Maximum scattered linear sets and complete caps in Galois spaces*

Daniele Bartoli, Massimo Giulietti, Giuseppe Marino and Olga Polverino

Abstract

Explicit constructions of infinite families of scattered $\mathbb{F}_q$–linear sets in $PG(r-1,q^t)$ of maximal rank $\frac{rt}{2}$, for t even, are provided. When $q=2$ and r is odd, these linear sets correspond to complete caps in $AG(r,2^t)$ fixed by a translation group of size $2^{\frac{rt}{2}}$. The doubling construction applied to such caps gives complete caps in $AG(r+1,2^t)$ of size $2^{\frac{rt}{2}+1}$. For Galois spaces of even dimension greater than 2 and even square order, this solves the long-standing problem of establishing whether the theoretical lower bound for the size of a complete cap is substantially sharp.

Keywords: Galois spaces, linear sets, complete caps.

1 Introduction

Let $\Lambda = PG(V,\mathbb{F}_{q^t}) = PG(r-1,q^t)$, $q=p^h$, p prime, with V vector space of dimension r over $\mathbb{F}_{q^t}$, and let L be a set of points of Λ. The set L is said to be an $\mathbb{F}_q$–*linear* set of Λ of rank t if

*The research was supported by Ministry for Education, University and Research of Italy MIUR (Project PRIN 2012 ”Geometrie di Galois e strutture di incidenza”) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM)

it is defined by the non-zero vectors of an $\mathbb{F}_q$-vector subspace U of V of dimension t, i.e.

$$L = L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^t}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}.$$

We point out that different vector subspaces can define the same linear set. For this reason a linear set and the vector space defining it must be considered as coming in pair.

Let $\Omega = PG(W, \mathbb{F}_{q^t})$ be a subspace of Λ and let L_U be an $\mathbb{F}_q$-linear set of Λ. Then $\Omega \cap L_U$ is an $\mathbb{F}_q$–linear set of Ω defined by the $\mathbb{F}_q$–vector subspace $U \cap W$ and, if $dim_{\mathbb{F}_q}(W \cap U) = i$, we say that Ω has *weight* i in L_U. Hence a point of Λ belongs to L_U if and only if it has weight at least 1 and if L_U has rank k, then $|L_U| \leq q^{k-1} + q^{k-2} + \cdots + q + 1$. For further details on linear sets see [18], [11], [12], [13], [14].

An $\mathbb{F}_q$–linear set L_U of Λ of rank k is *scattered* if all of its points have weight 1, or equivalently, if L_U has maximum size $q^{k-1} + q^{k-2} + \cdots + q + 1$. A scattered $\mathbb{F}_q$–linear set of Λ of highest possible rank is a *maximum scattered* $\mathbb{F}_q$*–linear set* of Λ; see [3].

In [3] the authors obtain the following result on the rank of a maximum scattered linear set; see also [9].

Theorem 1.1. ([3, Thms 2.1, 4.3 and 4.2]) *If L_U is a maximum scattered $\mathbb{F}_q$-linear set of $PG(r-1, q^t)$ of rank k, then*

$$k = \frac{rt}{2} \quad \textit{if } r \textit{ is even,}$$
$$\frac{rt-t}{2} \leq k \leq \frac{rt}{2} \quad \textit{if } r \textit{ is odd.}$$

Also, if rt is even and L_U is a maximum scattered $\mathbb{F}_q$-linear set of $PG(r-1, q^t)$ of rank $\frac{rt}{2}$, then L_U is a two-intersection set (with respect to hyperplanes) in $PG(r-1, q^t)$ with intersection numbers $\theta_{\frac{rt}{2}-t-1}(q) = \frac{q^{\frac{rt}{2}-t}-1}{q-1}$ and $\theta_{\frac{rt}{2}-t}(q) = \frac{q^{\frac{rt}{2}-t+1}}{q-1}$.

When r is even there always exists an $\mathbb{F}_q$–scattered linear set of rank $\frac{rt}{2}$ in $PG(r-1, q^t)$ (see [9, Theorem 2.5.5] for an explicit example) whereas, when r is **odd**, the upper bound $\frac{rt}{2}$ is attained in the following cases:

- $r = 3$, $t = 2$ (Baer subplanes),
- $r = 3$, $t = 4$ ([2, Section 3]),
- $r > 3$, $t = 2$, $q = 2$ ([3, Thm. 4.4]),
- $r \geq 3$, $(t-1)|r$ (t even), $q > 2$ ([3, Thm. 4.4]).

This means that, for a given value of r, examples of maximum scattered linear sets have been shown to exist only for a small number of t's. It should be also noted that, differently from what happens for r even, in the case r odd the proof of Theorem 4.4 in [3] shows the existence of such maximum scattered linear sets without giving explicit examples.

In the first part of this paper we construct three different families of scattered $\mathbb{F}_q$–linear sets in $PG(2, q^t)$, $t \geq 4$ even, of rank $\frac{3t}{2}$, for infinite values of the prime power q. This allows us to produce for each integer $r \geq 5$, scattered $\mathbb{F}_q$–linear sets in $PG(r-1, q^t)$ of rank $\frac{rt}{2}$ (t even). More precisely we show that

Theorem 1.2. *There exist examples of scattered $\mathbb{F}_q$–linear sets in $PG(r-1, q^t)$, t even, of rank $\frac{rt}{2}$ in the following cases:*

- $q = 2$ *and* $t \geq 4$*;*
- $q \geq 2$ *and* $t \not\equiv 0 \mod 3$*;*
- $q \equiv 1 \mod 3$ *and* $t \equiv 0 \mod 3$*.*

In the second part of the paper we point out the relationship between maximum scattered linear sets and complete caps in affine spaces over finite fields of even characteristic. A cap in an affine or projective Galois space is a set of points no three of which collinear; a cap which is maximal with respect to set-theoretical inclusion is said to be complete. A long-standing issue in Finite Geometry is to ask for explicit constructions of small complete caps in Galois spaces. The trivial lower bound for the size of a complete cap in a Galois space of dimension n and order q is

$$\sqrt{2} \cdot \sqrt{q}^{n-1}. \tag{1}$$

If q is even and n is odd, such bound is substantially sharp: the existence of a complete cap of size $3q+2$ in $PG(3,q)$ was showed by Segre [19], whose construction was later generalized by Pambianco and Storme [17] to complete caps of size $2q^s$ in $AG(2s+1,q)$. Otherwise, all known infinite families of complete caps have size far from (1); see the survey paper [7]. Here we prove that (1) is essentially sharp also when $n \geq 4$ is even, provided that q is an even square.

Theorem 1.3. *Let $q = 2^t$, t even, and $n \geq 4$ even. Then there exists a complete cap in $AG(n,q)$ of size $2\sqrt{q}^{n-1}$.*

Theorem 1.3 relies on the fact that $\mathbb{F}_2$–linear sets in $PG(r-1,2^t)$ of maximal rank $\frac{rt}{2}$, for t even and r odd, naturally correspond to complete caps in $AG(r,2^t)$ fixed by a translation group of size $2^{\frac{rt}{2}}$. Then the scattered $\mathbb{F}_2$–linear sets of maximal rank described in this paper, together with the doubling construction for translation caps as described in [6], provide complete caps in $AG(r+1,q)$ of size $2q^{\frac{r}{2}}$, for $q = 2^t$. We point out that complete caps in the projective space $PG(r+1,q)$ with size of the same order of magnitude can also be constructed (see Remark 4.8).

2 Constructions of maximum scattered linear sets in $PG(2,q^{2n})$

In this section we want to construct infinite families of scattered $\mathbb{F}_q$–linear sets of rank $3n$ in the projective plane $PG(2,q^{2n})$, with $n \geq 2$. Note that, by Theorem 1.1, such scattered linear sets are two intersection sets (with respect to the lines) of the plane.

