International Journal of Pure and Applied Mathematics
Volume 35 No. 2 2007, 171-174

BASE LOCI OF HOMOGENEOUS FORMS IN THE PROJECTIVE PLANE OVER A FINITE FIELD

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

Abstract: Fix a finite set $S \subset \mathbf{P}^2$ defined over $\mathbb{F}_q$. Here we give conditions on $e \geq 1$, d and S such that there is a degree d plane curve defined over $\mathbb{F}_{q^e}$, containing S and avoiding another fixed finite subset of $\mathbf{P}^2$.

AMS Subject Classification: 14N05
Key Words: finite projective plane, homogeneous form, base locus

1. Base Loci of Homogeneous Forms

Fix a prime p, a p-power q, an integer $e \geq 1$ and a set $S \subset \mathbf{P}^2(\mathbb{F}_{q^e})$ which is invariant by the action of the Galois group of the field extension $[\mathbb{F}_{q^e} : \mathbb{F}_q]$. Set $\mathbf{P}^2 := \mathbf{P}^2(\bar{\mathbb{F}}_q)$. For all integers $d > 0$ and $f \geq e$ set $B(S; d, f, e) := \{P \in \mathbf{P}^2(\mathbb{F}_{q^f}) : u(P) = 0$ for all $u \in H^0(\mathbf{P}^2, \mathcal{I}_S(d))\}$ and $B(S; d, e) := B(S; d, e, e)$. Since $H^0(\mathbf{P}^2, \mathcal{I}_S(d))$ has a basis formed by homogeneous degree d forms defined over $\mathbb{F}_{q^f}$, in the definition of the sets $B(S; d, f, e)$ it is sufficient to use all homogeneous degree forms vanishing on S and with coefficients in $\mathbb{F}_q$. We will mainly be interested in the case $e = 1$. The case $e = 2$ is connected with Hermitian forms. Since $\bar{\mathbb{F}}_q$ and any projective space over $\bar{\mathbb{F}}_q$ is irreducible in the Zariski topology, it is easy to find the existence of $u \in H^0(\mathbf{P}^2, \mathcal{I}_S(d))$ such that $u(P) \neq 0$ for all $P \in \mathbf{P}^2(\mathbb{F}_{q^f}) \backslash B(S; d, f, e)$. It is easy to check that quite often no such u defined over $\mathbb{F}_{q^f}$ exists (see Remark 2). For any set $A \subset \mathbf{P}^2$ and any

Received: December 11, 2006

integer $d > 0$ set $B(A, d) := \{P \in \mathbf{P}^2 : u(P) = 0 \text{ for every } u \in H^0(\mathbf{P}^2, \mathcal{I}_A(d))\}$.

Remark 1. Fix a finite set $S \subset \mathbf{P}^2$, $S \neq \emptyset$. It is easy to check that $B(S, d) = S$ for all integers $d \geq \sharp(S)$ and that $B(S, d-1) = S$, unless S is contained in a line. Now assume that S is defined over $\mathbb{F}_q$, i.e. assume the existence of an integer $e \geq 1$ such that $S \subset \mathbf{P}^2(\mathbb{F}_{q^e})$ and S is invariant for the action on $\mathbf{P}^2(\mathbb{F}_{q^e})$ of the Galois group of the field extension $[\mathbb{F}_{q^e} : \mathbb{F}_q]$. Hence for all integers $t > 0$ the $\bar{\mathbb{F}}_q$-vector space $H^0(\mathbf{P}^2, \mathcal{I}_S(t))$ has a basis formed by degree t polynomials with coefficients in $\mathbb{F}_q$. Hence $B(S; t, f, e) = B(S, t) \cap \mathbf{P}^2(\mathbb{F}_{q^f})$ for all integers $f \geq e \geq 1$.

Remark 2. Fix a prime power q and an integer d such that $2 \leq d \leq q$. Let $D \subset \mathbf{P}^2$ be a line and a set $S \subset \mathbf{P}^2(\mathbb{F}_q)$ such that $\sharp(S \cap D) = d - 1$ and $B(S, d) = S$. By Remark 1 the latter condition is always satisfied if $\sharp(S) \leq d$. Fix $u \in H^0(\mathbf{P}^2, \mathcal{I}_S(d-1))\backslash\{0\}$ defined over $\mathbb{F}_q$. Hence $u|D$ has exactly d solutions defined over $\mathbb{F}_q$ and hence it vanishes at at least one point of $\mathbf{P}^2(\mathbb{F}_q)$. Hence no degree d polynomial of degree d defined over $\mathbb{F}_q$ vanishes at all points of S, but at no point of $\mathbf{P}^2(\mathbb{F}_q)\backslash S$. To find one such polynomial we need to use coefficients in $\mathbb{F}_{q^e}$ with $e \geq 2$. Indeed, any $e \geq 2$ will do this job.

The previous example is our motivation for the following result.

