A class of linear sets in PG(1, q^5)

Montanucci, Maria; Zanella, Corrado

Published in:
Finite Fields and Their Applications

Link to article, DOI:
10.1016/j.ffa.2021.101983

Publication date:
2021

Document Version
Peer reviewed version

A class of linear sets in PG$(1, q^5)$

Maria Montanucci - Corrado Zanella

November 25, 2021

Abstract

Maximum scattered linear sets in PG$(1, q^n)$ have been completely classified for $n \leq 4$, see [B. Csajbók and C. Zanella, Discrete Math. 341 (2018), 74–80; M. Lavrauw and G. Van de Voorde, Des. Codes Cryptogr. 56 (2010), 89–104]. Here a wide class of linear sets in PG$(1, q^5)$ is studied which depends on two parameters. Conditions for the existence, in this class, of possible new maximum scattered linear sets in PG$(1, q^5)$ are exhibited.

AMS subject classification: 51E20, 05B25

Keywords: Linear set, Finite projective line, Subgeometry, Finite projective space

1 Introduction

A point in PG$(1, q^t)$ is the $\mathbb{F}_{q^t}$-span $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^t}}$ of a nonzero vector $\mathbf{v}$ in a two-dimensional vector space, say W, over $\mathbb{F}_{q^t}$. If U is a subspace over $\mathbb{F}_q$ of W, then $L_U = \{\langle \mathbf{v} \rangle_{\mathbb{F}_{q^t}} : \mathbf{v} \in U \setminus \{\mathbf{0}\}\}$ denotes the associated $\mathbb{F}_q$-*linear set* (or simply *linear set*) in PG$(1, q^t)$. The *rank* of such a linear set is $r = \dim_{\mathbb{F}_q} U$. Any linear set in PG$(1, q^t)$ of rank greater than t coincides with the whole projective line. The *weight* of a point $P = \langle \mathbf{v} \rangle_{\mathbb{F}_{q^t}}$ of L_U is $w_{L_U}(P) = \dim_{\mathbb{F}_q}(U \cap P)$. If the rank and the size of L_U are r and $(q^r - 1)/(q - 1)$, respectively, then L_U is *scattered*. Equivalently, L_U is scattered if and only if all its points have weight one. A scattered $\mathbb{F}_q$-linear set of rank t in PG$(1, q^t)$ is *maximum scattered* (MSLS for short). For any $\varphi \in \Gamma\mathrm{L}(2, q^t)$ with related collineation $\tilde{\varphi} \in \mathrm{P}\Gamma\mathrm{L}(2, q^t)$ and any $\mathbb{F}_q$-linear set L_U, $L_{U^\varphi} = (L_U)^{\tilde{\varphi}}$. As it was showed in [8], the converse is not true; that is, there are examples of MSLSs $L_U = L_V \subseteq$ PG$(1, q^t)$ such that no

$\varphi \in \Gamma\mathrm{L}(2,q^t)$ exists satisfying $U^\varphi = V$. See also [6] for the problem of the ΓL-equivalence of the underlying $\mathbb{F}_q$-subspaces of two linear sets.

Up to our knowledge, only three types of MSLS in $\mathrm{PG}(1,q^5)$ are known:

- The *linear set of pseudoregulus type* $L_0 = \{\langle (u,u^q)\rangle_{\mathbb{F}_{q^5}} : u \in \mathbb{F}_{q^5}^*\}$; see [9] for a geometric description.
- L_1^η and L_2^η, where

$$L_s^\eta = \{\langle (x, \eta x^{q^s} + x^{q^{5-s}})\rangle_{\mathbb{F}_{q^5}} \ : \ x \in \mathbb{F}_{q^5}^*\},\ \mathrm{N}_{q^5/q}(\eta) \notin \{0,1\}.$$

  They were constructed by Lunardon-Polverino [13] for $s=1$ and by Sheekey [16] for $s=2$ (see also [15]). We will refer to MSLS in $\mathrm{PG}(1,q^5)$ of type L_1^η and L_s^η with $s=2$ as MSLS of *Lunardon-Polverino type* and *Sheekey type*, respectively.

For any η, η' with $\mathrm{N}_{q^5/q}(\eta), \mathrm{N}_{q^5/q}(\eta')^5 \notin \{0,1\}$, L_1^η and $L_2^{\eta'}$ are not $\mathrm{P\Gamma L}(2,q^5)$-equivalent [5, Theorem 5.5]. The aim of this paper is to find algebraic conditions for possible new examples that on the other hand could also serve to prove their nonexistence. Up to our knowledge, the problem of the classification of the MSLSs in $\mathrm{PG}(1,q^5)$ remains open.

In Section 2, a canonical form $L_{\alpha,\beta}$ is found for a wide class of linear sets in $\mathrm{PG}(1,q^5)$. Based on the representation given in [14, Theorems 1 and 2], any linear set $\mathbb{L}$ of rank five in $\mathrm{PG}(1,q^5)$ can be obtained as the projection of a canonical subgeometry $\Sigma \cong \mathrm{PG}(4,q)$ from a plane Λ of $\mathrm{PG}(4,q^5)$ such that $\Lambda \cap \Sigma = \emptyset$. Let σ denote a generator of the collineation group fixing Σ pointwise. As a consequence of [9, Theorem 2.3], assuming that the linear set $\mathbb{L}$ is maximum scattered, it is a linear set of pseudoregulus type if and only if at least one of the intersections $\Lambda \cap \Lambda^\sigma$ and $\Lambda \cap \Lambda^{\sigma^2}$ is not a point. So it is assumed that $P = \Lambda \cap \Lambda^\sigma$ is a point. Adding the assumption that the projective closure $\overline{P, P^\sigma, P^{\sigma^2}, P^{\sigma^3}, P^{\sigma^4}}$ is equal to $\mathrm{PG}(4,q^5)$ leads to the algebraic form in Equation (2), namely $L_{\alpha,\beta} = \{\langle (x - \alpha x^{q^2}, x^q - \beta x^{q^2})\rangle_{\mathbb{F}_{q^5}} : x \in \mathbb{F}_{q^5}^*\}$ for $\mathbb{L}$.

Sections 3 and 4 are based on the interpretation of algebraic equations in one unknown in $\mathbb{F}_{q^5}$ as algebraic varieties in $\mathbb{A}^5(\mathbb{F}_q)$. More precisely, taking a basis $\mathcal{B}$ of $\mathbb{F}_{q^5}$ over $\mathbb{F}_q$, from $f(x)=0$ a set of five equations is obtained by equating to zero the coordinates of $f(x)$ with respect to $\mathcal{B}$.

In Section 3 it is shown that if q is large enough, then there are no MSLSs of type $L_{0,\beta}$. This is consequence of a stronger result (Lemma 3.1), stating that for $q \geq 223$ any element of $\mathbb{F}_{q^5}^*$ is equal to $(uv^q - u^q v)/(u^{q^2} v - u v^{q^2})$ for some $u, v \in \mathbb{F}_{q^5}^*$ such that $\dim\langle u, v\rangle_{\mathbb{F}_q} = 2$. The proof is achieved by

proving the existence of suitable $\mathbb{F}_q$-rational points of the degree-5 hypersurface given by Equation (12) in $\mathbb{A}^5(\mathbb{F}_q)$ not lying on a special hyperplane. The aforementioned degree-5 hypersurface can be also seen as a variety in $\mathrm{PG}(4,q)$ as its model in Equation (12) is given by a homogeneous polynomial. This is based on a recent bound by Slavov [17] for the number of $\mathbb{F}_q$-rational points on hypersurfaces (see Proposition 3.2). An exhaustive computer search allowed to extend such a result also to $q \leq 17$.

Any MSLS of type $L_{\alpha,0}$ is of Lunardon-Polverino type. If $\alpha^q = \beta^{q+1}$, then either $L_{\alpha,\beta}$ is of pseudoregulus type, or it has rank less than five (Proposition 2.5). Motivated by this, in Sections 4 and 5 MSLSs $L_{\alpha,\beta}$ are dealt with under the assumption $\alpha\beta \neq 0$.

Proposition 4.3 states that any MSLS of type $L_{\alpha,\beta}$ satisfies the condition $\alpha^q/\beta^{q+1} \in \mathbb{F}_q$. This is a consequence of the existence of $\mathbb{F}_q$-rational points on a special quartic curve $\mathcal{Q}$ described explicitly in Equation (18). In order to prove that, $\mathcal{Q}$ is shown to be irreducible, allowing to apply the Hasse-Weil bound. No $L_{\alpha,\beta}$ with $\alpha\beta \neq 0$ is of Lunardon-Polverino type (Lemma 5.1). A necessary and sufficient condition is proved for a MSLS $L_{\alpha,\beta}$ to be of Sheekey type, that for $q \leq 11$ is always satisfied (Theorem 5.5). The proof is based on the results by Csajbók, Marino and Polverino [5, Theorem 5.4], implying that if a linear set L_U is $\mathrm{P\Gamma L}(2,q^5)$-equivalent to a Sheekey's L_2^η, then U is $\Gamma\mathrm{L}(2,q^5)$-equivalent to the underlying $\mathbb{F}_q$-subspace of a (possibly different) Sheekey linear set.

2 Canonical forms

cforms

Let $\Sigma \cong \mathrm{PG}(4,q)$ be an $\mathbb{F}_q$-canonical subgeometry of $\mathrm{PG}(4,q^5)$; that is, the set of all points of $\mathrm{PG}(4,q^5)$ having coordinates rational over $\mathbb{F}_q$ with respect to some projective reference system. Furthermore, let $\sigma \in \mathrm{P\Gamma L}(5,q^5)$ of order five fixing Σ pointwise. In this section $\mathbb{L}$ denotes a maximum scattered $\mathbb{F}_q$-linear set in $\mathrm{PG}(1,q^5)$, not of pseudoregulus type. By [9, 14], $\mathbb{L}$ is the projection $p_\Lambda(\Sigma)$ with vertex a plane Λ such that $\Lambda \cap \Sigma = \emptyset$, and $\dim(\Lambda \cap \Lambda^\tau) = 0$ for any generator τ of $\langle\sigma\rangle$.

The *standard subgeometry* Σ is the set of all points of type

$$P_u = \langle (u, u^q, u^{q^2}, u^{q^3}, u^{q^4}) \rangle_{\mathbb{F}_{q^5}},\ u \in \mathbb{F}_{q^5}^*.$$

and $P_u = P_v$ if and only if $u/v \in \mathbb{F}_q$. A possible choice for σ is

$$\sigma : \langle (X_0, X_1, X_2, X_3, X_4) \rangle_{\mathbb{F}_{q^5}} \mapsto \langle (X_4^q, X_0^q, X_1^q, X_2^q, X_3^q) \rangle_{\mathbb{F}_{q^5}}.$$

The *height* of a point P with respect Σ, denoted by $\mathrm{ht}(P)$, is the projective dimension of the σ-cyclic subspace $\overline{P, P^\sigma, P^{\sigma^2}, P^{\sigma^3}, P^{\sigma^4}}$ ([1]). Note that $\mathrm{ht}(\Lambda \cap \Lambda^\sigma) = \mathrm{ht}(\Lambda \cap \Lambda^{\sigma^4})$ and $\mathrm{ht}(\Lambda \cap \Lambda^{\sigma^2}) = \mathrm{ht}(\Lambda \cap \Lambda^{\sigma^3})$.

As usual, if $f(x) = \sum_{i=0}^{4} a_i x^{q^i}$ is a q-polynomial, then

$$L_f = \{\langle (x, f(x)) \rangle_{\mathbb{F}_{q^5}} : x \in \mathbb{F}_{q^5}^*\}$$

denotes the related linear set.

Proposition 2.1. *There exists a q-polynomial $f(x) = \sum_{i=1}^{4} a_i x^{q^i}$ with $a_4 = 1$, such that $\mathbb{L}$ is projectively equivalent to L_f, or $\mathbb{L}$ is projectively equivalent to L_g where $g(x) = ax^{q^2} + x^{q^3}$, $a \in \mathbb{F}_{q^5}^*$, $\mathrm{N}_{q^5/q}(a) \neq 0, 1$.*

Proof. Up to projective equivalence, $\mathbb{L} = L_h$ with $h = \sum_{i=1}^{4} a_i x^{q^i}$ may be assumed. If $a_4 \neq 0$ a further projectivity leads to $a_4 = 1$. If $a_1 \neq 0$, then $\mathbb{L} = L_{\hat{h}}$ where $\hat{h} = \sum_{i=1}^{4} a_i^{q^{5-i}} x^{q^{5-i}}$ [1, Lemma 2.6], [6, Lemma 3.1], leading once again to the desired form. Finally, if $a_1 = a_4 = 0$, then $a_2 a_3 \neq 0$ since otherwise $\mathbb{L}$ would be of pseudoregulus type. In this case $\mathrm{N}_{q^5/q}(a) \neq 1$ is a necessary and sufficient condition for the linear set to be scattered [2, Cor. 3.7]. □

In the following, $O_0 = \langle (1,0,0,0,0) \rangle_{\mathbb{F}_{q^5}}$, $O_1 = \langle (0,1,0,0,0) \rangle_{\mathbb{F}_{q^5}}$, and so on.

height Sh

Proposition 2.2. *Let $g(x) = ax^{q^2} + x^{q^3}$, $a \in \mathbb{F}_{q^5}^*$. Then L_g is the projection of the standard subgeometry from the vertex*

$$\Lambda = \overline{O_1, O_4, \langle (0,0,1,-a,0) \rangle_{\mathbb{F}_{q^5}}}.$$

The intersection $\Lambda \cap \Lambda^{\sigma^i}$ is a point for any $i = 1, 2, 3, 4$. Furthermore, $\Lambda \cap \Lambda^\sigma$ has height four if and only if $\mathrm{N}_{q^5/q}(a)^2 - \mathrm{N}_{q^5/q}(a) + 1 \neq 0$, whereas $\Lambda \cap \Lambda^{\sigma^2} = O_1$ has height four for any $a \in \mathbb{F}_{q^5}^*$.

