J Algebr Comb (2007) 25:149–168
DOI 10.1007/s10801-006-0029-0

Small complete caps in Galois affine spaces

Massimo Giulietti

Received: 19 December 2005 / Accepted: 5 July 2006 /
Published online: 18 August 2006

Abstract Some new families of caps in Galois affine spaces $AG(N, q)$ of dimension $N \equiv 0 \pmod 4$ and odd order q are constructed. Such caps are proven to be complete by using some new ideas depending on the concept of a regular point with respect to a complete plane arc. As a corollary, an improvement on the currently known upper bounds on the size of the smallest complete caps in $AG(N, q)$ is obtained.

Keywords Affine space · Complete cap · Complete arc

1. Introduction

A k-cap in $AG(N, q)$, the affine N-dimensional space over the finite field with q elements $\mathbb{F}_q$, is a set of k points no three of which are collinear. A k-cap is said to be complete if it is not contained in a $(k + 1)$-cap. A k-cap in $AG(2, q)$ is also called a k-arc.

The central problem on caps is determining the maximal and minimal sizes of complete caps in a given space, see the survey papers [1, 13] and the references therein. As the only complete cap in $AG(N, 2)$ is the whole $AG(N, 2)$, from now on we assume $q > 2$. For the size $t_2(AG(N, q))$ of the smallest complete cap in $AG(N, q)$, the trivial lower bound is $t_2(AG(N, q)) > \sqrt{2}q^{\frac{N-1}{2}}$. Unlike the even order case, where for every dimension $N \geq 3$ there exist complete caps in $AG(N, q)$ with less than $q^{\frac{N}{2}}$ points ([9, 10, 16, 17], see Remark 1.5), for q odd complete k-caps in $AG(N, q)$ with $k \leq q^{\frac{N}{2}}$ are known to exist only for $N \equiv 2 \pmod 4$ and for small values of N and q

This research was performed within the activity of GNSAGA of the Italian INDAM, with the financial support of the Italian Ministry MIUR, project "Strutture geometriche, combinatorica e loro applicazioni", PRIN 2004–2005.

M. Giulietti (✉)
Dipartimento di Matematica e Informatica, Università di Perugia, 06123, Italy
e-mail: giuliet@dipmat.unipg.it

([2, 6, 7, 8, 15], see Remark 1.5). The aim of this paper is to describe small complete caps in $AG(N,q)$ with q odd and $N \equiv 0 \pmod 4$. Our results are summarized in the following theorems.

Theorem 1.1. *Let q be odd and $s \geq 1$. For any k for which there exists a complete k-cap in $AG(s,q)$, there also exists a complete $(q^{2s}k)$-cap in $AG(4s,q)$.*

The proof of Theorem 1.1 is constructive. First, certain q^{2s}-caps in $AG(4s,q)$ are constructed by using an idea of Davydov and Östergård [8]. Then, k copies of such caps are put together in a proper way in order to obtain complete $(q^{2s}k)$-caps.

Theorem 1.2. *Let q be odd and $s \geq 1$.*
(A) *If $q > 5$, then there exists a complete cap of size $q^{2s-1}(q+2)$ in $AG(4s,q)$.*
(B) *If $q > 13$, then there exists a complete cap of size q^{2s} in $AG(4s,q)$.*
(C) *If $q > 76^2$, then there exists a complete cap of size $\frac{1}{2}(q^{2s} - 3q^{2s-1})$ in $AG(4s,q)$.*

It should be noted that the caps in Theorem 1.2 are constructed by the known *cartesian product* method, see [1, Theorem 4]. However, the proof of their completeness needs some new ideas depending on the concept of a regular point with respect to a complete arc in $AG(2,q)$, see Proposition 4.2, which can be viewed as an extension of the concept of a regular point with respect to a conic due to Segre [18].

Theorem 1.2 has the following corollary.

Corollary 1.3. *If q is odd, $q > 13$, and $N \equiv 0 \pmod 4$, then*

$$t_2(AG(N,q)) \leq q^{\frac{N}{2}}.$$

If, in addition, $q > 76^2$ then

$$t_2(AG(N,q)) \leq \frac{1}{2}\left(q^{\frac{N}{2}} - 3q^{\frac{N}{2}-1}\right).$$

Results on complete caps in projective spaces can be deduced from results on complete caps in affine spaces, and conversely. Let $PG(N,q)$ be the projective N-dimensional space over $\mathbb{F}_q$; also let $t_2(N,q)$ be the minimum size of a complete cap in $PG(N,q)$, and $m_2(N,q)$ be the maximum size of a complete cap in $PG(N,q)$. For any hyperplane $\mathcal{H}_\infty$ of $PG(N,q)$, the affine space obtained by removing the points of $\mathcal{H}_\infty$ is isomorphic to $AG(N,q)$. A complete k-cap K in $PG(N,q)$ can then be viewed as a complete cap in $AG(N,q)$, provided that there exists a hyperplane containing no point of K. Conversely, for any embedding of $AG(N,q)$ in $PG(N,q)$, it is always possible to obtain a complete cap in $PG(N,q)$ from a complete cap of $AG(N,q)$ by adding some points on the hyperplane at infinity. Therefore $t_2(N,q) \leq t_2(AG(N,q)) + m_2(N-1,q)$. The following bounds then follow from (B) and (C) of Theorem 1.2.

Corollary 1.4. *Let $t_2(N,q)$ be the minimum size of a complete cap in $PG(N,q)$. Let $m_2(N-1,q)$ be the maximum size of a complete cap in $PG(N-1,q)$. Assume q is odd and $N \equiv 0 \pmod 4$.*
- *If $q > 13$, then $t_2(N,q) \le q^{\frac{N}{2}} + m_2(N-1,q)$.*
- *If $q > 76^2$, then $t_2(N,q) \le \frac{1}{2}(q^{\frac{N}{2}} - 3q^{\frac{N}{2}-1}) + m_2(N-1,q)$.*

In particular,
- *if $q > 13$, then $t_2(4,q) \le 2q^2 + 1$;*
- *if $q > 76^2$, then $t_2(4,q) \le \frac{3}{2}q^2 - \frac{3}{2}q + 1$.*

Note that the bound $t_2(4,q) \le 2q^2 + 1$ is a new result for $q > 17$, as smaller complete caps in $PG(4,q)$ are known for $q \in \{7, 9, 11, 13, 17\}$ (see [6, Table 4]).

Finally, it should be noted that the problem of determining the minimun size of a complete cap in a given space is of particular interest in Coding Theory, see e.g. the survey paper [13]. In Section 6 some features of the linear codes associated to the caps presented in this paper are considered.

Remark 1.5. A computer search has shown that for each of the caps in $PG(N,q)$ described in [2, 6, 7], there exists a hyperplane disjoint from the cap; this happens for the caps constructed in [15] for $N \in \{3,4\}$ as well, with the exception of the 72-cap in $PG(4,8)$. Therefore such caps can be viewed as complete caps in $AG(N,q)$. Also, some known constructions of infinite families of complete caps in $PG(N,q)$ are based on a complete cap K in an affine space $PG(N,q) \setminus \mathcal{H}_\infty$, to which some properly chosen points on $\mathcal{H}_\infty$ are added (see [8, 10, 16, 17]; note that in [8, 16, 17] the completeness of K in the affine space is proven without being explicitly stated). Results on $t_2(AG(N,q))$ that can be deduced from [8, 10, 16, 17] are reported in the following table.

q	N	$t_2(AG(N,q)) \le$	Reference
q even, $q > 2$	$N = 3$	$2q$	[17, Paragraph 3]
q even, $q > 2$	N even	$q^{\frac{N}{2}}$	[16, Section 3]
q even, $q > 2$	N odd	$2q^{\frac{N-1}{2}}$	[16, Section 3]
q even, $q \ge 32$	N even	$\frac{1}{2}q^{\frac{N}{2}}$	[10, Theorem 1.2]
q odd, $q \ge 5$	$N \equiv 2 \pmod 4$	$q^{\frac{N}{2}}$	[8, Theorem 2]

2. Caps of size $q^{\frac{N}{2}}$ in $AG(N,q)$, N even

Throughout this section, we assume that q is an odd prime power and that N is even. Let $q' = q^{\frac{N}{2}}$. Fix a basis of $\mathbb{F}_{q'}$ as a linear space over $\mathbb{F}_q$, and identify points in $AG(N,q)$ with vectors of $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$.

Our starting point is the following result, due to Davydov and Östergård (it follows immediately from the proof of Theorem 2 in [8]).

Proposition 2.1. *The point set* $K = \{(\alpha, \alpha^2) \mid \alpha \in \mathbb{F}_{q'}\}$ *is a cap in* $AG(N, q)$. *If* $N \equiv 2 \pmod 4$, *then* K *is complete.*

The first assertion of Proposition 2.1 can be generalized as follows.

