On small dense sets in Galois planes

M. Giulietti*

Dipartimento di Matematica e Informatica
Università di Perugia, Italy
giuliet@dipmat.unipg.it

Submitted: Jul 17, 2007; Accepted: Oct 31, 2007; Published: Nov 5, 2007
Mathematics Subject Classification: 51E20

Abstract

This paper deals with new infinite families of small dense sets in desarguesian projective planes $PG(2,q)$. A general construction of dense sets of size about $3q^{2/3}$ is presented. Better results are obtained for specific values of q. In several cases, an improvement on the best known upper bound on the size of the smallest dense set in $PG(2,q)$ is obtained.

1 Introduction

A dense set $\mathcal{K}$ in $PG(2,q)$, the projective plane coordinatized over the finite field with q elements $\mathbb{F}_q$, is a point-set whose secants cover $PG(2,q)$, that is, any point of $PG(2,q)$ belongs to a line joining two distinct points of $\mathcal{K}$. As well as being a natural geometrical problem, the construction of small dense sets in $PG(2,q)$ is relevant in other areas of Combinatorics, as dense sets are related to covering codes, see Section 4, and defining sets of block designs, see [2]; also, it has been recently pointed out in [13] that small dense sets are connected to the degree/diameter problem in Graph Theory [17].

A straightforward counting argument shows that a trivial lower bound for the size k of a dense set in $PG(2,q)$ is $k \geq \sqrt{2q}$, see e.g. [19]. On the other hand, for q square there is a nice example of a dense set of size $3\sqrt{q}$, namely the union of three non-concurrent lines of a subplane of $PG(2,q)$ of order $\sqrt{q}$.

If q is not a square, however, the trivial lower bound is far away from the size of the known examples. The existence of dense sets of size $\lfloor 5\sqrt{q \log q} \rfloor$ was shown by means of probabilistic methods, see [2, 14]. The smallest dense sets explicitly constructed so far have size approximately $cq^{\frac{3}{4}}$, with c a constant independent on q, see [1, 9, 18]; for

*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 2006-2007

a survey see [2, Sections 3,4]. A construction by Davydov and Östergård [6, Thm. 3] provides dense sets of size $2q/p + p$, where p is the characteristic of $\mathbb{F}_q$; note that in the special case where $q = p^3$, $p \geq 17$, the size of these dense sets is less than $q^{\frac{3}{4}}$.

The main result of the present paper is a general explicit construction of dense sets in $PG(2, q)$ of size about $3q^{\frac{2}{3}}$, see Theorem 3.2. For large non-square q, $q \neq p^3$, these are the smallest explicitly constructed dense sets, whereas for $q = p^3$ the size is the same as that of the example by Davydov and Östergård.

Using the same technique, smaller dense sets are provided for specific values of q, see Theorem 3.7 and Corollary 3.8; in some cases they even provide an improvement on the probabilistic bound, see Table 1.

Our constructions are essentially algebraic, and use linearized polynomials over the finite field $\mathbb{F}_q$. For properties of linearized polynomials see [15, Chapter 3]. In the affine line $AG(1, q)$, take a subset A whose points are coordinatized by an additive subgroup H of $\mathbb{F}_q$. Then H consists of the roots of a linearized polynomial $L_H(X)$. Let D_1 be the union of two copies of A, embedded in two parallel lines in $AG(2, q)$, namely the lines with equation $Y = 0$ and $Y = 1$. The condition for a point $P = (u, v)$ in $AG(2, q)$ to belong to some secant of D_1 is that the equation

$$L_H(X) - vL_H(Y) + u = 0$$

has at least one solution in $\mathbb{F}_{q^2}$. This certainly occurs when the equation

$$L_H(X) - vL_H(Y) = 0 \quad \text{has precisely } q \text{ solutions in } \mathbb{F}_q^2. \tag{1}$$

This leads to the purely algebraic problem of determining the values of v for which (1) holds. A complete solution is given in Section 2, see Proposition 2.5, by showing that this occurs if and only if $-v$ belongs to the set $\mathbb{F}_q \setminus \mathcal{M}_H$, with

$$\mathcal{M}_H := \left\{ \frac{L_{H_1}(\beta_1)^p}{L_{H_2}(\beta_2)^p} \right\}. \tag{2}$$

Here, H_1 and H_2 range over all subgroups of H of index p, that is $\mid H \mid / \mid H_i \mid = p$, while $\beta_i \in H \setminus H_i$.

This shows that the points which are not covered by the secants of D_1 are the points $P = (u, v)$ with $-v \in \mathcal{M}_H$. The final step of our construction consists in adding a possibly small number of points $Q_1, \ldots, Q_t$ to D_1 to obtain a dense set. For the general case, this is done by just ensuring that the secants Q_iQ_j cover all points uncovered by the secants of D_1. For special cases, the above construction can give better results when more than two copies of A are used.

It should be noted that sometimes in the literature dense sets are referred to as 1-*saturating* sets as well.