Proof. As regards the first assertion, just take into consideration the following singular matrix:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -a & 0 \\ 0 & 1 & 0 & 0 & 0 \\ u & u^q & u^{q^2} & u^{q^3} & u^{q^4} \\ u & 0 & 0 & au^{q^2} + u^{q^3} & 0 \end{pmatrix}. \qquad (1)$$ e:vertice

[1] $\overline{S}$ denotes the projective closure of S.

Straightforward computations give $\dim(\overline{\Lambda \cup \Lambda^\sigma}) = \dim(\overline{\Lambda \cup \Lambda^{\sigma^2}}) = 4$. The intersection $\Lambda \cap \Lambda^\sigma$ is the point $\langle (0,0,1,-a,a^{q+1}) \rangle_{\mathbb{F}_{q^5}}$, and

$$\det \begin{pmatrix} 0 & 0 & 1 & -a & a^{q+1} \\ a^{q^2+q} & 0 & 0 & 1 & -a^q \\ -a^{q^2} & a^{q^3+q^2} & 0 & 0 & 1 \\ 1 & -a^{q^3} & a^{q^4+q^3} & 0 & 0 \\ 0 & 1 & -a^{q^4} & a^{q^4+1} & 0 \end{pmatrix} = \mathrm{N}_{q^5/q}(a)^2 - \mathrm{N}_{q^5/q}(a) + 1. \ \square$$

The proof of the following is similar to the one of Proposition 2.2:

Proposition 2.3. *The Lunardon-Polverino linear set L_f with $f = ax^q + x^{q^4}$, $\mathrm{N}_{q^5/q}(a) \neq 0, 1$, is the projection of the standard subgeometry from the vertex*

$$\Lambda = \overline{O_2, O_3, \langle (0,1,0,0,-a) \rangle_{\mathbb{F}_{q^5}}}.$$

The point $\Lambda \cap \Lambda^\sigma = O_3$ has height four, whereas $\Lambda \cap \Lambda^{\sigma^2}$ has height four if and only if $\mathrm{N}_{q^5/q}(a)^2 - \mathrm{N}_{q^5/q}(a) + 1 \neq 0$.

height4

Proposition 2.4. *Assume $\mathrm{ht}(\Lambda \cap \Lambda^\sigma) = 4$. Then, up to projectivities,*

$$\mathbb{L} = L_{\alpha,\beta} = \{ \langle (x - \alpha x^{q^2}, x^q - \beta x^{q^2}) \rangle_{\mathbb{F}_{q^5}} : x \in \mathbb{F}_{q^5}^* \} \tag{2}$$ e:canonicasi

for some $\alpha, \beta \in \mathbb{F}_{q^5}$ satisfying $\alpha^q \neq \beta^{q+1}$.

Proof. Since the setwise stabilizer $\mathrm{PGL}(5, q^5)_{\{\Sigma\}}$ acts transitively on the points of $\mathrm{PG}(4, q^5)$ of height four, [4, Proposition 3.1], it may be assumed that $O_4 = \Lambda \cap \Lambda^\sigma$. This in turn implies $O_3 \in \Lambda$, and

$$\Lambda = \overline{\langle (a,b,c,0,0) \rangle_{\mathbb{F}_{q^5}}, O_3, O_4} \tag{3}$$ e:zero

for some $a, b, c \in \mathbb{F}_{q^5}$, not all zero. The hyperplane coordinates of the span of Λ and P_u are

$$[cu^q - bu^{q^2} : -cu + au^{q^2} : bu - au^q : 0 : 0].$$

So, for $c = 0$ the linear set $\mathbb{L}$ is projectively equivalent to

$$\{ \langle (x^{q^2}, bx - ax^q) \rangle_{\mathbb{F}_{q^5}} : x \in \mathbb{F}_{q^5}^* \} = \{ \langle (x, bx^{q^3} - ax^{q^4}) \rangle_{\mathbb{F}_{q^5}} : x \in \mathbb{F}_{q^5}^* \},$$

and by [1, Lemma 2.6], [6, Lemma 3.1] this can be expressed in the form L_f where $f = dx^q + ex^{q^2}$; more precisely, $d = -a^q$ and $e = b^{q^2}$. Since L is not of pseudoregulus type, $de \neq 0$. In this case $\mathbb{L}$ is projectively equivalent

to $L_{0,-ed^{-1}}$. If $c \neq 0$, then $c = 1$ may be assumed. Let $f_1(u) = u^q - bu^{q^2}$, $f_2(u) = -u + au^{q^2}$, $f_3(u) = bu - au^q$. Clearly $f_3 = -af_1 - bf_2$. So, taking into account that $\mathbb{L}$ is scattered, the pairs $(f_1(u), f_2(u))$ and $(f_1(v), f_2(v))$ are $\mathbb{F}_q$-linearly dependent if and only if u and v are. Therefore $f_1(u)$ and $f_2(u)$ can be chosen as homogeneous coordinates of the points of $\mathbb{L}$.

If the intersection $\Lambda \cap \Lambda^\sigma$ is not a point then $\mathbb{L}$ is a linear set of pseudoregulus type, a contradiction. Furthermore, direct computations show that $\Lambda \cap \Lambda^\sigma$ is a point if and only if $b^{q+1} - ca^q \neq 0$. This implies $\alpha^q \neq \beta^{q+1}$. □

equivPSE **Proposition 2.5.** *(i) The linear set $L_{\alpha,\beta}$ has rank less than five if and only if*

$$\alpha^q = \beta^{q+1} \quad \text{and} \quad \mathrm{N}_{q^5/q}(\alpha) = \mathrm{N}_{q^5/q}(\beta) = 1. \tag{4}$$ eqalphabeta

(ii) If $\alpha^q \neq \beta^{q+1}$, then $L_{\alpha,\beta}$ is not of pseudoregulus type.

(iii) If $\alpha^q = \beta^{q+1}$ and $(\mathrm{N}_{q^5/q}(\alpha), \mathrm{N}_{q^5/q}(\beta)) \neq (1,1)$, then $L_{\alpha,\beta}$ is of pseudoregulus type.

Proof. Note that $x - \alpha x^{q^2}$ has non-trivial zeros if and only if $\mathrm{N}_{q^5/q}(\alpha) = 1$ and $x^q - \beta x^{q^2}$ has non-trivial zeros if and only if $\mathrm{N}_{q^5/q}(\beta) = 1$. Also, $L_{\alpha,\beta}$ is of rank less than 5 if and only if there is a common non-trivial root of the defining polynomials, that is, there exists $x \in \mathbb{F}_{q^5}^*$ such that $x^{(q+1)(1-q)} = \alpha$ and $x^{(1-q)q} = \beta$. This is equivalent to Equation (4).

Since for $\alpha^q \neq \beta^{q+1}$ both $\Lambda \cap \Lambda^\sigma$ and $\Lambda \cap \Lambda^{\sigma^2}$ are points, no linear set of type $L_{\alpha,\beta}$ satisfying such inequality is of pseudoregulus type, whereas, as mentioned in proof of Proposition 2.4, if $\alpha^q = \beta^{q+1}$, then $\Lambda \cap \Lambda^\sigma$ is a line, so $L_{\alpha,\beta}$ is of pseudoregulus type. □

Remarks.
1) For $\beta = 0$ and $\mathrm{N}_{q^5/q}(\alpha) \neq -1$, Equation (2) defines a linear set of Lunardon-Polverino type. As a matter of fact take $y = x^q$, then up to projective equivalence $L_{\alpha,\beta}$ is

$$\{\langle (y, -\alpha y + y^{q^4}) \rangle_{\mathbb{F}_{q^5}} : y \in \mathbb{F}_{q^5}^*\}$$

which is maximum scattered if and only if $\mathrm{N}_{q^5/q}(-\alpha) \neq 1$ [13].
2) Similarly to Proposition 2.4, if $\mathrm{ht}(\Lambda \cap \Lambda^{\sigma^2}) = 4$ and $\mathbb{L}$ is not of Sheekey type, then $\mathbb{L}$ is projectively equivalent to

$$\{\langle (x - \alpha x^{q^3}, x^q - \beta x^{q^3}) \rangle_{\mathbb{F}_{q^5}} : x \in \mathbb{F}_{q^5}^*\}$$

for some $\alpha, \beta \in \mathbb{F}_{q^5}$ not both zero.

3 On some binomial linear sets

lem1 **Lemma 3.1.** *Let $q \geq 223$. Then any $b \in \mathbb{F}_{q^5}^*$ can be written as*

$$b = \frac{uv^q - u^q v}{u^{q^2} v - u v^{q^2}} \tag{5}$$ eq1

for some $u, v \in \mathbb{F}_{q^5}^*$ such that $\dim\langle u, v\rangle_{\mathbb{F}_q} = 2$.

We will use the following preliminary result.

prelvar **Lemma 3.2.** [17, Corollary 7] *Let $G \in \mathbb{F}_q[x_1, \ldots, x_n]$ be an absolutely irreducible polynomial of degree d, and let $H \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial of degree e, not divisible by G. Then there exists a nonsingular zero of G over $\mathbb{F}_q$, which is not a zero of H, provided that*

$$q > \frac{1}{4}\left((d-1)((d-2) + \sqrt{(d-1)^2(d-2)^2 + 4(d^2+de+10)}\right)^2. \tag{6}$$ eqs

Now we can proceed with the proof of Lemma 3.1.

Proof. First note that the right hand side of Equation (5) only makes sense when $\dim\langle u, v\rangle_{\mathbb{F}_q} = 2$.

Let b be an arbitrary element of $\mathbb{F}_{q^5}^*$. Clearly,

$$(u^{q^2} v - u v^{q^2})b = uv^q - u^q v$$

holds for $u, v \in \mathbb{F}_{q^5}^*$ if and only if

$$v^{q^2+1}\left(\left(\frac{u}{v}\right)^{q^2} - \left(\frac{u}{v}\right)\right)b = -v^{q+1}\left(\left(\frac{u}{v}\right)^{q} - \left(\frac{u}{v}\right)\right),$$

which is equivalent to

$$\left(\left(\frac{u}{v}\right)^{q^2} - \left(\frac{u}{v}\right)\right)b = -\frac{1}{v^{q^2-q}}\left(\left(\frac{u}{v}\right)^{q} - \left(\frac{u}{v}\right)\right), \tag{7}$$ eq2

since $v \neq 0$. Let $x := u/v$ and $y = 1/v^q$. Then Equation (7) reads,

$$y^{q-1} = -b\left(\frac{x^{q^2} - x}{x^q - x}\right). \tag{8}$$ eq3

Note that if we can find a couple (x, y) where $x \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$ and $y \in \mathbb{F}_{q^5}^*$ such that Equation (8) is satisfied, then we can find a couple $(u, v) \in \mathbb{F}_{q^5}^* \times \mathbb{F}_{q^5}^*$ satisfying Equation (7) simply defining $v = \nu$, where $\nu^q = 1/y$ and $u = vx$.

Given $x \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$, there exists $y \in \mathbb{F}_{q^5}^*$ such that Equation (8) is satisfied if and only if

$$\left(-b\left(\frac{x^{q^2}-x}{x^q-x}\right)\right)^m = -b^m\left(\frac{x^{q^2}-x}{x^q-x}\right)^m = 1, \tag{9}$$ eq4

where $m = (q^5-1)/(q-1)$. In fact if $y \in \mathbb{F}_{q^5}^*$ exists then it is sufficient to use that $(y^{q-1})^m = y^{q^5-1} = 1$ to note that Equation (9) is satisfied. Conversely, if Equation (9) is satisfied, then $-b(x^{q^2}-x)/(x^q-x)$ is a $(q-1)$-th power in $\mathbb{F}_{q^5}$ and hence it is sufficient to define y to be an arbitrary $(q-1)$-th root of $-b(x^{q^2}-x)/(x^q-x)$.

Hence our aim is to show that for any $a \in \mathbb{F}_q^*$, there exists $x \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$ such that

$$(x^{q^2}-x)^m = a(x^q-x)^m, \tag{10}$$ eq5

so that defining $a := -b^m$ the claim will follow.

A geometrical interpretation of Equation (10) as the set of $\mathbb{F}_q$-rational points of an algebraic variety in $\mathbb{A}^5(\mathbb{F}_q)$ can be given as follows.

