A NOTE ON RATIONAL NORMAL CURVES TOTALLY TANGENT TO A HERMITIAN VARIETY

ICHIRO SHIMADA

Abstract. Let q be a power of a prime integer p, and let X be a Hermitian variety of degree $q+1$ in the n-dimensional projective space. We count the number of rational normal curves that are tangent to X at distinct $q+1$ points with intersection multiplicity n. This generalizes a result of B. Segre on the permutable pairs of a Hermitian curve and a smooth conic.

1. Introduction

Throughout this paper, we fix a power $q := p^{\nu}$ of a prime integer p. Let k denote the algebraic closure of the finite field $\mathbb{F}_{q^2}$.

Let n be an integer ≥ 2. We say that a hypersurface X of $\mathbb{P}^n$ defined over $\mathbb{F}_{q^2}$ is a *Hermitian variety* if X is projectively isomorphic over $\mathbb{F}_{q^2}$ to the Fermat variety

$$X_I := \{x_0^{q+1} + \cdots + x_n^{q+1} = 0\} \ \subset \ \mathbb{P}^n$$

of degree $q+1$. (Strictly speaking, one should say that X is a Hermitian variety of rank $n+1$. Since we treat only nonsingular Hermitian varieties in this paper, we omit the term "of rank $n+1$".) We say that a hypersurface X of $\mathbb{P}^n$ defined over k is a *k-Hermitian variety* if X is projectively isomorphic over k to X_I. By definition, the projective automorphism group $\mathrm{Aut}(X) \subset \mathrm{PGL}_{n+1}(k)$ of a k-Hermitian variety X is conjugate to $\mathrm{Aut}(X_I) = \mathrm{PGU}_{n+1}(\mathbb{F}_{q^2})$ in $\mathrm{PGL}_{n+1}(k)$.

Let X be a k-Hermitian variety in $\mathbb{P}^n$. A rational normal curve Γ in $\mathbb{P}^n$ defined over k is said to be *totally tangent to X* if Γ is tangent

---

2000 *Mathematics Subject Classification.* 51E20, 14M99.
Partially supported by JSPS Grants-in-Aid for Scientific Research (B) No.20340002 .

to X at distinct $q+1$ points and the intersection multiplicity at each intersection point is n.

A subset S of a rational normal curve Γ is called a *Baer subset* if there exists a coordinate $t : \Gamma \xrightarrow{\sim} \mathbb{P}^1$ on Γ such that S is the inverse image by t of the set $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ of $\mathbb{F}_q$-rational points of $\mathbb{P}^1$.

The purpose of this paper is to prove the following:

Theorem 1. *Suppose that* $n \not\equiv 0 \pmod p$ *and* $2n \le q$. *Let* X *be a* k*-Hermitian variety in* $\mathbb{P}^n$.

(1) *The set* R_X *of rational normal curves totally tangent to* X *is non-empty, and* $\mathrm{Aut}(X)$ *acts on* R_X *transitively with the stabilizer subgroup isomorphic to* $\mathrm{PGL}_2(\mathbb{F}_q)$. *In particular, we have*

$$|R_X| = |\mathrm{PGU}_{n+1}(\mathbb{F}_{q^2})|/|\mathrm{PGL}_2(\mathbb{F}_q)|.$$

(2) *For any* $\Gamma \in R_X$, *the points in* $\Gamma \cap X$ *form a Baer subset of* Γ.

(3) *If* X *is a Hermitian variety, then every* $\Gamma \in R_X$ *is defined over* $\mathbb{F}_{q^2}$ *and every point of* $\Gamma \cap X$ *is* $\mathbb{F}_{q^2}$*-rational.*

The study of Hermitian varieties was initiated by B. Segre in [5]. Since then, Hermitian varieties have been intensively studied mainly from combinatorial point of view in finite geometry. (See, for example, Chapter 23 of [3]). B. Segre obtained Theorem 1 for the case $n = 2$ in the investigation of commutative pairs of polarities [5, n. 81]. We give a simple proof of the higher-dimensional analogue (Theorem 1) of his result using arguments of projective geometry over k.

