On cutting blocking sets and their codes

Daniele Bartoli Antonio Cossidente Giuseppe Marino Francesco Pavese

Abstract

Let $\mathrm{PG}(r,q)$ be the r–dimensional projective space over the finite field $\mathrm{GF}(q)$. A set $\mathcal{X}$ of points of $\mathrm{PG}(r,q)$ is a cutting blocking set if for each hyperplane Π of $\mathrm{PG}(r,q)$ the set $\Pi \cap \mathcal{X}$ spans Π. 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 $\mathrm{PG}(3,q^3)$ of size $3(q+1)(q^2+1)$ as a union of three pairwise disjoint q–order subgeometries and a cutting blocking set of $\mathrm{PG}(5,q)$ of size $7(q+1)$ from seven lines of a Desarguesian line spread of $\mathrm{PG}(5,q)$. 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 $\mathrm{PG}(r,q)$ be the r–dimensional projective space over the finite field $\mathrm{GF}(q)$. We will denote by $(X_1, X_2, \ldots, X_{r+1})$ the homogeneous projective coordinates of a point of $\mathrm{PG}(r,q)$. A set $\mathcal{X}$ of points of $\mathrm{PG}(r,q)$ is said to be a *t–fold blocking set* if every hyperplane of $\mathrm{PG}(r,q)$ meets $\mathcal{X}$ in at least t points.

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

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 Π of $\mathrm{PG}(r,q)$ is spanned by $\Pi \cap \mathcal{X}$

D. Bartoli: Dipartimento di Matematica e Informatica, Università di Perugia, Perugia, Italy; *e-mail*: daniele.bartoli@unipg.it

A. Cossidente: Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Contrada Macchia Romana, 85100, Potenza, Italy; *e-mail*: antonio.cossidente@unibas.it

G. Marino: Dipartimento di Matematica e Applicazioni "Renato Caccioppoli", Università degli Studi di Napoli "Federico II", Complesso Universitario di Monte Sant'Angelo, Cupa Nuova Cintia 21, 80126, Napoli, Italy; *e-mail*: giuseppe.marino@unina.it

F. Pavese: Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, Via Orabona 4, 70125 Bari, Italy; *e-mail*: francesco.pavese@poliba.it

Mathematics Subject Classification (2020): Primary 51E21; 94B05. Secondary 94B25; 51E20.

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 [1, 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 $\mathrm{PG}(r,q)$, called ρ–saturating sets, were studied.

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

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

Definition 1.3. *Let $\mathcal{L}$ be a lineset of $\mathrm{PG}(r,q)$. The lines of $\mathcal{L}$ are said to be in* higgledy–piggledy arrangement *if the set of points covered by the lines of $\mathcal{L}$ 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 $\mathrm{PG}(2,q)$ this number is three and it is known that in $\mathrm{PG}(3,q)$ the smallest set of lines in higgledy–piggledy arrangement has to contain four (pairwise disjoint) lines; see [20]. In $\mathrm{PG}(4,q)$, if q is large enough, it is possible to find a set of six pairwise disjoint lines in higgledy–piggledy arrangement [4, Proposition 12]. More generally, it is known that a set of lines of $\mathrm{PG}(r,q)$ in higgledy–piggledy arrangement has to contain at least $\lfloor \frac{r}{2} \rfloor + r$ 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 $\mathrm{PG}(r,q)$ of size at most $(2r-1)(q+1)$. Thus

$$\frac{r}{e}q + \frac{r-1}{2} \leq \boldsymbol{s}_{q^r}(r,r-1) \leq (2r-1)(q+1),$$

which improves on the known upper bounds for the size of the smallest saturating set whenever $r \geq 6$. 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 $\mathrm{PG}(3,q^3)$ there exists a minimal cutting blocking set of size $3(q+1)(q^2+1)$.*

(ii) In $\mathrm{PG}(5,q)$ 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 $\mathrm{PG}(3,q^3)$ 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 $\mathrm{PG}(5,q)$ in higgledy–piggledy arrangement. There arises a minimal cutting blocking set of $\mathrm{PG}(5,q)$ 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 $\mathrm{PG}(3,q^9)$ and of a 4–saturating set of $\mathrm{PG}(5,q^5)$ if $q>2$:

$$\frac{3}{e}q^3+1 \le \boldsymbol{s}_{q^9}(3,2) \le 3(q+1)(q^2+1),$$
$$\frac{5}{e}q+2 \le \boldsymbol{s}_{q^5}(5,4) \le 7(q+1).$$

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 $u=(u_1,\dots,u_n)\in \mathrm{GF}(q^n)$, its *support* is the set $supp(u)=\{i \mid u_i\neq 0\}$ and the *Hamming weight* $w(u)$ of u is the cardinality of its support. The *Hamming distance* on $\mathrm{GF}(q)^n$ is defined as $d(u,v)=|supp(u-v)|$, for every pair of vectors $u,v\in\mathrm{GF}(q)$. A *q–ary linear code* of dimension k and length n, or an $[n,k]_q$ code, $\mathcal{C}$ is a k–dimensional vector subspace of $\mathrm{GF}(q)^n$. The elements of $\mathcal{C}$ are called *codewords*. A *generator matrix* of $\mathcal{C}$ is a matrix whose rows form a basis of $\mathcal{C}$ as a vector space over $\mathrm{GF}(q)$. The *minimum distance of* $\mathcal{C}$ is $d=\min\{w(u) \mid u\in\mathcal{C}, u\neq 0\}$. Let $u,v\in\mathrm{GF}(q)^n$. The vector u is *ρ–covered by v* if $d(u,v)\le\rho$. The *covering radius* of a code $\mathcal{C}$ is the smallest integer ρ such that every vector of $\mathrm{GF}(q^n)$ if ρ–covered by at least one codeword of $\mathcal{C}$. If d or ρ are needed, then $\mathcal{C}$ is said to be an $[n,k,d]_q$ code or an $[n,k]_q\rho$ code. The weight distribution of $\mathcal{C}$ is the sequence $A_0(\mathcal{C}),\dots,A_n(\mathcal{C})$, where $A_i(\mathcal{C})=|\{u\in\mathcal{C} \mid w(u)=i\}|$. For $u=(u_1,\dots,u_n), v=(v_1,\dots,v_n)\in\mathrm{GF}(q)^n$, let $u\cdot v=\sum_{i=1}^n u_iv_i$ be the Euclidean inner product between u and v. For a code $\mathcal{C}$, its *dual code* is $\mathcal{C}^\perp=\{v\in\mathrm{GF}(q)^n \mid v\cdot c=0,\forall c\in\mathcal{C}\}$. The dimension of the dual code $\mathcal{C}^\perp$ or the codimension of $\mathcal{C}$ is $n-k$. Any matrix which is a generator matrix of $\mathcal{C}^\perp$ is called a *parity check matrix* of $\mathcal{C}$. If $\mathcal{C}$ is a linear $[n,k]_q\rho$ code, with parity check matrix N, its covering radius is the smallest ρ such that every $w\in\mathrm{GF}(q)^{n-k}$ can be written as a linear combination of at most ρ 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 $\mathrm{PG}(r,q)$ can be considered as columns of a parity check matrix of a q–ary linear code of codimension $r+1$. In particular, a ρ–saturating set of $\mathrm{PG}(r,q)$ of size n corresponds to a parity check matrix of an $[n,n-(r+1)]_q(\rho+1)$ code; see [13, 14] and references therein.

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

minimal.

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

$$d = n - \max\{|H \cap \mathcal{Z}| \quad : \quad H \text{ hyperplane of } \mathrm{PG}(r, q)\}.$$

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 $\mathrm{PG}(r, q)$ represented by the columns of a generator matrix M of an $[n, r+1]_q$ code form a set of n points (counted with multiplicity) of $\mathrm{PG}(r, q)$. Viceversa, the code generated by the matrix having the representatives of the points of a projective $[n, r+1, d]_q$ system $\mathcal{Z}$ as columns, gives an $[n, r+1]_q$ linear code. Moreover, for any non–zero vector $u = (u_1, u_2, \ldots, u_{r+1}) \in \mathrm{GF}(q)^{r+1}$, the hyperplane of $\mathrm{PG}(r, q)$ with equation $u_1X_1 + u_2X_2 + \cdots + u_{r+1}X_{r+1} = 0$ contains $|\mathcal{Z}| - w$ points of $\mathcal{Z}$ 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 $[n, r+1]_q$ linear codes are equivalent to minimal cutting blocking sets of $\mathrm{PG}(r, q)$ of size n; see [1, 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 [1, Problem 2], [2], and [32, Open Problem 24]. In this regard, if $\boldsymbol{m}(r+1, q)$ 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 $\mathrm{PG}(r, q)$, $q > 2r-1$, in hyggledy–piggledy arrangement provided in [20], the following upper bound can be derived:

$$r(q+1) \leq \boldsymbol{m}(r+1, q) \leq (2r-1)(q+1).$$

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:

$$\begin{array}{rll} 3(q^3+1) \leq \boldsymbol{m}(4, q^3) \leq 3(q+1)(q^2+1), & & \text{see Theorem 2.26;} \\ 5(q+1) \leq \boldsymbol{m}(6, q) \leq 7(q+1), & & \text{see Proposition 3.16.} \end{array}$$

