ON DENSE SETS RELATED TO PLANE ALGEBRAIC CURVES

MASSIMO GIULIETTI AND FERNANDO TORRES

ABSTRACT. We show that certain subsets of $\mathbf{F}_q$-rational points of the curve $XZ^{n-1} = Y^n$ are dense sets in $\mathbf{P}^2(\mathbf{F}_q)$.

1. INTRODUCTION

A point-set $\mathcal{K}$ of $\mathbf{P}^2(\mathbf{F}_q)$, the projective plane over a finite field $\mathbf{F}_q$ of q elements, is called *dense* provided that any point of the projective plane belongs to a line joining two different points of $\mathcal{K}$. A dense set is called *minimal* if it is so with respect to the set-theoretical inclusion.

Dense sets were introduced by Bartocci [1] as a generalization of the so-called *complete arcs*, namely maximal (with respect to the set-theoretical inclusion) subsets of points of $\mathbf{P}^2(\mathbf{F}_q)$ such that no three of which are collinear. Dense sets are also related to blocking sets, cf. [9, p. 28], as well as to linear codes with covering radius two, cf. [3] and the references therein.

An interesting and difficult problem in finite geometry is to determine the spectrum of the sizes k of minimal dense sets in $\mathbf{P}^2(\mathbf{F}_q)$. It is known that

$$\frac{3+\sqrt{8q+1}}{2} \leq k \leq q+2\,,$$

where the lower bound was noticed by Lunelli and Sce [7] and the upper bound by Bartocci [1]. The union of a line and a point outside the line shows that the upper bound is sharp. If q is not a square, the lower bound is far away from the size of the examples constructed so far; indeed, the smallest dense sets that are currently known have size $\lfloor 6\sqrt{3q\log q} \rfloor$ and their

MSC: 51E21; 14H50.

Keywords: Dense sets; Arcs; Algebraic plane curves over finite fields.

This research was performed within the activity of GNSAGA of the Italian CNR, with the financial support of the Italian Ministry MIUR, project "Strutture geometriche, combinatorica e loro applicazioni", PRIN 2001-2002. The second author acknowledges financial support from the " Secretaria de Estado de Educación y Universidades del Ministerio de Educación, Cultura y Deportes de Espanña"; grant SB2000-0225.

existence was proved by Kovács [5] by means of probabilistic methods. On the other hand, for q square Szőnyi [8] and Ughi [11] independently provided with a nice example of a minimal dense set of size $3\sqrt{q}$, namely the union of three non-concurrent lines of a subplane of $\mathbf{P}^2(\mathbf{F}_q)$ of order $\sqrt{q}$. This example was generalized by Davydov and Östergård [3, Thm. 3] who showed the existence of minimal dense sets of size at most $2q/p + p$, where p is the characteristic of $\mathbf{F}_q$.

Let h be a proper divisor of $q-1$. Bartocci [1] constructed dense sets of size at most $2(q-1)/h+3$ for $q \geq C$, where C is a constant depending just on h. Similarly, Szőnyi [9, Thm. 4.4] constructed dense sets of size $(q-1)/h+h+2$ for $q > [(h-1)^2 + \sqrt{h^4 - 4h^3 + 8h^2 + 1}]^2$. Both constructions are based on a result of Korchmáros [4, p. 330] concerning the completeness property of the arc $\mathcal{K}_{(q-1)/h,2}$ defined below. More precisely, Bartocci's example consists of two projectively equivalent copies of $\mathcal{K}_{(q-1)/h,2}$ and three extra points, whereas Szőnyi's adds $h+2$ collinear points to $\mathcal{K}_{(q-1)/h,2}$.

In this paper we investigate the density in $\mathbf{P}^2(\mathbf{F}_q)$ of the set

$$\mathcal{K}'_{d,n} := \mathcal{K}_{d,n} \cup \{(1:0:0)\}, \quad \text{where} \quad \mathcal{K}_{d,n} := \{(\eta^{in} : \eta^i : 1) : i = 1, \ldots, d\},$$

d and n are positive integers such that d divides $q-1$, and η is a d-th primitive root of the unity in $\mathbf{F}_q$. Notice that $\mathcal{K}'_{d,n}$ is a subset of $\mathbf{F}_q$-rational points of the curve $\mathcal{C}_n : XZ^{n-1} = Y^n$. Our main result is the following.

