Innovations in Incidence Geometry
Volume 6-7 (2007-2008), Pages 139–151
ISSN 1781-6475

On sharply transitive sets in PG$(2, q)$

Alexander A. Davydov Massimo Giulietti
Stefano Marcugini Fernanda Pambianco

Abstract

In PG$(2, q)$ a point set K is *sharply transitive* if the collineation group preserving K has a subgroup acting on K as a sharply transitive permutation group. By a result of Korchmáros, sharply transitive hyperovals only exist for a few values of q, namely $q = 2, 4$ and 16. In general, sharply transitive complete arcs of even size in PG$(2, q)$ with q even seem to be sporadic. In this paper, we construct sharply transitive complete $6(\sqrt{q}-1)$-arcs for $q = 4^{2h+1}$, $h \leq 4$. As far as we are concerned, these are the smallest known complete arcs in PG$(2, 4^7)$ and in PG$(2, 4^9)$; also, 42 seems to be a new value of the spectrum of the sizes of complete arcs in PG$(2, 4^3)$. Our construction applies to any q which is an odd power of 4, but the problem of the completeness of the resulting sharply transitive arc remains open for $q \geq 4^{11}$. In the second part of this paper, sharply transitive subsets arising as orbits under a Singer subgroup are considered and their characters, that is the possible intersection numbers with lines, are investigated. Subsets of PG$(2, q)$ and certain linear codes are strongly related and the above results from the point of view of coding theory will also be discussed.

Keywords: complete arcs, transitive arcs, intersection numbers

MSC 2000: 51E21

1 Introduction

A collineation group G of PG$(2, q)$, q power of a prime p, has a faithful action on the set of points of the plane and some point orbits of G may have remarkable geometric properties. This has emerged from previous work on transitive ovals, hyperovals, arcs, (k, n)-arcs, blocking sets and subplanes [3, 4, 20, 21, 23, 24].

Well-known sharply transitive complete arcs other than the conics are the cyclic $(q - \sqrt{q} + 1)$-arcs in PG$(2, q)$ for any square q [5, 13, 14, 19], the Lunelli-

Sce hyperoval in $\mathsf{PG}(2,16)$, and the regular hyperovals in $\mathsf{PG}(2,2)$ and $\mathsf{PG}(2,4)$. Some more examples, especially for q odd, are also known in the literature, see [24].

In the first part of the paper we deal with sharply transitive arcs in $\mathsf{PG}(2,q)$ for q even. Apart from small q's, complete sharply transitive arcs of even size appear to be rare objects. Non-existence results are found in [20, 24, 23]. Korchmáros [20] showed that no sharply transitive hyperoval for either $q = 8$ or $q \geq 32$ exists. The group G cannot be both cyclic and linear, as proved by Storme and Van Maldeghem [24]. By a result of Storme [23], if G is linear and does not fix a line, a point, a triangle, or an imaginary triangle (that is, a triangle in $\mathsf{PG}(2,q^3)$), then the size of the sharply transitive arc is in $\{6, 18, 36, 72\}$.

Our contribution is on the positive side. We exhibit a complete sharply transitive $6(\sqrt{q}-1)$-arc in $\mathsf{PG}(2,q)$ for each $q = 4^{2h+1}$, $1 \leq h \leq 4$. For $h = 3$ and $h = 4$ this seems to be the smallest known complete arc in $\mathsf{PG}(2,4^{2h+1})$. Also, as far as we are concerned, no other example of a complete 42-arc in $\mathsf{PG}(2,64)$ is known [9]. As we prove in section 2, the above arcs are members of an infinite class of sharply transitive arcs of size $6(\sqrt{q}-1)$ in $\mathsf{PG}(2,q)$, with $q = 4^{2h+1}$, $h \geq 0$. When $h = 0$, then the hyperoval in $\mathsf{PG}(2,4)$ is obtained. It is still open the problem of determining whether other arcs in the family are complete.

In the second part of the paper, the case where G is a subgroup of the Singer group of $\mathsf{PG}(2,q)$ is taken into consideration. Let S be a Singer subgroup, that is a subgroup of the Singer group, then $|S| = \frac{q^2+q+1}{t}$ with t a divisor of q^2+q+1.

