No. 759

# Mutually M-intersecting Hermitian Varieties

by

Ryoh Fuji-Hara and Nobuko Miyamoto

October 1997

# Mutually $M$-intersecting Hermitian Varieties

Ryoh Fuji-Hara and Nobuko Miyamoto
(fujihara@sk.tsukuba.ac.jp)
(nmiyamot@sk.tsukuba.ac.jp)

Institute of Policy and Planning Sciences,
University of Tsukuba,
Tsukuba, Ibaraki, Japan 305

**Abstract**

Let $M$ be a set of a few integers. We consider a set of varieties in $\mathrm{PG}(n,q)$ such that each variety contains $\rho$ points and the number of points in the intersection of two distinct varieties is contained in $M$. Such set is called a set of mutually $M$-intersecting varieties. In this paper, it will be shown that there exist new sets of mutually $M$-intersecting varieties by using Hermitian varieties in $\mathrm{PG}(2,q^2)$ and a unitary group of order $q+1$.

Let $f$ be a homogeneous polynomial. The set of points $x$ of $\mathrm{PG}(n,q)$ satisfying $f(x)=0$ is called a *variety* and denoted by $V(f)$. In a previous paper [4], we proposed a problem called *mutually $M$-intersecting varieties*. It is a set of varieties $V(f_1)$, $V(f_2)$, $\cdots, V(f_s)$ which satisfies the following three conditions:

(i) $M$ is a set of non-negative integers.

(ii) $|V(f_i)| = \rho$ for $1 \le i \le s$.

(iii) $|V(f_i) \cap V(f_j)| \in M$ for $1 \le i,j \le s$, $i \ne j$.

We will use $\mathcal{V}(\rho, M)$ to denote the set and $\mathcal{V}(\rho,\mu)$ when $M$ is a singleton $\{\mu\}$. Note $s = |\mathcal{V}(\rho, M)|$.

Some results on mutually $\{\mu\}$-intersecting varieties are shown in [4]. Using quadrics and a projective group on $\mathrm{PG}(3,q)$, we obtained $\mathcal{V}(q^2+1, q+1)$ consisting of $q^2$ varieties and $\mathcal{V}((q+1)^2, 3q+1)$ of $q^2$ varieties. Finding $\mathcal{V}(\rho, M)$ which consists of a number of varieties is an interesting problem. $\mathcal{V}(\rho, M)$ is useful to construct combinatorial designs such as $(r,\lambda)$-design and arrays like orthogonal, incomplete orthogonal or balanced arrays [2], [3]. In this paper, we will use results on intersections of Hermitian varieties shown by Kestenband [8] and construct new sets of mutually M-intersecting Hermitian varieties in $\mathrm{PG}(2,q^2)$ with $M$ of a few integers.

## 1 Hermitian variety

A $(n+1) \times (n+1)$ square matrix $H = (h_{ij})$ with elements from GF$(q^2)$ is called a *Hermitian matrix* if $h_{ij} = h_{ji}^q$ for all $i, j$. Let $A^{(q)} = (a_{ij}^q)$ for a matrix $A = (a_{ij})$, $a_{ij} \in$ GF$(q^2)$. A *Hermitian variety* (abbreviated to HV) is defined as $\{x \in \mathrm{PG}(2, q^2)\ ;\ f(x) = x^T H x^{(q)} = 0\}$, where $H$ is a Hermitian matrix. Here we use $V(H)$ instead of $V(f)$ to denote the Hermitian variety. Two Hermitian matrices $H$ and $G$ are said to be *equivalent* if there exists a nonsingular matrix $P$ over GF$(q^2)$ such that $P^T H P^{(q)} = G$. When $H$ is a rank $r$ Hermitian matrix, $V(H)$ is called a *rank* $r$ HV. A rank $n+1$ HV in PG$(n, q^2)$ is also called a nondegenerate HV. The properties of a HV in PG$(2, q^2)$ have been studied [1], [8]. A HV in PG$(2, q^2)$ contains $q^2+1$, $q^3+q^2+1$ or $q^3+1$ points, according to the rank 1, 2, or 3, respectively. It is also known that any non-singular Hermitian matrix is equivalent to a unit matrix $I$.