Proposition 2.2. *Let* $j \in \{0, 1, \dots, \frac{N}{2} - 1\}$. *Then the point set*

$$K_j = \left\{\left(\alpha, \alpha^{q^j+1}\right) \,\middle|\, \alpha \in \mathbb{F}_{q'}\right\}$$

is a cap in $AG(N, q)$.

Proof: Let $\bar{q} = q^j$. Assume that $(\gamma, \gamma^{\bar{q}+1})$ belongs to the line joining $(\alpha, \alpha^{\bar{q}+1})$ to $(\beta, \beta^{\bar{q}+1})$, with α, β, γ pairwise distinct elements in $\mathbb{F}_{q'}$. By [12, Lemma 2.1], there exists $t \in \mathbb{F}_q$, $t \neq 0$, $t \neq 1$, such that

$$\begin{cases} \gamma = \alpha + t(\beta - \alpha) \\ \gamma^{\bar{q}+1} = \alpha^{\bar{q}+1} + t(\beta^{\bar{q}+1} - \alpha^{\bar{q}+1}) \end{cases}.$$

As $(\beta - \alpha)^{\bar{q}} = \beta^{\bar{q}} - \alpha^{\bar{q}}$, it follows that

$$0 = t(1-t)(\beta - \alpha)^{\bar{q}+1},$$

which is impossible. □

Note that for any $\eta \in \mathbb{F}_{q'}$, $j \in \{0, 1, \dots, \frac{N}{2} - 1\}$, the map

$$\begin{aligned} L_\eta : \mathbb{F}_{q'} \times \mathbb{F}_{q'} &\to \mathbb{F}_{q'} \times \mathbb{F}_{q'} \\ (X, Y) &\mapsto \left(X, Y + \eta X^{q^j} + \eta^{q^j} X\right) \end{aligned}$$

is $\mathbb{F}_q$-linear. Then the map

$$\begin{aligned} \Phi_\eta : AG(N, q) &\to AG(N, q) \\ (X, Y) &\mapsto L_\eta(X, Y) + \left(\eta, \eta^{q^j+1}\right) \end{aligned}$$

is an affinity of $AG(N, q)$. It is straightforward to check that the group of affinities of $AG(N, q)$,

$$G_j := \{\Phi_\eta \mid \eta \in \mathbb{F}_{q'}\},$$

acts regularly on the points of the cap K_j from Proposition 2.2.

Let H_j be the subgroup of the multiplicative group of $\mathbb{F}_{q'}$ consisting of the non-zero $(q^j + 1)$-th powers in $\mathbb{F}_{q'}$. Also, let C_j consist of the union of sets $(t - t^2)H_j$ with t ranging over $\mathbb{F}_q$.

Lemma 2.3. *Let K_j be as in Proposition 2.2. A point $P=(a,b)\in AG(N,q)$ belongs to a secant of K_j if and only if $b-a^{q^j+1}\in C_j$.*

Proof: Let $\bar{q}=q^j$. Assume that P belongs to the line joining $(\alpha,\alpha^{\bar{q}+1})$ to $(\beta,\beta^{\bar{q}+1})$. Then there exists $t\in\mathbb{F}_q$ such that

$$\begin{cases} a=\alpha+t(\beta-\alpha) \\ b=\alpha^{\bar{q}+1}+t(\beta^{\bar{q}+1}-\alpha^{\bar{q}+1}). \end{cases}$$

Then

$$b-a^{\bar{q}+1}=t(1-t)(\beta-\alpha)^{\bar{q}+1}\in C_j.$$

Conversely, let $t\in\mathbb{F}_q$ be such that $b-a^{\bar{q}+1}\in(t-t^2)H_j$. Clearly $t\in\{0,1\}$ if and only if $P\in K_j$. Assume then that $t\notin\{0,1\}$. Let $\gamma\in\mathbb{F}_{q'}$ be such that $\gamma^{\bar{q}+1}=\frac{b-a^{\bar{q}+1}}{t-t^2}$. Note that $\gamma\neq 0$, as otherwise $P\in K_j$. Let $\alpha=a-t\gamma$ and $\beta=a+(1-t)\gamma$. Then it is straightforward to check that

$$a=\alpha+t(\beta-\alpha)\,,\quad b=\alpha^{\bar{q}+1}+t(\beta^{\bar{q}+1}-\alpha^{\bar{q}+1}),$$

that is, P belongs to the line joining $(\alpha,\alpha^{\bar{q}+1})$ and $(\beta,\beta^{\bar{q}+1})$. □

The following lemma is a well-known result on finite fields (see e.g. [12])

Lemma 2.4. *If $q>3$, then the set $\{t-t^2\mid t\in\mathbb{F}_q\}$ contains both a non-zero square in $\mathbb{F}_q$ and a non-square in $\mathbb{F}_q$.*

Proposition 2.5. *Let K_j be as in Proposition 2.2. If $q>3$, then K_j is complete if and only if $N\equiv 2 \pmod 4$ and $(q^{\frac{N}{2}}-1,q^j+1)=2$.*

Proof: By Lemma 2.3, the cap K_j is complete if and only if the set C_j coincides with $\mathbb{F}_{q'}$. Note that every non-zero square in $\mathbb{F}_q$ is an element of H_j, since $a^2=a^{q^j+1}$ holds for any $a\in\mathbb{F}_q$. Then, by Lemma 2.4,

$$C_j=H_j\cup sH_j\cup\{0\},$$

s being any non-square in $\mathbb{F}_q$. The set C_j then coincides with $\mathbb{F}_{q'}$ if and only if both of the following conditions hold:

(i) the index of H_j as a subgroup of the multiplicative group of $\mathbb{F}_{q'}$ is equal to 2, that is $(q^{\frac{N}{2}}-1,q^j+1)=2$;
(ii) any non-square element in $\mathbb{F}_q$ belongs to $\mathbb{F}_{q'}\setminus H_j$.

Note that condition (i) is equivalent to H_j coinciding with the subgroup of non-zero squares in $\mathbb{F}_{q'}$. Therefore, provided that (i) holds, condition (ii) is equivalent to $\frac{N}{2}$ being odd. This completes the proof. □

We end this section by noticing that the completeness of K_j holds in a stronger sense.

Lemma 2.6. *Let K_j be as in Proposition 2.2. Assume that $q > 3$, $N \equiv 2 \pmod 4$ and $(q^{\frac{N}{2}} - 1, q^j + 1) = 2$. Let $P = (a, b) \in AG(N, q) \setminus K_j$. If $b - a^{q^j+1}$ is a non-zero square in $\mathbb{F}_{q'}$, then for any $t \in \mathbb{F}_q$ such that $t - t^2$ is a non-zero square in $\mathbb{F}_q$ there exist $P_1, P_2 \in K_j$ such that $P = P_1 + t(P_2 - P_1)$. Similarly, if $b - a^{q^j+1}$ is a non-square in $\mathbb{F}_{q'}$, then for any $t \in \mathbb{F}_q$ such that $t - t^2$ is a non-square in $\mathbb{F}_q$ there exist $P_1, P_2 \in K_j$ such that $P = P_1 + t(P_2 - P_1)$.*

Proof: Assume that $b - a^{q^j+1}$ is a non-zero square in $\mathbb{F}_{q'}$, and let $t \in \mathbb{F}_q$ be such that $t - t^2$ is a non-zero square in $\mathbb{F}_q$. Then $b - a^{q^j+1} \in (t - t^2)S$, where S is the set of non-zero squares in $\mathbb{F}_{q'}$. As $(q^{\frac{N}{2}} - 1, q^j + 1) = 2$, S coincides with the subgroup H_j. Note also that $t \in \mathbb{F}_q$ implies $t^2 = t^{q^j+1}$. Then there exists $\gamma \in \mathbb{F}_{q'}$ such that $\gamma^{q^j+1} = \frac{b-a^{q^j+1}}{t-t^{q^j+1}}$. Note that $\gamma \neq 0$, as otherwise $P \in K_j$. Let $\alpha = a - t\gamma$ and $\beta = \alpha + \gamma$. Then it is straightforward to check that

$$a = \alpha + t(\beta - \alpha), \quad b = \alpha^{q^j+1} + t\left(\beta^{q^j+1} - \alpha^{q^j+1}\right),$$

that is, $P = P_1 + t(P_2 - P_1)$, where $P_1 = (\alpha, \alpha^{q^j+1})$ and $P_2 = (\beta, \beta^{q^j+1})$.

The proof of the assertion for $b - a^{q^j+1}$ non-square in $\mathbb{F}_{q'}$ is analogous. □

3. Proof of Theorem 1.1

We keep the notation used in Section 2. Throughout this section, N is assumed to be divisible by 4.