Since the Singer group is sharply transitive on $\mathsf{PG}(2,q)$, any two point orbits under S are projectively equivalent. Let E_t be one of such orbits. For t small, an important feature of E_t is to have only a few characters. Even, E_t may happen to have only two characters. Some sufficient conditions for this, where q is a square, are due to Hamilton and Penttila [15]. In particular, this is the case when either t divides $q - \sqrt{q} + 1$ [10], or q is a fourth power and t divides $(q^2+q+1)/(\sqrt{q}+\sqrt[4]{q}+1)$ [12], or $p \equiv 2 \pmod 3$ and $t = 3$ [7]. For some sporadic examples with q non-square, see [2]. The case $t = 3$ was thoroughly investigated in [6, 8].

A useful tool in this investigation is the map $\phi_t : i \mapsto p \cdot i \pmod t$. Actually, as p does not divide t, ϕ_t is a permutation of $\mathbb{Z}_t$. Hamilton and Penttila observed that E_t has only two characters provided that ϕ_t has only two cycles, the trivial one and the other consisting of the remaining $t-1$ elements. A natural generalization which will be shown in section 3 is that E_t has a few characters provided that ϕ_t has only a few cycles. More precisely, if ϕ_t has r cycles, then E_t has at most r characters. From this, a sufficient condition on (q,t) is obtained in order that E_t has at most three characters, see Proposition 3.12. Interestingly, E_7 is always a set with at most three characters. Furthermore, when t is small, then the largest character of E_t is small compared to the size of E_t, see Theorem 3.10. We point out in section 4 that in some cases the linear codes arising from E_t are optimal as their parameters attain the Griesmer bound, see Table 1.

2 A family of transitive arcs of size $6(\sqrt{q}-1)$

Throughout this section, we assume that $q = 4^{2h+1}$, for some integer $h \geq 1$. Denote $(X : Y : T)$ the homogenous coordinates of a point in PG$(2, q)$. Let

$$c = 3(2^{2h+1} - 1) = 3(\sqrt{q} - 1).$$

Note that c is a divisor of $q - 1$.

Let α be a primitive c-th root of unity in $\mathbb{F}_q$. Consider the following collineations of PG$(2, q)$:

$$\eta\colon (X : Y : T) \mapsto (\alpha X : \alpha^{-1} Y : T)\,, \text{ and}$$
$$\phi\colon (X : Y : T) \mapsto (\alpha^{\sqrt{q}-1} Y^{\sqrt{q}} : \alpha^{\sqrt{q}-1} X^{\sqrt{q}} : T^{\sqrt{q}})\,.$$

It is straightforward to check that ϕ is an involution, whereas η has order c. As

$$\phi\eta\phi = \eta^{2\sqrt{q}-3},$$

the group G generated by ϕ and η has order $2c$.

Let K be the orbit of $P = (1 : 1 : 1)$ under the action of G. Note that the stabilizer of P in G is trivial, whence $|K| = 2c$.

Proposition 2.1. *The point set K is an arc in* PG$(2, q)$*, which is complete for $q = 4^{2h+1}$, $1 \leq h \leq 4$.*

Proof. Note that $K = K_1 \cup K_2$, where

$$K_1 = \left\{(\alpha^i : \alpha^{-i} : 1) \mid i = 0, \ldots, c-1\right\}, \text{ and}$$
$$K_2 = \left\{(\alpha^i : \alpha^{-i+2\sqrt{q}-2} : 1) \mid i = 0, \ldots, c-1\right\}.$$

As both K_1 and K_2 are subsets of an irreducible conic, and ϕ is an involution mapping K_1 on K_2, we only need to show that no line joining a point $S \in K_1$ and a point $R \in K_2$ meets K_1 in a point different from S. Also, as the group generated by η acts transitively on both K_1 and K_2, $S = P$ can be assumed. Let $R = (\alpha^j : \alpha^{-j+2\sqrt{q}-2} : 1)$, and let l_{SR} denote the line through S and R. Then a number of cases can occur. When $j \not\equiv 0 \pmod{\sqrt{q}-1}$, the line l_{SR} meets the conic $\mathcal{C} : XY = T^2$ in P and in $Q = \left(\beta : \frac{1}{\beta} : 1\right)$ with $\beta = \frac{\alpha^j+1}{\alpha^{-j+2\sqrt{q}-2}+1}$. If $j = 0$, then l_{SR} meets $\mathcal{C}$ in P and in $(0:1:0)$. If $j = 2\sqrt{q}-2$ then the intersection of l_{SR} and $\mathcal{C}$ consists of P and $(1:0:0)$. Finally, if $j = \sqrt{q}-1$ then P is the only common point of l_{SR} and $\mathcal{C}$.

