International Journal of Pure and Applied Mathematics

Volume 36 No. 2 2007, 285-291

SUBSPACES OF A FINITE PROJECTIVE SPACE CONTAINING MANY POINTS OF A GIVEN SET

E. Ballico

Department of Mathematics
University of Trento
380 50 Povo (Trento) - Via Sommarive, 14, ITALY
e-mail: ballico@science.unitn.it

Abstract: Fix $S \subseteq \mathbf{P}^n(\mathbb{F}_q)$. For each integer $1 \leq t < n$ let $\sigma(S,t)$ denote the maximal number of points of S contained in a t-dimensional linear subspace. Here we compute these integers (for certain t) when S arises from Veronese varieties or embeddings of a hyperbolic or an elliptic quadric surface.

AMS Subject Classification: 14N05, 05C38
Key Words: elliptic quadric surface, Veronese variety, finite projective space, hyperbolic quadric surface

*

Fix a prime power q, an integer $n > 0$ and a set $S \subseteq \mathbf{P}^n(\mathbb{F}_q)$. For all integers $b > a \geq 0$ let $G(a,b)$ denote the Grassmannian of all a-dimensional linear subspaces of $\mathbf{P}^n(\bar{\mathbb{F}}_q)$. Hence $G(a,b)(\mathbb{F}_q)$ is the Grassmannian of all a-dimensional linear subspaces of $\mathbf{P}^n(\mathbb{F}_q)$. Set $\Sigma(S,0) := \Sigma(S,0)' := S$. For all integers $t > 0$ set $\Sigma(S,t)' := \{M \in G(t,n)(\mathbb{F}_q) : \sharp(S \cap M) \geq t+2\}$. Set $\Sigma(S,1) := \Sigma(S,1)'$. For all integers $t \geq 2$ set $\Sigma(S,t) := \{M \in \Sigma(S,t)' : \text{there is } P \in M \cap S \text{ not contained in any } W \in \Sigma(S,a)' \text{ for all } 1 \leq a \leq t-1\}$. We will say that $P, Q \in S$ are t-connected (resp. weakly t-connected) if either $P = Q$ or there is $D \in \Sigma(S,t)$ (resp. $D \in \Sigma(S,t)'$) such that $\{P,Q\} \subset D$. Notice that P, Q are 1-connected if and only if they are weakly 1-connected. Now fix an integer $t > 0$ and $A \subset S$ such that $\dim(\langle A \rangle) \leq t$. Let $E(A,S,t)$ be the set of all $M \in G(t,n)(\mathbb{F}_q)$ such that $A \subseteq M$ and $\sharp(S \cap M)$ is maximal. Set $\sigma(A,S,T) := \sharp(S \cap M)$ for

Received: February 11, 2007

any $M \in E(A,S,t)$. Let $E(S,t)$ be the set of all $M \in G(t,n)(\mathbb{F}_q)$ such that $\sharp(S \cap M)$ is maximal. Set $\sigma(S,t) := \sharp(S \cap M)$ for any $M \in E(S,t)$. Notice that $\sigma(S,t) = (q^{t+1}-1)/(q-1)$ if and only if S contains some $M \in G(t,n)(\mathbb{F}_q)$.

Here we will study the function $\sigma(S,t)$ when S is one of the following examples, respectively the Veronese varieties and the elliptic quadric surface, while we will study a weaker property for the hyperbolic quadric surface (see Proposition 3).

Example 1. Fix a prime power q and positive integers m, x. Set $n := \binom{m+d}{m} - 1$. Let $X \subset \mathbf{P}^N$ be the order x Veronese embedding of $\mathbf{P}^m$. Hence $X \cong \mathbf{P}^m$ and $\mathcal{O}_X(1) \cong \mathcal{O}_{\mathbf{P}^m}(x)$. X is defined over $\mathbb{F}_q$ and $\sharp(X(\mathbb{F}_q)) = (q^m-1)/(q-1)$. Set $S := X(\mathbb{F}_q)$. Notice that any $x+1$ points of S are in linearly general position. Hence we may take as t any integer such that $1 \le t \le x$. If $2t+1 \le x$, then $V = \emptyset$, while if $t < x$, then $V' = \emptyset$.

