such that \( \pi \cap \Sigma \) is a \( q \)-order subplane of \( \pi \), with \( P \notin \pi \). A plane \( \sigma \) of \( \text{PG}(3, q^3) \) containing \( P \) intersects \( \pi \) in a line \( r \) and \( |\sigma \cap \Sigma| \) equals 1, \( q + 1 \) or \( q^2 + q + 1 \), according as \( r \cap \pi_0 \) equals 0, 1 or \( q + 1 \), respectively. From Lemma 2.1 there are \( q(q^2 - 1)(q^2 + q + 1) \) lines intersecting \( \pi_0 \) in one point and \( q^3(q - 1)(q^2 - 1) \) lines disjoint from \( \pi_0 \). Hence apart from the \( (q + 1)(q^2 + 1) \) planes of \( \text{PG}(3, q^3) \) intersecting \( \Sigma \) in a \( q \)-order subplane, there are \( q(q^2 + q + 1)(q^4 - 1) \) planes of \( \text{PG}(3, q^3) \) meeting \( \Sigma \) in a \( q \)-order subline and \( q^3(q^2 - 1)(q^4 - 1) \) planes of \( \text{PG}(3, q^3) \) having in common with \( \Sigma \) exactly one point.

We will refer to a line or a plane of \( \text{PG}(3, q^3) \) intersecting a \( q \)-order subgeometry \( \Sigma \) in \( q + 1 \) or \( q^2 + q + 1 \) points as a line or a plane of \( \Sigma \), respectively. Let \( \Sigma_1 = \text{PG}(3, q) \) be the canonical \( q \)-order subgeometry embedded in \( \text{PG}(3, q^3) \). Let \( G = \text{PGL}(4, q) \) be the stabilizer of \( \Sigma_1 \) in \( \text{PGL}(4, q^3) \) and let \( \iota \) be the collineation of order three of \( \text{PG}(3, q^3) \) fixing pointwise \( \Sigma_1 \).

**Lemma 2.17.** The group \( G \) has three orbits on points of \( \text{PG}(3, q^3) \):

- \( \Sigma_1 \);
- \( \mathcal{O}_2 \) of size \( q(q^2 + q + 1)(q^4 - 1) \) consisting of points lying on exactly one line of \( \Sigma_1 \);
- \( \mathcal{O}_3 \) of size \( q^3(q^2 - 1)(q^4 - 1) \).

**Proof.** Let \( \pi \) be a plane of \( \Sigma_1 \) and let \( G_\pi \) be the stabilizer of \( \pi \) in \( G \). The group \( G \) is transitive on the \( (q + 1)(q^2 + 1) \) planes of \( \Sigma_1 \), hence the three \( G_\pi \)-orbits on points of \( \pi \) give rise to \( \Sigma_1 \), \( \mathcal{O}_2 \), \( \mathcal{O}_3 \). To compute their size, note that two planes of \( \Sigma_1 \) have in common \( q + 1 \) points of \( \Sigma_1 \) and \( q^3 - q \) points of \( \mathcal{O}_2 \) and that a point of \( \mathcal{O}_2 \) lies on exactly \( q + 1 \) planes of \( \Sigma_1 \).

Note that a point \( P \in \text{PG}(3, q^3) \setminus \Sigma_1 \) belongs to \( \mathcal{O}_2 \) or \( \mathcal{O}_3 \) according as the points \( P, P^\iota, P^{\iota^2} \) span a line or a plane of \( \Sigma_1 \), respectively.

**Lemma 2.18.** The group \( G \) has five orbits on lines of \( \text{PG}(3, q^3) \):

- \( \mathcal{L}_1 \) of size \( (q^2 + 1)(q^2 + q + 1) \) consisting of lines of \( \Sigma_1 \). A line of \( \mathcal{L}_1 \) has \( q + 1 \) points in common with \( \Sigma_1 \) and \( q^3 - q \) points in common with \( \mathcal{O}_2 \);
- \( \mathcal{L}_2 \) of size \( q(q + 1)(q^2 + q + 1)(q^4 - 1) \) consisting of lines meeting \( \Sigma_1 \) in one point and contained in a plane of \( \Sigma_1 \). A line of \( \mathcal{L}_2 \) consists of one point of \( \Sigma_1 \), \( q^2 \) points of \( \mathcal{O}_2 \) and \( q^3 - q^2 \) points of \( \mathcal{O}_3 \);
- \( \mathcal{L}_3 \) of size \( q^3(q^2 - 1)(q^4 - 1) \) consisting of lines meeting \( \Sigma_1 \) in one point and not contained in a plane of \( \Sigma_1 \). A line of \( \mathcal{L}_3 \) has one point in common with \( \Sigma_1 \) and \( q^3 \) points in common with \( \mathcal{O}_3 \);
Lemma 2.19. Let \( \ell \) be a line of \( \Sigma_1 \) containing \( \ell \) just as \( \ell \in L_2 \cup L_4 \) or \( \ell \in L_3 \cup L_5 \). Moreover, if \( \ell \in L_2 \cup L_4 \), then \( |\ell \cap \Sigma_1| = 1 \), whereas if \( \ell \in L_3 \cup L_5 \), then \( |\ell \cap \Sigma_1| = 0 \). It follows that if \( \ell \in L_2 \) there are \( q^2 \) planes of \( \text{PG}(3, q^3) \) containing \( \ell \) and meeting \( \Sigma_1 \) in \( q + 1 \) points, whereas if \( \ell \in L_3 \) there are \( q^2 + q + 1 \) planes of
On the other hand, since there are other \( \ell \) of \( \Sigma_1 \) containing \( \ell \). Through \( \ell \) there pass \( q^3 \) planes distinct from \( \pi \) and \( |\Sigma_1 \setminus \pi| = q^3 \). Since every plane has at least a point in common with \( \Sigma_1 \), we have that necessarily every plane through \( \ell \) distinct from \( \pi \) has exactly one point in common with \( \Sigma_1 \). If \( \ell \in \mathcal{L}_5 \), from the proof of Lemma 2.18, \( \ell \) is contained in a unique hyperbolic quadric \( \mathcal{H} \) of PG(3, \( q^3 \)) such that \( \mathcal{H} \cap \Sigma_1 \) is a hyperbolic quadric of \( \Sigma_1 \). Hence there are at least \( q + 1 \) planes containing \( \ell \) and meeting \( \Sigma_1 \) in \( q + 1 \) points. On the other hand, since there are other \( q^3 - q \) planes through \( \ell \) and \( |\Sigma_1 \setminus (\Sigma_1 \cap \mathcal{H})| = q^3 - q \), every other plane through \( \ell \) has to share with \( \Sigma_1 \) exactly one point. \( \square \)

Let \( S \) be a Singer group of \( \Sigma_1 \). Then \( S \) is a subgroup of order \( (q + 1)(q^2 + 1) \) of a Singer group \( \bar{S} \) of PG(3, \( q^3 \)). Let \( \bar{S}' \) be the unique subgroup of \( \bar{S} \) of order \( (q^2 - q + 1)(q^3 - q^2 + 1) \). Thus a non-trivial element of \( \bar{S}' \) maps \( \Sigma_1 \) to a \( q \)-order subgeometry of PG(3, \( q^3 \)) distinct from \( \Sigma_1 \). Since \( S \) acts regularly on the points of PG(3, \( q^3 \)) and \( \bar{S} = \langle S, \bar{S}' \rangle \), we have that necessarily these \( (q^2 - q + 1)(q^3 - q^2 + 1) \) \( q \)-order subgeometries so obtained are pairwise disjoint. Hence they form a partition \( \mathcal{P} \) of the points of PG(3, \( q^3 \)) into \( q \)-order subgeometries. Since \( S \) is a subgroup of \( G \), it follows that a \( q \)-order subgeometry of \( \mathcal{P} \) and distinct from \( \Sigma_1 \) consists either of points of \( O_2 \) or of points of \( O_3 \). In particular there are \( q^3(q - 1)(q^2 - 1) \) members of \( \mathcal{P} \) consisting of points of \( O_3 \) and hence \( q^4 - q \) members of \( \mathcal{P} \) formed by points of \( O_2 \). Recall the following results.