Hence, we can assume that $j \not\equiv 0 \pmod{\sqrt{q}-1}$. The point Q belongs to K_1 only if $\beta^c = 1$, that is,

$$\beta^3 = \alpha^{3j} \frac{1+\alpha^j+\alpha^{2j}+\alpha^{3j}}{1+\alpha^j+\alpha^{3j}+\alpha^{2\sqrt{q}-2}(\alpha^j+\alpha^{2j})} \in \mathbb{F}_{\sqrt{q}}\,, \tag{1}$$

where $\mathbb{F}_{\sqrt{q}}$ denotes the subfield of $\mathbb{F}_q$ of order $\sqrt{q}$.

Note that the group of c-th roots of unity in $\mathbb{F}_q$ can be partitioned in the three cosets of the multiplicative group of $\mathbb{F}_{\sqrt{q}}$:

$$E_0 = \mathbb{F}^\star_{\sqrt{q}}\,, \quad E_1 = \alpha\mathbb{F}^\star_{\sqrt{q}}\,, \quad E_2 = \alpha^2\mathbb{F}^\star_{\sqrt{q}}\,.$$

As $\sqrt{q}-1 \equiv 1 \pmod 3$, we have that $E_1 = \alpha^{\sqrt{q}-1}E_0$, $E_2 = \alpha^{2\sqrt{q}-2}E_0$. Three cases need to be distinguished.

- $\alpha^j \in E_0$. In this case all the powers of α^j belong to $\mathbb{F}_{\sqrt{q}}$, whence (1) holds if and only if $\alpha^{2\sqrt{q}-2} \in \mathbb{F}_{\sqrt{q}}$, which is clearly impossible.
- $\alpha^j \in E_1$. Write $\alpha^j = \alpha^{\sqrt{q}-1}\gamma$ for $\gamma \in \mathbb{F}_{\sqrt{q}}$, $\gamma \neq 1$. Then, taking into account that $\alpha^{2\sqrt{q}-2} + \alpha^{\sqrt{q}-1} = 1$, condition (1) reads

  $$1 + \frac{\gamma+\gamma^2}{1+\gamma+\gamma^3+\alpha^{\sqrt{q}-1}(\gamma+\gamma^2)} \in \mathbb{F}_{\sqrt{q}}\,,$$

  which is impossible as $\alpha^{\sqrt{q}-1} \notin \mathbb{F}_{\sqrt{q}}$.
- $\alpha^j \in E_2$. Write $\alpha^j = \alpha^{2\sqrt{q}-2}\gamma$ for $\gamma \in \mathbb{F}_{\sqrt{q}}$, $\gamma \neq 1$. In this case (1) reads

  $$\frac{1+\gamma+\gamma^3+\alpha^{\sqrt{q}-1}(\gamma+\gamma^2)}{1+\gamma+\gamma^2+\gamma^3} \in \mathbb{F}_{\sqrt{q}}\,,$$

  which is again impossible as $\alpha^{\sqrt{q}-1} \notin \mathbb{F}_{\sqrt{q}}$.

Therefore, K is an arc. The completeness of K for $q = 4^{2h+1}$, $1 \le h \le 4$, has been obtained as a result of a computer search. □

For $h > 4$ we have not been able to establish whether the arc K is complete or not.

Remark 2.2. It is worth noticing that G is not the full collineation group of K. It is straighforward to check that the collineation

$$\psi\colon (X:Y:T) \mapsto (Y^4 : X^4 : T^4)$$

preserves K and fixes the point $(1:1:1)$. As ψ has order $4h+2$, the size of the collineation group of K is at least $6(4h+2)(\sqrt{q}-1)$. Actually it has been checked by means of a computer search that the collineation group of K coincides with the group generated by G and ψ when either $h=1$ or $h=2$. When $h=0$, the collineation group of K is the whole symmetric group S_6, see e.g. [16, p. 369].