2 On the number of solutions of certain equations over $\mathbb{F}_q$

Let $q = p^\ell$ with p prime, and let H be an additive subgroup of $\mathbb{F}_q$ of size p^s with $2s \leq \ell$. Also, let

$$L_H(X) = \prod_{h \in H} (X - h) \in \mathbb{F}_q[X]. \tag{3}$$

Then L_H is a linearized polynomial, that is, there exist $\beta_0, \dots, \beta_s \in \mathbb{F}_q$ such that $L_H(X) = \sum_{i=0}^s \beta_i X^{p^i}$, see e.g. [15, Theorem 3.52].

For $m \in \mathbb{F}_q$, let

$$F_m(X, Y) = L_H(X) - mL_H(Y). \tag{4}$$

As the evaluation map $(x, y) \mapsto F_m(x, y)$ is an additive map from $\mathbb{F}_q^2$ to $\mathbb{F}_q$, the equation $F_m(X, Y) = 0$ has at least q solutions in $\mathbb{F}_q^2$. The aim of this section is to determine for what $m \in \mathbb{F}_q$ the number of solutions of $F_m(X, Y) = 0$ is precisely q, see Proposition 2.5.

Let $\mathbb{F}_p$ denote the prime subfield of $\mathbb{F}_q$.

Lemma 2.1. *If $m \in \mathbb{F}_p$, then the number of solutions in $\mathbb{F}_q^2$ of the equation $F_m(X, Y) = 0$ is qp^s.*

Proof. Note that as $m \in \mathbb{F}_p$, $mL_H(Y) = L_H(mY)$ holds. Then,

$$F_m(X, Y) = L_H(X - mY) = \prod_{h \in H} (X - mY - h).$$

As the equation $X - mY - h = 0$ has q solutions in $\mathbb{F}_q^2$, the claim follows. □

Lemma 2.2. *For any $\alpha \in \mathbb{F}_q$,*

$$X^p - \alpha^{p-1} X = \prod_{i \in \mathbb{F}_p} (X - i\alpha)\,.$$

Proof. The assertion is trivial for $\alpha = 0$. For $\alpha \neq 0$, the claim follows from

$$\prod_{i \in \mathbb{F}_p} (X - i\alpha) = \alpha^p \prod_{i \in \mathbb{F}_p} \left(\frac{X}{\alpha} - i \right) = \alpha^p \left(\left(\frac{X}{\alpha} \right)^p - \frac{X}{\alpha} \right)\,.$$

□

For any subgroup H' of H of size p^{s-1}, pick an element $\beta \in H \setminus H'$ and let

$$a_{H'} = L_{H'}(\beta)^{p-1}. \tag{5}$$

Note that $a_{H'}$ does not depend on β. In fact,

$$\prod_{h \in H} (X - h) = \prod_{i \in \mathbb{F}_p} \prod_{h' \in H'} (X - h' - i\beta) = \prod_{i \in \mathbb{F}_p} L_{H'}(X - i\beta) = \prod_{i \in \mathbb{F}_p} \left(L_{H'}(X) - iL_{H'}(\beta) \right)\,,$$

and then, by Lemma 2.2,

$$L_H(X) = L_{H'}(X)^p - a_{H'} L_{H'}(X). \tag{6}$$

Also, if $a_{H_1} = a_{H_2}$ holds for two subgroups H_1 and H_2 of H, then by (6) it follows that

$$(L_{H_1}(X) - L_{H_2}(X))^p = a_{H_1}(L_{H_1}(X) - L_{H_2}(X));$$

this yields $L_{H_1}(X) = L_{H_2}(X)$, whence $H_1 = H_2$.

Let

$$\mathcal{M}_H := \left\{ \frac{L_{H_1}(\beta_1)^p}{L_{H_2}(\beta_2)^p} \mid H_1, H_2 \text{ subgroups of } H \text{ of size } p^{s-1},\ \beta_i \in H \setminus H_i \right\}. \tag{7}$$

Note that for any $\lambda \in \mathbb{F}_p$,

$$\frac{L_{H_1}(\lambda\beta_1)^p}{L_{H_2}(\beta_2)^p} = \lambda \frac{L_{H_1}(\beta_1)^p}{L_{H_2}(\beta_2)^p},$$

whence $\lambda\mathcal{M}_H = \mathcal{M}_H$ holds provided that $\lambda \neq 0$. In particular,

$$-\mathcal{M}_H = \mathcal{M}_H. \tag{8}$$

As $H_1 = H_2$ is allowed in (7), we also have that

$$\mathbb{F}_p^* \subseteq \mathcal{M}_H. \tag{9}$$

Lemma 2.3. *For any $m \in \mathcal{M}_H$, the equation $F_m(X, Y) = 0$ has at least pq solutions.*

Proof. Fix H_1, H_2 subgroups of H of size p^{s-1}, $\beta_1 \in H \setminus H_1$, and $\beta_2 \in H \setminus H_2$, in such a way that $m = \frac{L_{H_1}(\beta_1)^p}{L_{H_2}(\beta_2)^p}$. Let $\alpha = \frac{L_{H_1}(\beta_1)}{L_{H_2}(\beta_2)}$. We claim that

$$F_m(X, Y) = \prod_{i \in \mathbb{F}_p} (L_{H_1}(X - i\beta_1) - \alpha L_{H_2}(Y)). \tag{10}$$