Notation. (1) For simplicity, we put

$$\widetilde{G} := \mathrm{GL}_{n+1}(k) \quad \text{and} \quad G := \mathrm{PGL}_{n+1}(k).$$

We let G act on $\mathbb{P}^n$ from *right*. For $T \in \widetilde{G}$, we denote by $[T] \in G$ the image of T by the natural homomorphism $\widetilde{G} \to G$. The entries $a_{i,j}$ of a matrix $A = (a_{i,j}) \in \widetilde{G}$ are indexed by

$$N := \{\ (i,j) \in \mathbb{Z}^2 \ \mid\ 0 \le i \le n,\ \ 0 \le j \le n\ \}.$$

(2) Let M be a matrix with entries in k. We denote by ${}^tM$ the transpose of M, and by $\overline{M}$ the matrix obtained from M by applying $a \mapsto a^q$ to the entries.

2. Proof of Theorem 1

The following well-known proposition is the main tool of the proof.

Proposition 2. *The map* $\lambda : \widetilde{G} \to \widetilde{G}$ *defined by* $\lambda(T) := T\,{}^t\overline{T}$ *is surjective. The image of* $\mathrm{GL}_{n+1}(\mathbb{F}_{q^2}) \subset \widetilde{G}$ *by* λ *is equal to the set*

$$\mathcal{H} := \{\ H \in \mathrm{GL}_{n+1}(\mathbb{F}_{q^2})\ \mid\ H = {}^t\overline{H}\ \}$$

of Hermitian matrices over $\mathbb{F}_{q^2}$.

Proof. The first part is a variant of Lang's theorem [4], and can be proved by means of differentials (see [7] or [1, 16.4]). The second part is due to B. Segre [5, n. 3]. See also [6, Section 1]. □

For a matrix $A = (a_{i,j}) \in \widetilde{G}$, we define a homogeneous polynomial f_A of degree $q+1$ by

$$f_A := \sum_{(i,j)\in N} a_{i,j} x_i x_j^q.$$

If $g = [T] \in G$, then the image X_I^g of the Fermat hypersurface X_I by g is defined by $f_{\lambda(T^{-1})} = 0$. Hence we obtain the following:

Corollary 3. *A hypersurface* X *of* $\mathbb{P}^n$ *is a* k*-Hermitian variety if and only if there exists a matrix* $A \in \widetilde{G}$ *such that* X *is defined by* $f_A = 0$. *A hypersurface* X *is a Hermitian variety if and only if there exists a Hermitian matrix* $H \in \mathcal{H}$ *over* $\mathbb{F}_{q^2}$ *such that* X *is defined by* $f_H = 0$.

Let $\mathcal{V}$ denote the set of all k-Hermitian varieties in $\mathbb{P}^n$. For $A \in \widetilde{G}$, let $X_A \in \mathcal{V}$ denote the hypersurface defined by $f_A = 0$. (The Fermat hypersurface X_I is defined by $f_I = 0$, where $I \in \widetilde{G}$ is the identity matrix.) Remark that G acts on $\mathcal{V}$ transitively.

Let $\mathcal{R}$ denote the set of all rational normal curves in $\mathbb{P}^n$, and let $\mathcal{P}$ be the set of pairs

$$[\Gamma, (Q_0, Q_1, Q_\infty)],$$

where $\Gamma \in \mathcal{R}$, and Q_0, Q_1, Q_∞ are ordered three distinct points of Γ. Let $\Gamma_0 \in \mathcal{R}$ be the image of the morphism $\phi_0 : \mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ given by

$$\phi_0(t) := [1 : t : \cdots : t^n] \in \mathbb{P}^n.$$

We put

$$P_0 := \phi_0(0), \quad P_1 := \phi_0(1), \quad P_\infty := \phi_0(\infty).$$

Then we have $[\Gamma_0, (P_0, P_1, P_\infty)] \in \mathcal{P}$.

Lemma 4. *The action of G on $\mathcal{P}$ is simply transitive.*

Proof. The action of G on $\mathcal{R}$ is transitive by the definition of rational normal curves. Let $\Sigma_0 \subset G$ denote the stabilizer subgroup of $\Gamma_0 \in \mathcal{R}$. Then we have a natural homomorphism

$$\psi : \Sigma_0 \to \mathrm{Aut}(\Gamma_0) \cong \mathrm{PGL}_2(k).$$

Note that $\mathrm{Aut}(\Gamma_0)$ acts on the set of ordered three distinct points of Γ_0 simple-transitively. Hence it is enough to show that ψ is an isomorphism. Since Γ_0 contains $n+2$ points such that any $n+1$ of them are linearly independent in $\mathbb{P}^n$, ψ is injective. Since $\mathrm{PGL}_2(k)$ is generated by the linear transformations

$$t \mapsto at+b \quad \text{and} \quad t \mapsto 1/(t-c), \quad \text{where} \quad a \in k^\times \ \text{and} \ b, c \in k,$$

