



## **Saturating linear sets of minimal rank**

Daniele Bartoli, Martino Borello, Giuseppe Marino

### **► To cite this version:**

Daniele Bartoli, Martino Borello, Giuseppe Marino. Saturating linear sets of minimal rank. *Finite Fields and Their Applications*, 2024, 95, pp.102390. [⟨10.1016/j.ffa.2024.102390⟩](https://doi.org/10.1016/j.ffa.2024.102390). [⟨hal-04508482⟩](https://hal.science/hal-04508482)

**HAL Id: hal-04508482**

**<https://hal.science/hal-04508482v1>**

Submitted on 18 Mar 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

# Saturating linear sets of minimal rank

Daniele Bartoli<sup>1</sup>, Martino Borello<sup>2</sup>, and Giuseppe Marino<sup>3</sup>

<sup>1</sup>Department of Mathematics and Informatics, University of Perugia, Perugia, Italy,  
`daniele.bartoli@unipg.it`

<sup>2</sup>Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA,  
Université Sorbonne Paris Nord, CNRS, UMR 7539, France,  
`martino.borello@univ-paris8.fr`

<sup>3</sup>Department of Mathematics and Applications “R. Caccioppoli”, University of Naples  
Federico II, Napoli, Italy, `giuseppe.marino@unina.it`

## Abstract

Saturating sets are combinatorial objects in projective spaces over finite fields that have been intensively investigated in the last three decades. They are related to the so-called covering problem of codes in the Hamming metric. In this paper, we consider the recently introduced linear version of such sets, which is, in turn, related to the covering problem in the rank metric. The main questions in this context are how small the rank of a saturating linear set can be and how to construct saturating linear sets of small rank. Recently, Bonini, Borello, and Byrne provided a lower bound on the rank of saturating linear sets in a given projective space, which is shown to be tight in some cases. In this paper, we provide construction of saturating linear sets meeting the lower bound and we develop a link between the saturating property and the scatteredness of linear sets. The last part of the paper is devoted to show some parameters for which the bound is not tight.

**Keywords:** Linear sets, saturating sets, rank-metric codes, covering radius.

**MSC2020.** Primary: 05B40, 51E20, 52C17. Secondary: 11T71, 94B75.

## Introduction

A set  $S \subseteq \text{PG}(k-1, q^m)$  is called  $\rho$ -saturating if every point of  $\text{PG}(k-1, q^m)$  lies in a subspace generated by  $\rho+1$  points of  $S$ . The term saturated was coined by [33], but used with a slightly different meaning. The above definition comes from [30] and it has been consolidated in [16].

There is a classical correspondence between  $\rho$ -saturating sets and linear codes with covering radius  $\rho + 1$ , obtained by considering the vector representatives of  $S$  as the columns of a parity check matrix of a linear code. It is natural to wonder how small a  $\rho$ -saturating set in  $\text{PG}(k-1, q^m)$  can be. This is equivalent, in the coding-theoretical language, to the so-called *covering problem* (see [12, Chapter 1]). Many bounds and construction of small saturating sets has been given over the last two decades (see for example [15, 17, 28] and references therein).

If  $m \geq 2$ , instead of simply considering sets of points, we may look at linear sets: a linear set associated to an  $\mathbb{F}_q$ -vector space  $U$  in  $\mathbb{F}_{q^m}^k$  is the set of points

$$L_U := \{\langle u \rangle_{\mathbb{F}_{q^m}} : u \in U \setminus \{0\}\} \subseteq \text{PG}(k-1, q^m),$$

where  $\langle u \rangle_{\mathbb{F}_{q^m}}$  denotes the projective point corresponding to  $u$ . Such objects were introduced in [27] in order to construct blocking sets and they have been the subject of intense research over the last years. The  $\mathbb{F}_q$ -dimension of  $U$  is also called *rank* of the linear set. Intuitively, saturating linear sets would not be the smallest ones, in fact, they would be quite large in cardinality. However, a natural question is how small the rank of a  $\rho$ -saturating linear set in  $\text{PG}(k-1, q^m)$  can be. As shown in [8], this is equivalent to the covering problem for rank-metric codes. Let us underline that the knowledge of the covering properties of a rank-metric code has important consequences for applications: the *covering radius* is the least integer  $\rho$  such that every element of the ambient space is in a ball of radius  $\rho$  centered in some codeword. It measures the maximum weight of any correctable error in the ambient space and it characterizes the maximality of the code (namely, if the code is contained in another with the same minimum distance). See [9] for more details. In general, it is much harder to compute the covering radius than the minimum distance of a code. While there is a wide literature on the covering problem in the Hamming metric, there are relatively few papers on the subject in the rank-metric case [9, 10, 18, 19].

In the current work, we continue the investigation of the geometrical approach to such problem introduced in [8]. Let  $s_{q^m/q}(k, \rho)$  denotes the smallest rank of a  $(\rho-1)$ -saturating linear set in  $\text{PG}(k-1, q^m)$ . In [8], it is proved that

$$s_{q^m/q}(k, \rho) \geq \begin{cases} \left\lceil \frac{mk}{\rho} \right\rceil - m + \rho & \text{if } q > 2, \\ \left\lceil \frac{mk-1}{\rho} \right\rceil - m + \rho & \text{if } q = 2, \rho > 1, \\ m(k-1) + 1 & \text{if } q = 2, \rho = 1. \end{cases} \quad (1)$$

and it is shown that (1) is tight for some values of  $q, m, k$  and  $\rho$ . In this paper, we first extend the results in [8] by proving that (1) is tight whenever  $\rho$  divides  $k$ . Secondly, we show some covering properties of  $h$ -scattered linear sets of large rank, which are particular linear sets introduced first in [14]. As a byproduct, thanks to known results on the existence of maximum  $h$ -scattered linear sets, we get other saturating linear sets of small rank and, in some cases not covered by previous results, we get the tightness of the bound (1). The last part of the paper is devoted to

the proof that there exist values of  $q, m, k$  and  $\rho$  for which the bound (1) is not met, clarifying then that the bound (1) is not always tight.

**Outline:** Section 1 is devoted to define and give preliminary results about the main objects of the paper. In Section 2 we provide constructions of small saturating linear sets showing the tightness of the lower bound (1) for some parameters, whereas in Section 3 we prove that the bound is not always tight. Finally, in Section 4 we resume our results and present some open problems.

## 1 Preliminaries

Throughout this paper,  $q$  is a prime power,  $[t]$  denotes the set  $\{1, 2, \dots, t\} \subseteq \mathbb{Z}$ ,  $k \in [n]$ ,  $m \geq 2$ ,  $\rho \in [\min\{k, m\}]$ ,  $\mathbb{F}_q$  denotes the finite field of order  $q$  and  $V(k, q^m)$  is a vector space of dimension  $k$  over  $\mathbb{F}_{q^m}$ . Also,  $N_{q^m/q}(z)$  and  $\text{Tr}_{q^m/q}(z)$  denote the (standard) norm and trace from  $\mathbb{F}_{q^m}$  to  $\mathbb{F}_q$  of  $z \in \mathbb{F}_{q^m}$ .

The projective geometry  $\text{PG}(k-1, q)$  with underlying vector space  $\mathbb{F}_q^k$  is

$$\text{PG}(k-1, q) := (\mathbb{F}_q^k \setminus \{0\}) / \sim,$$

where, for  $u, v \in \mathbb{F}_q^k \setminus \{0\}$ ,  $u \sim v$  if and only if  $u = \lambda v$  for some  $\lambda \in \mathbb{F}_q \setminus \{0\}$ .

**Definition 1.1.** Let  $\mathcal{S} \subseteq \text{PG}(k-1, q^m)$ .

- (a) A point  $Q \in \text{PG}(k-1, q^m)$  is said to be  $(\rho-1)$ -saturated by  $\mathcal{S}$  if there exist  $\rho$  points  $P_1, \dots, P_\rho \in \mathcal{S}$  such that  $Q \in \langle P_1, \dots, P_\rho \rangle_{\mathbb{F}_{q^m}}$ . We also say that  $\mathcal{S}$   $\rho$ -covers  $Q$ .
- (b) The set  $\mathcal{S}$  is  $(\rho-1)$ -saturating set of  $\text{PG}(k-1, q^m)$  if every point  $Q \in \text{PG}(k-1, q^m)$  is  $(\rho-1)$ -saturated by  $\mathcal{S}$  and  $\rho$  is the smallest value with this property.

In order to introduce the  $q$ -analogue of the above definition, we need to introduce the notion of linear sets. These are combinatorial objects, introduced by Lunardon in [27], which are subject of intense research over the last two decades. A thorough presentation of linear sets can be found in [31].

**Definition 1.2.** Let  $U$  be an  $\mathbb{F}_q$ -subspace of  $V(k, q^m)$  of  $\mathbb{F}_q$ -dimension  $n$ . The  $\mathbb{F}_q$ -linear set in  $\text{PG}(k-1, q^m)$  of rank  $n$  associated to  $U$  is the set

$$L_U := \{\langle u \rangle_{\mathbb{F}_{q^m}} : u \in U \setminus \{0\}\},$$

where  $\langle u \rangle_{\mathbb{F}_{q^m}}$  denotes the projective point corresponding to  $u$ . If the size of  $L_U$  is maximal, i.e.  $|L_U| = \frac{q^n-1}{q-1}$ , then  $L_U$  is called scattered.

**Definition 1.3.** Let  $\Lambda = \text{PG}(T, q^m)$  be a projective subspace of  $\text{PG}(k-1, q^m)$  with underlying vector space  $T \subseteq V(k, q^m)$ . Then  $L_{U \cap T} = L_U \cap \Lambda$ , and the weight of  $\Lambda$  in  $L_U$  is defined as

$$w_{L_U}(\Lambda) = \dim_{\mathbb{F}_q}(U \cap T).$$

If  $\dim_{\mathbb{F}_q}(U \cap T) = i$ , one shall say that  $\Lambda$  has weight  $i$  in  $L_U$ .

We are now ready to define the main object of the paper, introduced first in [8].

**Definition 1.4.** An  $\mathbb{F}_q$ -subspace  $U$  in  $V(k, q^m)$  is a rank  $\rho$ -saturating system if  $L_U$  is a  $(\rho-1)$ -saturating set in  $\text{PG}(k-1, q^m)$ . This last is called a  $(\rho-1)$ -saturating linear set.

For an  $\mathbb{F}_q$ -subspace  $U$  in  $V(k, q^m)$  of  $\mathbb{F}_q$ -dimension  $n$ , let us consider a  $k \times n$  matrix  $G$  whose columns are the elements of an  $\mathbb{F}_q$ -basis of  $U$ . The  $\mathbb{F}_{q^m}$ -vector space  $\mathcal{C}$  generated by its rows is called a code associated to  $U$ . The dual code  $\mathcal{C}^\perp$  is the orthogonal space with respect to the standard inner product.

**Definition 1.5.** The rank covering radius of a code  $\mathcal{C} \leq \mathbb{F}_{q^m}^n$  is the integer

$$\rho_{\text{rk}}(\mathcal{C}) := \max\{\min\{\dim_{\mathbb{F}_q}\langle x_1 - c_1, x_2 - c_2, \dots, x_n - c_n \rangle_{\mathbb{F}_q} : c \in \mathcal{C}\} : x \in \mathbb{F}_{q^m}^n\}.$$

The following relation holds between the rank covering radius and rank saturating systems.

**Theorem 1.6** ([8, Theorem 2.5]). Let  $U$  be an  $\mathbb{F}_q$ -subspace in  $V(k, q^m)$  and  $\mathcal{C}$  a code associated to  $U$ . Then,  $U$  is a rank  $\rho$ -saturating system if and only if  $\rho_{\text{rk}}(\mathcal{C}^\perp) = \rho$ .

From both a geometric and a coding theoretical point of view, it is meaningful to ask how small the  $\mathbb{F}_q$ -dimension of a rank  $\rho$ -saturating system in  $V(k, q^m)$  can be. Hence, let us introduce the following notation.

**Definition 1.7** ([8]). For fixed  $\rho, q, k, m$ ,  $s_{q^m/q}(k, \rho)$  denotes the minimal  $\mathbb{F}_q$ -dimension of a rank  $\rho$ -saturating system in  $V(k, q^m)$ , or, equivalently, smallest rank of a  $(\rho-1)$ -saturating linear set in  $\text{PG}(k-1, q^m)$ .

In [8], the following bounds are proved.