2 Cutting blocking sets from subgeometries

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

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

Here we consider certain pointsets of $\mathrm{PG}(1, q^3)$, 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* $\mathrm{PG}(2,q^3)$*, let* π_0 *be a* q*–order subplane and let* H *be the stabilizer of* π_0 *in* $\mathrm{PGL}(3,q^3)$*. The group* H *has three orbits on the points of* $\mathrm{PG}(2,q^3)$*:*

- π_0*;*
- $\mathcal{O}_2'$ *consisting of the* $q(q^2-1)(q^2+q+1)$ *points of* $\mathrm{PG}(2,q^3)$ *lying on exactly one extended subline of* π_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* $\mathrm{PG}(2,q^3)$*:*

- *the* q^2+q+1 *extended sublines of* π_0*;*
- $\mathcal{L}_2'$ *consisting of the* $q(q^2-1)(q^2+q+1)$ *lines of* $\mathrm{PG}(2,q^3)$ *intersecting* π_0 *in one point;*
- *their complement* $\mathcal{L}_3'$ *of size* $q^3(q-1)(q^2-1)$ *formed by lines disjoint from* π_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 π_0 containing R_1, and let R_2 be a point of $\mathcal{O}_3'$. In geometric terms, a club of $\mathrm{PG}(1,q^3)$ can be defined in two distinct ways.

i) By extension. By extending the sublines of π_0 to lines of $\mathrm{PG}(2,q^3)$ and intersecting these with the line ℓ_1, one obtains a *club of* ℓ_1 *with head* $\ell_1 \cap \pi_0$.

ii) By projection. By projecting the points of π_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 $\mathrm{PG}(1,q^3)$ are projectively equivalent.
- A club of $\mathrm{PG}(1,q^3)$ 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 π_0 through a point of π_0 or from a subline of π_0 according as the club is obtained by extension or by projection, respectively.

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

i) By extension. By extending the sublines of π_0 to lines of $\mathrm{PG}(2,q^3)$ and intersecting these with the line ℓ_2, one obtains a *splash of* ℓ_2.

ii) By projection. By projecting the points of π_0 from R_2 onto a line m not containing R_2, one obtains a *splash of* m.

A splash has the following properties.

- All splashes of $\mathrm{PG}(1,q^3)$ are projectively equivalent.
- A splash of $\mathrm{PG}(1,q^3)$ 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 π_0 through a point of π_0 or from a subline of π_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 π_0 of a dual subconic of π_0 or from a subconic of π_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 $\mathrm{PGL}(2,q^3)$ 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 $\mathrm{PG}(1,q^3)$ that will be used in the paper.

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

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

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

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

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

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

If $z\in \mathrm{GF}(q)$ or $z=x+a$, where $a\in \mathrm{GF}(q)$, 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

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

where

$$\begin{aligned} r_\xi &= \{(\xi(x+a)-\xi^q(x^q+a), x\xi^q(x^q+a)-x^q\xi(x+a)) \mid a\in \mathrm{GF}(q)\}\cup\{(\xi-\xi^q, x\xi^q-x^q\xi)\},\\ r'_\xi &= \{(\xi^q(x^q+a)-\xi(x+a), x\xi(x+a)-x^q\xi^q(x^q+a)) \mid a\in \mathrm{GF}(q)\}\cup\{(\xi^q-\xi, x\xi-x^q\xi^q)\}. \end{aligned}$$

Lemma 2.2. *Let r'_ξ be a q–order subline of $\mathcal{F}_2$ such that $|r'_\xi \cap r_1| = i$, $0 \le i \le 2$. Then there is a subgroup of K if order $q+1-i$ fixing r'_ξ.*

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 $\xi \in \mathrm{GF}(q)$ and $r'_\xi = r'_1$, where

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

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

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

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

- If $r'_\xi \cap r_1 = \{(1,b)\}$, for a fixed $b\in \mathrm{GF}(q)$, then $\xi = \frac{1}{(x+b)^2}$ and

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

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

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

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

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

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

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

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

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

A member of Γ, say γ_c, is induced by the following matrix

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

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

- If $r'_\xi \cap r_1 = \{(1, b_1), (1, b_2)\}$, for two fixed elements $b_1, b_2 \in \mathrm{GF}(q)$, then $\xi = \frac{1}{(x+b_1)(x+b_2)}$. In this case the subline $r'_\xi = r'_{(x+b_1)^{-1}(x+b_2)^{-1}}$ turns out to be

$$\{R_a \mid a \in \mathrm{GF}(q)\} \quad \cup \quad \{R = (x + x^q + b_1 + b_2, b_1b_2 - x^{q+1})\},$$

where

$$R_a = (x^{q+1} + a(x + x^q) + a(b_1 + b_2) - b_1b_2, (b_1 + b_2 - a)x^{q+1} + b_1b_2(x + x^q + a)).$$

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

$$\left\{ \begin{pmatrix} c & d \\ -db_1b_2 & c + d(b_1 + b_2) \end{pmatrix} \ : \ c, d \in \mathrm{GF}(q), (c + b_1d)(c + b_2d) \neq 0 \right\}.$$

A non–trivial projectivity of Γ, say γ_c, is induced by the following matrix

$$\begin{pmatrix} c & 1 \\ -b_1b_2 & c + b_1 + b_2 \end{pmatrix},$$

for some $c \in \mathrm{GF}(q) \setminus \{-b_1, -b_2\}$. Then $\gamma_c(R) = R_{-c}$ and $\gamma_c(R_a)$ equals R or $R_{\frac{ac+b_1b_2}{b_1+b_2+c-a}}$, according as $c = a - b_1 - b_2$ or $c \neq a - b_1 - b_2$. Hence γ_c fixes $r'_{(x+b_1)^{-1}(x+b_2)^{-1}}$.

Assume that r'_ξ is such that $|r'_\xi \cap r_1| = 0$. Let s_1, s_2 be elements of $\mathrm{GF}(q)$ such that the polynomial $f(X) = X^2 + s_1X + s_2$ is irreducible over $\mathrm{GF}(q)$. This means that there exists $u \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ 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

$$r'_\xi = r'_{(x+u)^{-1}(x+u^q)^{-1}} = r'_{\frac{1}{(x+u)(x+u^q)}} = \{R_a \mid a \in \mathrm{GF}(q)\} \ \cup \ \{R = (x + x^q - s_1, s_2 - x^{q+1})\},$$

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 Γ be the subgroup of K of order $q + 1$ induced by the subgroup of $\mathrm{GL}(2, q)$ given by

$$\left\{ \begin{pmatrix} c & d \\ -s_2d & c - s_1d \end{pmatrix} \ : \ c, d \in \mathrm{GF}(q), (c, d) \neq (0, 0) \right\}.$$

A non–trivial projectivity of Γ, say γ_c, is induced by the following matrix

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

for some $c \in \mathrm{GF}(q)$. Then $\gamma_c(R) = R_{-c}$ and $\gamma_c(R_a)$ equals R or $R_{\frac{ac+s_2}{c-a-s_1}}$, according as $c = a + s_1$ or $c \neq a + s_1$. Hence γ_c fixes $r'_{(x+u)^{-1}(x+u^q)^{-1}}$. □

Lemma 2.3. *No non–trivial projectivity of K fixes $\mathcal{S}_x$.*

Proof. Let γ be the projectivity of K associated with the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q).$$

Then

$$\gamma(t^q - t, xt - x^q t^q) = -\left((bx^q - a)t^q - (bx - a)t, \frac{c - dx}{bx - a}(bx - a)t - \frac{c - dx^q}{bx^q - a}(bx^q - a)t^q\right).$$

Hence $\gamma(\mathcal{S}_x) = \mathcal{S}_{\frac{c-dx}{bx-a}}$. Hence $\mathcal{S}_x \neq \gamma(\mathcal{S}_x)$ unless $b = c = 0$ and $a = d$, i.e., γ is the identity. □

Proposition 2.4. *Let $\mathcal{S}$ be a splash of $\mathrm{PG}(1,q^3)$ and let s, s' be two q–order sublines of $\mathcal{S}$ 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 $Stab_{\mathrm{PGL}(2,q^3)}(s)$.*

Proof. Since $\mathrm{PGL}(2,q^3)$ is transitive on its splashes and the stabilizer of $\mathcal{S}$ in $\mathrm{PGL}(2,q^3)$ is transitive on its q–order sublines, we may assume w.l.o.g. that $\mathcal{S} = \mathcal{S}_x$ 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 $Stab_{\mathrm{PGL}(2,q^3)}(s)$ fixing s'. Viceversa, if s' belongs to the same family as s, we claim that no non–trivial element of $Stab_{\mathrm{PGL}(2,q^3)}(s)$ fixes s'. Assume on the contrary that there exists such a projectivity γ. Then from Lemma 2.3 we have that $\mathcal{S} \neq \gamma(\mathcal{S})$, where s, s' are two q–order sublines of both $\mathcal{S}$ and $\gamma(\mathcal{S})$, contradicting [8, Theorem 5.2]. □

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

Proof. Let s be a q–order subline. In $\mathrm{PG}(1,q^3)$, there are $(q-1)(q+1)^2(q^2+1)$ q–order sublines intersecting s in exactly one point. Let $\mathcal{B}$ denote the set of such sublines. It can be easily checked that a subgroup of order q of $Stab_{\mathrm{PGL}(2,q^3)}(s)$ acts on points of $\mathrm{PG}(1,q^3)$ 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 $\mathrm{PG}(1,q^3)$. Therefore there is a subset $\mathcal{B}'$ of $\mathcal{B}$ consisting of $(q^2-1)(q+1)$ q–order sublines that are stabilized by a subgroup of order q of $Stab_{\mathrm{PGL}(2,q^3)}(s)$.