Consider the finite field $\mathbb{F}_{q^{6n}}$ as a 3–dimensional vector space over its subfield $\mathbb{F}_{q^{2n}}$, $n \geq 2$, and let $\mathbb{P} = PG(\mathbb{F}_{q^{6n}}, \mathbb{F}_{q^{2n}}) = PG(2,q^{2n})$ be the associated projective plane.

The following proposition can be easily verified.

Proposition 2.1. *Let $f : \mathbb{F}_{q^{3n}} \to \mathbb{F}_{q^{3n}}$ be an $\mathbb{F}_q$–linear map, ω an element of $\mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ and consider the subset of $\mathbb{F}_{q^{6n}}$*

$$U = \{f(x) + x\omega : \ x \in \mathbb{F}_{q^{3n}}\}$$

Then, the set

$$L_U = \{\langle f(x) + x\omega\rangle_{\mathbb{F}_{q^{2n}}} : \ x \in \mathbb{F}^*_{q^{3n}}\} \tag{2}$$

is an $\mathbb{F}_q$–linear of rank $3n$ of the projective plane $\mathbb{P} = PG(2, q^{2n})$. Also, put

$$Q_f := \left\{ \frac{f(x) + x\omega}{f(y) + y\omega} : \ x, y \in \mathbb{F}_{q^{3n}}, \ y \neq 0 \right\},$$

the set L_U turns out to be scattered if and only if $Q_f \cap \mathbb{F}_{q^{2n}} = \mathbb{F}_q$.

Proof. We first observe that $\{1, \omega\}$ is an $\mathbb{F}_{q^n}$–basis of $\mathbb{F}_{q^{2n}}$ and an $\mathbb{F}_{q^{3n}}$–basis of $\mathbb{F}_{q^{6n}}$, as well. Also, since f is an $\mathbb{F}_q$–linear map, the subset $U = \{f(x) + x\omega : \ x \in \mathbb{F}_{q^{3n}}\}$ of $\mathbb{F}_{q^{6n}}$ is closed under addition and $\mathbb{F}_q$–scalar multiplication, and hence it is an $\mathbb{F}_q$–vector subspace of $\mathbb{F}_{q^{6n}}$. This means that the set L_U turns out to be an $\mathbb{F}_q$–linear set of rank $3n$ of the plane $\mathbb{P}$. Also, L_U is not scattered if and only if there exists a point $P_x := \langle f(x) + x\omega\rangle_{\mathbb{F}_{q^{2n}}}$ of L_U, with $x \in \mathbb{F}^*_{q^{3n}}$, having weight grater than 1, and hence there exist $y \in \mathbb{F}^*_{q^{3n}}$ and $\lambda \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_q$ such that

$$f(x) + x\omega = \lambda(f(y) + y\omega). \tag{3}$$

The assertion follows. ∎

Let now

$$\omega^2 = A + B\omega, \tag{4}$$

with $A, B \in \mathbb{F}_{q^n}$ and $A \neq 0$, and suppose that there exist $x, y \in \mathbb{F}^*_{q^{3n}}$ and $\lambda \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_q$ satisfying Equation (3). Such an equation implies that

$$\left(\frac{f(x) + x\omega}{f(y) + y\omega}\right)^{q^{2n}} = \frac{f(x) + x\omega}{f(y) + y\omega},$$

i.e., taking (4) into account, we get

$$f(x)^{q^{2n}}f(y)+x^{q^{2n}}yA+(f(x)^{q^{2n}}y+f(y)x^{q^{2n}}+x^{q^{2n}}yB)\omega=$$

$$=f(y)^{q^{2n}}f(x)+y^{q^{2n}}xA+(f(y)^{q^{2n}}x+f(x)y^{q^{2n}}+y^{q^{2n}}xB)\omega.$$

Since $\{1,\omega\}$ is an $\mathbb{F}_{q^{3n}}$–basis of $\mathbb{F}_{q^{6n}}$, the above equality is equivalent to

$$\begin{cases} f(x)^{q^{2n}}f(y)-f(y)^{q^{2n}}f(x)=(xy^{q^{2n}}-yx^{q^{2n}})A \\ f(x)^{q^{2n}}y+f(y)x^{q^{2n}}-f(y)^{q^{2n}}x-f(x)y^{q^{2n}}=(xy^{q^{2n}}-yx^{q^{2n}})B \end{cases}.$$

The previous arguments allow us to reformulate the previous proposition in the following way which will be useful in the sequel.

Proposition 2.2. *Let $f:\mathbb{F}_{q^{3n}}\to\mathbb{F}_{q^{3n}}$ be an $\mathbb{F}_q$–linear map and ω an element of $\mathbb{F}_{q^{2n}}\setminus\mathbb{F}_{q^n}$ such that $\omega^2=A+B\omega$, with $A,B\in\mathbb{F}_{q^n}$ and $A\neq 0$. The set*

$$L_U=\{\langle f(x)+x\omega\rangle_{\mathbb{F}_{q^{2n}}}:\ x\in\mathbb{F}^*_{q^{3n}}\}$$

turns out to be a scattered $\mathbb{F}_q$–linear of rank $3n$ of the projective plane $\mathbb{P}=PG(2,q^{2n})$ if and only if for each pair $(x,y)\in\mathbb{F}^*_{q^{3n}}\times\mathbb{F}^*_{q^{3n}}$ satisfying the following equations

$$f(x)^{q^{2n}}f(y)-f(y)^{q^{2n}}f(x)=(xy^{q^{2n}}-yx^{q^{2n}})A \tag{5}$$

$$f(x)^{q^{2n}}y+f(y)x^{q^{2n}}-f(y)^{q^{2n}}x-f(x)y^{q^{2n}}=(xy^{q^{2n}}-yx^{q^{2n}})B, \tag{6}$$

the quotient

$$\lambda:=\frac{f(x)+x\omega}{f(y)+y\omega} \tag{7}$$

is an element of $\mathbb{F}^*_q$.

In the sequel we will exhibit examples of $\mathbb{F}_q$–linear maps of $\mathbb{F}_{q^{3n}}$ satisfying the previous properties. In particular, we face with the monomial and the binomial cases.

Monomial case: $f(x) := ax^{q^i}$, $a \in \mathbb{F}^*_{q^{3n}}$ **and** $1 \leq i \leq 3n-1$

In such a case we first show that for any value of $q \geq 2$, under suitable assumptions on $a \in \mathbb{F}^*_{q^{3n}}$ and on the integers i and n, we get a scattered $\mathbb{F}_q$–linear set of the projective plane $PG(2, q^{2n})$ of rank $3n$. Denoting by $N_{q^{3n}/q^3}(\cdot)$ the norm function from $\mathbb{F}_{q^{3n}}$ over $\mathbb{F}_{q^3}$, we have the following

Theorem 2.3. *For any prime power $q \geq 2$ and any integer $n \not\equiv 0 \bmod 3$, the set*

$$L_U = \{\langle ax^{q^i} + x\omega\rangle_{\mathbb{F}_{q^{2n}}} : x \in \mathbb{F}^*_{q^{3n}}\}$$

satisfying the following assumptions:

(*i*) $gcd(i, 2n) = 1$ *and* $gcd(i, 3n) = 3$

(*ii*) $N_{q^{3n}/q^3}(a) \notin \mathbb{F}_q$

is a scattered $\mathbb{F}_q$–linear set of the projective plane $PG(2, q^{2n})$ of rank $3n$.