**Theorem 1.8** ([8, Theorems 3.3 and 3.4]). The function  $s_{q^m/q}(k, \rho)$  satisfies the bounds

$$s_{q^m/q}(k, \rho) \geq \begin{cases} \left\lceil \frac{mk}{\rho} \right\rceil - m + \rho & \text{if } q > 2, \\ \left\lceil \frac{mk-1}{\rho} \right\rceil - m + \rho & \text{if } q = 2, \rho > 1, \\ m(k-1) + 1 & \text{if } q = 2, \rho = 1. \end{cases} \quad (2)$$

$$s_{q^m/q}(k, \rho) \leq m(k - \rho) + \rho. \quad (3)$$

**Remark 1.9.** *Let us resume here all other known properties of  $s_{q^m/q}(k, \rho)$ . By [8, Theorem 3.6] and [8, Theorem 3.8], the following holds, for all positive integers  $m, k, k', \rho \in [\min\{k, m\}]$ ,  $\rho' \in [\min\{k', m\}]$ .*

- (a) *If  $\rho < \min\{k, m\}$ , then  $s_{q^m/q}(k, \rho + 1) \leq s_{q^m/q}(k, \rho)$ .*
- (b)  *$s_{q^m/q}(k, \rho) < s_{q^m/q}(k + 1, \rho)$ .*
- (c) *If  $\rho < m$ , then  $s_{q^m/q}(k + 1, \rho + 1) \leq s_{q^m/q}(k, \rho) + 1$ .*
- (d) *If  $\rho + \rho' \leq \min\{k + k', m\}$ ,  $s_{q^m/q}(k + k', \rho + \rho') \leq s_{q^m/q}(k, \rho) + s_{q^m/q}(k', \rho')$ .*

*Using linear cutting blocking sets, introduced in [1], one gets*

$$s_{q^{r(k-1)/q}}(k, k-1) \leq 2k + r - 2,$$

*(see [8, Corollary 4.7.]) and  $s_{q^{2r}/q}(3, 2) \leq r + 3$  for all  $r \geq 4$  (an easy consequence of [22, Theorem 7.16]).*

*Using subgeometries (see [8, Theorem 4.14.]), one gets*

$$s_{q^{tr}/q}(t(r-1) + 1 + h, t(r-1) + 1) \leq th + t(r-1) + 1,$$

*for  $t, s \geq 2, h \geq 0$ .*

*Finally,  $s_{q^m/q}(k, \rho)$  is determined in the following case (see [8, Section 5]):*

$$\begin{aligned} s_{q^m/q}(k, 1) &= m(k-1) + 1, & \text{for all } m, k \geq 2, \\ s_{q^m/q}(k, k) &= k, & \text{for all } m, k \geq 2, \\ s_{q^{2r}/q}(3, 2) &= r + 2, & \text{for } r \neq 3, 5 \pmod{6} \text{ and } r \geq 4, \\ s_{q^{2r}/q}(3, 2) &= r + 2, & \text{for } \gcd(r, (q^{2s} - q^s + 1)!) = 1, r \text{ odd}, 1 \leq s \leq r, \gcd(r, s) = 1 \text{ (see [25])}, \\ s_{q^{10}/q}(3, 2) &= 7, & \text{for } q = p^{15h+s}, p \in \{2, 3\}, \gcd(s, 15) = 1 \text{ (see [4])}, \\ s_{q^{10}/q}(3, 2) &= 7, & \text{for } q = 5^{15h+1}, \text{ (see [4])}, \\ s_{q^{10}/q}(3, 2) &= 7, & \text{for } q \text{ odd}, q = 2, 3 \pmod{5} \text{ and for } q = 2^{2h+1}, h \geq 1, \text{ (see [25])}, \\ s_{q^{2r}/q}(2r, 2r-1) &= 2r + 1, & \text{for all } r \geq 2. \end{aligned}$$

## 2 Saturating systems meeting the lower bound

In this section we aim to present saturating systems of minimal  $\mathbb{F}_q$ -dimension.

The first construction is based essentially on the notion of Moore matrix. Let us recall that a square matrix over  $\mathbb{F}_q$  is a Moore matrix if it has successive powers of the Frobenius automorphism applied to its columns. It is invertible if and only if the elements in the left hand column are linearly independent over  $\mathbb{F}_q$ .

**Theorem 2.1.** *Let  $k = \rho t$  for some integer  $t \geq 1$ . Then*

$$U := \{(x_1, x_1^q, \dots, x_1^{q^{\rho-1}}, x_2, x_2^q, \dots, x_2^{q^{\rho-1}}, \dots, x_{t-1}, x_{t-1}^q, \dots, x_{t-1}^{q^{\rho-1}}, a_1, a_2, \dots, a_\rho)^T : x_i \in \mathbb{F}_{q^m}, a_j \in \mathbb{F}_q\}.$$

*is rank  $\rho$ -saturating. Therefore,*

$$s_{q^m/q}(\rho t, \rho) = m(t-1) + \rho.$$

*Proof.* Let  $r = t-1$  and consider the  $\mathbb{F}_q$ -vector space

$$U := \{(x_1, x_1^q, \dots, x_1^{q^{\rho-1}}, x_2, x_2^q, \dots, x_2^{q^{\rho-1}}, \dots, x_r, x_r^q, \dots, x_r^{q^{\rho-1}}, a_1, a_2, \dots, a_\rho)^T : x_i \in \mathbb{F}_{q^m}, a_j \in \mathbb{F}_q\}.$$

Let

$$v = (Y_1^{(1)}, \dots, Y_\rho^{(1)}, Y_1^{(2)}, \dots, Y_\rho^{(2)}, \dots, Y_1^{(r)}, \dots, Y_\rho^{(r)}, A_1, \dots, A_\rho)^T \in V(k, q^m).$$

We want to determine

$$u_i = (x_1^{(i)}, \dots, (x_1^{(i)})^{q^{\rho-1}}, x_2^{(i)}, \dots, (x_2^{(i)})^{q^{\rho-1}}, \dots, x_r^{(i)}, \dots, (x_r^{(i)})^{q^{\rho-1}}, a_1^{(i)}, a_2^{(i)}, \dots, a_\rho^{(i)})^T \in U$$

such that

$$v \in \langle u_1, \dots, u_\rho \rangle_{\mathbb{F}_q^m}.$$

Let  $s \in \{0, \dots, \rho\}$  be the  $\mathbb{F}_q$ -rank of  $A_1, \dots, A_\rho$ .

Without loss of generality we can suppose that  $A_1, \dots, A_s$  are  $\mathbb{F}_q$ -linear independent and

$$A_j = \sum_{h=1}^s \alpha_j^{(h)} A_h,$$

for  $j \in \{s+1, \dots, \rho\}$  and  $\alpha_j^{(h)} \in \mathbb{F}_q$ . Set  $\lambda_i = A_i$ , for  $i \in [s]$  and choose

$$\begin{pmatrix} a_1^{(1)} & a_2^{(1)} & \cdots & a_\rho^{(1)} \\ a_1^{(2)} & a_2^{(2)} & \cdots & a_\rho^{(2)} \\ \vdots & \vdots & & \vdots \\ a_1^{(k)} & a_2^{(k)} & \cdots & a_\rho^{(k)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & \alpha_{s+1}^{(1)} & \alpha_{s+2}^{(1)} & \cdots & \alpha_\rho^{(1)} \\ 0 & 1 & \cdots & 0 & \alpha_{s+1}^{(2)} & \alpha_{s+2}^{(2)} & \cdots & \alpha_\rho^{(2)} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{s+1}^{(s)} & \alpha_{s+2}^{(s)} & \cdots & \alpha_\rho^{(s)} \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \quad (4)$$

Consider  $\lambda_{s+1}, \dots, \lambda_\rho$  such that  $A_1, \dots, A_s, \lambda_{s+1}, \dots, \lambda_\rho$  are  $\mathbb{F}_q$ -linear independent.

Thus for each  $j \in [r]$  there exists a unique  $(x_j^{(1)}, \dots, x_j^{(\rho)})^T \in \mathbb{F}_{q^m}^\rho$  such that

$$(x_j^{(1)}, \dots, x_j^{(\rho)}) \begin{pmatrix} \lambda_1 & \sqrt[q]{\lambda_1} & \cdots & \sqrt[q^{\rho-1}]{\lambda_1} \\ \lambda_2 & \sqrt[q]{\lambda_2} & \cdots & \sqrt[q^{\rho-1}]{\lambda_2} \\ \vdots & \vdots & & \vdots \\ \lambda_\rho & \sqrt[q]{\lambda_\rho} & \cdots & \sqrt[q^{\rho-1}]{\lambda_\rho} \end{pmatrix} = \left( Y_1^{(j)}, \sqrt[q]{Y_2^{(j)}}, \dots, \sqrt[q^{\rho-1}]{Y_\rho^{(j)}} \right),$$

i.e.

$$(\lambda_1, \dots, \lambda_\rho) \begin{pmatrix} x_j^{(1)} & (x_j^{(1)})^q & \dots & (x_j^{(1)})^{q^{\rho-1}} \\ x_j^{(2)} & (x_j^{(2)})^q & \dots & (x_j^{(2)})^{q^{\rho-1}} \\ \vdots & \vdots & & \vdots \\ x_j^{(\rho)} & (x_j^{(\rho)})^q & \dots & (x_j^{(\rho)})^{q^{\rho-1}} \end{pmatrix} = (Y_1^{(j)}, Y_2^{(j)}, \dots, Y_\rho^{(j)}).$$

This, together with (4), provides a choice for  $u_i$ ,  $i \in [\rho]$  such that  $v \in \langle u_1, \dots, u_\rho \rangle_{\mathbb{F}_{q^m}}$  and shows that any vector  $v \in V(k, q^m)$  is  $\rho$ -saturated.

Such a  $\rho$  is minimal since

$$s_{q^m/q}(\rho t, \rho - 1) \geq \frac{\rho}{\rho - 1} \cdot m(t - 1) + \frac{m}{\rho - 1} + \rho - 1 > m(t - 1) + \rho,$$

for  $q > 2$ , and similarly for  $q = 2$ . □

**Remark 2.2.** Observe that in Theorem 2.1 one can also consider the set

$$U := \{(x_1, x_1^{q^{s_1}}, \dots, x_1^{q^{s_1(\rho-1)}}, \dots, x_r, x_r^{q^{s_r}}, \dots, x_r^{q^{s_r(\rho-1)}}, a_1, a_2, \dots, a_\rho)^T : x_i \in \mathbb{F}_{q^m}, a_j \in \mathbb{F}_q\},$$

with  $\gcd(m, s_j) = 1$  and prove with the same arguments that  $U$  is rank  $\rho$ -saturating.

The second construction is based on the following generalization of scattered linear sets, introduced first in [14].

**Definition 2.3.** Let  $U$  be an  $\mathbb{F}_q$ -subspace of  $V(k, q^m)$  and  $h < k$  be a positive integer. Then  $U$  is called  $h$ -scattered if  $\langle U \rangle_{\mathbb{F}_{q^m}} = V$  and for every  $\mathbb{F}_{q^m}$ -subspace  $W$  of  $V$  of dimension  $h$ ,  $\dim_{\mathbb{F}_q}(W \cap U) \leq h$ .

The  $\mathbb{F}_q$ -dimension of an  $h$ -scattered subspace is upper bounded as follows.

**Theorem 2.4** ([14, Theorem 2.3.]). Let  $U$  be an  $h$ -scattered  $\mathbb{F}_q$ -subspace of  $V(k, q^m)$ . Then either

$$\dim_{\mathbb{F}_q} U \leq \left\lfloor \frac{km}{h+1} \right\rfloor, \tag{5}$$

or  $\dim_{\mathbb{F}_q} U = k$  and  $U$  defines a subgeometry of  $\text{PG}(k-1, q^m)$  and it is  $(k-1)$ -scattered.

**Definition 2.5.** An  $h$ -scattered  $\mathbb{F}_q$ -subspace of  $V(k, q^m)$  whose  $\mathbb{F}_q$ -dimension meets the bound (5) is called maximum  $h$ -scattered.

**Remark 2.6.** The upper bound (5) is known to be achieved in the following cases:

- (a)  $h = 1$  and  $mk$  is even, see [2, 5, 6, 13];
- (b)  $h = 1$ ,  $k = 3$ ,  $m = 3$ , see [4];



- (c)  $h = 1, k = 3, m = 5, q = p^{15t+s}$  with  $p \in \{2, 3\}$  and  $\gcd(s, 15) = 1$  or  $q = 5^{15t+1}$ , see [4];
- (d)  $h = 1, k = 3, m = 5, q$  odd and  $q \equiv 2, 3 \pmod{5}$  or  $q = 2^{2t+1}$  with  $t \geq 1$ , see [25];
- (e)  $h = m - 3$  and  $m \geq 4$  is even and  $k = r(m - 2)/2$  where  $r \geq 3$  is odd, see [14, Theorem 3.6];
- (f)  $h = k - 1$  and  $k \leq m$ , see [14, Lemma 2.2];
- (g)  $(h + 1) | k$  and  $m \geq h + 1$ , see [14, 29].