Theorem 1. *Fix a prime power q, integers $d \geq 2$, $e \geq 1$, and $S \subset \mathbf{P}^2(\mathbb{F}_{q^e})$, $S \neq \mathbf{P}^2(\mathbb{F}_{q^e})$, invariant by the action of the Galois group of the field extension $[\mathbb{F}_{q^e} : \mathbb{F}_q]$, such that $B(S, d, e) = S$. Set $h := \sharp(\mathbf{P}^2(\mathbb{F}_{q^e}\backslash S)$ and $f := \max\{h, e\}$. Then there exists a degree d homogeneous polynomial u with coefficients in $\mathbb{F}_{q^f}$ such that $u(P) = 0$ for every $P \in S$ and $u(Q) \neq 0$ for every $Q \in \mathbf{P}^2(\mathbb{F}_{q^e}\backslash S)$.*

Now we will consider the existence of degree d plane curves containing S, smooth at each point of $\mathbf{P}^2(\mathbb{F}_q)$ and defined over a small extension of $\mathbb{F}_q$, and prove the following results.

Theorem 2. *Fix a prime power q, integers $d \geq 2$, $e \geq 1$, and $S \subset \mathbf{P}^2(\mathbb{F}_{q^e})$, $S \neq \mathbf{P}^2(\mathbb{F}_{q^e})$. Assume that the homogeneous ideal of S is generated by forms of degree at most d. If $\sharp(S) \leq 2q^e$, then there exists a degree plane curve C defined over $\mathbb{F}_{q^e}$, containing S and smooth at each point of S.*

Theorem 3. *Fix a prime power q, integers $d \geq 2$, $e \geq 1$, and $S \subset \mathbf{P}^2(\mathbb{F}_{q^e})$, $S \neq \mathbf{P}^2(\mathbb{F}_{q^e})$. Assume that the homogeneous ideal of S is generated by forms of degree at most d. Set $\alpha := \sharp(\mathbf{P}^2(\mathbb{F}_q)\backslash S$. If $\sharp(S) + 2\alpha \leq 2q^e$, then there exists a degree plane curve C defined over $\mathbb{F}_{q^e}$, containing S and smooth at each point of S and at not containing any point of $\mathbf{P}^2(\mathbb{F}_q)\backslash S$.*

Remark 3. Instead of $\mathbf{P}^2(\mathbb{F}_q)\backslash S$ we may take in the thesis of Theorem 3 any $A \subseteq \mathbf{P}^2(\mathbb{F}_{q^e})$ using the integer $\sharp(A)$ instead of the integer α.

For any homogeneous degree d polynomial u such that $u \ne 0$, let $(u)_0$ denote its scheme-theoretic base locus, i.e. the associated degree d curve (which may have multiple components). For any integer $d > 0$ and any scheme $Z \subseteq \mathbf{P}^2$ let $\widetilde{B}(Z,d)$ denote the scheme theoretic intersection of all curves $(u)_0$ with $u \in H^0(\mathbf{P}^2, \mathcal{I}_Z(d))\backslash\{0\}$. We will see any finite set $S \subset \mathbf{P}^2$ as a reduced zero-dimensional scheme. With this convention $B(S,d) = \widetilde{B}(S,d)_{red}$. If $f \ge e \ge 1$ are integers, $S \subset \mathbf{P}^2(\mathbb{F}_{q^e})$ and $\widetilde{B}(S,d)$ is zero-dimensional, let $\widetilde{B}(S,d,f,e)$ denote the union of all connected components of $\widetilde{B}(S,d)$ whose support is contained in $\mathbf{P}^2(\mathbb{F}_{q^f})$. From now on we assume that $B(Z,d)$ is zero-dimensional. For any $P \in \mathbf{P}^2$ let $A(Z,d;P)$ denote the connected component of $\widetilde{B}(Z,d)$ which is supported by P. Thus $A(Z,d;P) = \emptyset$ if and only if $P \notin \widetilde{B}(Z,d)_{red}$. If Z and P are defined over $\mathbb{F}_{q^e}$, then $A(Z,d;P)$ is defined over $\mathbb{F}_{q^e}$. For any $P \in \mathbf{P}^2$, let $2P$ denote the closed zer-dimensional subscheme of $\mathbf{P}^2$ with ${\mathcal{I}_P}^2$ as its ideal sheaf, If P is defined over $\mathbb{F}_{q^e}$, then $2P$ is defined over $\mathbb{F}_{q^e}$.

Proof of Theorem 1. Let V be the $h^0(\mathbf{P}^2, \mathcal{I}_S(d))$-dimensional $\mathbb{F}_{q^f}$-vector space of all degree d homogeneous forms vanishing on S and with coefficients in $\mathbb{F}_{q^f}$. For any $Q \in \mathbf{P}^2(\mathbb{F}_{q^e})$ set $V(-Q) := \{u \in V : u(Q) = 0\}$. Since $f \ge e$, $V(-Q)$ is a $\mathbb{F}_{q^f}$-vector space. Since $B(S,d,e) = S$ and $f \ge e$, for every $Q \in \mathbf{P}^2(\mathbb{F}_{q^e})\backslash S$ is a $\mathbb{F}_{q^f}$-hyperplane. Thus $\sharp(V(-Q)) = \sharp(V)/q^f$ for all $Q \in \mathbf{P}^2(\mathbb{F}_{q^e})\backslash S$. Since $0 \in V(-Q)$ for all Q and $f \ge h$, we get $\sharp(V) > \sum_Q \sharp(V(-Q))$. Hence there is $u \in V$ such that $u(Q) \ne 0$ for all $Q \in \mathbf{P}^2(\mathbb{F}_{q^e})\backslash S$. □