Proof. By Proposition 2.2, in order to prove the statement we have first to determine the solutions $x, y \in \mathbb{F}^*_{q^{3n}}$ of Equations (5) and (6), where we have chosen $f(x) = ax^{q^i}$, with $a \in \mathbb{F}^*_{q^{3n}}$ and $1 \leq i \leq 3n-1$ and satisfying Conditions (*i*) and (*ii*). With these assumptions, Equations (5) and (6) become

$$a^{q^{2n}+1}(x^{q^{2n}}y - xy^{q^{2n}})^{q^i} = (xy^{q^{2n}} - yx^{q^{2n}})A \tag{8}$$

and

$$a^{q^{2n}}(x^{q^{2n+i}}y - xy^{q^{2n+i}}) + a(x^{q^{2n}}y^{q^i} - x^{q^i}y^{q^{2n}}) = (xy^{q^{2n}} - yx^{q^{2n}})B. \tag{9}$$

Let $s := xy^{q^{2n}} - yx^{q^{2n}}$. By (8), if $s \neq 0$, then s turns out to be a solution in $\mathbb{F}_{q^{3n}}$ of the equation

$$z^{q^i-1} = -\frac{A}{a^{q^{2n}+1}} \tag{10}$$

and, from Conditions (i), Equation (10) has solutions if and only if $N_{q^{3n}/q^3}\Big(-\frac{A}{a^{q^{2n}+1}}\Big) = 1$, namely

$$(-1)^n N_{q^{3n}/q^3}(A) = (N_{q^{3n}/q^3}(a))^{q+1} \qquad \text{if } 2n \equiv 1 \bmod 3 \tag{11}$$

or

$$(-1)^n N_{q^{3n}/q^3}(A) = (N_{q^{3n}/q^3}(a))^{q^2+1} \qquad \text{if } 2n \equiv -1 \bmod 3. \tag{12}$$

Since $A \in \mathbb{F}^*_{q^n}$ and since $n \not\equiv 0 \bmod 3$, we get $N_{q^{3n}/q^3}(A) \in \mathbb{F}_q$ and from Condition (ii) it follows that both Equations (11) and (12) cannot be satisfied. This means that $s = 0$ and hence $x = \alpha y$, for some $\alpha \in \mathbb{F}^*_{q^n}$. Substituting in (9), we get

$$(\alpha^{q^i} - \alpha)(a^{q^{2n}} y^{q^{2n+i}+1} - a y^{q^{2n}+q^i}) = 0. \tag{13}$$

If $\alpha^{q^i} \neq \alpha$, raising the previous equation to the q^n–th power, then

$$y^{(q^n-1)(q^i-1)} = a^{1-q^n},$$

i.e.

$$(a y^{q^i-1})^{q^n-1} = 1,$$

which is verified if and only if $y^{q^i-1} = \frac{\beta}{a}$, for some $\beta \in \mathbb{F}^*_{q^n}$. This means that $y \in \mathbb{F}^*_{q^{3n}}$ turns out to be a solution of the equation $z^{q^i-1} = \beta/a$ and, from Conditions (i), this happens if and only if

$$N_{q^{3n}/q^3}(\beta) = N_{q^{3n}/q^3}(a).$$

Since $\beta \in \mathbb{F}_{q^n}$, from Conditions (i) it follows $N_{q^{3n}/q^3}(\beta) \in \mathbb{F}^*_q$ and taking Condition (ii) into account, we get a contradiction. Hence the element $\alpha \in \mathbb{F}_{q^n}$ is such that $\alpha^{q^i} = \alpha$, and since $gcd(i,n) = 1$, we get $\alpha \in \mathbb{F}^*_q$. Substituting $x = \alpha y$ in (7) we get $\lambda = \alpha \in \mathbb{F}^*_q$, proving the assertion by Proposition 2.2. ■

Observe that the $3n$–dimensional $\mathbb{F}_q$–vector subspace U of $F_{q^{6n}}$ defining the linear set L_U of Theorem 2.3 is also an n–dimensional $\mathbb{F}_{q^3}$–vector subspace. In particular, when $n = 2$, U is a 2–dimensional $\mathbb{F}_{q^3}$–subspace of $\mathbb{F}_{q^{12}}$ and hence it can be always seen as the set of zeros of a polynomial

$$x^{q^6} + \alpha x^{q^3} + \beta x \in \mathbb{F}_{q^{12}}[x],$$

where $N_{q^{12}/q^3}(\beta) = 1$ and $\alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1}$; see [1]. Hence, the examples of scattered $\mathbb{F}_q$–linear sets of rank 6 constructed in $PG(2, q^4)$ by [2] belong to the family presented in Theorem 2.3.

Now, we will construct, for $q \equiv 1 \bmod 3$, another family of scattered $\mathbb{F}_q$–linear sets of $PG(2, q^{2n})$ of rank $3n$ defined by an $\mathbb{F}_q$–vector subspace which is not an $\mathbb{F}_{q^3}$–subspace. Indeed,

Theorem 2.4. *For any prime power $q \equiv 1 \bmod 3$ and any integer $n \geq 2$, the set*

$$L_U = \{\langle ax^{q^i} + x\omega\rangle_{\mathbb{F}_{q^{2n}}} : \ x \in \mathbb{F}^*_{q^{3n}}\}$$

satisfying the following assumptions

(I) $\quad gcd(i, 2n) = gcd(i, 3n) = 1,$

(II) $\quad \left(N_{q^{3n}/q}(a)\right)^{\frac{q-1}{3}} \neq 1$

is a scattered $\mathbb{F}_q$–linear set of the projective plane $PG(2, q^{2n})$ of rank $3n$.

Proof. The first part of the proof is the same as in Theorem 2.3. So, we have to determine the solutions $x, y \in \mathbb{F}^*_{q^{3n}}$ of Equations (8) and (9). Putting again $s := xy^{q^{2n}} - yx^{q^{2n}}$, if $s \neq 0$, from the previous equality, s turns out to be a solution in $\mathbb{F}^*_{q^{3n}}$ of (10) and, from Conditions (I). Equation (10) has solutions if and only if $N_{q^{3n}/q}\Big(-\frac{A}{a^{q^{2n}+1}}\Big) = 1$, namely

$$(N_{q^{3n}/q}(a))^2 = (-1)^n (N_{q^n/q}(A))^3, \tag{14}$$

implying

$$\left(\left(N_{q^{3n}/q}(a)\right)^{\frac{q-1}{3}}\right)^2 = (-1)^{\frac{n(q-1)}{3}}. \tag{15}$$

If $\frac{n(q-1)}{3}$ is even, Condition (II) implies that q is odd and $\left(N_{q^{3n}/q}(a)\right)^{\frac{q-1}{3}} = -1$, and raising this equality to the 3–rd power we get a contradiction. If $\frac{n(q-1)}{3}$ is odd, then q is even, and hence $\left(N_{q^{3n}/q}(a)\right)^{\frac{q-1}{3}} = 1$, again contradicting Condition (II). This means that $s = 0$ and hence $x = \alpha y$, for some $\alpha \in \mathbb{F}^*_{q^n}$, and arguing again as in the previous proof, if $\alpha^{q^i} \neq \alpha$, then $y \in \mathbb{F}^*_{q^{3n}}$ turns out to be a solution of the equation $z^{q^i-1} = \beta/a$, for some $\beta \in \mathbb{F}^*_{q^n}$. From Conditions (I), this happens if and only if

$$(N_{q^n/q}(\beta))^3 = N_{q^{3n}/q}(a),$$

which means that $N_{q^n/q}(\beta)$ is a solution in $\mathbb{F}^*_q$ of the equation $z^3 = N_{q^{3n}/q}(a)$, contradicting Condition (II). Hence the element $\alpha \in \mathbb{F}^*_{q^n}$ is such that $\alpha^{q^i} = \alpha$, and since $gcd(i,n) = 1$, we get $\alpha \in \mathbb{F}^*_q$, yielding as in the previous proof $\lambda \in \mathbb{F}^*_q$. By Proposition 2.2, we have the assertion. ■

Putting together Theorems 2.3 and 2.4 we get the following

Theorem 2.5.