**Theorem 2.7.** *Let  $m \geq h + 1$ . If  $U$  is an  $h$ -scattered  $\mathbb{F}_q$ -subspace of  $V(k, q^m)$  of  $\mathbb{F}_q$ -dimension (at least)  $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$ , then  $U$  is rank  $\rho$ -saturating, with  $\rho \leq h + 1$ .*

*Proof.* Let  $P := \langle v \rangle_{\mathbb{F}_{q^m}}$  with  $P \notin L_U$  and project  $U$  from  $P$  to a hyperplane  $\mathcal{H}$  of  $V(k, q^m)$  not containing  $\langle v \rangle_{\mathbb{F}_{q^m}}$ . Let  $\overline{U}$  be such a projection. Then  $\overline{U}$  is a subspace of  $\mathcal{H}$  of  $\mathbb{F}_q$ -dimension  $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$  which is not  $h$ -scattered since its dimension exceeds the upper bound in Theorem 2.4. Hence there exists an  $\mathbb{F}_{q^m}$ -subspace  $\mathcal{M}$  of  $\mathcal{H}$  of  $\mathbb{F}_{q^m}$ -dimension  $h$  such that  $\dim_{\mathbb{F}_q}(\mathcal{M} \cap \overline{U}) \geq h + 1$ . Let  $\mathcal{N} = \langle v, \mathcal{M} \rangle_{\mathbb{F}_{q^m}}$ , which is clearly of  $\mathbb{F}_{q^m}$ -dimension  $h + 1$  and such that  $\dim_{\mathbb{F}_q}(\mathcal{N} \cap U) \geq h + 1$ . Let  $u_1, \dots, u_{h+1} \in \mathcal{N} \cap U$  be  $h + 1$  linearly independent vectors over  $\mathbb{F}_q$ . The  $\mathbb{F}_{q^m}$ -vector space  $\langle u_1, \dots, u_{h+1} \rangle_{\mathbb{F}_{q^m}}$  must have dimension  $h + 1$ , since otherwise we would get a contradiction with  $U$  being  $h$ -scattered. So  $\mathcal{N} = \langle u_1, \dots, u_{h+1} \rangle_{\mathbb{F}_{q^m}}$ . Hence  $v \in \mathcal{N}$  is  $(h + 1)$ -saturated by  $U$ .  $\square$

**Corollary 2.8.** *Let  $m \geq 4$  be an even integer. For  $q > 2$ , if  $r = 3$  and  $m < 12$  or  $r > 3$  odd, then*

$$\frac{mr}{2} - 2 \leq s_{q^m/q} \left( \frac{r(m-2)}{2}, m-2 \right) \leq \frac{mr}{2} - 1.$$

*For  $q = 2$ , the same holds if  $r = 3$  and  $m < 10$  or  $r > 3$  odd.*

*Proof.* If  $r \geq 3$  is odd and  $m \geq 4$  is even, as recalled in Remark 2.6, there exists a maximum  $(m-3)$ -scattered subspace, say  $W$ , in  $V(r(m-2)/2, q^m)$ . Let  $U$  be a subspace of  $W$  of dimension

$$\left\lfloor \frac{m(\frac{r(m-2)}{2} - 1)}{m-2} \right\rfloor + 1 = \frac{mr}{2} - 1.$$

By Theorem 2.7,  $U$  is  $\rho$ -saturating with  $\rho \leq m - 2$ . We have that  $U$  cannot be rank  $h$ -saturating with  $h < m - 2$ , because otherwise its  $\mathbb{F}_q$ -dimension would be smaller than the lower bound (1). Actually, for  $q > 2$ ,

$$\left\lceil \frac{m}{m-2-t} \cdot \frac{r(m-2)}{2} \right\rceil - 2 - t > \frac{mr}{2} - 1$$

for all  $0 < t < m - 2$ , when either  $r \geq 4$  or  $r = 3$  and  $m < 12$ .

For  $q = 2$ , exactly the same arguments, with the slightly different lower bound, lead to the stated result.  $\square$

**Corollary 2.9.** *If  $mk$  is even, then*

$$\left\lceil \frac{m(k-2)}{2} \right\rceil + 2 \leq s_{q^m/q}(k, 2) \leq \left\lfloor \frac{m(k-1)}{2} \right\rfloor + 1 = \left\lceil \frac{m(k-2)}{2} \right\rceil + 2 + \left\lfloor \frac{m}{2} \right\rfloor - 1.$$

*In particular  $s_{q^2/q}(k, 2) = k$ . Moreover,*

$$s_{q^5/q}(3, 2) \in \{5, 6\}$$

*for  $q = p^t$  with  $p \in \{2, 3, 5\}$  and*

$$s_{q^3/q}(3, 2) = 4.$$

*Proof.* The proof works exactly as for Corollary 2.8, in the case stated in Remark 2.6 for  $h = 1$ . Proving that  $\rho = 2$  it is much easier here, with simple inequalities.  $\square$

**Remark 2.10.** *Note that Theorem 2.7 does not give stronger results in the case  $\rho|k$ .*

### 3 Non-tightness of the lower bound

In this section we will show that the lower bound (1) is not tight in general. In order to do it, we will consider  $s_{q^4/q}(3, 2)$ . The lower bound states that

$$s_{q^4/q}(3, 2) \geq 4$$

and it is easy to realize that

$$s_{q^4/q}(3, 2) \leq 5,$$

because an example of rank 2-saturating system of rank 5 is obtained considering an  $\mathbb{F}_q$ -linear sets of rank 5 with a line of weight 4 (with a scattered underlying space) and a point outside it. MAGMA computational results show that  $s_{16/2}(3, 2) = s_{81/3}(3, 2) = 5$ , so that the lower bound is not tight in the binary and ternary case. In the rest of the section we aim to generalize this result for infinitely many values of  $q$ . We will prove the following.

**Theorem 3.1.** *If  $q$  is even and large enough, then  $s_{q^4/q}(3, 2) = 5$ .*

Since most of the calculations and results will be based on the parity of  $q$ , let us *suppose, from now on, that  $q$  is even*.

We want to show that for any  $\mathbb{F}_q$ -linear set  $L_U$  of rank 4 in  $\text{PG}(2, q^4)$ , there exists a point  $P \notin L_U$  for which do not pass any secant line to  $L_U$ . The proof of the theorem will be divided into four lemmas. The proof of the last three is very technical and it is left to the Appendix.

Let  $X_0, X_1, X_2$  be homogeneous projective coordinates in  $\text{PG}(2, q^4)$  and let  $(a_0 : a_1 : a_2)$  denote the coordinates of a point of the plane. We will use frequently the following general result.

**Remark 3.2.** Let  $L_U$  be a linear set in  $\text{PG}(k-1, q^m)$ ,  $H$  a hyperplane and  $P$  a point not belonging to  $L_U$  nor to  $H$ . If the projection of  $L_U$  from  $P$  to  $H$  is scattered, then the point is not 1-saturated, because otherwise in the projection we would find a point of weight at least 2.

**Lemma 3.3.** Let  $L_U$  be an  $\mathbb{F}_q$ -linear set of rank 4 in  $\text{PG}(2, q^4)$ . If  $U$  is rank 2-saturating, then, up to  $\text{GL}(3, q^4)$ -equivalence,

$$U = U_{\alpha, \beta} = \left\{ (x, x^q + \alpha x^{q^3}, x^{q^2} + \beta x^{q^3})^T : x \in \mathbb{F}_{q^4} \right\},$$

with  $\alpha \in \mathbb{F}_{q^2}$ ,  $\beta \in \mathbb{F}_{q^4}$  such that  $\alpha^{q+1} = 1$  and  $\beta^{(q^2+1)(q-1)} = 1$ .

*Proof.* Note that we can always assume that  $U = \{(x, f(x), g(x))^T : x \in \mathbb{F}_{q^4}\}$ , with  $f, g$  two  $\mathbb{F}_q$ -linear maps of  $\mathbb{F}_{q^4}$ . Up to  $\text{GL}(3, q^4)$ -equivalence, one of the following cases occur

- 1)  $U = \{(x, x^q, x^{q^2})^T : x \in \mathbb{F}_{q^4}\}$ ;
- 2)  $U_\alpha = \{(x, x^q + \alpha x^{q^2}, x^{q^3})^T : x \in \mathbb{F}_{q^4}\}$ , with  $\alpha \in \mathbb{F}_{q^4}^*$ ;
- 3)  $U_\alpha = \{(x, x^q + \alpha x^{q^3}, x^{q^2})^T : x \in \mathbb{F}_{q^4}\}$  with  $\alpha \in \mathbb{F}_{q^4}^*$ ;
- 4)  $U_{\alpha, \beta} = \{(x, x^q + \alpha x^{q^3}, x^{q^2} + \beta x^{q^3})^T : x \in \mathbb{F}_{q^4}\}$  with  $\alpha, \beta \in \mathbb{F}_{q^4}^*$ ;

Case 1) (resp. Case 2)). By projecting  $L_U$  (resp.  $L_{U_\alpha}$ ) from the point  $(0 : 0 : 1)$  (resp.  $(0 : 1 : 0)$ ) to the line with equation  $X_2 = 0$  (resp.  $X_1 = 0$ ), we obtain the set

$$\{(x : x^q) : x \in \mathbb{F}_{q^4}\},$$

(resp.  $\{(x : x^{q^3}) : x \in \mathbb{F}_{q^4}\}$ ) which is scattered and thus the point  $(0 : 0 : 1)$  (resp.  $(0 : 1 : 0)$ ) is not saturated, since through such a point there does not pass any secant line to  $L_U$  (resp.  $L_{U_\alpha}$ ).

Case 3) First, by substituting  $x$  by  $\lambda x$  with  $\lambda \in \mathbb{F}_{q^4}^*$  and dividing by  $\lambda^q$ , the  $\mathbb{F}_q$ -subspace  $U_\alpha$  is equivalent to

$$\{(x, x^q + \alpha \lambda^{q^3-q} x^{q^3}, x^{q^2}) : x \in \mathbb{F}_{q^4}\}$$

and since

$$\mathbb{F}_{q^4}^* = \left\{ \alpha z : \alpha \in \mathbb{F}_{q^2}^*, z \in \mathbb{F}_{q^4}, z^{q^2+1} = 1 \right\},$$

we have that  $\alpha$  can be chosen in  $\mathbb{F}_{q^2}^*$ .

If  $\alpha^{q+1} \neq 1$  then by projecting  $L_U$  (resp.  $L_{U_\alpha}$ ) from the point  $(0 : 0 : 1)$  to the line with equation  $X_2 = 0$ , we obtain the set

$$\{(x : x^q + \alpha \lambda^{q-q^3} x^{q^3}) : x \in \mathbb{F}_{q^4}\},$$

which is scattered and thus the point  $(0 : 0 : 1)$  is not saturated.

Consider the case  $\alpha = 1$ . Note that the point  $(1 : 0 : 1)$  is of weight 2. By projecting  $L_U$  from the point  $(1 : 0 : 0)$  to the line with equation  $X_0 = 0$ , we obtain the set

$$\Lambda := \left\{ (x^q + x^{q^3} : x^{q^2}) : x \in \mathbb{F}_{q^4} \right\} = \left\{ (x^q + x^{q^3} : x) : x \in \mathbb{F}_{q^4} \right\}.$$

Now,  $(0 : 1)$  is the unique point of  $\Lambda$  of weight 2 and this means that all the lines through  $(1 : 0 : 0)$  intersect  $L_U$  in a unique point and thus  $L_U$  is not saturating.

Suppose now  $\alpha^{q+1} = 1$  and  $\alpha \neq 1$ . Let  $\omega \in \mathbb{F}_{q^2}$  such that  $\omega^q + \omega + \alpha \neq 0$ . By projecting  $L_U$  from the point  $(1 : 0 : \omega)$  to the line with equation  $X_0 = 0$ , we obtain the set

$$\Lambda := \left\{ (x^q + \alpha x^{q^3} : x^{q^2} + \omega x) : x \in \mathbb{F}_{q^4} \right\}.$$

The function  $x \mapsto x^q + \alpha x^{q^3}$  is a bijection, whose inverse is  $x \mapsto \frac{\alpha}{1+\alpha^2}x^q + \frac{\alpha^2}{1+\alpha^2}x^{q^3}$ . This means that the set  $\Lambda$  is equivalent to

$$\left\{ \left( x : \frac{\alpha}{1+\alpha^2}x^{q^3} + \frac{\alpha^2}{1+\alpha^2}x^q + \omega \frac{\alpha}{1+\alpha^2}x^q + \omega \frac{\alpha^2}{1+\alpha^2}x^{q^3} \right) : x \in \mathbb{F}_{q^4} \right\},$$

and so

$$\Lambda \simeq \left\{ (x : (\alpha + 1)x^{q^3} + (\omega + \alpha)x^q) : x \in \mathbb{F}_{q^4} \right\},$$

which is scattered if and only if  $N_{q^4/q}((\omega + \alpha)/(\omega\alpha + 1)) \neq 1$ .

Since both  $\alpha$  and  $\omega$  belong to  $\mathbb{F}_{q^2}$ , the previous condition is equivalent to

$$\frac{(\omega + \alpha)(\omega^q + 1/\alpha)}{(\omega\alpha + 1)(\omega^q/\alpha + 1)} \neq 1,$$

that is

$$\omega^q + \omega + \alpha \neq 0.$$

Thus  $(1 : 0 : \omega)$  is not saturated.

