Des. Codes Cryptogr. (2016) 81:269–281
DOI 10.1007/s10623-015-0141-z

# On the equivalence of linear sets

**Bence Csajbók**[1] · **Corrado Zanella**[1]

Received: 14 January 2015 / Revised: 26 September 2015 / Accepted: 6 October 2015 /
Published online: 22 October 2015


**Abstract** Let $L$ be a linear set of pseudoregulus type in a line $\ell$ in $\Sigma^* = \mathrm{PG}(t-1, q^t)$, $t = 5$ or $t > 6$. We provide examples of $q$-order canonical subgeometries $\Sigma_1,\ \Sigma_2 \subset \Sigma^*$ such that there is a $(t-3)$-subspace $\Gamma \subset \Sigma^* \setminus (\Sigma_1 \cup \Sigma_2 \cup \ell)$ with the property that for $i = 1, 2$, $L$ is the projection of $\Sigma_i$ from center $\Gamma$ and there exists no collineation $\phi$ of $\Sigma^*$ such that $\Gamma^\phi = \Gamma$ and $\Sigma_1^\phi = \Sigma_2$. Condition (ii) given in Theorem 3 in Lavrauw and Van de Voorde (Des Codes Cryptogr 56:89–104, 2010) states the existence of a collineation between the projecting configurations (each of them consisting of a center and a subgeometry), which give rise by means of projections to two linear sets. It follows from our examples that this condition is not necessary for the equivalence of two linear sets as stated there. We characterize the linear sets for which the condition above is actually necessary.

**Keywords** Linear set · Subgeometry · Finite field · Finite projective space · Collineation

**Mathematics Subject Classification** 51E20

## 1 Introduction

If $V$ is a vector space over the finite field $\mathbb{F}_{q^t}$, then $\mathrm{PG}_{q^t}(V)$ denotes the projective space whose points are the one-dimensional $\mathbb{F}_{q^t}$-subspaces of $V$. If $V$ has dimension $n$ over $\mathbb{F}_{q^t}$, then $\mathrm{PG}_{q^t}(V) = \mathrm{PG}(n-1, q^t)$. For a point set $T \subset \mathrm{PG}(n-1, q^t)$ we denote by $\langle T \rangle$ the projective subspace of $\mathrm{PG}(n-1, q^t)$ spanned by the points in $T$. For $m \mid t$ and a set of

Communicated by M. Lavrauw.

✉ Corrado Zanella
corrado.zanella@unipd.it

Bence Csajbók
csajbok.bence@gmail.com

[1] Dipartimento di Tecnica e Gestione dei Sistemi Industriali, Università di Padova, Stradella S. Nicola, 3, 36100 Vicenza, Italy

elements $S \subset V$ we denote by $\langle S \rangle_{q^m}$ the $\mathbb{F}_{q^m}$-vector subspace of $V$ spanned by the vectors in $S$. For the rest of the paper we assume that $q = p^e$ is a power of the prime $p$.

Let $R = \mathbb{F}_{q^t}^r$. The *field reduction map* [8] $\mathcal{F}_{r,t,q}$ is a map from the points of $\mathrm{PG}_{q^t}(R) = \mathrm{PG}(r-1, q^t)$ to the $(t-1)$-subspaces of $\mathrm{PG}_q(R) = \mathrm{PG}(rt-1, q)$. Let $P = \mathrm{PG}_{q^t}(T)$ be a point of $\mathrm{PG}(r-1, q^t)$, where $T$ is a one-dimensional $\mathbb{F}_{q^t}$-subspace of $R$. Then $\mathcal{F}_{r,t,q}(P) := \mathrm{PG}_q(T)$. As $\dim_{\mathbb{F}_q}(T) = t$, it follows that $\mathcal{F}_{r,t,q}(P)$ is a $(t-1)$-dimensional subspace of $\mathrm{PG}(rt-1, q)$. Denote the point set of $\mathrm{PG}(r-1, q^t)$ by $\mathcal{P}$. Then $\mathcal{F}_{r,t,q}(\mathcal{P})$ is a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$ [13]. Let $S$ be a subspace of $\mathrm{PG}(rt-1, q) = \mathrm{PG}_q(R)$, then

$$\mathcal{B}(S) := \left\{ P \in \mathrm{PG}\left(r-1, q^t\right) : \mathcal{F}_{r,t,q}(P) \cap S \neq \emptyset \right\}.$$

When $S$ is an $\mathbb{F}_q$-vector space of $R$, then we define $\mathcal{B}(S)$ analogously. A point set $L \subseteq \mathrm{PG}(r-1, q^t)$ is said to be $\mathbb{F}_q$-*linear* (or just *linear*) *of rank* $n$ if $L = \mathcal{B}(S)$ for some $(n-1)$-subspace $S \subseteq \mathrm{PG}(rt-1, q)$. If $L$ has size $(q^n-1)/(q-1)$ (which is the maximum size for a linear set of rank $n$), then $L$ is a *scattered* linear set. For further information on linear sets see [8,17].

**Definition 1** Let $\mathrm{PG}_{q^t}(V) = \mathrm{PG}(n-1, q^t)$ and let $W$ be an $\mathbb{F}_q$-vector subspace of $V$. If $\dim_{\mathbb{F}_q}(W) = \dim_{\mathbb{F}_{q^t}}(V) = n$ and $\langle W \rangle_{q^t} = V$, then $\Sigma' = \{\langle w \rangle_{q^t} : w \in W^*\}$ is a *canonical subgeometry* of $\mathrm{PG}_{q^t}(V)$.

Let $\Sigma' \cong \mathrm{PG}(n-1, q)$ be a canonical subgeometry of $\Sigma^* = \mathrm{PG}(n-1, q^t)$. Let $\Gamma \subset \Sigma^* \setminus \Sigma'$ be an $(n-1-r)$-subspace and let $\Lambda \subset \Sigma^* \setminus \Gamma$ be an $(r-1)$-subspace of $\Sigma^*$. The projection of $\Sigma'$ from *center* $\Gamma$ to *axis* $\Lambda$ is the point set

$$L = p_{\Gamma,\Lambda}\left(\Sigma'\right) := \left\{ \langle \Gamma, P \rangle \cap \Lambda \colon P \in \Sigma' \right\}. \tag{1}$$

In [15] Lunardon and Polverino characterized linear sets as projections of canonical subgeometries. They proved the following.

**Theorem 1** ([15, Theorems 1 and 2]) *Let $\Sigma^*$, $\Sigma'$, $\Lambda$, $\Gamma$ and $L = p_{\Gamma,\Lambda}(\Sigma')$ be defined as above. Then $L$ is an $\mathbb{F}_q$-linear set of rank $n$ and $\langle L \rangle = \Lambda$. Conversely, if $L$ is an $\mathbb{F}_q$-linear set of rank $n$ of $\Lambda = \mathrm{PG}(r-1, q^t) \subset \Sigma^*$ and $\langle L \rangle = \Lambda$, then there is an $(n-1-r)$-subspace $\Gamma$ disjoint from $\Lambda$ and a canonical subgeometry $\Sigma' \cong \mathrm{PG}(n-1, q)$ disjoint from $\Gamma$ such that $L = p_{\Gamma,\Lambda}(\Sigma')$.*

Note that when $r = n$ in Theorem 1, then $L = p_{\Gamma,\Lambda}(\Sigma') = \Sigma'$, hence $L$ is a canonical subgeometry. We rephrase here a theorem by Lavrauw and Van de Voorde.

**Theorem 2** ([6, Theorem 3]) *For $i = 1, 2$, let $\Sigma_i \cong \mathrm{PG}(n-1, q)$ be two canonical subgeometries of $\Sigma^* = \mathrm{PG}(n-1, q^t)$ and let $\Gamma_i$ be two $(n-1-r)$-subspaces of $\Sigma^*$, such that $\Gamma_i \cap \Sigma_i = \emptyset$. Let $\Lambda_i \subset \Sigma^* \setminus \Gamma_i$ be two $(r-1)$-subspaces and let $L_i = p_{\Gamma_i,\Lambda_i}(\Sigma_i)$. Suppose that $L_i$ is not an $\mathbb{F}_q$-linear set of rank $k < n$. Then the following statements are equivalent.*

(i) *There exists a collineation $\alpha \colon \Lambda_1 \to \Lambda_2$, such that ${L_1}^\alpha = L_2$,*
(ii) *there exists a collineation $\beta$ of $\Sigma^*$ such that ${\Sigma_1}^\beta = \Sigma_2$ and ${\Gamma_1}^\beta = \Gamma_2$,*
(iii) *for all canonical subgeometries $\Sigma \cong \mathrm{PG}(n-1, q)$ in $\Sigma^*$, there exist $\delta, \phi, \psi$ collineations of $\Sigma^*$, such that[1] ${\Sigma}^\delta = \Sigma$, ${\Gamma_1}^{\phi\delta} = {\Gamma_2}^\psi$, ${\Sigma_1}^\phi = \Sigma$ and ${\Sigma_2}^\psi = \Sigma$.*

We are going to prove that the implication (i) $\Rightarrow$ (ii) does not hold. In Sects. 3 and 4, we will show this in the case when $L_1 = L_2$ is a linear set of pseudoregulus type in $\mathrm{PG}(1, q^n)$,

[1] Compositions are executed from the left to the right.

for $n = 5$ or $n > 6$. In Sect. 5 a characterization will be given of the linear sets for which (i) $\Rightarrow$ (ii) holds.