Let us count in two ways the couples $(\mathcal{Z}, s')$, where $\mathcal{Z}$ is a splash of $\mathrm{PG}(1,q^3)$ containing s and s' is a further q–order subline of $\mathcal{Z}$ belonging to the same family of s. From Proposition 2.4, s' belongs necessarily to $\mathcal{B} \setminus \mathcal{B}'$. Hence s' can be chosen in $q^2(q+1)(q^2-1)$ ways, and from [8, 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 $\mathrm{PG}(1,q^3)$ 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 $\mathcal{S}_1$, $\mathcal{S}_2$ be two distinct splashes of $\mathrm{PG}(1,q^3)$ having a q–order subline s in common. Then $\mathcal{S}_1$, $\mathcal{S}_2$ share a q–order subline belonging to the opposite family of s.*

Proof. We may assume w.l.o.g. that $\mathcal{S}_1 = \mathcal{S}_x$, where x is a fixed element of $\mathrm{GF}(q^3) \setminus \mathrm{GF}(q)$ and that $s = r_1$. Let s' be a q–order subline of $\mathcal{S}_x$ 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 γ of $\Gamma_{s'}$ maps $\mathcal{S}_x$ to a splash of $\mathrm{PG}(1, q^3)$ distinct from $\mathcal{S}_x$. Hence $\gamma(\mathcal{S}_x)$ will share with $\mathcal{S}_x$ both s and s'. In particular $|\mathcal{S}_x^{\Gamma_{s'}}| = q+1-i$. Moreover if s', s'' are two distinct q–order sublines of $\mathcal{S}_x$ belonging to the opposite family of s, then $\mathcal{S}_x^{\Gamma_{s'}} \cap \mathcal{S}_x^{\Gamma_{s''}} = \{\mathcal{S}_x\}$, otherwise if $\mathcal{S} \in \mathcal{S}_x^{\Gamma_{s'}} \cap \mathcal{S}_x^{\Gamma_{s''}}$ and $\mathcal{S} \neq \mathcal{S}_x$, then $\mathcal{S}$ would contain s, s' and s'' and hence would share with $\mathcal{S}_x$ 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 $\mathrm{PG}(1, q^3)$ distinct from $\mathcal{S}_x$ such that each of them shares with $\mathcal{S}_x$ the q–order subline s and a further q–order subline belonging to the opposite family of s. The result now follows from Theorem 2.5. □

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

In $\mathrm{PG}(2, q^3)$, with the same notation used in Lemma 2.1, let π_0 be a q–order subplane and let ℓ be a line of $\mathcal{L}_3'$. The line ℓ contains q^2+q+1 points of $\mathcal{O}_2'$ and q^3-q^2-q points of $\mathcal{O}_3'$. Moreover $\ell \cap \mathcal{O}_2'$ is a splash $\mathcal{S}$ of ℓ obtained by extending the q^2+q+1 sublines of π_0. Let $\mathcal{F}_1$ be the family of q–order sublines of $\mathcal{S}$ arising from the extended sublines of π_0 of certain dual subconics of π_0 and let $\mathcal{F}_2$ be the family of q–order sublines of $\mathcal{S}$ arising from the extended sublines of π_0 through a point of π_0. Let s be a fixed element of $\mathcal{F}_1$ and let $\mathcal{D}$ be the set of extended sublines of the dual subconic of π_0 which gives rise to s. Then $\mathcal{D}$ consists of $q+1$ extended sublines of π_0 such that through a point of $\mathrm{PG}(2, q^3)$ there pass at most 2 lines of $\mathcal{D}$ and through a point of s there is exactly one line of $\mathcal{D}$. Moreover two distinct lines of $\mathcal{D}$ meet in a point of π_0. There are other $q^2(q+1)$ lines of $\mathrm{PG}(2, q^3)$ having at least a point in common with both s and π_0. Let $\mathcal{E}$ denote the set of such lines. In particular a line of $\mathcal{E}$ has exactly one point in common with both s and π_0, i.e., $\mathcal{E} \subset \mathcal{L}_2'$. Through a point of s there are q^2 lines of $\mathcal{E}$ and through a point of π_0 there are $q+1$, q or $q-1$ lines of $\mathcal{E}$, according as there pass 0, 1 or 2 lines of $\mathcal{D}$, respectively. A line of $\mathcal{D}$ contains $q+1$ points of π_0 and q^3-q points of $\mathcal{O}_2'$, whereas a line of $\mathcal{E}$ contains one point of π_0, q^2 points of $\mathcal{O}_2'$ and q^3-q^2 points of $\mathcal{O}_3'$. The main aim of this subsection is to bound the number of points of $\mathrm{PG}(2, q^3)$ lying on at least a line of $\mathcal{E}$. The following result [7, Lemma 5.6] will be useful.

Lemma 2.7 ([7])**.** *Let r_1, r_2 be lines of $\mathrm{PG}(2, q^3)$ 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 $\mathcal{D}$ and not lying on $\pi_0 \cup s$, there passes at most one line of $\mathcal{E}$.*

Proof. Assume by contradiction that there is a point P on a line $r \in \mathcal{D}$, with $P \notin \pi_0 \cup s$, such that there are two lines of $\mathcal{E}$, 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 π_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 π_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 π_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 $\mathrm{PG}(2, q^3)$ 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 π_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 π_0 from P onto ℓ we get a club $\mathcal{C}$ of ℓ with head point R. Since $R \notin s$, the q–order subline s is not contained in $\mathcal{C}$. From [28, 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 ℓ_A and ℓ_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 π_0 containing P, A and B, 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 π_0 passing through T_A and T_B. Thus by projecting $m \cap \pi_0$ from P onto ℓ the subline s' is obtained. Furthermore an extended subline of π_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 ℓ we get s'. On the other hand s' is also obtained by projecting $m \cap \pi_0$ from P onto ℓ, 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 π_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 π_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 π_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 $\mathcal{C}_A \cap \mathcal{C}_B$ and $|\mathcal{C}_A \cap \mathcal{C}_B| \geq 3q-2$, contradicting [28, Theorem 23]. Therefore $|\mathcal{C}_A \cap \mathcal{C}_B| = 2q$.

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

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

Proof. Let r be an extended subline of π_0 with $r \notin \mathcal{D}$. Then $\bar{r} = r \cap \pi_0$ is a q–order subline. From Lemma 2.7, there is a unique point R of $\mathrm{PG}(2, q^3)$ with $R \notin r \cup \ell$ such that the q–order subline s is obtained by projecting $\bar{r}$ from R onto ℓ. If R were in π_0, then every extended subline of π_0 passing through R would lie in $\mathcal{D}$, contradicting the fact that through a point of π_0 there pass at most two lines of $\mathcal{D}$. If R were in $\mathcal{O}'_2$, then either R would lie on a line of $\mathcal{D}$, contradicting Lemma 2.8 or R would not lie on a line of $\mathcal{D}$, contradicting Lemma 2.9, whenever $q > 2$. □

Corollary 2.12. *If through a point of $\mathcal{O}'_3 \setminus \mathcal{I}$ there pass three lines of $\mathcal{E}$, then the points in common between these three lines and π_0 are not collinear.*

Proof. Assume that there is a point $P \in \mathcal{O}'_3$ such that through P there are three lines of $\mathcal{E}$, 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 π_0 containing T_1, T_2, T_3 is projected from P onto the unique q–order subline of ℓ containing Q_1, Q_2, Q_3, namely s. The extended subline r containing T_1, T_2, T_3 cannot belong to $\mathcal{D}$. Otherwise let $R = r \cap \ell$ and the line joining P and R meets π_0 in a point of $r \cap \pi_0$, i.e., $P \in r$, a contradiction. It follows that $P \in \mathcal{I}$. □

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

Proof. Let P be a point of $\mathcal{O}'_3 \setminus \mathcal{I}$. By projecting π_0 from P onto ℓ, we get a splash $\mathcal{S}'$ of ℓ. If $\mathcal{S} = \mathcal{S}'$, then there are $q+1$ lines of $\mathrm{PG}(2, q^3)$ passing through P and meeting both s and π_0 in at least one point and hence $P \in \mathcal{I}$, which is not the case. Hence $\mathcal{S} \neq \mathcal{S}'$. Assume by contradiction that there are at least four lines of $\mathcal{E}$ through the point P. Then $|s \cap \mathcal{S}'| \geq 4$. By [28, Theorem 8], it follows that s is a q–order subline of $\mathcal{S}'$ as well. Since $\mathcal{S}$ and $\mathcal{S}'$ have in common s, from Theorem 2.6, we have that $\mathcal{S}$ and $\mathcal{S}'$ 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 $\mathcal{S}'$, then s is obtained by projecting the points of a subconic of π_0 from P onto ℓ. Hence, when s' is considered as a q–order subline of $\mathcal{S}'$, it is obtained by projecting a subline $\bar{r}$ of π_0 from P onto ℓ. Similarly, since s, as a q–order subline of $\mathcal{S}$, arises from the extended sublines of a dual subconic of π_0, we have that when s' is considered as a q–order subline of $\mathcal{S}$, it is obtained by extending the sublines of π_0 through a point T of π_0. Let r be the line of $\mathrm{PG}(2, q^3)$ 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 π_0 at a point of $\bar{r}$. Hence $m = r$ and $P \in \mathcal{O}'_2$, 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 ℓ.