From [12, Theorem 2.35] we know that $\mathbb{F}_{q^5}$ admits a normal basis over $\mathbb{F}_q$, that is a basis of type $\{\gamma, \gamma^q, \gamma^{q^2}, \gamma^{q^3}, \gamma^{q^4}\}$ for some $\gamma \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$. So every solution x of Equation (10) can be written as $x = \sum_{i=0}^4 x_i \gamma^{q^i}$ where $x_i \in \mathbb{F}_q$ for every $i = 0, \dots 4$. By applying the identification $\mathbb{F}_{q^5} \cong \mathbb{F}_q^5$ the q elements of $\mathbb{F}_q$ in $\mathbb{F}_{q^5}$ can be identified with the elements of type $x = \sum_{i=0}^4 \xi \gamma^{q^i}$ where $\xi \in \mathbb{F}_q$ as $\mathrm{Tr}_{q^5/q}(\gamma) = \gamma + \gamma^q + \gamma^{q^2} + \gamma^{q^3} + \gamma^{q^4} \in \mathbb{F}_q^*$; while Equation (10) can be rewritten as a system of 5 equations in 5 variables of type

$$\mathcal{V} : \begin{cases} C_0(x_0, \dots, x_4) = a', \\ C_1(x_0, \dots, x_4) = a', \\ C_2(x_0, \dots, x_4) = a', \\ C_3(x_0, \dots, x_4) = a', \\ C_4(x_0, \dots, x_4) = a' \end{cases} \tag{11}$$ eq8

where $a' = a(\mathrm{Tr}_{q^5/q}(\gamma))^{-1}$. Indeed the algebraic variety $\mathcal{V} \subseteq \mathbb{A}^4(\mathbb{F}_q)$ is obtained by forcing each coefficient $C_i(x_0, \dots, x_4)$ of γ^{q^i} in $(x^{q^2}-x)^m/(x^q-x)^m = ((x^q-x)^{q-1}+1)^m$ to be equal to a' for $i = 0, \dots, 4$.

We apply the following change of variables in $\mathbb{F}_{q^5}$ (whose matrix is a so-called Moore matrix and is nonsingular):

$$\begin{cases} A = x_0\gamma + x_1\gamma^q + x_2\gamma^{q^2} + x_3\gamma^{q^3} + x_4\gamma^{q^4}, \\ B = x_4\gamma + x_0\gamma^q + x_1\gamma^{q^2} + x_2\gamma^{q^3} + x_3\gamma^{q^4}, \\ C = x_3\gamma + x_4\gamma^q + x_0\gamma^{q^2} + x_1\gamma^{q^3} + x_2\gamma^{q^4}, \\ D = x_2\gamma + x_3\gamma^q + x_4\gamma^{q^2} + x_0\gamma^{q^3} + x_1\gamma^{q^4}, \\ E = x_1\gamma + x_2\gamma^q + x_3\gamma^{q^2} + x_4\gamma^{q^3} + x_0\gamma^{q^4}, \end{cases}$$

that is $(A, B, C, D, E) = (x, x^q, x^{q^2}, x^{q^3}, x^{q^4})$. In these new variables, recalling that $m = q^4 + q^3 + q^2 + q + 1$, Equation (10) reads,

$$\mathcal{H} : (C-A)(D-B)(E-C)(A-D)(B-E) - a(B-A)(C-B)(D-C)(E-D)(A-E) = 0, \tag{12}$$

eq9

which is a hypersurface in $\mathbb{A}^5(\mathbb{F}_{q^5})$. We showed that the change of variables implies that the algebraic variety $\mathcal{V} \subseteq \mathbb{A}^5(\mathbb{F}_q)$ is birationally isomorphic to the hypersurface $\mathcal{H}$ over $\mathbb{F}_{q^5}$. Since the dimension of a variety is a birational invariant, also $\mathcal{V}$ is a hypersurface of degree 5 in $\mathbb{A}^5(\mathbb{F}_q)$, that is $C_i = C_j$ for $i, j = 0, \ldots, 4$.

Also, for the same reason we can show that $\mathcal{H}$ is absolutely irreducible to prove the absolute irreducibility of $\mathcal{V}$.

To ensure the existence of at least one point of the algebraic variety in Equation (11), we will use the following strategy.

- We prove that $\mathcal{H}$ is absolutely irreducible, so that $\mathcal{V} \subseteq \mathbb{A}^5(\mathbb{F}_q)$ is an absolutely irreducible hypersurface of degree 5.
- We apply Lemma 3.2 with respect to the hyperplane $H(x_0, \ldots, x_4) = x_0 - x_1 = 0$ to ensure the existence of a point $P = (p_0, p_1, p_2, p_3, p_4) \in \mathcal{V}$ with $p_0 \neq p_1$. Recalling that the elements in $\mathbb{F}_q$ are identified with the vectors in $\mathbb{F}_q^5$ of type (a, a, a, a, a) with $a \in \mathbb{F}_q$ this implies the existence of a solution $x \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$ of Equation (10).

We start with some preliminary observations that will help us to deal with the first point of the aforementioned strategy. First, note that the variety $\mathcal{H}$ can also be seen as a projective variety in $\mathrm{PG}(4, q)$ as the defining polynomial in Equation (12) is homogeneous. Doing so we can consider the projective transformation τ given by $\tau : (A, B, C, D, E) \mapsto (B, C, D, E, A)$. Then the map τ has order 5 and fixes $\mathcal{H}$. Also when de-homogenizing with respect to the variable E, monomials in $\mathcal{H}$ have degree $3, 4$ or 5 in the variables A, B, C and D. Finally since the degree of $\mathcal{H}$ is five either $\mathcal{H}$ is

absolutely irreducible, or it has a linear component (hyperplane) or it splits in an absolutely irreducible cubic and an absolutely irreducible quadric. We divide the proof in two steps accordingly.

- **Step 1: $\mathcal{H}$ has no linear component.** Let $t : a_1A + b_1B + c_1C + d_1D + e_1E = 0$ be a linear component of $\mathcal{H}$ in $PG(4, q)$. There are clearly two possibilities: either t is not fixed by τ or $\tau(t) = t$.

  Suppose that the first case occurs, that is, $\tau(t) \neq t$. Since $\mathcal{H}$ is fixed by τ also $\tau^i(t)$ is a linear component of $\mathcal{H}$ for all $i \geq 0$. The fact that τ has order 5 implies hence, that $\mathcal{H}$ decomposes completely as the union of such (five) linear components, namely t and $\tau^i(t)$ with $i = 1, \ldots, 4$. However as observed before, each monomial in (12) has degree at least 3 in the variables A, B, C and D, implying that the same should happen for the product of t and all the $\tau(t)^i$'s with $i = 1, 2, 3, 4$. This implies that t is a binomial in A, B, C, D and E. Indeed if at least 3 terms appear in t then there must exist a monomial in A, B, C, D and E of degree at least 3 in E, and hence of degree at most 2 in the other variables. However the term $-CD^2E^2$ that appears in $\mathcal{H}$ cannot be obtained by any product of t and the $\tau^i(t)$'s when only two terms appear in t, which is a contradiction.

  Assume hence that $\tau(t) = t$, that is, $a_1 = b_1 = c_1 = d_1 = e_1 \neq 0$. Since$a_1 \neq 0$ then $A = (b_1B+c_1C+d_1D+e_1E+f_1)/a_1$. Substituting in $\mathcal{H}$ and considering the evaluation at $(A, B, C, 0, 0)$ we get that $b_1 = 0$, a contradiction.

- **Step 2: $\mathcal{H}$ does not split as the product of an absolutely irreducible cubic and an absolutely irreducible quadric.**

  Assume by contradiction that the projective variety $\mathcal{H}$ has a quadric component $\mathcal{C}$. Then $\mathcal{C}$ must be fixed by τ, as $\mathcal{H}$ has degree 5 and hence cannot have $\tau(\mathcal{C})$ as an additional component. This implies that $\mathcal{C}$ can be written as

$$\mathcal{C} : \alpha(a_1A^2 + b_1B^2 + c_1C^2 + d_1D^2 + e_1E^2)$$

$$+\beta(a_{1,2}AB + a_{2,3}BC + a_{3,4}CD + a_{4,5}DE + a_{5,1}AE)$$

$$+\gamma(a_{1,3}AC + a_{2,4}BD + a_{3,5}CE + a_{4,1}DA + a_{5,2}BE) = 0,$$

  where all the coefficients apart from possibly α, β, γ are non-zero. Evaluating the resultant of $\mathcal{H}$ and $\mathcal{C}$ with respect to B in $(A, B, C, 0, 0)$ we

get that $\alpha a_1 A^2 + \alpha c_1 C^2 + \gamma a_{13} AC$ is identically zero, which in particular yields $\alpha a_1 = \gamma a_{13} = 0$, that is, $\alpha = \gamma = 0$. By direct substitution in the same resultant and the corresponding evaluation in $(0, B, 0, D, E)$ we get $\beta = 0$, a contradiction.This method can fail only if all the coefficients of terms involving A in $\mathcal{C}$ are equal to zero. However,this is not possible as it would immediately imply that $\alpha = \beta = \gamma = 0$.

This shows that $\mathcal{H}$ (and hence $\mathcal{V}$) is absolutely irreducible.

From Lemma 3.2 applied with respect to the hyperplane $H(x_0, \ldots, x_4) = x_0 - x_1$ we get that if

$$q > \left\lfloor \frac{1}{4}\left((5-1)((5-2) + \sqrt{(5-1)^2(5-2)^2 + 4(25 + 5 \cdot 1 + 10)}\right)^2 \right\rfloor = 216$$

then $\mathcal{V}$ has at least an $\mathbb{F}_q$-rational point P which does not correspond to a solution of Equation (10) in $\mathbb{F}_q$. Since in our hypothesis $q \geq 223$ the claim follows. □

prop2 **Proposition 3.3.** *Let $q \geq 223$ and let $f(x) = x^q + bx^{q^2}$ for some $b \in \mathbb{F}_{q^5}^*$. Then $L_f = \{\langle (x, f(x)) \rangle_{\mathbb{F}_{q^5}} : x \in \mathbb{F}_{q^5}^*\}$ is not a maximum scattered linear set of* $\mathrm{PG}(1, q^5)$.

Proof. It is enough to show that there exists $m \in \mathbb{F}_{q^5}$ such that $h_m(x) := mx + x^q + bx^{q^2}$ has q^2 roots in $\mathbb{F}_{q^5}$. From Lemma 3.1, there exist $u, v \in \mathbb{F}_{q^5}^*$ such that Equation (5) is satisfied and $\dim \langle u, v \rangle_{\mathbb{F}_q} = 2$. Put $m = (u^q v^{q^2} - u^{q^2} v^q)/(u^{q^2} v - u v^{q^2})$. Then by direct checking $h_m(u) = h_m(v) = 0$. □

rem34 **Remark 3.4.** Proposition 3.3 has been extended by an exhaustive computer search using GAP also to any $q \leq 17$.

Remark 3.5. By Proposition 3.3 and Remark 3.4, for $\beta \neq 0$ no $L_{0,\beta}$ is scattered for $q \geq 223$ or $q \leq 17$.

4 The linear sets $L_{\alpha,\beta}$

Let $L_{\alpha,\beta}$ denote the linear set defined in Equation (2). Motivated by Propositions 2.5 and 3.3 and Remark 3.4 at the end of Section 2, we will always assume $\alpha^q \neq \beta^{q+1}$ and $\alpha\beta \neq 0$. Since the point $\langle (0, 1) \rangle_{\mathbb{F}_{q^5}}$ has weight less or

equal to one, $L_{\alpha,\beta}$ is maximum scattered if and only if there is no $m \in \mathbb{F}_{q^5}$ such that

$$h_m(x) := m(x - \alpha x^{q^2}) + (x^q - \beta x^{q^2}) = mx + x^q - x^{q^2}(\beta + m\alpha) \qquad (13)$$ eqh

has q^2 roots in $\mathbb{F}_{q^5}$, that is, if and only if there is no $m \in \mathbb{F}_{q^5}$ such that $h_m(x)$ has a two-dimensional kernel.