In this paper, the results which lead to counterexamples are presented in a general setting. In the remainder of this introduction some hints are given to a better understanding of the key facts.

### 1.1 A minimal counterexample

The idea of a counterexample arose from the investigation of the linear sets of pseudoregulus type [3,14]. A minimal counterexample to Theorem 2 (i) $\Rightarrow$ (ii) can be obtained as follows. In $\mathrm{PG}(4, q^5)$, with coordinates $X_1, X_2, \ldots, X_5$, let $\Gamma$ be the plane of equations $X_1 = X_2 = 0$, and let $\ell$ be the line $X_3 = X_4 = X_5 = 0$. The sets

$$\Sigma_1 = \left\{ \left\langle \left(\lambda, \lambda^q, \lambda^{q^2}, \lambda^{q^3}, \lambda^{q^4}\right) \right\rangle_{q^5} : \lambda \in \mathbb{F}_{q^5}^* \right\}$$

and

$$\Sigma_2 = \left\{ \left\langle \left(\lambda, \lambda^{q^2}, \lambda^q, \lambda^{q^3}, \lambda^{q^4}\right) \right\rangle_{q^5} : \lambda \in \mathbb{F}_{q^5}^* \right\}$$

are canonical subgeometries. Defining $\mathrm{PG}(4, q) = \{\langle x \rangle_q : x \in \mathbb{F}_{q^5}^*\}$, the map $\varphi_1 : \mathrm{PG}(4, q) \to \Sigma_1$ defined by $\langle x \rangle_q^{\varphi_1} = \langle x, x^q, x^{q^2}, x^{q^3}, x^{q^4} \rangle_{q^5}$ is a collineation, as well as the map $\varphi_2 : \mathrm{PG}(4, q) \to \Sigma_2$ similarly defined. By [3,14], the projections $p_{\Gamma,\ell}(\Sigma_1)$ and $p_{\Gamma,\ell}(\Sigma_2)$ coincide, and are a linear set of pseudoregulus type, say $\mathbb{L} = \{\langle (\lambda, \lambda^q, 0, 0, 0) \rangle_{q^5} : \lambda \in \mathbb{F}_{q^5}^*\}$.

Now assume that as stated in Theorem 2 (ii) a collineation $\beta$ of $\mathrm{PG}(4, q^5)$ exists such that $\Gamma^\beta = \Gamma$, and $\Sigma_1^\beta = \Sigma_2$. It is shown in Theorem 5 that a projectivity exists having the same two properties; call it $\phi$. By the arguments in Lemma 1 in Sect. 4, the collineation $\varphi_2 \phi^{-1} \varphi_1^{-1}$ of $\mathrm{PG}(4, q)$ is the composition of a projectivity and either the map $\langle x \rangle_q \mapsto \langle x^{\theta_1} \rangle_q$ (cfr. (6)), or the map

$$\langle x \rangle_q \mapsto \left\langle x^{-\theta_1} \right\rangle_q = \left\langle x^{\theta_4 - \theta_1} \right\rangle_q = \left\langle x^{q^2 \theta_2} \right\rangle_q ,$$

which in turn is the composition of a projectivity and $\langle x \rangle_q \mapsto \langle x^{\theta_2} \rangle_q$. However, by Corollary 2 in Sect. 3, no map of type $\langle x \rangle_q \mapsto \langle x^{\theta_s} \rangle_q$ with $0 < s < t = 5$ is a collineation, and this is a contradiction.

### 1.2 Construction of counterexamples using condition (A) in Section 5

In Sect. 5 counterexamples are found with essentially distinct arguments. Theorem 7 states that a counterexample to Theorem 2 (i) $\Rightarrow$ (ii) can always be constructed in case the following condition does not hold: (A) For any two $(n-1)$-subspaces $U, U' \subset \mathrm{PG}(rt - 1, q)$, such that $\mathcal{B}(U) = L = \mathcal{B}(U')$, a collineation $\gamma \in \mathrm{P\Gamma L}(rt, q)$ exists, such that $U^\gamma = U'$, $\gamma$ preserves the Desarguesian spread $\mathcal{F}_{r,t,q}(\mathcal{P})$, and the induced map on $\mathrm{PG}(r - 1, q^t)$ is a collineation.

If $L = \mathcal{B}(\mathcal{Q}_{t-1,q})$, where $\mathcal{Q}_{t-1,q} \subset \mathrm{PG}(2t - 1, q)$ is the nonsingular hypersurface of degree $t$ studied in [5], then $L$ is a linear set of pseudoregulus type in $\mathrm{PG}(1, q^t)$.

In [5] all linear subspaces contained in $\mathcal{Q}_{t-1,q}$ are described for $q \geq t$. For $t \geq 4$ there exist two $(t-1)$-subspaces, say $U$ and $U'$, that are contained in $\mathcal{Q}_{t-1,q}$, and such that for any element $\gamma$ of the stabilizer of $\mathcal{Q}_{t-1,q}$, preserving the standard Desarguesian spread, it holds

$U^\gamma \neq U'$. For $t \geq 5$, $t \neq 6$, it is possible to choose $U$ and $U'$ with the additional property $\mathcal{B}(U) = L = \mathcal{B}(U')$. This leads to the counterexample of the previous subsection and its generalisations.

### 1.3 On the proof of [6, Theorem 3]

In the opinion of the authors of this paper, the proof of [6, Theorem 3] contains a wrong argument. The map $\delta$ defined at p. 93, line 21, is declared to be a projectivity, but is dealt with as a linear map e.g. in (1), as well as $p_2$ is. Such a $\delta$ is assumed to satisfy both conditions (i) $\delta$ maps an $\mathbb{F}_q$-vector space associated with $\Sigma_1^\chi$ onto an $\mathbb{F}_q$-vector space associated with $\Sigma_2$, and (ii) $p_2(a_i) = p_2(a_i^\delta)$, $i = 0, \ldots, m$. However, in the case of the minimal example in Sect. 1.1, no such $\delta$ exists.

## 2 Linear sets of pseudoregulus type in a projective line

A family of scattered $\mathbb{F}_q$-linear sets of rank $tm$ of $\mathrm{PG}(2m-1, q^t)$, called of *pseudoregulus type*, have been introduced in [16] for $m = 2$ and $t = 3$, further generalized in [7] for $m \geq 2$ and $t = 3$ and finally in [14] for $m \geq 1$ and $t \geq 2$ (for $t = 2$ they are the same as Baer subgeometries, see [14, Remark 3.4]). We will only consider linear sets of pseudoregulus type in $\mathrm{PG}(1, q^t)$. It has been proved in [14, Sect. 4] and in [3, Remark 2.2] that all linear sets of pseudoregulus type in $\mathrm{PG}(1, q^t)$ are $\mathrm{PGL}(2, q^t)$-equivalent and hence we can define them as follows.