- *If* $n \not\equiv 0 \bmod 3$, *there exist scattered* $\mathbb{F}_q$*–linear sets in* $PG(2, q^{2n})$ *of rank* $3n$ *for each prime power* $q \geq 2$.
- *If* $n \equiv 0 \bmod 3$, *there exist scattered* $\mathbb{F}_q$*–linear sets in* $PG(2, q^{2n})$ *of rank* $3n$ *for each prime power* $q \equiv 1 \bmod 3$.

Binomial case: $f(x) := ax^{q^i} + by^{q^j}$**,** $a, b \in \mathbb{F}^*_{q^{3n}}$ **and** $1 \leq i, j \leq 3n-1$

With this type of function it is clear that the linear set (2) has $\mathbb{F}_q$ as maximum subfield of linearity when $\gcd(i, j, 2n) = 1$. In particular we will study the case when $j = 2n + i$ and, obviously $\gcd(i, 2n) = 1$. First of all we need a technical lemma. Denoting by $Tr_{q^{3n}/q}(\cdot)$ the trace function from $\mathbb{F}_{q^{3n}}$ over $\mathbb{F}_q$, we can consider the non–degenerate symmetric bilinear form of $\mathbb{F}_{q^{3n}}$ over $\mathbb{F}_q$ defined by the following rule $< x, y >:= Tr_{q^{3n}/q}(xy)$. Then the adjoint map $\bar{\varphi}$

of an $\mathbb{F}_q$–linear map $\varphi(x)=\sum_{i=0}^{3n-1} a_i x^{q^i}$ of $\mathbb{F}_{q^{3n}}$ is $\bar{\varphi}(x)=\sum_{i=0}^{3n-1} a_i^{q^{3n-i}} x^{q^{3n-i}}$ (see e.g. [15, Sec. 2.2]). Now, we can prove the following

Lemma 2.6. *Let φ be an $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^{3n}}$ and $\bar{\varphi}$ the adjoint of φ with respect to the bilinear form $<,>$. Then the maps defined by $\varphi(x)/x$ and $\bar{\varphi}(x)/x$ have the same image.*

Proof. Let $\mathbb{V}=\mathbb{F}_{q^{3n}}\times\mathbb{F}_{q^{3n}}$ and let $\sigma:\mathbb{V}\times\mathbb{V}\longrightarrow\mathbb{F}_{q^{3n}}$ be the non-degenerate alternating bilinear form of $\mathbb{V}$ defined by $\sigma((x,y),(u,v))=xv-yu$. Then

$$\sigma'((x,y),(u,v))=Tr_{q^{3n}/q}(\sigma((x,y),(u,v)))$$

is a non-degenerate alternating bilinear form on $\mathbb{V}$, when $\mathbb{V}$ is regarded as a $6n$-dimensional vector space over $\mathbb{F}_q$. Let $\perp$ and $\perp'$ be the orthogonal complement maps defined by σ and σ' on the lattices of the $\mathbb{F}_{q^{3n}}$-subspaces and the $\mathbb{F}_q$-subspaces of $\mathbb{V}$, respectively. Recall that if W is an $\mathbb{F}_{q^{3n}}$-subspace of $\mathbb{V}$ and U is an $\mathbb{F}_q$-subspace of $\mathbb{V}$ then

$$dim_{\mathbb{F}_{q^{3n}}} W^{\perp}+dim_{\mathbb{F}_{q^{3n}}} W=2$$

and

$$\dim_{\mathbb{F}_q} U^{\perp'}+\dim_{\mathbb{F}_q} U=6n.$$

Also, it is easy to see that $W^{\perp}=W^{\perp'}$ for each $\mathbb{F}_{q^{3n}}$-subspace W of $\mathbb{V}$ and, since σ is an alternating form, if W is an 1-dimensional $\mathbb{F}_{q^{3n}}$-subspace of $\mathbb{V}$, then $W^{\perp}=W$. Let $U_\varphi=\{(x,\varphi(x)) : x\in F_{q^{3n}}\}$, where φ is an $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^{3n}}$. Then U_φ is a $3n$-dimensional $\mathbb{F}_q$-subspace of $\mathbb{V}$ and a direct calculation shows that $U_\varphi^{\perp'}=U_{\bar{\varphi}}$. Note that an element $t\in\mathbb{F}_{q^{3n}}$ belongs to the image of the map $\varphi(x)/x$ if and only if the point $P_t=\langle(1,t)\rangle_{\mathbb{F}_{q^{3n}}}$ of $PG(\mathbb{V},\mathbb{F}_{q^{3n}})=PG(1,q^{3n})$ belongs to the $\mathbb{F}_q$-linear set L_{U_φ}. Since $P_t^{\perp}=P_t^{\perp'}=P_t$, by using the Grassmann formula, we get

$$P_t\in L_{U_\varphi}\Leftrightarrow dim_{\mathbb{F}_q}(U_\varphi\cap P_t)\geq 1\Leftrightarrow dim_{\mathbb{F}_q}(U_\varphi^{\perp'}\cap P_t^{\perp'})\geq 1\Leftrightarrow dim_{\mathbb{F}_q}(U_{\bar{\varphi}}\cap P_t)\geq 1\Leftrightarrow P_t\in L_{U_{\bar{\varphi}}},$$

i.e., $t \in \mathbb{F}_{q^{3n}}$ belongs to the image of the map $\varphi(x)/x$ if and only if t belongs to the image of the map $\bar{\varphi}(x)/x$. ■

Now we can show the following result.

Proposition 2.7. *Let $f := f_{i,a,b} : x \in \mathbb{F}_{q^{3n}} \to ax^{q^i} + bx^{q^{2n+i}} \in \mathbb{F}_{q^{3n}}$, with $a, b \in \mathbb{F}^*_{q^{3n}}$ and $gcd(i, 2n) = 1$, and let ω be an element of $\mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ such that $\omega^2 = A + B\omega$, with $A, B \in \mathbb{F}_{q^n}$ and $A \neq 0$. If*

$$\frac{f_{i,a,b}(x)}{x} \notin \mathbb{F}_{q^n} \quad \textit{for each } x \in \mathbb{F}^*_{q^{3n}} \tag{16}$$

then the set

$$L_U = \{\langle f_{i,a,b}(x) + wx\rangle_{\mathbb{F}_{q^{2n}}} : x \in \mathbb{F}^*_{q^{3n}}\rangle$$

turns out to be a scattered $\mathbb{F}_q$–linear of rank $3n$ of the projective plane $\mathbb{P} = PG(\mathbb{F}_{q^{6n}}, \mathbb{F}_{q^{2n}}) = PG(2, q^{2n})$.