Using this fact, we prove the following characterization of maximum scattered $\mathbb{F}_q$-linear sets of type $L_{\alpha,\beta}$. It follows as a direct application of [7, Theorem 3.3 and Section 3.3].

char **Lemma 4.1.** *Let $\alpha, \beta \in \mathbb{F}_{q^5}$ with $(\alpha, \beta) \neq (0, 0)$. Then $L_{\alpha,\beta}$ is maximum scattered if and only if there is no $\lambda \in \mathbb{F}_{q^5}$ such that ([2])*

$$\begin{cases} N(\lambda) = -1, \\ \lambda^q \beta^{q^3+q+1} + \beta^{q^3}(1-\lambda\alpha)^{q+1} - \lambda^{q^2+q+1}(1-\lambda\alpha)^{q^3}\beta^{q+1} = 0. \end{cases} \qquad (14)$$ char1

Proof. As recalled, $L_{\alpha,\beta}$ is maximum scattered if and only if there is no $m \in \mathbb{F}_{q^5}$ such that $h_m(x)$ has maximum kernel. We note that both $m \neq 0$ and $\beta + m\alpha \neq 0$ can be assumed. Indeed $h_0(x) = x^q - x^{q^2}\beta$ and such polynomial has clearly less than q^2 roots. The same holds if $\beta + m\alpha = 0$ as in this case $h_m(x) = mx + x^q$. So, $L_{\alpha,\beta}$ is maximum scattered if and only if there is no $m \in \mathbb{F}_{q^5}^*$ with $\beta + m\alpha \neq 0$ such that the polynomial $k_m(x) = a_0 x + a_1 x^q - x^{q^2}$ has maximum kernel, where

$$a_0 = \frac{m}{\beta + m\alpha}, \quad \text{and} \quad a_1 = \frac{1}{\beta + m\alpha}.$$

From [7, Theorem 3.3 and Section 3.3] $k_m(x)$ has maximum kernel if and only if

$$\begin{cases} N\left(\frac{m}{\beta+m\alpha}\right) = -1, \\ \left(\frac{m}{\beta+m\alpha}\right)^q + \left(\frac{1}{\beta+m\alpha}\right)^{q+1} = \left(\frac{m}{\beta+m\alpha}\right)^{q^2+q+1}\left(\frac{1}{\beta+m\alpha}\right)^{q^3}. \end{cases} \qquad (15)$$ maxker

Write $\lambda = m/(\beta + m\alpha)$, so that $m = \lambda\beta/(1 - \lambda\alpha)$ and $1/(\beta + m\alpha) = (1 - \lambda\alpha)/\beta$. We get that $L_{\alpha,\beta}$ is maximum scattered if and only if there is no $\lambda \in \mathbb{F}_{q^5}$ such that

[2] In order to simplify the notation, from now on we write $N(-)$ instead of $\mathrm{N}_{q^5/q}(-)$.

$$\begin{cases} N(\lambda) = -1, \\ \lambda^q + \frac{(1-\lambda\alpha)^{q+1}}{\beta^{q+1}} = \lambda^{q^2+q+1} \frac{(1-\lambda\alpha)^{q^3}}{\beta^{q^3}}. \end{cases} \tag{16}$$ rewr

and this is equivalent to Equation (14). □

Our aim is to show with the help of Lemma 4.1 that if $\alpha^q/\beta^{q+1} \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$, $\beta \neq 0$, then $L_{\alpha,\beta}$ is not maximum scattered.

Applying the same strategy as in the proof of Lemma 3.1, we write $\lambda = l\gamma + \sum_{i=i}^{4} l_i \gamma^{q^i}$ where $\{\gamma, \gamma^q, \ldots, \gamma^{q^4}\}$ is a normal basis of $\mathbb{F}_{q^5}$ over $\mathbb{F}_q$. In this way, the set of solutions of Equation (14) (equivalently Equation (16)) coincides with the set of $\mathbb{F}_q$-rational points of an algebraic variety $\mathcal{V}_2$ in $\mathbb{A}^5(\mathbb{F}_q)$ given by the equations

$$\mathcal{V}_2 : \begin{cases} EQ_1 : \ l \cdot l_1 \cdot l_2 \cdot l_3 \cdot l_4 = -1, \\ EQ_2 : \ l_1\beta^{q^3+q+1} + \beta^{q^3}(1 - l_1\alpha^q)(1 - l\alpha) - l_2 \cdot l_1 \cdot l \cdot (1 - l_3\alpha^{q^3})\beta^{q+1} = 0, \\ EQ_{2q} : \ l_2\beta^{q^4+q^2+q} + \beta^{q^4}(1 - l_2\alpha^{q^2})(1 - l_1\alpha^q) - l_3 \cdot l_2 \cdot l_1 \cdot (1 - l_4\alpha^{q^4})\beta^{q^2+q} = 0, \\ EQ_{2q^2} : \ l_3\beta^{1+q^3+q^2} + \beta(1 - l_3\alpha^{q^3})(1 - l_2\alpha^{q^2}) - l_4 \cdot l_3 \cdot l_2 \cdot (1 - l\alpha)\beta^{q^3+q^2} = 0, \\ EQ_{2q^3} : \ l_4\beta^{q+q^4+q^3} + \beta^q(1 - l_4\alpha^{q^4})(1 - l_3\alpha^{q^3}) - l \cdot l_4 \cdot l_3 \cdot (1 - l_1\alpha^q)\beta^{q^4+q^3} = 0, \\ EQ_{2q^4} : \ l\beta^{q^2+1+q^4} + \beta^{q^2}(1 - l\alpha)(1 - l_4\alpha^{q^4}) - l_1 \cdot l \cdot l_4 \cdot (1 - l_2\alpha^{q^2})\beta^{1+q^4} = 0. \end{cases} \tag{17}$$ altro

Hence in the following we will prove that $L_{\alpha,\beta}$ with $\alpha^q/\beta^{q+1} \notin \mathbb{F}_q$ is not maximum scattered proving that Equation (17) has an $\mathbb{F}_q$-rational solution. To this aim we will study the variety $\mathcal{V}_2$ proving that it is equivalent to an algebraic curve of degree 4. Since the dimension is a birational invariant this will show that also $\mathcal{V}_2$ is an algebraic curve. Showing that the curve of degree 4 is absolutely irreducible of genus at most 3, and using again that genus and irreducibility are invariant, we will obtain the same properties for $\mathcal{V}_2$. At this point, the existence of an $\mathbb{F}_{q^5}$-rational point of $\mathcal{V}_2$ will be ensured by the Hasse-Weil Theorem.

According to this general strategy, we start with the following technical lemma.

prel1 **Lemma 4.2.** *Let $\alpha, \beta \in \mathbb{F}_{q^5}$ with $\beta \neq 0$ and $\alpha^q/\beta^{q+1} \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$. Then the variety $\mathcal{V}_2$, is equivalent to the quartic curve $\mathcal{Q} : \ F(X, Y) = 0$, where*

$$
\begin{aligned}
F(X,Y) = {} & X^2Y^2\beta^{q^2+q+1}\alpha^{q^4+2q^3+q^2} - X^2Y^2\beta\alpha^{q^4+2q^3+2q^2} - X^2Y^2\beta^{q^3+2q^2+q}\alpha^{q^3} \\
& + X^2Y^2\beta^{q^3+q^2}\alpha^{q^3+q^2} + X^2YN(\beta)\alpha^{q^3+q^2} - 2X^2Y\beta^{q^2+q+1}\alpha^{q^4+q^3+q^2} \\
& - X^2Y\beta^{q^4+q^3+1}\alpha^{q^3+2q^2} + 2X^2Y\beta\alpha^{q^4+q^3+2q^2} + X^2Y\beta^{q^3+2q^2+q} \\
& - X^2Y\beta^{q^3+q^2}\alpha^{q^2} - X^2N(\beta)\alpha^{q^2} + X^2\beta^{q^2+q+1}\alpha^{q^4+q^2} + X^2\beta^{q^4+q^3+1}\alpha^{2q^2} \\
& - X^2\beta\alpha^{q^4+2q^2} + XY^2\beta^{q^3+2q^2+q+1}\alpha^{q^4+q^3} - XY^2\beta^{2q^3+q^2+q+1}\alpha^{q^4} \\
& - 2XY^2\beta^{q^3+q^2+1}\alpha^{q^4+q^3+q^2} + 2XY^2\beta\alpha^{q^4+2q^3+q^2} + XY^2\beta^{2q^3+2q^2} \\
& - XY^2\beta^{q^3+q^2}\alpha^{q^3} + XYN(\beta)\beta^{q^3+q^2} - XY\beta^{q^3+2q^2+q+1}\alpha^{q^4} \\
& - XYN(\beta)\alpha^{q^3} + 2XY\beta^{q^2+q+1}\alpha^{q^4+q^3} - XY\beta^{q^4+2q^3+q^2+1}\alpha^{q^2} \\
& + 2XY\beta^{q^3+q^2+1}\alpha^{q^4+q^2} + 2XY\beta^{q^4+q^3+1}\alpha^{q^3+q^2} - 4XY\beta\alpha^{q^4+q^3+q^2} \\
& - XY\beta^{2q^3+2q^2+q}\alpha - XY\beta^{q^4+2q^3+2q^2}\alpha^q + XY\beta^{q^3+q^2}N(\alpha) \\
& + XY\beta^{q^3+q^2} + XN(\beta) - X\beta^{q^2+q+1}\alpha^{q^4} - 2X\beta^{q^4+q^3+1}\alpha^{q^2} \\
& + 2X\beta\alpha^{q^4+q2} + X\beta^{q^4+2q^3+q^2}\alpha^{q^2+q+1} - X\beta^{q^3+q^2}\alpha^{q^4+q^2+q+1} - Y^2\beta^{2q^3+2q^2+1}\alpha^{q^4} \\
& + 2Y^2\beta^{q^3+q^2+1}\alpha^{q^4+q^3} - Y^2\beta\alpha^{q^4+2q^3} + Y\beta^{q^4+2q^3+q^2+1} - 2Y\beta^{q^3+q^2+1}\alpha^{q^4} \\
& - Y\beta^{q^4+q^3+1}\alpha^{q^3} + 2Y\beta\alpha^{q^4+q^3} + Y\beta^{2q^3+2q^2}\alpha^{q^4+q+1} - Y\beta^{q^3+q^2}\alpha^{q^4+q^3+q+1} \\
& + \beta^{q^4+q^3+1} - \beta\alpha^{q^4} - \beta^{q^4+2q^3+q^2}\alpha^{q+1} + \beta^{q^3+q^2}\alpha^{q^4+q+1}. \qquad (18)
\end{aligned}
$$

quartica

Proof. First we note that the polynomial $F(X,Y)$ defines indeed a quartic curve, that is, the coefficient of X^2Y^2 does not vanish. Indeed this coefficient coincides with

$$
\beta^{q^2+q+1}\alpha^{q^4+2q^3+q^2} - \beta\alpha^{q^4+2q^3+2q^2} - \beta^{q^3+2q^2+q}\alpha^{q^3} + \beta^{q^3+q^2}\alpha^{q^3+q^2} =
$$

$$
(\beta^{q+1} - \alpha^q)^q(\beta\alpha^{q^4+2q^3+q^2} - \beta^{q^3+q^2}\alpha^{q^3}).
$$

Clearly $\beta^{q+1} - \alpha^q \neq 0$ as $\alpha^q/\beta^{q+1} \notin \mathbb{F}_q$. If $\beta\alpha^{q^4+2q^3+q^2} - \beta^{q^3+q^2}\alpha^{q^3} = 0$ then since both β and α are non-zero we get $\alpha^{q^4+q^3+q^2} = \beta^{q^3+q^2-1}$. This implies that $N(\alpha) = \alpha^{q+1}\beta^{q^3+q^2-1} \in \mathbb{F}_q$. However

$$
\alpha^{q+1}\beta^{q^3+q^2-1} = \left(\frac{\alpha^q}{\beta^{q+1}}\right)(\alpha\beta^{q^3+q^2+q}) = \left(\frac{\alpha^q}{\beta^{q+1}}\right)^{q^4+1} N(\beta),
$$

and hence also $(\alpha^q/\beta^{q+1})^{q^4+1} \in \mathbb{F}_q$. Since $\alpha^q/\beta^{q+1} \in \mathbb{F}_{q^5}$, we get that $\alpha^q/\beta^{q+1} \in \mathbb{F}_q$, which is not possible. The following computations can be checked using MAGMA. The system of equations (17) admits a solution if

and only if $l_4 = -1/(l \cdot l_1 \cdot l_2 \cdot l_3)$ and EQ_2,EQ_{2q} and EQ_{2q^i} evaluated at $(l, l_1, l_2, l_3, -1/(l \cdot l_1 \cdot l_2 \cdot l_3))$ are equal to zero for all $i = 2, \ldots, 4$. Clearly $l, l_1, l_2, l_3, l_4 \neq 0$. Since

$$EQ_{2q^2}(l, l_1, l_2, l_3, -1/(l \cdot l_1 \cdot l_2 \cdot l_3)) : \; l \cdot (l_1 \cdot l_2 \cdot l_3 \cdot \beta\alpha^{q^3+q^2} - l_1 \cdot l_2 \cdot \beta\alpha^{q^2}$$

$$+l_1 \cdot l_3 \cdot \beta^{q^3+q^2+1} - l_1 \cdot l_3 \cdot \beta\alpha^{q^3} + l_1\beta - \beta^{q^3+q^2}\alpha) + \beta^{q^3+q^2} = 0,$$

we get

$$l_4 = -\frac{1}{l \cdot l_1 \cdot l_2 \cdot l_3}, \; l = \frac{-\beta^{q^3+q^2}}{P(l_1, l_2, l_3)},$$

with

$$P(l_1, l_2, l_3) = l_1 \cdot l_2 \cdot l_3 \cdot \beta\alpha^{q^3+q^2} - l_1 \cdot l_2 \cdot \beta\alpha^{q^2} + l_1 \cdot l_3 \cdot \beta^{q^3+q^2+1} - l_1 \cdot l_3 \cdot \beta\alpha^{q^3} + l_1\beta - \beta^{q^3+q^2}\alpha$$

and EQ_2,EQ_{2q} and EQ_{2q^i} evaluated at $(-\beta^{q^3+q^2}/P(l_1, l_2, l_3), l_1, l_2, l_3, -1/(l \cdot l_1 \cdot l_2 \cdot l_3))$ are equal to zero for $i = 3, 4$. Clearly $P(l_1, l_2, l_3) \neq 0$ as $\beta \neq 0$. Now, $EQ_{2q} = 0$ implies

$$C_1(l_2, l_3)l_1 + C_2(l_2, l_3) = 0,$$

where

$$C_1(l_2, l_3) = l_2 l_3 \beta^{q+1}\alpha^{q^4+q^3+q^2} - l_2 \cdot l_3 \beta^{q^3+q^2+q} - l_2\beta^{q+1}\alpha^{q^4+q^2} + l_2\beta^{q^4+q^3}\alpha^{q^2+q}$$

$$+l_3\beta^{q^3+q^2+q+1}\alpha^{q^4} - l_3\beta^{q+1}\alpha^{q^4+q^2} + \beta^{q+1}\alpha^{q^4} - \beta^{q^4+q^3}\alpha^q,$$

and

$$C_2(l_2, l_3) = \beta^{q^3}(l_2\beta^{q^4+q^2+q} - l_2\beta^{q^4}\alpha^{q^2} - \beta^{q^2+q}\alpha^{q^4+1} + \beta^{q^4}).$$

We distinguish two cases: $C_1(l_2, l_3) = C_2(l_2, l_3) = 0$ or $l_1 = -C_2(l_2, l_3)/C_1(l_2, l_3)$.