Example 2. Fix positive integers m, r, x, y. Set $X := \mathbf{P}^m \times \mathbf{P}^r$, $n := \binom{m+x}{m} \cdot \binom{r+y}{r} - 1$ and $R := \mathcal{O}_X(x,y) \in \mathrm{Pic}(X)$. R is very ample and induces an embedding $\phi : X \to \mathbf{P}^n$ defined over $\mathbb{F}_q$. Set $S := \phi(X)(\mathbb{F}_q) \subseteq \mathbf{P}^n(\mathbb{F}_q)$. Hence $\sharp(S) = (q^{m+1}-1)(q^{r+1}-1)/(q-1)^2$. Since the Segre variety X is cut out by quadrics, any line of $\mathbf{P}^n$ intersecting X in at least 3 points is contained in X. If $x \ge 2$ and $y \ge 2$, then there is no such line and hence $\Sigma(S,1) = \emptyset$. If $x \ge 2$ and $y = 1$, then $P, Q \in S$ are 1-connected if and only if there is $O \in \mathbf{P}^m(\mathbb{F}_q)$ such that $\{P,Q\} \subset \phi(\{O\} \times \mathbf{P}^m)$. A similar result hold if $x = 1$ and $y \ge 2$. If $x = y = 1$, then $P, Q \in S$ are 1-connected if and only if either there is $O \in \mathbf{P}^m(\mathbb{F}_q)$ such that $\{P,Q\} \subset \phi(\{O\} \times \mathbf{P}^r)$ or there is $O' \in \mathbf{P}^r(\mathbb{F}_q)$ such that $\{P,Q\} \subset \phi(\mathbf{P}^m \times \{O\})$. To study this example it is sufficient to do the case $x \ge y$. We will often silently use that for all $P, Q \in S$ there are lines $D \subseteq \mathbf{P}^m$, $L \subseteq \mathbf{P}^r$ such that $\{P,Q\} \subset \phi(D \times L)(\mathbb{F}_q)$. Set $n_1 := \binom{m+x}{m} - 1$ and $n_2 := \binom{r+y}{r} - 1$. Let S_1 (resp. S_2) denote the set S given by Example 1 with respect to the data $(m', x') := (m, x)$ (resp. $(m', x') := (r, y)$). Let $\pi_1 : \mathbf{P}^m \times \mathbf{P}^r \to \mathbf{P}^m$ and $\pi_2 : \mathbf{P}^m \times \mathbf{P}^r \to \mathbf{P}^r$ denote the projections. π_i induces a surjection $\rho_i : S \to S_i$. Notice that $S \cong S_1 \times S_2$ (Segre embedding).

Now we state our main results.

Theorem 1. *Take the set-up of Example 1.*
(a) $\sigma(S,t) = t+1$ *for* $1 \le t \le x-1$.
(b) If $q \ge x+1$, *then* $\sigma(S,x) = q+2$.
(c) If $q \le x$, *then* $\sigma(S,x) = x$.
(d) Assume $m = 2$, $x+1 \le t \le (x^2+3x)/2$ *and* $q > (x-2)^2$. *Write* $t = (2x+2-c)c/2 + a - 1$ *for uniquely determined integers* c, a *such that* $0 \le c \le x-1$ *and* $0 \le a \le x-c$. *Then* $\sigma(S,t) = (x-c)q + a + 1$.

(e) Assume $m \geq 2$ and $q \geq x+1$. Fix an integer t such that $x+1 \leq t \leq \binom{x+2}{2} - 1$ and write $t = (2x+2-c)c/2 + a - 1$ for uniquely determined integers c, a such that $0 \leq c \leq x-1$ and $0 \leq a \leq x-c$. Then $\sigma(S,t) \geq (x-c)q + a + 1$.