**Definition 2** ([3,14]) A point set $L$ of $\mathrm{PG}_{q^t}(\mathbb{F}_{q^t}^2) = \mathrm{PG}(1, q^t)$, $t \geq 2$, is called a *linear set of pseudoregulus type* if $L$ is projectively equivalent to

$$\mathbb{L} := \left\{ \langle (\lambda, \lambda^q) \rangle_{q^t} : \lambda \in \mathbb{F}_{q^t}^* \right\}. \tag{2}$$

**Definition 3** Let $t \geq 2$ be an integer and let $\pi$ be a permutation of $N_{t-1} := \{0, 1, 2, \ldots, t-1\}$. We define $\Sigma_\pi$ as the following set of points in $\mathrm{PG}_{q^t}(\mathbb{F}_{q^t}^t) = \mathrm{PG}(t-1, q^t)$.

$$\Sigma_\pi := \left\{ \left\langle \left( \alpha^{q^{\pi(0)}}, \alpha^{q^{\pi(1)}}, \alpha^{q^{\pi(2)}}, \ldots, \alpha^{q^{\pi(t-1)}} \right) \right\rangle_{q^t} : \alpha \in \mathbb{F}_{q^t}^* \right\}. \tag{3}$$

**Proposition 1** *Consider $\mathbb{F}_{q^t}$ as a vector space over $\mathbb{F}_q$ and let $\Sigma = \mathrm{PG}_q(\mathbb{F}_{q^t}) \cong \mathrm{PG}(t-1, q)$. Let $\pi$ be a permutation of $N_{t-1}$. Then the following statements hold.*

1. *$S_\pi := \{(\alpha^{q^{\pi(0)}}, \alpha^{q^{\pi(1)}}, \alpha^{q^{\pi(2)}}, \ldots, \alpha^{q^{\pi(t-1)}}) : \alpha \in \mathbb{F}_{q^t}\}$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^t}^t$.*
2. *$\phi'_\pi : \mathbb{F}_{q^t} \to S_\pi : \alpha \mapsto (\alpha^{q^{\pi(0)}}, \alpha^{q^{\pi(1)}}, \alpha^{q^{\pi(2)}}, \ldots, \alpha^{q^{\pi(t-1)}})$ is a vector space isomorphism.*
3. *$\langle \Sigma_\pi \rangle = \mathrm{PG}(t-1, q^t)$.*
4. *The map*

$$\phi_\pi : \Sigma \to \Sigma_\pi : \langle \alpha \rangle_q \mapsto \left\langle \left( \alpha^{q^{\pi(0)}}, \alpha^{q^{\pi(1)}}, \alpha^{q^{\pi(2)}}, \ldots, \alpha^{q^{\pi(t-1)}} \right) \right\rangle_{q^t} \tag{4}$$

*is a collineation.*

*Proof* 1. and 2. are trivial, and 1.,2.,3. together imply 4., so it is enough to show 3. Let $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{F}_{q^t}$ and denote by $M_\pi$ the $t \times t$ matrix over $\mathbb{F}_{q^t}$ whose $j$th row is $\phi'_\pi(\alpha_j)$ for $j = 1, 2, \ldots, t$. According to [12, Lemma 3.51], $\det(M_{id}) \neq 0$ if and only if $\alpha_1, \alpha_2, \ldots, \alpha_t$

are linearly independent over $\mathbb{F}_q$. As $M_\pi$ can be obtained by permuting the columns of $M_{id}$, it follows that $\det(M_\pi) \neq 0$ if and only if $\det(M_{id}) \neq 0$. As $\dim_{\mathbb{F}_q}(\mathbb{F}_{q^t}) = t$, it follows that $\dim_{\mathbb{F}_{q^t}}(S_\pi) = t$ and hence 3. follows. □

Let $\Sigma^* = \mathrm{PG}(t-1, q^t)$, and denote the coordinates in $\Sigma^*$ by $X_1, X_2, \ldots, X_t$. Let $\Lambda \cong \mathrm{PG}(1, q^t)$ be the line $X_3 = \ldots = X_t = 0$ and let $\Gamma \cong \mathrm{PG}(t-3, q^t)$ be the $(t-3)$-subspace $X_1 = X_2 = 0$ in $\Sigma^*$. Let $\pi$ be a permutation of $N_{t-1}$, it is easy to see that if $\gcd(\pi(1) - \pi(0), t) = 1$, then $p_{\Gamma,\Lambda}(\Sigma_\pi) = \mathbb{L}$, see for example [14, Remark 4.2]. If $\phi$ is a collineation of $\Sigma^*$ such that $\Sigma_{id}^\phi = \Sigma_\pi$, then

$$\widetilde{\phi} := \phi_\pi \phi^{-1} \phi_{id}^{-1} \tag{5}$$

[see (4)] is a collineation of $\Sigma$. To study the action of $\widetilde{\phi}$ we need some results regarding the $\Theta_s$ map defined in the next section.

## 3 The $\Theta_s$ map

As before, let $\Sigma$ denote the $\mathrm{PG}(t-1, q)$ associated to $\mathbb{F}_{q^t}$.

**Definition 4** For an integer $s \geq -1$ let $\theta_s$ denote the number of points of $\mathrm{PG}(s, q)$, that is

$$\theta_s = \frac{q^{s+1} - 1}{q - 1}. \tag{6}$$

The map $\Theta_s \colon \Sigma \to \Sigma$ is defined as follows. For each $x \in \mathbb{F}_{q^t}^*$ let

$$\Theta_s(\langle x \rangle_q) = \langle x^{\theta_s} \rangle_q.$$

*Remark 1* If $s, d \geq -1$ are two integers, then $\Theta_s = \Theta_d$ if and only if $s \equiv d \pmod{t}$. As we do not use this result, the proof is left to the reader.

In Sect. 4 we show the following. If $\phi$ is a collineation such that $\Sigma_{id}^\phi = \Sigma_\pi$ and $\Gamma^\phi = \Gamma$, then $\widetilde{\phi} = \Theta_s \Omega$ [see (5)] for some collineation $\Omega$ and integer $0 \leq s < t$. Note that $\Theta_0$ is the identity. In Corollary 2, we prove that $\Theta_s$, with $0 < s < t$, is not a collineation of $\mathrm{PG}(t-1, q)$. It will follow that in most cases $\widetilde{\phi}$ is not a collineation and hence such $\phi$ cannot exist.

To determine whether $\Theta_s$ is a collineation or not we need some results regarding difference sets. A $(v, k, \lambda)$-*difference set* is a $k$-subset $D$ of a group $G$ of order $v$ such that the list of non-zero differences (if the group is written additively) contains each non-zero group element exactly $\lambda$ times. If the group is cyclic etc., then we say that the difference set is cyclic etc. For our purposes here, it is enough to consider cyclic difference sets, so from now on we assume that $G$ is cyclic. Let $D$ be a $(v, k, \lambda)$-difference set of $G$ and let $j$ be an integer. By $D + j$ and $jD$ we mean $\{d + j \colon d \in D\}$ modulo $v$ and $\{jd \colon d \in D\}$ modulo $v$. Note that $D + j$ is also a $(v, k, \lambda)$-difference set of $G$. If $\gcd(j, v) \neq 1$, then let $t := v/\gcd(j, v)$ and let $d_1 - d_2 = t$, where $d_1, d_2 \in D$. As $v \mid tj$, it follows that $jd_1 \equiv jd_2 \pmod{v}$ and hence $|jD| < |D|$. On the other hand, if $\gcd(j, v) = 1$, then $jD$ is also a $(v, k, \lambda)$-difference set of $G$. The integer $m$ is a *(numerical) multiplier* of $D$ if $mD = D + g$ for some integer $g$. The *trace* of $\beta \in \mathbb{F}_{q^t}$ is $\mathrm{Tr}(\beta) = \mathrm{Tr}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta) = \sum_{i=0}^{t-1} \beta^{q^i}$.

**Theorem 3** ([18, Theorem 2.1.1]) *Let $\alpha$ be a generator of the multiplicative group of $\mathbb{F}_{q^t}$, $t \geq 3$. The set of integers $D := \{i \colon 0 \leq i < \theta_{t-1}, \mathrm{Tr}(\alpha^i) = 0\}$ modulo $\theta_{t-1}$ forms a*

*(cyclic) difference set in* $\mathbb{Z}_{\theta_{t-1}}$ *(written additively), with parameters* $(\theta_{t-1}, \theta_{t-2}, \theta_{t-3})$*. The set of points of* $\mathrm{PG}_q(\mathbb{F}_{q^t}) \cong \mathrm{PG}(t-1,q)$ *which corresponds to the set* $D$*, i. e. the point set* $\mathcal{H}_D := \{\langle \alpha^i \rangle_q : i \in D\}$*, is a hyperplane of* $\mathrm{PG}(t-1,q)$*. Moreover, the hyperplanes of* $\mathrm{PG}(t-1,q)$ *are the sets* $\mathcal{H}_{D+j} := \{\langle \alpha^i \rangle_q : i \in D + j\}$*, where* $0 \le j < \theta_{t-1}$.

The difference sets constructed in Theorem 3 are called *classical Singer difference sets*. The next theorem describes the multipliers of these difference sets.