- **Case 1:** $C_1(l_2, l_3) = C_2(l_2, l_3) = 0$**.** Hence

$$l_2 = \frac{\beta^{q^2+q}\alpha^{q^4+1} - \beta^{q^4}}{\beta^{q^4+q^2+q} - \beta^{q^4}\alpha^{q^2}},$$

and

$$l_3 = -P_2/P_1,$$

where

$$P_1 = N(\beta)\alpha^{q^4} - \beta^{q^4+q+1}\alpha^{q^4+q^3} + \beta^{q+1}\alpha^{2q^4+q^3+q^2+1} - \beta^{q^4+q^3+1}\alpha^{q^4+q^2}$$

$$-\beta^{q^4+q^2+q}\alpha^{q^4+1}+\beta^{q^4+q^3},$$

$$P_2=\beta^{q^4+q+1}\alpha^{q^4}-\beta^{q+1}\alpha^{2q^4+q^2+1}-\beta^{2q^4+q^3}\alpha^q+\beta^{q^4+q^3}\alpha^{q^4+q^2+q+1}.$$

Indeed if $P_1=P_2=0$ then $\alpha^q/\beta^{q+1}\in\mathbb{F}_q$. This fact can observed noting that from $P_2=0$, either $\beta=(\beta^{q^4+q^3}\alpha^q)/(\beta^q\alpha^{q^4})$ or $\beta=\alpha^{q^3+q+1}$. In the former case $\alpha^q/\beta^{q+1}=\alpha^{q^4}/\beta^{q^4+q^3}=(\alpha^q/\beta^{q+1})^{q^3}$. In the latter case $\alpha^q/\beta^{q+1}=1/N(\alpha)$. Substituting l_2 and l_3 in EQ_{2q^3} we get

$$l_1Q_1+Q_2=0,$$

where

$$Q_1=\beta^{q^4+2q^3+q^2}(\beta^{q^4}-\alpha^{q^4+q^2+1})(\beta^{q+1}-\alpha^q)(\beta^{2q+q^2}\alpha^{q^4+1}-\beta^{2q^4+q^3+q^2+q}\alpha^q$$

$$+\beta^{2q^4+q}\alpha^{q^3+q}-\beta^{q^4+q}N(\alpha)-\beta^{q^4+q}+\beta^{2q^4+q^3}\alpha^{q^2+q}),$$

and

$$Q_2=\beta^{q^4+2q^3+q^2}(\beta^{q+1}-\alpha^q)^q(\beta^{1+2q+q^2+q^3+2q^4}\alpha^{q^4+1}-\beta^{1+2q+q^2+q^4}\alpha^{2q^4+1}$$

$$-\beta^{1+2q+2q^4}\alpha^{1+q^3+q^4}+\beta^{1+2q+q^4}\alpha^{2+q^2+2q^4}-\beta^{1+q+q^3+2q^4}\alpha^{1+q^2+q^4}+\beta^{1+q+2q^4}\alpha^{q^4}$$

$$-\beta^{2q+q^2+q^3+q^4}\alpha^{2+q^4}+\beta^{2q+q^2}\alpha^{2+2q^4}+\beta^{q+q^3+2q^4}\alpha+\beta^{q+2q^4}\alpha^{1+q+q^3+q^4}$$

$$-\beta^{q+q^4}\alpha^{q^4+1}N(\alpha)-\beta^{q+q^4}\alpha^{q^4}-\beta^{q^3+3q^4}\alpha^q+\beta^{q^3+2q^4}\alpha^{1+q+q^2+q^4}).$$

If $Q_1=Q_2=0$ then using again that $\alpha^q/\beta^{q+1}\notin\mathbb{F}_q$, $\beta^{2q+q^2}\alpha^{q^4+1}-\beta^{2q^4+q^3+q^2+q}\alpha^q+\beta^{2q^4+q}\alpha^{q^3+q}-\beta^{q^4+q}N(\alpha)-\beta^{q^4+q}+\beta^{2q^4+q^3}\alpha^{q^2+q}=0$ and $\beta^{1+2q+q^2+q^3+2q^4}\alpha^{q^4+1}-\beta^{1+2q+q^2+q^4}\alpha^{2q^4+1}-\beta^{1+2q+2q^4}\alpha^{1+q^3+q^4}+\beta^{1+2q+q^4}\alpha^{2+q^2+2q^4}-\beta^{1+q+q^3+2q^4}\alpha^{1+q^2+q^4}+\beta^{1+q+2q^4}\alpha^{q^4}-\beta^{2q+q^2+q^3+q^4}\alpha^{2+q^4}+\beta^{2q+q^2}\alpha^{2+2q^4}+\beta^{q+q^3+2q^4}\alpha+\beta^{q+2q^4}\alpha^{1+q+q^3+q^4}-\beta^{q+q^4}\alpha^{q^4+1}N(\alpha)-\beta^{q+q^4}\alpha^{q^4}-\beta^{q^3+3q^4}\alpha^q+\beta^{q^3+2q^4}\alpha^{1+q+q^2+q^4}=0$.

If $\beta^{2q}\alpha^{q^4+1}-\beta^{2q^4+q^3+q}\alpha^q=0$ then also $\beta^{2q^4+q}\alpha^{q^3+q}-\beta^{q^4+q}N(\alpha)-\beta^{q^4+q}+\beta^{2q^4+q^3}\alpha^{q^2+q}=0$ from the first equation. From the first equation $\beta^q=\beta^{2q^4+q^3}\alpha^q/\alpha^{q^4+1}$. Substituting to the second equation yields $0=\beta^{2q^4}\alpha^{q^3+q}-\beta^{q^4}N(\alpha)-\beta^{q^4}+\alpha^{q^4+q^2+1}=(\beta^{q^4}-\alpha^{q^4+q^2+1})(\beta^{q^4}\alpha^{q^3+q}-1)$. Hence $\alpha^q/\beta^{q+1}\in\mathbb{F}_q$, a contradiction.

Hence $\beta^{q^2}=(-\beta^{q+2q^4}\alpha^{q^3+q}+\beta^{q^4+q}N(\alpha)+\beta^{q^4+q}-\beta^{2q^4+q^3}\alpha^{q^2+q})/(\beta^{2q}\alpha^{q^4+1}-\beta^{2q^4+q^3+q}\alpha^q)$ for the first equation. Substituting β^{q^2} in the second equation we get that either $\beta^q\alpha-\beta^{q^4}\alpha^q=0$, or $\beta^q\alpha^{q^4+q^3+1}-\beta^{q^4+q^3}=$

0, or $\beta^{q+1}\alpha^{q^4} - \beta^{q^4+q^3}\alpha^q = 0$. If $\beta^q\alpha - \beta^{q^4}\alpha^q = 0$ then substituting β^{q^2} in the expressions of l_3 and l_4 above we get that l and l_4 are function of α and β. This fact is compatible with the description already obtained for l_4 if and only if $-\beta^{2q^3+q}\alpha + 2\beta^{q^3+q}\alpha^{q^4+q^3+q+1} - \beta^q\alpha^{2q^4+2q^3+2q+1} = \alpha\beta(\beta^{q^3} - \alpha^{q^4+q^3+q})$, which is not possible. If the second case occurs then, subsituting again l_2, l_3 and β^{q^4} we get that $\alpha^{q^4+1}\beta^q(\beta^q\alpha^{q^3} - \beta^{q^3}\alpha^{q^2})(\beta^q\alpha^{1+q+2q^3+q^4}\beta^{q^3})(b - \alpha^{q^3+q+1}) = 0$. In any case $\alpha^q/\beta^{q+1} \in \mathbb{F}_q$. The last case implies that $\alpha^q/\beta^{q+1} \in \mathbb{F}_{q^3}$, so that again we get a contradiction.

This shows that $l_1 = -Q_2/Q_1$. Substituting l_1 we get that all the conditions are satisfied. Hence the related point of $\mathcal{V}_2$ is

$$l_4 = -\frac{1}{l \cdot l_1 \cdot l_2 \cdot l_3},\ l = \frac{-\beta^{q^3+q^2}}{P(l_1, l_2, l_3)},\ l_2 = \frac{\beta^{q^2+q}\alpha^{q^4+1} - \beta^{q^4}}{\beta^{q^4+q^2+q} - \beta^{q^4}\alpha^{q^2}},$$

$$l_3 = \frac{-P_2}{P_1},\ l_1 = \frac{-Q_2}{Q_1}.$$

Substituting in $F(l_2, l_3)$ the value $l_2 = \frac{\beta^{q^2+q}\alpha^{q^4+1} - \beta^{q^4}}{\beta^{q^4+q^2+q} - \beta^{q^4}\alpha^{q^2}}$ we get that $l_3 = -P_2/P_1$ is a solution. This implies that $[l_1, l_2]$ is a point of the quartic.

- **Case 2:** $l_1 = -C_2(l_2, l_3)/C_1(l_2, l_3)$**.** Substituting the expression of l_1 in EQ_2, EQ_{2q^3} and EQ_{2q^4} we get that all the conditions are satisfied once $F(l_2, l_3) = 0$ (cf. Equation (18)).

  This shows that in any case a point of $\mathcal{V}_2$ corresponds uniquely to a point of the quartic $F(l_2, l_3) = 0$. Hence the variety $\mathcal{V}_2$ is a curve.

□

Following the general strategy described before we are going to show that the quartic $\mathcal{Q}$ is absolutely irreducible. Since its genus is at most $g = (4-1)(4-2)/2 = 3$, and irreducibility, genus and dimension are birationally invariant, from Lemma 4.2 and the Hasse-Weil bound we would obtain that the number of $\mathbb{F}_q$-rational points of $\mathcal{V}_2$ is at least:

$$q + 1 - 2g\sqrt{q} \geq q + 1 - 6\sqrt{q} > 0$$

provided that $q \geq 37$. If $q < 37$ it can be easily checked with MAGMA that the quartic $\mathcal{Q}$ has at least an $\mathbb{F}_{q^5}$-rational point of type $[\ell, \ell^q]$, implying by linearity of the other variables, a solution $[\ell, \ell^q, \ldots, \ell^{q^4}]$ of $\mathcal{V}_2$ and hence a solution of Equation (14).

nonMS **Proposition 4.3.** *Let $\alpha, \beta \in \mathbb{F}_{q^5}$ with $\beta \neq 0$ and $\alpha^q/\beta^{q+1} \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$. Then $L_{\alpha,\beta}$ is not maximum scattered.*

Proof. From Lemma 4.2 it is sufficient to show that the quartic $\mathcal{Q}$ is absolutely irreducible. The irreducibility of $\mathcal{Q}$ is equivalent to the non-existence of lines or quadrics as components.

To do so, we observe first that the shape of the quartic $\mathcal{Q}$ can help us to specify how components can look like a priori. Indeed linear components of $\mathcal{Q}$ can only be of type $X - A = 0$ or $Y - B = 0$, while quadric components can only be of type $XY + AX + BY + C = 0$, $X^2 + AX + BY + C = 0$ or $Y^2 + AX + BY + C = 0$. This follows from Equation (18), as the only monomial of degree 4 in $F(X, Y)$ is X^2Y^2.

- **Step 1: $\mathcal{Q}$ has not linear components.**

  If $\mathcal{Q}$ has a linear component, say L_1 since it is either of type $X - A = 0$ or $Y - B = 0$, we get that either $F(A, Y)$ or $F(X, B)$ should be identically zero for some A and B. These two cases has been analyzed using MAGMA and the code called *C1* attached in Appendix 6. In any case a contradiction is obtained by proving that the coefficients of $F(A, Y)$ (resp. $F(X, B)$) with respect to Y (resp. X) cannot vanish at the same time, unless $\alpha^q/\beta^{q+1} \in \mathbb{F}_q$.

- **Step 2: $\mathcal{Q}$ is not the product of two irreducible quadrics.**

  Nore first that $(X^2 + AX + BY + C)(Y^2 + DX + EY + F)$ cannot be a factorization of $F(X, Y)$. This is true because the coefficients of X^3 and Y^3 in $F(X, Y)$ are zero, implying that $D = B = 0$ and hence that the two quadrics are reducible. Hence the only case to analyze is the one in which a factorization of $F(X, Y)$ is given by a product of type

  $$(XY + AX + BY + C)(XY + DX + EY + F),$$

  up to multiply by the coefficient of X^2Y^2 in $F(X, Y)$. Also this case has been analyzed using MAGMA, code *C2* in the appendix and in any case a contradiction to $\alpha^q/\beta^{q+1} \notin \mathbb{F}_q$ is obtained.