Theorem 1.1. *$\mathcal{K}'_{d,n}$ is a dense set in $\mathbf{P}^2(\mathbf{F}_q)$ of size $d+1$ provided that the following conditions hold:*

(1) $n \geq 3$;
(2) *the characteristic p of $\mathbf{F}_q$ does not divide n;*
(3) *$(n-1)$ divides d;*
(4) $\gcd(d,n) > 1$;
(5) $q \geq \frac{[(hn-1)(hn-2)+\sqrt{(hn-1)^2(hn-2)^2+4(h^2n+3hn)}]^2}{4}$, *where $h = (q-1)/d$.*

The size of Szőnyi's examples is approximately $\sqrt{2}q^{3/4}$ and ours is $(2n/\sqrt{17})q^{3/4}$. For q large enough, we also mention the existence of complete arcs (hence of dense sets) of size at most $5q^{3/4}$ contained in a non-singular cubic; however this construction is not explicit (see [9, Thm. 3.7]).

Although the size of our examples is slightly larger than Bartocci and Szőnyi's, we provide with explicit construction of dense sets which are subsets of $\mathbf{F}_q$-rational points of a single irreducible algebraic curve, namely $\mathcal{C}_n$.

The method of the proof of Theorem 1.1 (see Proposition 2.1) follows Segre's and the Lombardo-Radice method as described in [10, p. 208].

2. The set $\mathcal{K}_{d,n}$ and certain plane curves

In this section we show that the density of $\mathcal{K}'_{d,n}$ in $\mathbf{P}^2(\mathbf{F}_q)$ is naturally related to the existence of certain $\mathbf{F}_q$-rational points in the projective plane curves C_P defined below as well as to arithmetical conditions between d and n. To begin with, we notice that

$$\mathcal{K}_{d,n} = \{(t^{hn} : t^h : 1) \mid t \in \mathbf{F}_q^*\},$$

with $h = (q-1)/d$. In fact, for $a \in \mathbf{F}_q$ we have that $a = \eta^i \Leftrightarrow a^d = 1 \Leftrightarrow a = t^h$ for some $t \in \mathbf{F}_q^*$.

If $(X : Y : Z)$ are homogeneous coordinates of $\mathbf{P}^2(\mathbf{F})$, where $\mathbf{F}$ is the algebraic closure of $\mathbf{F}_q$, we set $x := X/Z$ and $y := Y/Z$. We let p be the characteristic of $\mathbf{F}_q$.

For $P \in \mathbf{P}^2(\mathbf{F}_q)$ different from the fundamental points $(1:0:0)$, $(0:1:0)$, and $(0:0:1)$, let C_P be the projective plane curve defined by the affine equation $f_P(x,y) = 0$, where

$$f_P(x,y) := \begin{cases} u - v\frac{x^{hn}-y^{hn}}{x^h-y^h} + x^h y^h \frac{x^{h(n-1)}-y^{h(n-1)}}{x^h-y^h}, & \text{if } P = (u:v:1), \\ 1 - v\frac{x^{hn}-y^{hn}}{x^h-y^h}, & \text{if } P = (1:v:0). \end{cases}$$

The motivation to consider these curves comes from the next result.

Proposition 2.1. *For a non-fundamental point $P = (u : v : w)$, there exists a line through P meeting the set $\mathcal{K}_{d,n}$ in at least two distinct points if and only if the curve C_P has an $\mathbf{F}_q$-rational point $(x_0 : y_0 : 1)$ such that $x_0 \neq 0$, $y_0 \neq 0$, and $x_0^h \neq y_0^h$.*

Proof. For $x_0, y_0 \in \mathbf{F}_q^*$ such that $x_0^h \neq y_0^h$, we have that

$$\det \begin{pmatrix} x_0^{hn} & x_0^h & 1 \\ y_0^{hn} & y_0^h & 1 \\ u & v & w \end{pmatrix} = 0 \qquad \text{if and only if} \qquad f_P(x_0, y_0) = 0,$$

and the result follows. □

On the other hand, for the remaining fundamental points in $\mathbf{P}^2(\mathbf{F}_q) \setminus \mathcal{K}'_{d,n}$, the following holds.