Proof. By Proposition 2.2, in order to prove the statement we have first to determine the solutions $x, y \in \mathbb{F}^*_{q^{3n}}$ of Equations (5) and (6), with $f(x) = f_{i,a,b}(x)$ fulfilling Condition (16). With this choice Equation (5) becomes

$$G(s) := b^{q^{2n}+1} s^{q^{2n+i}} - b^{q^{2n}} a s^{q^{n+i}} + a^{q^{2n}+1} s^{q^i} + As = 0,$$

where $s = xy^{q^{2n}} - yx^{q^{2n}}$. By (16), $f_{i,a,b}(x) \neq 0$ for each $x \in \mathbb{F}^*_{q^{3n}}$ and then $N_{q^{3n}/q^n}(a) \neq -N_{q^{3n}/q^n}(b)$. Hence $G(s) = 0$ if and only if $a^{q^n} G(s) + b^{q^{2n}} G(s)^{q^n} = 0$, i.e.

$$(N_{q^{3n}/q^n}(a) + N_{q^{3n}/q^n}(b)) s^{q^i} + A b^{q^{2n}} s^{q^n} + a^{q^n} As = 0. \tag{17}$$

Let $L := N_{q^{3n}/q^n}(a) + N_{q^{3n}/q^n}(b)$ and note that by (16) $L \neq 0$. This means that if s_0 is a non-zero solution of (17), then s_0 satisfies the following equation

$$\frac{b^{q^{2n-i}} s_0^{q^{n-i}} + a^{q^{n-i}} s_0^{q^{3n-i}}}{s_0} = \left(\frac{-L}{A}\right)^{q^{3n-i}},$$

i.e. there exists $s_0 \in \mathbb{F}^*_{q^{3n}}$ such that

$$\frac{f_{n-i,b^{q^{2n-i}},a^{q^{n-i}}}(s_0)}{s_0} \in \mathbb{F}_{q^n},$$

and hence

$$\left(\frac{f_{n-i,b^{q^{2n-i}},a^{q^{n-i}}}(s_0)}{s_0}\right)^{q^{2n}} = \frac{f_{n-i,b^{q^{n-i}},a^{q^{3n-i}}}(s_0^{q^{2n}})}{s_0^{q^{2n}}} \in \mathbb{F}_{q^n}.$$

Now, by Lemma 2.6 the maps $f_{i,a,b}(x)/x$ and $\bar{f}_{i,a,b}(x)/x$ have the same image and a direct calculation shows that

$$\bar{f}_{i,a,b} = f_{n-i,b^{q^{n-i}},a^{q^{3n-i}}},$$

hence by (16)

$$\frac{f_{n-i,b^{q^{n-i}},a^{q^{3n-i}}}(x)}{x} \notin \mathbb{F}_{q^n} \quad \text{for each } x \in \mathbb{F}^*_{q^{3n}}.$$

This means that Equation (17) only admits the zero solution, i.e. $s = xy^{q^{2n}} - yx^{q^{2n}} = 0$, which implies $x = \alpha y$ for some $\alpha \in \mathbb{F}^*_{q^n}$. Now, from Equation (6), substituting $f_{i,a,b}(x) = ax^{q^i} + bx^{q^{2n+i}}$ and $x = \alpha y$, we get

$$(\alpha^{q^i} - \alpha)(f_{i,a,b}(y)^{q^{2n}} y - f_{i,a,b}(y)y^{q^{2n}}) = 0.$$

If $\alpha^{q^i} \neq \alpha$, we get from the previous equation

$$f_{i,a,b}(y)^{q^{2n}} y = f_{i,a,b}(y)y^{q^{2n}}$$

for some $y \in \mathbb{F}^*_{q^{3n}}$, i.e. $f_{i,a,b}(y)/y \in \mathbb{F}_{q^n}$, a contradiction. Hence the element $\alpha \in \mathbb{F}^*_{q^n}$ is such that $\alpha^{q^i} = \alpha$, and since $gcd(i,n) = 1$, we get $\alpha \in \mathbb{F}^*_q$. As in Theorems 2.3 and 2.4, putting $x = \alpha y$, with $x, y \in \mathbb{F}^*_{q^{3n}}$ and $\alpha \in \mathbb{F}^*_q$ in (7) we get $\lambda = \alpha \in \mathbb{F}^*_q$, proving the assertion by Proposition 2.2. ■

In what follows we will prove that if $q = 2$, $i = 1$ and $a = 1$, then there exists at least an element $b \in \mathbb{F}^*_{q^{3n}}$ such that Condition (16) is satisfied. To this end we need the following preliminary result.

Lemma 2.8. *Set $n > 1$ and $q = 2$, consider the function $H(t) = (1-t)/t^j$ defined in $\mathbb{F}_{q^{3n}}^*$, where $j = \frac{q^{2n+1}-1}{q-1} = 2^{2n+1} - 1$. Then there exists at least an element $b \in \mathbb{F}_{2^{3n}}^*$ not in the image of H and such that $N_{2^{3n}/2^n}(b) \neq 1$.*

Proof. First of all notice that $\{H(t) \mid t \in \mathbb{F}_{2^{3n}}^*\} = \{t^m + t^{m-1} \mid t \in \mathbb{F}_{2^{3n}}^*\}$, with $m = 2^{3n} - j = 2^{3n} - 2^{2n+1} + 1$. The function $\theta : \mathbb{F}_{2^{3n}} \to \mathbb{F}_{2^{3n}}$, defined by $\theta(x) = x^{q^{n-1}}$, is an automorphism of $\mathbb{F}_{2^{3n}}$ and hence

$$N_{2^{3n}/2^n}(x) = 1 \iff N_{2^{3n}/2^n}(\theta(x)) = 1.$$

Therefore

$$\exists\, b \in \mathbb{F}_{2^{3n}}^* \;:\; b \notin Im(H),\; N_{2^{3n}/2^n}(b) \neq 1 \iff$$

$$\exists\, b \in \mathbb{F}_{2^{3n}}^* \;:\; b \notin Im(\theta \circ H),\; N_{2^{3n}/2^n}(b) \neq 1.$$

We have that

$$G(t) = (\theta \circ H)(t) = t^{(2^{3n}-2^{2n+1}+1)2^{n-1}} + t^{(2^{3n}-2^{2n+1})2^{n-1}} = t^{2^n-1} + t^{2^{n-1}-1}.$$

Since $n > 1$ and $G(0) = G(1) = 0$, $G(t)$ is not a permutation polynomial and it has degree $2^n - 1$. Then by [20], its value set has size at most $2^{3n} - \frac{2^{3n}-1}{2^n-1} = 2^{3n} - (2^{2n} + 2^n + 1)$. The number of elements of $\mathbb{F}_{2^{3n}}$ having norm over $\mathbb{F}_{2^n}$ equal to 1 is exactly $2^{2n} + 2^n + 1$. In the following we will prove that there exist at least $2^n + 2$ elements in the value set of G having norm over $\mathbb{F}_{2^n}$ equal to 1. Note that an element having norm equal to 1 has the form x^{2^n-1} for some $x \in \mathbb{F}_{2^{3n}}^*$. Consider the curve $\mathcal{C}$ defined by

$$f(x,y) = y^{2^n-1} + y^{2^{n-1}-1} + x^{2^n-1} = 0.$$

An affine $\mathbb{F}_{2^{3n}}$-rational point of $\mathcal{C}$ having $x, y \neq 0$ corresponds to an element $b = x^{2^n-1}$ belonging to the image of G such that $N_{2^{3n}/2^n}(b) = 1$. Intersecting the curve $\mathcal{C}$ with the lines $\ell_t : x = ty$ we get that the coordinates of the $\mathbb{F}_{2^{3n}}$-rational points of $\mathcal{C}$ having $x, y \neq 0$ are of the form

$$x = \frac{t}{(t^{2^n-1}-1)^{2^{2n+1}}} \qquad y = \frac{1}{(t^{2^n-1}-1)^{2^{2n+1}}},$$

where $t \in \mathbb{F}_{2^{3n}} \setminus \mathbb{F}_{2^n}$. Hence $\mathcal{C}$ has exactly

$$2^{3n} - 2^n$$

affine $\mathbb{F}_{2^{3n}}$-rational points not lying on the two axes. Now, since the same value of $x_0^{2^n-1}$ is obtained $2^n - 1$ times and since on the vertical line $x = x_0$ the curve $\mathcal{C}$ has at most $2^n - 1$ points, we have that the same element in the image of G, with norm 1, can be obtained from at most $(2^n - 1)^2$ points of $\mathcal{C}$. Then there are at least

$$\frac{2^{3n} - 2^n}{(2^n - 1)^2} > 2^n + 2$$

elements in the image of G having norm equal to 1. This proves that there exists at least an element $b \in \mathbb{F}_{2^{3n}}^*$ not in the image of H and of norm different from 1. ■