Case 4) By substituting  $x$  by  $\lambda x$  with  $\lambda \in \mathbb{F}_{q^4}^*$  and dividing by  $\lambda^q$ , the  $\mathbb{F}_q$ -subspace  $U_{\alpha,\beta}$  is equivalent to

$$\left\{ (x, x^q + \alpha \lambda^{q^3-q} x^{q^3}, x^{q^2} + \beta \lambda^{q^3-q^2} x^{q^3}) : x \in \mathbb{F}_{q^4} \right\}$$

and since

$$\mathbb{F}_{q^4}^* = \left\{ \alpha z : \alpha \in \mathbb{F}_{q^2}^*, z \in \mathbb{F}_{q^4}, z^{q^2+1} = 1 \right\},$$

we have that  $\alpha$  can be chosen in  $\mathbb{F}_{q^2}^*$ . Also, substituting  $x$  by  $\lambda x$  with  $\lambda \in \mathbb{F}_{q^2}^*$  and dividing by  $\lambda$ , the  $\mathbb{F}_q$ -subspace  $U_{\alpha,\beta}$ , with  $\alpha \in \mathbb{F}_{q^2}^*$  is equivalent to

$$\left\{ (x, x^q + \alpha x^{q^3}, x^{q^2} + \beta \lambda^{q-1} x^{q^3}) : x \in \mathbb{F}_{q^4} \right\}$$

and since

$$\mathbb{F}_{q^4}^* = \left\{ \beta z : \beta \in \mathbb{F}_{q^4}, z \in \mathbb{F}_{q^2}, \beta^{(q^2+1)(q-1)} = 1, z^{q+1} = 1 \right\},$$

we have that  $\beta$  can be chosen in  $\mathbb{F}_{q^4}$  such that  $\beta^{(q^2+1)(q-1)} = 1$ . Finally, by projecting  $L_{U_{\alpha,\beta}}$  from the point  $(0 : 0 : 1)$  to the line with equation  $X_2 = 0$ , we have that the set

$$\left\{ (x : x^q + \alpha x^{q^3}) : x \in \mathbb{F}_{q^4} \right\}$$

is scattered if and only if  $N_{q^4/q}(\alpha) \neq 1$ . This means that if  $\alpha \in \mathbb{F}_{q^2}$  and  $\alpha^{q+1} \neq 1$ , then the point  $(0 : 0 : 1)$  is not 1-saturated. Hence we can reduce to the study of the  $\mathbb{F}_q$ -subspace  $U_{\alpha,\beta}$  with  $\alpha \in \mathbb{F}_{q^2}$ ,  $\beta \in \mathbb{F}_{q^4}$  such that  $\alpha^{q+1} = 1$  and  $\beta^{(q^2+1)(q-1)} = 1$ .  $\square$

**Lemma 3.4.** *Let  $\alpha^{q+1} = 1$ ,  $\beta^{(q^2+1)(q-1)} = 1$ , with  $\alpha \neq 1$ . If  $q$  is large enough, then  $U_{\alpha,\beta}$  is not 2-saturating.*

**Lemma 3.5.** *Let  $\alpha = 1$ ,  $\beta \in \mathbb{F}_q^*$ . If  $q \geq 64$  then  $U_{\alpha,\beta}$  is not 2-saturating.*

**Lemma 3.6.** *Let  $\alpha = 1$ ,  $\beta \notin \mathbb{F}_q$ . If  $q \geq 64$  then  $U_{\alpha,\beta}$  is not 2-saturating.*

Theorem 3.1 now follows from the above three lemmas, whose proofs are in the Appendix.

## 4 Conclusion and open problems

In this paper we continued the investigation of saturating linear sets of small rank introduced in [8]. In the following remark we resume all the parameters for which we know the exact value of  $s_{q^m/q}(k, \rho)$ .

**Remark 4.1.** *The lower bound (1) is met in the following cases:*

$$\begin{aligned} s_{q^m/q}(\rho t, \rho) &= m(t-1) + \rho, & \text{for all } t \geq 1, m \geq 2, \\ s_{q^2/q}(k, 2) &= k, & \text{for all } k \geq 2, \\ s_{q^3/q}(3, 2) &= 4, \\ s_{q^{2r}/q}(3, 2) &= r+2, & \text{for } r \neq 3, 5 \pmod{6} \text{ and } r \geq 4, \\ s_{q^{2r}/q}(3, 2) &= r+2, & \text{for } \gcd(r, (q^{2s} - q^s + 1)!) = 1, r \text{ odd}, 1 \leq s \leq r, \gcd(r, s) = 1, \\ s_{q^{10}/q}(3, 2) &= 7, & \text{for } q = p^{15h+s}, p \in \{2, 3\}, \gcd(s, 15) = 1 \text{ and for } q = 5^{15h+1}, \\ s_{q^{10}/q}(3, 2) &= 7, & \text{for } q \text{ odd}, q = 2, 3 \pmod{5} \text{ and for } q = 2^{2h+1}, h \geq 1, \\ s_{q^{2r}/q}(3, 2) &= r+2, & \text{for } q \text{ odd}, q = 2, 3 \pmod{5} \text{ and for } q = 2^{2h+1}, h \geq 1, r \text{ odd}, \\ s_{q^{2r}/q}(2r, 2r-1) &= 2r+1, & \text{for all } r \geq 2. \end{aligned}$$

As shown in Section 3, there are some parameters for which (1) is not tight: for  $q$  even and large enough,  $s_{q^4/q}(3, 2) = 5 > 4$ .

The theory of saturating linear sets of small rank needs surely further investigations. We propose some open questions.

**Question 4.2.** *In Section 3 we showed that  $s_{q^4/q}(3, 2) = 5$  for  $q$  even and large enough. Can we prove the same result for  $q$  odd?*

The answer to the above question would need to adapt all results and calculations to the odd characteristic. A more ambitious result would be a general answer to the following.

**Question 4.3.** *Is it possible to characterize the parameters for which the bound is not tight?*

A generalized version of Remark 3.2 would probably help in finding an answer, at least for some (small) dimensions.

About the constructions, a classification of saturating linear sets meeting the bound would be interesting. A possible step towards such classification would be the following.

**Question 4.4.** *Can we find examples of rank  $\rho$ -saturating sets in  $V(\rho t, q^m)$  of minimal  $\mathbb{F}_q$ -dimension non-equivalent to those in Theorem 2.1 and Remark 2.2?*

## Acknowledgments

This research was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The second author was partially supported by the ANR-21-CE39-0009 - BARRACUDA (French *Agence Nationale de la Recherche*).

## References

- [1] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Linear cutting blocking sets and minimal codes in the rank metric. *Journal of Combinatorial Theory, Series A*, 192:105658, 2022.
- [2] S. Ball, A. Blokhuis, and M. Lavrauw. Linear  $(q+1)$ -fold blocking sets in  $\text{PG}(2, q^4)$ . *Finite Fields and Their Applications*, 6(4):294–301, 2000.
- [3] D. Bartoli. Hasse-weil type theorems and relevant classes of polynomial functions. *London Mathematical Society Lecture Note Series, Proceedings of 28th British Combinatorial Conference*, Cambridge University Press, to appear.
- [4] D. Bartoli, B. Csajbók, G. Marino, and R. Trombetti. Evasive subspaces. *Journal of Combinatorial Designs*, 29(8):533–551, 2021.
- [5] D. Bartoli, M. Giulietti, G. Marino, and O. Polverino. Maximum scattered linear sets and complete caps in Galois spaces. *Combinatorica*, 38:255–278, 2018.

- [6] A. Blokhuis and M. Lavrauw. Scattered spaces with respect to a spread in  $\text{PG}(n, q)$ . *Geometriae Dedicata*, 81:231–243, 2000.
- [7] E. Bombieri. Counting points on curves over finite fields. In *Séminaire Bourbaki : vol. 1972/73, exposés 418-435*, number 15 in Séminaire Bourbaki. Springer-Verlag, 1974. talk:430.
- [8] M. Bonini, M. Borello, and E. Byrne. Saturating systems and the rank covering radius. *to appear in Journal of Algebraic Combinatorics*, 2023.
- [9] E. Byrne and A. Ravagnani. Covering radius of matrix codes endowed with the rank metric. *SIAM Journal on Discrete Mathematics*, 31(2):927–944, 2017.
- [10] E. Byrne and A. Ravagnani. An Assmus–Mattson theorem for rank metric codes. *SIAM Journal on Discrete Mathematics*, 33(3):1242–1260, 2019.
- [11] A. Cafure and G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields and their Applications*, 12(2):155–185, 2006.
- [12] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. *Covering codes*. Elsevier, 1997.
- [13] B. Csajbók, G. Marino, O. Polverino, and F. Zullo. Maximum scattered linear sets and mrd-codes. *Journal of Algebraic Combinatorics*, 46:517–531, 2017.
- [14] B. Csajbók, G. Marino, O. Polverino, and F. Zullo. Generalising the scattered property of subspaces. *Combinatorica*, 41(2):237–262, 2021.
- [15] A. A. Davydov, S. Marcugini, and F. Pambianco. On saturating sets in projective spaces. *Journal of Combinatorial Theory, Series A*, 103(1):1–15, 2003.
- [16] A. A. Davydov and P. R. Östergård. On saturating sets in small projective geometries. *European Journal of Combinatorics*, 21(5):563–570, 2000.
- [17] L. Denaux. Constructing saturating sets in projective spaces using subgeometries. *Designs, Codes and Cryptography*, 90(9):2113–2144, 2022.
- [18] M. Gadouneau and Z. Yan. Packing and covering properties of rank metric codes. *IEEE Transactions on Information Theory*, 54(9):3873–3883, 2008.
- [19] M. Gadouneau and Z. Yan. Bounds on covering codes with the rank metric. *IEEE Communications Letters*, 13(9):691–693, 2009.
- [20] S. R. Ghorpade and G. Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Mosc. Math. J.*, 2(3):589–631, 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday.

- [21] S. R. Ghorpade and G. Lachaud. Number of solutions of equations over finite fields and a conjecture of Lang and Weil. In *Number theory and discrete mathematics (Chandigarh, 2000)*, Trends Math., pages 269–291. Birkhäuser, Basel, 2002.
- [22] A. Gruica, A. Ravagnani, J. Sheekey, and F. Zullo. Generalised scattered subspaces. *arXiv preprint arXiv:2207.01027*, 2022.
- [23] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.
- [24] S. Lang and A. Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76:819–827, 1954.
- [25] S. Lia, G. Longobardi, G. Marino, and R. Trombetti. Short rank-metric codes and scattered subspaces. *arXiv preprint arXiv:2306.01315*, 2023.
- [26] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.
- [27] G. Lunardon. Normal spreads. *Geom. Dedicata*, 75(3):245–261, 1999.
- [28] Z. L. Nagy. Saturating sets in projective planes and hypergraph covers. *Discrete Mathematics*, 341(4):1078–1083, 2018.
- [29] V. Napolitano, O. Polverino, G. Zini, and F. Zullo. Linear sets from projection of desarguesian spreads. *Finite Fields and Their Applications*, 71:101798, 2021.
- [30] F. Pambianco and L. Storme. Small complete caps in spaces of even characteristic. *Journal of Combinatorial Theory, Series A*, 75(1):70–84, 1996.
- [31] O. Polverino. Linear sets in finite projective spaces. *Discrete Mathematics*, 310(22):3096–3107, 2010.
- [32] W. Schmidt. *Equations over finite fields: an elementary approach*. Kendrick Press, Heber City, UT, second edition, 2004.
- [33] E. Ughi. Saturated configurations of points in projective Galois spaces. *European Journal of Combinatorics*, 8(3):325–334, 1987.



## A Appendix

In this Appendix we will make use of algebraic varieties over finite fields; see [3] for a survey on links between algebraic varieties over finite fields and relevant combinatorial objects.

A variety and more specifically a curve, i.e. a variety of dimension 1, are described by a certain set of equations with coefficients in a finite field  $\mathbb{F}_q$ . A variety defined by a unique equation is called a hypersurface. We say that a variety  $\mathcal{V}$  is *absolutely irreducible* if there are no varieties  $\mathcal{V}'$  and  $\mathcal{V}''$  defined over the algebraic closure of  $\mathbb{F}_q$  and different from  $\mathcal{V}$  such that  $\mathcal{V} = \mathcal{V}' \cup \mathcal{V}''$ . If a variety  $\mathcal{V} \subseteq \text{PG}(k-1, q)$  is defined by  $F_i(X_0, \dots, X_k) = 0$ , for  $i \in [s]$ , an  $\mathbb{F}_q$ -rational point of  $\mathcal{V}$  is a point  $(x_0 : \dots : x_k) \in \text{PG}(k-1, q)$  such that  $F_i(x_0, \dots, x_k) = 0$ , for  $i \in [s]$ . A point is affine if  $x_0 \neq 0$ . The set of the  $\mathbb{F}_q$ -rational points of  $\mathcal{V}$  is usually denoted by  $\mathcal{V}(\mathbb{F}_q)$ .

In what follows, we mainly focus on algebraic hypersurfaces, i.e. algebraic varieties that may be defined by a single implicit equation. An algebraic hypersurface defined over a finite field  $\mathbb{F}_q$  is *absolutely irreducible* if the associated polynomial is irreducible over every algebraic extension of  $\mathbb{F}_q$ . An absolutely irreducible  $\mathbb{F}_q$ -rational component of a hypersurface  $\mathcal{S}$ , defined by the polynomial  $F$ , is simply an absolutely irreducible hypersurface such that the associated polynomial has coefficients in  $\mathbb{F}_q$  and it is a factor of  $F$ . For a deeper introduction to algebraic varieties we refer the interested reader to [23].

In the small-degree regime (usually when  $\max\{\deg(f), \deg(g)\} \lesssim \sqrt[4]{q}$ ), the existence of an absolutely irreducible component in a hypersurface (or more in general a variety) yields the existence of suitable  $\mathbb{F}_q$ -rational points of the hypersurface itself, due to estimates on the number of  $\mathbb{F}_q$ -rational points of an algebraic variety such as the Lang-Weil bound [24] and its generalizations.