In order to prove (10), note first that by Lemma 2.2

$$\prod_{i \in \mathbb{F}_p} (L_{H_1}(X - i\beta_1) - \alpha L_{H_2}(Y)) = (L_{H_1}(X) - \alpha L_{H_2}(Y))^p - a_{H_1}(L_{H_1}(X) - \alpha L_{H_2}(Y)).$$

Then, Equation (6) for $H' = H_1$ gives

$$\prod_{i \in \mathbb{F}_p} (L_{H_1}(X - i\beta_1) - \alpha L_{H_2}(Y)) = L_H(X) - \alpha^p L_{H_2}(Y)^p + a_{H_1}\alpha L_{H_2}(Y).$$

As $a_{H_1}\alpha = \alpha^p a_{H_2}$ and $m = \alpha^p$, Equation (6) for $H' = H_2$ implies (10).

Now, the set of solutions of $L_{H_1}(X) - \alpha L_{H_2}(Y) = 0$ has size at least q, as it is the nucleus of an $\mathbb{F}_p$-linear map from $\mathbb{F}_q^2$ to $\mathbb{F}_q$. As the solutions of $L_{H_1}(X - i\beta_1) - \alpha L_{H_2}(Y) = 0$ are obtained from those of $L_{H_1}(X) - \alpha L_{H_2}(Y) = 0$ by the substitution $X \mapsto X + i\beta_1$, (10) yields that $F_m(X, Y) = 0$ has at least pq solutions. $\square$

Lemma 2.4. *The size of $\mathcal{M}_H$ is at most $(p^s-1)^2/(p-1)$.*

Proof. Note that for each pair H_1, H_2 of subgroups of H of size p^{s-1} there are precisely $p-1$ elements in $\mathcal{M}_H$ of type $L_{H_1}(\beta_1)^p/L_{H_2}(\beta_2)^p$. In fact,

$$\left(\frac{L_{H_1}(\beta_1)^p}{L_{H_2}(\beta_2)^p}\right)^{p-1} = \frac{a_{H_1}^p}{a_{H_2}^p}.$$

As a_{H_1}/a_{H_2} only depends on H_1 and H_2, the claim follows.

Now, the number of additive subgroups of H of size p^{s-1} is $(p^s-1)/(p-1)$. Therefore $\mathcal{M}_H$ consists of at most

$$(p-1)\cdot\left(\frac{p^s-1}{p-1}\right)^2$$

elements. □

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

Proposition 2.5. *Let $F_m(X,Y)$ be as in* (4)*. The equation $F_m(X,Y)=0$ has more than q solutions if and only if either $m \in \mathcal{M}_H$ or $m=0$.*

Proof. The claim for $m=0$ follows from Lemma 2.1. Assume then that $m \neq 0$. Denote ν_m the number of solutions of $F_m(X,Y)=0$. Also, denote $\mathbb{F}_q^*/\mathbb{F}_p^*$ the factor group of the multiplicative group of $\mathbb{F}_q^*$ by $\mathbb{F}_p^*$. Consider the map

$$\begin{aligned}\Phi:\ \ &\{(H_1,H_2)\mid H_1,H_2 \text{ subgroups of } H \text{ of size } p^{s-1},\ H_1\neq H_2\} \to \mathbb{F}_q^*/\mathbb{F}_p^*\\ &(H_1,H_2)\mapsto \tfrac{L_{H_1}(\beta_1)^p}{L_{H_2}(\beta_2)^p}\ \mathbb{F}_p^*\,,\end{aligned}$$

with $\beta_i \in H\setminus H_i$. Note that Φ is well defined: for any $\beta_i, \beta_i' \in H\setminus H_i$, $L_{H_i}(\beta_i)^p = \lambda L_{H_i}(\beta_i')^p$ for some $\lambda \in \mathbb{F}_p^*$, as

$$L_{H_i}(\beta_i)^{p-1} = L_{H_i}(\beta_i')^{p-1} = a_{H_i}$$

(see (5)).

For any $\mu \in \mathcal{M}_H$, the size of $\Phi^{-1}(\mu\mathbb{F}_p^*)$ is related to ν_μ. More precisely,

$$\#\Phi^{-1}(\mu\mathbb{F}_p^*) \leq \frac{\frac{\nu_\mu}{q}-1}{p-1}. \tag{11}$$

In order to prove (11), write the unique factorization of F_μ as follows:

$$F_\mu(X,Y) = P_1(X,Y)\cdot P_2(X,Y)\cdot\ldots\cdot P_r(X,Y).$$

Note that the multiplicity of each factor is 1. In fact, all the roots of $L_H(X)$ are simple, whence both the partial derivatives of F_μ are non-zero constants. Assume that $\Phi(H_1,H_2)=\mu\mathbb{F}_p^*$. Let $\alpha = \frac{L_{H_1}(\beta_1)}{L_{H_2}(\beta_2)}$, and note that, by Equation (10),

$$F_\mu(X,Y) = (L_{H_1}(X)-\alpha L_{H_2}(Y))\prod_{i\in\mathbb{F}_p^*}(L_{H_1}(X-i\beta_1)-\alpha L_{H_2}(Y))\,.$$