Now, we are able to prove

Proposition 2.9. *Let $f_{i,a,b}$ be the $\mathbb{F}_q$–linear map of $\mathbb{F}_{q^{3n}}$ as defined in Proposition 2.7 and put $i = a = 1$. If $q = 2$, there exists at least one element $b \in \mathbb{F}_{2^{3n}}^*$ such that*

$$\frac{f_{1,1,b}(x)}{x} \notin \mathbb{F}_{2^n} \quad \textit{for each } x \in \mathbb{F}_{2^{3n}}^*. \tag{18}$$

Proof. Taking $q = 2$ and $i = a = 1$ in $f_{i,a,b}(x) = ax^{2^i} + bx^{2^{2n+i}}$, Condition (18) reads

$$\frac{x^2 + bx^{2^{2n+1}}}{x} = x + bx^{2^{2n+1}-1} \notin \mathbb{F}_{2^n} \quad \text{for each } x \in \mathbb{F}_{2^{3n}}^*. \tag{19}$$

Let $g(x) := \frac{f_{1,1,b}(x)}{x} = x + bx^{2^{2n+1}-1}$ for each $x \in \mathbb{F}_{2^{3n}}^*$. Note that since $g(\eta x) = \eta g(x)$ for each $\eta \in \mathbb{F}_{q^n}$, Condition (19) is satisfied if $g(x) \neq 0$ and $g(x) \neq 1$ for each $x \in \mathbb{F}_{2^{3n}}^*$. If there is an element $x_0 \in \mathbb{F}_{q^{3n}}^*$ such that $g(x_0) = 1$, then the corresponding b belongs to the image of the function H defined in Lemma 2.8. If there is an element $x_0 \in \mathbb{F}_{q^{3n}}^*$ such that $g(x_0) = 0$, then the corresponding b has norm equal to 1. By Lemma 2.8 there is an element $b_0 \in \mathbb{F}_{2^{3n}}^*$ not belonging to the image of H and having norm different from 1. This implies that Condition (19), for b_0, is satisfied and hence $f_{1,1,b_0}$ satisfies Condition (18). ■

Putting together Propositions 2.7 and 2.9 we get the following

Theorem 2.10. *For each integer $n > 1$, the set*

$$L_U = \{\langle x^2 + bx^{2^{2n+1}} + x\omega\rangle_{\mathbb{F}_{2^{2n}}} : \ x \in \mathbb{F}^*_{2^{3n}}\},$$

where $b \in \mathbb{F}^*_{2^{3n}}$ with $N_{2^{3n}/2^n}(b) \neq 1$ and such that

$$x + bx^{2^{2n+1}-1} \notin \mathbb{F}_{2^n} \quad \textit{for each } x \in \mathbb{F}^*_{2^{3n}}$$

is a scattered $\mathbb{F}_2$–linear set of the projective plane $PG(2, 2^{2n})$ of rank $3n$.

Remark 2.11. MAGMA computational results show that for $n = 3$ and $q \in \{3, 4, 5\}$ there exist elements $b \in \mathbb{F}^*_{q^{3n}}$ for which the functions $f_{1,1,b}$ satisfy Condition (18) yielding $\mathbb{F}_q$–scattered linear sets in $PG(2, q^6)$, $q \in \{3, 4, 5\}$, of rank 9. However, taking Theorems 2.5 and 2.10 into account, the existence of a family of scattered $\mathbb{F}_q$–linear sets in $PG(2, q^{2n})$ for each $n \equiv 0 \bmod 3$, $q \not\equiv 1 \bmod 3$ and $q > 2$, remains an open problem.

3 Constructions in $PG(r-1, q^t)$

First of all we prove the following

Theorem 3.1. *Let $\mathbb{P} = PG(\mathbb{V}, F_{q^t}) = PG(r-1, q^t)$ be a projective space and let*

$$\mathbb{V} = V_1 \oplus_{\mathbb{F}_{q^t}} \cdots \oplus_{\mathbb{F}_{q^t}} V_m, \tag{20}$$

with $\dim V_i = s_i \geq 2$ and $i \in \{1, \ldots, m\}$. If L_{U_i} is a scattered $\mathbb{F}_q$–linear set of $PG(V_i, \mathbb{F}_{q^t}) = PG(s_i - 1, q^t)$ then L_W, where

$$W = U_1 \oplus_{\mathbb{F}_q} \cdots \oplus_{\mathbb{F}_q} U_m, \tag{21}$$

is a scattered $\mathbb{F}_q$–linear set of $\mathbb{P}$.

Also, L_W has maximum rank $\frac{rt}{2}$ if and only if each L_{U_i} has maximum rank $\frac{s_i t}{2}$.

Proof. Let k_i be the rank of L_{U_i}. By Theorem 1.1 $k_i \leq \frac{s_i t}{2}$ for each $i \in \{1, \ldots, m\}$. It is clear that L_W is an $\mathbb{F}_q$–linear set of $\mathbb{P}$ of rank $\sum_{i=1}^m k_i \leq \sum_{i=1}^m \frac{s_i t}{2} = \frac{rt}{2}$. If $P := \langle \underline{w} \rangle$ is a point of L_W with weight grater than 1, then there exist $\underline{w}' \in W$, $\underline{w}' \neq \underline{0}$, and $\lambda \in \mathbb{F}_{q^t} \setminus \mathbb{F}_q$ such that $\underline{w} = \lambda \underline{w}'$. By (21), the vectors $\underline{w}$ and $\underline{w}'$ can be uniquely written as

$$\underline{w} = \underline{u}_1 + \cdots + \underline{u}_m \quad \text{and} \quad \underline{w}' = \underline{u}'_1 + \cdots + \underline{u}'_m,$$

where $\underline{u}_i, \underline{u}'_i \in U_i$ for each $i \in \{1, \ldots, m\}$. Taking $\underline{w} = \lambda \underline{w}'$ and (20) into account, from the previous equalities we get $\underline{u}_i = \lambda \underline{u}'_i$ for each $i \in \{1, \ldots, m\}$. Suppose that $j \in \{1, \ldots, m\}$ is the smallest number such that $\underline{u}_j \neq \underline{0}$. Then $\underline{u}_j = \lambda \underline{u}'_j$, with $\underline{u}_j \in U_j$, and since L_{U_j} is scattered we get $\lambda \in \mathbb{F}_q^*$, a contradiction. The last part is obvious. ∎

The previous theorem can be naturally applied when r is even by considering scattered $\mathbb{F}_q$–linear sets of rank t on $\frac{r}{2}$ lines, say ℓ_i, spanning the whole space $PG(r-1, q^t)$. In such a way we get a scattered $\mathbb{F}_q$–linear set in $PG(r-1, q^t)$ of rank $\frac{rt}{2}$. We will call this construction of *type* $(C1)$. Some scattered linear sets reflecting this construction are those called *of pseudoregulus type* (see [13, Definitions 3.1 and 4.1]), for which each scattered linear set on ℓ_i is of pseudoregulus type (see [13, Remark 4.5]). Linear sets of pseudoregulus type have been also studied in [16], [10], [12] and to this family belongs the first explicit example of scattered linear sets obtained by Construction $(C1)$ (see proof of [9, Thm. 2.5.5]). Also, from [13, Example 4.6 (i) and (ii)] it is clear that, by using Construction $(C1)$, we can also obtain scattered linear sets in $PG(r-1, q^t)$, r even, of rank $\frac{rt}{2}$ which are not of pseudoregulus type.