**Theorem 4** ([18, Corollary 1.3.4 and Proposition 3.1.1]) *Let* $D$ *be a classical Singer difference set with parameters as in Theorem 3. Then the multipliers of* $D$ *are the powers of* $p$ *modulo* $\theta_{t-1}$.

For a subset $\mathcal{X} \subseteq \Sigma$ and an integer $m$, let $\mathcal{X}^m = \{\langle x^m \rangle_q : \langle x \rangle_q \in \mathcal{X}\}$.

**Corollary 1** *Let* $t \ge 3$ *and* $m$ *be two integers. The* $\Sigma \to \Sigma$ *map,* $\langle x \rangle_q \mapsto \langle x^m \rangle_q$ *is a collineation if and only if* $m \equiv p^h \pmod{\theta_{t-1}}$*, for some* $h \in \mathbb{N}$.

*Proof* The map $\langle x \rangle_q \mapsto \langle x^m \rangle_q$ is a collineation if and only if it maps hyperplanes into hyperplanes. Let $\alpha$, $D$ and $\mathcal{H}_{D+j}$ for $0 \le j < \theta_{t-1}$ be defined as in Theorem 3. For any hyperplane $\mathcal{H}_{D+j}$ of $\Sigma$ the point set $\mathcal{H}^m_{D+j} = \{\langle \alpha^{mi} \rangle_q : i \in D + j\}$ is a hyperplane if and only if $\{mi : i \in D + j\} = mD + mj$ is a translate of $D$, i.e when $mD + mj = D + k$ for some $k$ and hence $mD = D + g$ (with $g = k - mj$), which is equivalent to saying that $m$ is a multiplier of $D$. The assertion follows from Theorem 4. □

**Corollary 2** *Let* $t \ge 3$*. For* $0 < s < t$ *the map* $\Theta_s$ *is not a collineation.*

*Proof* According to Corollary 1, it is enough to show that for any $0 < s < t$ there is no integer $h$ such that $\theta_s \equiv p^h \pmod{\theta_{t-1}}$. Note that $q^t = (q-1)\theta_{t-1} + 1$, thus $p^0 = 1 \equiv q^t \pmod{\theta_{t-1}}$. It is therefore enough to show the assertion when $p^h < q^t$. Suppose, contrary to our claim, that $\theta_s \equiv p^h \pmod{\theta_{t-1}}$ for some $p^h < q^t$ and $0 < s < t$. Since $p^h \not\equiv 0 \pmod{\theta_{t-1}}$, we have $s \le t - 2$ and

$$\theta_s q^t / p^h \equiv q^t \equiv 1 \pmod{\theta_{t-1}}. \tag{7}$$

It is easy to see that $p^h \ne 1$. If $1 < p^h < \theta_{t-1}$, then $p^h = \theta_s$, which cannot be as $p$ does not divide $\theta_s$. So we may assume $\theta_{t-1} < p^h < q^t$. In this case $p^h < q^t(p^h - \theta_{t-1})$, thus $q^t\theta_{t-1} < p^h(q^t - 1)$ and hence $q^t/p^h < (q^t - 1)/\theta_{t-1} = q - 1$. On the other hand we have $1 < q^t/p^h$ and hence

$$1 < \theta_s q^t / p^h < \theta_{t-2}(q-1) = q^{t-1} - 1 < \theta_{t-1},$$

contrary to (7). □

**Proposition 2** *For* $0 \le s < t$*, the map* $\langle x \rangle_q \mapsto \langle x^{-\theta_s} \rangle_q$ *is the composition of* $\Theta_{t-s-2}$ *and a projectivity of* $\Sigma$.

*Proof* For each $x \in \mathbb{F}^*_{q^t}$ we have $x^{\theta_{t-1}} \in \mathbb{F}^*_q$, thus

$$\left\langle x^{-\theta_s} \right\rangle_q = \left\langle x^{\theta_{t-1}-\theta_s} \right\rangle_q = \Theta_{t-s-2} \left\langle x^{q^{s+1}} \right\rangle_q .$$

As $\langle x \rangle_q \mapsto \langle x^{q^h} \rangle_q$ is a projectivity for each $h$, the assertion follows. □

## 4 Linear sets obtained via non-equivalent projections

**Definition 5** For an integer $h$ let $\Phi_h$ denote the collineation of $\Sigma^* = \mathrm{PG}(t-1, q^t)$, defined as

$$\langle(\alpha_0, \alpha_1, \ldots, \alpha_{t-1})\rangle_{q^t}^{\Phi_h} = \left\langle\left(\alpha_0^{p^h}, \alpha_1^{p^h}, \ldots, \alpha_{t-1}^{p^h}\right)\right\rangle_{q^t}.$$

**Proposition 3** *For each integer $h$ and permutation $\pi$ of $N_{t-1}$, $\Phi_h$ fixes $\Sigma_\pi$.*

*Proof* For each $\alpha \in \mathbb{F}_{q^t}^*$ we have

$$\left\langle\left(\alpha^{q^{\pi(0)}}, \alpha^{q^{\pi(1)}}, \ldots, \alpha^{q^{\pi(t-1)}}\right)\right\rangle_{q^t}^{\Phi_h} = \left\langle\left(\beta^{q^{\pi(0)}}, \beta^{q^{\pi(1)}}, \ldots, \beta^{q^{\pi(t-1)}}\right)\right\rangle_{q^t},$$

where $\beta = \alpha^{p^h}$. □

**Proposition 4** *Let $\pi$ be a permutation of $N_{t-1}$ and let $\omega$ be the permutation defined such that $\omega(i) \equiv \pi(i) - \pi(0) \pmod t$ for each $i \in N_{t-1}$. Then $\Sigma_\pi = \Sigma_\omega$.*

*Proof* Let $h = -\pi(0)e$, where $q = p^e$, $p$ prime. It is easy to see that $\Phi_h(\Sigma_\pi) = \Sigma_\omega$. As $\Phi_h$ fixes $\Sigma_\pi$ the assertion follows. □

**Lemma 1** *Let $\Gamma \cong \mathrm{PG}(t-3, q^t)$ be the $(t-3)$-space $X_1 = X_2 = 0$ in $\Sigma^* = \mathrm{PG}(t-1, q^t)$, $t \geq 3$. If $\phi$ is a projectivity of $\Sigma^*$ and $\pi$ is a permutation of $N_{t-1}$ such that $\Sigma_{id}^\phi = \Sigma_\pi$ and $\Gamma^\phi = \Gamma$, then $\pi(1) - \pi(0) \equiv \pm 1 \pmod t$, or $\gcd(\pi(1) - \pi(0), t) > 1$.*

*Proof* Suppose $\gcd(\pi(1) - \pi(0), t) = 1$. Let $M = (m_{ij})_{1 \leq i,j \leq t} \in \mathrm{GL}(t, q^t)$ be a matrix associated with $\phi$. As $\phi$ fixes $\Gamma$, we have $m_{ij} = 0$ when $i = 1, 2$ and $3 \leq j \leq t$. Denote the $2 \times 2$ matrix $(m_{ij})_{1 \leq i,j \leq 2}$ by $A$. As $M$ is non-singular, the same holds for $A$. According to Proposition 4 we may assume $\pi(0) = 0$. Let $\mu = \pi(1)$, whence $\gcd(\mu, t) = 1$. As $\Sigma_{id}^\phi = \Sigma_\pi$, for each $\alpha \in \mathbb{F}_{q^t}^*$ there exist $\delta_\alpha, t_\alpha \in \mathbb{F}_{q^t}^*$ such that

$$\delta_\alpha t_\alpha = m_{11}\alpha + m_{12}\alpha^q, \tag{8}$$

$$\delta_\alpha t_\alpha^{q^\mu} = m_{21}\alpha + m_{22}\alpha^q. \tag{9}$$

Let $N$ denote the norm function from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$, that is $N(x) = x^{\theta_{t-1}}$. As $N(\delta_\alpha t_\alpha^{q^\mu}) = N(\delta_\alpha t_\alpha) N(t_\alpha^{q^\mu - 1}) = N(\delta_\alpha t_\alpha)$, it follows that

$$N\left(m_{11}\alpha + m_{12}\alpha^q\right) = N\left(m_{21}\alpha + m_{22}\alpha^q\right),$$
$$N\left(m_{11} + m_{12}\alpha^{q-1}\right) = N\left(m_{21} + m_{22}\alpha^{q-1}\right),$$

and hence for each $(q-1)$th power $z$ of $\mathbb{F}_{q^t}^*$ we have

$$P(z) := N(m_{11} + m_{12}z) - N(m_{21} + m_{22}z) = 0,$$

where $P(z)$ is a polynomial of degree at most $\theta_{t-1}$.