Assume without loss of generality that $P_1(0,0)=0$, so that $P_1(X,Y)$ divides $L_{H_1}(X)-\alpha L_{H_2}(Y)$. We consider two actions of the group H on the set of irreducible factors of F_μ. For each $h\in H$, let $(P_i(X,Y))^{\sigma_1(h)}=P_i(X+h,Y)$, and $(P_i(X,Y))^{\sigma_2(h)}=P_i(X,Y+h)$. Assume that the stabilizer S_1 of $P_1(X,Y)$ with respect to the action σ_1 has order p^t. Then the X-degree of $P_1(X,Y)$ is at least p^t. Note also that the orbit of $P_1(X,Y)$ with respect to σ_1 consists of p^{s-t} factors, each of which has X-degree not smaller than p^t. As the X-degree of F_μ is p^s, we have that $r=p^{s-t}$, and that the X-degree of $P_1(X,Y)$ is precisely p^t. Taking into account that S_1 stabilizes $P_1(X,Y)$, we have that for any $h\in S_1$ the polynomial $X+h$ divides $P_1(X,Y)-P_1(0,Y)$, whence

$$P_1(X,Y)-P_1(0,Y)=Q(Y)L_{S_1}(X) \tag{12}$$

for some polynomial Q. Now, let S_2 be the stabilizer of $P_1(X,Y)$ under the action σ_2, and let $p^{t'}$ be the order of S_2. The above argument yields that $r=p^{s-t'}$, and therefore $t=t'$. Also,

$$P_1(X,Y)-P_1(X,0)=\bar{Q}(X)L_{S_2}(Y) \tag{13}$$

for some polynomial $\bar{Q}$. As the degrees of $P_1(X,Y)$, $L_{S_1}(X)$, $L_{S_2}(Y)$ are all equal to p^t, Equation (12) together with (13) imply that

$$P_1(X,Y)=\gamma L_{S_1}(X)-\gamma' L_{S_2}(Y),$$

for some γ', $\gamma\in\mathbb{F}_q$. Therefore,

$$\nu_\mu\geq qr=qp^{s-t}.$$

As $P_1(X,Y)$ divides $L_{H_1}(X)-\alpha L_{H_2}(Y)$, and as H_1 is the stabilizer of the set of factors of $L_{H_1}(X)-\alpha L_{H_2}(Y)$ with respect to the action σ_1, the group S_1 is a subgroup of H_1. The number of possibilities for subgroups H_1 is then less than or equal to the number of subgroups of H of size p^{s-1} containing S_1, which is $\frac{p^{s-t}-1}{p-1}$. Also, for a fixed H_1, there is at most one possibility for H_2; in fact, $\Phi(H_1,H_2)=\Phi(H_1,H_2')$ yields $a_{H_2}=a_{H_2'}$, which has already been noticed to imply $H_2=H_2'$. Then

$$\#\Phi^{-1}(\mu\mathbb{F}_p^*)\leq\frac{p^{s-t}-1}{p-1},$$

and therefore (11) is fulfilled.

Now, let M be the size of $\mathcal{M}_H\setminus\mathbb{F}_p$. By counting the number of pairs $(x,y)\in\mathbb{F}_q^2$ such that $L_H(x)\neq 0$ and $L_H(y)\neq 0$, we obtain

$$(q-p^s)^2=\sum_{m\in\mathbb{F}_q^*}\left(\nu_m-p^{2s}\right).$$

Then, taking into account Lemma 2.1,

$$(q-p^s)^2\geq(p-1)(qp^s-p^{2s})+(q-p-M)(q-p^{2s})-Mp^{2s}+\sum_{\mu\in\mathcal{M}_H\setminus\mathbb{F}_p}\nu_\mu. \tag{14}$$

Note that if equality holds in (14), then the proposition is proved. Straightforward computation yields that (14) is equivalent to

$$-M + \sum_{\mu \in \mathcal{M}_H \setminus \mathbb{F}_p} \frac{\nu_\mu}{q} \leq (p^s - p)(p^s - 1).$$

Let M_v be the number of elements μ in $\mathcal{M}_H \setminus \mathbb{F}_p$ such that $\nu_\mu = qp^v$. Then

$$-M + \sum_{\mu \in \mathcal{M}_H \setminus \mathbb{F}_p} \frac{\nu_\mu}{q} = \sum_v M_v(p^v - 1).$$

On the other hand, taking into account (11), we obtain that

$$\sum_v M_v(p^v - 1) \geq \sum_{\mu \mathbb{F}_p^* \in Im(\Phi)} (p-1)^2 \# \Phi^{-1}(\mu \mathbb{F}_p^*) = (p-1)^2 \frac{p^s - 1}{p - 1} \frac{p^s - p}{p - 1} = (p^s - p)(p^s - 1).$$

Therefore equality must hold in (14), and the claim is proved. □

3 Dense sets in $PG(2, q)$

Let $q = p^\ell$. For an additive subgroup H of $\mathbb{F}_q$ of size p^s with $2s \leq \ell$, let $L_H(X)$ be as in (3), and $\mathcal{M}_H$ be as in (7). For an element $\alpha \in \mathbb{F}_q$, define

$$D_{H,\alpha} = \{(L_H(a) : \alpha : 1) \mid a \in \mathbb{F}_q\} \subset PG(2, q). \tag{15}$$

As a corollary to Proposition 2.5, the following result is obtained.