□

5 On the equivalence of $L_{\alpha,\beta}$ with known linear sets in $\mathrm{PG}(1, q^5)$

According to [5, Proposition 5.1 and Theorem 5.4] the maximum scattered $\mathbb{F}_q$-linear set $L_{\alpha,\beta}$ is equivalent to some L_s^η (see Sect. 1 for its definition) if

and only if there exist $A, B, C, D, \lambda \in \mathbb{F}_{q^5}$ with $AD - BC \neq 0$, $\lambda \neq 0$ and τ automorphism of $\mathbb{F}_{q^5}$ such that

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x^\tau - \alpha^\tau x^{q^2\tau} \\ x^{q\tau} - \beta^\tau x^{q^2\tau} \end{pmatrix} = \begin{pmatrix} z \\ f_{s,\eta}(\lambda z) \end{pmatrix} \tag{19}$$

eq

where $f_{s,\eta}(z) = \eta z^{q^s} + z^{q^{5-s}}$. We note that it is sufficient to consider the case $\lambda = 1$ as

$$\begin{pmatrix} z \\ f_{s,\eta}(\lambda z) \end{pmatrix} = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ f_{s,\eta}(x) \end{pmatrix},$$

with $z = \lambda^{-1}x$. We first deal with the case $s = 1$. Then defining $y = x^\tau$, Equation (19) reads

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} y - \alpha^\tau y^{q^2} \\ y^q - \beta^\tau y^{q^2} \end{pmatrix} = \begin{pmatrix} z \\ \eta z^q + z^{q^4} \end{pmatrix}.$$

Hence,

$$\begin{cases} A = 0, \\ \beta^{\tau q} B^q \eta = 0, \\ C\alpha^\tau + D\beta^\tau = -\eta B^q, \\ D = -\beta^{q^4\tau} B^{q^4}, \\ C = B^{q^4}. \end{cases} \tag{20}$$

eqLP

As stated in Section 2, if $\beta = 0$ then $L_{\alpha,\beta}$ is equivalent to L_1^η. If $\beta \neq 0$ then from Equation (20) $B = 0 = A$, which is not possible. The following lemma is now proved.

equivLP

Lemma 5.1. *Let $L_{\alpha,\beta}$ be maximum scattered. Then $L_{\alpha,\beta}$ is equivalent to L_1^η for some $\eta \in \mathbb{F}_{q^5}$ wih $N(\eta) \neq 1$ if and only if $\beta = 0$ and $N(\alpha) \neq -1$.*

We now analyze the case $s = 2$. If

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x^\tau - \alpha^\tau x^{q^2\tau} \\ x^{q\tau} - \beta^\tau x^{q^2\tau} \end{pmatrix} = \begin{pmatrix} z \\ \eta z^{q^2} + z^{q^3} \end{pmatrix},$$

then

$$\begin{cases} C = -A^{q^3}\alpha^{q^3\tau} - B^{q^3}\beta^{q^3\tau}, \\ D = 0, \\ \eta A^{q^2} + C\alpha^\tau = 0, \\ A^{q^3} + \eta B^{q^2} = 0, \\ B^{q^3} - \eta[A^{q^2}\alpha^{q^2\tau} + B^{q^2}\beta^{q^2\tau}] = 0. \end{cases} \tag{21}$$

eqS

Define $A^{q^3} = -\eta B^{q^2}$ so that $A^{q^2} = -\eta^{q^4} B^q$. Since $\alpha = 0$ would imply the contradiction $A = B = 0$, we can also define $C = -(\eta A^{q^2})/\alpha^\tau = (\eta^{q^4+1} B^q)/\alpha^\tau$. At this point (21) reads

$$\begin{cases} \eta^{q^4+1} B^q - \eta B^{q^2} \alpha^{(q^3+1)\tau} + \alpha^\tau \beta^{q^3\tau} B^{q^3} = 0, \\ B^{q^3} + \eta^{q^4+1} \alpha^{q^2\tau} B^q - \eta B^{q^2} \beta^{q^2\tau} = 0, \end{cases}$$

which is equivalent to require that the polynomials

$$\begin{cases} P_1(B) := B^{q^2} - \eta^{q^4} \beta^{q\tau} B^q + \eta^{q^4+q^3} \alpha^\tau B = 0, \\ P_2(B) := \alpha^{q^4\tau} \beta^{q^2\tau} B^{q^2} - \eta^{q^4} \alpha^{(q^4+q^2)\tau} B^q + \eta^{q^4+q^3} B = 0, \end{cases} \tag{22}$$ eqS2

have at least one common root $B \in \mathbb{F}_{q^5}^*$. Since $\alpha, \beta \neq 0$, (22) is equivalent to

$$\begin{cases} \beta^{q^2\tau} \alpha^{q^4\tau} P_1(B) - P_2(B) = 0, \\ P_2(B) = 0. \end{cases} \tag{23}$$ eqS21

Since $\beta^{q+1} \neq \alpha^q$ as otherwise $L_{\alpha,\beta}$ is of pseudoregulus type, (23) reads

$$\begin{cases} \alpha^{q^4\tau} \beta^{q^2\tau} B^{q^2} - \eta^{q^4} \alpha^{(q^4+q^2)\tau} B^q + \eta^{q^4+q^3} B = 0, \\ -B^q + \frac{\eta^{q^3} (\beta^{q^2\tau} \alpha^{(q^4+q)\tau} - 1)}{\alpha^{q^4\tau} (\beta^{(q+1)\tau} - \alpha^{q\tau})^q} B = 0. \end{cases}$$

Since in general $-B^q + kB = 0$, $B \neq 0$ implies $N(k) = 1$, we obtain

$$\begin{cases} \alpha^{q^4\tau} \beta^{q^2\tau} B^{q^2} - \eta^{q^4} \alpha^{(q^4+q^2)\tau} B^q + \eta^{q^4+q^3} B = 0, \\ -B^q + \frac{\eta^{q^3} (\beta^{q^2\tau} \alpha^{(q^4+q)\tau} - 1)}{\alpha^{q^4\tau} (\beta^{(q+1)\tau} - \alpha^{q\tau})^q} B = 0, \\ N\left(\frac{\eta^{q^2} (\beta^{q\tau} \alpha^{(q^3+1)\tau} - 1)}{\alpha^{q^3\tau} (\beta^{(q+1)\tau} - \alpha^{q\tau})} \right) = 1. \end{cases} \tag{24}$$ eqS22

Hence we write

$$\eta^{q^2} = \lambda \left(\frac{\alpha^{q^3} (\beta^{(q+1)} - \alpha^q)}{\beta^q \alpha^{q^3+1} - 1} \right)^\tau$$

where $N(\lambda) = 1$, so that $B^q = \lambda^q B$. Substituting in P_2 and recalling that $B \neq 0$ we get

$$\alpha^{q^4\tau} \beta^{q^2\tau} \lambda^{q^2+q} - \eta^{q^4} \alpha^{(q^4+q^2)\tau} \lambda^q + \eta^{q^4+q^3} = 0$$

and taking the q^4-power and dividing by λ^{q+1}

$$\alpha^{q^3\tau}\beta^{q\tau} - \left(\frac{\alpha^{q^3}(\beta^{(q+1)} - \alpha^q)}{\beta^q\alpha^{q^3+1} - 1}\right)^{q\tau} \alpha^{(q^3+q)\tau} + \left(\frac{\alpha^{q^3}(\beta^{(q+1)} - \alpha^q)}{\beta^q\alpha^{q^3+1} - 1}\right)^{(q+1)\tau} = 0,$$

which is equivalent to

$$\alpha^{q^4}\beta^{q^2+q+1} - \alpha^{q^4+q^2}\beta - \alpha^{q^4+q}\beta^{q^2} + N(\alpha) - \beta^q\alpha^{q^3+1} + 1 = 0. \qquad (25) \quad \boxed{\texttt{condSh}}$$

Furthermore if the previous condition is satisfied, recalling our definition of η, then $L_{\alpha,\beta}$ is maximum scattered if and only if

$$N\left(\frac{\alpha^{q^3}(\beta^{(q+1)} - \alpha^q)}{\beta^q\alpha^{q^3+1} - 1}\right) \neq 1.$$

This proves the following lemma.

$\boxed{\texttt{equivSh}}$ **Lemma 5.2.** *A linear set $L_{\alpha,\beta}$ is equivalent to L_2^η for some $\eta \in \mathbb{F}_{q^5}$ if and only if Equation* (25) *is satisfied.*

If this is the case then $L_{\alpha,\beta}$ is maximum scattered if and only if

$$N\left(\frac{\alpha^{q^3}(\beta^{(q+1)} - \alpha^q)}{\beta^q\alpha^{q^3+1} - 1}\right) \neq 1.$$

Remark 5.3. It can be checked with MAGMA or GAP that using Lemmas 5.1 and 5.2 then no new maximum scattered linear sets of type $L_{\alpha,\beta}$ can be obtained for $q \leq 11$.

From $N(\alpha) + 1 \in \mathbb{F}_q$, we note that a necessary condition for Equation (25) to hold is that

$$\alpha^{q^4}\beta^{q^2+q+1} - \alpha^{q^4+q^2}\beta - \alpha^{q^4+q}\beta^{q^2} - \beta^q\alpha^{q^3+1} = \alpha\beta^{q^3+q^2+q} - \alpha^{q^3+1}\beta^q - \alpha^{q^2+1}\beta^{q^3} - \beta^{q^2}\alpha^{q^4+q},$$

which is equivalent to

$$\alpha^{q^4}\beta(\beta^{q^2+q} - \alpha^{q^2}) = \alpha\beta^{q^3}(\beta^{q^2+q} - \alpha^{q^2}).$$

Since $\beta^{q+1} \neq \alpha^q$ from Lemma 2.5 we get $\alpha^{q^4}\beta - \alpha\beta^{q^3} = 0$ and hence

$$\alpha^q/\beta^{q+1} \in \mathbb{F}_q^*. \qquad (26) \quad \boxed{\texttt{sh1}}$$

Hence let $\alpha^q/\beta^{q+1} = \lambda \in \mathbb{F}_q^*$. In this case Equation (25) reads

$$\lambda^5 N(\beta)^2 + \lambda(1 - 3\lambda)N(\beta) + 1 = 0. \qquad (27) \quad \boxed{\texttt{sh2}}$$

Thus, from Lemma 5.2 if α and β satisfy (26) and (27) $L_{\alpha,\beta}$ is equivalent to L_2^η with $\eta = \alpha^{q^3}(\beta^{(q+1)} - \alpha^q)/(\beta^q\alpha^{q^3+1} - 1)$. It follows that $L_{\alpha,\beta}$ is maximum scattered if and only if

$$N(\eta) = N\left(\frac{\alpha^{q^3}(\beta^{(q+1)} - \alpha^q)}{\beta^q\alpha^{q^3+1} - 1}\right) = N\left(\frac{\lambda\beta^{q^3+q^2}(\beta^{q+1} - \lambda\beta^{q+1})}{\beta^q\lambda^2\beta^{q^4+q^3+q^2+1} - 1}\right) =$$

$$N(\beta)^4 \cdot N\left(\frac{\lambda(1-\lambda)}{\lambda^2 N(\beta) - 1}\right) \neq 1.$$

Since $\lambda \in \mathbb{F}_q^*$ we get that equivalently

$$\lambda^5(1-\lambda)^5 N(\beta)^4 \neq (\lambda^2 N(\beta) - 1)^5. \tag{28}$$ ms

Computing the resultant of the polynomials $\lambda^5(1-\lambda)^5Y^4 - (\lambda^2 Y - 1)^5$ and $\lambda^5 Y^2 + \lambda(1-3\lambda)Y + 1$ with respect to Y we get $\lambda^{14}(\lambda-1)^{10}$. Hence if $\lambda^5(1-\lambda)^5 N_{q^5/q}(\beta)^4 = (\lambda^2 N_{q^5/q}(\beta) - 1)^5$ then either $\lambda = 0$ or $\lambda = 1$. If $\lambda = 0$ then $\alpha = 0$, contradicting (25). If $\lambda = 1$ then $L_{\alpha,\beta}$ is of pseudoregulus type, a contradiction.

Thus the following remark holds.

remSh **Remark 5.4.** A linear set of type $L_{\alpha,\beta}$ is equivalent to L_2^η if and only if $\alpha^q/\beta^{q+1} = \lambda \in \mathbb{F}_q^* \setminus \{1\}$ and Equation (27) holds. If it is the case then $L_{\alpha,\beta}$ is maximum scattered.