We claim $m_{11}m_{21} = 0$ and $m_{12}m_{22} = 0$. First suppose $m_{11}m_{21} \neq 0$. Then the coefficient of $z^q$ in $P(z)$ is

$$m_{12}^q N(m_{11})/m_{11}^q - m_{22}^q N(m_{21})/m_{21}^q. \tag{10}$$

The coefficient of $z^{q+1}$ is

$$m_{12}^{q+1} N(m_{11})/m_{11}^{q+1} - m_{22}^{q+1} N(m_{21})/m_{21}^{q+1}. \tag{11}$$

As $P(z)$ vanishes for each $z$ with $z^{\theta_{t-1}}=1$, we have $P(z)=a(z^{\theta_{t-1}}-1)$ for some $a\in\mathbb{F}_{q^t}$. It follows that (10) and (11) are zero, thus if $m_{12}m_{22}\neq 0$, then

$$m_{12}/m_{11}=m_{22}/m_{21},$$

and hence $\det(A)=0$, a contradiction. On the other hand if one of $\{m_{12},m_{22}\}$ is zero, then both of them are zero, thus we obtain again $\det(A)=0$. Now suppose $m_{12}m_{22}\neq 0$. Then the coefficient of $z^{\theta_{t-1}-q}$ in $P(z)$ is

$$m_{11}^q N(m_{12})/m_{12}^q - m_{21}^q N(m_{22})/m_{22}^q. \tag{12}$$

As before, it follows that (12) is zero. Together with $m_{11}m_{21}=0$, it means that $m_{11}$ and $m_{21}$ are both zero, and hence $\det(A)=0$, a contradiction.

First we consider the case when $A$ is diagonal, i.e. $m_{12}=m_{21}=0$. We may assume $m_{11}=1$. Then (8) and (9) yield

$$t_\alpha^{q^\mu-1}=m_{22}\alpha^{q-1}.$$

The last equation implies that a $\rho\in\mathbb{F}_{q^n}^*$ exists such that $\rho^{q-1}=m_{22}$. Then for any $x\in\mathbb{F}_{q^t}^*$ the following holds:

$$\begin{aligned}\left\langle \frac{x^{\theta_{\mu-1}}}{\rho}\right\rangle_q^{\phi_{id}\phi} &= \left\langle \left(\frac{x^{\theta_{\mu-1}}}{\rho},\frac{x^{q\theta_{\mu-1}}}{\rho^q},\ldots,\frac{x^{q^{t-1}\theta_{\mu-1}}}{\rho^{q^{t-1}}}\right)\right\rangle_{q^t}^{\phi}\\ &= \left\langle \left(\frac{x^{\theta_{\mu-1}}}{\rho},\frac{x^{q\theta_{\mu-1}}}{\rho},*\right)\right\rangle_{q^t} = \left\langle \left(1,x^{q^\mu-1},*\right)\right\rangle_{q^t}\in\Sigma_\pi;\\ \langle x\rangle_q^{\phi_\pi} &= \left\langle \left(x,x^{q^\mu},*\right)\right\rangle_{q^t} = \left\langle \left(1,x^{q^\mu-1},*\right)\right\rangle_{q^t}\in\Sigma_\pi.\end{aligned}$$

Since $\mu$ and $t$ are coprime, $\Sigma_\pi$ contains exactly one element of the form $\langle(1,x^{q^\mu-1},*)\rangle_{q^t}$. It follows that for any $x\in\mathbb{F}_{q^t}^*$

$$\left\langle x^{\theta_{\mu-1}}/\rho\right\rangle_q^{\phi_{id}\phi}=\langle x\rangle_q^{\phi_\pi},$$

and hence $\phi_\pi\phi^{-1}\phi_{id}^{-1}\colon\Sigma\to\Sigma$ which maps $\langle x\rangle_q$ to $\langle x^{\theta_{\mu-1}}/\rho\rangle_q$ is a collineation. Since the map $\langle y\rangle_q\mapsto\langle y/\rho\rangle_q$ is a collineation of $\Sigma$, Corollary 2 yields that $\phi_\pi\phi^{-1}\phi_{id}^{-1}$ is a collineation only if $\mu=1$.

Now consider the case when $m_{11}=m_{22}=0$. We may assume $m_{12}=1$. Then (8) and (9) yield

$$t_\alpha^{q^\mu-1}=m_{21}\alpha^{1-q}.$$

This implies that a $\rho\in\mathbb{F}_{q^t}^*$ exists such that $\rho^{q-1}=m_{21}$. As before, it follows that

$$\left\langle x^{-\theta_{\mu-1}}\rho\right\rangle_q^{\phi_{id}\phi}=\langle x\rangle_q^{\phi_\pi},$$

for each $x\in\mathbb{F}_{q^t}^*$ and hence $\phi_\pi\phi^{-1}\phi_{id}^{-1}\colon\Sigma\to\Sigma$ which maps $\langle x\rangle_q$ to $\langle x^{-\theta_{\mu-1}}\rho\rangle_q$ is a collineation. Proposition 2 and Corollary 2 yield that this happens only if $\mu=t-1$. □

**Theorem 5** *Let $\Gamma\cong\mathrm{PG}(t-3,q^t)$ be the $(t-3)$-space $X_1=X_2=0$ in $\Sigma^*=\mathrm{PG}(t-1,q^t)$, $t\geq 3$. If $\phi$ is a collineation of $\Sigma^*$ such that $\Sigma_{id}^\phi=\Sigma_\pi$ and $\Gamma^\phi=\Gamma$, then $\pi(1)-\pi(0)\equiv\pm1 \pmod t$, or $\gcd(\pi(1)-\pi(0),t)>1$.*

*Proof* According to the Fundamental Theorem of Projective Geometry we may assume $\phi = \Phi_h \Omega$, where $\Omega$ is a projectivity and $\Phi_h$ is as in Definition 5. As $\Phi_h$ fixes $\Gamma$ and $\Sigma_{id}$, it follows that $\Omega$ satisfies the conditions of Lemma 1 and hence the assertion follows. □

**Corollary 3** *If $t = 5$ or $t > 6$, then any linear set of pseudoregulus type in $\mathrm{PG}(1, q^t)$ can be obtained as the projection of two different subgeometries, $\Sigma_1 \cong \Sigma_2 \cong \mathrm{PG}(t-1, q)$, from a center $\Gamma \cong \mathrm{PG}(t-3, q^t)$ to an axis $\Lambda \cong \mathrm{PG}(1, q^t)$ in the ambient space $\Sigma^* = \mathrm{PG}(t-1, q^t)$, such that there exists no collineation $\phi$ of $\Sigma^*$ with $\Gamma^\phi = \Gamma$ and $\Sigma_1^\phi = \Sigma_2$.*

*Proof* Let $\Lambda$ be the line $X_3 = \cdots = X_t = 0$ and let $\Gamma$ be the $(t-3)$-subspace $X_1 = X_2 = 0$ in $\Sigma^*$. As $t = 5$ or $t > 6$, we have $\varphi(t) \geq 3$, where $\varphi$ is the Euler function. Thus we may choose a permutation $\pi$ of $N_{t-1}$ such that $\gcd(\pi(1)-\pi(0), t) = 1$ and $\pi(1)-\pi(0) \notin \{-1, 1\}$. Let $\Sigma_1 = \Sigma_{id}$ and $\Sigma_2 = \Sigma_\pi$. Then $p_{\Gamma,\Lambda}(\Sigma_1) = p_{\Gamma,\Lambda}(\Sigma_2) \cong \mathbb{L}$ and the assertion follows from Theorem 5. □

Note that $\mathbb{L}$ is not a linear set of rank $k < t$, thus (i) $\Rightarrow$ (ii) in Theorem 2 cannot hold without further conditions.

## 5 Equivalence of linear sets

We say that the pair $(L, n)$, where $L$ is a linear set of rank $n$ in $\mathrm{PG}(r-1, q^t)$, satisfies condition (A), if the following holds.

(A) For any two $(n-1)$-subspaces $U, U' \subset \mathrm{PG}(rt-1, q)$, such that $\mathcal{B}(U) = L = \mathcal{B}(U')$, a collineation $\gamma \in \mathrm{P\Gamma L}(rt, q)$ exists, such that $U^\gamma = U'$, $\gamma$ preserves the Desarguesian spread $\mathcal{F}_{r,t,q}(\mathcal{P})$, and the induced map on $\mathrm{PG}(r-1, q^t)$ is a collineation (which will again be denoted by $\gamma$).