**Theorem A.1** (Lang-Weil Theorem). *Let  $\mathcal{V} \subseteq \text{PG}(k-1, q)$  be an absolutely irreducible variety of dimension  $n$  and degree  $d$ . Then there exists a constant  $C$  depending only on  $k$ ,  $n$ , and  $d$  such that*

$$\left| \#(\mathcal{V}(\mathbb{F}_q)) - \sum_{i=0}^n q^i \right| \leq (d-1)(d-2)q^{n-1/2} + Cq^{n-1}.$$

Although the constant  $C$  was not computed in [24], explicit estimates have been provided for instance in [7, 11, 20, 21, 26, 32] and they have the general shape  $C = r(d)$  provided that  $q > s(n, d)$ , where  $r$  and  $s$  are polynomials of (usually) small degree. We refer to [11] for a survey on these bounds. In the following we will make use of Theorem A.1 in small degree regime. Actually, for a variety having an absolutely irreducible component defined over  $\mathbb{F}_q$ , when the degree of the variety is nondepending on  $q$  and for  $q$  large enough, Theorem A.1 yields the existence of roughly  $q^n - O(q^{n-1/2})$   $\mathbb{F}_q$ -rational points.

Consider

$$d_{\alpha,\beta}(C) := ((\alpha^4 + 1)C^4 + \alpha(\alpha + 1)^2 \text{Tr}_{q^4/q}(\beta)C^3 + (\alpha^4 \beta^{q^3+q} + \alpha^2 \text{Tr}_{q^4/q}(\beta^{q+1}) + \beta^{q^2+1})C^2 + \alpha(\alpha^2(\beta^{q^3+q+1} + \beta^{q^3+q^2+q}) + \alpha \text{Tr}_{q^4/q}(\beta) + \beta^{q^2+q+1} + \beta^{q^3+q^2+1})C + \alpha^2(\text{N}_{q^4/q}(\beta) + 1))^2,$$

$$f_{\alpha,\beta}(C) := \alpha^3 \beta^{q^3} C^{q^2+q+1} + \alpha \beta^{q^2} C^{q^3+q+1} + \alpha \beta C^{q^3+q^2+q} + \alpha^3 \beta^q C^{q^3+q^2+1} + (\alpha^3 + \alpha^2 \beta^{q^3+q^2})C^{q+1} + \alpha^4 \beta^{q^3+q} C^{q^2+1} + (\alpha^2 \beta^{q^2+q} + \alpha)C^{q^3+1} + (\alpha^3 + \alpha^2 \beta^{q+1} C^{q^3+q^2} + (\alpha^2 \beta^{q^3+1} + \alpha)C^{q^2+q} + \beta^{q^2+1} C^{q^3+q} + (\alpha^3 \beta^{q^3+q^2+q} + \alpha^2 \beta^{q^3})C + (\alpha^2 \beta + \alpha \beta^{q^3+q^2+1})C^q + (\alpha^3 \beta^{q^3+q+1} + \alpha^2 \beta^q)C^{q^2} + (\alpha^2 \beta^{q^2} + \alpha \beta^{q^2+q+1})C^{q^3} + \alpha^2 \text{N}_{q^4/q}(\beta),$$

and

$$g_{\alpha,\beta}(C) := \text{N}_{q^4/q}(\alpha C^{q+1} + \alpha C^{q^3+1} + \alpha^2 \beta^q C + \beta C^q + \alpha \beta^{q+1}) \left( (\alpha + 1)C^{q^3+q^2+q+1} + (\alpha^3 + \alpha^2 + \alpha)\beta^{q^3} C^{q^2+q+1} + \alpha \beta^{q^2} C^{q^3+q+1} + (\alpha^3 + \alpha^2 \beta^{q^3+q^2})C^{q+1} + \beta^q(\alpha^3 + \alpha^2 + \alpha)C^{q^3+q^2+1} + (\alpha^4 + \alpha^3 + \alpha^2)\beta^{q^3+q}C^{q^2+1} + (\beta^{q^2+q} + 1)\alpha^2 C^{q^3+1} + \alpha^3(\beta^{q^3+q^2+q} + \beta^{q^3})C + \alpha \beta C^{q^3+q^2+q} + \alpha^2(\beta^{q^3+1} + 1)C^{q^2+q} + \beta^{q^2+1} C^{q^3+q} + (\alpha^2 \beta + \alpha \beta^{q^3+q^2+1})C^q + (\alpha^3 + \alpha^2 \beta^{q+1})C^{q^3+q^2} + \alpha^3(\beta^{q^3+q+1} + \beta^q)C^{q^2} + (\alpha^2 \beta^{q^2} + \alpha \beta^{q^2+q+1})C^{q^3} + \alpha^3 + \alpha^2 \beta^{q^3+q^2+q+1} + \alpha^2 \right) \cdot \left( (\alpha^4 + \alpha^2)C^{q^3+q^2+q+1} + \alpha^3 \text{Tr}_{q^4/q}(\beta^{q^3} C^{q^2+q+1}) + (\alpha^2 \beta^{q^2+q^3} + \alpha)C^{q+1} + \alpha^4 \beta^{q^3+q} C^{q^2+1} + \alpha^2 \beta^{q^2+1} C^{q^3+q}(\alpha^2 \beta^{q^2+q} + \alpha)C^{q^3+1} + (\alpha^2 \beta^{q^3+1} + \alpha)C^{q^2+q} + (\alpha^2 \beta^{q+1} + \alpha)C^{q^3+q^2} + (\alpha^3 \beta^{q^3+q^2+q} + \alpha^2 \beta^{q^3})C + (\alpha \beta^{q^3+q^2+1} + \beta)C^q + (\alpha^3 \beta^{q^3+q+1} + \alpha^2 \beta^q)C^{q^2} + (\alpha \beta^{q^2+q+1} + \beta^{q^2})C^{q^3} + \alpha^2 \beta^{q^3+q^2+q+1} + \alpha^2 + 1 \right).$$

Let

$$\Gamma_{\alpha,\beta} := \{c \in \mathbb{F}_q^4 : f_{\alpha,\beta}(c) = 0, \quad (c^2 \alpha^2 + \beta^2)(c^{2q+2} \alpha^2 + c^{2q} \beta^2 + 1) d_{\alpha,\beta}(c) g_{\alpha,\beta}(c) \neq 0\}.$$

**Lemma A.2.** *Let  $\alpha^{q+1} = 1$ ,  $\beta^{(q^2+1)(q-1)} = 1$ , with  $\alpha \neq 1$ . If  $q$  is large enough then  $\Gamma_{\alpha,\beta} \neq \emptyset$ .*

*Proof.* First observe that the polynomials  $f_{\alpha,\beta}(C)$ ,  $d_{\alpha,\beta}(C)$ ,  $g_{\alpha,\beta}(C)$  are nonvanishing.

To prove that  $\Gamma_{\alpha,\beta}$  is not empty, we will make use the following approach. Set  $X := C$ ,  $Y := C^q$ ,  $Z := C^{q^2}$ ,  $T := C^{q^3}$ , let  $\{\xi, \xi^q, \xi^{q^2}, \xi^{q^3}\}$  be a normal basis of  $\mathbb{F}_{q^4}$  over  $\mathbb{F}_q$ , and write  $C = C_0 \xi + C_1 \xi^q + C_2 \xi^{q^2} + C_3 \xi^{q^3}$ , where  $C_0, C_1, C_2, C_3 \in \mathbb{F}_q$ . Also, let  $\alpha = \alpha_0 \xi + \alpha_1 \xi^q + \alpha_2 \xi^{q^2} + \alpha_3 \xi^{q^3}$  and  $\beta = \beta_0 \xi + \beta_1 \xi^q + \beta_2 \xi^{q^2} + \beta_3 \xi^{q^3}$ .

Write  $f_{\alpha,\beta}(C)$  as  $f_{\alpha,\beta}(X, Y, Z, T)$ . Since  $\alpha^{q+1} = 1$ ,  $(f_{\alpha,\beta}(C))^q = f_{\alpha,\beta}(C)$  and thus the hypersurface defined by  $\mathcal{Y} : f_{\alpha,\beta}(C_0\xi + C_1\xi^q + C_2\xi^{q^2} + C_3\xi^{q^3}) = 0$  is  $\mathbb{F}_q$ -rational and projectively  $\mathbb{F}_{q^4}$ -isomorphic to the hypersurface  $\mathcal{X} : f_{\alpha,\beta}(X, Y, Z, T) = 0$  and of degree 3.

Note that  $\mathcal{X}$  is of degree one in  $T$  and thus is reducible only if  $f_{\alpha,\beta}(X, Y, Z, T) = \ell_1(X, Y, Z)T + \ell_2(X, Y, Z)$  possesses a factor depending only on  $X, Y, Z$ , which should be a common factor of the coefficient  $\ell_1(X, Y, Z)$  and  $\ell_2(X, Y, Z)$ . That is to say, the resultant between  $\ell_1(X, Y, Z)$  and  $\ell_2(X, Y, Z)$  with respect to  $Y$  should vanish. This is not possible since  $\alpha\beta \neq 0$ , as easy computations show.

The argument above yields the absolutely irreducibility of  $\mathcal{X}$  and thus of  $\mathcal{Y}$ , since the absolutely irreducibility is preserved by projectivity. Because  $\mathcal{Y}$  is defined over  $\mathbb{F}_q$  and absolutely irreducible, it has dimension 3 and it contains roughly at least  $q^3 - O(q^{5/2})$   $\mathbb{F}_q$ -rational points  $(x_0, y_0, z_0, t_0)$  which correspond to values  $C = x_0\xi + y_0\xi^q + x_2\xi^{q^2} + x_3\xi^{q^3}$  satisfying  $f_{\alpha,\beta}(C) = 0$ .

In order to show the existence of values  $C \in \mathbb{F}_{q^4}$  in  $\Gamma_{\alpha,\beta}$  it is enough to show that the hypersurface

$$\mathcal{Z} : (X^2\alpha^2 + \beta^2)(X^2Y^2\alpha^2 + \beta^2Y^2 + 1) d_{\alpha,\beta}(X, Y, Z, T) g_{\alpha,\beta}(X, Y, Z, T) = 0$$

does not contain  $\mathcal{X}$ , so that  $\mathcal{Z} \cap \mathcal{X}$  is subvariety of codimension one in  $\mathcal{X}$ . We have only to check that this actually holds for the hypersurface  $g_{\alpha,\beta}(X, Y, Z, T) = 0$ , being trivial for the other components of  $\mathcal{Z}$ . The four factors of degree 3 in  $g_{\alpha,\beta}(X, Y, Z, T)$  cannot be factors of  $f_{\alpha,\beta}(X, Y, Z, T)$ , being this polynomial irreducible. It can be easily checked that the resultants of each of two other factors of  $g_{\alpha,\beta}(X, Y, Z, T)$  and  $f_{\alpha,\beta}(X, Y, Z, T)$  with respect to  $T$  are non-vanishing polynomials and thus  $\mathcal{X}$  and  $\mathcal{Z}$  do not share any component. Thus  $\mathcal{Z} \cap \mathcal{X}$  is of dimension 2 and there are at most  $O(q^2)$   $\mathbb{F}_q$ -rational points  $(x_0, y_0, z_0, t_0)$  whose corresponding value  $C = x_0\xi + y_0\xi^q + x_2\xi^{q^2} + x_3\xi^{q^3}$  satisfies  $f_{\alpha,\beta}(C) = 0$  and  $(C^2\alpha^2 + \beta^2)(C^{2q+2}\alpha^2 + C^{2q}\beta^2 + 1) d_{\alpha,\beta}(C) g_{\alpha,\beta}(C) = 0$ . This yields  $|\Gamma_{\alpha,\beta}| = q^3 - O(q^{5/2})$  and the claim follows.  $\square$

*Proof of Lemma 3.4.* We will prove that each point  $P_C := (0 : 1 : C) \in \text{PG}(2, q^4)$ ,  $C \in \Gamma_{\alpha,\beta}$ , is not 1-saturated by  $L_{U_{\alpha,\beta}}$ . Since by Lemma A.2  $\Gamma_{\alpha,\beta} \neq \emptyset$ , this will prove the claim.

Since  $U_{\alpha,\beta}$  is 2-saturating if and only if  $U_{\alpha^2,\beta^2}$  is 2-saturating, in the following, for the seek of convenience we will consider this latter case.

The point  $P_C$  does not belong to  $L_{U_{\alpha^2,\beta^2}}$  for any  $C \in \mathbb{F}_{q^2}$ .

Recall that  $P_C$  is saturated if and only if

$$\det \begin{pmatrix} x & x^q + \alpha^2 x^{q^3} & x^{q^2} + \beta^2 x^{q^3} \\ y & y^q + \alpha^2 y^{q^3} & y^{q^2} + \beta^2 y^{q^3} \\ 0 & 1 & C \end{pmatrix} = 0$$

for some  $x, y \in \mathbb{F}_{q^4}$  with  $xy^q - x^q y \neq 0$ . By direct checking, the above determinant reads

$$F_0(x, y) := C^2 xy^q + xy^{q^2} + C^2 \alpha^2 xy^{q^3} + \beta^2 xy^{q^3} + C^2 x^q y + x^{q^2} y + C^2 \alpha^2 x^{q^3} y + \beta^2 x^{q^3} y.$$

Denote by  $F_i(x, y) := (F_0(x, y))^i$ ,  $i = 1, 2, 3$ .