it is enough to find matrices $M_{a,b} \in \widetilde{G}$ and $N_c \in \widetilde{G}$ such that

$$\begin{aligned} [1, at+b, \dots, (at+b)^n] &= [1, t, \dots, t^n]\, M_{a,b} \quad \text{and} \\ [(t-c)^n, (t-c)^{n-1}, \dots, 1] &= [1, t, \dots, t^n]\, N_c \end{aligned}$$

hold for any $a \in k^\times$ and $b, c \in k$. This is immediate. □

We denote by $\mathcal{I} \subset \mathcal{V} \times \mathcal{P}$ the set of all triples $[X, \Gamma, (Q_0, Q_1, Q_\infty)]$ such that

(1) $X \in \mathcal{V}$ and $[\Gamma, (Q_0, Q_1, Q_\infty)] \in \mathcal{P}$,
(2) Γ is totally tangent to X, and
(3) Q_0, Q_1, Q_∞ are contained in $\Gamma \cap X$.

We then consider the incidence diagram

$$\begin{array}{ccc} \mathcal{I} & \xrightarrow{p_1} & \mathcal{V} \\ {\scriptstyle p_{23}} \downarrow & & \\ \mathcal{P}. & & \end{array}$$

Note that G acts on $\mathcal{I}$, and that the projections p_1 and p_{23} are G-equivariant.

We consider the Hermitian matrix $B = (b_{i,j}) \in \mathcal{H}$, where

$$b_{i,j} := \begin{cases} \binom{n}{i}(-1)^i & \text{if } i+j=n, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$\phi_0^* f_B = \sum_{i=0}^{n} \binom{n}{i} (-1)^i t^i t^{q(n-i)} = (t^q - t)^n,$$

and hence $[X_B, \Gamma_0, (P_0, P_1, P_\infty)]$ is a point of $\mathcal{I}$. Since $\mathcal{I} \neq \emptyset$ and the action of G on $\mathcal{V}$ is transitive, the G-equivariant map p_1 is surjective. Thus $R_X \neq \emptyset$ holds for any $X \in \mathcal{V}$.

The following proposition is proved in the next section.

Proposition 5. *Suppose that* $n \not\equiv 0 \pmod p$ *and* $n \leq 2q$. *Then the fiber of* p_{23} *over* $[\Gamma_0, (P_0, P_1, P_\infty)] \in \mathcal{P}$ *consists of a single point* $[X_B, \Gamma_0, (P_0, P_1, P_\infty)] \in \mathcal{I}$. *In particular,* p_{23} *is a bijection.*

Theorem 1 follows from Proposition 5 as follows. First note that, for any $X \in \mathcal{V}$, the map $[X, \Gamma, (Q_0, Q_1, Q_\infty)] \mapsto \Gamma$ gives a surjection

$$\rho_X \ : \ p_1^{-1}(X) \ \to \ R_X.$$

Proposition 5 implies that G acts on $\mathcal{I}$ simple-transitively. If $S \subset \Gamma$ is a Baer subset of $\Gamma \in \mathcal{R}$, then $S^g \subset \Gamma^g$ is a Baer subset of Γ^g for any $g \in G$. Since $\Gamma_0 \cap X_B$ is a Baer subset of Γ_0, we see that $\Gamma \cap X$ is a Baer subset of Γ for any $[X, \Gamma, (Q_0, Q_1, Q_\infty)] \in \mathcal{I}$. Therefore the assertion (2) follows. Since p_1 is G-equivariant, the stabilizer subgroup $\mathrm{Aut}(X)$ of X in G acts on the fiber $p_1^{-1}(X)$ simple-transitively for any $X \in \mathcal{V}$. Note that ρ_X is $\mathrm{Aut}(X)$-equivariant. Hence the stabilizer subgroup $\mathrm{Stab}(\Gamma)$ of $\Gamma \in R_X$ in $\mathrm{Aut}(X)$ acts on the fiber $\rho_X^{-1}(\Gamma)$ simple-transitively. Moreover, since Γ contains $n+2$ points such that any $n+1$ of them are linearly independent, $\mathrm{Stab}(\Gamma)$ is embedded into $\mathrm{Aut}(\Gamma) \cong \mathrm{PGL}_2(k)$. Since $\rho_X^{-1}(\Gamma)$ is the set of ordered three distinct points of the Baer subset $\Gamma \cap X$ of Γ, we see that $\mathrm{Stab}(\Gamma)$ is conjugate to $\mathrm{PGL}_2(\mathbb{F}_q)$ as a subgroup of $\mathrm{Aut}(\Gamma) \cong \mathrm{PGL}_2(k)$. Thus the assertion (1) follows. The assertion (3) is immediate from the facts that X_B is Hermitian, that Γ_0 is defined over $\mathbb{F}_{q^2}$, and that every points of $\Gamma_0 \cap X_B$ is $\mathbb{F}_{q^2}$-rational. $\square$