Lemma 2.20 ([11]). No plane of PG(3, \( q^3 \)) meets two distinct members of \( \mathcal{P} \) in \( q^2 + q + 1 \) points.

Lemma 2.21 ([19], [22]). Under the action of \( S \), the lines of \( \mathcal{L}_1 \) are partitioned into \( q + 1 \) orbits:

- one orbit consisting of \( q^2 + 1 \) pairwise disjoint lines;
- \( q \) orbits \( \mathcal{R}_1, \ldots, \mathcal{R}_q \) each of size \( (q + 1)(q^2 + 1) \). Through a point of \( \Sigma_1 \) there pass \( q + 1 \) lines of \( \mathcal{R}_i \) no three in a plane of \( \Sigma_1 \) and a plane of \( \Sigma_1 \) contains \( q + 1 \) lines of \( \mathcal{R}_i \) no three through a point.

Note that if two lines of \( \Sigma_1 \) meet, then necessarily their intersection point belongs to \( \Sigma_1 \). Let \( \ell \) be a line of \( \mathcal{R}_1 \) and let \( L \) be a point of \( \ell \cap O_2 \). Set \( \Sigma_2 = L^S \). We will show that there exists a \( q \)-order subgeometry of \( \mathcal{P} \) consisting of points of \( O_3 \) that together with \( \Sigma_1 \cup \Sigma_2 \) forms a cutting blocking set.

Proposition 2.22. There are exactly \( (q^3 + q^2 + 1)(q + 1)(q^2 + 1) \) lines of PG(3, \( q^3 \)) having at least a point in common with \( \Sigma_1 \) and \( \Sigma_2 \). In particular \( (q + 1)(q^2 + 1) \) of these are lines of \( \Sigma_1 \) and \( q^2(q + 1)(q^2 + 1) \) are lines of \( \mathcal{L}_2 \) meeting both \( \Sigma_1 \) and \( \Sigma_2 \) in one point.

Proof. Since \( |\Sigma_2| = |L^S| = |\ell^S| = |\mathcal{R}_1| \) and the unique line of \( \mathcal{R}_1 \) through \( L \) is \( \ell \), necessarily \( \ell \) meets \( \Sigma_2 \) in \( L \). Hence every line of \( \mathcal{R}_1 \) has exactly one point in common with \( \Sigma_2 \). Moreover no other line of \( \Sigma_1 \) may have a point in common with \( \Sigma_2 \). Therefore a line of PG(3, \( q^3 \)) not belonging to \( \mathcal{R}_1 \) and having at least a point in common with \( \Sigma_1 \) and \( \Sigma_2 \) belongs to either \( \mathcal{L}_2 \) or \( \mathcal{L}_4 \). Let \( \pi \) be a plane of \( \Sigma_1 \) with \( \ell \subset \pi \). Since there are exactly \( q + 1 \) lines of \( \mathcal{R}_1 \) contained in \( \pi \) and every line of \( \mathcal{R}_1 \) has exactly one point in common with \( \Sigma_2 \), we have that \( |\pi \cap \Sigma_2| \geq q + 1 \). From Lemma 2.20 we have that \( \pi \cap \Sigma_2 \) consists of \( q + 1 \) points of a \( q \)-order subline, say \( s \).
Through the point $L$ of $s$ there pass $q^2$ lines of $L_2$ that are contained in $\pi$. Varying the plane $\pi$ among the $q + 1$ planes of $\Sigma_1$ containing $\ell$, we have that there are $q^2(q + 1)$ lines of $L_2$ through $L$ meeting both $\Sigma_1$ and $\Sigma_2$ in one point. Since $q^3 + q^2 = |\Sigma_1 \setminus \ell|$, we have that every line through $L$ distinct from $\ell$ and intersecting $\Sigma_1$ in at least one point has exactly one point in common with $\Sigma_1$. Since $\Sigma_2 = L^S$, it follows that there are exactly $q^2(q + 1)^2(q^2 + 1)$ lines of $L_2$ meeting both $\Sigma_1$ and $\Sigma_2$ in one point. □

**Corollary 2.23.** A line of $\Sigma_2$ is disjoint from $\Sigma_1$.

From Proposition 2.22 the $(q + 1)(q^2 + 1)$ lines of $R_1$ have $q + 1$ points in common with $\Sigma_1$ and one point in common with $\Sigma_2$ and there is a subset of $L_2$, say $R$, consisting of $q^2(q + 1)^2(q^2 + 1)$ lines meeting both $\Sigma_1$ and $\Sigma_2$ in exactly one point. Let $\pi$ be a plane of $\Sigma_1$. From the proof of Proposition 2.22 we have that $\pi \cap \Sigma_2$ is a $q$–order subline, say $s$. There are $q + 1$ lines of $R_1$ contained in $\pi$ and the set $D$ of these $q + 1$ lines consists of the extended sublines of a dual subconic of $\pi \cap \Sigma_1$; see 22. Moreover there are $q^2(q + 1)$ lines of $R$ contained in $\pi$; let $E$ be the set of these lines. Note that $D \cup E$ is the set of lines of $\pi$ having at least a point in common with both $s$ and $\pi \cap \Sigma_1$.

**Lemma 2.24.** If $r_1$ and $r_2$ are two distinct lines of $R_1 \cup R$ such that $r_1 \cap r_2 \in O_3$, then the plane spanned by $r_1$ and $r_2$ is a plane of $\Sigma_1$.

**Proof.** Since no point of $O_3$ lies on a line of $R_1$, we have that $r_1, r_2 \in R$. Moreover $|\Sigma_1 \cap O_3| = |\Sigma_2 \cap O_3| = 0$ and hence $r_1 \cap r_2 \notin \Sigma_1 \cup \Sigma_2$. Since $r_i \in L_2$, $i = 1, 2$, there is a plane of $\Sigma_1$, say $\pi_i$, containing $r_i$, $i = 1, 2$. Assume by contradiction that $\sigma = \langle r_1, r_2 \rangle$ is not a plane of $\Sigma_1$. Then $\pi_1 \neq \pi_2$ and $r_1 \cap r_2 \in \pi_1 \cap \pi_2$, a contradiction since two planes of $\Sigma_1$ meet in a line of $\Sigma_1$, which contains no point of $O_3$. □

**Proposition 2.25.** There exists a point $P \in O_3$ such that $P$ is not contained in a line of $R_1 \cup R$.

**Proof.** Since no point of $O_3$ lies on a line of $R_1$, we have that if a point of $O_3$ lies on some line of $R_1 \cup R$ then such a line belongs to $R$. From Lemma 2.24 if $P \in O_3$ and if $r_1$ and $r_2$ are two distinct lines of $R$ such that $P = r_1 \cap r_2$, then $r_1$ and $r_2$ are contained in a plane of $\Sigma_1$. Therefore, by Theorem 2.14 through a point of $O_3$, there pass $0, 1, 2, 3$ or $q + 1$ lines of $R$. Fix a plane of $\Sigma_1$, say $\pi$, and let $z_i$ denote the number of points $Q \in O_3 \cap \pi$ such that there are $i$ lines of $R$ through $Q$, $i = 2, 3, q + 1$. Since $S$ is transitive on planes of $\Sigma_1$ and two distinct planes of $\Sigma_1$ have no point of $O_3$ in common, we have that there are exactly $z_i(q + 1)(q^2 + 1)$ points of $O_3$ such that there are $i$ lines of $R$ through $Q$, $i = 2, 3, q + 1$. In the last case, since $z_{q+1} = q^2$, the points of $O_3$ contained in the $q + 1$ lines of $R$ are exactly $q^2(q + 1)(q^2 + 1)$ and every plane of $\Sigma_1$ contains $q^2$ of these points. Since a line of $R$ contains $q^3 - q^2$ points of $O_3$, it follows that the number of points of $O_3$ lying on at least one line of $R$ equals

$$
(q^3 - q^2)|R| - q \cdot z_{q+1}(q + 1)(q^2 + 1) - z_2(q + 1)(q^2 + 1) - 2 \cdot z_3(q + 1)(q^2 + 1)\\
= (q + 1)(q^2 + 1)(q^6 - q^4 - q^3 - z_2 - 2z_3),
$$

17
which is smaller than \(|O_3| = (q + 1)(q^2 + 1)(q^6 - q^5 - q^4 + q^3)|\), since \(z_2 + 2z_3 > q^5 - 2q^3\), whenever \(q \geq 5\), by Proposition 2.15. If \(q \leq 4\), then some computations performed with Magma \([10]\] confirm the statement.

