LATTICES OF ALGEBRAIC CYCLES ON FERMAT VARIETIES IN POSITIVE CHARACTERISTICS

ICHIRO SHIMADA

Dedicated to Professor Tetsuji Shioda for his 60th birthday

Abstract. Let X be the Fermat hypersurface of dimension $2m$ and of degree $q+1$ defined over an algebraically closed field of characteristic $p>0$, where q is a power of p, and let $NL^m(X)$ be the free abelian group of numerical equivalence classes of linear subspaces of dimension m contained in X. By the intersection form, we regard $NL^m(X)$ as a lattice. Investigating the configuration of these linear subspaces, we show that the rank of $NL^m(X)$ is equal to the $2m$ th Betti number of X, that the intersection form multiplied by $(-1)^m$ is positive definite on the primitive part of $NL^m(X)$, and that the discriminant of $NL^m(X)$ is a power of p. Let $\mathcal{L}^m(X)$ be the primitive part of $NL^m(X)$ equipped with the intersection form multiplied by $(-1)^m$. In the case $p=q=2$, the lattice $\mathcal{L}^m(X)$ is described in terms of certain codes associated with the unitary geometry over $\mathbb{F}_2$. The lattice $\mathcal{L}^2(X)$ is isomorphic to the laminated lattice of rank 22. This explains Conway's identification $\cdot 222 \cong PSU(6,2)$ geometrically. The lattice $\mathcal{L}^3(X)$ is of discriminant $2^{16}\cdot 3$, minimal norm 8, and kissing number 109421928.

1. Introduction

Let p be a prime integer, and $q=p^\nu$ a power of p, where ν is a positive integer. Let X be the Fermat hypersurface of dimension $2m$ and of degree $q+1$ defined over an algebraically closed field $\bar{k}$ of characteristic $p>0$; that is, the hypersurface X in $\mathbb{P}^{2m+1}$ is defined by the homogeneous equation

$$x_0^{q+1}+\cdots+x_{2m+1}^{q+1}=0.$$

Let $\mathrm{CH}^m(X)$ be the Chow group of algebraic cycles on X with codimension m modulo the rational equivalence. We have the intersection form on $\mathrm{CH}^m(X)$, which is $\mathbb{Z}$-valued, bilinear and symmetric. We define $N^m(X)$ to be the quotient group of $\mathrm{CH}^m(X)$ by the numerical equivalence. Here an element α of $\mathrm{CH}^m(X)$ is said to be numerically equivalent to zero if $\alpha.\beta=0$ holds for any $\beta\in\mathrm{CH}^m(X)$. Tate [16] proved that X is supersingular; that is, each element of the middle cohomology group $H^{2m}(X,\mathbb{Q}_l)(m)$ of X is represented by an element of $\mathrm{CH}^m(X)\otimes_{\mathbb{Z}}\mathbb{Q}_l$. (See also Shioda and Katsura [15].) In particular, the numerical equivalence on $\mathrm{CH}^m(X)$ coincides with the homological equivalence, and $N^m(X)$ is embedded in $H^{2m}(X,\mathbb{Q}_l)(m)$. Moreover, because the intersection form is $\mathbb{Z}$-valued, the subgroup $N^m(X)$ of $H^{2m}(X,\mathbb{Q}_l)(m)$ is finitely generated, and its rank is equal to the $2m$ th Betti number $b_{2m}(X)$ of X.

1991 *Mathematics Subject Classification.* Primary 14C25, 11H31; Secondary 51D25.

Research partially supported by the Inamori Foundation.

On the other hand, the hypersurface X contains many linear subspaces of dimension m. The number of these linear subspaces is given by $\prod_{\nu=0}^{m}(q^{2\nu+1}+1)$ (cf. Corollary 2.22). Let $NL^m(X)$ be the subgroup of $N^m(X)$ generated by the numerical equivalence classes of these linear subspaces. Our first result is as follows.

Theorem 1.1. (1) *The rank of $NL^m(X)$ is equal to $b_{2m}(X)$.*

(2) *The signature of the intersection form on $NL^m(X)\otimes_{\mathbb{Z}}\mathbb{R}$ is $(1, b_{2m}(X)-1)$ when m is odd, while it is $(b_{2m}(X), 0)$ when m is even.*

(3) *The discriminant of the intersection form on $NL^m(X)$ is a power of p.*

This result not only gives a new proof to the supersingularity of X but also implies that $N^m(X)/NL^m(X)$ is at most a finite p-group. It is quite plausible that $N^m(X)$ actually coincides with $NL^m(X)$, but this conjecture is not yet verified. Shioda [13] studied the Néron-Severi group of a complex Fermat surface, and asked whether it is generated by the numerical equivalence classes of lines on the Fermat surface (cf. [13, Question 7.4]).