Let  $G_1(x, y), G_2(x, y), G_3(x, y)$  be the polynomials

$$\begin{aligned} G_1(x, y) &:= (C^2 y^q + y^{q^2} + C^2 \alpha^2 y^{q^3} + \beta^2 y^{q^3}) F_1(x, y) + (C^{2q} y^q + \alpha^2 \beta^{2q} y^q) F_0(x, y), \\ G_2(x, y) &:= (C^2 y^q + y^{q^2} + C^2 \alpha^2 y^{q^3} + \beta^2 y^{q^3}) F_2(x, y) + y^{q^2} F_0(x, y), \\ G_3(x, y) &:= (C^2 y^q + y^{q^2} + C^2 \alpha^2 y^{q^3} + \beta^2 y^{q^3}) F_3(x, y) + C^{2q^3} \alpha^2 y^{q^3} F_0(x, y). \end{aligned}$$

One can check that  $G_i$  are  $q$ -linearized polynomials in  $x$  containing only  $x^q, x^{q^2}, x^{q^3}$ . We consider now the polynomials  $H_1$  and  $H_2$

$$\begin{aligned} H_1(x, y) &:= u G_1(x, y) + v G_2(x, y), \\ H_2(x, y) &:= w G_1(x, y) + v G_3(x, y), \end{aligned}$$

where

$$\begin{aligned} u &:= y^{q^2} (C^2 y + (\alpha^2 C^{2q^2+2} + \beta^{2q^2} C^2) y^q + (\alpha^2 C^{2q^2} + \beta^{2q^2}) y^{q^2} \\ &\quad + (\alpha^4 C^{2q^2} + \alpha^2 \beta^{2q^2} C^2 + \alpha^2 \beta^2 C^{2q^2} + \beta^{2q^2+2}) y^{q^3}) \\ v &:= (C^{2q} + \alpha^2 \beta^{2q}) y^{q^2+1} + (C^{2+2q} 2\alpha^2 + C^2 \alpha^4 \beta^{2q} + C^{2q} \beta^2 + \alpha^2 \beta^{2q+2}) y^{q^3+1} + C^{2q+2} \alpha^2 y^{q^2+q} \\ &\quad + C^2 \alpha^2 y^{q^3+q} + C^{2q} \alpha^2 y^{2q^2} + (C^{2q+2} \alpha^4 + C^{2q} \alpha^2 \beta^2 + \alpha^2) y^{q^3+q^2} + (C^2 \alpha^4 + \alpha^2 \beta^2) y^{2q^3}, \\ w &:= \alpha^2 (C^{2q^3+2} y + C^2 y^q + y^{q^2} + C^2 \alpha^2 y^{q^3} + \beta^2 y^{q^3}) y^{q^3}. \end{aligned}$$

Now,

$$H_1(x, y) = (C^2 y^q + y^{q^2} + C^2 \alpha^2 y^{q^3} + \beta^2 y^{q^3}) (x y^q + x^q y)^{q^2} L_1(y)$$

and

$$H_2(x, y) = (C^2 y^q + y^{q^2} + C^2 \alpha^2 y^{q^3} + \beta^2 y^{q^3}) (x y^q + x^q y)^{q^2} L_2(y),$$

where

$$\begin{aligned} L_1(y) &:= (C^{2q+2} \alpha^2 + C^2 \alpha^4 \beta^{2q} + C^{2q} \beta^2 + \alpha^2 \beta^{2q+2}) y^2 + (C^{2q^2+2q+2} \alpha^4 + C^{2q+2} \alpha^2 \beta^{2q^2} \\ &\quad + C^{2q^2+2} \alpha^6 \beta^{2q} + C^2 \alpha^4 \beta^{2q^2+2q} + C^2 \alpha^2 + C^{2q^2+2q} \alpha^2 \beta^2 + C^{2q} \beta^{2q^2+2} + C^{2q^2} \alpha^4 \beta^{2q+2} \\ &\quad + \alpha^2 \beta^{2q^2+2q+2}) y^{q+1} + (C^{2q+2} \alpha^4 + C^{2q^2} 2 + C^{2q} \alpha^2 \beta^2 + C^{2q^2} \alpha^2 \beta^{2q}) y^{q^2+1} \\ &\quad + (C^{2q^2+2q+2} \alpha^2 + C^{2q^2+2} \alpha^4 \beta^{2q} + C^2 \alpha^4 + C^{2q^2+2q} \beta^2 + C^{2q^2} \alpha^2 \beta^{2q+2} + \alpha^2 \beta^2) y^{q^3+1} \\ &\quad + (C^{2q+2} \alpha^4 + C^2 \alpha^2 \beta^{2q^2}) y^{2q} + (C^{2q^2+2q+2} \alpha^2 + C^{2q^2} \alpha^4 + \alpha^2 \beta^{2q^2}) y^{q^2+q} \\ &\quad + (C^{2q^2+2} \alpha^6 + C^{2q^2+2} \alpha^2 + C^2 \alpha^4 \beta^{2q^2} + C^{2q^2} \alpha^4 \beta^2 + \alpha^2 \beta^{2q^2+2}) y^{q^3+q} \\ &\quad + C^{2q^2+2q} \alpha^2 y^{2q^2} + (C^{2q^2+2q+2} \alpha^4 + C^{2q^2+2q} \alpha^2 \beta^2 + C^{2q^2} \alpha^2) y^{q^3+q^2} \\ &\quad + (C^{2q^2+2} \alpha^4 + C^{2q^2} \alpha^2 \beta^2) y^{2q^3} \end{aligned}$$

and

$$\begin{aligned}
L_2(y) := & (C^{2q^3+2q^2}\alpha^2 + C^{2q^3}\alpha^4\beta^{2q})y^2 + (C^{2q^3+2q^2+2}\alpha^4 + C^{2q}\alpha^2 + \alpha^4\beta^{2q})y^{q+1} \\
& + (C^{2q^3+2q}\alpha^4 + C^{2q^3+2q} + C^{2q}\alpha^2\beta^{2q^3} + C^{2q^3}\alpha^2\beta^{2q} + \alpha^4\beta^{2q^3+2q})y^{q^2+1} \\
& + (C^{2q^3+2q+2}\alpha^2 + C^{2q+2}\alpha^4\beta^{2q^3} + C^{2q^3+2}\alpha^4\beta^{2q} + C^2\alpha^6\beta^{2q^3+2q} + C^{2q^3+2q}\beta^2 + \\
& C^{2q}\alpha^2\beta^{2q^3+2} + C^{2q^3}\alpha^4 + C^{2q^3}\alpha^2\beta^{2q+2} + \alpha^4\beta^{2q^3+2q+2})y^{q^3+1} + C^{2q+2}\alpha^4y^{2q} \\
& + (C^{2q^3+2q+2}\alpha^2 + C^{2q+2}\alpha^4\beta^{2q^3} + C^{2q}\alpha^4)y^{q^2+q} + (C^{2q+2}\alpha^6 + C^{2q^3+2}\alpha^2 + C^2\alpha^4\beta^{2q^3} \\
& + C^{2q}\alpha^4\beta^2)y^{q^3+q^2} + (C^{2q^3+2q}\alpha^2 + C^{2q}\alpha^4\beta^{2q^3})y^{q^2} + (C^{2q^3+2q+2}\alpha^4 + C^{2q+2}\alpha^6\beta^{2q^3} \\
& + C^{2q^3+2q}\alpha^2\beta^2 + C^{2q}\alpha^4\beta^{2q^3+2} + C^{2q^3}\alpha^2 + \alpha^4\beta^{2q^3})y^{q^3+q^2} \\
& + (C^{2q^3+2}\alpha^4 + C^2\alpha^6\beta^{2q^3} + C^{2q^3}\alpha^2\beta^2 + \alpha^4\beta^{2q^3+2})y^{2q^3}.
\end{aligned}$$

Note that the determinant of the Dickson matrix of  $C^2y^q + y^{q^2} + C^2\alpha^2y^{q^3} + \beta^2y^{q^3}$  is  $d_{\alpha,\beta}(C)$  and thus  $d_{\alpha,\beta}(C) \neq 0$  for any  $C \in \Gamma_{\alpha,\beta}$ .

We already excluded the case  $xy^q + x^qy = 0$  and thus from  $H_1(x, y) = H_2(x, y) = 0$  one gets  $L_1(y) = L_2(y) = 0$ . Let  $P(y) := \alpha^2C^{2q^3}(C^q + \alpha\beta^q)^2L_1(y) + (C^q + \alpha\beta^q)^2(C\alpha + \beta)^2L_2(y) = (C^q + \alpha\beta^q)^2Q(y)$ . From  $Q(y) = 0$  one gets  $y = U/V$ , where

$$\begin{aligned}
U := & (\alpha^2(C^2y^q + y^{q^2} + C^2\alpha^2y^{q^3} + y^{q^3}\beta^2) \cdot \\
& ((C^{2q+2}\alpha^4 + C^{2q}\alpha^2\beta^2 + C^{2q^3+2q^2}\alpha^4 + C^{2q^3}\alpha^2\beta^{2q^2})y^q \\
& + (C^{2q^3+2q+2}\alpha^2 + C^{2q+2}\alpha^4\beta^{2q^3} + C^{2q^3+2q^2+2q}\alpha^2 + C^{2q^3+2q}\beta^2 + C^{2q}\alpha^2\beta^{2q^3+2})y^{q^2} \\
& + (C^{2q^3+2}\alpha^2 + C^2\alpha^4\beta^{2q^3} + C^{2q^3+2q^2}\alpha^2 + C^{2q^3}\beta^2 + \alpha^2\beta^{2q^3+2})y^{q^3}),
\end{aligned}$$

$$\begin{aligned}
V := & (C^4C^{2q^3+2q}\alpha^6 + C^{2q+2}C^{2q^3+2q^2}\alpha^6 + C^{2q^3+2q+2}\alpha^4\beta^2 + C^{2q^3+2q+2}\alpha^4\beta^{2q^2} + C^{2q+2}\alpha^4 \\
& + C^{2q^3+2q^2+2}\alpha^8\beta^{2q} + C^{2q^3+2}\alpha^6\beta^{2q}\beta^{2q^2} + C^{2q^3+2}\alpha^4 + C^2\alpha^6\beta^{2q} + C^{2q}C^{2q^3+2q^2}\alpha^4\beta^2 \\
& + C^{2q^3+2q}\alpha^2\beta^2\beta^{2q^2} + C^{2q}\alpha^2\beta^2 + C^{2q^3+2q^2}\alpha^6\beta^{2q+2} + C^{2q^3}\alpha^4\beta^{2q+2}\beta^{2q^2} + \alpha^4\beta^{2q+2})y^q \\
& + (C^{2q^3+2q+2}\alpha^2 + C^{2q+2}\alpha^4\beta^{2q^3} + C^{2q^3+2}\alpha^4\beta^{2q} + C^2\alpha^6\beta^{2q^3+2q} + C^{2q}C^{2q^3+2q^2}\alpha^2 \\
& + C^{2q^3+2q}\beta^2 + C^{2q}\alpha^2\beta^{2q^3+2} + C^{2q^3+2q^2}\alpha^4\beta^{2q} + C^{2q^3}\alpha^2\beta^{2q+2} + \alpha^4\beta^{2q^3+2q+2})y^{q^2} \\
& + (C^4C^{2q^3+2q}\alpha^4 + C^4C^{2q}\alpha^6\beta^{2q^3} + C^4C^{2q^3}\alpha^6\beta^{2q} + C^4\alpha^8\beta^{2q^3+2q} + C^{2q+2}C^{2q^3+2q^2}\alpha^4 \\
& + C^{2q^3+2q^2+2}\alpha^6\beta^{2q} + C^{2q}C^{2q^3+2q^2}\alpha^2\beta^2 + C^{2q^3+2q}\beta^4 + C^{2q}\alpha^2\beta^4\beta^{2q^3} + C^{2q^3+2q^2}\alpha^4\beta^{2q+2} \\
& + C^{2q^3}\alpha^2\beta^4\beta^{2q} + \alpha^4\beta^4\beta^{2q^3+2q})y^{q^3}.
\end{aligned}$$