3. Proof of Proposition 5

Suppose that $A = (a_{i,j}) \in \widetilde{G}$ satisfies $[X_A, \Gamma_0, (P_0, P_1, P_\infty)] \in \mathcal{I}$. We will show that $A = c\,B$ for some $c \in k^\times$.

By the definition of $\mathcal{I}$, there exists a polynomial $h \in k[t]$ such that the polynomial

$$\phi_0^* f_A = \sum_{(i,j)\in N} a_{i,j} t^{i+qj}$$

is equal to h^n, and that, regarded as a polynomial of degree $q+1$, h has distinct $q+1$ roots including 0, 1 and ∞. In particular, we have $\deg h = q$ and $h(0) = 0$. Thus we can set

$$h = \sum_{\nu=1}^{q} b_\nu t^\nu.$$

Since $\deg h = q$ and since $t = 0$ is a simple root of $h = 0$, we have

$$b_q \neq 0 \quad \text{and} \quad b_1 \neq 0.$$

Let c_m denote the coefficient of t^m in $\phi_0^* f_A$. We have $c_m = 0$ if no $(i,j) \in N$ satisfy $i + qj = m$. By the assumption $2n \leq q$, we have

$$c_m = 0 \quad \text{if} \quad n < m < q \ \text{ or } \ n + q(n-1) < m < qn. \tag{3.1}$$

We will show that

$$b_\mu = 0 \quad \text{if} \quad n < \mu < q. \tag{3.2}$$

Let l be the largest integer such that $l < q$ and $b_l \neq 0$. Since $n \not\equiv 0 \pmod p$ and $b_q \neq 0$, the coefficient $n\,b_q^{n-1} b_l$ of $t^{l+q(n-1)}$ in h^n is non-zero. Therefore $c_{l+q(n-1)} \neq 0$ follows from $\phi_0^* f_A = h^n$. By (3.1) and $l < q$, we have $l \leq n$. Hence (3.2) holds. In the same way, we will show that

$$b_\mu = 0 \quad \text{if} \quad 1 < \mu < q - n + 1. \tag{3.3}$$

Let l be the smallest integer such that $l > 1$ and $b_l \neq 0$. Since $n \not\equiv 0 \pmod p$ and $b_1 \neq 0$, the coefficient $n\,b_1^{n-1} b_l$ of t^{n-1+l} in h^n is non-zero. Therefore $c_{n-1+l} \neq 0$ follows from $\phi_0^* f_A = h^n$. By (3.1) and $l > 1$, we have $n - 1 + l \geq q$. Hence (3.3) holds.

Combining (3.2), (3.3) with the assumption $2n \le q$, we see that h is of the form $b_q t^q + b_1 t$. Since $h(1) = 0$, we have

$$h = b(t^q - t) \quad \text{for some } b \in k^{\times}.$$

From $\phi_0^* f_A = h^n$, we see that $A = b^n B$. □

Remark 6. In [2], another generalization of B. Segre's result [5, n. 81] is obtained.

References

[1] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[2] Giorgio Donati and Nicola Durante. On the intersection of a Hermitian curve with a conic. *Des. Codes Cryptogr.*, 57(3):347–360, 2010.

[3] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[4] Serge Lang. Algebraic groups over finite fields. *Amer. J. Math.*, 78:555–563, 1956.

[5] Beniamino Segre. Forme e geometrie hermitiane, con particolare riguardo al caso finito. *Ann. Mat. Pura Appl. (4)*, 70:1–201, 1965.

[6] Ichiro Shimada. Lattices of algebraic cycles on Fermat varieties in positive characteristics. *Proc. London Math. Soc. (3)*, 82(1):131–172, 2001.

[7] Robert Steinberg. On theorems of Lie-Kolchin, Borel, and Lang. In *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*, pages 349–354. Academic Press, New York, 1977.

Department of Mathematics, Graduate School of Science, Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526 JAPAN

E-mail address: `shimada@math.sci.hiroshima-u.ac.jp`