By Proposition 2.25 there is a point \(P \in O_3\) with the property that no line of \(PG(3, q^3)\) having at least a point in common with \(\Sigma_1\) and \(\Sigma_2\) passes through \(P\). Let \(\Sigma_3 = P^S\).

**Theorem 2.26.** The set \(\Sigma_1 \cup \Sigma_2 \cup \Sigma_3\) is a cutting blocking set of \(PG(3, q^3)\) of size \(3(q + 1)(q^2 + 1)\).

**Proof.** First observe that no line of \(PG(3, q^3)\) has at least a point in common with each of the subgeometries \(\Sigma_1\), \(\Sigma_2\) and \(\Sigma_3\). Assume on the contrary that \(\ell\) is a line of \(R_1 \cup R\) having a point \(R\) in common with \(\Sigma_3\). Since \(\Sigma_3 = P^S\), there is a projectivity \(\gamma\) of \(S\) mapping \(R\) to \(P\) and hence \(\ell \cap \gamma\) is a line of \(R_1 \cup R\) containing \(P\), contradicting the fact that no line of \(R_1 \cup R\) passes through \(P\).

Let \(\Pi\) be a plane of \(PG(3, q^3)\). Then \(|\Pi \cap \Sigma_i| \geq 1\) and hence \(|\Pi \cap (\Sigma_1 \cup \Sigma_2 \cup \Sigma_3)| \geq 3\). Suppose by contradiction that \(\Sigma_1 \cup \Sigma_2 \cup \Sigma_3\) is not a cutting blocking set of \(PG(3, q^3)\). Hence there is a plane \(\Pi\) of \(PG(3, q^3)\) such that the points of \(\Pi \cap (\Sigma_1 \cup \Sigma_2 \cup \Sigma_3)\) are on a line, say \(r\). It follows that \(|\Pi \cap (\Sigma_1 \cup \Sigma_2 \cup \Sigma_3)| \geq 3\) and \(r\) is a line of \(PG(3, q^3)\) having at least one point in common with each of the subgeometries \(\Sigma_1\), \(\Sigma_2\) and \(\Sigma_3\); a contradiction.

**Proposition 2.27.** The cutting blocking set \(\Sigma_1 \cup \Sigma_2 \cup \Sigma_3\) of \(PG(3, q^3)\) is minimal.

**Proof.** Since \(S\) acts transitively on \(\Sigma_i\), it is enough to prove that through a point of \(\Sigma_i\), there is a plane of \(PG(3, q^3)\) intersecting each of the three relevant subgeometries in exactly one point. Let \(r\) be a line of \(R\). Then \(|r \cap \Sigma_1| = |r \cap \Sigma_2| = 1\) and \(|r \cap \Sigma_3| = 0\). Since \(r \in L_2\), from Lemma 2.19 there are \(q^2 + 1\) planes through \(r\) intersecting \(\Sigma_1\) in at least \(q + 1\) points. Similarly, from Lemma 2.19 we deduce that there are at most \(q^2 + q + 1\) planes through \(r\) having in common at least \(q + 1\) points with \(\Sigma_2\) and at most \(q + 1\) planes through \(r\) intersecting \(\Sigma_3\) in at least \(q + 1\) points. Taking into account Lemma 2.16 we have that there are at least \(q^3 + 1 - (q^2 + 1) - (q^2 + q + 1) - (q + 1) = q^3 - 2(q^2 + q + 1)\) planes through \(r\) having exactly one point in common with each of the subgeometries \(\Sigma_1\), \(\Sigma_2\) and \(\Sigma_3\). Hence if \(q \geq 3\), we are done. If \(q = 2\), Magma computations \([10]\] show the assertion.

**Proposition 2.28.** To the set \(\Sigma_1 \cup \Sigma_2 \cup \Sigma_3\) there corresponds a \([3(q + 1)(q^2 + 1), 4]_{q^3}\) reduced minimal linear code with possible weights \(3q^3 + 3q^2 + 3q\), \(3q^3 + 3q^2 + 2q\), \(3q^3 + 3q^2 + q\), \(3q^3 + 3q^2\), \(3q^3 + 3q^2 + q\) and \(3q^3 + 2q^2 + q\).

**Proof.** It is enough to observe that, from Lemma 2.16 and Lemma 2.20 a plane of \(PG(3, q^3)\) can intersect the set \(\Sigma_1 \cup \Sigma_2 \cup \Sigma_3\) in \(3\), \(q + 3\), \(2q + 3\), \(3q + 3\), \(q^2 + 2q + 3\) or \(q^2 + q + 3\) points.

### 3 Cutting blocking sets from lines in hyggledy–piggledy arrangement

In \(PG(3, q)\) let \(\ell_1, \ell_2, \ell_3\) three pairwise skew lines. There are \(q + 1\) lines meeting \(\ell_i\), \(1 \leq i \leq 3\), in one point. These lines form a *regulus*, say \(R\) and are contained in a hyperbolic quadric \(Q^+(3, q)\).
Let $\mathcal{R}^0$ denote the opposite regulus of $\mathcal{R}$. It follows that a set of lines of $\text{PG}(3,q)$ in hyggledy–piggledy arrangement has to contain at least four elements. Let $r$ be a line external to $\mathcal{Q}^+(3,q)$. Then the set $\mathcal{B}$ consisting of the $4(q+1)$ points of $\ell_1 \cup \ell_2 \cup \ell_3 \cup r$ forms a cutting blocking set, see for instance [20, Example 9], [13] Theorem 3.7.

**Proposition 3.1.** In $\text{PG}(3,q)$, $q > 2$, the cutting blocking set $\mathcal{B}$ is minimal.

**Proof.** Let $P \in r$ and let $\sigma$ be the plane spanned by $P$ and a line $s$ of $\mathcal{R}^0 \setminus \{\ell_1, \ell_2, \ell_3\}$. Then $\sigma$ meets the hyperbolic quadric $\mathcal{Q}^+(3,q)$ in two lines, one of which is $s$ and the other one, say $s'$, belongs to $\mathcal{R}$. Note that $\ell_i \cap \sigma \in s'$, $i = 1, 2, 3$, and hence $((\mathcal{B} \setminus \{P\}) \cap \sigma) = s' \neq \sigma$. If $P \in \ell_i$, let $Q$ be the hyperbolic quadric obtained by considering the regulus of $\text{PG}(3,q)$ containing the lines $\ell_j, \ell_k$ and $r$, where $\{i,j,k\}$ is a permutation of $\{1,2,3\}$. By repeating the same argument, interchanging $\mathcal{Q}^+(3,q)$ with $Q$, $r$ with $\ell_i$ and $\ell_1, \ell_2, \ell_3$ with $\ell_j, \ell_k$, $r$, we have that $\mathcal{B} \setminus \{P\}$ is not a cutting blocking set.

**Proposition 3.2.** The code associated with the minimal cutting blocking set of Proposition 3.1 is a $[4(q+1),4]_q$ reduced minimal linear code with weights $3q$ and $4q$ and weight distribution $A_{3q} = 4(q^2 - 1)$ and $A_{4q} = (q^2 - 3)(q^2 - 1)$.