On the other hand s' is obtained by projecting $\bar{r}$ from P onto ℓ, with $P \neq T$. This contradicts Lemma 2.7. □

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* $\mathrm{PG}(2,q^3)$, $q>2$, *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 $P \in \mathcal{O}'_2 \setminus s$ 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 π_0 incident with one line of $\mathcal{D}$, $q(q+1)/2$ points of π_0 incident with 2 lines of $\mathcal{D}$ and $q(q-1)/2$ points of π_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 $2(z_2+z'_2)+6(z_3+z'_3)+q^2 \cdot q(q+1)$. 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 $z_2 + 3z_3 \geq (q^3-q)(q^3-1)/2$. On the other hand, from Corollary 2.12, we have that the value z_3 cannot exceed the number of triangles of π_0, that is $q^3(q+1)(q^2+q+1)/6$. Hence

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

whenever $q \geq 5$. □

2.3 Cutting blocking sets of $\mathrm{PG}(3,q^3)$ as union of three q–order subgeometries

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

Lemma 2.16. *A plane of $\mathrm{PG}(3,q^3)$ shares with a q–order subgeometry of $\mathrm{PG}(3,q^3)$ 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 Σ be a q–order subgeometry of $\mathrm{PG}(3,q^3)$, let P be a point of Σ and let π be a plane of $\mathrm{PG}(3,q^3)$ such that $\pi_0=\pi\cap\Sigma$ is a q–order subplane of π, with $P\notin\pi$. A plane σ of $\mathrm{PG}(3,q^3)$ containing P intersects π 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, in π there are $q(q^2-1)(q^2+q+1)$ lines intersecting π_0 in one point and $q^3(q-1)(q^2-1)$ lines disjoint from π_0. Hence apart from the $(q+1)(q^2+1)$ planes of $\mathrm{PG}(3,q^3)$ intersecting Σ in a q–order subplane, there are $q(q^2+q+1)(q^4-1)$ planes of $\mathrm{PG}(3,q^3)$ meeting Σ in a q–order subline and $q^3(q^2-1)(q^4-1)$ planes of $\mathrm{PG}(3,q^3)$ having in common with Σ exactly one point. □

We will refer to a line or a plane of $\mathrm{PG}(3,q^3)$ intersecting a q–order subgeometry Σ in $q+1$ or q^2+q+1 points as a line or a plane of Σ, respectively. Let $\Sigma_1=\mathrm{PG}(3,q)$ be the canonical q–order subgeometry embedded in $\mathrm{PG}(3,q^3)$. Let $G=\mathrm{PGL}(4,q)$ be the stabilizer of Σ_1 in $\mathrm{PGL}(4,q^3)$ and let ι be the collineation of order three of $\mathrm{PG}(3,q^3)$ fixing pointwise Σ_1.

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

- *Σ_1;*
- *$\mathcal{O}_2$ of size $q(q^2+q+1)(q^4-1)$ consisting of points lying on exactly one line of Σ_1;*
- *$\mathcal{O}_3$ of size $q^3(q^2-1)(q^4-1)$.*

Proof. Let π be a plane of Σ_1 and let G_π be the stabilizer of π in G. The group G is transitive on the $(q+1)(q^2+1)$ planes of Σ_1, hence the three G_π–orbits on points of π give rise to Σ_1, $\mathcal{O}_2$, $\mathcal{O}_3$. To compute their size, note that two planes of Σ_1 have in common $q+1$ points of Σ_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 Σ_1. □

Note that a point $P\in\mathrm{PG}(3,q^3)\setminus\Sigma_1$ belongs to $\mathcal{O}_2$ or $\mathcal{O}_3$ according as the points P,P^ι,P^{ι^2} span a line or a plane of Σ_1, respectively.

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

- *$\mathcal{L}_1$ of size $(q^2+1)(q^2+q+1)$ consisting of lines of Σ_1. A line of $\mathcal{L}_1$ has $q+1$ points in common with Σ_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 Σ_1 in one point and contained in a plane of Σ_1. A line of $\mathcal{L}_2$ consists of one point of Σ_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 Σ_1 in one point and not contained in a plane of Σ_1. A line of $\mathcal{L}_3$ has one point in common with Σ_1 and q^3 points in common with $\mathcal{O}_3$;*

- $\mathcal{L}_4$ *of size* $q^3(q^2-1)(q^4-1)$ *consisting of lines disjoint from* Σ_1 *and contained in a plane of* Σ_1*. A line of* $\mathcal{L}_4$ *consists of* q^2+q+1 *points of* $\mathcal{O}_2$ *and* q^3-q^2-q *points of* $\mathcal{O}_3$*;*

- $\mathcal{L}_5$ *of size* $q^5(q^3-1)(q^4-1)$ *consisting of lines disjoint from* Σ_1 *and not contained in a plane of* Σ_1*. A line of* $\mathcal{L}_5$ *has* $q+1$ *points in common with* $\mathcal{O}_2$ *and* q^3-q *points in common with* $\mathcal{O}_3$*.*

Proof. Let π be a plane of Σ_1 and let G_π be the stabilizer of π in G. Under the action of G the three G_π–line orbits give rise to $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}_4$, respectively. Note that a line of $\mathcal{L}_2$ has q^2 points of $\mathcal{O}_2$ and q^3-q^2 points of $\mathcal{O}_3$, whereas a line belonging to $\mathcal{L}_4$ has q^2+q+1 points of $\mathcal{O}_2$ and q^3-q^2-q points of $\mathcal{O}_3$.

Let $\mathcal{Q}$ be a quadratic cone of $\mathrm{PG}(3,q^3)$ such that $\mathcal{Q}\cap\Sigma_1$ is a quadratic cone of Σ_1. Thus the vertex of $\mathcal{Q}$, say V, belongs to Σ_1 and ι stabilizes $\mathcal{Q}$. If r is a line of $\mathcal{Q}$ such that $r\cap\Sigma_1=\{V\}$ and P is a point of r, with $P\neq V$, then $P\in\mathcal{O}_3$, otherwise the three lines r, r^ι, r^{ι^2} of $\mathcal{Q}$ would lie on a plane, a contradiction. This means that $|r\cap\mathcal{O}_3|=q^3$ and that r cannot be contained in a plane of Σ_1. On the other hand, if π is a plane of Σ_1 and $V\notin\pi$, then $\pi\cap\mathcal{Q}$ is a non–degenerate conic $\mathcal{Q}(2,q^3)$ and $\mathcal{Q}(2,q^3)\cap\Sigma_1$ is a non–degenerate subconic $\mathcal{Q}(2,q)$ of $\mathcal{Q}(2,q^3)$ contained in $\pi\cap\Sigma_1$. Let $R=\pi\cap r$. Then $\pi=\langle R,R^\iota,R^{\iota^2}\rangle$ and $R,R^\iota,R^{\iota^2}\in\mathcal{Q}(2,q^3)$. Note that there are exactly q^2+q+1 non–degenerate conics of π passing through R,R^ι,R^{ι^2} and intersecting $\pi\cap\Sigma_1$ in a non–degenerate subconic. This set of q^2+q+1 conics gives rise to the so called circumscribed bundle of $\pi\cap\Sigma_1$; see [3]. It follows that the line r is contained in exactly q^2+q+1 quadratic cones of $\mathrm{PG}(3,q^3)$ such that their intersection with Σ_1 is a quadratic cone of Σ_1. Since the stabilizer of $\mathcal{Q}$ in G is transitive on the q^3-q lines of $\mathcal{Q}$ meeting Σ_1 exactly in V and G is transitive on the $q^2(q^3-1)(q^2+1)(q+1)$ quadratic cones of Σ_1 [24, Section 15.3], we have that $r^G=\mathcal{L}_3$.