In $N^m(X)$, we have the numerical equivalence class h of the intersection of X with a general linear subspace of $\mathbb{P}^{2m+1}$ of dimension $m+1$. We define the primitive part $N^m_{\mathrm{prim}}(X)$ of $N^m(X)$ to be the orthogonal complement $(h)^{\perp}$ of h. The assertion (2) of Theorem 1.1 implies the following.

Corollary 1.2. *The intersection form multiplied by $(-1)^m$ is positive definite on $N^m_{\mathrm{prim}}(X)$.*

When X is a surface, this corollary follows from the Hodge index theorem, which is valid in any characteristics. Over the complex number field, the corresponding result follows immediately from the Hodge theory.

We put

$$\mathcal{L}^m(X) := (-1)^m(NL^m(X)\cap N^m_{\mathrm{prim}}(X)),$$

where the factor $(-1)^m$ means that the intersection form is multiplied by $(-1)^m$. Then $\mathcal{L}^m(X)$ is a positive definite lattice. Our second result describes the structure of this lattice when $p=q=2$.

Suppose that $p=q=2$. Let k be the finite field $\mathbb{F}_4$, and let T be the set of k-rational points of the projective space $\mathbb{P}^m$ defined over k. We identify the power set 2^T of T with the vector space $\mathbb{F}_2^T$ of $\mathbb{F}_2$-valued functions on T in such a way that a subset S of T corresponds to the function from T to $\mathbb{F}_2$ whose pre-image of $1\in\mathbb{F}_2$ is exactly S. Via this identification, an addition is defined on 2^T by the symmetric difference;

$$S_1+S_2 := (S_1\cup S_2)\setminus(S_1\cap S_2).$$

A square matrix $A=(a_{ij})$ of size $m+1$ with coefficients in k is said to be *Hermitian* if it satisfies ${}^tA=A^{(2)}$, where $A^{(2)} := (a_{ij}^2)$. For a Hermitian matrix A, let $Y_A(k)$ be the set of k-rational points of the subvariety Y_A of $\mathbb{P}^m$ defined by the homogeneous equation

$$\sum_{i,j=0}^{m} a_{ij}x_ix_j^2 = 0.$$

When A is the zero matrix O, we have $Y_O(k)=T$. Let R be the finite ring $\mathbb{Z}/(2^{m+1})$, and R^T the R-module of R-valued functions on T. For a subset S of T, we define $\overline{V}_S \in R^T$ to be the function given by

$$\overline{V}_S(H) := \begin{cases} 1 & \text{if } H \in S, \\ 0 & \text{if } H \in T \setminus S. \end{cases}$$

Let $\widetilde{T}$ be the disjoint union of T and $\{\varphi\}$, where φ is a formal element, and $R^{\widetilde{T}}$ the R-module of R-valued functions on $\widetilde{T}$. For a function $\bar{v} \in R^T$, we define its *extension* $\bar{v}^{\sim} \in R^{\widetilde{T}}$ to be the unique function from $\widetilde{T}$ to R that satisfies

$$\bar{v}^{\sim}|_T = \bar{v} \quad \text{and} \quad \bar{v}^{\sim}(\varphi) = \sum_{H \in T} \bar{v}(H).$$

For an R-submodule M of R^T, we define $M^{\sim}$ to be the set $\{\bar{v}^{\sim} : \bar{v} \in M\}$, which is obviously an R-submodule of $R^{\widetilde{T}}$ isomorphic to M as an R-module. Let $\mathbb{Z}^{\widetilde{T}}$ be the free abelian group of $\mathbb{Z}$-valued functions on $\widetilde{T}$. We equip $\mathbb{Z}^{\widetilde{T}}$ with a $\mathbb{Q}$-valued positive definite symmetric bilinear form defined by

$$(v, w)_T := \frac{1}{2^{m+1}} \Big(\sum_{H \in T} v(H)w(H) + 3\, v(\varphi)w(\varphi) \Big). \tag{1.1}$$

Definition 1.3. We define $\mathcal{H}_m$ to be the linear subspace of $\mathbb{F}_2^T$ generated by the subsets $Y_A(k)$ of T, where A runs through the set of all Hermitian matrices. Let $\overline{L}^m$ be the submodule of R^T generated by the vectors $\overline{V}_T$ and $2\,\overline{V}_S$, where S runs through $\mathcal{H}_m$. We define $\widetilde{L}^m$ to be the pull-back of the extension $(\overline{L}^m)^{\sim}$ of $\overline{L}^m$ by the natural homomorphism $\mathbb{Z}^{\widetilde{T}} \to R^{\widetilde{T}}$.

It turns out that the symmetric bilinear form $(\ ,\ )_T$ takes values in $\mathbb{Z}$ on $\widetilde{L}^m$, so that $\widetilde{L}^m$ becomes a lattice. Note that the rank $|T| + 1$ of $\widetilde{L}^m$ is equal to the rank $b_{2m}(X) - 1$ of $\mathcal{L}^m(X)$.

Theorem 1.4. *The lattice $\mathcal{L}^m(X)$ is isomorphic to $\widetilde{L}^m$.*

We will study the structure of $\mathcal{L}^m(X)$ in detail for $m \le 3$.