Substituting it in  $L_1(y) = 0$  we obtain

$$\alpha^2(C^2\alpha^2 + \beta^2)(C^{2q+2}\alpha^2 + C^{2q}\beta^2 + 1)(C^2y^q + y^{q^2} + C^2\alpha^2y^{q^3} + \beta^2y^{q^3})y^qM(y) = 0, \quad (6)$$

where

$$M(y) = a_{00}^2y^{2q^3} + a_{01}^2y^{q^3+q^2} + a_{10}^2y^{q^3+q} + a_{02}^2y^{2q^2} + a_{11}^2y^{q^2+q} + a_{20}^2y^{2q},$$

with

$$\begin{aligned}
a_{00} &:= \alpha(C^{q^2+q} + C^{q^2}\alpha\beta^q + \alpha)(C^{q^3+1}\alpha + C\alpha^2\beta^{q^3} + C^{q^3+q^2}\alpha + C^{q^3}\beta + \alpha\beta^{q^3+1}) \\
&\quad \cdot (C^{q+1}\alpha + C^{q^3+1}\alpha + C\alpha^2\beta^q + C^q\beta + \alpha\beta^{q+1}), \\
a_{01} &:= (C^q + \alpha\beta^q)(C^{q^3+1}\alpha + C\alpha^2\beta^{q^3} + C^{q^3+q^2}\alpha + C^{q^3}\beta + \alpha\beta^{q^3+1})f_{\alpha,\beta}(C), \\
a_{02} &:= (C^{q^3+q}\alpha^2 + C^{q^3+q} + C^q\alpha\beta^{q^3} + C^{q^3}\alpha\beta^q + \alpha^2\beta^{q^3+q}) \\
&\quad \cdot (C^{q^3+1}\alpha + C\alpha^2\beta^{q^3} + C^{q^3+q^2}\alpha + C^{q^3}\beta + \alpha\beta^{q^3+1}) \\
&\quad \cdot (C^{q+1}\alpha + C^{q^2+q}\alpha + C^q\beta^{q^2} + C^{q^2}\alpha^2\beta^q + \alpha\beta^{q^2+q}), \\
a_{10} &:= \alpha(C^{q+1}\alpha + C^{q^3+1}\alpha + C\alpha^2\beta^q + C^q\beta + \alpha\beta^{q+1})f_{\alpha,\beta}(C), \\
a_{11} &:= \alpha C^{q^3}(C^{q+1}\alpha + C^{q^2+q}\alpha + C^q\beta^{q^2} + C^{q^2}\alpha^2\beta^q + \alpha\beta^{q^2+q})f_{\alpha,\beta}(C), \\
a_{20} &:= \alpha^2(C^{q^3+q^2}\alpha + C^{q^3}\beta^{q^2} + 1)(C^{q+1}\alpha + C^{q^2+q}\alpha + C^q\beta^{q^2} + C^{q^2}\alpha^2\beta^q + \alpha\beta^{q^2+q}) \\
&\quad (C^{q+1}\alpha + C^{q^3+1}\alpha + C\alpha^2\beta^q + C^q\beta + \alpha\beta^{q+1}).
\end{aligned}$$

Since  $C \in \Gamma_{\alpha,\beta}$  and  $\alpha y \neq 0$ , (6) yields  $M(y) = 0$ . Also, from  $f_{\alpha,\beta}(C) = 0$ ,  $M(y) = (a_{00}y^{q^3} + a_{02}y^{q^2} + a_{20}y^q)^2$ . We will show that  $M(y)$  has only the zero root in  $\mathbb{F}_{q^4}$ . To this aim consider the Dickson matrix associated with  $M(y)$

$$\begin{pmatrix} 0 & a_{20} & a_{02} & a_{00} \\ a_{00}^q & 0 & a_{20}^q & a_{02}^q \\ a_{02}^{q^2} & a_{00}^{q^2} & 0 & a_{20}^{q^2} \\ a_{20}^{q^3} & a_{02}^{q^3} & a_{00}^{q^3} & 0 \end{pmatrix},$$

whose determinant is precisely  $g_{\alpha,\beta}(C)$ , which is nonvanishing since  $C \in \Gamma_{\alpha,\beta}$ .

This shows that  $P_C$  is not saturated by  $L_{U_{\alpha,\beta}}$  and the claim follows.  $\square$

Let

$$r_0(z) := (z^4 - z)(z - \beta)(z^2 + z\beta^2 + z\beta + 1)(z^2 + z\beta^3 + z\beta^2 + z\beta + \beta^3 + \beta^2 + 1)(z\beta^3 + \beta + 1),$$

and

$$\Delta_0 := \left\{ z \in \mathbb{F}_q : \text{Tr}_{q/2} \left( \frac{(z\beta^3 + z\beta^2 + z + \beta)(z + \beta)}{z^2\beta^4} \right) = 0, r_0(z) \neq 0 \right\}.$$

**Lemma A.3.** *Let  $\beta \in \mathbb{F}_q^*$ . If  $q \geq 64$  then  $\Delta_0 \neq \emptyset$ .*

*Proof.* Recall that  $\text{Tr}_{q/2} \left( \frac{(z\beta^3 + z\beta^2 + z + \beta)(z + \beta)}{z^2\beta^4} \right) = 0$  if and only if there exists  $x \in \mathbb{F}_q$  such that  $x^2 + x + \frac{(z\beta^3 + z\beta^2 + z + \beta)(z + \beta)}{z^2\beta^4} = 0$ .

Consider the plane  $\mathbb{F}_q$ -rational curve

$$C : X^2 + X + \frac{(Z\beta^3 + Z\beta^2 + Z + \beta)(Z + \beta)}{Z^2\beta^4} = 0.$$

It is birationally equivalent to

$$\left(X + \frac{1}{\beta Z}\right)^2 + X + \frac{1}{\beta Z} + \frac{(Z\beta^3 + Z\beta^2 + Z + \beta)(Z + \beta)}{Z^2\beta^4} = 0,$$

that is

$$X^2 + X + \frac{\beta^3 + \beta^2 + 1}{\beta^4} + \frac{1}{Z} = 0,$$

which is clearly absolutely irreducible and of genus at most 3. This means that there are at least  $q - 2\sqrt{q}$   $\mathbb{F}_q$ -rational points in  $\mathcal{C}$  and thus  $\frac{q-2\sqrt{q}}{2} - 1$  values  $z \in \mathbb{F}_q$  for which

$$\mathrm{Tr}_{q/2} \left( \frac{(z\beta^3 + z\beta^2 + z + \beta)(z + \beta)}{z^2\beta^4} \right) = 0.$$

Among these values, at most 10 satisfy  $r_0(z) = 0$ . Since  $q \geq 64$ ,  $\Delta_0 \neq \emptyset$ .  $\square$

*Proof of Lemma 3.5.* We will prove that for each  $\beta$  there exists  $z \in \mathbb{F}_q$  such that the point  $(1 : z_0 : \beta)$  is not 1-saturated, by proving that the set

$$\{(x^q + x^{q^3} + zx, x^{q^2} + \beta x^{q^3} + \beta x) : x \in \mathbb{F}_{q^4}\} \subseteq \mathrm{PG}(1, q^4)$$

is scattered.

Let us consider  $z \in \Delta_0 \neq \emptyset$ . First we prove that the point  $(1 : 0) \in \mathrm{PG}(1, q^4)$  is of weight 0. This can be readily seen as the Dickson matrix of  $x^{q^2} + \beta x^{q^3} + \beta x$  is non-singular.

We consider now a point  $(m : 1) \in \mathrm{PG}(1, q^4)$  with  $m \in \mathbb{F}_{q^4}$ . Such a point is of weight at most one if and only if the rank of

$$M := \begin{pmatrix} m\beta + z & 1 & m & 1 + m\beta \\ 1 + mq\beta & m^q\beta + z & 1 & m^q \\ m^{q^2} & 1 + m^{q^2}\beta & m^{q^2}\beta + z & 1 \\ 1 & m^{q^3} & 1 + m^{q^3}\beta & m^{q^3}\beta + z \end{pmatrix}$$

is at least three. Let  $f_1 = \det(N_1)$  and  $f_2 = \det(N_2)$  be the determinants of the north-right and south-right  $3 \times 3$  submatrix of  $M$ , respectively.

Then

$$\begin{aligned} f_1 &:= \beta^3 m^{q^3+q^2+1} + (z\beta + \beta^2) m^{q^2+1} + (z\beta + \beta^2 + \beta + 1) m^{q^3+1} \\ &\quad + (z + \beta) m + \beta m^{q^3+q^2} + (z\beta + \beta) m^{q^2} + (z\beta + z) m^{q^3} + z^2; \\ f_2 &:= (\beta^3 + \beta^2 + 1) m^{q^3+q^2+1} + (\beta^2 + \beta) m^{q^2+1} + (z\beta + \beta^2) m^{q^3+1} \\ &\quad + (\beta + 1) m + (z\beta^2 + z\beta + \beta) m^{q^3+q^2} + (z\beta + \beta + 1) m^{q^2} + (z^2 + z\beta) m^{q^3}. \end{aligned}$$

Using  $f_1 = 0$  and  $(f_1)^{q^3} = 0$  to eliminate  $m^{q^3}$  and  $m^{q^2}$  from  $(f_2)^{q^3} = 0$ , one gets

$$((\beta^2 + \beta) m^{q+1} + \beta m + (z + \beta) m^q + 1)((z\beta^3 + \beta + 1) m^{q+1} + (z^2\beta + z) m^q + (z^2\beta + z) m + z^2\beta + z^2) = 0.$$

- Suppose that  $(\beta^2 + \beta)m^{q+1} + \beta m + (z + \beta)m^q + 1 = 0$ . Then  $(m\beta^2 + m\beta + z + \beta)m^q = m\beta + 1$ . So  $m \neq 0$ . Also,  $m\beta^2 + m\beta + z + \beta = 0$  would imply  $m\beta + 1 = 0$  and thus  $z = 1$ , a contradiction. Since  $m \in \mathbb{F}_{q^4}$  this yields  $z^3(m^2\beta^2 + m^2\beta + mz + 1) = 0$ . Using  $m^q = \frac{m\beta+1}{m\beta^2+m\beta+z+\beta}$  again in  $(f_2)^{q^3} = 0$  one gets

$$(m\beta + z)(m\beta^2 + m\beta + m + z + \beta)(mz\beta^2 + mz\beta + m\beta + z^2 + \beta + 1) = 0.$$

Since  $z \notin \mathbb{F}_4 \cup \{\beta\}$ , none of these three factors vanishes. Also, combining each of them with  $m^2\beta^2 + m^2\beta + mz + 1 = 0$ , necessarily

$$\beta z(z + 1) = 0,$$

or

$$z(z^2 + z\beta^3 + z\beta^2 + z\beta + \beta^3 + \beta^2 + 1) = 0,$$

or

$$\beta z(z + 1)(z^2 + z\beta^3 + z\beta^2 + z\beta + \beta^3 + \beta^2 + 1) = 0,$$

a contradiction to  $z \in \Delta_0$ .

- Suppose that  $(z\beta^3 + \beta + 1)m^{q+1} + (z^2\beta + z)m^q + (z^2\beta + z)m + z^2\beta + z^2 = 0$ . Since  $z \in \Delta_0$ ,  $z\beta^3 + \beta + 1 \neq 1$ . Then  $(mz\beta^3 + m\beta + m + z^2\beta + z)m^q = mz^2\beta + mz + z^2\beta + z^2$ . Clearly  $m = 0$  is not possible. Also  $mz\beta^3 + m\beta + m + z^2\beta + z = 0$  yields  $mz^2\beta + mz + z^2\beta + z^2 = 0$  and thus  $z\beta(z^2 + z\beta^2 + z\beta + 1) = 0$ , a contradiction to  $z \in \Delta_0$ . From  $m^q = \frac{mz^2\beta + mz + z^2\beta + z^2}{mz\beta^3 + m\beta + m + z^2\beta + z}$ , substituting it in  $\det(M) = 0$  one gets

$$\beta z((z\beta^3 + z\beta^2 + z + \beta)m^2 + z^2\beta^2m + z^3 + z^2\beta) = 0.$$

Note that  $(z\beta^3 + z\beta^2 + z + \beta)m^2 + z^2\beta^2m + z^3 + z^2\beta = 0$  is an equation in  $m$  defined over  $\mathbb{F}_q$ . Since  $\text{Tr}_{q/2} \left( \frac{(z\beta^3 + z\beta^2 + z + \beta)(z + \beta)}{z^2\beta^4} \right) = 0$ ,  $m \in \mathbb{F}_q$  and thus

$$\frac{mz^2\beta + mz + z^2\beta + z^2}{mz\beta^3 + m\beta + m + z^2\beta + z} = m.$$

Together with  $(z\beta^3 + z\beta^2 + z + \beta)m^2 + z^2\beta^2m + z^3 + z^2\beta = 0$ , this gives

$$\beta z(z^2 + z\beta^2 + z\beta + 1) = 0,$$

a contradiction to  $z \in \Delta_0$ .