Let $\mathcal{H}$ be a hyperbolic quadric of $\mathrm{PG}(3,q^3)$ such that $\mathcal{H}\cap\Sigma_1$ is a hyperbolic quadric of Σ_1. Thus $\mathcal{H}$ contains $2(q^3+1)$ lines of $\mathrm{PG}(3,q^3)$ on two reguli, say R_1 and R_2. Among these $2(q^3+1)$ lines, there are $2(q+1)$ that belong to $\mathcal{L}_1$ and that are on two reguli of Σ_1, say $\bar{R}_1\subset R_1$ and $\bar{R}_2\subset R_2$. If t is a line of $R_1\setminus\bar{R}_1$ and P is a point of t, then $P\in\mathcal{O}_2$ if and only if P is on a line of $\bar{R}_2$. Similarly if $t\in R_2\setminus\bar{R}_2$. This means that $|t\cap\mathcal{O}_2|=q+1$, $|t\cap\mathcal{O}_3|=q^3-q$ and that t cannot be contained in a plane of Σ_1. Moreover the line t is contained in exactly one hyperbolic quadric of $\mathrm{PG}(3,q^3)$ such that $\mathcal{H}\cap\Sigma_1$ is a hyperbolic quadric of Σ_1, otherwise the three lines t, t^ι, t^{ι^2} would lie on two distinct reguli of $\mathrm{PG}(3,q^3)$, a contradiction. Since the stabilizer of $\mathcal{H}$ in G is transitive on the $2(q^3-q)$ lines of $\mathcal{H}$ disjoint from Σ_1 and G is transitive on the $q^4(q^3-1)(q^2+1)$ reguli of Σ_1 [24, Section 15.3], we have that $t^G=\mathcal{L}_5$. □

Lemma 2.19. *The number of planes of* $\mathrm{PG}(3,q^3)$ *intersecting* Σ_1 *in at least* $q+1$ *points and passing through a line* ℓ *of* $\mathrm{PG}(3,q^3)$*, with* $|\ell\cap\Sigma_1|\leq 1$*, equals either* q^2+1*, or* q^2+q+1*, or* 1*, or* $q+1$ *according as* ℓ *belongs either to* $\mathcal{L}_2$*, or* $\mathcal{L}_3$*, or* $\mathcal{L}_4$*, or* $\mathcal{L}_5$*, respectively.*

Proof. Let ℓ be a line of $\mathrm{PG}(3,q^3)$ such that ℓ is not a line of Σ_1. Then there is one or no plane of Σ_1 containing ℓ just as $\ell\in\mathcal{L}_2\cup\mathcal{L}_4$ or $\ell\in\mathcal{L}_3\cup\mathcal{L}_5$. Moreover, if $\ell\in\mathcal{L}_2\cup\mathcal{L}_4$, then $|\ell\cap\Sigma_1|=1$, whereas if $\ell\in\mathcal{L}_3\cup\mathcal{L}_5$, then $|\ell\cap\Sigma_1|=0$. It follows that if $\ell\in\mathcal{L}_2$ there are q^2 planes of $\mathrm{PG}(3,q^3)$ containing ℓ and meeting Σ_1 in $q+1$ points, whereas if $\ell\in\mathcal{L}_3$ there are q^2+q+1 planes of

Σ_1 containing ℓ and sharing $q+1$ points with Σ_1. If $\ell \in \mathcal{L}_4$, let π be the unique plane of Σ_1 containing ℓ. Through ℓ there pass q^3 planes distinct from π and $|\Sigma_1 \setminus \pi| = q^3$. Since every plane has at least a point in common with Σ_1, we have that necessarily every plane through ℓ distinct from π has exactly one point in common with Σ_1. If $\ell \in \mathcal{L}_5$, from the proof of Lemma 2.18, ℓ is contained in a unique hyperbolic quadric $\mathcal{H}$ of $\mathrm{PG}(3,q^3)$ such that $\mathcal{H} \cap \Sigma_1$ is a hyperbolic quadric of Σ_1. Hence there are at least $q+1$ planes containing ℓ and meeting Σ_1 in $q+1$ points. On the other hand, since there are other q^3-q planes through ℓ and $|\Sigma_1 \setminus (\Sigma_1 \cap \mathcal{H})| = q^3-q$, every other plane through ℓ has to share with Σ_1 exactly one point. □

Let S be a Singer group of Σ_1. Then S is a subgroup of order $(q+1)(q^2+1)$ of a Singer group $\bar{S}$ of $\mathrm{PG}(3,q^3)$. Let $\bar{S}'$ be the unique subgroup of $\bar{S}$ of order $(q^2-q+1)(q^4-q^2+1)$. Thus a non–trivial element of $\bar{S}'$ maps Σ_1 to a q–order subgeometry of $\mathrm{PG}(3,q^3)$ distinct from Σ_1. Since $\bar{S}$ acts regularly on the points of $\mathrm{PG}(3,q^3)$ and $\bar{S} = \langle S, \bar{S}' \rangle$, we have that necessarily these $(q^2-q+1)(q^4-q^2+1)$ q–order subgeometries so obtained are pairwise disjoint. Hence they form a partition $\mathcal{P}$ of the points of $\mathrm{PG}(3,q^3)$ into q–order subgeometries. Since S is a subgroup of G, it follows that a q–order subgeometry of $\mathcal{P}$ and distinct from Σ_1 consists either of points of $\mathcal{O}_2$ or of points of $\mathcal{O}_3$. In particular there are $q^3(q-1)(q^2-1)$ members of $\mathcal{P}$ consisting of points of $\mathcal{O}_3$ and hence q^4-q members of $\mathcal{P}$ formed by points of $\mathcal{O}_2$. Recall the following results.

Lemma 2.20 ([11]). *No plane of* $\mathrm{PG}(3,q^3)$ *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* Σ_1 *there pass* $q+1$ *lines of* $\mathcal{R}_i$ *no three in a plane of* Σ_1 *and a plane of* Σ_1 *contains* $q+1$ *lines of* $\mathcal{R}_i$ *no three through a point.*

Note that if two lines of Σ_1 meet, then necessarily their intersection point belongs to Σ_1. Let ℓ be a line of $\mathcal{R}_1$ and let L be a point of $\ell \cap \mathcal{O}_2$. Set $\Sigma_2 = L^S$. We will show that there exists a q–order subgeometry of $\mathcal{P}$ consisting of points of $\mathcal{O}_3$ 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* $\mathrm{PG}(3,q^3)$ *having at least a point in common with* Σ_1 *and* Σ_2*. In particular* $(q+1)(q^2+1)$ *of these are lines of* Σ_1 *and* $q^2(q+1)^2(q^2+1)$ *are lines of* $\mathcal{L}_2$ *meeting both* Σ_1 *and* Σ_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 ℓ, necessarily ℓ meets Σ_2 in L. Hence every line of $\mathcal{R}_1$ has exactly one point in common with Σ_2. Moreover no other line of Σ_1 may have a point in common with Σ_2. Therefore a line of $\mathrm{PG}(3,q^3)$ not belonging to $\mathcal{R}_1$ and having at least a point in common with Σ_1 and Σ_2 belongs to either $\mathcal{L}_2$ or $\mathcal{L}_4$. Let π be a plane of Σ_1 with $\ell \subset \pi$. Since there are exactly $q+1$ lines of $\mathcal{R}_1$ contained in π and every line of $\mathcal{R}_1$ has exactly one point in common with Σ_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 $\mathcal{L}_2$ that are contained in π. Varying the plane π among the $q+1$ planes of Σ_1 containing ℓ, we have that there are $q^2(q+1)$ lines of $\mathcal{L}_2$ through L meeting both Σ_1 and Σ_2 in one point. Since $q^3+q^2 = |\Sigma_1 \setminus \ell|$, we have that every line through L distinct from ℓ and intersecting Σ_1 in at least one point has exactly one point in common with Σ_1. Since $\Sigma_2 = L^S$, it follows that there are exactly $q^2(q+1)^2(q^2+1)$ lines of $\mathcal{L}_2$ meeting both Σ_1 and Σ_2 in one point. □

Corollary 2.23. *A line of Σ_2 is disjoint from Σ_1.*

From Proposition 2.22, the $(q+1)(q^2+1)$ lines of $\mathcal{R}_1$ have $q+1$ points in common with Σ_1 and one point in common with Σ_2 and there is a subset of $\mathcal{L}_2$, say $\mathcal{R}$, consisting of $q^2(q+1)^2(q^2+1)$ lines meeting both Σ_1 and Σ_2 in exactly one point. Let π be a plane of Σ_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 $\mathcal{R}_1$ contained in π and the set $\mathcal{D}$ 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 $\mathcal{R}$ contained in π; let $\mathcal{E}$ be the set of these lines. Note that $\mathcal{D} \cup \mathcal{E}$ is the set of lines of π 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 $\mathcal{R}_1 \cup \mathcal{R}$ such that $r_1 \cap r_2 \in \mathcal{O}_3$, then the plane spanned by r_1 and r_2 is a plane of Σ_1.*

Proof. Since no point of $\mathcal{O}_3$ lies on a line of $\mathcal{R}_1$, we have that $r_1, r_2 \in \mathcal{R}$. Moreover $|\Sigma_1 \cap \mathcal{O}_3| = |\Sigma_2 \cap \mathcal{O}_3| = 0$ and hence $r_1 \cap r_2 \notin \Sigma_1 \cup \Sigma_2$. Since $r_i \in \mathcal{L}_2$, $i = 1, 2$, there is a plane of Σ_1, say π_i, containing r_i, $i = 1, 2$. Assume by contradiction that $\sigma = \langle r_1, r_2 \rangle$ is not a plane of Σ_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 Σ_1 meet in a line of Σ_1, which contains no point of $\mathcal{O}_3$. □

Proposition 2.25. *There exists a point $P \in \mathcal{O}_3$ such that P is not contained in a line of $\mathcal{R}_1 \cup \mathcal{R}$.*