Proposition 2.2. (1) *There exists a line through the point $(0:1:0)$ meeting $\mathcal{K}_{d,n}$ in two different points if and only if $\gcd(d,n) > 1$;*

(2) *there exists a line through the point $(0:0:1)$ meeting $\mathcal{K}_{d,n}$ in two different points if and only if $\gcd(d, n-1) > 1$.*

Proof. (1) We look for two different integers i and j between 1 and d such that the points $(0:1:0)$, $(\eta^{in}:\eta^{i}:1)$, and $(\eta^{jn}:\eta^{j}:1)$ are collinear; equivalently, we must have that $\eta^{in}=\eta^{jn}$; i.e., d must divide $(i-j)n$ and the result follows.

(2) Similar to (1). □

Now, since we will use the lower bound of the generalized Hasse-Weil theorem for plane curves in order to analize the existence of $\mathbf{F}_q$-rational points as required by Proposition 2.1, the next step is to investigate the absolute irreducibility of the curves $\mathcal{C}_P$. We use the following criterion due to Bartocci and Segre:

Lemma 2.3. ([2, Lemma 8]) *Let $\mathcal{C}$ be a projective plane curve of degree k defined over an arbitrary field $\mathbf{K}$. Then the curve is absolutely irreducible; i.e. it is irreducible over the algebraic closure of $\mathbf{K}$, provided that there exists a point $P\in\mathcal{C}$ and a tangent line ℓ of $\mathcal{C}$ at P such that the following three conditions hold:*

(1) *ℓ has multiplicity one;*
(2) *the intersection multiplicity of $\mathcal{C}$ and ℓ at P is k;*
(3) *the tangent lines of $\mathcal{C}$ at P are not components of $\mathcal{C}$.*

Lemma 2.4. *If $P=(u:v:1)$, with $u\neq v^n$ and $v\neq 0$, then the curve $\mathcal{C}_P$ is absolutely irreducible.*

Proof. The homogenization of $f_P(x,y)$ is given by

(2.1)

$$F_P(X,Y,Z)=uZ^{hn}-v\sum_{i=1}^{n}(X^h)^{n-i}(Y^h)^{i-1}Z^h+\sum_{i=1}^{n-1}(X^h)^{n-i}(Y^h)^i\,.$$

Then the point $(0:1:0)$ is an h-fold singular point for $\mathcal{C}_P$, and the tangent lines at this point have equations $X=\alpha Z$ with $\alpha^h=v$. These tangents are distinct since p does not divide h; in addition, by Bézout's theorem, the intersection multiplicity of any tangent of $\mathcal{C}_P$ at $(0:1:0)$ is equal to nh (the degree of $\mathcal{C}_P$) since the set-intersection of each tangent with (2.1) give rises to $(u-v^n)Z^{hn}=0$; i.e., it is just the point $(0:1:0)$ itself. These properties imply the result via Lemma 2.3. □

Lemma 2.5. *If $P=(u:0:1)$, with $u\neq 0$, then the curve $\mathcal{C}_P$ is absolutely irreducible provided that the following conditions hold:*

(1) *$n\geq 3$;*
(2) *p does not divide $n-1$.*

Proof. The hypothesis on p implies the existence in $\mathbf{F}$ of a $h(n-1)$-th root of unity, say a; we notice that $a^h \neq 1$ as $n \geq 3$. Set $F = F_P$. Now from (2.1), $F(X,Y,0) = X^hY^h(X^{h(n-1)} - Y^{h(n-1)})/(X^h - Y^h)$ so that $Q := (1 : a : 0) \in \mathcal{C}_P$. We claim that Q is in fact a non-singular point of the curve. Indeed, here we have $F_Z(Q) = 0$, as $hn \geq 2$, $F_X(Q) = -aF_Y(Q)$, and $F_X(Q) = h(n-1)a^h/(1-a^h)$ which is different from zero by hypothesis. In particular, $Y = aX$ is the tangent line at P whose intersection with (2.1) implies $uZ^{hn} = 0$, i.e., it is just the point Q itself. Therefore the results follows from Lemma 2.3. □