**Proof.** It is enough to observe that there are exactly $4(q+1)$ planes containing one of the four relevant lines and hence meeting $\mathcal{B}$ in $q+4$ points and that the remaining $(q^2 - 3)(q+1)$ planes meet $\mathcal{B}$ in four points.

In $\text{PG}(r,q)$, let $\mathcal{C} = \{(1,t,\ldots,t^{r-1},t^r) \mid t \in \text{GF}(q)\} \cup \{(0,0,\ldots,0,1)\}$ be the normal rational curve of $\text{PG}(r,q)$. Then $\mathcal{C}$ consists of $q+1$ points of $\text{PG}(r,q)$ no $k+2$ of which in a $k$–space of $\text{PG}(r,q)$. Also, for each point $P$ of $\mathcal{C}$ there is a distinguished line $t_P$ passing through $P$, that is the tangent to $\mathcal{C}$ at $P$, where $t_P = \langle P, P' \rangle$, $P' = (0,1,2t,\ldots,(n-1)t^{n-2},nt^{n-1})$ if $P \neq (0,0,\ldots,0,1)$, and $P' = (0,0,\ldots,1,0)$ if $P = (0,0,\ldots,0,1)$. Moreover no two tangent lines to $\mathcal{C}$ have a point in common (cf. [20, Lemma 6.31]). For further properties of the normal rational curve we refer the reader to [26, Section 6.5]. The following result has been proved in [20, Theorem 20].

**Theorem 3.3** ([20]). If $p > r$ and $q > 2r - 1$, then arbitrary $2r-1$ distinct tangent lines to $\mathcal{C}$ constitute a set of lines of $\text{PG}(r,q)$ in hyggledy–piggledy arrangement.

**Remark 3.4.** From the construction of Fancsali and Sziklai, there arises a cutting blocking set of $\text{PG}(r,q)$ of size $(2r-1)(q+1)$. However the cutting blocking set so obtained is in general not minimal. For instance in $\text{PG}(4,11)$ with the aid of Magma [10] it is possible to see that suitably selecting six tangent lines to $\mathcal{C}$, a minimal cutting blocking set of $\text{PG}(4,11)$ is obtained.

**Problem 3.5.** Determine the minimum number of lines tangent to a normal rational curve in $\text{PG}(r,q)$ such that the set of points covered by these lines forms a minimal cutting blocking set.

Assume that $p > r$ and that $q > 2r - 1$. Let $\bar{S}$ be the set of points covered by $2r - 1$ arbitrarily chosen tangent lines to $\mathcal{C}$. Let $S$ be a pointset such that $S \subseteq \bar{S}$ and $S$ is a minimal cutting blocking set.
Proposition 3.6. A hyperplane of PG(r, q) contains at most r − 2 lines that are tangent to C.

Proof. By induction on r. Let r = 3. Since no two lines tangent to C have a point in common, a plane of PG(3, q) contains at most one tangent line to C. Assume that the result holds true for r − 1. Let C be a normal rational curve of the projective space PG(r, q) equipped with homogeneous projective coordinates X_1, . . . , X_{r+1}. Suppose by contradiction that a hyperplane H of PG(r, q) contains r − 1 lines tangent to C. Denote by P a point of C ∩ H, where t_P, the line tangent to C at P, is contained in H. Let Γ be a hyperplane of PG(r, q) such that P ∉ Γ. From Lemma [26, Theorem 6.30], we may assume that P = (0, 0, . . . , 0, 1). By projecting the q points of C \ {P} and the line t_P from P onto Γ : X_{r+1} = 0, we obtain the normal rational curve C' = {(1, t, . . . , t^{r−1}, 0) | t ∈ GF(q)} ∪ {(0, 0, . . . , 1, 0)} of Γ. On the other hand, by projecting from P onto Γ the line tangent to C at a point R, R ≠ P, we get the line ⟨R, R'⟩ that is tangent to C' at R, where R = (1, t, . . . , t^{r−1}, 0) and R' = (0, 1, . . . , (r−1)t^{r−2}, 0). Observe that by projecting the r − 1 tangent lines to C contained in H we get r − 2 lines that are tangent to C' and are contained in the (r−2)−space H ∩ Γ ⊂ Γ, a contradiction.

Proposition 3.7. Let p > r and q > 2r − 1. The code associated with the minimal cutting blocking set S is a [[|S|, r + 1]_q reduced minimal linear code, where |S| ≤ (2r − 1)(q + 1) and minimum distance d ≥ |S| − (r−2)q−2r+1.

Proof. The statement follows from Proposition 3.6.

3.1 Lines of PG(5, q) in higgledy–piggledy arrangement

Let PG(2, q^2) be the Desarguesian projective plane. Its underlying vector space V(3, q^2) can be considered as a 6-dimensional vector space V(6, q) via the inclusion GF(q) ⊂ GF(q^2). Each point in PG(2, q^2) corresponds to a 1-dimensional vector subspace in V(3, q^2) which in turn corresponds to a 2-dimensional vector subspace in V(6, q), i.e., a line of PG(5, q). Extending this map from (subsets of) points of PG(2, q^2) to subsets of points of PG(5, q) we obtain a map φ : PG(2, q^2) → PG(5, q), called field reduction map.

The set D = {φ(P) | P ∈ PG(2, q^2)} is a Desarguesian line–spread of PG(5, q). The incidence structure whose points are the elements of D and whose lines are the solids of PG(5, q) joining two distinct elements of D, is isomorphic to PG(2, q^2). A degenerate Hermitian curve of rank 2 of PG(2, q^2) is a cone having as vertex a point and as base a Baer subline. In what follows we will refer to a degenerate Hermitian curve of rank 2 as a degenerate Hermitian curve. Let Π be a solid of PG(5, q) and let φ^{-1}(Π) = {P ∈ PG(2, q^2) : |φ(P) ∩ Π| ≥ 1}. Then either Π contains q^2 + 1 lines of D and φ^{-1}(Π) is a line of PG(2, q^2) or there is exactly one line ℓ of D in Π and φ^{-1}(Π) is a degenerate Hermitian curve H of PG(2, q^2). Note that to such a degenerate Hermitian curve there correspond q + 1 solids of PG(5, q), say Π_i, 1 ≤ i ≤ q + 1, such that Π_i ∩ Π_j = ℓ, if i ≠ j, and \bigcup_{i=1}^{q+1} Π_i = \bigcup \{φ(P) | P ∈ H\}.

Lemma 3.8. Let P be a set of points of PG(2, q^2) not on a line of PG(2, q^2) and not on a degenerate Hermitian curve of PG(2, q^2). Then L = {φ(P) | P ∈ P} is a set of lines of PG(5, q) in higgledy–piggledy position.
Proof. Assume by contradiction that the lines of $\mathcal{L}$ are not in higgledy–piggledy position. Then there would exist a solid $\Pi$ of $\text{PG}(5, q)$ meeting every line of $\mathcal{L}$ and $\mathcal{P}$ would be contained in $\phi^{-1}(\Pi)$, a contradiction. \qed

In $\text{PG}(2, q^2)$, consider the set $\mathcal{P}$ consisting of the following four points:

$$P_1 = (1, 0, 0), \ P_2 = (0, 1, 0), \ P_3 = (0, 0, 1), \ P_4 = (1, 1, 1).$$

There is a unique Baer subplane of $\text{PG}(2, q^2)$ containing the four points of $\bar{\mathcal{P}}$, namely the canonical Baer subplane $\pi$.

**Lemma 3.9.** There are exactly $q^3 + 4q^2 + 1$ degenerate Hermitian curve containing the four points of $\bar{\mathcal{P}}$.