Kestenband [8] has showed a classification of $V(H)$ in PG$(2, q^2)$ with respect to intersections with $V(I)$. Note that the minimal polynomial $m(x)$ of a matrix $H$ satisfies $m(H) = 0$ and $m'(H) \neq 0$ for any polynomial $m'(x)$ with $deg(m'(x)) < deg(m(x))$.

**Result (B.C. Kestenband)**
Let $H$ be a non-singular Hermitian matrix. Let $m(x)$ and $g(x)$ be minimal and characteristic polynomial of it respectively. $V(H) \cap V(I)$ contains

(1) $(q+1)^2$ points, if $m(x) = g(x) = (x-\alpha)(x-\beta)(x-\gamma)$, $\alpha$, $\beta$, $\gamma$ distinct elements of GF$(q)$.

(2) $q^2+q+1$ points, if $m(x) = g(x) = (x-\alpha)(x-\beta)^2$, $\alpha$, $\beta$, distinct elements of GF$(q)$.

(3) $q+1$ collinear points if $m(x) = (x-\alpha)(x-\beta)$ , $\alpha$, $\beta$, distinct elements of GF$(q)$.

(4) $q^2+1$ points, if $m(x) = g(x) = (x-\alpha)p(x)$, $\alpha \in$ GF$(q)$, $p(x)$ : irreducible over GF$(q)$.

(5) $q^2+1$ points, if $m(x) = g(x) = (x-\lambda)^3$ .

(6) one point if $m(x) = (x-\lambda)^2$.

(7) $q^2-q+1$ points, no three of which are collinear, if $g(x)$ is irreducible over GF$(q^2)$.

In addition to the above result, Kestenband [7] generated a set $\chi$ consisting of $q^2+q+1$ Hermitian matrices with irreducible characteristic polynomials over GF$(q)$. The set of varieties from $\chi$ directly forms $\mathcal{V}(q^3+1, q^2-q+1)$. Since $\chi$ is isomorphic to PG$(2,q)$, the incidence matrix of the varieties $\mathcal{V}(q^3+1, q^2-q+1)$ and the points on PG$(2,q^2)$ contains $q^2-q+1$ copies of PG$(2,q)$. In the next section, we use a Hermitian matrix with minimal polynomial $(x-1)^3$ and construct new mutually $M$-intersecting varieties which are different from the result of Kestenband.

## 2 Constructions

We assume in the rest of this paper that $q$ is an even prime power. A matrix $U$ is unitary if $U^T U^{(q)} = I$. Consider the following unitary matrix $U$ and group $\mathcal{U}$ of order $q+1$ over GF$(q^2)$.

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, \quad \text{where } \alpha^{q+1} = 1,\ \alpha \neq 1 \text{ over GF}(q^2),$$

$$\mathcal{U} = \{I, U, U^2, \ldots, U^q\}.$$

Let $H$ be a non-singular Hermitian matrix with minimal polynomial $m(x) = (x-1)^3$. Without loss of generality, we can put

$$H = \begin{pmatrix} 1 & a & 0 \\ a^q & 1 & b \\ 0 & b^q & 1 \end{pmatrix}, \quad \text{where } a, b \in \text{GF}(q^2) \setminus \{0\}, \quad a^{q+1} + b^{q+1} = 0.$$

Using above unitary group $\mathcal{U}$, we define a set of HV's by

$$\mathcal{H} = \{V(H_1), V(H_2), \ldots, V(H_{q+1})\} \text{ ,where } H_i = U^{i^T} H U^{i^{(q)}}, \quad U^i \in \mathcal{U}.$$

Then $H_i$ is expressed by

$$H_i = \begin{pmatrix} 1 & a\alpha^{iq} & 0 \\ a^q\alpha^i & 1 & b\alpha^{iq} \\ 0 & b^q\alpha^i & 1 \end{pmatrix}.$$

Note that any $V(H_i) \in \mathcal{H}$ is a nondegenerate HV and it contains $q^3+1$ points.