Theorem 2. *Fix an integer $x \geq 2$ prime power q such that $q > 2x^2$. Let $\mathbb{E}$ be the elliptic quadric surface over $\mathbb{F}_q$ and let $S \subset \mathbf{P}^n(\mathbb{F}_q)$, $n := x^2 + 2x$, be the embedding of $\mathbb{E}(\mathbb{F}_q)$ by the complete linear system $|\mathcal{O}_{\mathbb{E}}(x,x)|$. Fix integers a, e such that $1 \leq a < x$ and $0 \leq e \leq x-a$. Then $\sigma(S, a(y+1)+e-1) = aq+2-a+e$.*

Remark 1. Assume $P, Q \in S$ and the existence of $M \in \Sigma(S,t)'$ such that $P, Q \subset M$ and $S \neq S \cap M$. Fix any $O \in S \backslash S \cap M$. Notice that $\langle M \cup \{O\} \rangle \in \Sigma(S, t+1)'$. Hence P, Q are weakly $(t+1)$-connected.

Remark 2. Take the set-up of Example 1 with $x = 1$. Hence $n = m$, $\Sigma(S,t)' = G(t,n)(\mathbb{F}_q)$ for all $1 \leq t \leq n$ and all $P, Q \in S$ are weakly t-connected for all $1 \leq t \leq n$. If $m \geq 2$, then S is 2-connected. S is not t-connected for any $t \geq 3$.

Remark 3. Take the set-up of Example 1 and assume $x \geq 2$ and $q \geq x+1$. Fix $P, Q \in S$ such that $P \neq Q$. Let D be the line spanned by $\{P, Q\}$. Any $x+1$ points of S are linearly independent. Take any $A \subset S$ such that $\sharp(A) = x+2$. A is not linearly independent if and only if it corresponds to collinear points of $\mathbf{P}^m$. Since $\sharp(D(\mathbb{F}_q) = q+1 \geq x+2$, we get that P, Q are not weakly t-connected if $t \leq x-1$, they are x-linked and they are weakly t-connected for all $t \geq x+1$ (use Remark 1).

Remark 4. Take the set-up of Example 2. Assume $x = y = 1$. All $P, Q \in S$ are 2-connected. Hence all P, Q are weakly t-connected for all $t \in \{2, \dots, n\}$.

Proposition 1. *Take the set-up of Example 2. Assume $x \geq y \geq 1$ and $q \geq x+1$. Fix $P, Q \in S$ such that $P \neq Q$.*

(i) Assume $\rho_1(P) = \rho_1(Q)$. P, Q are not weakly t-connected for all $t < y$. They are t-connected for all $t \geq y$.

(ii) Assume $\rho_2(P) = \rho_2(Q)$. P, Q are not weakly t-connected for all $t < x$. They are t-connected for all $t \geq x$.

(iii) Assume $\rho_1(P) \neq \rho_1(Q)$ and $\rho_2(P) \neq \rho_2(Q)$. Then they are t-connected.

Proof. Notice that for any $A \in S$, $\dim(\langle A \rangle) \geq \dim(\langle \rho_i(A) \rangle)$, $i = 1, 2$. First assume $\rho_1(P) = \rho_1(Q)$. Since $P \neq Q$, we have $\rho_2(P) \neq \rho_2(Q)$. Apply Remark 3 with respect to the data $m' := r$ and $x' := y$ and Remark 1. We get that P, Q are not weakly t-linked for all $t < y$, they are y-linked and weakly t-linked for all $t > y$. Now fix an integer t such that $y+1 < t \leq n-1$. Fix the line $L \subseteq \mathbf{P}^r$ spanned by $\rho - 2(P)$ and $\rho_2(Q)$. Take $B \subset D(\mathbb{F}_q)$ such that $\sharp(B) = y$, $P \notin B$