3 Characters of cyclic sets of Singer type

Let $q=p^h$ for some prime p and some positive integer h. Following Singer [22], the projective plane $\mathsf{PG}(2,q)$ can be represented by means of a cubic extension $\mathbb{F}_{q^3}$ of $\mathbb{F}_q$: points are non-zero elements of $\mathbb{F}_{q^3}$ such that two elements $x,y\in\mathbb{F}_{q^3}$ represent the same point if and only if $x=\lambda y$ for some $\lambda\in\mathbb{F}_q$. Let ω denote a primitive element in $\mathbb{F}_{q^3}$. As the set

$$\left\{\omega^0,\omega^1,\dots,\omega^{q^2+q}\right\}$$

contains exactly one element from each class representing a point, one gets a representative system for points by choosing ω^i, where i ranges over $\mathbb{Z}_v$, with $v=q^2+q+1$, so that both $\sigma\colon\omega^i\mapsto\omega^{i+1}$ and $\tau\colon\omega^i\mapsto\omega^{ip}$ become permutations on the points of $\mathsf{PG}(2,q)$. The cyclic group G generated by σ is a subgroup of $\mathsf{PGL}(3,q)$ acting regularly on the set of points of $\mathsf{PG}(2,q)$. Actually, up to conjugacy, this is the only cyclic group acting regularly on the set of points of $\mathsf{PG}(2,q)$, and in the sequel it will be referred to as the Singer group of $\mathsf{PG}(2,q)$. The group U generated by τ is a group of collineations of $\mathsf{PG}(2,q)$ which normalizes every subgroup of G in $P\Gamma L(2,q)$; moreover, the order of U is $3h$. Throughout this section, the point represented by ω^i will be denoted by P_i.

For any divisor n of q^2+q+1, let $O_0,\dots,O_{t-1}$ be the orbits of $\mathsf{PG}(2,q)$ under the unique subgroup S_n of G of order n. Clearly, $t=(q^2+q+1)/n$ and $|O_i|=n$. Indexes can be arranged in such a way that both $P_0\in O_0$ and $O_s=\sigma^s(O_0)$ hold. Note that τ acts on the set of orbits $O_0,\dots,O_{t-1}$ as follows: $\tau(O_i)=O_{pi\pmod t}$.

The following definition will be useful.

Definition 3.1. Let $s(p,t)$ be the number of orbits of $\mathbb{Z}_t\setminus\{0\}$ under the action of the permutation group generated by the map

$$i\mapsto p\cdot i\,.$$

Note that $s(p,t)\le\frac{t-1}{2}$ unless $p\equiv 1\pmod t$, which can only happen for $t=3$.

Proposition 3.2. *Let $s(p,t)$ be as in Definition 3.1. Then the cyclic group generated by τ acts on the set $O_1,\ldots,O_{t-1}$ with a number of orbits equal to $s(p,t)$.*

When t is prime the integer $s(p,t)$ can be easily computed.

Proposition 3.3. *Let t be a prime. Then $s(p,t)$ divides $t-1$ and $s(p,t)$ is the least integer i such that $p \equiv \omega^i \pmod t$ for some primitive element $\omega \in \mathbb{Z}_t$.*

Proof. Let e be the order of $p \pmod t$ in the multiplicative group of $\mathbb{Z}_t$. Then $s(p,t) = \frac{t-1}{e}$, and $p \pmod t$ is the $s(p,t)$-th power of a primitive element in $\mathbb{Z}_t$. This proves the assertion. □

Proposition 3.4. *If $t \le 7$, then $s(p,t) \le 2$.*

Proof. The assertion is obvious for $t = 3$. As q^2+q+1 is odd, neither cases $t = 2$ nor $t = 4$ can occur. It is straightforward to check that q^2+q+1 is not divisible by 5 either, for any prime power q. When $t = 7$, we consider the subgroup H generated by q in the multiplicative group of $\mathbb{Z}_7$. It certainly contains the subgroup generated by p. As $7 \mid q^3-1 = (q^2+q+1)(q-1)$, the order of H is a divisor of 3. As $q \not\equiv 1 \pmod 7$, such order is precisely 3. □