Now let $P = (v^n : v : 1)$, with $v \neq 0$. From (2.1) it follows that each line defined by either $X = \alpha Z$ or $Y = \alpha Z$, where $\alpha^h = v$, is a component of $\mathcal{C}_P$. More precisely, $F_P(X,Y,Z) = (X^h - vZ^h)(Y^h - vZ^h)G_P(X,Y,Z)$, where

$$G_P(X,Y,Z) := \sum_{i=1}^{n-1}\sum_{j=1}^{i}(X^h)^{n-1-i}(Y^h)^{i-j}(vZ^h)^{j-1}\,.$$

We let $\mathcal{C}'_P$ be the projective plane curve defined by $G_P(X,Y,Z) = 0$. Here, although we do not have a criterion to decide whether or not this curve is absolutely irreducible, based on the following remark we can give a numerical sufficient condition under which $\mathcal{C}'_P$ will have at least an absolutely irreducible component defined over $\mathbf{F}_q$.

Remark 2.6. Let $\mathcal{C}$ be a plane curve over $\mathbf{F}_q$ and P a non-singular $\mathbf{F}_q$-rational point of $\mathcal{C}$. Then any absolutely irreducible component of $\mathcal{C}$ passing through P is also defined over $\mathbf{F}_q$. Indeed, this follows as P belongs to the component and its image under the corresponding Frobenius morphism.

Lemma 2.7. *If $P = (v^n : v : 1)$, with $v \neq 0$, then the curve $\mathcal{C}'_P$ has an absolutely irreducible component defined over $\mathbf{F}_q$ provided that:*

(1) $n \geq 3$;
(2) $h(n-1)$ *divides* $q-1$.

Proof. As in the proof of Lemma 2.5, there exists $a \in \mathbf{F}$ such that $a^{h(n-1)} = 1$ but $a^h \neq 1$. In addition such $a \in \mathbf{F}_q$ by hypothesis (2). Set $F = F_P$ and $G = G_P$. Since $G(X,Y,0) = (X^{h(n-1)} - Y^{h(n-1)})/(X^h - Y^h)$ and $n \geq 3$, the point $Q := (1 : a : 0) \in \mathcal{C}'_P$. The proof then follows from the previous remark once we show that Q is non-singular. To see this we use $F = (X^h - vZ^h)(Y^h - vZ^h)G$ to conclude that $F_X(Q) = a^hG_X(Q)$. From (2.1) we easily see that $F_X(Q) = h(n-1)a^h/(1-a^h)$ and the result follows as p does not divide $n-1$. □

Remark 2.8. Condition (2) in the previous lemma is not necessary in general for the existence of absolutely irreducible components of $\mathcal{C}'_P$ defined

over $\mathbf{F}_q$. As for an example, let $p \neq 3$, $n = 4$, q a power p such that $h = 2$ (so that $p \neq 2$). For $P = (v^4 : v : 1)$, $v \in \mathbf{F}_q^*$, we are going to show that the curve $\mathcal{C} := \mathcal{C}'_P$ given by

$$G(X, Y, Z) = G_P(X, Y, Z) = X^4 + X^2Y^2 + Y^4 + (X^2 + Y^2)vZ + v^2Z^2 = 0$$

is absolutely irreducible or splits into two absolutely irreducible conics defined both over $\mathbf{F}_q$. To begin with, we notice that in the line $Z = 0$ the curve has four non-singular points, namely $Q_1 := (1 : w : 0)$, $Q_2 := (1 : w^2 : 1)$, $Q_3 := (1 : -w : 1)$, and $Q_4 := (1 : -w^2 : 0)$ where w is a 3-th primitive root of unity. We also notice that the linear maps $T(X : Y : Z) = (Y : X : Z)$ and $S(X : Y : Z) = (X : -Y : Z)$ induce involutions on the curve.