Let $s = \frac{N}{4}$ and $\bar{q} = q^s$. Fix a basis of $\mathbb{F}_{\bar{q}}$ over $\mathbb{F}_q$, so that any subset of points of $AG(s, q)$ can be viewed as a subset of $\mathbb{F}_{\bar{q}}$. Also, let $q' = q^{2s}$.

Proposition 3.1. *Let C be a cap in $AG(s, q)$, viewed as a subset of $\mathbb{F}_{\bar{q}}$. Let w be a primitive element of $\mathbb{F}_{q'}$. Then the point set*

$$\bar{K} = \bigcup_{\nu \in C} \left\{(\alpha, \alpha^{\bar{q}+1} + w\nu) \mid \alpha \in \mathbb{F}_{q'}\right\}$$

is a cap in $AG(N, q)$ that is preserved by the group G_s.

Proof: For $\nu \in C$, denote by $K_\nu = \{(\alpha, \alpha^{\bar{q}+1} + w\nu) \mid \alpha \in \mathbb{F}_{q'}\}$. Clearly each K_ν is affinely equivalent to K_s, whence K_ν is a cap in $AG(N, q)$.

Note that G_s acts regularly on K_ν. Then to prove the assertion it is enough to show that $P_1 = (0, w\nu_1)$, $P_2 = (\alpha, \alpha^{\bar{q}+1} + w\nu_2)$, $P_3 = (\beta, \beta^{\bar{q}+1} + w\nu_3)$ are not collinear for any $\alpha, \beta \in \mathbb{F}_{q'}$, ν_1, ν_2, ν_3 in C. Suppose on the contrary that there exists $t \in \mathbb{F}_q$

such that

$$\begin{cases} 0 = \alpha + t(\beta - \alpha) \\ w\nu_1 = \alpha^{\bar{q}+1} + w\nu_2 + t(\beta^{\bar{q}+1} + w\nu_3 - \alpha^{\bar{q}+1} - w\nu_2). \end{cases}$$

Then

$$w(\nu_1 - \nu_2 - t(\nu_3 - \nu_2)) = \alpha^{\bar{q}+1} + t(\beta^{\bar{q}+1} - \alpha^{\bar{q}+1}). \tag{3.1}$$

Note that both $\nu_1 - \nu_2 - t(\nu_3 - \nu_2)$ and $\alpha^{\bar{q}+1} + t(\beta^{\bar{q}+1} - \alpha^{\bar{q}+1})$ belong to $\mathbb{F}_{\bar{q}}$. Then (3.1) yields $\nu_1 = \nu_2 + t(\nu_3 - \nu_2)$, which is impossible as C is a cap in $AG(s, q)$. □

Proposition 3.2. *Let $\bar{K}$ be as in Proposition* 3.1. *If C is complete in $AG(s, q)$, then $\bar{K}$ is a complete cap in $AG(N, q)$.*

Proof: Let $P = (a, b)$ in $AG(N, q) \setminus \bar{K}$. Let $b - a^{\bar{q}+1} = u + wv$, with $u, v \in \mathbb{F}_{\bar{q}}$. Assume first that $v \in C$. Fix an element $t \in \mathbb{F}_q$ such that $t - t^2 \neq 0$. As $\frac{u}{t-t^2} \in \mathbb{F}_{\bar{q}}$, there exists $\gamma \in \mathbb{F}_{q'}$ such that $\gamma^{\bar{q}+1} = \frac{u}{t-t^2}$. Note that $\gamma \neq 0$, as otherwise $P \in \bar{K}$. Let $\alpha = a - t\gamma$ and $\beta = a + (1-t)\gamma$. Then it is straightforward to check that

$$a = \alpha + t(\beta - \alpha), \quad b = \alpha^{\bar{q}+1} + wv + t(\beta^{\bar{q}+1} - \alpha^{\bar{q}+1}),$$

that is, P belongs to the line joining $(\alpha, \alpha^{\bar{q}+1} + wv)$ and $(\beta, \beta^{\bar{q}+1} + wv)$.

Assume now that $v \notin C$. As C is a complete cap, there exist ν_1, ν_2 in C such that $v = \nu_1 + t(\nu_2 - \nu_1)$ for some $t \in \mathbb{F}_q$. Note that $\frac{u}{t-t^2} \in \mathbb{F}_{\bar{q}}$ implies that there exists $\gamma \in \mathbb{F}_{q'}$ such that $\gamma^{\bar{q}+1} = \frac{u}{t-t^2}$. Let $\alpha = a - t\gamma$ and $\beta = a + (1-t)\gamma$. Then

$$a = \alpha + t(\beta - \alpha), \quad b = \alpha^{\bar{q}+1} + w\nu_1 + t(\beta^{\bar{q}+1} + w\nu_2 - \alpha^{\bar{q}+1} - w\nu_1),$$

that is, P belongs to the line joining $(\alpha, \alpha^{\bar{q}+1} + w\nu_1)$ and $(\beta, \beta^{\bar{q}+1} + w\nu_2)$. □

Proof of Theorem 1.1: Theorem 1.1 is a straightforward corollary to Proposition 3.2. □

Remark 3.3. Proposition 3.2 provides a description of a complete $(2q^2)$-cap $\bar{K}$ in $AG(4, q)$, namely

$$\bar{K} = \left\{(\alpha, \alpha^{q+1}) \mid \alpha \in \mathbb{F}_{q^2}\right\} \cup \left\{(\alpha, \alpha^{q+1} + w) \mid \alpha \in \mathbb{F}_{q^2}\right\},$$

with w a primitive element of $\mathbb{F}_{q^2}$.

Remark 3.4. Let $N = 2^{2n+1}m$, with $n \geq 1$, m odd. Then the construction described in Proposition 3.2, together with Proposition 2.1, provide an explicit description of a complete cap in $AG(N, q)$ of size

$$q^{\frac{N}{2}} q^{\frac{N}{8}} \cdots q^{4m} q^m = q^{\frac{N}{2}(1+\frac{1}{4}+\frac{1}{16}+\cdots+\frac{1}{4^{n-1}})} q^m = q^{\frac{2N-m}{3}}.$$

4. Caps arising from arcs admitting few regular points

Throughout this section, q is assumed to be odd and N divisible by 4. Let $q' = q^{\frac{N-2}{2}}$. Fix a basis of $\mathbb{F}_{q'}$ as a linear space over $\mathbb{F}_q$, and identify points in $AG(N,q)$ with vectors of $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_q \times \mathbb{F}_q$. Also, let c be a non-square in $\mathbb{F}_q$. Note that as $\frac{N-2}{2}$ is odd, c is a non-square in $\mathbb{F}_{q'}$ as well.

For an arc A in $AG(2,q)$, let

$$K_A = \{(\alpha, \alpha^2, u, v) \in AG(N,q) \mid \alpha \in \mathbb{F}_{q'}, \quad (u,v) \in A\}.$$

As K_A is the cartesian product of a cap in $AG(N-2)$ by an arc A, by [1, Theorem 4] K_A is a cap in $AG(N,q)$. To investigate the completeness of K_A in $AG(N,q)$, the concept of a regular point with respect to a complete arc in $AG(2,q)$ is useful. According to Segre [18], given three pairwise distinct points P, P_1, P_2 on a line ℓ in $AG(2,q)$, P is external or internal to the segment P_1P_2 depending on whether

$$(x-x_1)(x-x_2) \quad \text{is a non-zero square in } \mathbb{F}_q \text{ or not,} \tag{4.1}$$

where x, x_1 and x_2 are the coordinates of P, P_1 and P_2 with respect to any affine frame of ℓ. Definition 13 in [18] extends as follows.

Definition 4.1. Let A be a complete arc in $AG(2,q)$. A point $P \in AG(2,q) \backslash A$ is *regular* with respect to A if P is external to any segment P_1P_2, with $P_1, P_2 \in A$ collinear with P. The point P is said to be *pseudo-regular* with respect to A if it is internal to any segment P_1P_2, with $P_1, P_2 \in A$ collinear with P.

Now we are in a position to prove the following proposition.