It is well known (see e.g. [11, 2.3.1]) that under the action of a cyclic collineation group of a finite projective plane π, the point set and the line set of π have the same cyclic structure. Therefore, as τ fixes P_0, at least one line l_0 has to be left invariant by τ. Set

$$m_i = |l_0 \cap O_i| \,. \tag{2}$$

Lemma 3.5. *Let l be any line in $\mathsf{PG}(2,q)$. Then*

$$|l \cap O_0| = m_i$$

for some $i = 0,\ldots,t+1$.

Proof. The group G acts regularly on the set of lines of $\mathsf{PG}(2,q)$. Therefore, $l = \sigma^j(l_0)$ for some $j = 0,\ldots,q^2+q$. Let $O_i = (\sigma^j)^{-1}(O_0)$. Then clearly $|l \cap O_0| = m_i$. □

Lemma 3.6. *The number of distinct values of the integers m_i is at most $s(p,t)+1$, with $s(p,t)$ as in Definition 3.1.*

Proof. As l_0 is fixed by τ, $m_i = m_{pi \pmod t}$ holds. This proves the assertion. □

Then the following result is obtained.

Theorem 3.7. *Let E_t be any orbit under the action of the subgroup of the Singer group of size $(q^2 + q + 1)/t$, and let $s = s(p, t)$ be as in Definition 3.1. Then the number of characters of E_t is at most $s(r, t) + 1$.*

Some lower and upper bounds on the characters of O_0 will be provided.

Lemma 3.8. *Let m_i be as in (2). Then*

(i) $\sum_{i=0}^{t-1} m_i = q + 1$;

(ii) $\sum_{i=0}^{t-1} m_i^2 = \dfrac{q^2 + (t+1)q + 1}{t}$.

Proof. The former assertion is trivial. To prove (ii), we consider the action of S_n on the set of lines of PG$(2, q)$. For $i = 0, \dots, t-1$, let L_i be the line orbit under S_n containing $\sigma^i(l_0)$.

For any $u = 0, \dots, q^2 + q$, let s_u be such that $0 \le s_u \le t - 1$ and $s_u \equiv -u \pmod t$. As the collineation σ^u maps the orbit O_{s_u} on O_0,

$$|\sigma^u(l_0) \cap O_0| = |l_0 \cap O_{s_u}| = m_{s_u}$$

holds. This proves that for any $i = 0, \dots, t-1$ the line orbit L_i consists of lines meeting O_0 in the same number of points $m_{-i \pmod t}$. Then, as O_0 and L_i have the same size, through any point $P \in O_0$ there pass exactly $m_{-i \pmod t}$ lines in L_i, each of which meets O_0 in $m_{-i \pmod t}$ points. Therefore, the points on O_0 can be counted as follows:

$$\frac{q^2 + q + 1}{t} = 1 + \sum_{i=0}^{t-1} m_i(m_i - 1),$$

or, equivalently,

$$\frac{q^2 + q + 1}{t} + q = \sum_{i=0}^{t-1} m_i^2, \tag{3}$$

whence the assertion follows. □

Corollary 3.9. *Let $s = s(p, t)$ be as in Definition 3.1. Let $O_{i_1}, \dots, O_{i_s}$ be orbit representatives of the action of τ on the orbits $O_1, \dots, O_{t-1}$. If t is prime, then*

(i) $m_0 + \dfrac{t-1}{s} \sum_{j=1}^{s} m_{i_j} = q + 1$;

(ii) $m_0^2 + \dfrac{t-1}{s} \sum_{j=1}^{s} m_{i_j}^2 = \dfrac{q^2 + (t+1)q + 1}{t}$.