□



Consider the following polynomials

$$\begin{aligned}
h_1(z) &:= \beta^{q+1}z(z+1)(z^2 + (\beta + \beta^{q^3})z + \beta + \beta^{q^3}); \\
h_2(z) &:= z^5 + (\beta^{q^2+q+1} + \beta^{q+1} + \beta + \beta^{q^2} + \beta^{q^3})z^4 + (\beta^{q^2+q+2} + \beta^{q+2} + \beta^{q^2+2q+1} + \beta^{2q+1} \\
&\quad + \beta^{q^3+q+1} + \beta^{q^2+1} + \beta + \beta^{q^2} + \beta^{q^2+q} + \beta^q + \beta^{q^2} + \beta^{q^3} + 1)z^3 \\
&\quad + (\beta^{q^2+q+2} + \beta^{q^3+2q+1} + \beta^{2q+1} + \beta^{q+1} + \beta^{q^3+2q} + \beta^{2q} + \beta^{q^2+q} + \beta^{q^3+q} + \beta^q + \beta^{q^2})z^2 \\
&\quad + (\beta^{q^2+q+2} + \beta^{q+2} + \beta^{q^2+2q+1} + \beta^{q^3+q+1} + \beta^{q^2+1} + \beta^{q^3+q} + \beta^q + \beta^{q^2})z \\
&\quad + \beta^{q^2+q+2} + \beta^{q^3+2q+1} + \beta^{q^2+q+1} + \beta^{q^3+2q}; \\
h_3(z) &:= \beta(z+1)(z^5 + (\beta + \beta^{q^3+q^2+q} + \beta^{q^2+q} + \beta^q + \beta^{q^3})z^4 + (\beta^{q^2+q+1} + \beta + \beta^{q^3+q^2+2q} \\
&\quad + \beta^{q^2+2q} + \beta^{q^3+2q^2+q} + \beta^{2q^2+q} + \beta^{q^3+q} + \beta^q + \beta^{2q^2} + \beta^{q^3+q^2} + \beta^{q^2} + \beta^{q^3} + 1)z^3 \\
&\quad + (\beta^{q^2+q+1} + \beta^{2q^2+1} + \beta^{q^2+1} + \beta^{q^3+q^2+2q} + \beta^{2q^2+q} + \beta^{q^2+q} + \beta^{2q^2} + \beta^{q^3+q^2} + \beta^{q^2} + \beta^{q^3})z^2 \\
&\quad + (\beta^{q^2+q+1} + \beta^{q^2+1} + \beta^{q^3+q^2+2q} + \beta^{q^2+2q} + \beta^{q^3+2q^2+q} + \beta^{q^3+q} + \beta^{q^2} + \beta^{q^3})z \\
&\quad + \beta^{q^2+q+1} + \beta^{2q^2+1} + \beta^{q^3+q^2+2q} + \beta^{q^3+q^2+q}); \\
h_4(z) &:= \text{Tr}_{q^4/q}(\beta + \beta^{q+1})z^3 + (\text{Tr}_{q^4/q}(\beta^{q^2+q+1}) + \beta^{q^2+1} + \beta^{q^3+q})z^2 + \text{Tr}_{q^4/q}(\beta)z + \text{Tr}_{q^4/q}(\beta^{q+1}).
\end{aligned}$$

Let

$$\Delta_1 := \{z \in \mathbb{F}_q : z(z+1)(z\beta^{q^2+1} + \beta + \beta^{q^2})(z^2 + z\beta^{q^2+q} + z\beta^{q^2} + \beta^q + \beta^{q^2} + 1)h_1(z)h_2(z)hg_3(z)h_4(z) \neq 0\}.$$

*Proof of Lemma 3.6.* The proof is similar to the one of Lemma 3.5. First note that since  $\beta^{q^3+q} = \beta^{q^2+q}$ ,  $\beta \notin \mathbb{F}_q$  yields  $\beta \notin \mathbb{F}_{q^2}$ . We will prove that for each such  $\beta$  there exists  $z \in \Delta_1$  such that the point  $(1 : z : \beta)$  is not 1-saturated. This holds if the set

$$\{(x^q + x^{q^3} + zx, x^{q^2} + \beta x^{q^3} + \beta x) : x \in \mathbb{F}_{q^4}\} \subseteq \text{PG}(1, q^4)$$

is scattered. Arguing as in the proof of Lemma 3.5, it can be shown that the point  $(0 : 1)$  is of weight 1. To investigate the weight of a point  $(1 : m)$ ,  $m \in \mathbb{F}_{q^4}$ , we consider the rank of

$$M := \begin{pmatrix} m\beta + z & 1 & m & 1 + m\beta \\ 1 + m^q\beta^q & m^q\beta^q + z^q & 1 & m^q \\ m^{q^2} & 1 + m^{q^2}\beta^{q^2} & m^{q^2}\beta^{q^2} + z^{q^2} & 1 \\ 1 & m^{q^3} & 1 + m^{q^3}\beta^{q^3} & m^{q^3}\beta^{q^3} + z^{q^3} \end{pmatrix}.$$

We will prove that for each choice of  $\beta$  the rank of  $M$  is at least three independently of  $m \in \mathbb{F}_{q^4}$ . Let  $f_1 = \det(N_1)$  and  $f_2 = \det(N_2)$  be the determinants of the north-right and south-right  $3 \times 3$  submatrix of  $M$ , respectively. In this case,

$$\begin{aligned}
f_1(z) &:= (\beta^{q^3+q^2+q} + \beta^{q^2+q} + \beta^{q^3+q})m^{q^3+q^2+q} + (z\beta^q + \beta^{q^3+q})m^{q^3+q} + (z\beta^{q^2} + z)m^{q^2} \\
&\quad + \beta^q m^{q^2+q} + (z\beta^{q^3} + \beta^{q^3+q^2} + \beta^{q^2} + 1)m^{q^3+q^2} + (z\beta^q + \beta^q)m^q + (z + \beta^{q^3})m^{q^3} + z^2; \\
f_2(z) &:= (\beta^{q^3+q^2+q} + \beta^{q^3+q} + 1)m^{q^3+q^2+q} + (z\beta^{q^2+q} + z\beta^q + \beta^{q^2})m^{q^2+q} + (\beta^{q^3+q} + \beta^q)m^{q^3+q} \\
&\quad + (z\beta^q + \beta^q + 1)m^q + (z\beta^{q^3} + \beta^{q^3+q^2})m^{q^3+q^2} + (z^2 + z\beta^{q^2})m^{q^2} + (\beta^{q^3} + 1)m^{q^3}.
\end{aligned}$$

Using  $f_1 = 0$  and  $(f_1)^{q^3} = 0$  to eliminate  $m^{q^3}$  and  $m^{q^2}$  from  $(f_2)^{q^3} = 0$ , one gets

$$(\beta^{q+1} + \beta)m^{q+1} + \beta m + (z + \beta^q)m^q + 1 = 0$$

or

$$\begin{aligned} & (z\beta^{q^2+q+1} + z\beta^{q+1} + z\beta^{q^2+1} + \beta^{q^2+1} + \beta^{q^2+q} + \beta^q + 1)m^{q+1} \\ & + (z^2\beta + z + \beta + \beta^{q^2})m + (z^2\beta^{q^2} + z\beta^q + z\beta^{q^2} + z)m^q + z^2\beta^{q^2} + z^2 = 0. \end{aligned}$$

- Suppose that  $(\beta^{q+1} + \beta)m^{q+1} + \beta m + (z + \beta^q)m^q + 1 = 0$ . Then  $(m\beta^{q+1} + m\beta + z + \beta^q)m^q = m\beta + 1$ . Clearly  $m \neq 0$ . Also,  $m\beta^{q+1} + m\beta + z + \beta^q = 0$  would imply  $m\beta + 1 = 0$  and thus  $z = 1$ , a contradiction. Since  $m \in \mathbb{F}_{q^4}$ , this yields

$$\begin{aligned} & \left( (\beta^{q+1} + \beta)z^3 + (\beta^{q+2} + \beta^2 + \beta^{q^3+q+1} + \beta^{q+1} + \beta^{q^2+1} + \beta^{q^3+1})z^2 \right. \\ & \left. + (\beta^{q+2} + \beta^{q^2+2} + \beta^{q^2+1} + \beta^{q^3+1})z + \beta^{q^2+2} + \beta^{q^3+q+1} \right)m^2 \\ & + \left( z^4 + \text{Tr}_{q^4/q}(\beta)z^3 + (\text{Tr}_{q^4/q}(\beta) + \beta^{q^2+1} + \beta^{q^3+q})z^2 + \beta^{q^2+1} + \beta^{q^3+q} \right)m \\ & + z^3 + z^2\beta^q + z^2\beta^{q^2} + z\beta^q + z\beta^{q^2} = 0. \end{aligned} \tag{7}$$

Using  $m^q = \frac{m\beta+1}{m\beta^{q+1}+m\beta+z+\beta^q}$  again in  $(f_2)^{q^3} = 0$  one gets

$$(m\beta+z)(m\beta^{q+1}+m\beta+m+z+\beta^q)(mz\beta^{q+1}+mz\beta+m\beta^{q+1}+m\beta^{q^2+1}+m\beta+z^2+z\beta^q+z\beta^{q^2}+\beta^q+1) = 0.$$

Since  $\beta \notin \mathbb{F}_q$ , none of these three factors vanishes. Also, combining each of them with (7), necessarily

$$h_1(z)h_2(z)h_3(z) = 0,$$

a contradiction to  $z \in \Delta_1$ .

- Suppose that

$$\begin{aligned} & (z\beta^{q^2+q+1} + z\beta^{q+1} + z\beta^{q^2+1} + \beta^{q^2+1} + \beta^{q^2+q} + \beta^q + 1)m^{q+1} \\ & + (z^2\beta + z + \beta + \beta^{q^2})m + (z^2\beta^{q^2} + z\beta^q + z\beta^{q^2} + z)m^q + z^2\beta^{q^2} + z^2 = 0. \end{aligned}$$

Then  $((z\beta^{q^2+q+1} + z\beta^{q+1} + z\beta^{q^2+1} + \beta^{q^2+1} + \beta^{q^2+q} + \beta^q + 1)m + (z^2\beta^{q^2} + z\beta^q + z\beta^{q^2} + z))m^q = (z^2\beta + z + \beta + \beta^{q^2})m + z^2\beta^{q^2} + z^2$ . Clearly  $m = 0$  is not possible.

Also  $(z\beta^{q^2+q+1} + z\beta^{q+1} + z\beta^{q^2+1} + \beta^{q^2+1} + \beta^{q^2+q} + \beta^q + 1)m + (z^2\beta^{q^2} + z\beta^q + z\beta^{q^2} + z) = 0$  yields  $(z^2\beta + z + \beta + \beta^{q^2})m + z^2\beta^{q^2} + z^2 = 0$  and thus  $z(z\beta^{q^2+1} + \beta + \beta^{q^2})(z^2 + z\beta^{q^2+q} + z\beta^{q^2} + \beta^q + \beta^{q^2} + 1) = 0$ , a contradiction to  $z \in \Delta_1$ .

Thus

$$m^q = \frac{(z^2\beta + z + \beta + \beta^{q^2})m + z^2\beta^{q^2} + z^2}{(z\beta^{q^2+q+1} + z\beta^{q+1} + z\beta^{q^2+1} + \beta^{q^2+1} + \beta^{q^2+q} + \beta^q + 1)m + (z^2\beta^{q^2} + z\beta^q + z\beta^{q^2} + z)}$$

and since  $m \in \mathbb{F}_{q^4}$ , necessarily  $h_4(z)(a_2(z)m^2 + a_1(z)m + a_0(z)) = 0$ , where

$$\begin{aligned}
a_2(z) &:= (\beta^{q^3+q^2+q+2} + \beta^{q^3+q^3+2} + \beta^{q+1})z^3 + (\beta^{q^2+q+2} + \beta^{q^3+q^2+2} + \beta^{q^2+2} + \beta^2 \\
&\quad + \beta^{q^2+q+1} + \beta^{q+1} + \beta^{q^3+q^2+1} + \beta^{q^2+1} + \beta^{q^3+1} + \beta + \beta^q)z^2 \\
&\quad + (\beta^{q^3+q+2} + \beta^{q^2+2} + \beta^{q^3+q^2+q+1} + \beta^{q^2+q+1} + \beta^{q+1} + \beta^{q^3+q^2+1} + \beta^{q^2+1} \\
&\quad + \beta^{q^3+q^2+q} + \beta^q + \beta^{q^3})z + \beta^{q+2} + \beta^2 + \beta^{q^2+q+1} + \beta^{q^3+q+1} + \beta^{q^2+1} + \\
&\quad \beta + \beta^{q^3+q^2+q} + \beta^{q^2}; \\
a_1(z) &:= \beta^{q^3+q^2+q+1}z^4 + \text{Tr}_{q^4/q}(\beta + \beta^{q+1} + \beta^{q^2+q+1})z^3 \\
&\quad + (\text{Tr}_{q^4/q}(\beta^{q+1} + \beta^{q^2+q+1}) + \beta^{q^2+1} + \beta^{q^3+q})z^2 + \text{Tr}_{q^4/q}(\beta)z + \text{Tr}_{q^4/q}(\beta^{q+1}); \\
a_0(z) &:= z^2(\beta^{q^3+q^2}z^3 + (\beta^{q^3+q^2+q} + \beta^{q^2} + \beta^{q^3})z^2 + (\beta^{q^3+q} + \beta^q + \beta^{q^3+q^2} + \beta^{q^3})z \\
&\quad + \beta^{q^2+q} + \beta^q + \beta^{q^3+q^2} + \beta^{q^3})
\end{aligned}$$

Since  $\beta \notin \mathbb{F}_q$  (and thus not belonging to  $\mathbb{F}_{q^2}$ ) the polynomial  $a_2(z)m^2 + a_1(z)m + a_0(z)$  is nonvanishing, since  $a_2(z) \not\equiv 0$ . Also, the resultant between  $a_2(z)m^2 + a_1(z)m + a_0(z)$  and  $f_2$  with respect to  $m$  is a polynomial of degree 38 in  $z$  whose leading coefficient is  $\beta^{q^3+3q^2+2q^2+4}(\beta^q + \beta^{q^2} + \beta^{q^2+q} + \beta^{q^3+q^2})$ , which is never zero, since  $\beta \notin \mathbb{F}_q$ . Since  $q \geq 64$  it is always possible to choose  $z \in \Delta_1$  to be not a root of such a polynomial.

The claim follows. □