Claim. The curve $\mathcal{C}$ has no linear components.

As a way of contradiction, suppose that L_1 is a linear component of $\mathcal{C}$. Thus $\mathcal{C}$ splits into four different lines: L_1, $L_2 := T(L_1)$, $L_3 := S(L_1)$, and $L_4 := S(L_2)$, as the following properties hold: (i) T and S permutate the points Q_i's, (ii) two different points Q_i and Q_j cannot belong both to the same line L_k (otherwise Z would divide $G(X, Y, Z)$), and (iii) for each i $T(Q_i) \neq S(Q_i)$. Reorder the lines in such a way that $Q_i \in L_i$, and let $AX + BY + CZ = 0$ be the equation of L_1. Then L_2, L_3, and L_4 are defined respectively by $BX + AY + cZ = 0$, $AX - BY + cZ = 0$, and $BX - AY + CZ = 0$. In addition, $L_4 = T(L_3)$; i.e., L_4 is also defined by $-BX + AY + CZ = 0$ and from the last two equations we get $C = 0$ meaning that $G(X, Y, Z)$ is independent of Z, a contradiction.

Therefore if the curve is not absolutely irreducible, it splits into two irreducible conics (over $\mathbf{F}$), say $\mathcal{C}_1$ and $\mathcal{C}_2$, such that $Q_1 \in \mathcal{C}_1$. We will show now that $\mathcal{C}_1$ is defined over $\mathbf{F}_q$ (a posteriori $\mathcal{C}_2$ will do too); otherwise, $\mathcal{C}_2 = \Phi(\mathcal{C}_1)$. Now, as $Q_2 = \Phi(Q_1)$, then $Q_2 \notin \mathcal{C}_1$ since Q_2 is a non-singular point; therefore one and only one of the following two possibilities can occur (i) $Q_3 \in \mathcal{C}_1$ or (ii) $Q_4 \in \mathcal{C}_1$. In case (i) $G(X, Y, 0)$ has $(1, w)$ and $(1, -w)$ as zeroes so that $\mathcal{C}_1$ is defined by an equation of type $(Y - wX)(Y + wX) + rZ + DZ^2 = 0$ where r is linear form in X and Y and $D \in \mathbf{F}^*$. Then $\mathcal{C}_2$ is defined by $(Y - w^2X)(Y + w^2X) + \Phi(r)Z + D^qZ = 0$. We get a contradiction by comparing $G(X, Y, Z)$ with the product of the two above quadrics. Case (ii) is handled in the same way.

Finally, for points on $Z = 0$ we have:

Lemma 2.9. *If $P = (1 : v : 0)$, with $v \neq 0$, then the curve $\mathcal{C}_P$ is absolutely irreducible provided that:*

(1) *$h(n - 1) \geq 2$ and $n \geq 2$;*
(2) *p does not divide n.*

Proof. The proof is similar to that of Lemma 2.5. Here the homogenization of f_P is given by

$$F(X,Y,Z) = F_P(X,Y,Z) = Z^{h(n-1)} - v(X^{hn} - Y^{hn})/(X^h - Y^h)\,.$$

There exists $a \in \mathbf{F}$ such that $a^{hn} = 1$ but $a^h \neq 1$ (as $n \geq 2$) so that $Q := (1 : a : 0) \in \mathcal{C}_P$. Now $F_Z(Q) = 0$ as $h(n-1) \geq 2$, $F_Y(Q) = aF_X(Q)$, and $F_X(Q) = -hnv/(1-a^h)$. Thus Q is non-singular and the tangent line at Q is $Y = aX$. Moreover, this line intersects the curve just in Q. Now the result follows from Lemma 2.3. □