Proof of Theorem 1.2

Putting together Theorems 2.3, 2.4 and 2.10 and Theorem 3.1, it follows that when t is even and $r \geq 5$ we have several ways to construct scattered $\mathbb{F}_q$–linear sets in $PG(\mathbb{V}, F_{q^t}) = PG(r-1, q^t)$ of rank $\frac{rt}{2}$, by decomposing $\mathbb{V}$ as a direct sum over $\mathbb{F}_{q^t}$ of vector spaces of dimension 2 and 3, proving in this way Theorem 1.2. Obviously, the greater is the integer r, the wider are these possible constructions.

Remark 3.2. From Theorem 1.1, each scattered $\mathbb{F}_q$-linear set of $PG(r-1, q^{2n})$ of rank rn is a two–intersection set of the space with respect to the hyperplanes with intersection numbers $\theta_{(r-2)n-1}(q) = \frac{q^{(r-2)n}-1}{q-1}$ and $\theta_{(r-2)n}(q) = \frac{q^{(r-2)n+1}-1}{q-1}$. Then, L_U is a $\theta_{(r-2)n-1}(q)$*–fold blocking set* (with respect to hyperplanes) in $PG(r-1, q^{2n})$ ([3, Thm. 6.1]) and gives to rise two-weight linear codes and strongly regular graphs (see [5] and [3, Sec. 5]). As observed in [4], we want to stress that the parameters of these two–intersection sets are not new. Indeed, sets with the same parameters can be obtained by taking the disjoint union of $\frac{q^n-1}{q-1}$ Baer subgeometries in $PG(r-1, q^{2n})$ isomorphic to $PG(r-1, q^n)$. This set is called *of type I* in [4]. Also in [4, Thm. 2.2], the authors show that a scattered $\mathbb{F}_q$–linear set of maximum rank cannot contain any Baer subgeometry of $PG(r-1, q^{2n})$ and hence the corresponding two–intersection set is not isomorphic to a set of type I.

4 Small complete caps from maximum scattered linear sets

Many links between the theory of linear sets and a large number of geometrical objects are known. Among them, two-intersection sets, blocking sets or multiple blocking sets, translation ovoids of polar spaces, translation spreads of the Cayley Generalized Hexagon $H(q)$. Also, linear sets are widely used in the construction of finite semifields. In this section we describe a connection between F_2–linear sets and another classical object in Finite Geometry: complete caps in Galois spaces. Such a connection is indeed fruitful; in fact, the results of the previous section on F_2–linear sets provide a solution, for spaces of even square order, to the long-standing problem of establishing whether the theoretical lower bound for the size of a complete cap is substantially sharp.

We first recall a Definition from [6, Sec. 2].

Definition 4.1. *Let $q = 2^t$ and let G be an additive subgroup of $\mathbb{F}_q^r$. Let*

$$\mathcal{K}_G := \{P_v \mid v \in G\} \subset AG(r, q),$$

where P_v is the affine point with coordinates $(a_1, a_2, \ldots, a_r)$ corresponding to the vector $v = (a_1, a_2, \ldots, a_r) \in \mathbb{F}_q^r$. A translation cap *is a cap in $AG(r, q)$ which coincides with $\mathcal{K}_G$ for some additive subgroup G of $\mathbb{F}_q^r$.*

Translation caps can be characterized as follows.

Theorem 4.2. [6, Lemma 2.1] *For an additive subgroup G of $\mathbb{F}_q^r$, q even, the set K_G is a translation cap if and only if any two non-zero distinct vectors in G are $\mathbb{F}_q$-linearly independent.*

Proposition 4.3. *An $\mathbb{F}_2$–scattered linear set in $PG(r-1, 2^t)$, $t > 1$, corresponds to a translation cap in $AG(r, 2^t)$ and viceversa.*

Proof. Let U be an $\mathbb{F}_2$-vector subspace of $V = \mathbb{F}_{2^t}^r$, $t > 1$, corresponding to the scattered linear set L_U in $PG(V, \mathbb{F}_{2^t})$. Since U in an additive subgroup of V, by Theorem 4.2, $\mathcal{K}_U$ is a translation cap if and only if there no two distinct vectors in U are $\mathbb{F}_{2^t}$-linearly dependent. This happens if and only all the elements of U correspond to distinct points of L_U, that is L_U is a scattered $\mathbb{F}_2$–linear set. ■

Let $\mathcal{SL}$ and $\mathcal{TC}$ be the sets of all the scattered linear sets in $PG(r-1, 2^t)$ and all the translation caps in $AG(r, 2^t)$. Form the previous theorem we can deduce the existence of a bijective function

$$\varphi : \mathcal{SL} \to \mathcal{TC}$$

which sends L_U to $\varphi(L_U) = \mathcal{K}_U$ for each $\mathbb{F}_2$-vector subspace U of $V = \mathbb{F}_{2^t}^r$.

Proposition 4.4. *Let U_1 and U_2 such that $\mathcal{K}_{U_1}$ and $\mathcal{K}_{U_2}$ are equivalent under the action of $A\Gamma L(r, 2^t)$. Then $\varphi^{-1}(\mathcal{K}_{U_1})$ and $\varphi^{-1}(\mathcal{K}_{U_2})$ are equivalent under the action of $P\Gamma L(r, 2^t)$.*

Proof. Let $f \in A\Gamma L(r, 2^t)$ be such that $f(\mathcal{K}_{U_1}) = \mathcal{K}_{U_2}$. Then f contains no translations, since it has to fix the 0-vector. Then $f = M\tau$ with $M \in GL(r, 2^t)$ and $\tau \in Aut(\mathbb{F}_{2^t})$. Let

$$\mathcal{K}_{U_1} = \{0, P_1, P_2, \dots, P_n\}, \qquad \mathcal{K}_{U_2} = \{0, Q_1, Q_2, \dots, Q_n\},$$

with $f(0) = 0$ and $f(P_i) = Q_i$. Also, let $\varphi^{-1}(\mathcal{K}_{U_1}) = \{\widetilde{P}_1, \widetilde{P}_2, \dots, \widetilde{P}_n\}$ and $\varphi^{-1}(\mathcal{K}_{U_2}) = \{\widetilde{Q}_1, \widetilde{Q}_2, \dots, \widetilde{Q}_n\}$, with $\widetilde{P}_i = \lambda_i P_i$, $\widetilde{Q}_i = \mu_i Q_i$ and $\lambda_i, \mu_i \neq 0$ for all $i = 1, \dots, n$. Consider $g = \frac{1}{\det(M)} M\tau \in P\Gamma L(r, 2^h)$. Then

$$g(\widetilde{P}_i) = \left(\frac{1}{\det(M)} M\tau\right)(\widetilde{P}_i) = \left(\frac{1}{\det(M)} M\tau\right)(\lambda_i P_i) =$$

$$= \frac{\tau(\lambda_i)}{\det(M)} (M\tau)(P_i) = \frac{\tau(\lambda_i)}{\det(M)} Q_i = \frac{\tau(\lambda_i)}{\mu_i \det(M)} \widetilde{Q}_i.$$

Then g sends $\widetilde{P}_i$ to $\widetilde{Q}_i$ and $\varphi^{-1}(\mathcal{K}_{U_1})$ is projectively equivalent to $\varphi^{-1}(\mathcal{K}_{U_2})$. ■

By [6, Proposition 2.5] the maximum size of a translation cap in $AG(r, q)$, $q = 2^t$ and $t > 1$, is $q^{\frac{r}{2}}$; if the bound is attained then the cap is said to be a *maximal* translation cap. We recall two further results from [6].