*Proof.* Let $\mathcal{H}$ be a degenerate Hermitian curve containing the four points of $\bar{\mathcal{P}}$ and let $V$ be its vertex. Assume first that $V \in \pi$. If $V \notin \{(0, 1, 1), (1, 0, 1), (1, 1, 0)\}$, then at least three of the lines of $\mathcal{H}$ meet $\pi$ in a Baer subline. In this case the $q + 1$ lines of $\mathcal{H}$ have all $q + 1$ points in common with $\pi$. Hence $\pi \subset \mathcal{H}$ and $\mathcal{H}$ is uniquely determined by $V$. If $V \in \{(0, 1, 1), (1, 0, 1), (1, 1, 0)\}$, then either $\pi \subset \mathcal{H}$ and $\mathcal{H}$ is uniquely determined or $\mathcal{H}$ intersects $\pi$ in the two lines through $V$ whose union contains the four points of $\bar{\mathcal{P}}$ and there are $3q$ choices for $\mathcal{H}$. Assume now that $V \notin \pi$. In this case $\pi \not\subset \mathcal{H}$ and $\mathcal{H} \cap \pi$ is a quadric. Since the quadric $\mathcal{H} \cap \pi$ contains at least four points no three on a line, we have that either $\mathcal{H} \cap \pi$ consists of two intersecting Baer sublines of $\pi$ containing the four points of $\pi$ or $\mathcal{H} \cap \pi$ is a non–degenerate Baer conic $\bar{\mathcal{C}} \subset \pi$. In the former case $V$ lies on a line secant to $\bar{\mathcal{P}}$ and for a fixed $V$ there is a unique $\mathcal{H}$. Hence there are $6(q^2 - q)$ degenerate Hermitian curves of this type. In the latter case, from [17, Corollary 6.2], we have that $V \in \mathcal{C}$, where $\mathcal{C}$ is the unique non–degenerate conic of $\text{PG}(2, q^2)$ such that $\mathcal{C} \cap \pi = \bar{\mathcal{C}}$, and for a fixed $V$ there is a unique $\mathcal{H}$. Since there are $q - 2$ of such non–degenerate conics, it follows that there are $(q - 2)(q^2 - q)$ degenerate Hermitian curves of this type. \qed

The degenerate Hermitian curves of the previous lemma are listed and described below.

- $q^2 + q + 1$ degenerate Hermitian curves of type

$$X_1^q X_2 - X_1 X_2^q = 0,$$

$$a(X_1^q X_2 - X_1 X_2^q) - (X_1^q X_3 - X_1 X_3^q) = 0, \ a \in \text{GF}(q), \ (3.1)$$

$$b(X_1^q X_2 - X_1 X_2^q) - a(X_1^q X_3 - X_1 X_3^q) + X_2^q X_3 - X_2 X_3^q = 0, \ a, b \in \text{GF}(q).$$

They contain $\pi$ and their vertices lie in $\pi$.

- $3q$ degenerate Hermitian curves of type

$$X_1^q X_3 - \alpha X_1 X_3^q - X_2^q X_3 + \alpha X_2 X_3^q = 0,$$

$$X_1^q X_2 - \alpha X_1 X_2^q + \alpha X_2^q X_3 - X_2 X_3^q = 0,$$

$$X_1^q X_2 - \alpha X_1 X_2^q - X_1^q X_3 + \alpha X_1 X_3^q = 0, \ \alpha \in \text{GF}(q^2) \setminus \{1\}, \ \alpha^{q+1} = 1. \ (3.2)$$

They meet $\pi$ in $2q + 1$ points and their vertices belong to $\{(0, 1, 1), (1, 0, 1), (1, 1, 0)\}$. 

21
\[ 6(q^2 - q) \text{ degenerate Hermitian curves of type} \]
\[
(1 - \alpha^3)X_1^2X_2 - (1 - \alpha)\alpha^qX_1X_2^q - (1 - \alpha^q)X_1^qX_3 + (1 - \alpha)X_1X_3^q = 0, \\
(1 - \alpha)\alpha^qX_1^2X_2 - (1 - \alpha^q)\alpha X_1X_2^q + (1 - \alpha^q)X_2^qX_3 - (1 - \alpha)X_2X_3^q = 0, \\
(1 - \alpha)\alpha^qX_1^2X_3 - (1 - \alpha^q)\alpha X_1X_3^q - (1 - \alpha)X_2^qX_3 + (1 - \alpha^q)X_2X_3^q = 0, \tag{3.3}
\]
\[
\alpha^{q+1}(X_1^2X_2 - X_1X_2^q) - \alpha^qX_1^3X_3 + \alpha X_1X_2^qX_3 + \alpha^qX_2^qX_3 - \alpha X_2X_3^q = 0, \\
\alpha^qX_1^2X_2 - \alpha X_1X_2^q - \alpha^{q+1}(X_1^qX_3 - X_1X_3^q) + \alpha X_2^qX_3 - \alpha^qX_2X_3^q = 0, \\
\alpha X_1^3X_2 - \alpha^qX_1X_2^q + \alpha^qX_1X_3^q + \alpha^{q+1}(X_2^qX_3 - X_2X_3^q) = 0, \alpha \in \text{GF}(q^2) \setminus \text{GF}(q). \tag{3.4}
\]

They meet \( \pi \) in \( 2q + 1 \) points and their vertices are not in \( \pi \) and on some line secant to \( \bar{P} \).

\bullet \quad (q - 2)(q^2 - q) \text{ degenerate Hermitian curves of type} \]
\[
(1 - \delta)t^qX_1^qX_2 - (1 - \delta)tX_1X_2^q - (1 - \delta)tX_1X_3 - (1 - \delta)X_1X_3^qX_3 + (1 - \delta)tX_2^qX_3 - (1 - \delta)X_2X_3^q = 0, \\
\delta \in \text{GF}(q) \setminus \{0, 1\}, t \in \text{GF}(q^2) \setminus \text{GF}(q). \tag{3.4}
\]

They meet \( \pi \) in \( q + 1 \) points and their vertices are not in \( \pi \) and on \( q - 2 \) non-degenerate conics of PG(2, \( q^2 \)).

**Lemma 3.10.** There exists at least a degenerate Hermitian curve of PG(2, \( q^2 \)) passing through six points.

**Proof.** Consider a set of six points of PG(2, \( q^2 \)). If there were not four points out of the six points no three on a line, then these six points would lie on at most three concurrent lines and hence on at least a degenerate Hermitian curve of PG(2, \( q^2 \)). Thus we may assume that there are four points no three of them on a line and, by the action of PGL(3, \( q^2 \)), that these four points are those of \( \bar{P} \). Let \( P \) and \( Q \) be the remaining two points. If at least one of the points \( P \) and \( Q \) lies in \( \pi \), then there will be at least one degenerate Hermitian curve of type \( [3.1] \) containing the six points. Assume that \( P, Q \notin \pi \) and let \( \ell_P \) and \( \ell_Q \) be the lines of PG(2, \( q^2 \)) containing \( P \) and \( Q \), respectively, and meeting the Baer subplane \( \pi \) in \( q + 1 \) points. Then \( |\ell_P \cap \ell_Q \cap \pi| \geq 1 \). In this case the degenerate Hermitian curve of type \( [3.1] \) having as vertex a point of \( \ell_P \cap \ell_Q \) and containing \( \ell_P \) and \( \ell_Q \) will contain the six points. \( \Box \)

**Corollary 3.11.** A set of points of PG(2, \( q^2 \)) not contained in a degenerate Hermitian curve of PG(2, \( q^2 \)) has at least seven points.

### 3.1.1 Seven lines of PG(5, \( q \)) in higgledy–piggledy arrangement

In this section we obtain a set of seven points of PG(2, \( q^2 \)) not contained in a degenerate Hermitian curve of PG(2, \( q^2 \)) and hence, as a by product, a set of seven lines of PG(5, \( q \)) in higgledy–piggledy arrangement.
Let $G$ be the group of projectivities of order three generated by

\[
\begin{pmatrix}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0
\end{pmatrix}.
\]

Then the group $G$ fixes $P_1$ and permutes in a unique orbit the remaining three points of $\bar{P}$. Note that since the group $G$ fixes $\bar{P}$, then the set of degenerate Hermitian curves of each of the four types described above is preserved by $G$.