Proposition 4.2. *Let A be a complete arc in $AG(2,q)$ such that no point in $AG(2,q)$ is either regular or pseudo-regular with respect to A. Then K_A is a complete cap in $AG(N,q)$.*

Proof: Fix a point $P = (a,b,x,y) \in AG(N,q) \setminus K_A$. Assume first that $(x,y) \in A$. Then Lemma 2.6 for $j=0$ ensures the existence of $t \in \mathbb{F}_q$, $\alpha, \beta \in \mathbb{F}_{q'}$, $\alpha \neq \beta$, such that

$$(a,b) = (\alpha, \alpha^2) + t((\beta, \beta^2) - (\alpha, \alpha^2)),$$

that is

$$(a,b,x,y) = (\alpha, \alpha^2, x, y) + t((\beta, \beta^2, x, y) - (\alpha, \alpha^2, x, y)).$$

If $b = a^2$, then by completeness of A there exists $t \in \mathbb{F}_q$, $(u_1, v_1), (u_2, v_2) \in A$, such that

$$(x,y) = (u_1, v_1) + t\left((u_2, v_2) - (u_1, v_1)\right),$$

that is

$$(a, b, x, y) = (a, b, u_1, v_1) + t\,((a, b, u_2, v_2) - (a, b, u_1, v_1))\,.$$

Now, assume that $(x, y) \notin A$ and that $a^2 - b$ is a non-square in $\mathbb{F}_{q'}$. As (x, y) is not a regular point with respect to A, there exists $t \in \mathbb{F}_q$, $(u_1, v_1), (u_2, v_2) \in A$, such that

$$(x, y) = (u_1, v_1) + t\,((u_2, v_2) - (u_1, v_1))\,,$$

with $t^2 - t$ a non-square in $\mathbb{F}_q$. By Lemma 2.6, there exist $\alpha, \beta \in \mathbb{F}_{q'}$, $\alpha \neq \beta$, such that

$$(a, b) = (\alpha, \alpha^2) + t((\beta, \beta^2) - (\alpha, \alpha^2)).$$

Then

$$(a, b, x, y) = (a, b, u_1, v_1) + t\,((a, b, u_2, v_2) - (a, b, u_1, v_1))\,. \tag{4.2}$$

If $(x, y) \notin A$ and $a^2 - b$ is non-zero square in $\mathbb{F}_{q'}$, then the same argument yields (4.2). This completes the proof. □

Proposition 4.3. *Let A be a complete arc in $AG(2, q)$, admitting exactly one regular point (x_0, y_0) and no pseudo-regular point. Then*

$$K = K_A \cup \left\{(\alpha, \alpha^2 - c, x_0, y_0) \mid \alpha \in \mathbb{F}_{q'}\right\}$$

is a complete cap in $AG(N, q)$.

Proof: Let $K_0 = \{(\alpha, \alpha^2 - c, x_0, y_0) \mid \alpha \in \mathbb{F}_{q'}\}$. Note that K_0 is a cap contained in the subspace $\Sigma = AG(N - 2, q) \times \{(x_0, y_0)\}$. As K_A is disjoint from Σ, to prove that K is a cap we only need to show that no point in K_0 is collinear with two points in K_A. Assume on the contrary that

$$(\alpha, \alpha^2 - c, x_0, y_0) = (\beta, \beta^2, u_1, v_1) + t((\gamma, \gamma^2, u_2, v_2) - (\beta, \beta^2, u_1, v_1))$$

for some $(u_1, v_1), (u_2, v_2) \in A$, $t \in \mathbb{F}_q$, $\alpha, \beta, \gamma \in \mathbb{F}_{q'}$. Then,

$$(x_0, y_0) = (u_1, v_1) + t\,((u_2, v_2) - (u_1, v_1)).$$

As (x_0, y_0) is regular with respect to A, $t^2 - t$ is a non-zero square in $\mathbb{F}_q$. On the other hand,

$$\begin{cases} \alpha = \beta + t(\gamma - \beta) \\ \alpha^2 - c = \beta^2 + t(\gamma^2 - \beta^2) \end{cases}$$

implies $c = (t^2 - t)(\gamma - \beta)^2$, which is a contradiction as c is not a square in $\mathbb{F}_{q'}$.

To prove that K is complete, fix a point $P = (a, b, x, y) \in AG(N, q) \setminus K$. If either (a) $(x, y) \in A$, or (b) $b = a^2$, or (c) $(x, y) \notin A$ and $a^2 - b$ is a non-square in $\mathbb{F}_{q'}$, or (d) $(x, y) \notin A$, $(x, y) \neq (x_0, y_0)$ and $a^2 - b$ is a non-zero square in $\mathbb{F}_{q'}$, then one can argue as in the proof of Proposition 4.2. Therefore, we only need to consider the case $(x, y) = (x_0, y_0)$, and $a^2 - b$ is a non-zero square in $\mathbb{F}_{q'}$. Note that by Proposition 2.1 the point $(a, b + c)$ in $AG(N - 2, q)$ is collinear with (α, α^2) and (β, β^2) for some $\alpha, \beta \in \mathbb{F}_{q'}$. Then $P = (a, b, x_0, y_0)$ is collinear with $(\alpha, \alpha^2 - c, x_0, y_0)$ and $(\beta, \beta^2 - c, x_0, y_0)$. □

A similar result holds for A being a complete arc admitting exactly one pseudo-regular point and no regular point. The proof is omitted as it is similar to that of Proposition 4.3.

Proposition 4.4. *Let A be a complete arc in $AG(2, q)$, admitting exactly one pseudo-regular point (x_0, y_0) and no regular point. Then*

$$K = K_A \cup \{(\alpha, \alpha^2 - c^2, x_0, y_0) \mid \alpha \in \mathbb{F}_{q'}\}$$

is a complete cap in $AG(N, q)$.

Now both (A) and (B) of Theorem 1.2 can be easily proven.

Proof of (A) of Theorem 1.2: Let A be the complete arc in $AG(2, q)$, q odd, consisting of the $(q + 1)$ points of an ellipse. In [18] it is proven that for $q > 5$ the center of the ellipse is the only regular point with respect to A; also, no point in $AG(2, q) \setminus A$ is pseudo-regular with respect to A. Then the assertion follows from Proposition 4.3. □

Proof of (B) of Theorem 1.2: Let A be the complete arc in $AG(2, q)$, q odd, consisting of the $(q - 1)$ points of a hyperbola. By a result in [18], if $q > 13$ the center of the hyperbola is the only point in $AG(2, q) \setminus A$ which is either regular or pseudo-regular with respect to A. Then the assertion follows from Propositions 4.3 and 4.4. □

5. Small complete caps arising from plane cubic curves

Statement (C) of Theorem 1.2 follows from Propositions 4.2, together with the existence of a complete $(\frac{q-3}{2})$-arc A in $AG(2, q)$ admitting neither regular nor pseudo-regular points in $AG(2, q)$.

Let q be odd, and let w be a primitive element of $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_q$, $\alpha \neq 0$, $\alpha \neq w$, let

$$P_\alpha := \left(\frac{(\alpha - 1)^3}{\alpha^2 - w\alpha}, \frac{\alpha}{\alpha - w} \right) \in AG(2, q).$$

Denote by S the set of non-zero squares in $\mathbb{F}_q$, and let

$$A := \{P_\alpha \mid \alpha \in \mathbb{F}_q \setminus S,\ \ \alpha \neq 0,\ \ \alpha \neq w\}.$$

Note that A is contained in the set of $\mathbb{F}_q$-rational affine points of the plane cubic curve

$$\mathcal{E}: w^2(1-Y)XY + ((w-1)Y+1)^3 = 0.$$

Proposition 5.1. *The point set A is a $(\frac{q-3}{2})$-arc in $AG(2,q)$.*

Proof: Assume that three distinct points $P_\alpha, P_\beta, P_\gamma \in A$ are collinear. Then,

$$\det\begin{pmatrix}(\alpha-1)^3 & \alpha^2 & \alpha^2-w\alpha\\ (\beta-1)^3 & \beta^2 & \beta^2-w\beta\\ (\gamma-1)^3 & \gamma^2 & \gamma^2-w\gamma\end{pmatrix} = 0\,.$$

Hence,

$$w(\alpha-\gamma)(\alpha-\beta)(\beta-\gamma)(\alpha\beta\gamma-1) = 0\,,$$

which is impossible as $\alpha\beta\gamma$ is not a square in $\mathbb{F}_q$. □

For $u, v \in \mathbb{F}_q$, let $G_{u,v}(X,Y)$ be the following polynomial:

$$\begin{aligned}G_{u,v}(X,Y) = {} & w^4X^4Y^4(1-v) + w^4X^2Y^2(X^2+Y^2)v\\ & + w^2X^2Y^2(-uw-3vw-3(1-v))\\ & + w(X^2+Y^2)(1-v) + vw\,.\end{aligned} \tag{5.1}$$

Let $\mathcal{X}_{u,v}$ be the algebraic plane curve defined by $G_{u,v}(X,Y)=0$. The completeness of A is related to the existence of some $\mathbb{F}_q$-rational points of $\mathcal{X}_{u,v}$.