Theorem 3.10. *Let E_t be any orbit under the action of the subgroup of the Singer group of size $(q^2+q+1)/t$, and let $s = s(p,t)$ be as in Definition* 3.1*. If t is prime, then all but at most one character ℓ satisfy*

$$\frac{q+1-\left(1+\sqrt{ts}\right)\sqrt{q}}{t} \leq \ell \leq \frac{q+1+\left(1+\sqrt{ts}\right)\sqrt{q}}{t}, \tag{4}$$

and if $\tilde{\ell}$ is the possible exception, then

$$\frac{q+1-(t-1)\sqrt{q}}{t} \leq \tilde{\ell} \leq \frac{q+1+(t-1)\sqrt{q}}{t}. \tag{5}$$

Proof. Let $O_{i_1}, \ldots, O_{i_s}$ be orbit representatives of the action of τ on the orbits $O_1, \ldots, O_{t-1}$. Assume without loss of generality that $E_t = O_0$. We are going to prove that

$$\frac{q+1-(t-1)\sqrt{q}}{t} \leq m_0 \leq \frac{q+1+(t-1)\sqrt{q}}{t} \tag{6}$$

and, for each $j = 1, \ldots, s$,

$$\frac{q+1-\left(1+\sqrt{ts}\right)\sqrt{q}}{t} \leq m_{i_j} \leq \frac{q+1+\left(1+\sqrt{ts}\right)\sqrt{q}}{t}. \tag{7}$$

Let $\bar{x}$ the arithmetic mean of $\{m_{i_1}, \ldots, m_{i_s}\}$, and let V be its variance. Let $\bar{y} = \bar{x}^2 + V$. By Corollary 3.9 we have that

$$\left(q+1-(t-1)\bar{x}\right)^2 + (t-1)\bar{y} = \frac{q^2+(t+1)q+1}{t}.$$

By straightforward computation it follows that

$$\bar{x}\left(2(q+1)-t\bar{x}\right) = \frac{q^2+q+1}{t} + V.$$

Then $\bar{x}\left(2(q+1)-t\bar{x}\right) \geq \frac{q^2+q+1}{t}$ implies that

$$\frac{q+1-\sqrt{q}}{t} \leq \bar{x} \leq \frac{q+1+\sqrt{q}}{t}. \tag{8}$$

Then (6) follows from (8), taking into account that $m_0 = q+1-(t-1)\bar{x}$.

Also, since $\bar{x}\left(2(q+1)-t\bar{x}\right) \leq \frac{q^2+2q+1}{t}$, we have that $V \leq \frac{q}{t}$. Then Chebyshev's inequality yields

$$|m_{i_j} - \bar{x}| \leq \sqrt{s\frac{q}{t}},$$

whence, taking into account (8), equation (7) follows. □

Note that equality in (5) can hold, for instance when $t = q - \sqrt{q} + 1$. In this case, E_t is a Baer subplane and $\tilde{\ell} = \sqrt{q} + 1$.

The case $s(p,t) = 1$ was thoroughly investigated in [15].

When $s(p,t) = 2$, Theorem 3.10 can be slightly improved. Let $t = 2d + 1$ and assume without loss of generality that

$$m_1 = \cdots = m_d \geq m_{d+1} = \cdots = m_{t-1} .$$

Let $U_1 = m_1 + m_{d+1}$ and $U_2 = m_1 - m_{d+1}$. Then from Corollary 3.9 the following equality is easily obtained:

$$2(q^2 + q + 1) + \frac{t^2 U_1^2}{2} - 2t(q+1)U_1 = -\frac{tU_2^2}{2} ,$$

that is,

$$tU_2^2 + (tU_1 - 2q - 2)^2 = 4q .$$

Therefore,

$$m_1 \leq m_{d+1} + 2\frac{\sqrt{q}}{\sqrt{t}} .$$

On the other hand (8) yields that

$$m_{d+1} \leq -m_1 + \frac{2}{t}(q + \sqrt{q} + 1) .$$

Then

$$2m_1 \leq \frac{2}{t}(q + \sqrt{q} + 1) + 2\frac{\sqrt{q}}{\sqrt{t}} ,$$

and finally the following improvement of (7) is obtained.

Proposition 3.11. *Assume that $s(p,t) = 2$ and that t is prime. Then for all but one characters ℓ of E_t, the following holds:*

$$\frac{q + 1 - (1 + \sqrt{t})\sqrt{q}}{t} \leq \ell \leq \frac{q + 1 + (1 + \sqrt{t})\sqrt{q}}{t} .$$

A sufficient condition for $s(p,t) = 2$ is pointed out.