Summarizing, the following theorem collects all the possibile equivalences of maximum scattered linear sets of type $L_{\alpha,\beta}$ and known linear sets.

equivAll **Theorem 5.5.** *Let $L_{\alpha,\beta}$ be scattered, $\alpha\beta \neq 0$, $\alpha^q \neq \beta^{q+1}$. Then*

- $\lambda = \alpha^q/\beta^{q+1} \in \mathbb{F}_q$*;*
- *$L_{\alpha,\beta}$ is equivalent (up to collineations) neither to L_1^η for any η, nor to a linear set of pseudoregulus type;*
- *$L_{\alpha,\beta}$ is equivalent to the Sheekey linear set L_2^η for some η if and only if $\lambda^5 \mathrm{N}_{q^5/q}(\beta)^2 + \lambda(1-3\lambda)\mathrm{N}_{q^5/q}(\beta) + 1 = 0$; so,*
- *if $\lambda^5 \mathrm{N}_{q^5/q}(\beta)^2 + \lambda(1-3\lambda)\mathrm{N}_{q^5/q}(\beta) + 1 \neq 0$, then $L_{\alpha,\beta}$ is of a new type; this does not occur for $q \leq 11$.*

Remark 5.6. Even though every maximum scattered linear set either of pseudoregulus type or of Lunardon-Polverino type is $L_{\alpha,\beta}$ for some $\alpha, \beta \in$

$\mathbb{F}_{q^5}$, the same statement is not true in general for Sheekey linear sets L_2^η with $N(\eta) \neq 1$.

Indeed let $\eta \in \mathbb{F}_{q^5}^*$ such that $N(\eta)^2 - N(\eta) + 1 = 0$. This implies that $q \not\equiv 2 \pmod 3$. From Theorem 5.5 we want to show that there are no $\lambda \in \mathbb{F}_q^* \setminus \{1\}$ and $\beta \in \mathbb{F}_{q^5}^*$ such that

$$\begin{cases} \eta = \frac{\lambda\beta^{q^3+q^2}(\beta^{q+1}-\lambda\beta^{q+1})}{\beta^q\lambda^2\beta^{q^4+q^3+q^2+1}-1}, \\ \lambda^5 N(\beta)^2 + \lambda(1-3\lambda)N(\beta) + 1 = 0. \end{cases}$$

Suppose by contradiction that $\eta = \frac{\lambda\beta^{q^3+q^2}(\beta^{q+1}-\lambda\beta^{q+1})}{\beta^q\lambda^2\beta^{q^4+q^3+q^2+1}-1}$ and $\lambda^5 N(\beta)^2 + \lambda(1-3\lambda)N(\beta) + 1 = 0$. Then as in Equation (28), we have that

$$N(\eta) = N(\beta)^4 \cdot N_{q^5/q}\left(\frac{\lambda(1-\lambda)}{\lambda^2 N(\beta) - 1}\right) = N(\beta)^4 \frac{\lambda^5(1-\lambda)^5}{((\lambda^2 N(\beta) - 1)^5}$$

and hence $N(\eta)^2 - N(\eta) + 1 = 0$ implies

$$N(\beta)^8\lambda^{10}(1-\lambda)^{10} - N(\beta)^4\lambda^5(1-\lambda)^5(\lambda^2 N(\beta) - 1)^5 + (\lambda^2 N(\beta) - 1)^{10} = 0.$$

Since the resultant of the polynomials $P_1(\lambda, N) = N^8\lambda^{10}(1-\lambda)^{10} - N^4\lambda^5(1-\lambda)^5(\lambda^2 N - 1)^5 + (\lambda^2 N - 1)^{10}$ and $P_2(\lambda, N) = \lambda^5 N^2 + \lambda(1-3\lambda)N + 1$ with respect to N is $\lambda^{28}(\lambda-1)^{22}$ and $\lambda \in \mathbb{F}_q^* \setminus \{1\}$ we have a contradiction. From Proposition 2.2 the cases $N(\eta)^2 - N(\eta) + 1 = 0$ are exactly those for which $\Lambda \cap \Lambda^\sigma$ has not height four. This explicit construction is hence consistent with Proposition 2.4.

We end this section with the following question.

Question 5.7. It has been proven in Proposition 4.3 that for $\beta \neq 0$, $\alpha^q/\beta^{q+1} \in \mathbb{F}_q$ is a necessary condition for $L_{\alpha,\beta}$ to be maximum scattered. From Lemma 5.1, $L_{\alpha,\beta}$ is equivalent to L_1^η for some η with $N(\eta) \neq 1$ if and only if $\beta = 0$, while if $\alpha^q/\beta^{q+1} = 1$ then $L_{\alpha,\beta}$ is of pseudoregulus type. From Remark 5.4 $L_{\alpha,\beta}$ is equivalent to $L_{2,\eta}$ for some η with $N(\eta) \neq 1$ if and only if $\lambda = \alpha^q/\beta^{q+1} \in \mathbb{F}_q^* \setminus \{1\}$ and (27) holds. Is it true that $L_{\alpha,\beta}$ with $\alpha^q/\beta^{q+1} \in \mathbb{F}_q^* \setminus \{1\}$ is maximum scattered if and only if it is equivalent to L_2^η for some $N(\eta) \neq 1$? If the answer to this question is negative then the family of $L_{\alpha,\beta}$ contains new maximum scattered linear sets. Otherwise, it would provide a new characterization of the known maximum scattered linear sets in $\mathrm{PG}(1, q^5)$.

References

[1] D. Bartoli - M. Giulietti - G. Marino - O. Polverino: Maximum scattered linear sets and complete caps in Galois spaces. Combinatorica 38 (2018), 255–278.

[2] D. Bartoli - Y. Zhou: Exceptional scattered polynomials. J. Algebra 509 (2018), 507–534.

[3] A. Blokhuis - M. Lavrauw: Scattered spaces with respect to a spread in PG(n, q). Geom. Dedicata 81 (2000), 231–243.

[4] G. Bonoli - O. Polverino: $\mathbb{F}_q$-linear blocking sets in PG$(2, q^4)$. Innov. Incidence Geom. 2 (2005), 35–56.

[5] B. Csajbók - G. Marino - O. Polverino: A Carlitz type result for linearized polynomials. Ars Math. Contemp. 16 (2019), 585–608.

[6] B. Csajbók - G. Marino - O. Polverino: Classes and equivalence of linear sets in PG$(1, q^n)$. J. Combin. Theory Ser. A 157 (2018), 402–426.

[7] B. Csajbók - G. Marino - O. Polverino - F. Zullo: A characterization of linearized polynomials with maximum kernel. Finite Fields Appl. 56 (2019), 109–130.

[8] B. Csajbók - C. Zanella: On the equivalence of linear sets. Des. Codes Cryptogr. 81 (2016), 269–281.

[9] B. Csajbók - C. Zanella: On scattered linear sets of pseudoregulus type in PG$(1, q^t)$. Finite Fields Appl. 41 (2016), 34–54.

[10] B. Csajbók - C. Zanella: Maximum scattered $\mathbb{F}_q$-linear sets of PG$(1, q^4)$. Discrete Math. 341 (2018), 74–80.

[11] M. Lavrauw - G. Van de Voorde: On linear sets on a projective line. Des. Codes Cryptogr. 56 (2010), 89–104.

[12] R. Lidl - H. Niederreiter: Finite fields. Vol. 20. Cambridge university press, 1997.

[13] G. Lunardon - O. Polverino: Blocking sets and derivable partial spreads. J. Algebraic Combin. 14 (2001), 49–56.

[14] G. Lunardon - O. Polverino: Translation ovoids of orthogonal polar spaces. Forum Math. 16 (2004), 663–669.

[15] G. Lunardon- R. Trombetti - Y. Zhou: Generalized Twisted Gabidulin Codes. J. Combin. Theory Ser. A 159 (2018), 79–106.

[16] J. Sheekey: A new family of linear maximum rank distance codes. Adv. Math. Commun. 10 (3) (2016) 475–488.

[17] K. Slavov: An application of random plane slicing to counting $\mathbb{F}_q$-points on hypersurfaces. Finite Fields Appl. 48 (2017), 60–67.

Maria Montanucci
Technical University of Denmark
Asmussens Allé
Building 303B, room 150
2800 Kgs. Lyngby
Denmark

Corrado Zanella
Dipartimento di Tecnica e Gestione dei Sistemi Industriali
Università degli Studi di Padova
Stradella S. Nicola, 3
36100 Vicenza VI
Italy

6 Appendix: MAGMA code for Proposition 4.3

appendix

In the MAGMA codes C1 and C2 the following notation has been used: $a := \alpha$ and $b := \beta$. For all $i = 1, \ldots, 4$, ai (resp. bi) denotes α^{q^i} (resp. β^{q^i}).

6.1 The code C1

```
K<X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,C,D,E,F> := PolynomialRing(Integers(), 18);

Q:=X^2*Y^2*b*b1*b2*a2*a3^2*a4 - X^2*Y^2*b*a2^2*a3^2*a4 - X^2*Y^2*b1*b2^2*b3*a3 +
    X^2*Y^2*b2*b3*a2*a3 + X^2*Y*b*b1*b2*b3*b4*a2*a3 - 2*X^2*Y*b*b1*b2*a2*a3*a4 -
    X^2*Y*b*b3*b4*a2^2*a3 + 2*X^2*Y*b*a2^2*a3*a4 + X^2*Y*b1*b2^2*b3 -
    X^2*Y*b2*b3*a2 - X^2*b*b1*b2*b3*b4*a2 + X^2*b*b1*b2*a2*a4 + X^2*b*b3*b4*a2^2
    - X^2*b*a2^2*a4 + X*Y^2*b*b1*b2^2*b3*a3*a4 - X*Y^2*b*b1*b2*a3^2*a4 -
    2*X*Y^2*b*b2*b3*a2*a3*a4 + 2*X*Y^2*b*a2*a3^2*a4 + X*Y^2*b2^2*b3^2 -
```

```
    X*Y^2*b2*b3*a3 + X*Y*b*b1*b2^2*b3^2*b4 - X*Y*b*b1*b2^2*b3*a4 -
    X*Y*b*b1*b2*b3*b4*a3 + 2*X*Y*b*b1*b2*a3*a4 - X*Y*b*b2*b3^2*b4*a2 +
    2*X*Y*b*b2*b3*a2*a4 + 2*X*Y*b*b3*b4*a2*a3 - 4*X*Y*b*a2*a3*a4 -
    X*Y*b1*b2^2*b3^2*a - X*Y*b2^2*b3^2*b4*a1 + X*Y*b2*b3*a*a1*a2*a3*a4 +
    X*Y*b2*b3 + X*b*b1*b2*b3*b4 - X*b*b1*b2*a4 - 2*X*b*b3*b4*a2 + 2*X*b*a2*a4 +
    X*b2*b3^2*b4*a*a1*a2 - X*b2*b3*a*a1*a2*a4 - Y^2*b*b2^2*b3^2*a4 +
    2*Y^2*b*b2*b3*a3*a4 - Y^2*b*a3^2*a4 + Y*b*b2*b3^2*b4 - 2*Y*b*b2*b3*a4 -
    Y*b*b3*b4*a3 + 2*Y*b*a3*a4 + Y*b2^2*b3^2*a*a1*a4 - Y*b2*b3*a*a1*a3*a4 +
    b*b3*b4 - b*a4 - b2*b3^2*b4*a*a1 + b2*b3*a*a1*a4;


//SUBCASE 1: L1 is the line X-A=0;

pol:=Evaluate(Q,[A,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,C,D,E,F]);
//{Factorization(Coefficients(pol,Y)[i]): i in [1..#Coefficients(pol,Y)]};

//    1:      <a2*A - 1, 1>,
//    2:      <b3*b4 - a4, 1>, cannot occur
//    3:      <b*b1*b2*A - b*a2*A + b - b2*b3*a*a1, 1>

//Analysis of 1:

pol1:=Numerator(Evaluate(Q,[1/a2,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,C,D,E,F]));
//{Factorization(Coefficients(pol1,Y)[i]): i in [1..#Coefficients(pol1,Y)]
| Coefficients(pol1,Y)[i] ne 0};

//         <b3, 1>,
//         <b2, 2>,
//         <b1*a3 - b3*a2, 1>,
//         <b*a2*a4 - 1, 1>

//in any case a1/(b1*b) is in Fq, contradiction;

//Analysis of 3:

pol2:=Numerator(Evaluate(Q,[-(b - b2*b3*a*a1)/(b*b1*b2 - b*a2),Y,b,b1,b2,b3,b4,
a,a1,a2,a3,a4,A,B,C,D,E,F]));
//{Factorization(Coefficients(pol2,Y)[i]): i in [1..#Coefficients(pol2,Y)] |
 Coefficients(pol2,Y)[i] ne 0};

//         <b3, 1>, cannot occur
//         <b2, 2>, cannot occur
//         <b - a*a1*a3, 1>, cannot occur
//         <b^2*b1*b2*b3*a4 - b^2*b1*a3*a4 - b^2*b3*a2*a4 + b*b3*a*a1*a2*a3*a4 +
//             b*b3 - b2*b3^2*a*a1, 1>

new:=b^2*b1*b2*b3*a4 - b^2*b1*a3*a4 - b^2*b3*a2*a4 + b*b3*a*a1*a2*a3*a4 + b*b3
 - b2*b3^2*a*a1;
pol3:=Resultant(pol2,new,a3);
```

```
//{Factorization(Coefficients(pol3,Y)[i]): i in [1..#Coefficients(pol3,Y)] |
Coefficients(pol3,Y)[i] ne 0};

//        <a4, 1>,
//        <b3, 1>,
//        <b2, 2>,
//        <b, 2>,
//        <b - b2*b3*a*a1, 1>,
//        <b*a4 - b3*a, 1>,
//        <b*b1 - b3*a*a1*a2, 2>,
//        <b*b1*a4 - b3*b4*a1, 1>

//in any case a contradiction is obtained;



//SUBCASE 2: L1 is the line Y-B=0;


pol:=Evaluate(Q,[X,B,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,C,D,E,F]);
//{Factorization(Coefficients(pol,X)[i]): i in [1..#Coefficients(pol,X)]};

//1:        <a3*B - 1, 1>,
//2:        <b1*b2 - a2, 1>, cannot occur
//3:        <b*b3*b4*a2 + b*a2*a3*a4*B - b*a2*a4 - b2*b3*B, 1>

//Analysis of 1:

pol1:=Numerator(Evaluate(Q,[X,1/a3,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,C,D,E,F]));
//{Factorization(Coefficients(pol1,X)[i]): i in [1..#Coefficients(pol1,X)] |
Coefficients(pol1,X)[i] ne 0};

//        <b3, 2>,
//        <b2, 1>,
//        <b2*a4 - b4*a3, 1>,
//       <b - a*a1*a3, 1>

//in any case a contradiction is obtained;

//Analysis of 3:

pol2:=Numerator(Evaluate(Q,[X,-(b*b3*b4*a2- b*a2*a4)/(b*a2*a3*a4- b2*b3),b,b1,
b2,b3,b4,a,a1,a2,a3,a4,A,B,C,D,E,F]));
//{Factorization(Coefficients(pol2,X)[i]): i in [1..#Coefficients(pol2,X)] |
 Coefficients(pol2,X)[i] ne 0};

//        <b3, 2>, cannot occur
//        <b3*b4 - a4, 1>, cannot occur
//        <b2, 1>, cannot occur
```

```
//         <b*a2*a4 - 1, 1>, cannot occur
//         <b^2*b2*b3*b4*a2 - b^2*b2*a2*a4 - b^2*b4*a2*a3 + b*b2*a*a1*a2*a3*a4 +
//             b*b2 - b2^2*b3*a*a1, 1>

new:=b^2*b2*b3*b4*a2 - b^2*b2*a2*a4 - b^2*b4*a2*a3 + b*b2*a*a1*a2*a3*a4
+b*b2 - b2^2*b3*a*a1;
pol3:=Resultant(pol2,new,a3);
{Factorization(Coefficients(pol3,X)[i]): i in [1..#Coefficients(pol3,X)] |
 Coefficients(pol3,X)[i] ne 0};

//         <a2, 1>,
//         <b3, 2>,
//         <b3*b4 - a4, 2>,
//         <b2, 2>,
//         <b, 2>,
//         <b*a2 - b2*a1, 1>,
//         <b*a2*a4 - 1, 1>,
//         <b*b4*a2 - b1*b2*a, 1>

//a contradiction is obtained in any case;
```