Proposition 5.2. *Let $P=(u,v)$ be a point in $AG(2,q)\setminus A$. There exist two distinct points of A collinear with P if and only if the curve $\mathcal{X}_{u,v}$ has an $\mathbb{F}_q$-rational affine point (x,y) satisfying*

$$\text{(i) } x^2 \neq y^2, x^2 \neq 0, y^2 \neq 0, x^2 \neq 1, y^2 \neq 1.$$

Proof: Assume that P is collinear with two points P_α and P_β in A. Then

$$\det\begin{pmatrix}(\alpha-1)^3 & \alpha^2 & \alpha^2-w\alpha\\ (\beta-1)^3 & \beta^2 & \beta^2-w\beta\\ u & v & 1\end{pmatrix} = 0\,, \tag{5.2}$$

that is,

$$\begin{aligned}\alpha^2\beta^2(1-v) + \alpha\beta(\alpha+\beta)(wv) + \alpha\beta(-uw-3vw-3(1-v))\\ + (\alpha+\beta)(1-v) + vw = 0\,.\end{aligned}$$

As α and β are both non-square in $\mathbb{F}_q$, there exist $x, y \in \mathbb{F}_q \setminus \{0\}$ such that $\alpha = wx^2$, $\beta = wy^2$, $x^2 \neq y^2$. Also, both $x^2 \neq 1$ and $y^2 \neq 1$ hold, since $\alpha \neq w$ and $\beta \neq w$.

Conversely, assume that $\mathcal{X}_{u,v}$ admits an $\mathbb{F}_q$-rational point (x, y) satisfying (i). Then (5.2) holds for $\alpha = wx^2$ and $\beta = wy^2$, whence P is collinear with P_α and P_β. As both P_α and P_β belong to A, the proof is complete. □

Proposition 5.3. *If either the point $P = (u, v) \in AG(2, q)$ does not belong to $\mathcal{E}$, or $v \in \{0, 1\}$, then either $\mathcal{X}_{u,v}$ is absolutely irreducible, or it consists of two absolutely irreducible $\mathbb{F}_q$-rational quartic curves. If $P \in \mathcal{E}$ and $v(v-1) \neq 0$, then $\mathcal{X}_{u,v}$ consists of the four lines $X = \pm\sqrt{\frac{v}{v-1}}$, $Y = \pm\sqrt{\frac{v}{v-1}}$, together with two irreducible conics of equations*

$$XY - \sqrt{\frac{v-1}{vw^3}} = 0\,, \qquad XY + \sqrt{\frac{v-1}{vw^3}} = 0\,.$$

Proposition 5.3 essentially arises from straightforward computation. A detailed proof is the object of the Appendix.

Proposition 5.4. *If $q > 413$, the arc A is complete.*

Proof: Let $P = (u, v)$ be a point in $AG(2, q) \setminus A$. Note that if $P \in \mathcal{E} \setminus A$ and $v(v-1) \neq 0$, then $\frac{v-1}{vw^3}$ is a square in $\mathbb{F}_q$. Let $\mathcal{X}'$ be an absolutely irreducible non-linear component of $\mathcal{X}_{u,v}$. By Proposition 5.3 the curve $\mathcal{X}'$ is $\mathbb{F}_q$-rational. Also, by Riemann Theorem [19, p. 132], the genus $g_{\mathcal{X}'}$ of $\mathcal{X}'$ is at most 9. Then Hasse-Weil Theorem [19, p. 170] yields that the number of $\mathbb{F}_q$-rational places of $\mathcal{X}'$ is at least $q + 1 - 18\sqrt{q}$. We need to prove that there exists an $\mathbb{F}_q$-rational point $(x, y) \in \mathcal{X}'$ satisfying (i) of Proposition 5.2. Note that (i) is equivalent to (x, y) not belonging to the union of 8 lines, 6 of which being either vertical or horizontal. Let M be the number of places of $\mathcal{X}'$ centered at points which are either infinite points, or are points (x, y) not satisfying (i) of Proposition 5.2. The number of places of $\mathcal{X}'$ centered on affine points of a given line is at most 8; such number is reduced to 4 when the line is either vertical or horizontal. Also, the number of infinite points of $\mathcal{X}'$ is at most 8. This yields that M is less than or equal to 48. Note that

$$q + 1 - 18\sqrt{q} > 48$$

if and only if $\sqrt{q} > 9 + \sqrt{128}$. This condition is implied by the hypothesis $q > 413$. Then the assertion follows from Proposition 5.2. □

Proposition 5.5. *If $q > 76^2$, no point in $AG(2, q) \setminus A$ is either regular or pseudo-regular with respect to A.*

Proof: Assume that $P = (u, v) \in AG(2, q) \setminus A$ is regular with respect to A. This means that P is external to the segment $P_\alpha P_\beta$ for any $P_\alpha, P_\beta \in A$ collinear with P. By (4.1) this means that

$$\left(v - \frac{\alpha}{\alpha - w}\right)\left(v - \frac{\beta}{\beta - w}\right) \in S,$$

or, equivalently,

$$(\alpha - w)(\beta - w)(v(\alpha - w) - \alpha)(v(\beta - w) - \beta) \in S.$$

Let $x^2 = \alpha/w$ and $y^2 = \beta/w$. Then by the proof of Proposition 5.2 we have that for any $\mathbb{F}_q$-rational point (x, y) of $\mathcal{X}_{u,v}$ satisfying (i) of Proposition 5.2,

$$(x^2 - 1)(y^2 - 1)(v(x^2 - 1) - x^2)(v(y^2 - 1) - y^2) \in S.$$

Equivalently, the space curve $\mathcal{S}_{u,v}$ of equation

$$\begin{cases} G_{u,v}(X, Y) = 0 \\ (X^2 - 1)(Y^2 - 1)(v(X^2 - 1) - X^2)(v(Y^2 - 1) - Y^2) = wZ^2 \end{cases}$$

has no $\mathbb{F}_q$-rational points (x, y, z) satisfying (i) of Proposition 5.2, together with (ii) $z \neq 0$.

The next step is to prove that $\mathcal{S}_{u,v}$ has an absolutely irreducible $\mathbb{F}_q$-rational component. Let $\mathcal{X}' : G'(X, Y) = 0$ be any non-linear component of $\mathcal{X}_{u,v}$. By Proposition 5.3, the curve $\mathcal{X}'$ is $\mathbb{F}_q$-rational. Let $\overline{\mathbb{F}}_q(\mathcal{X}') = \overline{\mathbb{F}}_q(\xi, \eta)$ be the function field of $\mathcal{X}'$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$ and (ξ, η) satisfy $G'(\xi, \eta) = 0$.

The curve $\mathcal{S}'$ of equation

$$\begin{cases} G'(X, Y) = 0 \\ (X^2 - 1)(Y^2 - 1)(v(X^2 - 1) - X^2)(v(Y^2 - 1) - Y^2) = wZ^2 \end{cases}$$

is clearly an $\mathbb{F}_q$-rational component of $\mathcal{S}_{u,v}$. Such component is absolutely irreducible provided that the rational function

$$\mu = (\xi^2 - 1)(\eta^2 - 1)(v(\xi^2 - 1) - \xi^2)(v(\eta^2 - 1) - \eta^2)$$

is not a square in the function field $\overline{\mathbb{F}}_q(\mathcal{X}')$. Straightforward computation yields that if $P \neq P_{w^{-2}}$, then for a non-singular point Q of $\mathcal{X}'$ on the line $X = 1$, the valuation $v_Q(\mu)$ of μ at Q is an odd integer; if $P = P_{w^{-2}}$, then $v_Q(\mu)$ turns out to be odd for a point Q on the line $X = \xi$, with ξ any square root of w^3 in $\overline{\mathbb{F}}_q$. This yields that μ is not a square, whence $\mathcal{S}'$ is absolutely irreducible.

Now, let π denote the rational map from $\mathcal{S}'$ to $\mathcal{X}'$ such that $\pi(x, y, z) = (x, y)$ for any affine point $(x, y, z) \in \mathcal{S}'$. By the Hurwitz genus formula [19, p. 88], the genus

$g_{\mathcal{S}'}$ of $\mathcal{S}'$ satisfies

$$2g_{\mathcal{S}'} - 2 = 2(2g_{\mathcal{X}'} - 2) + R\,,$$

where $g_{\mathcal{X}'}$ is the genus of $\mathcal{X}'$ and R is the number of ramification places of π. By Riemann Theorem, $g_{\mathcal{X}'} \leq 9$. Note that any ramification place of π is either a zero of μ centered at an affine point of $\mathcal{X}'$, or is centered at an infinite point of $\mathcal{X}'$. The zeros of μ centered at an affine point of $\mathcal{X}'$ correspond to the affine points of $\mathcal{X}'$ lying on the union of 8 lines, each of which being either vertical or horizontal. Then the number of such zeros is at most 32. As the number of places centered at infinite points of $\mathcal{X}'$ is at most 8, we have that $R \leq 40$. Therefore, $g_{\mathcal{S}'} \leq 37$. Then by the Hasse-Weil Theorem, the number of $\mathbb{F}_q$-rational places of $\mathcal{S}'$ is at least $q + 1 - 74\sqrt{q}$.