Proposition 3.12. *Let t be a prime number such that $6 \mid (t-1)$. Let $q = p^h$ be such that $p \equiv \omega^2$ for some primitive element ω in $\mathbb{Z}_t$. Let ω^i be a primitive 6-th roots of unity in $\mathbb{Z}_t$. If either*

$$h = i + d\left(\frac{t-1}{2}\right) \quad \text{or} \quad h = 2i + d\left(\frac{t-1}{2}\right)$$

for some positive integer d, then both $t \mid q^2 + q + 1$ and $s(r,t) = 2$ hold.

Proof. Note that ω^{2i} and ω^{4i} are two distinct roots of X^2+X+1. The condition $t \mid p^{2h}+p^h+1$ is then equivalent to either $p^h \equiv \omega^{2i} \pmod t$ or $p^h \equiv \omega^{4i} \pmod t$. As $p \equiv \omega^2$, the claim follows. □

Remark 3.13. When $p \equiv 1 \pmod 3$, $s(p,3)=2$ holds. Then by Theorem 3.7 the number of characters of E_3 is at most 3. Actually, in [8] it was proved that equality holds.

Remark 3.14. In [2], two sporadic examples of sets E_t with $s(p,t)>1$ and only 2 characters were pointed out. Whether these are the only examples remains an open problem.

4 Linear codes arising from sharply transitive sets

Given a subset K of n points in $\mathrm{PG}(2,q)$, the matrix whose columns are homogenous coordinates of the points in K can be viewed as a generator matrix for an $[n,3,d]_q$-code, that is, a q-ary linear code C_K of length n, dimension 3 and minimum distance d. The same matrix is a parity check matrix for the dual code $C_K^{\perp}$.

The relationship between subsets of $\mathrm{PG}(2,q)$ and their associated codes has been thoroughly investigated, see for instance the survey paper [17]. In particular, the weight distributions of both C_K and $C_K^{\perp}$ is determined by the geometry of K, as codewords in C_K of weight w correspond to lines meeting K in exactly $n-w$ points.

Denote by $r(K)$ the largest character of K. As the minimum distance d of C_K is $n-r(K)$, the case when $r(K)$ is small with respect to n is of particular interest when the error capability of C_K is considered. In particular, optimal codes are obtained when the Griesmer bound $n \geq \sum_{i=0}^{2}\lceil d/q^i \rceil$ [25, Theorem 5.2.6] is attained, that is, when

$$n > (r(K)-2)q + r(K)\,.$$

On the other hand, when K is a complete arc the dual code $C_K^{\perp}$ has good covering properties. More precisely, $C_K^{\perp}$ is a quasi-perfect MDS code with best covering density when n is as small as possible. It should also be pointed out that if K is fixed by a group G of collineations of $\mathrm{PG}(2,q)$, then G is isomorphic to a semilinear automorphism group of both C_K and $C_K^{\perp}$, which can be a useful tool for efficient decoding, see [18].

The following corollary to Theorem 3.10 is immediately obtained.

Theorem 4.1. *Let E_t be any orbit under the action of the subgroup of the Singer group of size $(q^2+q+1)/t$. If t is prime, then*

$$r(E_t) \leq \frac{q+1}{t} + \frac{t-1}{t}\sqrt{q}\,.$$

Theorem 4.1 yields that if t is small, then the size n of E_t is large with respect to $r(E_t)$. In general, the best that can be done to get a set with large size with respect to its maximum character r is taking the union of $\lfloor r/2 \rfloor$ conics, see the survey paper [1]. This gives arcs for which n/q is about $r/2$. For a set E_t, Theorem 4.1 yields that n/q is greater than $r - \sqrt{tr}$. It is worth noticing that the Griesmer bound is attained by E_t for the following values of q and t (the computation of $r(E_t)$ is a result of a computer search).

q	t	n	$r(E_t)$
23	7	79	5
29	13	67	4
32	7	151	6
81	7	949	13
109	21	571	7
256	13	5061	21
343	37	3189	11
625	21	18631	31

Table 1: $[n, 3, n - r(E_t)]_q$-codes attaining the Griesmer bound

References

[1] **S. Ball** and **J. W. P. Hirschfeld**, Bounds on (n, r)-arcs and their application to linear codes, *Finite Fields Appl.* **11** (2005), 326–336.