In the next theorem we follow the proof of [2, Theorem 2.4] by Bonoli and Polverino.

**Theorem 6** *For $i = 1, 2$, let $\Sigma_i \cong \mathrm{PG}(n-1, q)$ be two canonical subgeometries of $\Sigma^* = \mathrm{PG}(n-1, q^t)$ and let $\Gamma_i$ be two $(n-1-r)$-subspaces of $\Sigma^*$, such that $\Gamma_i \cap \Sigma_i = \emptyset$. Let $\Lambda_i \subset \Sigma^* \setminus \Gamma_i$ be two $(r-1)$-subspaces and let $L_i = p_{\Gamma_i,\Lambda_i}(\Sigma_i)$. Suppose that $(L_2, n)$ satisfies condition (A). Then* (i) $\Rightarrow$ (ii), *where* (i) *and* (ii) *are the conditions stated in Theorem 2.*

*Proof* The collineation $\alpha$ in Theorem 2 can be extended to an element $\widehat{\alpha} \in \mathrm{P\Gamma L}(n, q^t)$ such that $\Gamma_1^{\widehat{\alpha}} = \Gamma_2$. Then $L_2 = L_1^{\widehat{\alpha}} = p_{\Gamma_2,\Lambda_2}(\Sigma_1^{\widehat{\alpha}})$. Hence it is sufficient to prove the existence of a collineation $\phi \in \mathrm{P\Gamma L}(n, q^t)$ such that $\Gamma_2^\phi = \Gamma_2$ and $\Sigma_1^{\widehat{\alpha}\phi} = \Sigma_2$. If such $\phi$ exists, then $\beta := \widehat{\alpha}\phi$.

So it is enough to prove the assertion when $\Gamma_1 = \Gamma_2 =: \Gamma$, $\Lambda_1 = \Lambda_2 =: \Lambda$ and $L_1 = L_2 =: L$. Let $\Sigma^* = \mathrm{PG}_{q^t}(\mathbb{F}_{q^t}^n)$ and for $j = 1, 2$, let $\Sigma_j = \mathcal{B}(V_j)$, where $V_j$ is an $n$-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^t}^n$. As $\Sigma_j$ is a canonical subgeometry, we have $\langle V_j \rangle_{q^t} = \mathbb{F}_{q^t}^n$, for $j = 1, 2$. Let $V_1 = \langle v_1, v_2, \ldots v_n \rangle_q$. Also let $\Gamma = \mathrm{PG}_{q^t}(Z)$ and $\Lambda = \mathrm{PG}_{q^t}(R)$. Note that $V_j' := (V_j + Z) \cap R$ is an $n$-dimensional $\mathbb{F}_q$-vector space in $R$. As $p_{\Gamma,\Lambda}(\Sigma_1) = p_{\Gamma,\Lambda}(\Sigma_2) = L$, it follows that $\mathcal{B}(V_1') = \mathcal{B}(V_2')$. As $(L, n)$ satisfies condition $(A)$, it follows that there exists a non-singular $\mathbb{F}_{q^t}$-semilinear map $\gamma' \colon R \to R$ such that $V_1'^{\gamma'} = V_2'$. The map $\gamma'$ can be extended to a non-singular semilinear map $\widehat{\gamma} \colon \mathbb{F}_{q^t}^n \to \mathbb{F}_{q^t}^n$ such that $Z^{\widehat{\gamma}} = Z$. Then for each vector $v \in \mathbb{F}_{q^t}^n$ and $\mu \in \mathbb{F}_{q^t}$ we have $(\mu v)^{\widehat{\gamma}} = \mu^{p^k} v^{\widehat{\gamma}}$ for some integer $k$. Since all of $R + Z = \mathbb{F}_{q^t}^n$ and $V_j + Z$ $(j = 1, 2)$ are direct sums, for any $v \in V_j \setminus \{0\}$ and $z \in Z$, the

intersection $(\langle v\rangle_q + Z) \cap R$ is a one-dimensional $\mathbb{F}_q$-subspace, say $\langle v'\rangle_q$, with $v' \in V'_j$; this implies $hv' = v + z'$ for some $z' \in Z$ and $h \in \mathbb{F}_q$, whence $v + z = hv' + (z - z') \in V'_j + Z$. This implies $V_j + Z \subseteq V'_j + Z$ and therefore $V_j + Z = V'_j + Z$. Then we have

$$V_2 + Z = V'_2 + Z = V_1'^{\widehat{\gamma}} + Z^{\widehat{\gamma}} = \left(V'_1 + Z\right)^{\widehat{\gamma}} = (V_1 + Z)^{\widehat{\gamma}},$$

and hence for each $i = 1, 2, \ldots, n$, $v_i^{\widehat{\gamma}} = v'_i + z_i$ for some $v'_i \in V_2$ and $z_i \in Z$. We claim that $v'_1, v'_2, \ldots, v'_n$ is an $\mathbb{F}_q$-basis of $V_2$. To see this, suppose $\sum_{i=1}^n \lambda_i v'_i = 0$ with $\lambda_i \in \mathbb{F}_q$ for $i = 1, 2, \ldots, n$. Then $\sum_{i=1}^n \lambda_i v_i^{\widehat{\gamma}} = \sum_{i=1}^n \lambda_i z_i$. As on the left-hand side $v_1^{\widehat{\gamma}}, v_2^{\widehat{\gamma}}, \ldots, v_n^{\widehat{\gamma}}$ are $\mathbb{F}_q$-independent, it follows that either $\lambda_i = 0$ for $i = 1, 2, \ldots, n$, or there is a non-zero vector $z \in V_1^{\widehat{\gamma}} \cap Z$. The map $\widehat{\gamma}$ fixes $Z$ and hence in the latter case $z^{\widehat{\gamma}^{-1}} \in V_1 \cap Z$, a contradiction because of $V_1 \cap Z = \{0\}$. As $\Sigma_2$ is a canonical subgeometry, it follows that $v'_1, v'_2, \ldots, v'_n$ are linearly independent over $\mathbb{F}_{q^t}$. Let $f$ be the $\mathbb{F}_{q^t}$-semilinear map of $\mathbb{F}_{q^t}^n$ such that $v_i^f = v'_i$ for each $i = 1, 2, \ldots, n$ and $(\mu v)^f = \mu^{p^k} v^f$ for each $\mu \in \mathbb{F}_{q^t}$ and $v \in \mathbb{F}_{q^t}^n$. If $P = \langle z\rangle_{q^t} \in \Gamma$, then we have $z = \sum_{i=1}^n a_i v_i$ for some $a_i \in \mathbb{F}_{q^t}$. Then $z^f = \sum_{i=1}^n a_i^{p^k} v'_i = \sum_{i=1}^n a_i^{p^k} (v_i^{\widehat{\gamma}} - z_i) = z^{\widehat{\gamma}} - \sum_{i=1}^n a_i^{p^k} z_i \in Z$, and hence the collineation induced by $f$ fixes $\Gamma$ and maps $\Sigma_1$ to $\Sigma_2$. □

*Remark 2* In Theorem 6, it is not assumed, contrary to Theorem 2, that the linear sets are not of rank $<n$.

*Remark 3* By [2, Proposition 2.3], condition (A) holds for any $\mathbb{F}_q$-linear blocking set of exponent $e$ (where $p^e = q$) in $\mathrm{PG}(2, q^t)$.

*Remark 4* Up to the knowledge of the authors, no linear set is known which is not of pseudoregulus type in $\mathrm{PG}(1, q^t)$ and does not satisfy condition (A).