Remark 4. Fix a finite $S \subset \mathbf{P}^2$ and an integer d such that the scheme $\widetilde{B}(S,d)$ is zero-dimensional, i.e. such that $B(S,d)$ is finite. Set $M := H^0(\mathbf{P}^2\mathcal{I}_S(d))$. Fix $P \in \mathbf{P}^2$ and a zero-dimensional subscheme $\tau \subset \mathbf{P}^2$ such that $\text{length}(\tau) = 2$ and $\tau_{red} = \{P\}$, i.e. a tangent vector of $\mathbf{P}^2$ at P. Set $M(-P) := \{u \in M : u(P) = 0\}$, $M(-\tau) := \{u \in M : u|\tau \equiv 0\}$ and $M(-2P) := \{u \in M : u|2P \equiv 0\}$. Hence $M(-P) = M$ if $P \in B(S,d)$, while $M(-P)$ is a hyperplane of M if $P \notin B(S,d)$. Either $M(-\tau) = M(-P)$ or $M(-\tau)$ is a hyperplane of $M(-P)$. If $P \in B(S,d)$, then $M(-\tau) = M$ if and only if $\tau \subseteq \widetilde{B}(S,d)$. Either $M(-2P) = M(-2\tau)$ or $M(-2P)$ is a hyperplane of $M(-\tau)$.If $P \notin B(S,d)$, then $\dim(M(-\tau)) = \dim(M) - 2$ if and only if the differential at P of the rational map γ_M induced by the linear system $|M|$ (which is a morphism in a neighborhood of P) does not kill the tangent vector τ; furthermore, $\dim(M(-2P)) = \dim(M) - 3$ if and only if the differential of γ_M is injective. Now assume $P \in B(S,d)$; $M(-\tau) \ne M(-P) = M$ if and only if there is a curve $C \in |\mathcal{I}_S(d)|$ which is smooth at P and whose tangent line at P does not contain τ; we have $\dim(M(-2P)) = \dim(M(-P)) - 2$ if and only if $M(-\mu) \ne M(-P)$ for all tangent vectors μ of $\mathbf{P}^2$ at P and there are curves $C, C' \in |M|$ which are smooth at P and whose If S and P are defined over $\mathbb{F}_{q^e}$, then $M(-P)$ and $M(-2P)$ are defined over $\mathbb{F}_{q^e}$. If S, P and τ are defined over $\mathbb{F}_{q^e}$, then $M(-\tau)$ is defined over $\mathbb{F}_{q^e}$. Now assume that S and P are defined over $\mathbb{F}_{q^e}$ and write M_e, $M_e(-P)$ and $M_e(-2P)$ for the corresponding $\mathbb{F}_{q^e}$-vector subspaces of M. Notice that $\dim(M) = \dim(M_e)$, $\dim(M(-P)) = \dim(M_e(-P))$ and $\dim(M(-2P)) = \dim(M_e(-2P))$.

(a) If $\dim(M(-2P)) = \dim(M) - 3$, then $\sharp(M_e(-2P)) = \sharp(M_e)/3q^e$.

(b) If $\dim(M(-2P)) = \dim(M) - 2$, then $\sharp(M_e(-2P)) = \sharp(M_e)/2q^e$.

(c) If $\dim(M(-2P)) = \dim(M) - 1$, then $\sharp(M_e(-2P)) = \sharp(M_e)/q^e$.

Fix $P \in B(S, d)$. We have $\dim(M(-2P)) = \dim(M) - 2$ (resp. $\dim(M(-2P)) = \dim(M) - 1$) if and only if $A(S, d; P) = \{P\}$ with its reduced structure (resp. $A(S, d; P)$ is not reduced, but it does not contain the scheme $2P$.

Remark 5. Fix a finite $S \subset \mathbf{P}^2$ and an integer $d > 0$. Assume $h^1(\mathbf{P}^2, \mathcal{I}_S(d-1)) = 0$. By Castelnuovo-Mumford's Lemma the homogeneous ideal of S is generated by forms of degree at most d. Hence we may use the more easily checked assumption "$h^1(\mathbf{P}^2, \mathcal{I}_S(d-1)) = 0$" in the statement of Theorem 2.

Proof of Theorems 2 and 3. If the homogeneous ideal of S is generated by forms of degree at most P, then $A(S, d; P) = \{P\}$ for all $P \in S$. Apply Remark 4. To prove Theorem 3 also use that $M(-P) \neq M$ for all $P \in \mathbf{P}^2(\mathbb{F}_q)$ such that $P \neq S$. □

Acknowledgements

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