Let $P_5 = (1, x, \xi x)$, with $x \in GF(q) \setminus \{0\}, \xi \in GF(q^2)$ and let

\[ P_{x, \xi} = \bar{P} \cup P^G_5, \quad \text{where} \quad P^G_5 = \{(1, x, \xi x), (\xi x, 1, x), (x, \xi x, 1)\}. \tag{3.5} \]

Our aim is to determine the existence of $x$ and $\xi$ such that $|P_{x, \xi}| = 7$ and no degenerate Hermitian curve containing $\bar{P}$ contains $P_{x, \xi}$. Let $H$ be a degenerate Hermitian curve containing $\bar{P}$. Assume first that $H$ is defined by one of the Equations of (3.1) for some $a, b \in GF(q)$. Straightforward calculations show that if

\[ x^3 \neq 1 \text{ and } \xi^q \neq \xi, \tag{3.6} \]

then $P_{x, \xi} \not\subset H$. Let $H$ be defined by one of the equations of (3.2) for some $\alpha \in GF(q^2) \setminus \{1\}$, with $\alpha^{q+1} = 1$ or by one of the equations of (3.3) for some $\alpha \in GF(q^2) \setminus GF(q)$. In this case it can be seen that if either

\[ x \neq \pm 1 \text{ and } \xi \notin \left\{ \frac{\alpha - x}{x(\alpha - 1)} \mid \alpha^{q+1} = 1, \alpha \neq \pm 1 \right\} \cup \left\{ \frac{-1}{\alpha^q(1 + x)} \mid \alpha^{q+1} + \alpha^q + \alpha = 0, \alpha \neq 0, -2 \right\}, \tag{3.7} \]

or

\[ q \text{ is odd, } x = -1 \text{ and } \xi \notin \left\{ \frac{1 + \alpha}{1 - \alpha} \mid \alpha^{q+1} = 1, \alpha \neq \pm 1 \right\}, \tag{3.8} \]

then $P_{x, \xi} \not\subset H$. Assume now that either Conditions (3.6) and (3.7) or (3.6) and (3.8) hold true and that $H$ is given by Equation (3.4), for some $\delta \in GF(q) \setminus \{0, 1\}$ and $t \in GF(q^2) \setminus GF(q)$. Put

\[
\begin{align*}
A & := A(\delta, t) = t^q (1 - \delta - (1 - \delta t)x), \\
B & := B(\delta, t) = 1 - \delta t - (1 - \delta t)x, \\
C & := C(\delta, t) = \delta (t^q - t), \\
D & := D(\delta, t) = t - t^q, \\
E & := E(\delta, t) = (t - x)(1 - \delta t^q).
\end{align*}
\]

Suppose that $P_{x, \xi} \subset H$, then the following equations are satisfied.

\[
\begin{align*}
\xi^q E - \xi E^q - C - D &= 0 \\
\xi^q A - \xi A^q + C &= 0 \\
\xi^q B - \xi B^q + D &= 0.
\end{align*}
\tag{3.9}
\]

Note that $A + B + E = (x - 1)(\delta t^{q+1} + (\delta - 1)(t^q + t) - 1) \in GF(q)$ and hence summing up the three equations we get $(\xi^q - \xi)(x - 1)(\delta t^{q+1} + (\delta - 1)(t^q + t) - 1) = 0$. Moreover $A \neq 0$, since
Let \( t \in \text{GF}(q^2) \setminus \text{GF}(q) \). Then the previous system can be rewritten as follows:

\[
\begin{cases}
\delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\
\xi^q = (\xi A^q - C)/A \\
\xi (A^q B - AB^q) + AD - BC = 0.
\end{cases}
\]  

(3.10)

Note that \( A^q B - AB^q = 0 \) yields \( AD - BC = 0 \). Also, \((A^q B - AB^q, AD - BC) = (0, 0)\) if and only if \( A = -\delta B \), i.e.,

\[\delta xt^{q+1} + (1 - \delta - x)t^q + \delta ((\delta - 1)x - \delta) t + \delta = 0.\]

**Lemma 3.12.** For every \( x \in \text{GF}(q) \setminus \{0\} \) such that \( x^3 \neq 1 \), there are no \( \delta \in \text{GF}(q) \setminus \{0, 1\} \) and \( t \in \text{GF}(q^2) \setminus \text{GF}(q) \) such that

\[
\begin{cases}
\delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\
\delta xt^{q+1} + (1 - \delta - x)t^q + \delta ((\delta - 1)x - \delta) t + \delta = 0.
\end{cases}
\]  

(3.11)

Proof. By multiplying the first equation by \( x \) and by subtracting the second equation from it, we get

\[
\begin{cases}
\delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\
((1 + x)\delta - 1) t^q + \delta^2(1-x) + 2\delta x - x) t - x - \delta = 0.
\end{cases}
\]  

(3.11)

If \( x \neq -1 \) and \( \delta = 1/(x + 1) \), then from the second equation of (3.11) we have that \( t = \frac{(x+1)^3}{1-x} \in \text{GF}(q) \), a contradiction. Hence, from [25, Corollary 1.24], the second equation of (3.11) admits solutions in \( t \) if and only if \( \frac{\delta^2 (1-x) + 2\delta x - x}{1 - (1 + x)\delta} = -1 \), i.e., \( \delta^2 - \delta + 1 = 0 \). Therefore assume that \( q \not\equiv -1 \pmod{3} \) and \( \delta^2 = \delta - 1 \). In this case (3.11) reads

\[
\begin{cases}
t^{q+1} = -\delta \\
t^q + t = 1 - \delta,
\end{cases}
\]  

which in turn is equivalent to the following quadratic equation in \( t \)

\[t^2 + (\delta - 1)t - \delta = 0.\]  

(3.12)

If \( q \) is odd, (3.12) has one or two solutions according as \( \delta = -1 \) or \( \delta \neq -1 \) and these solutions are in \( \text{GF}(q) \). If \( q \) is even, note that \( \frac{\delta}{\delta + 1} = \frac{\delta^2 + 1}{\delta^2 + 1} = 1 \), where \( \text{Tr}_{q^2|2}(1) = 0 \), since \( q \not\equiv -1 \pmod{3} \). It follows that (3.12) has two solutions and these solutions are in \( \text{GF}(q) \). The proof is now complete.

By Lemma 3.12 we can assume \( A^q B - AB^q \neq 0 \) and so (3.10) reads

\[
\begin{cases}
\delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\
\xi = \frac{BC - AD}{A^q B - AB^q}.
\end{cases}
\]  

(3.13)

Note that if \( \omega = (\bar{x}, \bar{\xi}, \bar{\delta}, t) \) is a solution of (3.13) then

\[
\omega' = \left( \bar{x}, \bar{\xi}, \frac{\bar{\delta} - 1}{\bar{\delta}}, \frac{1 - \bar{\delta} t}{1 - \bar{\delta} t} \right) \quad \text{and} \quad \omega'' = \left( \bar{x}, \bar{\xi}, \frac{1}{1 - \bar{\delta}}, \frac{1 - \bar{\delta} t}{1 - \bar{\delta} t} \right)
\]
are solutions of (3.13) too. Also, \( \omega = \omega' \) yields \((1 - \delta)t^2 + \delta t - 1 = ((1 - \delta)t + 1)(t - 1) = 0 \) and \( t \in \text{GF}(q) \), a contradiction. Similarly, if \( \omega = \omega'' \) or \( \omega' = \omega'' \), then \( \delta t^2 - t + 1 - \delta = (\delta t - 1 + \delta)(t - 1) = 0 \) or \( \delta^2 t^2 - (\delta^2 + 1)t + 1 = (\delta^2 t - 1)(t - 1) = 0 \) and \( t \in \text{GF}(q) \), a contradiction. Let

\[
\Sigma = \{(\delta, t) \in (\text{GF}(q) \setminus \{0, 1\}, \text{GF}(q^2) \setminus \text{GF}(q)) \mid \delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0\}.
\]

It is readily seen that \( |\Sigma| \leq q^2 \).