and $Q \notin B$. Set $B' := B \cup \{P, Q\}$. Since S spans $\mathbf{P}^n$, there is $A \subset S \backslash D(\mathbb{F}_q)$ such that $\sharp(A) = t - 1 - y$ and $\dim(\langle A \cup B' \rangle) = t - 1$. Set $M := \langle A \cup B'$. The linear space M shows that P, Q are t-conected. Similarly, if $\rho_2(P) = \rho_2(Q)$, we get part (ii); here if $x > y$ we also use that $\dim(\langle A \rangle) \geq \dim(\langle \rho_1(A) \rangle)$ for all $A \subset S$. Now assume $\rho_1(P) \neq \rho_1(Q)$ and $\rho_2(P) \neq \rho_2(Q)$. Let $D \subset \mathbf{P}^m$ (resp. $D \subset \mathbf{P}^r$) be the line spanned by $\rho_1(P)$ and $\rho_1(Q)$ (resp. $\rho_2(P)$ and $\rho_2(Q)$). Using $D \times L$ we reduce the proof of part (iii) to the case $m = r = 1$. □

Remark 5. Let D be a geometrically integral projective curve defined over $\mathbb{F}_q$ and C its normalization. C is defined over $\mathbb{F}_q$ and $\sharp(C(\mathbb{F}_q)) \leq 2\lfloor p_a(C) \cdot \sqrt{q} \rfloor$. Since $\sharp(D(\mathbb{F}_q)) \leq \sharp(C(\mathbb{F}_q)) + \sharp(\mathrm{Sing}(D))$ and $p_a(D) \geq p_a(C) + \sharp(\mathrm{Sing}(D))$, we get $\sharp(D(\mathbb{F}_q)) \leq 2\lfloor p_a(D) \cdot \sqrt{q} \rfloor$.

Remark 6. Let $A \subset \mathbf{P}^2$ be an effective divisor defined over $\mathbb{F}_q$. Since every finite field is perfect, the effective divisor A_{red} is defined over $\mathbb{F}_q$. Notice that $\deg(A_{red}) \leq \deg(A)$ and $\deg(A_{red}) = \deg(A)$ if and only if $A = A_{red}$. Notice that $\sharp(A(\mathbb{F}_q)) = \sharp(A_{red}(\mathbb{F}_q))$.

Remark 7. Let $A \subset \mathbf{P}^2$ be an effective and reduced degree d divisor defined over $\mathbb{F}_q$. Assume that A is irreducible over $\mathbb{F}_q$, but that it is reducible over $\overline{\mathbb{F}}_q$. There is a minimal integer $e \geq 2$ such that each geometrically irreducible component of A is defined over $\mathbb{F}_{q^e}$. There are exactly e geometrically irreducible components of A, say $A_1, \dots, A_e$, which are permuted by the Galois group of the cyclic extension $[\mathbb{F}_{q^e} : \mathbb{F}_q]$. $A(\mathbb{F}_q) = A_1 \cap \dots \cap A_e$. Hence $d/e \in \mathbb{N}$. By Bézout's Theorem we get $\sharp(A(\mathbb{F}_q)) \leq (d/e)^2$ with strict inequality if $e > 2$. Thus $\sharp(A(\mathbb{F}_q)) \leq d^2/4$ and $\sharp(A(\mathbb{F}_q)) \leq d^2/9 - 1$ if $e \geq 3$.

Remark 8. Let $C \subset \mathbf{P}^1 \times \mathbf{P}^1$ an effective divisor of type (a, b). Then $p_a(C) = ab - a - b + 1$ (adjunction formula).