Proof. Since no point of $\mathcal{O}_3$ lies on a line of $\mathcal{R}_1$, we have that if a point of $\mathcal{O}_3$ lies on some line of $\mathcal{R}_1 \cup \mathcal{R}$ then such a line belongs to $\mathcal{R}$. From Lemma 2.24, if $P \in \mathcal{O}_3$ and if r_1 and r_2 are two distinct lines of $\mathcal{R}$ such that $P = r_1 \cap r_2$, then r_1 and r_2 are contained in a plane of Σ_1. Therefore, by Theorem 2.14, through a point of $\mathcal{O}_3$, there pass $0, 1, 2, 3$ or $q+1$ lines of $\mathcal{R}$. Fix a plane of Σ_1, say π, and let z_i denote the number of points $Q \in \mathcal{O}_3 \cap \pi$ such that there are i lines of $\mathcal{R}$ through Q, $i = 2, 3, q+1$. Since S is transitive on planes of Σ_1 and two distinct planes of Σ_1 have no point of $\mathcal{O}_3$ in common, we have that there are exactly $z_i(q+1)(q^2+1)$ points of $\mathcal{O}_3$ such that there are i lines of $\mathcal{R}$ through Q, $i = 2, 3, q+1$. In the last case, since $z_{q+1} = q^2$, the points of $\mathcal{O}_3$ contained in the $q+1$ lines of $\mathcal{R}$ are exactly $q^2(q+1)(q^2+1)$ and every plane of Σ_1 contains q^2 of these points. Since a line of $\mathcal{R}$ contains $q^3 - q^2$ points of $\mathcal{O}_3$, it follows that the number of points of $\mathcal{O}_3$ lying on at least one line of $\mathcal{R}$ equals

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

which is smaller than $|\mathcal{O}_3| = (q+1)(q^2+1)(q^6-q^5-q^4+q^3)$, 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 $P \in \mathcal{O}_3$ with the property that no line of $\mathrm{PG}(3,q^3)$ having at least a point in common with Σ_1 and Σ_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 $\mathrm{PG}(3,q^3)$ of size $3(q+1)(q^2+1)$.*

Proof. First observe that no line of $\mathrm{PG}(3,q^3)$ has at least a point in common with each of the subgeometries Σ_1, Σ_2 and Σ_3. Assume on the contrary that ℓ is a line of $\mathcal{R}_1 \cup \mathcal{R}$ having a point R in common with Σ_3. Since $\Sigma_3 = P^S$, there is a projectivity γ of S mapping R to P and hence ℓ^γ is a line of $\mathcal{R}_1 \cup \mathcal{R}$ containing P, contradicting the fact that no line of $\mathcal{R}_1 \cup \mathcal{R}$ passes through P.

Let Π be a plane of $\mathrm{PG}(3,q^3)$. 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 $\mathrm{PG}(3,q^3)$. Hence there is a plane Π of $\mathrm{PG}(3,q^3)$ 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 $\mathrm{PG}(3,q^3)$ having at least one point in common with each of the subgeometries Σ_1, Σ_2 and Σ_3; a contradiction. □

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

Proof. Since S acts transitively on Σ_i, it is enough to prove that through a point of Σ_i, there is a plane of $\mathrm{PG}(3,q^3)$ intersecting each of the three relevant subgeometries in exactly one point. Let r be a line of $\mathcal{R}$. Then $|r \cap \Sigma_1| = |r \cap \Sigma_2| = 1$ and $|r \cap \Sigma_3| = 0$. Since $r \in \mathcal{L}_2$, from Lemma 2.19, there are q^2+1 planes through r intersecting Σ_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 Σ_2 and at most $q+1$ planes through r intersecting Σ_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 Σ_1, Σ_2 and Σ_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 $3q^3+3q^2+3q$, $3q^3+3q^2+2q$, $3q^3+3q^2+q$, $3q^3+3q^2$, $3q^3+2q^2+q$ and $3q^3+2q^2$.*

Proof. It is enough to observe that, from Lemma 2.16 and Lemma 2.20, a plane of $\mathrm{PG}(3,q^3)$ 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+3q+3 points. □

3 Cutting blocking sets from lines in hyggledy–piggledy arrangement

In $\mathrm{PG}(3,q)$ let ℓ_1, ℓ_2, ℓ_3 three pairwise skew lines. There are $q+1$ lines meeting ℓ_i, $1 \leq i \leq 3$, in one point. These lines form a *regulus*, say $\mathcal{R}$ and are contained in a hyperbolic quadric $\mathcal{Q}^+(3,q)$.

Let $\mathcal{R}^o$ denote the opposite regulus of $\mathcal{R}$. It follows that a set of lines of $\mathrm{PG}(3,q)$ 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* $\mathrm{PG}(3,q)$, $q>2$, *the cutting blocking set* $\mathcal{B}$ *is minimal.*

Proof. Let $P \in r$ and let σ be the plane spanned by P and a line s of $\mathcal{R}^o \setminus \{\ell_1,\ell_2,\ell_3\}$. Then σ 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 $\langle(\mathcal{B}\setminus\{P\})\cap\sigma\rangle = s' \neq \sigma$. If $P \in \ell_i$, let $\mathcal{Q}$ be the hyperbolic quadric obtained by considering the regulus of $\mathrm{PG}(3,q)$ containing the lines ℓ_j, ℓ_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 $\mathcal{Q}$, r with ℓ_i and ℓ_1,ℓ_2,ℓ_3 with ℓ_j,ℓ_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 $\mathrm{PG}(r,q)$, let $\mathcal{C} = \{(1,t,\ldots,t^{r-1},t^r) \mid t \in \mathrm{GF}(q)\} \cup \{(0,0,\ldots,0,1)\}$ be the *normal rational curve* of $\mathrm{PG}(r,q)$. Then $\mathcal{C}$ consists of $q+1$ points of $\mathrm{PG}(r,q)$ no $k+2$ of which in a k–space of $\mathrm{PG}(r,q)$. 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. [26, 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* $\mathrm{PG}(r,q)$ *in higgledy–piggledy arrangement.*

Remark 3.4. From the construction of Fancsali and Sziklai, there arises a cutting blocking set of $\mathrm{PG}(r,q)$ of size $(2r-1)(q+1)$. However the cutting blocking set so obtained is in general not minimal. For instance in $\mathrm{PG}(4,11)$ 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 $\mathrm{PG}(4,11)$ is obtained.

Problem 3.5. Determine the minimum number of lines tangent to a normal rational curve in $\mathrm{PG}(r,q)$ 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 $\bar{\mathcal{S}}$ be the set of points covered by $2r-1$ arbitrarily chosen tangent lines to $\mathcal{C}$. Let $\mathcal{S}$ be a pointset such that $\mathcal{S} \subseteq \bar{\mathcal{S}}$ and $\mathcal{S}$ is a minimal cutting blocking set.

Proposition 3.6. *A hyperplane of* $\mathrm{PG}(r,q)$ *contains at most* $r-2$ *lines that are tangent to* $\mathcal{C}$.

Proof. By induction on r. Let $r=3$. Since no two lines tangent to $\mathcal{C}$ have a point in common, a plane of $\mathrm{PG}(3,q)$ contains at most one tangent line to $\mathcal{C}$. Assume that the result holds true for $r-1$. Let $\mathcal{C}$ be a normal rational curve of the projective space $\mathrm{PG}(r,q)$ equipped with homogeneous projective coordinates $X_1,\ldots,X_{r+1}$. Suppose by contradiction that a hyperplane H of $\mathrm{PG}(r,q)$ contains $r-1$ lines tangent to $\mathcal{C}$. Denote by P a point of $\mathcal{C}\cap H$, where t_P, the line tangent to $\mathcal{C}$ at P, is contained in H. Let Γ be a hyperplane of $\mathrm{PG}(r,q)$ such that $P\notin\Gamma$. From Lemma [26, Theorem 6.30], we may assume that $P=(0,0,\ldots,0,1)$. By projecting the q points of $\mathcal{C}\setminus\{P\}$ and the line t_P from P onto $\Gamma: X_{r+1}=0$, we obtain the normal rational curve $\mathcal{C}'=\{(1,t,\ldots,t^{r-1},0) \mid t\in\mathrm{GF}(q)\}\cup\{(0,0,\ldots,1,0)\}$ of Γ. On the other hand, by projecting from P onto Γ the line tangent to $\mathcal{C}$ at a point R, $R\neq P$, we get the line $\langle\bar{R},\bar{R}'\rangle$ that is tangent to $\mathcal{C}'$ at $\bar{R}$, where $\bar{R}=\big(1,t,\ldots,t^{r-1},0\big)$ and $\bar{R}'=\big(0,1,\ldots,(r-1)t^{r-2},0\big)$. Observe that by projecting the $r-1$ tangent lines to $\mathcal{C}$ contained in H we get $r-2$ lines that are tangent to $\mathcal{C}'$ and are contained in the $(r-2)$–space $H\cap\Gamma\subset\Gamma$, a contradiction. □

Proposition 3.7. *Let* $p>r$ *and* $q>2r-1$. *The code associated with the minimal cutting blocking set* $\mathcal{S}$ *is a* $[|\mathcal{S}|,r+1]_q$ *reduced minimal linear code, where* $|\mathcal{S}|\leq(2r-1)(q+1)$ *and minimum distance* $d\geq|\mathcal{S}|-(r-2)q-2r+1$.