Let M be the number of places of $\mathcal{S}'$ centered at points which are either infinite points, or are points (x, y, z) not satisfying conditions (i) of Proposition 5.2 and (ii). Places centered at points (x, y, z) not satisfying conditions (i) and (ii) are the places centered at affine points of the union of 9 planes. For each of the planes of equation $X = 0$, $X = \pm 1$, $Y = 0$, $Y = \pm 1$ there are at most 8 of such places, whereas for the plane $Z = 0$ and the planes $X = \pm Y$ there are at most 16 of them. Also, the number of places centered at infinite points of $\mathcal{S}'$ is at most 16. Therefore M is less than or equal to 96. Note that $q + 1 - 74\sqrt{q} > 96$ holds if and only if $\sqrt{q} > 37 + \sqrt{1464}$. Then the hypothesis $q > 76^2$ implies the existence of an $\mathbb{F}_q$-rational point $(x, y, z) \in \mathcal{S}_{u,v}$ satisfying (i) of Proposition 5.2 and (ii). But this is a contradiction.

Finally, let $P = (u, v) \in AG(2, q) \setminus A$ be pseudo-regular. Then a contradiction follows by the same arguments, provided that $\mathcal{S}_{u,v}$ is replaced with the curve

$$\begin{cases} G_{u,v}(X, Y) = 0 \\ (X^2 - 1)(Y^2 - 1)(v(X^2 - 1) - X^2)(v(Y^2 - 1) - Y^2) = Z^2. \end{cases}$$

□

Now we are in a position to complete the proof of Theorem 1.2.

Proof of (C) of Theorem 1.2: The assertion follows from Propositions 4.2 and 5.5.

□

6. Linear codes associated to complete caps

Complete k-caps in $PG(N, q)$ with $k > N + 1$ and linear $[k, k - N - 1, 4]$-codes with covering radius $\rho = 2$ over $\mathbb{F}_q$ are equivalent objects (with the exceptions of the complete 5-cap in $PG(3, 2)$ giving rise to a binary $[5, 1, 5]$-code, and the complete 11-cap in $PG(4, 3)$ corresponding to the Golay $[11, 6, 5]$-code over $\mathbb{F}_3$), see e.g. [9]. The code corresponding to a cap is defined by its parity check matrix, whose columns are the points of the cap treated as $(N + 1)$-dimensional vectors.

If $AG(N, q)$ is embedded in $PG(N, q)$, then a complete k-cap in $AG(N, q)$ can be viewed as a k-cap in $PG(N, q)$. The corresponding $[k, k - N - 1, 4]$-code has covering radius $\rho = 2$ if and only if K is complete in $PG(N, q)$ as well. If this does not happen the code still has good covering properties; more precisely, we prove that the number ζ of words at distance greater than two from the code is less then $\frac{1}{q}$ of the total number of words in $\mathbb{F}_q^k$. Let T be the set of points in $PG(N, q)$ that does not belong to any secant of the cap; as T is contained in the hyperplane at infinity, $\#T \le \frac{q^N-1}{q-1}$ holds. This means that the number ξ of vectors in $\mathbb{F}_q^{N+1}$ that are not an $\mathbb{F}_q$-linear combination of two points of the cap satisfies $\xi \le \#T(q-1) = q^N - 1$. Now, the inequality $\zeta \le \xi q^{k-N-1}$ holds as well. In fact, for any word $v \in \mathbb{F}_q^k$ at distance greater than 2 from the code, the multiplication of a parity check matrix H by v is a vector in $\mathbb{F}_q^{N+1}$ which is not an $\mathbb{F}_q$-linear combination of two columns of H; as the columns of H can be assumed to coincide with the points of the cap, the inequality follows from the fact that for any given $x \in \mathbb{F}_q^{N+1}$ there are exactly q^{k-N-1} words $v \in \mathbb{F}_q^k$ such that $Hv = x$. Then

$$\zeta \le \xi q^{k-N-1} \le q^{k-1} - q^{k-N-1} < \frac{\#\mathbb{F}_q^k}{q}.$$

One of the parameters characterizing the quality of an $[k, r, d]$-code $\mathbf{C}$ over $\mathbb{F}_q$ with covering radius ρ is its density $\mu(\mathbf{C})$, introduced in [3]:

$$\mu(\mathbf{C}) = \frac{1}{q^{k-r}} \sum_{i=0}^{\rho} (q-1)^i \binom{k}{i}.$$

Clearly, $\mu(\mathbf{C}) \ge 1$; equality holds when $\mathbf{C}$ is perfect. For an infinite family $\mathcal{U}$, consisting of $[k, r, d]_q$ codes $\mathbf{C}_k$ with the same covering radius ρ, the asymptotic parameter

$$\mu(\mathcal{U}) = \liminf_{k \to +\infty} \mu(\mathbf{C}_k)$$

is of interest [11]. In [5] the density of a $[k, r, d]$-code $\mathbf{C}$ is expressed in terms of the related subset of points in $PG(N, q)$ with $N = k - r + 1$. In particular, when $d = 4$ and $\rho = 2$ one can consider the associated complete k-cap K in $PG(N, q)$; the density of $\mathbf{C}$ turns out to be related to the average number of secants of K passing through a point in $PG(N, q) \setminus K$. This average number will be denoted by $s(K)$; it can be computed as follows:

$$s(K) = \frac{\binom{k}{2}(q-1)}{\#PG(N, q) - k} = \frac{(k^2 - k)(q-1)^2}{2\left(q^{N+1} - 1 - k(q-1)\right)}.$$

Corollary 1.4 implies the existence of a complete cap K_4 in $PG(4, q)$ of size $k \le 2q^2 + 1$ for $q > 13$. For such cap

$$s(K_4) \le \frac{q^2(2q^2+1)(q-1)^2}{q^5 - 2q^3 + 2q^2 - q} < 2q$$

holds. For $q > 76^2$ there exists a complete k-cap K_4' in $PG(4,q)$, with $k \le \frac{3}{2}q^2 - \frac{3}{2}q + 1$ (see Corollary 1.4 again). We have that

$$s(K_4') \le \frac{(\frac{9}{4}q^4 - \frac{9}{2}q^3 + \frac{9}{4}q^2 + \frac{3}{2}q^2 - \frac{3}{2}q)(q-1)^2}{2(q^5 - \frac{3}{2}q^3 + 3q^2 - \frac{3}{2}q - q)} < \frac{9}{8}q\,.$$

For caps K in spaces of dimension N greater than 4 satisfying the upper bounds of Corollary 1.4 it is not possible to provide a meaningful upper bound on $s(K)$, as no precise result on $m_2(N-1,q)$ is known for $N \ge 8$.

A parameter analogous to $s(K)$ can be defined for complete caps in affine spaces. For a complete k-cap K in $AG(N,q)$ let $s_A(K)$ denote the average number of secants of K passing through a point in $AG(N,q) \setminus K$. Equivalently,

$$s_A(K) = \frac{\binom{k}{2}(q-2)}{q^N - k}.$$

Let us consider the parameter $s_A(K)$ for the caps of Theorem 1.2. Let $N \equiv 0 \pmod 4$. Let

- $K_N^{(A)}$ be a complete k-cap in $AG(N,q)$, $q > 5$, with $k = q^{\frac{N}{2}} + q^{\frac{N-2}{2}}$,
- $K_N^{(B)}$ be a complete k-cap in $AG(N,q)$, $q > 13$, with $k = q^{\frac{N}{2}}$,
- $K_N^{(C)}$ be a complete k-cap in $AG(N,q)$, $q > 76^2$, with $k = \frac{1}{2}q^{\frac{N}{2}} - \frac{3}{2}q^{\frac{N-2}{2}}$.

Then parameters $s_A(K_N^{(A)})$, $s_A(K_N^{(B)})$, and $s_A(K_N^{(C)})$ can be easily computed, and their limits are as follows:

$$\lim_{N\to+\infty} s_A\big(K_N^{(A)}\big) = \lim_{N\to+\infty} s_A\big(K_N^{(B)}\big) = \frac{q-2}{2}, \quad \lim_{N\to+\infty} s_A\big(K_N^{(C)}\big) = \frac{q-2}{4}.$$

Appendix: Proof of Proposition 5.3

The plane curve $\mathcal{X}_{u,v} : G_{u,v}(X,Y) = 0$ is fixed by the following affine transformations:

$$\begin{array}{c} \varphi_1 : AG(2,\overline{\mathbb{F}}_q) \to AG(2,\overline{\mathbb{F}}_q) \\ (X,Y) \mapsto (-X,Y) \end{array}, \qquad \begin{array}{c} \varphi_2 : AG(2,\overline{\mathbb{F}}_q) \to AG(2,\overline{\mathbb{F}}_q) \\ (X,Y) \mapsto (Y,X) \end{array}.$$

The group D generated by φ_1 and φ_2 is a dihedral group of order 8.