**Theorem 7** *If $L$ is a linear set of rank $n$ in $\Lambda = \mathrm{PG}(r-1, q^t)$, $\langle L\rangle = \mathrm{PG}(r-1, q^t)$ and $(L, n)$ does not satisfy condition (A), then in $\mathrm{PG}(n-1, q^t) \supset \Lambda$ there are a subspace $\Gamma = \Gamma_1 = \Gamma_2$ disjoint from $\Lambda$, and two $q$-order canonical subgeometries $\Sigma_1, \Sigma_2 \subset \mathrm{PG}(n-1, q^t) \setminus \Gamma$ such that $L = p_{\Gamma,\Lambda}(\Sigma_1) = p_{\Gamma,\Lambda}(\Sigma_2)$, and such that condition (ii) in Theorem 2 does not hold.*

*Proof* Let $U_1$ and $U_2$ be two $(n-1)$-subspaces of $\mathrm{PG}_q(R)$, where $R$ is the $r$-dimensional $\mathbb{F}_{q^t}$-subspace of $\mathbb{F}_{q^t}^n$ such that $\Lambda = \mathrm{PG}_{q^t}(R)$. Assume that $\mathcal{B}(U_1) = L = \mathcal{B}(U_2)$. Let $W_i = \langle w_1^{(i)}, w_2^{(i)}, \ldots, w_n^{(i)}\rangle_q, i = 1, 2$, be the $n$-dimensional vector $\mathbb{F}_q$-subspaces of $R$ whose associated projective subspaces in $\mathrm{PG}(rt-1, q)$ are $U_1$ and $U_2$, respectively. From $\langle L\rangle = \mathrm{PG}(r-1, q^t)$ we may assume that $w_1^{(1)}, w_2^{(1)}, \ldots, w_r^{(1)}$ are $\mathbb{F}_{q^t}$-linearly independent, and also that $w_1^{(2)}, w_2^{(2)}, \ldots, w_r^{(2)}$ are $\mathbb{F}_{q^t}$-linearly independent. Let $\Gamma$ be an $(n-r-1)$-subspace in $\mathrm{PG}(n-1, q^t)$ disjoint from $\Lambda$, associated with the vector subspace $Z = \langle z_1, z_2, \ldots, z_{n-r}\rangle_{q^t}$. For $i = 1, 2$, let $\Sigma_i$ be the $\mathbb{F}_q$-linear set defined by the following $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^t}^n$:

$$V_i := \left\langle w_1^{(i)}, w_2^{(i)}, \ldots, w_r^{(i)}, w_{r+1}^{(i)} + z_1, w_{r+2}^{(i)} + z_2, \ldots, w_n^{(i)} + z_{n-r}\right\rangle_q.$$

Since those $n$ vectors of $\mathbb{F}_{q^t}^n$ are also $\mathbb{F}_{q^t}$-linearly independent, $\Sigma_i$ is a canonical $q$-order subgeometry. Furthermore, $w_1^{(i)}, w_2^{(i)}, \ldots, w_n^{(i)}, z_1, z_2, \ldots, z_{n-r}$ are $\mathbb{F}_q$-linearly independent, and this implies $\Sigma_i \cap \Gamma = \emptyset$. We summarize here some properties of our construction, which we will use later. For $i = 1, 2$ we have the following.

1. For each $w \in W_i$, there exists a unique $z_w \in Z$ such that $w + z_w \in V_i$,
2. if $w$ and $w'$ are two $\mathbb{F}_q$-independent vectors in $W_i$, then $w + z_w$ and $w' + z_{w'}$ are $\mathbb{F}_{q^t}$-independent vectors in $V_i$.

If $w = \sum_{j=1}^{n} \alpha_j w_j^{(i)}$ with $a_j \in \mathbb{F}_q$, $j = 1, 2, \ldots, n$, then let $z_w = \sum_{j=r+1}^{n} \alpha_j z_{j-r}$. The unicity of $z_w$ follows from $\Sigma_i \cap \Gamma = \emptyset$. To see 2., note that $\Psi_i : U_i \to \Sigma_i : \langle w \rangle_q \mapsto \langle w + z_w \rangle_{q^t}$ is a bijection, as $|U_i| = |\Sigma_i| = \theta_{n-1}$.

Now assume that condition (ii) in Theorem 2 holds. Let $\beta' : \mathbb{F}_{q^t}^n \to \mathbb{F}_{q^t}^n$ be the semilinear map associated with the collineation $\beta$; so, an integer $\nu$ exists such that for any $a \in \mathbb{F}_{q^t}$ and $v \in \mathbb{F}_{q^t}^n$ there holds $(av)^{\beta'} = a^{p^\nu} v^{\beta'}$. Denote by $\pi$ the canonical projection from $Z \oplus R$ to $R$. Fix an element $w \in W_1$. Then 1. and the condition $\Sigma_1^\beta = \Sigma_2$ imply the existence of $z_w \in Z$ and $\lambda \in \mathbb{F}_{q^t}^*$ depending on $z_w$ such that $\xi_\lambda := \lambda(w + z_w)^{\beta'} \in V_2$. Let $T_\lambda = \{v \in W_1 : \lambda v^{\beta'\pi} \in W_2\}$. Note that $T_\lambda$ is an $\mathbb{F}_q$-vector subspace of $R$. As $\lambda(w + z_w)^{\beta'} \in V_2$, we have $\lambda(w + z_w)^{\beta'\pi} = \lambda w^{\beta'\pi} \in V_2^\pi = W_2$, thus $w \in T_\lambda$. We are going to show that $W_1 = T_\lambda$. Suppose to the contrary that there exists $w' \in W_1 \setminus T_\lambda$. As $T_\lambda$ is an $\mathbb{F}_q$-vector space, $w$ and $w'$ are $\mathbb{F}_q$-independent. The same argument as above yields the existence of $z_{w'} \in Z$ and $\mu \in \mathbb{F}_{q^t}^*$ such that $\xi_\mu := \mu(w' + z_{w'})^{\beta'} \in V_2$ and hence $\mu w'^{\beta'\pi} \in W_2$. Then 2. yields that $\langle w + z_w \rangle_{q^t}$ and $\langle w' + z_{w'} \rangle_{q^t}$ are distinct points of $\Sigma_1$, and hence $\langle \xi_\lambda \rangle_{q^t}$ and $\langle \xi_\mu \rangle_{q^t}$ are distinct points of $\Sigma_2$. First we prove

$$\langle \xi_\lambda, \xi_\mu \rangle_{q^t} \cap V_2 = \langle \xi_\lambda, \xi_\mu \rangle_q. \tag{13}$$

Denote by $X$ de left hand side of (13). The inclusion $\supseteq$ trivially holds. Suppose to the contrary $\dim_{\mathbb{F}_q}(X) \geq 3$, then there exist three $\mathbb{F}_q$-independent vectors, $v_1, v_2, v_3 \in X$. We can extend the set $\{v_1, v_2, v_3\}$ to a basis of $V_2$. As $\dim_{\mathbb{F}_{q^t}}(\langle v_1, v_2, v_3 \rangle_{q^t}) = 2$, it follows that $\langle V_2 \rangle_{q^t} \neq \mathbb{F}_{q^t}^n$, a contradiction since $\Sigma_2$ is a canonical subgeometry.

Let $P_1 = \langle w + z_w \rangle_{q^t}$ and $P_2 = \langle w' + z_{w'} \rangle_{q^t}$. Denote by $\ell$ the $q$-order subline $\langle P_1, P_2 \rangle \cap \Sigma_1$. Then $\langle (w + z_w)^{\beta'} + (w' + z_{w'})^{\beta'} \rangle_{q^t} = \langle \xi_\lambda + \lambda\mu^{-1}\xi_\mu \rangle_{q^t} \in \ell^\beta \cap \Sigma_2$. It follows that there exists some $\delta \in \mathbb{F}_{q^t}^*$ such that $\delta(\xi_\lambda + \lambda\mu^{-1}\xi_\mu) \in V_2$. It follows from (13) that $\delta \in \mathbb{F}_q^*$ and $\delta\lambda\mu^{-1} \in \mathbb{F}_q^*$. Hence $\lambda\mu^{-1} \in \mathbb{F}_q^*$. This is a contradiction, as in this case $(\lambda\mu^{-1})\mu w'^{\beta'\pi} = \lambda w'^{\beta'\pi} \in W_2$, contradicting the choice of $w'$. Hence $T_\lambda = W_1$, that is, $\lambda w^{\beta'\pi} \in W_2$ for any $w \in W_1$.

Now define the map $\varphi' : R \to R : v \mapsto \lambda v^{\beta'\pi}$. As $\beta'$ is semilinear, $\pi$ is linear and $v \mapsto \lambda v$ is also linear, it follows that $\varphi'$ is $\mathbb{F}_{q^t}$-semilinear. Also, $\varphi'$ is non-singular. Let $\varphi$ be the associated collineation of $\Lambda$. Then

$$U_1^\varphi = \left\{ \left\langle \lambda w^{\beta'\pi} \right\rangle_q : w \in W_1^* \right\} = \mathrm{PG}_q(W_2) = U_2,$$

because of $T_\lambda = W_1$.