Proof. The statement follows from Proposition 3.6. □

3.1 Lines of $\mathrm{PG}(5,q)$ in higgledy–piggledy arrangement

Let $\mathrm{PG}(2,q^2)$ 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 $\mathrm{GF}(q)\subset\mathrm{GF}(q^2)$. Each point in $\mathrm{PG}(2,q^2)$ 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 $\mathrm{PG}(5,q)$. Extending this map from (subsets of) points of $\mathrm{PG}(2,q^2)$ to subsets of points of $\mathrm{PG}(5,q)$ we obtain a map $\phi:\mathrm{PG}(2,q^2)\to\mathrm{PG}(5,q)$, called *field reduction map*.

The set $\mathcal{D}=\{\phi(P)\mid P\in\mathrm{PG}(2,q^2)\}$ is a Desarguesian line–spread of $\mathrm{PG}(5,q)$. The incidence structure whose points are the elements of $\mathcal{D}$ and whose lines are the solids of $\mathrm{PG}(5,q)$ joining two distinct elements of $\mathcal{D}$, is isomorphic to $\mathrm{PG}(2,q^2)$. A degenerate Hermitian curve of rank 2 of $\mathrm{PG}(2,q^2)$ 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 $\mathrm{PG}(5,q)$ and let $\phi^{-1}(\Pi)=\{P\in\mathrm{PG}(2,q^2) \ : \ |\phi(P)\cap\Pi|\geq 1\}$. Then either Π contains q^2+1 lines of $\mathcal{D}$ and $\phi^{-1}(\Pi)$ is a line of $\mathrm{PG}(2,q^2)$ or there is exactly one line ℓ of $\mathcal{D}$ in Π and $\phi^{-1}(\Pi)$ is a degenerate Hermitian curve $\mathcal{H}$ of $\mathrm{PG}(2,q^2)$. Note that to such a degenerate Hermitian curve there correspond $q+1$ solids of $\mathrm{PG}(5,q)$, say Π_i, $1\leq i\leq q+1$, such that $\Pi_i\cap\Pi_j=\ell$, if $i\neq j$, and $\bigcup_{i=1}^{q+1}\Pi_i=\bigcup\{\phi(P) \mid P\in\mathcal{H}\}$.

Lemma 3.8. *Let* $\mathcal{P}$ *be a set of at least five points of* $\mathrm{PG}(2,q^2)$ *not on a line of* $\mathrm{PG}(2,q^2)$ *and not on a degenerate Hermitian curve of* $\mathrm{PG}(2,q^2)$. *Then* $\mathcal{L}=\{\phi(P) \mid P\in\mathcal{P}\}$ *is a set of lines of* $\mathrm{PG}(5,q)$ *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 Π of $\mathrm{PG}(5,q)$ meeting every line of $\mathcal{L}$ and $\mathcal{P}$ would be contained in $\phi^{-1}(\Pi)$, a contradiction. □

In $\mathrm{PG}(2,q^2)$, consider the set $\bar{\mathcal{P}}$ 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 $\mathrm{PG}(2,q^2)$ containing the four points of $\bar{\mathcal{P}}$, namely the canonical Baer subplane π.

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 π in a Baer subline. In this case the $q+1$ lines of $\mathcal{H}$ have all $q+1$ points in common with π. 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 π 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 π containing the four points of π or $\mathcal{H}\cap\pi$ is a non–degenerate Baer conic $\bar{C}\subset\pi$. 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 $\mathrm{PG}(2,q^2)$ 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. □

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

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

$$\begin{aligned}&X_1^qX_2-X_1X_2^q=0,\\&a(X_1^qX_2-X_1X_2^q)-(X_1^qX_3-X_1X_3^q)=0,\ a\in\mathrm{GF}(q),\\&b(X_1^qX_2-X_1X_2^q)-a(X_1^qX_3-X_1X_3^q)+X_2^qX_3-X_2X_3^q=0,\ a,b\in\mathrm{GF}(q).\end{aligned}\tag{3.1}$$

  They contain π and their vertices lie in π.

- $3q$ degenerate Hermitian curves of type

$$\begin{aligned}&X_1^qX_3-\alpha X_1X_3^q-X_2^qX_3+\alpha X_2X_3^q=0,\\&X_1^qX_2-\alpha X_1X_2^q+\alpha X_2^qX_3-X_2X_3^q=0,\\&X_1^qX_2-\alpha X_1X_2^q-X_1^qX_3+\alpha X_1X_3^q=0,\ \alpha\in\mathrm{GF}(q^2)\setminus\{1\},\ \alpha^{q+1}=1.\end{aligned}\tag{3.2}$$

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

- $6(q^2-q)$ degenerate Hermitian curves of type

$$\begin{aligned}
&(1-\alpha^q)\alpha X_1^qX_2-(1-\alpha)\alpha^qX_1X_2^q-(1-\alpha^q)X_1^qX_3+(1-\alpha)X_1X_3^q=0,\\
&(1-\alpha)\alpha^qX_1^qX_2-(1-\alpha^q)\alpha X_1X_2^q+(1-\alpha^q)X_2^qX_3-(1-\alpha)X_2X_3^q=0,\\
&(1-\alpha)\alpha^qX_1^qX_3-(1-\alpha^q)\alpha X_1X_3^q-(1-\alpha)X_2^qX_3+(1-\alpha^q)X_2X_3^q=0,\\
&\alpha^{q+1}(X_1^qX_2-X_1X_2^q)-\alpha^qX_1^qX_3+\alpha X_1X_3^q+\alpha^qX_2^qX_3-\alpha X_2X_3^q=0,\\
&\alpha^qX_1^qX_2-\alpha X_1X_2^q-\alpha^{q+1}(X_1^qX_3-X_1X_3^q)+\alpha X_2^qX_3-\alpha^qX_2X_3^q=0,\\
&\alpha X_1^qX_2-\alpha^qX_1X_2^q-\alpha X_1^qX_3+\alpha^qX_1X_3^q+\alpha^{q+1}(X_2^qX_3-X_2X_3^q)=0,\ \alpha\in\mathrm{GF}(q^2)\setminus\mathrm{GF}(q).
\end{aligned}\tag{3.3}$$

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

- $(q-2)(q^2-q)$ degenerate Hermitian curves of type

$$\begin{aligned}
&(1-\delta)t^qX_1^qX_2-(1-\delta)tX_1X_2^q-(1-\delta t)t^qX_1^qX_3\\
&\quad+(1-\delta t^q)tX_1X_3^q+(1-\delta t)X_2^qX_3-(1-\delta t^q)X_2X_3^q=0,\\
&\delta\in\mathrm{GF}(q)\setminus\{0,1\},t\in\mathrm{GF}(q^2)\setminus\mathrm{GF}(q).
\end{aligned}\tag{3.4}$$

  They meet π in $q+1$ points and their vertices are not in π and on $q-2$ non–degenerate conics of $\mathrm{PG}(2,q^2)$.

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

Proof. Consider a set of six points of $\mathrm{PG}(2,q^2)$. 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 $\mathrm{PG}(2,q^2)$. Thus we may assume that there are four points no three of them on a line and, by the action of $\mathrm{PGL}(3,q^2)$, that these four points are those of $\bar{\mathcal{P}}$. Let P and Q be the remaining two points. If at least one of the points P and Q lies in π, 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 ℓ_P and ℓ_Q be the lines of $\mathrm{PG}(2,q^2)$ containing P and Q, respectively, and meeting the Baer subplane π 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 ℓ_P and ℓ_Q will contain the six points. □

Corollary 3.11. *A set of at least five points of* $\mathrm{PG}(2,q^2)$ *not contained in a degenerate Hermitian curve of* $\mathrm{PG}(2,q^2)$ *has to contain seven points.*

3.1.1 Seven lines of $\mathrm{PG}(5,q)$ in higgledy–piggledy arrangement

In this section we obtain a set of seven points of $\mathrm{PG}(2,q^2)$ not contained in a degenerate Hermitian curve of $\mathrm{PG}(2,q^2)$ and hence, as a by product, a set of seven lines of $\mathrm{PG}(5,q)$ 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_4 and permutes in a unique orbit the remaining three points of $\bar{\mathcal{P}}$. Note that since the group G fixes $\bar{\mathcal{P}}$, 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 $x \in \mathrm{GF}(q) \setminus \{0\}, \xi \in \mathrm{GF}(q^2)$ and let

$$\mathcal{P}_{x,\xi} = \bar{\mathcal{P}} \cup P_5^G, \text{ where } P_5^G = \{(1, x, \xi x), (\xi x, 1, x), (x, \xi x, 1)\}. \tag{3.5}$$

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

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

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

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

or

$$q \text{ is odd, } x = -1 \text{ and } \xi \notin \left\{ \frac{1 + \alpha}{1 - \alpha} \;\middle|\; \alpha^{q+1} = 1, \alpha \neq \pm 1 \right\}, \tag{3.8}$$

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

$$\begin{aligned} A &:= A(\delta, t) = t^q \left(1 - \delta - (1 - \delta t)x\right), \\ B &:= B(\delta, t) = 1 - \delta t - (1 - \delta)tx, \\ C &:= C(\delta, t) = \delta(t^q - t), \\ D &:= D(\delta, t) = t - t^q, \\ E &:= E(\delta, t) = (t - x)(1 - \delta t^q). \end{aligned}$$

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

$$\begin{cases} \xi^q E - \xi E^q - C - D = 0 \\ \xi^q A - \xi A^q + C = 0 \\ \xi^q B - \xi B^q + D = 0. \end{cases} \tag{3.9}$$