**Theorem 3.13.** There exist \((x, \xi) \in \text{GF}(q) \setminus \{0, 1\} \times \text{GF}(q^2) \setminus \text{GF}(q)\) such that \( \mathcal{P}_{x, \xi} \) is a set of seven points and no degenerate Hermitian curve of PG(2, \( q^2 \)) contains it.

**Proof.** Fix \( x \in \text{GF}(q) \setminus \{0\} \), with \( x^3 \neq 1 \). We show the existence of an element \( \xi \in \text{GF}(q^2) \setminus \text{GF}(q) \) such that no degenerate Hermitian curve containing \( \mathcal{P} \) contains \( \mathcal{P}_{x, \xi} \), where \( \mathcal{P}_{x, \xi} \) is defined as in (3.5). Since Condition (3.6) is satisfied, taking into account Condition (3.7) or (3.8), we have that the number of values that \( \xi \) cannot assume is at most \( \frac{|\Sigma|}{3} - 2q \) if \( q \) is even and \( \frac{|\Sigma|}{3} - 2(q - 1) \) if \( q \) is odd. Indeed,

\[
\left| \left\{ \frac{\alpha - x}{x(\alpha - 1)} \mid \alpha^{q+1} = 1, \alpha \neq \pm 1 \right\} \right| = \begin{cases} q - 1 & \text{if } q \text{ is odd,} \\ q & \text{if } q \text{ is even,} \end{cases}
\]

and, if \( x \neq -1 \),

\[
\left| \left\{ \frac{-1}{\alpha^{q}(1 + x)} \mid \alpha^{q+1} + \alpha^q + \alpha = 0, \alpha \neq 0, -2 \right\} \right| = \begin{cases} q - 1 & \text{if } q \text{ is odd,} \\ q & \text{if } q \text{ is even.} \end{cases}
\]

Since in both cases the number of forbidden values for \( \xi \) is less than \( q^2 - q \), we have the assertion. \( \square \)

**Proposition 3.14.** Let \( \mathcal{P}_{x, \xi} \) be defined as in Theorem 3.13. No three points of \( \mathcal{P}_{x, \xi} \) are on a line of PG(2, \( q^2 \)).

**Proof.** Assume by contradiction that three points of \( \mathcal{P}_{x, \xi} \) are on a line of PG(2, \( q^2 \)). Then the determinant of the 3 \( \times \) 3 matrix whose rows are the coordinates of these points must be zero. Straightforward computations show that either \( \xi \) belongs to \( \text{GF}(q) \) or \( x \in \{0, 1\} \) and we have a contradiction from (3.16), or one of the following possibilities occurs:

\[
x^2 \xi^2 - x(x + 1)\xi + x^2 - x + 1 = 0, \quad (3.14)
\]

\[
\xi^2 = \frac{1}{x}. \quad (3.15)
\]

If (3.14) were satisfied, then either \( q \not\equiv -1 \pmod{3} \) and \( \xi \) should be in \( \text{GF}(q) \) or \( q \equiv -1 \pmod{3} \) and \( \xi \) should be equal to \( \frac{\alpha - x}{x(\alpha - 1)} \) for some \( \alpha \in \text{GF}(q^2) \setminus \text{GF}(q) \), with \( \alpha^2 - \alpha + 1 = 0 \) (and hence \( \alpha^{q+1} = 1 \)). From (3.6), (3.7), (3.8), in both cases we have a contradiction.

Suppose that (3.15) is satisfied. Then \( q \) has to be odd and \( x \) is non-square in \( \text{GF}(q) \). Let \( x \neq -1 \), otherwise \( q \equiv -1 \pmod{4} \) and as before \( \xi = \frac{1 + \alpha}{1 - \alpha} \), for some \( \alpha \in \text{GF}(q^2) \setminus \text{GF}(q) \), with \( \alpha^2 = -1 \) (and hence \( \alpha^{q+1} = 1 \)). We will show that there exists a degenerate Hermitian curve given by (3.3) containing \( \mathcal{P}_{x, \xi} \) and hence contradicting Theorem 3.13. Note that \( \xi^q = -\xi \). From
From (3.17), by using (3.18), it follows that if the latter case occurs, then

\[ \delta \]

By substituting (3.20) in Equation (3.19), after some calculations, we get

\[ (3.9) \], this implies that \( A + A^q \neq 0 \) and \( B + B^q \neq 0 \), otherwise \( C = 0 \) or \( D = 0 \), contradicting the fact that \( t \in GF(q^2) \setminus GF(q) \) and \( \delta \neq 0 \). From the second equation of (3.10), we have that

\[ \xi = \frac{C}{A + A^q} \]

where

\[ t \]

as \( x \) is a solution of (3.13). Moreover

\[ t^q + 1 = \frac{2(x + \delta)}{F(\delta)} \]

(3.17)

Equation (3.16) gives

\[ 2(x + \delta) + (t + t^q)F(\delta) = 0, \]

where \( F(\delta) = \delta^2(x - 1) - \delta(3x + 1) + x + 1. \)

Let \( x = -\delta \). Thus \( F(\delta) = F(-x) = (x + 1)(x^2 + x + 1) \neq 0 \), since \( x \neq -1 \) and \( x^3 \neq 1 \). It follows that \( t^q = -t \) and, from the first equation of (3.10), \( t^q + 1 = -\frac{1}{x} \). Therefore \( \xi = \frac{t + t^q}{2} = t \), where \( t^2 = \frac{1}{x} \) and \( (x, \xi, -x, \xi) \) is a solution of (3.13). Let \( x \neq -\delta \). Thus \( F(\delta) \neq 0 \). Moreover

\[ t + t^q = \frac{-2(x + \delta)}{F(\delta)}, \]

(3.18)

Observe that, from (3.17), \( t - t^q = \frac{2(x + \delta)}{F(\delta)} + 2t \) and by substituting it together with (3.17) into Equation (3.16), we have

\[ x^2 F(\delta)^2 + 2tx F(\delta)(x + \delta) + x(x + \delta)^2 = (F(\delta) + (x + \delta)(x - \delta x + \delta))^2. \]

(3.19)

From (3.17), by using (3.18), it follows that

\[ t^2 = \frac{-2t(2x + 1) + 2(\delta - 1)(x + \delta) + F(\delta)}{\delta F(\delta)}. \]

(3.20)

By substituting (3.20) in Equation (3.19), after some calculations, we get

\[ \delta^{-1} \frac{x(x + \delta)(x^2 - 1)(\delta - 1)}{x} \left( \delta - \frac{x + 1}{x} \right) \left( \delta - \frac{1}{x + 1} \right) = 0, \]

(3.21)

that is \( \delta = \frac{x + 1}{x} \) or \( \delta = \frac{1}{x + 1} \). In the former case \( \left( x, \xi, \frac{x + 1}{x}, \frac{x + \sqrt{7}}{x + 1} \right) \) is a solution of (3.13), whereas if the latter case occurs, then \( \left( x, \xi, \frac{1}{x + 1}, \frac{(x + 1)(-1 + \sqrt{7})}{x - 1} \right) \) is a solution of (3.13).

By construction the seven points obtained are left invariant by a group of order three.

**Theorem 3.15.** Let \( P_{x, \xi} \) be defined as in Theorem 3.13. The set \( \phi(P_{x, \xi}) = \{ \phi(P) \mid P \in P_{x, \xi} \} \) consists of seven lines of \( PG(5, q) \) in higgledy–piggledy arrangement.
Let $B$ be the set of $7(q+1)$ points of $\text{PG}(5,q)$ on the seven mutually skew lines $\ell_i$, $1 \leq i \leq 7$, constructed in the previous theorem.