As usual, for a point P and an algebraic plane curve $\mathcal{C}$, let $m_P(\mathcal{C})$ be the multiplicity of P as a point of $\mathcal{C}$. Also, for a line ℓ, let $I(\mathcal{C},\ell,P)$ denote the intersection multiplicity of $\mathcal{C}$ and ℓ at P. Denote by ℓ_∞ the line at infinity. Let X_∞ be the infinite point of the X-axis, and Y_∞ be the infinite point of the Y-axis. Finally, let $\iota \in \overline{\mathbb{F}}_q$ be one of the square roots of -1.

The proof of Proposition 5.3 is divided into four cases.

Proof of Proposition 5.3 for $v = 0$:

Some geometric features of $\mathcal{X}_{u,v}$ are the following:

(a1) the order of $\mathcal{X}_{u,v}$ is equal to 8;
(a2) $m_{X_\infty}(\mathcal{X}_{u,v}) = m_{Y_\infty}(\mathcal{X}_{u,v}) = 4$;
(a3) the only tangent of $\mathcal{X}_{u,v}$ at X_∞ is the X-axis; also, $I(\mathcal{X}_{u,v}, Y = 0, X_\infty) = 6$;
(a4) the only tangent of $\mathcal{X}_{u,v}$ at Y_∞ is the Y-axis; also, $I(\mathcal{X}_{u,v}, X = 0, Y_\infty) = 6$;
(a5) $m_{(0,0)} = 2$; the tangents of $\mathcal{X}_{u,v}$ at (0, 0) are $Y = \imath X$, $Y = -\imath X$.

Assume that $\mathcal{X}_{u,v}$ has a linear component ℓ. Then by (a2) ℓ passes through either X_∞ or Y_∞. By (a3) and (a4) this is impossible.

Let $\mathcal{C}_2$ be any irreducible conic component of $\mathcal{X}_{u,v}$. Then (a2) yields that $\mathcal{C}_2$ passes through both X_∞ and Y_∞. Also, by (a3) and (a4), the tangents of $\mathcal{C}_2$ at such points are the X-axis and the Y-axis respectively. Then $\mathcal{C}_2$ has equation $XY + k = 0$ for some $k \in \overline{\mathbb{F}}_q$. But it is straightforward that the polynomial $XY + k$ cannot divide $G_{u,v}(X, Y)$.

Let $\mathcal{C}_3$ be any absolutely irreducible cubic component of $\mathcal{X}_{u,v}$. Then $\mathcal{X}_{u,v}$ consists of $\mathcal{C}_3$ together with an absolutely irreducible component $\mathcal{C}_5$ of order 5. Note that $\mathcal{C}_3$ is fixed by both φ_1 and φ_2. Then $\mathcal{C}_3$ does not pass through (0, 0), otherwise $m_{(0,0)}(\mathcal{C}_3) = 2$, and by (a3) the X-axis would be a component of $\mathcal{C}_3$. Whence, $m_{\mathcal{C}_5}(0, 0) = 2$. Also, as $\mathcal{C}_3$ has at most one singular point, the point X_∞ is simple for $\mathcal{C}_3$ and therefore it is a point of multiplicity 3 for $\mathcal{C}_5$. Then $I(\mathcal{C}_5, Y = 0, (0, 0)) + I(\mathcal{C}_5, Y = 0, X_\infty) = 6$, which is a contradiction as the order of $\mathcal{C}_5$ is 5.

Then either $\mathcal{X}_{u,v}$ is absolutely irreducible, or $\mathcal{X}_{u,v}$ consists of two absolutely irreducible quartic curves, say $\mathcal{C}_4$ and $\mathcal{C}'_4$. Assume that $\mathcal{C}_4$ passes through (0, 0). If $\mathcal{C}'_4$ does not pass through (0, 0), then

$$m_{(0,0)}(\mathcal{C}_4) = m_{X_\infty}(\mathcal{C}_4) = m_{Y_\infty}(\mathcal{C}_4) = 2\,,$$

and therefore $I(\mathcal{C}'_4, \ell_\infty, X_\infty) + I(\mathcal{C}'_4, \ell_\infty, Y_\infty) = 6$, which is impossible. Then (0, 0) is a simple point for both $\mathcal{C}_4$ and $\mathcal{C}'_4$. By (a5), $\varphi_i(\mathcal{C}_4) = \mathcal{C}'_4$ for both $i = 1, 2$. Therefore, the affine transformation

$$\varphi_3 : AG(2, \overline{\mathbb{F}}_q) \to AG(2, \overline{\mathbb{F}}_q)$$
$$(X, Y) \mapsto (-Y, X)$$

preserves both $\mathcal{C}_4$ and $\mathcal{C}'_4$. Conditions

(i) $m_{X_\infty}(\mathcal{C}_4) = 2$,
(ii) the only tangent of $\mathcal{C}_4$ at X_∞ is the X-axis;
(iii) $I(\mathcal{C}_4, Y = 0, X_\infty) = 3$;

together with $\varphi_3(\mathcal{C}_4) = \mathcal{C}_4$ yield that $\mathcal{C}_4$ has equation $X^2Y^2 + k(X - Y) = 0$ for some $k \in \overline{\mathbb{F}}_q$. As $\varphi_1(\mathcal{C}_4) = \mathcal{C}'_4$, the curve $\mathcal{C}'_4$ has equation $X^2Y^2 - k(X - Y) = 0$. This is a contradiction, as the polynomial

$$(X^2Y^2 + k(X - Y))(X^2Y^2 - k(X - Y))$$

does not divide $G_{u,v}(X, Y)$.

Proof of Proposition 5.3 for $v = 1$:

Note that:

(b1) the order of $\mathcal{X}_{u,v}$ is equal to 6;
(b2) $m_{X_\infty}(\mathcal{X}_{u,v}) = m_{Y_\infty}(\mathcal{X}_{u,v}) = 2$;
(b3) the only tangent of $\mathcal{X}_{u,v}$ at X_∞ is the X-axis; also, $I(\mathcal{X}_{u,v}, Y = 0, X_\infty) = 6$;
(b4) the only tangent of $\mathcal{X}_{u,v}$ at Y_∞ is the Y-axis; also, $I(\mathcal{X}_{u,v}, X = 0, Y_\infty) = 6$;
(b5) the lines $\ell_1 : Y - \imath X = 0$ and $\ell_2 : Y + \imath X = 0$ are both tangents of $\mathcal{X}_{u,v}$ at their infinite points.

Assume that $\mathcal{X}_{u,v}$ has a linear component ℓ. Then by (b2) ℓ passes through either X_∞ or Y_∞. By (b3) and (b4) this is impossible.

If $\mathcal{X}_{u,v}$ consists either of an irreducible conic and an absolutely irreducible quartic curve, or of three irreducible conics, then one of such conics, say $\mathcal{C}_2$, must be fixed by the whole group D. Also, conditions (b2) and (b4) yield that $\mathcal{C}_2$ passes through both X_∞ and Y_∞. Therefore, $\mathcal{C}_2$ has equation $XY + k = 0$ for some $k \in \overline{\mathbb{F}}_q$. But it is straightforward that the polynomial $XY + k$ cannot divide $G_{u,v}(X, Y)$.

The only possibility for $\mathcal{X}_{u,v}$ being reducible is then that $\mathcal{X}_{u,v}$ consists of two absolutely irreducible cubic curves, say $\mathcal{C}_3$ and $\mathcal{C}'_3$. Assume that either X_∞ or Y_∞ is a singular point for one of such cubics, say $\mathcal{C}$. By (b2), (b3), and (b4), either $I(\mathcal{C}, Y = 0, X_\infty) = 6$ or $I(\mathcal{C}, X = 0, Y_\infty) = 6$, which is clearly impossible. Then $\mathcal{C} \cap \ell_\infty$ consists of X_∞, Y_∞ and one of the infinite points of the lines ℓ_1 and ℓ_2. Assume without loss of generality that $\mathcal{C}_3$ passes through the infinite point of ℓ_1. Then φ_3 preserves $\mathcal{C}_3$. Taking into account that $I(\mathcal{C}_3, X_\infty, Y = 0) = 3$, we obtain that an equation of $\mathcal{C}_3$ is $XY(Y - \imath X) + k = 0$ for some $k \in \overline{\mathbb{F}}_q$. Then $\mathcal{C}'_3$ has equation $XY(Y + \imath X) + k$. This is a contradiction, as the polynomial

$$(XY(Y - \imath X) + k)(XY(Y + \imath X) + k)$$

does not divide $G_{u,v}(X, Y)$.