Note that $A + B + E = (x - 1)(\delta t^{q+1} + (\delta - 1)(t^q + t) - 1) \in \mathrm{GF}(q)$ 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

$t \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$. Then the previous system can be rewritten as follows:

$$\begin{cases} \delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\ \xi^q = (\xi A^q - C)/A \\ \xi \left(A^q B - A B^q\right) + AD - BC = 0. \end{cases} \tag{3.10}$$

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

$$\delta x t^{q+1} + (1 - \delta - x) t^q + \delta \left((\delta - 1)x - \delta\right) t + \delta = 0.$$

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

$$\begin{cases} \delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\ \delta x t^{q+1} + (1 - \delta - x) t^q + \delta \left((\delta - 1)x - \delta\right) t + \delta = 0. \end{cases}$$

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

$$\begin{cases} \delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\ \left((1 + x)\delta - 1\right) t^q + \left(\delta^2 (1 - x) + 2\delta x - x\right) t - x - \delta = 0. \end{cases} \tag{3.11}$$

If $x \neq -1$ and $\delta = 1/(x + 1)$, then from the second equation of (3.11) we have that $t = \frac{(x+1)^3}{1-x^3} \in \mathrm{GF}(q)$, 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

$$t^2 + (\delta - 1)t - \delta = 0. \tag{3.12}$$

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

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

$$\begin{cases} \delta t^{q+1} + (\delta - 1)(t^q + t) - 1 = 0 \\ \xi = \dfrac{BC - AD}{A^q B - A B^q}. \end{cases} \tag{3.13}$$

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

$$\omega' = \left(\overline{x}, \overline{\xi}, \frac{\overline{\delta} - 1}{\overline{\delta}}, \frac{1 - \overline{\delta}\,\overline{t}}{(1 - \overline{\delta})\overline{t}}\right) \qquad \text{and} \qquad \omega'' = \left(\overline{x}, \overline{\xi}, \frac{1}{1 - \overline{\delta}}, \frac{1 - \overline{\delta}}{1 - \overline{\delta}\,\overline{t}}\right)$$

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 $t \in \mathrm{GF}(q)$, 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 $t \in \mathrm{GF}(q)$, a contradiction. Let

$$\Sigma = \left\{(\delta, t) \in \left(\mathrm{GF}(q) \setminus \{0,1\}, \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)\right) \;\mid\; \delta t^{q+1} + (\delta-1)(t^q+t) - 1 = 0\right\}.$$

It is readily seen that $|\Sigma| \le q^2$.

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

Proof. Fix $x \in \mathrm{GF}(q)\setminus\{0\}$, with $x^3 \neq 1$. We show the existence of an element $\xi \in \mathrm{GF}(q^2)\setminus\mathrm{GF}(q)$ such that no degenerate Hermitian curve containing $\bar{\mathcal{P}}$ 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 ξ 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 ξ is less than $q^2 - q$, we have the assertion. □

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 $\mathrm{PG}(2, q^2)$.*

Proof. Assume by contradiction that three points of $\mathcal{P}_{x,\xi}$ are on a line of $\mathrm{PG}(2, q^2)$. Then the determinant of the 3×3 matrix whose rows are the coordinates of these points must be zero. Straightforward computations show that either ξ belongs to $\mathrm{GF}(q)$ or $x \in \{0,1\}$ and we have a contradiction from (3.6), or one of the following possibilities occurs:

$$x^2\xi^2 - x(x+1)\xi + x^2 - x + 1 = 0, \tag{3.14}$$

$$\xi^2 = \frac{1}{x}. \tag{3.15}$$

If (3.14) were satisfied, then either $q \not\equiv -1 \pmod 3$ and ξ should be in $\mathrm{GF}(q)$ or $q \equiv -1 \pmod 3$ and ξ should be equal to $\frac{\alpha - x}{x(\alpha-1)}$, for some $\alpha \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$, 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 $\mathrm{GF}(q)$. Let $x \neq -1$, otherwise $q \equiv -1 \pmod 4$ and as before $\xi = \frac{1+\alpha}{1-\alpha}$, for some $\alpha \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$, with $\alpha^2 = -1$ (and hence $\alpha^{q+1} = 1$). We will show that there exists a degenerate Hermitian curve given by (3.4) containing $\mathcal{P}_{x,\xi}$ and hence contradicting Theorem 3.13. Note that $\xi^q = -\xi$. From

(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 $t \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ and $\delta \neq 0$. From the second equation of (3.10), we have that $\xi = \frac{C}{A+A^q}$, whereas from the third equation of (3.10), we obtain $A + A^q + \delta(B + B^q) = 0$. Taking into account the first equation of (3.10), we get

$$A + A^q = (t + t^q)(1 - \delta - 2x) + 2\delta t^{q+1}x = 2x + (t + t^q)(1 - \delta + x - 2\delta x).$$

Hence $\xi = \frac{C}{A+A^q} = \frac{D}{B+B^q}$, that is

$$\xi = \frac{t - t^q}{2 - (t + t^q)(x - \delta x + \delta)} = \frac{-\delta(t - t^q)}{2x + (t + t^q)(1 - \delta + x - 2\delta x)}. \tag{3.16}$$

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

$$t + t^q = \frac{-2(x + \delta)}{F(\delta)}, \tag{3.17}$$

$$t^{q+1} = \frac{2(\delta - 1)(x + \delta)}{\delta F(\delta)} + \delta^{-1}. \tag{3.18}$$

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

$$xt^2F(\delta)^2 + 2txF(\delta)(x + \delta) + x(x + \delta)^2 = \left(F(\delta) + (x + \delta)(x - \delta x + \delta)\right)^2. \tag{3.19}$$

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

$$t^2 = -\frac{2t\delta(x + \delta) + 2(\delta - 1)(x + \delta) + F(\delta)}{\delta F(\delta)}. \tag{3.20}$$

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

$$\delta^{-1}x(x + \delta)(x^2 - 1)(\delta - 1)\left(\delta - \frac{x + 1}{x}\right)\left(\delta - \frac{1}{x + 1}\right) = 0, \tag{3.21}$$

that is $\delta = \frac{x+1}{x}$ or $\delta = \frac{1}{x+1}$. In the former case $\left(x, \xi, \frac{x+1}{x}, \frac{x\pm\sqrt{x}}{x+1}\right)$ is a solution of (3.13), whereas if the latter case occurs, then $\left(x, \xi, \frac{1}{x+1}, \frac{(x+1)(-1\pm\sqrt{x})}{x-1}\right)$ 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 $\mathcal{P}_{x,\xi}$ be defined as in Theorem 3.13. The set $\phi(\mathcal{P}_{x,\xi}) = \{\phi(P) \mid P \in \mathcal{P}_{x,\xi}\}$ consists of seven lines of* $\mathrm{PG}(5, q)$ *in higgledy–piggledy arrangement.*

Let $\mathcal{B}$ be the set of $7(q+1)$ points of $\mathrm{PG}(5,q)$ on the seven mutually skew lines ℓ_i, $1 \le i \le 7$, constructed in the previous theorem.

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

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

Proposition 3.17. *To the set $\mathcal{B}$ 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 Γ of $\mathrm{PG}(5,q)$ contains exactly q^2+1 lines of the Desarguesian line–spread $\mathcal{D}$ of $\mathrm{PG}(5,q)$ and they are contained in a unique solid, say Π, where $\phi^{-1}(\Pi)$ is a line, say ℓ, of $\mathrm{PG}(2,q^2)$. From Proposition 3.14, $|\ell \cap \mathcal{P}| \le 2$ and hence at most two lines out of the seven lines $\{\ell_i \mid 1 \le i \le 7\}$ are contained in Γ. In particular, there are 21 lines of $\mathrm{PG}(2,q^2)$ meeting $\mathcal{P}$ in two points, $7(q^2-5)$ lines of $\mathrm{PG}(2,q^2)$ 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 Γ of $\mathrm{PG}(5,q)$ such that $|\Gamma \cap \mathcal{B}| \le 2(q+1)+5$, $7(q^2-5)(q+1)$ hyperplanes Γ of $\mathrm{PG}(5,q)$ such that $|\Gamma \cap \mathcal{B}| = (q+1)+6$ and $(q^4-6q^2+15)(q+1)$ hyperplanes Γ of $\mathrm{PG}(5,q)$ such that $|\Gamma \cap \mathcal{B}| = 7$. □

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 $\mathrm{PG}(2, q^3)$, *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 $\mathrm{PG}(6, q)$: 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.*, 53, (2021), no. 2, 327–341.

[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 $tR + \frac{R}{2}$, 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, *Des. Codes Cryptogr.*, (2021). `https://doi.org/10.1007/s10623-021-00951-y`.

[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 $\mathrm{PG}(3, p^3)$ and on related minihypers, *Des. Codes Cryptogr.*, 29, (2003), 105–122.

[22] D. Glynn, On a set of lines of $\mathrm{PG}(3, q)$ corresponding to a maximal cap contained in the Klein quadric of $\mathrm{PG}(5, q)$, *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 $\mathcal{S}_{n,n}$, *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, *IEEE Trans. Inform. Theory*, 67, (2021), no. 6, part 2, 3690–3700.

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