[2] **L. Batten** and **J. Dover**, Sets of type (m, n) in cubic order planes, *Des. Codes Cryptogr.* **16** (1999), 211–213.

[3] **M. Biliotti** and **G. Korchmáros**, Transitive blocking sets in cyclic projective planes, *Mitt. Math. Sem. Giessen* **201** (1991), 35–38.

[4] ______, Blocking sets which are preserved by transitive collineation groups, *Forum Math.* **4** (1992), 567–591.

[5] **E. Borós** and **T. Szőnyi**, On the sharpness of a theorem of B. Segre, *Combinatorica* **6** (1986), 261–268.

[6] **A. E. Brouwer**, A series of separable designs with application to pairwise orthogonal Latin squares, *European J. Combin.* **1** (1980), 137–146.

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

[8] **J. Coykendall** and **J. Dover**, Sets with few Intersection Numbers from Singer Subgroup Orbits, *European J. Combin.* **22** (2001), 455–464.

[9] **A. A. Davydov**, **G. Faina**, **S. Margucini** and **F. Pambianco**, Computer search in projective planes for the sizes of complete arcs, *J. Geom.* **82** (2005), 50–62.

[10] **M. de Finis**, On k-sets of type (m, n) in projective planes of square order, in *Finite Geometries and Designs*, P.J. Cameron, J.W.P. Hirschfeld and D.R. Hughes (Eds.), London Math. Soc. Lecture Notes Ser. **49** (1981), 98–103.

[11] **P. Dembowski**, *Finite Geometries*, Springer, Berlin, 1968.

[12] **M. J. de Resmini**, An infinite family of type (m, n) sets in PG$(2, q^2)$, q a square, *J. Geom.* **20** (1983), 36–43.

[13] **G. L. Ebert**, Partitioning projective geometries into caps, *Canad. J. Math.* **37** (1985), 1163-1175.

[14] **J. C. Fisher**, **J. W. P. Hirschfeld** and **J. A. Thas**, Complete arcs in planes of square orders, *Ann. Discrete Math.* **30** (1986), 243–250.

[15] **N. Hamilton** and **T. Penttila**, Sets of Type (a, b) From Subgroups of $\Gamma L(1, p^R)$, *J. Algebraic Combin.* **13** (2001), 67–76.

[16] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1998.

[17] **J. W. P. Hirschfeld** and **L. Storme**, The packing problem in statistics, coding theory and finite projective spaces, *J. Statist. Plann. Inference* **72** (1998), 355–380.

[18] **W. C. Huffman**, Codes and groups, *Handbook of coding theory, Vol.* II, 1345–1440, North-Holland, Amsterdam, 1998.

[19] **B. C. Kestenband**, Unital intersections in finite finite projective planes, *Geom. Dedicata* **11** (1981), 107-117.

[20] **G. Korchmáros**, Gruppi di collineazioni transitivi sui punti di una ovale [$(q+2)$-arco] di $S_{2,q}$, q pari, *Atti Semin. Mat. Fis. Univ. Modena* **27** (1978), 89–105.

[21] **C. M. O'Keefe** and **T. Penttila**, Symmetries of arcs, *J. Combin. Theory Ser. A* **66** (1994), 53–67.

[22] **J. Singer**, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.

[23] **L. Storme**, Transitive arcs in planes of even order, *European J. Combin.* **17** (1996), 757–768.

[24] **L. Storme** and **H. van Maldeghem**, Cyclic arcs in PG$(2,q)$, *J. Algebraic Combin.* **3** (1994), 113–128.

[25] **J. H. van Lint**, *An Introduction to Coding Theory*, Third edition, Springer, Berlin, 1998.

Alexander A. Davydov

Institute for Information Transmissin Problems, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, 127994 Moscow, Russian Federation

e-mail: adav@iitp.ru

Massimo Giulietti

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, 06123 Perugia, Italy

e-mail: giuliet@dipmat.unipg.it

Stefano Marcugini

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, 06123 Perugia, Italy

e-mail: gino@dipmat.unipg.it

Fernanda Pambianco

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, 06123 Perugia, Italy

e-mail: fernanda@dipmat.unipg.it