**Theorem 1** *Let $q$ be an even prime power. Then $\mathcal{H}$ is a set of mutually $M$-intersecting varieties $\mathcal{V}(q^3+1, q^2+1)$, where $|\mathcal{V}(q^3+1, q^2+1)| = q+1$.*

**Proof.** We will show that any distinct two HV's $V(H_i)$ and $V(H_j)$ of $\mathcal{H}$ have $q^2+1$ points in common. We can say that $|V(H_i) \cap V(H_j)| = |V(U^{i^T} H U^{i^{(q)}}) \cap V(U^{j^T} H U^{j^{(q)}})| = |V(U^{i+k^T} H U^{i+k^{(q)}}) \cap V(H)|$ for some $k$ such that $U^{j+k} = I$. So we only show that the number of points of $V(H_i) \cap V(H)$ for any $V(H_i) \in \mathcal{H}$, $H_i \neq H$ is $q^2+1$. Moreover we have $|V(H_i) \cap V(H)| = |V(P^T H_i P^{(q)}) \cap V(I)|$, where $P$ is a non-singular matrix such that $P^t H P^{(q)} = I$:

$$P = \begin{pmatrix} 1 & a^q t & a^q b^q t \\ 0 & t & b^q t^q \\ 0 & 0 & t^{-1} \end{pmatrix}, \quad \text{where } t^{q+1}(a^{q+1}+1) = 1 \text{ over } \mathrm{GF}(q^2).$$

The characteristic polynomial of $P^t H_i P^{(q)}$ is $\det(P^t H_i P^{(q)} - xI) = \det(P^t H_i P^{(q)} - x P^t H P^{(q)}) = \det(P^T)\det(H_i - xH_j)\det(P^{(q)}) = \det(H_i - xH_j) = (x-1)^3$. When the first row of $P^t H_i P^{(q)}$ is expressed by $p^T = (1, at^q(1+\alpha^i)^q, abt(1+\alpha^i)^q)$, the (1,1)-entry of $(P^t H_i P^{(q)} - I)^2$ is $p^T p^{(q)} + 1 = 1 + a^{q+1}t^{q+1}(1+\alpha^i)^{q+1} + a^{q+1}b^{q+1}t^{q+1}(1+\alpha^i)^{q+1} + 1 = a^{q+1}(1+\alpha^i)^{q+1} \neq 0$ by $t^{q+1}(1+b^{q+1}) = 1$. Since $(P^t H_i P^{(q)} - I)^2 \neq \mathbf{0}$, the minimal polynomial of $P^T H_j P^{(q)}$ is $(x-1)^3$. Hence we have $|V(H_i) \cap V(H)| = q^2+1$ from Result given by the previous section. ■

Next consider two non-singular Hermitian matrices $H$ and $H'$ both having the minimal polynomial $m(x) = (x-1)^3$. Then as we mentioned before, we can define two sets as follows:

$$\mathcal{H}_{a,b} = \{V(H_1), V(H_2), \ldots, V(H_{q+1})\}, \quad \text{where } H_i = U^{i^T} H U^{i^{(q)}}, \quad U^i \in \mathcal{U},$$

$$\mathcal{H}_{c,d} = \{V(H'_1), V(H'_2), \ldots, V(H'_{q+1})\}, \quad \text{where } H'_j = U^{j^T} H' U^{j^{(q)}}, \quad U^j \in \mathcal{U},$$

where

$$H = \begin{pmatrix} 1 & a & 0 \\ a^q & 1 & b \\ 0 & b^q & 1 \end{pmatrix}, \qquad H' = \begin{pmatrix} 1 & c & 0 \\ c^q & 1 & d \\ 0 & d^q & 1 \end{pmatrix},$$