Proposition 3.1. *Let α_1, α_2 be distinct elements in $\mathbb{F}_q$. Then a point $P = (u : v : 1)$ belongs to a line joining two points of $D_{H,\alpha_1} \cup D_{H,\alpha_2}$ provided that $v \notin (\alpha_2 - \alpha_1)\mathcal{M}_H + \alpha_2$.*

Proof. Assume that $v \notin (\alpha_2 - \alpha_1)\mathcal{M}_H + \alpha_2$ and that $v \neq \alpha_2$. Then by Proposition 2.5, the equation

$$L_H(X) + \frac{v - \alpha_2}{\alpha_1 - \alpha_2} L_H(Y) = 0$$

has precisely q solutions, or, equivalently, the additive map

$$(x, y) \mapsto L_H(x) + \frac{v - \alpha_2}{\alpha_1 - \alpha_2} L_H(y)$$

is surjective. This yields that there exists $b, b' \in \mathbb{F}_q$ such that

$$L_H(b) + \frac{v - \alpha_2}{\alpha_1 - \alpha_2} L_H(b') = u,$$

which is precisely the condition for the point $P = (u : v : 1)$ to belong to the line joining $(L_H(b' + b) : \alpha_1 : 1) \in D_{H,\alpha_1}$ and $(L_H(b) : \alpha_2 : 1) \in D_{H,\alpha_2}$.

If $v = \alpha_2$, then clearly P is collinear with two points in $\{(L_H(a) : \alpha_2 : 1) \mid a \in \mathbb{F}_q\}$. □

Theorem 3.2. *Let $q = p^\ell$, and let H be any additive subgroup of $\mathbb{F}_q$ of size p^s, with $2s \le \ell$. Let $L_H(X)$ be as in* (3)*, and $\mathcal{M}_H$ be as in* (7)*. Then the set*

$$\begin{aligned} D =& \{(L_H(a) : 1 : 1), (L_H(a) : 0 : 1) \mid a \in \mathbb{F}_q\} \cup \{(0 : m : 1) \mid m \in \mathcal{M}_H\} \\ & \cup \{(0 : 1 : 0), (1 : 0 : 0)\} \end{aligned}$$

is a dense set of size at most

$$\frac{2q}{p^s} + \frac{(p^s-1)^2}{p-1} + 1.$$

Proof. Let $P = (u : v : 1)$ be a point in $PG(2, q)$. If $v \notin \mathcal{M}_H$, then P belongs to the line joining two points of D by Proposition 3.1, together with (8). If $v \in \mathcal{M}_H$, then P is collinear with $(0 : v : 1) \in D$ and $(1 : 0 : 0) \in D$. Clearly the points $P = (u : v : 0)$ are covered by D as they are collinear with $(1 : 0 : 0)$ and $(0 : 1 : 0)$. Then D is a dense set.

The set $\{L_H(a) \mid a \in \mathbb{F}_q\}$ is the image of an $\mathbb{F}_p$-linear map on $\mathbb{F}_q \cong \mathbb{F}_p^\ell$ whose kernel has dimension s, therefore its size is $p^{\ell-s}$. Note that the point $(0 : 1 : 1)$ belongs to both $\{(L_H(a) : 1 : 1) \mid a \in \mathbb{F}_q\}$ and $\{(0 : m : 1) \mid m \in \mathcal{M}_H\}$. Then the upper bound on the size of D follows from Lemma 2.4. $\square$

The order of magnitude of the size of D of Theorem 3.2 is $p^{\max\{\ell-s,2s-1\}}$. If s is chosen as $\lceil \ell/3 \rceil$, then the size of D satisfies

$$\#D \le \begin{cases} 2q^{\frac{2}{3}} + 1 + \frac{q^{\frac{2}{3}} - 2q^{\frac{1}{3}} + 1}{p-1}, & \text{if } \ell \equiv 0 \pmod 3 \\ 2\left(\frac{q}{p}\right)^{\frac{2}{3}} + 1 + \frac{p^2\left(\frac{q}{p}\right)^{\frac{2}{3}} - 2p\left(\frac{q}{p}\right)^{\frac{1}{3}} + 1}{p-1}, & \text{if } \ell \equiv 1 \pmod 3 \\ 2\frac{1}{p}(qp)^{\frac{2}{3}} + 1 + \frac{(qp)^{\frac{2}{3}} - 2(qp)^{\frac{1}{3}} + 1}{p-1}, & \text{if } \ell \equiv 2 \pmod 3 \end{cases} .$$

Note that when $s = 1$, then $\mathcal{M}_H$ coincides with $\mathbb{F}_p^*$, and then the size of D is $2\frac{q}{p} + p$. A dense set of the same size and contained in three non-concurrent lines was constructed in [6, Thm. 3]. It can be proved by straightforward computation that it is not projectively equivalent to any dense set D constructed here.