Proof of Proposition 5.3 for $v(v - 1) \neq 0$, $(u, v) \notin \mathcal{E}$:

Let $\theta \in \overline{\mathbb{F}}_q$ be any square root of $\frac{v}{v-1}$. Note that:

(c1) the order of $\mathcal{X}_{u,v}$ is equal to 8;
(c2) $m_{X_\infty}(\mathcal{X}_{u,v}) = m_{Y_\infty}(\mathcal{X}_{u,v}) = 4$;
(c3) the tangents of $\mathcal{X}_{u,v}$ at X_∞ are the lines $Y = \pm\theta$, together with the X-axis; also,

$$I(\mathcal{X}_{u,v}, Y = 0, X_\infty) = I(\mathcal{X}_{u,v}, Y = \theta, X_\infty) = I(\mathcal{X}_{u,v}, Y = -\theta, X_\infty) = 6\,;$$

(c4) the tangents of $\mathcal{X}_{u,v}$ at Y_∞ are the lines $X = \pm\theta$, together with the Y-axis; also,

$$I(\mathcal{X}_{u,v}, X = 0, Y_\infty) = I(\mathcal{X}_{u,v}, X = \theta, Y_\infty) = I(\mathcal{X}_{u,v}, X = -\theta, Y_\infty) = 6\,;$$

(c5) points $Q_1 = (0, \theta)$, $Q_2 = (0, -\theta)$, $Q_3 = (\theta, 0)$, $Q_4 = (-\theta, 0)$ are all simple points of $\mathcal{X}_{u,v}$; also,

$$I(\mathcal{X}_{u,v}, Y = \theta, Q_1) = I(\mathcal{X}_{u,v}, Y = -\theta, Q_2) = 2\,,$$
$$I(\mathcal{X}_{u,v}, X = \theta, Q_3) = I(\mathcal{X}_{u,v}, X = -\theta, Q_4) = 2\,.$$

Assume that $\mathcal{X}_{u,v}$ has a linear component ℓ. Then by (c2) ℓ passes through either X_∞ or Y_∞. By (c3) and (c4) this is impossible.

Let $\mathcal{C}_2$ be an irreducible conic component of $\mathcal{X}_{u,v}$, and let $\mathcal{C}_6$ the (possibly reducible) sextic curve obtained from $\mathcal{X}_{u,v}$ by dismissing $\mathcal{C}_2$. As $\varphi_2(\mathcal{C}_2)$ is a conic component of $\mathcal{X}_{u,v}$ as well, one can assume without loss of generality that $\mathcal{C}_2$ passes through X_∞. Let ℓ denote the tangent of $\mathcal{C}_2$ at $\mathcal{X}_\infty$. If ℓ is the line $Y = \theta$, then $I(\mathcal{C}_6, Y = -\theta, X_\infty) + I(\mathcal{C}_6, Y = -\theta, (0, -\theta)) = 7$, which is impossible. The same contradiction is obtained if ℓ is the line $Y = -\theta$. Then (c3) yields that ℓ coincides with the X-axis. By (c4), both Q_1 and Q_2 lie on $\mathcal{C}_2$. But then $\mathcal{C}_2$ does not pass through either Y_∞ or Q_3. This is clearly impossible, as some point on the line $X = \theta$ must belong to $\mathcal{C}_2$.

Let $\mathcal{C}_3$ be any absolutely irreducible cubic component of $\mathcal{X}_{u,v}$. Then $\mathcal{X}_{u,v}$ consists of $\mathcal{C}_3$ together with an absolutely irreducible component $\mathcal{C}_5$ of degree 5. Note that $\mathcal{C}_3$ is fixed by both φ_1 and φ_2. Assume that $\mathcal{C}_3$ passes through one point of $E = \{Q_1, Q_2, Q_3, Q_4\}$; as D acts transitively on E, the curve $\mathcal{C}_3$ must pass through all points in E. But then no line can be the tangent to $\mathcal{C}_3$ at X_∞. Then $\mathcal{C}_3 \cap E = \emptyset$. This yields that the three lines $X = \theta$, $X = 0$, $X = -\theta$ intersect $\mathcal{C}_3$ only in Y_∞. Then $m_{Y_\infty}(\mathcal{C}_3) = 3$, which is impossible as $\mathcal{C}_3$ is an absolutely irreducible curve of degree 3.

If $\mathcal{X}_{u,v}$ is reducible, then $\mathcal{X}_{u,v}$ consists of two absolutely irreducible quartic curves, say $\mathcal{C}_4$ and $\mathcal{C}'_4$. We need to prove that both $\mathcal{C}_4$ and $\mathcal{C}'_4$ are $\mathbb{F}_q$-rational, or, equivalently, that the action of Frobenius collineation

$$\Phi : AG(2, \overline{\mathbb{F}}_q) \to AG(2, \overline{\mathbb{F}}_q)$$
$$(X, Y) \mapsto (X^q, Y^q)$$

on $\{\mathcal{C}_4, \mathcal{C}'_4\}$ is trivial. Note that if $\theta \in \mathbb{F}_q$, then $\Phi(\mathcal{C}_4) = \mathcal{C}'_4$, as otherwise $m_{Q_1}(\mathcal{X}_{u,v}) = 2$, contradicting (c5). Therefore, $\theta \notin \mathbb{F}_q$ can be assumed. Then $\Phi(Q_1) = Q_2$, $\Phi(Q_2) = Q_1$, $\Phi(Q_3) = Q_4$, and $\Phi(Q_4) = Q_3$. This yields that Φ acts on $\{\mathcal{C}_4, \mathcal{C}'_4\}$ as the affine transformation $(\varphi_3)^2$. $(\varphi_3)^2$ being the square of a map acting on $\{\mathcal{C}_4, \mathcal{C}'_4\}$, its action on $\{\mathcal{C}_4, \mathcal{C}'_4\}$ is trivial, and so is that of Φ. This completes the proof.

Proof of Proposition 5.3 for $v(v-1) \neq 0$, $(u, v) \in \mathcal{E}$:

It is straightforward to check that if $w^2 v(v-1)u = ((w-1)v+1)^3$, then the lines $X = \pm\sqrt{\frac{v}{v-1}}$, $Y = \pm\sqrt{\frac{v}{v-1}}$ and the irreducible conics

$$XY - \sqrt{\frac{v-1}{vw^3}} = 0\,, \qquad XY + \sqrt{\frac{v-1}{vw^3}} = 0$$

are components of $\mathcal{X}_{u,v}$.

Acknowledgments We are grateful to two anonymous referees for their very careful and helpful reports.

References

1. J. Bierbrauer, "Large caps," *J. Geom.* **76** (2003), 16–51.
2. J. Bierbrauer, S. Marcugini, and F. Pambianco, "The smallest size of a complete cap in $PG(3,7)$," *Discrete Math.*, to appear.
3. G.D. Cohen, A.C. Lobstein, and N.J.A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inform. Theory*, **32**(5) (1986), 680–694.
4. G.D. Cohen, I. Honkala, S. Litsyn, and A.C. Lobstein, *Covering Codes*, North-Holland, Amsterdam, 1997.
5. A.A. Davydov, S. Marcugini, and F. Pambianco, "On saturating sets in projective spaces," *J. Combin. Theory Ser. A* **103** (2003), 1–15.
6. A.A. Davydov, S. Marcugini, and F. Pambianco, "Complete caps in projective spaces" $PG(n,q)$, *J. Geom.* **80** (2004), 23–30.
7. A.A. Davydov, G. Faina, S. Marcugini and F. Pambianco, "Computer search in projective planes for the sizes of complete arcs," *J. Geom.* **82** (2005), 50–62.
8. A.A. Davydov and P.R.J. "Östergård, Recursive constructions of complete caps," *J. Statist. Planning Infer.* **95** (2001), 167–173.
9. E.M. Gabidulin, A.A. Davydov, and L.M. Tombak, "Linear codes with covering radius 2 and other new covering codes," *IEEE Trans. Inform. Theory* **37** (1991), 219–224.
10. M. Giulietti, Small complete caps in $PG(N,q)$, q even, submitted.
11. R.L. Graham and N.J.A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory* **39** (1993), 209–214.
12. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford 1998.
13. J.W.P. Hirschfeld and L. Storme, "The packing problem in statistics, coding theory and finite projective spaces: update 2001," in: Blokhuis, A. (ed.) et al., Finite geometries. *Proceedings of the fourth Isle of Thorns conference, Brighton, UK, April 2000*. Dordrecht: Kluwer Academic Publishers. *Dev. Math.* **3** (2001), 201–246.
14. J.J.E. Imber and D.L. Wehlau, "A family of small complete caps in $PG(n,2)$," *European J. Combin.*, **24** (2003), 613–615.
15. P.R.J "Östergård, Computer search for small complete caps," *J. Geom* **69** (2000), 172–179.
16. F. Pambianco and L. Storme, "Small complete caps in spaces of even characteristic," *J. Combin. Theory Ser. A* **75** (1996), 70–84.
17. B. Segre, "On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two," *Acta Arith.* **5** (1959), 315–332.
18. B. Segre, "Proprietà elementari relative ai segmenti ed alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois," *Ann. Mat. Pura Appl. IV Ser.* **96** (1973), 289–337.
19. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Verlag, Berlin-Heidelberg-New York, 1993.