Proposition 2. *Fix an integer $z \geq 1$ and assume $q > (z-2)^2$. Let C a degree d plane curve defined over $\mathbb{F}_q$ and such that $\sharp(C(\mathbb{F}_q)) \geq 1 + zq$. Then $\sharp(C(\mathbb{F}_q)) = 1 + zq$ and there exists $P \in \mathbf{P}^2(\mathbb{F}_q)$ such that C is the union of z lines, each of them containing P and defined over $\mathbb{F}_q$.*

Proof. By Remark 6 we may assume $C = C_{red}$. Since the cases $z = 1$ and $z = 2$ are trivially true, we may assume $z \geq 3$ and that the result is true for all positive integers $z' \leq z-1$. First assume that C is geometrically integral. Since $p_a(C) = (z-1)(z-2)/2$, Remark 5 gives $\sharp(C(\mathbb{F}_q)) \leq q+1+(z-1)(z-2) \cdot \sqrt{q}$. Hence $(z-1)q \geq (z-1)(z-2) \cdot \sqrt{q}$, contradiction. Now assume that C is geometrically reducible. If C is irreducible over $\mathbb{F}_q$, then $\sharp(C(\mathbb{F}_q)) \leq z/4 < zq$ (Remark 7). Hence we may assume that C is reducible over $\mathbb{F}_q$. Call C_1 one of

its irreducible components over $\mathbb{F}_q$ and C_2 the union of the other ones. We do not require that C_1 is geometrically irreducible. Set $z_i := \deg(C_i)$. Notice that $\sharp(C(\mathbb{F}_q)) \le \sharp(C_1(\mathbb{F}_q)) + \sharp(C_2(\mathbb{F}_q))$ with strict inequality if $C_1(\mathbb{F}_q) \cap C_2(\mathbb{F}_q) \neq \emptyset$. By the inductive assumption we get $\sharp(C_i(\mathbb{F}_q)) \le 1 + z_i q$ with strict inequality unless C_i is a union of z_i lines through some $P_i \in \mathbf{P}^2(\mathbb{F}_q)$ and each line is defined over $\mathbb{F}_q$. The inequality $q > (z-2)^2$ shows that at least one of these inequalities cannot be strict. Hence either C_1 is a line defined over $\mathbb{F}_q$ or C_2 is a union of lines defined over $\mathbb{F}_q$ and through the same point. Call C_i this union of lines and set $\{j\} := \{1,1\}\backslash\{i\}$. First assume $i = 2$. We also have $\sharp(C_j(\mathbb{F}_q)) \ge z_1 q$. By Remark 6 and the inequality $q \ge z_1$, C_1 cannot be geometrically reducible. Hence $\sharp(C(\mathbb{F}_q)) \le 1 + (z-z_1)q + (z_1-1)(z_1-2)\sqrt{q}$ (Remark 5). Since $(z_1-1)(z_1-2)\sqrt{q} \le (z-1)(z-2)\sqrt{q} - 1$, we get a contradiction. Now assume $i = 1$. If C_2 is reducible over $\mathbb{F}_q$, and call D_1 this component and D_2 the union of all others components of C. The previous part gives a contradiction (or that D_2 is a line). Similarly, Remark 6 implies every irreducible component of C_2 is defined over $\mathbb{F}_q$. In summary, C is the union of m lines defined over $\mathbb{F}_q$ for some $1 \le m \le z-1$ of a geometrically irreducible component D. Remark 5 gives $\sharp(C(\mathbb{F}_q)) \le q+1+(z-m-1)(z-m-2)\sqrt{q}$. The contradiction comes from the inequality $(z-m-1)(z-m-2)\sqrt{q} < -1 + (z-1)(z-2)\sqrt{q}$ and our assumption on q. □

Proof of Theorem 1. For parts (a), (b) and (c), see Remark 3.