In order to obtain a new upper bound on the size of the smallest dense set in $PG(2, q)$, a generalization of Theorem 3.2 is useful. Let $A = \{\alpha_1, \ldots, \alpha_k\}$ be any subset of k elements of $\mathbb{F}_q$, and let

$$D(A) = \bigcup_{i=1,\ldots,k} D_{H,\alpha_i}\,, \qquad \mathcal{M}(A) = \bigcap_{i,j=1,\ldots,k,\ i\neq j} (\alpha_j - \alpha_i)\mathcal{M}_H + \alpha_j. \tag{16}$$

Arguing as in the proof of Theorem 3.2, the following result can be easily obtained from Proposition 3.1.

Theorem 3.3. *The set*

$$D(H, A) = D(A) \cup \{(0 : m : 1) \mid m \in \mathcal{M}(A)\} \cup \{(0 : 1 : 0), (1 : 0 : 0)\}$$

is dense in $PG(2, q)$.

Computing the size of $D(H, A)$ is difficult in the general case, as we do not have enough information on the set $\mathcal{M}(A)$. However, by using some counting argument it is possible to prove the existence of sets A for which a useful upper bound on the size of $\mathcal{M}(A)$ can be established.

Proposition 3.4. *For any $v > 1$, there exists a set $A \subset \mathbb{F}_q$ of size $v + 1$ such that*

$$\#\mathcal{M}(A) \leq \frac{(\#\mathcal{M}_H)^v}{(q-1)^{v-1}}.$$

In order to prove Proposition 3.4, the following two lemmas are needed.

Lemma 3.5. *Let E_1 and E_2 be any two subsets of $\mathbb{F}_q^*$. Then there exists some $\alpha \in \mathbb{F}_q^*$ such that*

$$\#(E_1 \cap \alpha E_2) \leq \frac{\#E_1 \#E_2}{q-1}.$$

Proof. For any $\beta \in \mathbb{F}_q^*$, let $E^{(\beta)}$ be the subset of $\mathbb{F}_q^*$ consisting of those α for which $\beta \in \alpha E_2$. Then

$$\sum_{\beta \in \mathbb{F}_q^*} \#E^{(\beta)} = \#\{(\alpha, \beta) \in (\mathbb{F}_q^*)^2 \mid \beta \in \alpha E_2\} = \sum_{\alpha \in \mathbb{F}_q^*} \#\alpha E_2 = (q-1)\#E_2. \tag{17}$$

Note that the size of $E^{(\beta)}$ does not depend on β, since $E^{(\beta')} = \frac{\beta'}{\beta} E^{(\beta)}$. Therefore, (17) yields that $\#E^{(\beta)} = \#E_2$ for any $\beta \in \mathbb{F}_q^*$. Then

$$\#E_1 \#E_2 = \sum_{\beta \in E_1} \#E^{(\beta)} = \#\{(\alpha, \beta) \in (\mathbb{F}_q^*)^2 \mid \beta \in E_1 \cap \alpha E_2\} = \sum_{\alpha \in \mathbb{F}_q^*} \#(E_1 \cap \alpha E_2),$$

whence the claim follows. $\square$

Lemma 3.6. *Let E be a subset of $\mathbb{F}_q^*$, and let v be an integer greater than 1. Then there exist $\alpha_1 = 1, \alpha_2, \ldots, \alpha_v \in \mathbb{F}_q^*$ such that*

$$\# \bigcap_{i:=1,\ldots,v} \alpha_i E \leq (\#E)^v (q-1)^{1-v}.$$

Proof. We prove the assertion by induction on v. For $v = 2$ the claim is just Lemma 3.5 for $E_1 = E_2 = E$. Assume that the assertion holds for any $v' \leq v$. Then there exist $\alpha_1 = 1, \alpha_2, \ldots, \alpha_{v-1} \in \mathbb{F}_q^*$ such that

$$\# \bigcap_{i:=1,\ldots,v-1} \alpha_i E \leq (\#E)^{v-1} (q-1)^{2-v}.$$

Lemma 3.5 for $E_1 = \cap_{i:=1,\ldots,v-1} \alpha_i E$, $E_2 = E$, yields the assertion. $\square$

Proof of Proposition 3.4. According to Lemma 3.6, there exist $\alpha_1 = 1, \alpha_2, \dots, \alpha_v \in \mathbb{F}_q^*$ such that

$$\# \bigcap_{i:=1,\dots,v} -\alpha_i \mathcal{M}_H \leq (\#\mathcal{M}_H)^v (q-1)^{1-v}.$$

Let $A = \{0, \alpha_1, \dots, \alpha_n\}$, and let $\mathcal{M}(A)$ be as in (16). As

$$\mathcal{M}(A) \subseteq \bigcap_{i:=1,\dots,v} -\alpha_i \mathcal{M}_H,$$

the claim follows. □

As a straightforward corollary to Theorems 3.3 and 3.2, and Proposition 3.4, the following result is then obtained.