**Proposition 3.16.** The set $B$ is a minimal cutting blocking set of $\text{PG}(5,q)$.

**Proof.** We only need to show the minimality of $B$. Let $P$ be a point of $B$ and let $\ell_k$ be the line containing $P$, for a fixed $k \in \{1, \ldots, 7\}$. By Lemma 3.10 there are $q+1$ solids of $\text{PG}(5,q)$, $\Pi_i$, $1 \leq i \leq q+1$, such that each of the lines $\ell_j$, $1 \leq j \leq 7$, $j \neq k$, has at least one point in common with $\Pi_i$, $1 \leq i \leq q+1$. Moreover, from Theorem 3.15, $|\ell_k \cap \Pi_i| = 0$, $1 \leq i \leq q+1$. Let $\Gamma_i$ be the hyperplane spanned by $\Pi_i$ and $P$. Then there are at most six indices $i_1, \ldots, i_6$ such that $\Gamma_i \cap B \not\subset \Pi_i$. Hence if $q > 5$, there exists a hyperplane $\Gamma_{i'}$, $1 \leq i' \leq q+1$, $i' \notin \{i_1, \ldots, i_6\}$, such that $\Gamma_{i'} \cap B \subset \Pi_{i'}$. If $q \leq 5$, then some computations performed with Magma [10] confirm the statement.

**Proposition 3.17.** To the set $B$ there corresponds a $[7(q+1), 6]_q$ reduced minimal linear code with weights $5q$, $6q$ and $7q$ and weight distribution $A_{5q} = 21(q^2 - 1)$, $A_{6q} = 7(q^2 - 5)(q^2 - 1)$ and $A_{7q} = (q^4 - 6q^2 + 15)(q^2 - 1)$.

**Proof.** A hyperplane $\Gamma$ of $\text{PG}(5,q)$ contains exactly $q^2 + 1$ lines of the Desarguesian line–spread $D$ of $\text{PG}(5,q)$ and they are contained in a unique solid, say $\Pi$, where $\phi^{-1}(\Pi)$ is a line, say $\ell$, of $\text{PG}(2,q^2)$. From Proposition 3.14 $|\ell \cap \mathcal{P}| \leq 2$ and hence at most two lines out of the seven lines $\{\ell_i \mid 1 \leq i \leq 7\}$ are contained in $\Gamma$. In particular, there are 21 lines of $\text{PG}(2,q^2)$ meeting $\mathcal{P}$ in two points, $7(q^2 - 5)$ lines of $\text{PG}(2,q^2)$ intersecting $\mathcal{P}$ in one point and the remaining $q^4 - 6q^2 + 15$ lines do not share any point with $\mathcal{P}$. Hence there are $21(q+1)$ hyperplanes $\Gamma$ of $\text{PG}(5,q)$ such that $|\Gamma \cap B| \leq 2(q+1)+5$, $7(q^2 - 5)(q+1)$ hyperplanes $\Gamma$ of $\text{PG}(5,q)$ such that $|\Gamma \cap B| = (q+1)+6$ and $(q^4 - 6q^2 + 15)(q+1)$ hyperplanes $\Gamma$ of $\text{PG}(5,q)$ such that $|\Gamma \cap B| = 7$.

**Acknowledgments.** This work was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA–INdAM).

**References**

[1] G.N. Alfarano, M. Borello, A. Neri, A geometric characterization of minimal codes and their asymptotic performance, *Adv. Math. Commun.*, doi:10.3934/amc.2020104.

[2] G.N. Alfarano, M. Borello, A. Neri, A. Ravagnani, Three Combinatorial Perspectives on Minimal Codes, *arXiv:2010.16339*.

[3] R.D. Baker, J.M.N. Brown, G.L. Ebert, J.C. Fisher, Projective bundles, *Bull. Belg. Math. Soc. Simon Stevin*, 1, (1994), no. 3, 329–336.

[4] D. Bartoli, G. Kiss, S. Marcugini, F. Pambianco, Resolving sets for higher dimensional projective spaces, *Finite Fields Appl.*, 67, (2020), 101723.

[5] D. Bartoli, G. Micheli, G. Zini, F. Zullo, $r$-fat linearized polynomials over finite fields, submitted.
[6] S.G. Barwick, Wen-Ai Jackson, An investigation of the tangent splash of a subplane of PG(2,q³), *Des. Codes Cryptogr.*, 76, (2015), no. 3, 451–468.

[7] S.G. Barwick, Wen-Ai Jackson, Exterior splashes and linear sets of rank 3, *Discrete Math.*, 339, (2016), no. 5, 1613–1623.

[8] S.G. Barwick, Wen-Ai Jackson, The exterior splash in PG(6,q): carrier conics, *Adv. Geom.*, 17, (2017), no. 4, 407–422.

[9] M. Bonini, M. Borello, Minimal linear codes arising from blocking sets, *J. Algebraic Combin.*, https://doi.org/10.1007/s10801-019-00930-6.

[10] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, 24, (1997), 235–265.

[11] A.A. Bruen, Intersection of Baer subgeometries, *Arch. Math.*, 39, (1982), no. 3, 285–288.

[12] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes*, North–Holland, Amsterdam, 1997.

[13] A.A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco, Linear nonbinary covering codes and saturating sets in projective spaces, *Adv. Math. Commun.*, 5, (2011), no. 1, 119–147.

[14] A.A. Davydov, S. Marcugini, F. Pambianco, New covering codes of radius R, codimension tR and tR + \frac{t^2}{2}, and saturating sets in projective spaces, *Des. Codes Cryptogr.*, 87, (2019), no. 12, 2771–2792.

[15] U. Dempwolff, A note on the Figueroa planes, *Arch. Math.*, 43, (1984), 285–288.

[16] L. Denaux, Constructing saturating sets in projective spaces using subgeometries, *arXiv:2008.13459*.

[17] G. Donati, N. Durante, On the intersection of a Hermitian curve with a conic, *Des. Codes Cryptogr.*, 57, (2010), no. 3, 347–360.

[18] G. Donati, N. Durante, Scattered linear sets generated by collineations between pencils of lines, *J. Algebr. Combin.*, 40, (2014), 1121–1134.

[19] K. Drudge, On the orbits of Singer groups and their subgroups, *Electron. J. Combin.*, 9, (2002), no. 1, Paper 15, 10 pp.

[20] S.L. Fancsali, P. Sziklai, Lines in higgledy–piggledy arrangement, *Electron. J. Combin.*, 21, (2014), no. 2, Paper 2.56, 15 pp.

[21] S. Ferret, L. Storme, Results on maximal partial spreads in PG(3,p³) and on related minihypers, *Des. Codes Cryptogr.*, 29, (2003), 105–122.

[22] D. Glynn, On a set of lines of PG(3,q) corresponding to a maximal cap contained in the Klein quadric of PG(5,q), *Geom. Dedicata*, 26 (1988), no. 3, 273–280.
[23] T. Héger, B. Patkós, M. Takáts, Search problems in vector spaces, Des. Codes Cryptogr., 76, (2015), no. 2, 207–216.

[24] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1985.

[25] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1998.

[26] J.W.P. Hirschfeld, J.A. Thas, *General Galois geometries*, Springer Monographs in Mathematics, Springer, London, 2016.

[27] D.R. Hughes, F.C. Piper, *Projective planes*, Vol. 6. Springer-Verlag, New York-Berlin, 1973.

[28] M. Lavrauw, G. Van de Voorde, On linear sets on a projective line, Des. Codes Cryptogr., 56, (2010), no. 2-3, 89–104.

[29] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986.

[30] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Maximum scattered linear sets of pseudoregulus type and the Segre Variety $S_{n,n}$, J. Algebr. Combin., 39, (2014), 807–831.

[31] Lunardon, Polverino, Translation ovoids of orthogonal polar spaces, Forum Math., 16, (2004), 663–669.

[32] C. Tang, Y. Qiu, Q. Liao, Z. Zhou, Full Characterization of Minimal Linear Codes as Cutting Blocking Sets, arXiv:1911.09867v2.

[33] M. Tsfasman, S. Vlăduţ, D. Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs, 139. American Mathematical Society, Providence, RI, 2007.