We have constructed an example for which, if condition (ii) in Theorem 2 is satisfied, then also condition (A) must be satisfied: this concludes the proof. □

Scattered linear sets of pseudoregulus type in a line are, under the field reduction map, embeddings of minimum dimension of $\mathrm{PG}(t-1, q) \times \mathrm{PG}(t-1, q)$, which have been studied in [5]. These embeddings are projections of Segre varieties. A similar representation of the clubs as projections of Segre varieties can be found in [11] (see also [9]). By the arguments in the proof of [5, Theorem 16], $(\mathbb{L}, t)$ does not fulfill condition (A), for $t = 5$ or $t > 6$, where $\mathbb{L}$ is the scattered linear set of pseudoregulus type in $\mathrm{PG}(1, q^t)$. For in this case it is possible to

choose a subspace in the family $\mathcal{S}_1$ and a subspace in $\mathcal{S}_i$, $i \in \{2, 3, \ldots, t-2\}$, $\gcd(i, t) = 1$. By Theorem 7 this yields the counterexamples as shown in the previous sections. Many results in [6] are on linear sets in $\mathrm{PG}(1, q^3)$; hence, the following result can be of interest:

**Proposition 5** *Condition (A) is fulfilled by linear sets of rank three in* $\mathrm{PG}(1, q^3)$, $q > 2$, *for* $n = 3$.

*Proof* A linear set $L$ of rank three in $\mathrm{PG}(1, q^3)$ is either a point, or a club, or a scattered linear set.

If $L$ is a point, then from

$$\mathcal{B}(U) = \mathcal{B}\left(U'\right), \quad \dim(U) = \dim\left(U'\right) = 2, \tag{14}$$

one obtains $U = U' = \mathcal{F}_{2,3,q}(L)$. This implies (A).

Assume now that $L$ is a club. Denote by $H$ its head, which is uniquely defined [4,6]. Assume that the subspaces $U$ and $U'$ satisfy (14). Take a point $P = \langle (v_0, v_1)\rangle_{q^3} \in L \setminus H$ and let $A = \mathcal{F}_{2,3,q}(P) \cap U$ and $X = \mathcal{F}_{2,3,q}(P) \cap U'$. Then $A = \langle \alpha(v_0, v_1)\rangle_q$ and $X = \langle \beta(v_0, v_1)\rangle_q$ for some $\alpha, \beta \in \mathbb{F}_{q^3}^*$, and the map $\gamma\colon \langle (x_0, x_1)\rangle_q \mapsto \langle \beta\alpha^{-1}(x_0, x_1)\rangle_q$ is a projectivity of $\mathrm{PG}(5, q)$ belonging to the elementwise stabilizer of the Desarguesian spread, and mapping $A$ into $X$. Then $X \in U^\gamma \cap U' \setminus \mathcal{F}_{2,3,q}(H)$. The element of $\mathrm{P\Gamma L}(2, q^3)$ associated with $\gamma$ is the identity map. Denote by $\ell_1$ and $\ell_2$ the lines $U^\gamma \cap \mathcal{F}_{2,3,q}(H)$ and $U' \cap \mathcal{F}_{2,3,q}(H)$, respectively. If $\ell_1 = \ell_2$, then $U^\gamma = \langle \ell_1, X\rangle = U'$. Otherwise let $\ell'$ be a line in $U'$ through $X$ such that $\ell_1 \cap \ell_2 \notin \ell'$. The club $L$ does not contain irregular sublines [6, Corollary 13], [4, Proposition 5]. Applying this result to the $q$-order subline $\mathcal{B}(\ell')$, we have that a line $\ell$ in $U^\gamma$ exists such that $\mathcal{B}(\ell) = \mathcal{B}(\ell')$. The point $X$ is on $\ell$. The lines $\ell$, $\ell'$ of $\mathrm{PG}(5, q)$ are transversal lines to the regulus $\mathcal{F}_{2,3,q}(\mathcal{B}(\ell))$, having a common point, whence $\ell = \ell'$. This implies $U^\gamma = \langle \ell, \ell_1 \cap \ell_2\rangle = U'$ and (A).

Up to projectivities there is a unique scattered linear set in $\mathrm{PG}(1, q^3)$. To see this, fix a $q$-order canonical subgeometry $\Sigma$ of $\Sigma^* = \mathrm{PG}(2, q^3)$ and denote by $\mathcal{I}$ the set of points of $\Sigma^*$ not contained in a line of $\Sigma$. Denote by $G$ the stabilizer of $\Sigma$ in the group of projectivities of $\Sigma^*$. Each scattered linear set of rank three of $\mathrm{PG}(1, q^3)$ can be obtained as a projection of $\Sigma$ from a point in $\mathcal{I}$. In Theorem 2 the implication (ii) $\Rightarrow$ (i) holds and hence the number of projectively non-equivalent scattered linear sets of rank three in $\mathrm{PG}(1, q^3)$ is at most the number of orbits of $G$ on the points of $\mathcal{I}$. It follows from [2, Proposition 3.1] that $G$ is transitive on $\mathcal{I}$ and hence there is a unique scattered linear set of rank three in $\mathrm{PG}(1, q^3)$. An alternate proof can be obtained from [1], where the uniqueness of an exterior splash is proved, taking into account that the exterior splashes dealt with in that paper are precisely the scattered linear sets of rank three [10].

Assume that $L$ is a scattered linear set of rank three, hence a linear set of pseudoregulus type, and that (14) holds. Then $U$ and $U'$ are planes contained in the hypersurface $\mathcal{Q}_{2,q}$ defined in [5, Eqs. (7), (8)]. By [5, Corollary 10], $U = S_{h,k}$, $U' = S_{h',k'}$ for $h, h' \in \{1, 2\}$, $N(k) = N(k') = 1$. A collineation $\gamma$ satisfying (A) can be obtained in the form $\varphi_{0,0}(a, b)$ if $h = h'$, and $\psi_{0,0}(a, b)$ if $h \neq h'$, for suitable $a, b \in \mathbb{F}_{q^3}$. □

**Acknowledgments** This research was supported by the Italian Ministry of Education, University and Research (PRIN 2012 Project "Strutture geometriche, combinatoria e loro applicazioni").

## References

1. Barwick S.G., Jackson W.A.: Exterior splashes and linear sets of rank 3. arXiv:1404.1641v1.

2. Bonoli G., Polverino O.: $\mathbb{F}_q$-linear blocking sets in PG(2, $q^4$). Innov. Incid. Geom. **2**, 35–56 (2005).
3. Donati G., Durante N.: Scattered linear sets generated by collineations between pencils of lines. J. Algebr. Comb. **40**, 1121–1134 (2014).
4. Fancsali Sz.L., Sziklai P.: Description of the clubs. Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **51**, 141–146 (2008).
5. Lavrauw M., Sheekey J., Zanella C.: On embeddings of minimum dimension of PG$(n, q) \times$ PG$(n, q)$. Des. Codes Cryptogr. **74**, 427–440 (2015).
6. Lavrauw M., Van de Voorde G.: On linear sets on a projective line. Des. Codes Cryptogr. **56**, 89–104 (2010).
7. Lavrauw M., Van de Voorde G.: Scattered linear sets and pseudoreguli. Electron. J. Comb. **20**(1), P15 (2013).
8. Lavrauw M., Van de Voorde G.: Field reduction and linear sets on a projective line. In: Topics in Finite Fields, AMS Contemporary Math, vol. 623, pp. 271–293. American Mathematical Society, Providence (2015).
9. Lavrauw M., Zanella C.: Segre embeddings and finite semifields. Finite Fields Appl. **25**, 8–18 (2014).
10. Lavrauw M., Zanella C.: Subgeometries and linear sets on a projective line. Finite Fields Appl. **34**, 95–106 (2015).
11. Lavrauw M., Zanella C.: Subspaces intersecting each element of a regulus in one point, André-Bruck-Bose representation and clubs. arXiv:1409.1081.
12. Lidl R., Niederreiter H.: Finite Fields, 2nd edn. Cambridge University Press, Cambridge (1997).
13. Lunardon G.: Normal spreads. Geom. Dedicata **75**, 245–261 (1999).
14. Lunardon G., Marino G., Polverino O., Trombetti R.: Maximum scattered linear sets of pseudoregulus type and the Segre variety $\mathcal{S}_{n,n}$. J. Algebr. Comb. **39**, 807–831 (2014).
15. Lunardon G., Polverino O.: Translation ovoids of orthogonal polar spaces. Forum Math. **16**, 663–669 (2004).
16. Marino G., Polverino O., Trombetti R.: On $\mathbb{F}_q$-linear sets of PG(3, $q^3$) and semifields. J. Comb. Theory Ser. A **114**, 769–788 (2007).
17. Polverino O.: Linear sets in finite projective spaces. Discret. Math. **310**, 3096–3107 (2010).
18. Pott A.: Finite Geometry and Character Theory. Springer, Berlin (1995).