3. Proof of Theorem 1.1

We are going to apply Propositions 2.1 and 2.2; the hypotheses (4), (3), and (1) reduce the proof to that of

$$(*) \qquad \#\mathcal{C}_P(\mathbf{F}_q) > \#(\mathcal{C}_P(\mathbf{F}_q) \cap (XYZ = 0 \text{ or } X^h = Y^h)\,,$$

for any $P \in \mathbf{P}^2(\mathbf{F}_q)$, P different from a fundamental point. Now the hypotheses (1), (2) and (3) (the latter being equivalent to $h(n-1)$ divides $q-1$) implies the existence of an absolutely irreducible component of $\mathcal{C}_P$ defined over $\mathbf{F}_q$ by Lemmas 2.4, 2.5, 2.7, and 2.9. Hence we can use the the generalized Hasse-Weil lower bound for the number of $\mathbf{F}_q$-rational points of (possible singular) plane curves (see [6]) which for an absolutely irreducible projective plane algebraic curve $\mathcal{C}$ of degree k defined over $\mathbf{F}_q$ says that

$$\#\mathcal{C}(\mathbf{F}_q) \geq q + 1 - \sqrt{q}(k-1)(k-2)\,.$$

Since the absolutely irreducible curves arising from $\mathcal{C}_P$ have degree at most hn, by using the inequality above and Bézout's theorem we have that $(*)$ is fulfilled once

$$(3.1) \qquad q + 1 - \sqrt{q}(hn-1)(hn-2) > h^2n + 3hn\,.$$

This condition is equivalent to hypothesis (5) and Theorem 1.1 follows.

Remark 3.1. If in the hypothesis of Theorem 1.1 either (2) or (4) do not hold, then $\mathcal{K}'' := \mathcal{K}'_{d,n} \cup \{(0:1:0)\}$ is a dense set in $\mathbf{P}^2(\mathbf{F}_q)$ of size $d+2$. Indeed, we do not need to use either Proposition 2.2(1) or Lemma 2.9, as the line $Z = 0$ pass through two different points of $\mathcal{K}''$.

Remark 3.2. If we slightly change condition (3.1) to

$$q + 1 - \sqrt{q}(hn-1)(hn-2) > h^2n + 3hn + 1\,,$$

then $\mathcal{K}'_{d,n}$ is not a minimal dense set. Indeed, suppose that it is minimal and let $P \in \mathcal{K}_{d,n}$. Then there exists $Q \in \mathbf{P}^2(\mathbf{F}_q)$ such that any line through Q intersects $\mathcal{K}'_{d,n} \setminus \{P\}$ at most once. Thus the proof of Theorem 1.1, the above inequality and Proposition 2.1 imply $Q \in \{(0:1:0), (0:0:1)\}$. This is not possible by Proposition 2.2.

REFERENCES

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

[2] U. Bartocci and B. Segre, *Ovali ed altre curve nei piani di Galois di caratteristica due*, Acta Arith. **18** (1971), 423–449.

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

[4] G. Korchmáros, *New examples of complete k-arcs in $PG(2,q)$*, European J. Combin. **4** (1983), 329–334.

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

[6] D.B. Leep and C.C. Yeomans, *The number of points on a singular curve over a finite field*, Arch. Math. **63** (1994), 420–426.

[7] 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.

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

[9] T. Szőnyi, "Complete arcs in Galois planes: a survey", Quaderni del seminario di Geometrie Combinatorie **94**, Dip. Mat. G. Castelnuovo, Univ. di Roma La Sapienza, 1989.

[10] T. Szőnyi, "Some applications of algebraic curves in finite geometry and combinatorics", Surveys in combinatorics, 1997, London Math. Soc. Lecture Note Series **241**, 197–236, Cambridge University Press, Cambridge, 1997.

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

DIPARTIMENTO DI MATEMATICA E INFORMATICA, UNIVERSITÀ DEGLI STUDI DI PERUGIA, 06123 PERUGIA, ITALY

E-mail address: giuliet@dipmat.unipg.it

IMECC-UNICAMP, CX. P. 6065, CAMPINAS, 13083-970-SP, BRAZIL

E-mail address: ftorres@ime.unicamp.br

CURRENT ADDRESS: DEPARTAMENTO DE ALGEBRA, GEOMETRÍA Y TOPOLOGÍA, FACULTAD DE CIENCIAS - UNIVERSIDAD DE VALLADOLID, C/ PRADO DE LA MAGDALENA S/N 47005, VALLADOLID (SPAIN)

E-mail address: ftorres@agt.uva.es