6.2 The code C2

```
Q:=X^2*Y^2*b*b1*b2*a2*a3^2*a4 - X^2*Y^2*b*a2^2*a3^2*a4 - X^2*Y^2*b1*b2^2*b3*a3 +
    X^2*Y^2*b2*b3*a2*a3 + X^2*Y*b*b1*b2*b3*b4*a2*a3 - 2*X^2*Y*b*b1*b2*a2*a3*a4 -
    X^2*Y*b*b3*b4*a2^2*a3 + 2*X^2*Y*b*a2^2*a3*a4 + X^2*Y*b1*b2^2*b3 -
    X^2*Y*b2*b3*a2 - X^2*b*b1*b2*b3*b4*a2 + X^2*b*b1*b2*a2*a4 + X^2*b*b3*b4*a2^2
    - X^2*b*a2^2*a4 + X*Y^2*b*b1*b2^2*b3*a3*a4 - X*Y^2*b*b1*b2*a3^2*a4 -
    2*X*Y^2*b*b2*b3*a2*a3*a4 + 2*X*Y^2*b*a2*a3^2*a4 + X*Y^2*b2^2*b3^2 -
    X*Y^2*b2*b3*a3 + X*Y*b*b1*b2^2*b3^2*b4 - X*Y*b*b1*b2^2*b3*a4 -
    X*Y*b*b1*b2*b3*b4*a3 + 2*X*Y*b*b1*b2*a3*a4 - X*Y*b*b2*b3^2*b4*a2 +
    2*X*Y*b*b2*b3*a2*a4 + 2*X*Y*b*b3*b4*a2*a3 - 4*X*Y*b*a2*a3*a4 -
    X*Y*b1*b2^2*b3^2*a - X*Y*b2^2*b3^2*b4*a1 + X*Y*b2*b3*a*a1*a2*a3*a4 +
    X*Y*b2*b3 + X*b*b1*b2*b3*b4 - X*b*b1*b2*a4 - 2*X*b*b3*b4*a2 + 2*X*b*a2*a4 +
    X*b2*b3^2*b4*a*a1*a2 - X*b2*b3*a*a1*a2*a4 - Y^2*b*b2^2*b3^2*a4 +
    2*Y^2*b*b2*b3*a3*a4 - Y^2*b*a3^2*a4 + Y*b*b2*b3^2*b4 - 2*Y*b*b2*b3*a4 -
    Y*b*b3*b4*a3 + 2*Y*b*a3*a4 + Y*b2^2*b3^2*a*a1*a4 - Y*b2*b3*a*a1*a3*a4 +
    b*b3*b4 - b*a4 - b2*b3^2*b4*a*a1 + b2*b3*a*a1*a4;

//leading coefficient of Q;
lc:=b*b1*b2*a2*a3^2*a4 - b*a2^2*a3^2*a4 - b1*b2^2*b3*a3 +b2*b3*a2*a3;

FACT:=lc*(X*Y+A*X+B*Y+C)*(X*Y+D*X+E*Y+F);

pol:=Q-FACT;
SET:={};
for t in Coefficients(pol,X) do
for l in Coefficients(t,Y) do
```

```
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
//SET;

//FROM SET the following two conditions need to be satisfied at the same time;

COND1:=b*b3*b4*a2 + b*a2*a3^2*a4*A*D - b*a2*a4 - b2*b3*a3*A*D;

COND2:=b*b3*b4*a2*a3 - b*a2*a3^2*a4*A - b*a2*a3^2*a4*D - 2*b*a2*a3*a4 +
            b2*b3*a3*A + b2*b3*a3*D + b2*b3;

//Note that the resultant can be computed as
//the coefficient of D in COND1 cannot be zero;

//Factorization(Resultant(COND1,COND2,D));

//[
//    <a3, 1>, not possible;
// 1:     <a3*A + 1, 1>,
//    <b*a2*a3*a4 - b2*b3, 1>, not possible;
// 2:    <b*b3*b4*a2 - b*a2*a3*a4*A - b*a2*a4 + b2*b3*A, 1>

//CASES 1 and 2 will be analyzed separately;

////////////////////////////////////////////
//ANALYSIS OF CASE 1;

//Factorization(Numerator(Evaluate(COND1,[X,Y,b,b1,b2,b3,b4,a,
a1,a2,a3,a4,-1/a3,B,C,D,E,F])));

//  <b*b3*b4*a2 - b*a2*a3*a4*D - b*a2*a4 + b2*b3*D, 1>

pol1:=Numerator(Evaluate(pol,[X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,-1/a3,B,
C,-(b*b3*b4*a2-b*a2*a4)/(- b*a2*a3*a4+ b2*b3),E,F]));
SET:={};
for t in Coefficients(pol1,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
//SET;
//we get that the following 2 conditions need to be satisfied at the same time;

COND3:=b*b1*b2*a2*a3^2*a4*B*E + b*b2^2*b3^2*a4 - 2*b*b2*b3*a3*a4 -
```

```
            b*a2^2*a3^2*a4*B*E + b*a3^2*a4 - b1*b2^2*b3*a3*B*E +
            b2*b3*a2*a3*B*E;

COND4:=b*b1*b2^2*b3*a3*a4 - b*b1*b2*a2*a3^2*a4*B - b*b1*b2*a2*a3^2*a4*E -
            b*b1*b2*a3^2*a4 - 2*b*b2*b3*a2*a3*a4 + b*a2^2*a3^2*a4*B +
            b*a2^2*a3^2*a4*E + 2*b*a2*a3^2*a4 + b1*b2^2*b3*a3*B +
            b1*b2^2*b3*a3*E + b2^2*b3^2 - b2*b3*a2*a3*B - b2*b3*a2*a3*E -
            b2*b3*a3;

//Factorization(Resultant(COND3,COND4,E));

//we have two subcases that we will analyze separately;

//1.A: b1*b2*a3*B + b2*b3 - a2*a3*B - a3=0
// 1.B: b*b2*b3*a4 - b*a2*a3*a4*B - b*a3*a4 + b2*b3*B=0

////////////////////////////////////////////////
//The subcase 1.A;

//Factorization(Resultant(COND3, b1*b2*a3*B + b2*b3 - a2*a3*B - a3,B));

//b*b2*b3*a4 - b*a2*a3*a4*E - b*a3*a4 + b2*b3*E=0

pol2:=Numerator(Evaluate(pol1,[X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,
-(b2*b3- a3)/(b1*b2*a3- a2*a3),C,D,-(b*b2*b3*a4- b*a3*a4)/(- b*a2*a3*a4+ b2*b3),F]));
SET:={};
for t in Coefficients(pol2,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
//SET;

//b*b1*b2*a3*a4*C - b*b3*b4 - b*a2*a3*a4*C - b*a2*a3*a4*F
//+ 2*b*a4 -b2*b3*a*a1*a4 + b2*b3*F=0

pol2:=Numerator(Evaluate(pol2,[X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,
-(- b*a2*a3*a4*F + 2*b*a4 -b2*b3*a*a1*a4 + b2*b3*F- b*b3*b4 )
/(b*b1*b2*a3*a4- b*a2*a3*a4),D,E,F]));
SET:={};
for t in Coefficients(pol2,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
```

```
//SET;

//b*b3*b4 + b*a2*a3*a4*F - b*a4 - b2*b3*F

pol2:=Numerator(Evaluate(pol2,[X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,C,D,
E,-(b*b3*b4- b*a4)/(b*a2*a3*a4- b2*b3)]));
SET:={};
for t in Coefficients(pol2,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
//SET;

//    [
//        <a4, 1>,
//        <b3, 2>,
//        <b2, 2>,
//        <b*b4 - a, 1>,
//        <b*b1 - a1, 1>
//    ]
//a contradiction;

////////////////////////////////////////////////
//The subcase 1.B;

//Factorization(Resultant(COND3,b*b2*b3*a4 - b*a2*a3*a4*B - b*a3*a4 + b2*b3*B,B));

//b1*b2*a3*E + b2*b3 - a2*a3*E - a3

pol2:=Numerator(Evaluate(pol1,[X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,
-(b*b2*b3*a4- b*a3*a4)/(- b*a2*a3*a4+ b2*b3),C,D,-(b2*b3- a3)/(b1*b2*a3- a2*a3),F]));
SET:={};
for t in Coefficients(pol2,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
//SET;

//  b*b1*b2*a3*a4*F - b*b3*b4 - b*a2*a3*a4*C - b*a2*a3*a4*F
// + 2*b*a4 -b2*b3*a*a1*a4 + b2*b3*C=0

pol2:=Numerator(Evaluate(pol2,[X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,A,B,
-(b*b1*b2*a3*a4*F - b*b3*b4- b*a2*a3*a4*F + 2*b*a4 -b2*b3*a*a1*a4 )
```

```
/(- b*a2*a3*a4+ b2*b3),D,E,F]));
SET:={};
for t in Coefficients(pol2,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
//SET;

//We have two possibilities: either New1 or New2 is equal to zero, where

New1:=b1*b2*a3*a4*F - b3*b4 - a2*a3*a4*F + a4;
New2:=b*b1*b2*a3*F - b*a2*a3*F + b - b2*b3*a*a1;

pol2:=Resultant(pol2,New1,F);
SET:={};
for t in Coefficients(pol2,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
//SET;

//a contradiction;

//    [
//        <a4, 1>,
//        <a3, 2>,
//        <a*a1*a2*a3*a4 - 1, 1>,
//        <b3, 1>,
//        <b3*b4 - a4, 1>,
//        <b2, 2>,
//        <b1*b2 - a2, 2>,
//        <b*b1*a3*a4 - b3, 1>
//    ]

pol2:=Resultant(pol2,New2,F);
SET:={};
for t in Coefficients(pol2,X) do
for l in Coefficients(t,Y) do
if l ne 0 then
SET:=SET join {Factorization(l)};
end if;
end for;
end for;
```

```
//SET;

//same contradiction;

////////////////////////////////////////////////////////////////////
//ANALYSIS OF CASE 2: b*b3*b4*a2 - b*a2*a3*a4*A - b*a2*a4 + b2*b3*A=0;

Factorization(Numerator(Evaluate(COND1,[X,Y,b,b1,b2,b3,b4,a,a1,a2,a3,a4,
-(b*b3*b4*a2- b*a2*a4)/(- b*a2*a3*a4+ b2*b3),B,C,D,E,F])));

//a3*D + 1=0 is obtained;

//This means that the coefficients A and D are simply replaced in role
//with respect to the strategy proposed in CASE 1;
//The same contradiction is hence obtained by repeating the same steps;
```