$a, b, c, d \in \mathrm{GF}(q^2) \setminus \{0\}, \quad a^{q+1} + b^{q+1} = 0, \quad c^{q+1} + d^{q+1} = 0.$

In order to have $\mathcal{H}_{a,b}$ and $\mathcal{H}_{c,d}$ which are disjoint, we have to restrict $a$,$b$,$c$, and $d$. Let $w$ be a primitive element of the multiplicative group $\mathrm{GF}(q^2) \setminus \{0\}$ of order $q^2-1$. Let $K = \{1, w^{q-1}, \ldots, w^{q(q-1)}\}$ be a multiplicative subgroup of order $q+1$ and $K_k = K \cdot w^k$ for $k$ cosets of $K$, $0 \le k \le q-2$. Suppose $a \in K_l$, $0 \le l \le q-2$. Then the (2,2)-entry $a\alpha^{iq}$ of $H_i$ is also an element of $K_l$ since $\alpha$ is included in $K$. So for $1 \le i \le q+1$, $a\alpha^{iq}$ runs over all elements of $K_l$. From $a^{q+1} + b^{q+1} = 0$, $b$ must be contained in $K_l$. Hence we must choose $c$ and $d$ from cosets $K_k$, $k \neq l$, to satisfy $\mathcal{H}_{a,b} \cap \mathcal{H}_{c,d} = \phi$.

**Theorem 2** *Let $q$ be an even prime power. If $a$ and $c$ belong to different cosets $K_k$ and $K_l$ respectively, then $\mathcal{H}_{a,b} \cup \mathcal{H}_{c,d}$ is a set of mutually $M$-intersecting varieties $\mathcal{V}(q^3+1, M)$, where $M \subseteq \{q^2+1, (q+1)^2\}$ and $|\mathcal{V}(q^3+1, M)| = 2(q+1)$.*

**Proof.** From Theorem 1, $\mathcal{H}_{a,b}$ and $\mathcal{H}_{c,d}$ are both $\mathcal{V}(q^3+1, q^2+1)$. So we have to consider the number of points in the intersection of $V(H_i)$ and $V(H'_j)$ for $H_i \in \mathcal{H}_{a,b}$ and $H'_j \in \mathcal{H}_{c,d}$. It is easily seen that $|V(H_i) \cap V(H'_j)| = |V(H) \cap V(H'_{j+k})|$ for some $k$ such that $U^{i+k} = I$. And we have $|V(H) \cap V(H'_j)| = |V(I) \cap V(P^T H'_j P^{(q)})|$, where $P$ is a non-singular matrix such that $P^t H P^{(q)} = I$. The characteristic polynomial $g(x)$ of $P^t H'_j P^{(q)}$ is $(x-1)(x^2+\delta x+1)$, where $\delta = (ac^q + bd^q)\alpha^{qi} + (a^q c + b^q d)\alpha^i$. The quadratic equation $x^2+\delta x+1 = 0$ has one solution over $\mathrm{GF}(q)$ if $\delta = 0$. Then we have $g(x) = (x-1)^3$ and $(P^t H_j P^{(q)} - xI)^2 \neq 0$. Hence the minimal polynomial $m(x)$ of $P^t H'_j P^{(q)}$ is $m(x) = (x-1)^3$. When the equation $x^2+\delta x+1 = 0$ has two solutions, $m(x) = g(x) = (x-1)(x-\beta)(x-\gamma)$, where $1 \neq \beta \neq \gamma \in \mathrm{GF}(q)$. When the equation has no solutions, $m(x) = g(x) = (x-1)(x^2+\delta x+1)$; that is, $x^2+\delta x+1$ is irreducible over $\mathrm{GF}(q)$. Therefore $V(P^t H'_j P^{(q)})$ and $V(I)$ intersect on $q^2+1$ points or $(q+1)^2$ points. ∎

In the proof of Theorem 2, if $\delta = 0$, the minimal polynomial $m(x)$ of $P^t H'_j P^{(q)}$ is $(x-1)^3$. When $a = b$ and $c = d$, we always obtain $\delta = 0$. Since $|V(H) \cap V(H'_j)| = q^2+1$ for $H_i \in \mathcal{H}_{a,b}$ and $H'_j \in \mathcal{H}_{c,d}$, we can show the next Corollary.