Lemma 4.5. [6, Proposition 2.8] *If $\mathcal{K}_G$ is a maximal translation cap in $AG(r, 2^t)$, and $\mathcal{K}_H$ a maximal translation cap in $AG(\overline{r}, 2^t)$, then $\mathcal{K}_G \times \mathcal{K}_H$ is a maximal translation cap in $AG(r+\overline{r}, 2^t)$.*

Lemma 4.6. (Doubling construction) [6, Corollary 2.12] *If $\mathcal{K}_G$ is a maximal translation cap in $AG(r, 2^t)$, then $\mathcal{K}_{G\times\{0,1\}}$ is a complete cap in $AG(r+1, 2^t)$.*

We are now in a position to prove the key result of this section.

Proposition 4.7. *Let $q = 2^t$, t even, and $n \geq 4$ even. If there exists a maximum scattered linear set in $PG(2, q)$, then there exists a complete cap in $AG(n, q)$ with size $2q^{\frac{n-1}{2}}$.*

Proof. Let L be a maximum scattered $\mathbb{F}_2$–linear set of $PG(2, 2^t)$. Since t is even it has rank $\frac{3t}{2}$. By Proposition 4.3 it is equivalent to a translation cap $\mathcal{K}$ in $AG(3, 2^t)$ of size $2^{\frac{3t}{2}} = \sqrt{q}^3$. Since the upper bound of [6, Proposition 2.5] is attained, $\mathcal{K}$ is a maximal translation cap in $AG(3,2^t)$. Let $n \geq 4$ even and consider in $AG(n-1,2^t)$ the following cap of size $q^{\frac{n-1}{2}}$:

$$\overline{\mathcal{K}} = \left\{ \left(a,b,c,x_1,x_1^2,x_2,x_2^2,\ldots,x_{\frac{n-4}{2}},x_{\frac{n-4}{2}}^2\right) : (a,b,c) \in \mathcal{K}, x_i \in \mathbb{F}_{2^t} \right\}.$$

By Lemma 4.5, together with the fact that $\{(x,x^2) : x \in \mathbb{F}_{2^t})\}$ is a translation cap in $AG(2,2^t)$, $\overline{\mathcal{K}}$ is a maximal translation cap in $AG(n-1,2^t)$. Now the cap

$$\overline{\overline{\mathcal{K}}} = \left\{(a_1,\ldots,a_{n-1},0) : (a_1,\ldots,a_{n-1}) \in \overline{\mathcal{K}}\right\} \cup \left\{(a_1,\ldots,a_{n-1},1) : (a_1,\ldots,a_{n-1}) \in \overline{\mathcal{K}}\right\}$$

is a complete translation cap in $AG(n,2^t)$ of size $2q^{\frac{n-1}{2}}$ by Lemma 4.6. ■

The existence of a complete cap in $AG(n,q)$ of size $2q^{\frac{n-1}{2}}$, for $n \geq 4$ even and q an even square, now follows from Theorems 2.3, 2.4, 2.10 and Proposition 4.7. Theorem 1.3 in Introduction is then proved.

Remark 4.8. For q an even square and $n \geq 4$ even, the trivial lower bound for complete caps is substantially sharp not only in the affine space $AG(n,q)$ but also in the projective space $PG(n,q)$. In fact, it is possible to show that in $PG(2k+4,q)$, $k \geq 0$ there exists a complete cap of size at most $3q^{k+\frac{3}{2}} + 4q^{k+1} + 3\frac{q^{k+1}-1}{q-1}$ containing the translation cap of size $2q^{k+\frac{3}{2}}$ obtained in Theorem 1.3. The lengthy and technical proof is similar to those of [6, Theorem 4.7] and [8, Propositions 2.5 and 5.3], where a complete translation cap in $AG(n,q)$ is extended to a complete cap in $PG(n,q)$.

References

[1] S. Ball: Polynomials in finite geoemtries, in "Surveys in Combinatorics 1999" (J.D. Lamb and D.A. Preece, Eds), London Math. Soc. Lectures Note Series, Vol. 267, pp. 17–35, Cambridge Univ. Press, Cambridge, UK, 1999.

[2] S. Ball, A. Blokhuis and M. Lavrauw: Linear $(q+1)$-fold blocking sets in $PG(2,q^4)$, *Finite Fields Appl.* **6** n. 4 (2000), 294–301.

[3] A. Blokhuis and M. Lavrauw: Scattered spaces with respect to a spread in $PG(n,q)$, *Geom. Dedicata* **81** No.1–3 (2000), 231–243.

[4] A. Blokhuis and M. Lavrauw: On two-intersection sets with respect to hyperplanes in projective spaces, *J. Comb. Theory, Ser. A*, **99** No.2 (2002), 377–382.

[5] R. Calderbank and W.M. Kantor: The geometry of two-weight codes, *Bull. London Math. Soc.* **18** (1986), 97–122.

[6] M. Giulietti: Small complete caps in PG(N,q), q even, *Journal of Combinatorial Designs* **15**(5) (2007), 420–436.

[7] M. Giulietti: The geometry of covering codes: small complete caps and saturating sets in Galois spaces, in *Surveys in Combinatorics 2013 - London Mathematical Society Lecture Note Series* **409**, Cambridge University Press, 2013, pp. 51–90.

[8] M. Giulietti and F. Pasticci: Quasi-Perfect Linear Codes with Minimum Distance 4, *IEEE Transactions on Information Theory* **53**(5) (2007), 1928–1935.

[9] M. Lavrauw: *Scattered Spaces with respect to Spreads and Eggs in Finite Projective Spaces*, Ph.D. Thesis, 2001.

[10] M. Lavrauw, G. Marino, O. Polverino and R. Trombetti: $\mathbb{F}_q$–pseudoreguli of $PG(3,q^3)$ and scattered semifields of order q^6, *Finite Fields Appl.*, **17** (2011), 225–239.

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

[12] M. Lavrauw and G. Van de Voorde: Scattered linear sets and pseudoreguli, *The Electronic Journal of Comb.* **20**(1) (2013).

[13] G. Lunardon, G. Marino, O. Polverino and R. Trombetti: Maximum scattered linear sets of pseudoregulus type and the Segre Variety $\mathcal{S}_{n,n}$, *J. Algebr. Comb.*, **39** (2014), 807-831.

[14] G. Lunardon and O. Polverino: Translation ovoids of orthogonal polar spaces, *Forum Math.*, **16** (2004), 663–66.

[15] G. Marino and O. Polverino: *On the nuclei of a finite semifield*. Theory and applications of finite fields, Contemp. Math., **579**, Amer. Math. Soc., Providence, RI (2012), 123-141.

[16] G. Marino, O. Polverino and R. Trombetti: On $\mathbb{F}_q$–linear sets of $PG(3, q^3)$ and semifields, *J. Combin. Theory Ser. A* **114** (2007), 769–788.

[17] F. Pambianco and L. Storme: Small complete caps in spaces of even characteristic, *J. Combin. Theory Ser. A* **75**(1) (1996), 70–84.

[18] O. Polverino: Linear sets in Finite Projective Spaces, *Discrete Math.*, **310** (2010), 3096–3107.

[19] B. Segre: On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two, *Acta Arith.*, **5** (1959), 315–332.

[20] G. Turnwald: A new criterion for permutation polynomials, *Finite Fields Appl.* **1** (1995), 64–82.

Daniele Bartoli and Massimo Giulietti

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia,

I–06123 Perugia, Italy

daniele.bartoli@unipg.it, *massimo.giulietti@unipg.it*

Giuseppe Marino and Olga Polverino

Dipartimento di Matematica e Fisica,

Seconda Università degli Studi di Napoli,

I–81100 Caserta, Italy

giuseppe.marino@unina2.it, *olga.polverino@unina2.it*