(i) Here we will check part (d). Fix $P \in \mathbf{P}^2(\mathbb{F}_q)$. Let T be the union of z lines, each of them containing P and defined over $\mathbb{F}_q$. Let E the union of $S \cap T$ and (if $a > 0$) a further points of S. The set E proves the inequality $\sigma(S,t) \ge (z-c)q + a + 1$. Now we will check the opposite inequality. We fix $M \in E(S,t)$ and write $J := S \cap M$. Let B be the base locus of the linear system $|\mathcal{I}_J(x,y)|$. Hence $J \subseteq B$. Since J is defined over $\mathbb{F}_q$, B is defined over $\mathbb{F}_q$. Since $M \in E(S,t)$ we have $B \cap S = J$. Let D' be the divisorial part of B. Set $D := (D')_{red}$ and $J' := J\backslash D \cap S$. D' and hence D are defined over $\mathbb{F}_q$ (Remark 6). Since $(x-c)q + a + 1 > x^2$, $D \neq \emptyset$. Set $u := \deg(D)$. We have $u \le x-c$, because $(x+2)(x+1)/2 - t - 1 = h^0(\mathbf{P}^2, \mathcal{I}_J(x)) = h^0(\mathbf{P}^2, \mathcal{I}_{J'}(x-u))$. Proposition 2 implies $\sharp(J') = \sharp(J) - \sharp(D \cap S) \ge \sharp(J) - 1 - uq$. We need to check $\sharp(J') \le (x-c-u) + a$. First assume $u = x-c$. We have $\sharp(D \cap S) \le 1 + (x-c)q$ (Proposition 2). We use J' for the integers $x' := x-c$ and $t' := t - (x-c+2)(x-c+1)/2$. Since $t' \le x'+1$, we get $\sharp(J') \le t'+1$, proving part (d) when $u = x-c$. Now assume $u < x-c$. Hence $\sharp(J') \ge a+q > (x-u)^2$. By Bézout's Theorem the base-locus of the linear system $|\mathcal{I}_{J'}|$ is non-empty, contradicting the definition of D.

(ii) Part (e) is easy: fix a plane $M \subseteq \mathbf{P}^m$ defined over $\mathbb{F}_q$ and take $(x-c)$ lines of it through the same point. □

Remark 9. Let $A \subset \mathbf{P}^1 \times \mathbf{P}^1$ be an effective divisor defined over $\mathbb{F}_q$. Since every finite field is perfect, the effective divisor A_{red} is defined over $\mathbb{F}_q$. Let (a,b) (resp. (a',b')) denote the type of A (resp. A_{red}). Hence $a' \le a$, $b' \le b$ and both inequalities are strict if $A \neq A_{red}$. Notice that $\sharp(A(\mathbb{F}_q)) = \sharp(A_{red}(\mathbb{F}_q))$.

Remark 10. Fix positive integers a, b and a curve $A \subset \mathbf{P}^1 \times \mathbf{P}^1$ of type (a,b) defined over $\mathbb{F}_q$. Assume that A is irreducible over $\mathbb{F}_q$, but that it is reducible over $\bar{\mathbb{F}}_q$. There is a minimal integer $e \ge 2$ such that each geometrically irreducible component of A is defined over $\mathbb{F}_{q^e}$. There are exactly e geometrically irreducible components of A, say $A_1, \dots, A_e$, which are permuted by the Galois group of the cyclic extension $[\mathbb{F}_{q^e} : \mathbb{F}_q]$. $A(\mathbb{F}_q) = A_1 \cap \dots \cap A_e$. Notice that a/e and b/e are positive integers. We get $\sharp(A(\mathbb{F}_q)) \le 2a'b/e^2 \le ab/2$.

Proposition 3. *Fix non-negative integers a, b. Assume $q \ge (a+b)^2$. Let C be a positive divisor of type (a,b) on $\mathbf{P}^1 \times \mathbf{P}^1$ defined over $\mathbb{F}_q$ such that $\sharp(C(\mathbb{F}_q)) \ge (a+b)(q+1) - ab$. Then $\sharp(C(\mathbb{F}_q)) = (a+b)(q+1) - ab$ and C is the union of a curves of type $(1,0)$ and b curves of type $(0,1)$, all of them defined over $\mathbb{F}_q$.*