Theorem 3.7. *Let $q = p^\ell$, with ℓ odd. Let H be any additive subgroup of $\mathbb{F}_q$ of size p^s, with $2s + 1 = \ell$. Let $L_H(X)$ be as in (3), and $\mathcal{M}_H$ be as in (7). Then for any integer $v \geq 1$ there exists a dense set D in $PG(2, q)$ such that*

$$\#D \leq (v+1)p^{s+1} + (\#\mathcal{M}_H)^v (q-1)^{1-v} + 2. \tag{18}$$

Corollary 3.8. *Let $q = p^{2s+1}$. Then there exists a dense set in $PG(2, q)$ of size less than or equal to*

$$\min_{v=1,\dots,2s+1} \left\{ (v+1)p^{s+1} + \frac{(p^s - 1)^{2v}}{(p-1)^v (p^{(2s+1)} - 1)^{(v-1)}} + 2 \right\}.$$

Proof. The claim follows from Theorem 3.7, together with Lemma 2.4. □

For several values of s and p, Corollary 3.8 improves the probabilistic bound on the size of the smallest dense set in $PG(2, q)$, namely, there exists some integer v such that

$$(v+1)p^{s+1} + \frac{(p^s - 1)^{2v}}{(p-1)^v (p^{(2s+1)} - 1)^{(v-1)}} + 2 < 5\sqrt{q \log q}, \tag{19}$$

see Table 1.

Table 1 - Values of p, s, v for which (19) holds

s	p	v	s	p	v	s	p	v	s	p	v
1	$p \in [3,79]$	1	14	$p \in [5,29]$	8	26	$p=3$	16	36	$p=3$	22
2	$p \in [3,53]$	2	15	$p=3$	10	26	$p \in [5,13]$	14	36	$p=5$	20
3	$p \in [2,83]$	2	15	$p=5$	9	27	$p=3$	17	36	$p=7$	19
4	$p \in [2,53]$	3	15	$p \in [7,31]$	8	27	$p \in [5,7]$	15	37	$p=3$	23
5	$p=2$	4	16	$p=3$	10	27	$p \in [11,17]$	14	37	$p \in [5,7]$	20
5	$p \in [3,73]$	3	16	$p \in [5,23]$	9	28	$p=3$	18	38	$p=3$	24
6	$p=2$	5	17	$p=3$	11	28	$p=5$	16	38	$p=5$	21
6	$p \in [3,47]$	4	17	$p=5$	10	28	$p \in [7,13]$	15	38	$p=7$	20
7	$p=2$	6	17	$p \in [7,29]$	9	29	$p=3$	18	39	$p=3$	24
7	$p=3$	5	18	$p=3$	11	29	$p \in [5,7]$	16	39	$p \in [5,7]$	21
7	$p \in [5,61]$	4	18	$p \in [5,23]$	10	29	$p \in [11,13]$	15	40	$p=3$	25
8	$p=2$	7	19	$p=3$	12	30	$p=3$	19	40	$p=5$	22
8	$p \in [3,43]$	5	19	$p=5$	11	30	$p=5$	17	40	$p=7$	21
9	$p=2$	8	19	$p \in [7,23]$	10	30	$p \in [7,13]$	16	41	$p=3$	26
9	$p=3$	6	20	$p=3$	13	31	$p=3$	19	41	$p=5$	23
9	$p \in [5,47]$	5	20	$p \in [5,19]$	11	31	$p \in [5,7]$	17	41	$p=7$	22
10	$p=2$	9	21	$p=3$	13	31	$p \in [11,13]$	16	42	$p=3$	26
10	$p=3$	7	21	$p=5$	12	32	$p=3$	20	42	$p=5$	23
10	$p \in [5,37]$	6	21	$p \in [7,23]$	11	32	$p=5$	18	42	$p=7$	22
11	$p=2$	10	22	$p=3$	14	32	$p \in [7,11]$	17	43	$p=5$	24
11	$p=3$	7	22	$p \in [5,19]$	12	33	$p=3$	21	43	$p=7$	23
11	$p \in [5,43]$	6	23	$p=3$	15	33	$p \in [5,7]$	18	44	$p=5$	24
12	$p=2$	11	23	$p=5$	13	33	$p=11$	17	44	$p=7$	23
12	$p=3$	8	23	$p \in [7,19]$	12	34	$p=3$	21	45	$p=5$	25
12	$p \in [5,31]$	7	24	$p=3$	15	34	$p=5$	19	45	$p=7$	24
13	$p=2$	12	24	$p \in [5,17]$	13	34	$p \in [7,11]$	18	46	$p=5$	25
13	$p=3$	8	25	$p=3$	16	35	$p=3$	22	47	$p=5$	26
13	$p \in [5,37]$	7	25	$p \in [5,7]$	14	35	$p \in [5,7]$	19	48	$p=5$	26
14	$p=3$	9	25	$p \in [11,17]$	13	35	$p=11$	18	49	$p=5$	27

In order to produce concrete examples of small dense sets of type $D = D(H, A)$, with $\ell = 2s+1$, for which the strict inequality holds in (18), a computer search has been carried out. The sizes of the resulting dense sets are described in Table 2 below. Taking into account that for $q \leq 859$ dense sets of size smaller than $4p^{s+\frac{1}{2}}$ have been obtained by computer in [7, 8], only values of $q > 859$ are considered in Table 2.