**Corollary 1** *Let $q$ be an even prime power. If $a = b$ and $c = d$ then $\mathcal{H}_{a,b} \cup \mathcal{H}_{c,d}$ is a set of mutually $M$-intersecting varieties $\mathcal{V}(q^3+1, q^2+1)$ consisting of $2(q+1)$ varieties.*

Finally we want to collect a set of Hermitian varieties $\mathcal{H}_{a,b}$ as many as possible by choosing the values of $a$ and $b$ of $H$.

**Theorem 3** *Let $q$ be an even prime power. There exists a set of mutually $M$-intersecting varieties $\mathcal{V}(q^3+1, q^2+1)$ consisting of $q^2-1$ varieties.*

**Proof.** Let $J = \{1, w, \ldots, w^{q-2}\}$ be a set of representatives of the cosets $K_k = Kw^k$, $0 \leq k \leq q-2$. Consider a set of varieties $\bigcup_{a \in J} \mathcal{H}_{a,a}$. If we choose $a, c \in J$, $a \neq c$, then $\mathcal{H}_{a,a} \cup \mathcal{H}_{c,c}$ is $\mathcal{V}(q^3+1, q^2+1)$ by Corollary 1. Hence $\bigcup_{a \in J} \mathcal{H}_{a,a}$ is $\mathcal{V}(q^3+1, q^2+1)$ consisting of $(q+1)(q-1)$ varieties. ∎

**Theorem 4** *Let $q$ be an even prime power. There exists a set of mutually M-intersecting varieties $\mathcal{V}(q^3+1, \{q^2+1, (q+1)^2\})$ consisting of $(q+1)^2(q-1)$ varieties.*

**Proof.** Let $J = \{1, w, \ldots, w^{q-2}\}$ be a set of representatives of the cosets $K_k$. Let $L = \{(a,b)\,;\, a^{q+1}+b^{q+1} = 0, a \in J, b \in \mathrm{GF}(q^2)\}$. Then $L$ consists of $(q-1)(q+1)$ elements and $\mathcal{H}_{a,b} \cap \mathcal{H}_{c,d} = \phi$ for $(a,b), (c,d) \in L$, $(a,b) \neq (c,d)$. Therefore $\bigcup_{(a,b)\in L} \mathcal{H}_{a,b}$ is $\mathcal{V}(q^3+1, \{q^2+1, (q+1)^2\})$ by Theorem 2. ∎

We remark that we can add $V(I)$ to $\mathcal{V}(\rho, M)$ in all theorems because we can show $|V(H_i) \cap V(I)| = q^2+1$ for any $V(H_i) \in \mathcal{H}$.

## References


[ 1 ] R.C. Bose and I.M. Chakravarti, *Hermitian Varieties in a Finite Projective Space $PG(N, q^2)$*, Can. J. Math. 17 (1966), 1161-1182.

[ 2 ] R. Fuji-Hara and N. Miyamoto, *Balanced Arrays from Quadratic Functions*, submitted to J.S.P.I.

[ 3 ] R. Fuji-Hara and N. Miyamoto, *A Construction of Combinatorial arrays from Non-linear Functions*, submitted to Utilitas Math.

[ 4 ] R. Fuji-Hara and N. Miyamoto, *Mutually M-intersecting Varieties*, Congressus Numerantium (to appear).

[ 5 ] J.W.P. Hirschfeld, *Projective Geometries over Finite Field*, Oxford University Press, New York (1979).

[ 6 ] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, New York (1985).

[ 7 ] B.C. Kestenband, *Projective geometries that are Disjoint Union Caps*, Can. J. Math. 32, No.6 (1980), 1299-1305.

[ 8 ] B.C. Kestenband, *Unital Intersections in Finite Projective Planes*, Geometriae Dedicata 11 (1981), 107-117.