Proof. By Remark 9 we may assume that C is reduced. Since the case $ab = 0$ is trivial, we may assume $a > 0$ and $b > 0$. If $a = 1$, then every geometric ireducible component of C is smooth and rational. The same is true if $b = 1$. Hence Remark 10 gives that it is suffient to do the case $a \ge 2$ and $b \ge 2$ and use induction on the integer $a+b$. First assume C geometrically irreducible. Remarks 5 and 8 imply $\sharp(C(\mathbb{F}_q)) \le q+1+2(ab-a-b+1)\sqrt{q}$. We immediately get a contradiction, because $q \ge (a+b)^2$. Now assume that C is irreducible over $\mathbb{F}_q$, but geometrically reducible. Remark 10 gives $\sharp(C(\mathbb{F}_q)) \le ab/2$, contradiction. Hence we may assume that C is reducible over $\mathbb{F}_q$. Call C_1 one of its irreducible components over $\mathbb{F}_q$ and C_2 the union of the other components. We do not require that C_1 is geometrically irreducible. Let (a_i, b_i) denote the type of the curve C_i. Hence $a_i + b_i > 0$ for $i = 1, 2$, $a_1 + a_2 = a$ and $b_1 + b_2 = b$. Notice that $\sharp(C(\mathbb{F}_q)) \le \sharp(C_1(\mathbb{F}_q)) + \sharp(C_2(\mathbb{F}_q))$ with strict inequality if $C_1(\mathbb{F}_q) \cap C_2(\mathbb{F}_q) \neq \emptyset$. By the inductive assumption we get $\sharp(C_i(\mathbb{F}_q)) \le (a_i + b_i)(q+1)$ with strict inequality unless C_i is a union of a_i curves of type $(1,0)$ defined over $\mathbb{F}_q$, b_i curves of type $(0,1)$ defined over $\mathbb{F}_q$, and no two of these curves have a point of $\mathbf{P}^1 \times \mathbf{P}^1(\mathbb{F}_q)$ in common. Then we repeat the proof of Proposition 2 using the word "curve of type $(0,1)$ or of type $(1,0)$" instead of the word "line". □

Proposition 4. *Fix an integer $a \geq 1$ and a prime power $q > 4a^2$. Let D be an effective divisor of type (a, a) on an elliptic quadric surface $\mathbb{E}$. Then $\sharp(D(\mathbb{F}_q)) \leq aq + 2 - a)$ with equality if and only if therre are $P_1, P_2 \in \mathbb{E}(\mathbb{F}_q)$, D is the union of a smooth conics, say $C_1, \ldots, C_a$, each of defined over $\mathbb{F}_q$ and all of them through P_1 and P_2.*

Proof. Every effective divisor of $\mathbb{E}$ defined over $\mathbb{F}_q$ is of type (b, b) for some integer $b > 0$. Take any two smooth conics A, B on $\mathbb{F}_q$ defined over $\mathbb{F}_q$. Since $A \cdot B = 2$ (intersection product) either $A \cap B$ is formed by two distinct points belonging to $\mathbb{E}(\mathbb{F}_q)$ or $A \cap B$ is formed by a unique $P \in \mathbb{E}(\mathbb{F}_q)$ and A, B are tangent at P or $A \cap B$ is formed by two points of $E(\mathbb{F}_{q^2}) \backslash E(\mathbb{F}_q)$ which are conjugate for the involution of the hyperbolic quadric surface $E(\mathbb{E}(\mathbb{F}_{q^2}))$. Since $\sharp(\mathbb{E}(\mathbb{F}_q)) = q^2 + 1$, we see that only the first case may occur. Hence $\sharp((A \cup B)(\mathbb{F}_q)) = 2q$. Then we repeat the proof of Proposition 2 using the word "smooth conic" instead of the word "line". □

Proof of Theorem 2. Copy part (d) of the proof of Theorem 1 using Proposition 4 intead of Proposition 2. □

Acknowledgements

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

References

[1] K. Atkinson, A. Sharma, A partial characterization of poised Hermite-Birkhoff interpolation, *SIAM J. Numer. Anal.*, **6** (1969).

[2] R.A. Lorentz, *Multivariate Birkhoff Interpolation*, Lect. Notes in Math., **1516**, Springer, Berlin (1992).