Table 2 - Sizes of some dense sets in $PG(2,q)$ of type $D(H,A)$ with $\ell = 2s+1$

q	$\#A$	$\#D(H,A)$	q	$\#A$	$\#D(H,A)$
2^{11}	4	258	5^9	3	9609
2^{13}	4	532	7^5	2	1030
2^{15}	4	1162	7^7	3	7205
2^{17}	5	2576	7^9	3	50947
2^{19}	5	5210	11^5	2	3994
3^7	3	245	11^7	3	43947
3^9	3	764	13^5	2	6592
3^{11}	3	2771	13^7	3	85712
3^{13}	4	8788	17^5	2	14740
5^5	2	376	17^7	3	250599
5^7	3	1877	19^5	2	20578

4 Applications to covering codes

A code with covering radius R is a code such that every word is at distance at most R from a codeword. For linear covering codes over $\mathbb{F}_q$, it is relevant to investigate the so-called *length function* $l(m,R)_q$, that is the minimum length of a linear code over $\mathbb{F}_q$ with covering radius R and codimension m, see the monography [3]. It is well known that the minimum size of a dense set in $PG(2,q)$ coincides with $l(3,2)_q$, see e.g. [4]. From our Corollary 3.8, we then obtain the following result.

Theorem 4.1. *Let $q = p^\ell$, with $\ell = 2s+1$. Then*

$$l(3,2)_q \leq \min_{v=1,\dots,2s+1} \left\{ (v+1)p^{s+1} + \frac{(p^s-1)^{2v}}{(p-1)^v (p^{(2s+1)}-1)^{(v-1)}} + 2 \right\}.$$

It should also be noted that upper bounds on $l(m,2)_q$, $m \geq 5$ odd, can be obtained from small dense sets. In fact, from a dense set of size k in $PG(2,q)$ it can be constructed a linear code over $\mathbb{F}_q$ with covering radius 2, codimension $3+2m$, and length about $q^m k$, see [5, Theorem 1].

References

[1] U. Bartocci, *k-insiemi densi in piani di Galois*, Boll. Un. Mat. Ital. D **2** (1983), 71–77.

[2] E. Boros, T. Szőnyi, and K. Tichler *On defining sets for projective planes*, Discrete Math. **303** (2005), 17–31.

[3] G.D. Cohen, I. Honkala, S. Litsyn, and A.C. Lobstein, “Covering Codes”. Amsterdam, The Netherlands: Elsevier, 1997.

[4] A.A. Davydov, *Constructions and Families of Covering Codes and Saturated Sets of Points in Projective Geometry*, IEEE Trans. Inform. Theory **41** (1995), 2071–2080.

[5] A.A. Davydov, *Constructions and Families of Nonbinary Linear Codes with Covering Radius* 2, IEEE Trans. Inform. Theory **45** (1999), 1679–1686.

[6] A.A. Davydov and P.R.J. Östergård, *On saturating sets in small projective geometries*, European J. Combin. **21** (2000), 563–570.

[7] A.A. Davydov, S. Marcugini and F. Pambianco, *On saturating sets in projective spaces*, J. Combin. Theory Ser. A **103** (2003), 1–15.

[8] A.A. Davydov, S. Marcugini and F. Pambianco, *Linear Codes With Covering Radius* 2*,* 3 *and Saturating Sets in Projective Geometry*, IEEE Trans. Inform. Theory **50** (2004), 537–541.

[9] M. Giulietti and F. Torres, *On dense sets related to plane algebraic curves*, Ars Combinatoria **72** (2004), 33–40.

[10] B.D. Gray, N. Hamilton, C.M. O'Keefe, *On the size of the smallest defining set of* $PG(2, q)$, Bull. Inst. Combin. Appl. **21** (1997), 91–94.

[11] K. Gray, *Defining sets of single-transposition-free designs*, Utilitas Mathematica **38** (1990), 97–103.

[12] K. Gray, *On the minimum number of blocks defining a design*, Bull. Austral. Math. Soc. **41** (1990), 97–112.

[13] G. Kiss, I. Kovács, K. Kutnar, J. Ruff and P. Šparl, *A note on a geometric construction of large Cayley graphs of given degree and diameter*, submitted.

[14] S.J. Kovács, *Small saturated sets in finite projective planes* Rend. Mat. **12** (1992), 157–164.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, Enc. of Math. 20, Addison-Wesley, Reading, 1983.

[16] L. Lunelli and M. Sce, *Considerazioni aritmetiche e risultati sperimentali sui* $\{K; n\}_q$ *archi*, Ist. Lombardo Accad. Sci. Rend. A **98** (1964), 3–52.

[17] M. Miller and J. Širáň, *Moore graphs and beyond: A survey of the degree/diameter problem*, Electron. J. Comb., Dynamical Surveys DS14.

[18] T. Szőnyi, *Complete arcs in finite projective geometries*, Ph. D. Thesis, Univ. L. Eötvös, Budapest, 1984.

[19] E. Ughi, *Saturated configurations of points in projective Galois spaces*, European J. Combin. **8** (1987), 325–334.