When $\dim X = 2$, the lattice $\mathcal{L}^1(X) \cong \widetilde{L}^1$ is easily seen to be isomorphic to the root lattice of type E_6. In other words, the primitive part of the Néron-Severi lattice of the cubic Fermat surface in characteristic 2 does not differ from that of a nonsingular cubic surface in characteristic 0, which has been studied for many years in the relation with the configuration of the twenty-seven lines on a cubic surface. (See Manin [10].)

Theorem 1.5. *Suppose that $\dim X = 4$. Then the lattice $\mathcal{L}^2(X)$ is isomorphic to the laminated lattice Λ_{22} of rank 22.*

See the book by Conway and Sloane [2, Chapter 6] for the definition of the laminated lattice Λ_{22}. This lattice is obtained as a section of the Leech lattice, and the subgroup $\cdot 222$ of the automorphism group $\cdot 0$ of the Leech lattice acts on Λ_{22} (cf. [2, Chapter 10]). In search for the explanation of Conway's identification $\cdot 222 \cong PSU_6(2)$ (cf. [2, Chapter 10, Table 10.4]), Edge [4] suggested that there should be some correspondence between the planes contained in the cubic Fermat 4-fold X in characteristic 2 and certain vectors in the Leech lattice, and presented some numerical evidences. Using this putative correspondence, Jónsson and McKay constructed an embedding of the Mathieu group M_{22} into $PSU_6(2)$ explicitly in [9].

In the course of the proof of Theorem 1.5, we construct an embedding of $\widetilde{L}^2$ into the Leech lattice. Combining this embedding with the isomorphism $\mathcal{L}^2(X) \cong \widetilde{L}^2$ in Theorem 1.4, we can make a correspondence between *pairs* of planes contained in X and certain vectors of the Leech lattice. This correspondence explains the numerical coincidences given by Edge [4].

Theorem 1.6. *Suppose that* $\dim X = 6$. *Then the lattice* $\mathcal{L}^3(X)$ *of rank* 86 *has discriminant* $2^{16} \cdot 3$, *minimal norm* 8, *and kissing number* 109421928.

Recall that the normalized center density of a positive definite lattice L is defined to be

$$(\operatorname{disc} L)^{-1/2} \cdot (N_{\min}/4)^{r/2},$$

where $\operatorname{disc} L$, $N_{\min}$ and r are the discriminant, the minimal norm and the rank of L, respectively. By Theorem 1.6, the normalized center density of $\mathcal{L}^3(X)$ is equal to $2^{35}/\sqrt{3} = 2^{34.2075\dots}$. The Minkowski-Hlawka theorem (cf. [2, Chapter 1]) says that there is a lattice of rank 86 with normalized center density at least

$$\zeta(86) \cdot 2^{-85} \cdot V_{86}^{-1} = 2^{19.3208\dots},$$

where ζ is the Riemann zeta function and V_{86} is the volume of the 86-dimensional unit ball. Thus the lattice $\mathcal{L}^3(X)$ gives us a new example of sphere packing whose center density exceeds the Minkowski-Hlawka bound (cf. [2, Chapter 1, Table 1.3]).

Computing the norms of geometrically natural generators of $\mathcal{L}^m(X)$ and looking at the results for $m \le 3$, we are led to a guess that the minimal norm of $\mathcal{L}^m(X)$ is 2^m for every m. Shioda [14] and, independently, Elkies [5, 6] obtained many lattices of high center density as Mordell-Weil lattices of elliptic surfaces in positive characteristics. The minimal norm of a Mordell-Weil lattice is easily calculated from geometric invariants of the elliptic surface (cf. [14, Section 2]). For our lattices, unfortunately, we do not know any geometric method for determining the minimal norm. The proof of Theorem 1.6 is carried out using a computer, and the computation becomes intractable when $m \ge 4$.

Theorems 1.1 and 1.4 are proved by looking at the configuration of m-dimensional linear subspaces contained in X. In order to study the configuration, we investigate the action of the projective automorphism group of X on the set of linear subspaces on X. Our new tool for carrying out this investigation is the notion of *p-quadric hypersurfaces* and *special linear subspaces* (cf. Definitions 2.1 and 2.11). The notion of p-quadric hypersurfaces has been introduced by Shimada in [12, Introduction] in the study of unirationality of complete intersections in positive characteristics. Some of the results about the configuration we prove in this paper have been obtained by Segre [11] in the context of Hermitian hypersurfaces over finite fields.

We give a brief outline of our paper. In Section 2, we prove elementary facts about p-quadric hypersurfaces, Hermitian hypersurfaces, and special linear subspaces. A nonsingular hypersurface of degree $q + 1$ is p-quadric if and only if it is projectively isomorphic to the Fermat hypersurface of the same degree (cf. Proposition 2.3), and any m-dimensional linear subspace contained in a nonsingular p-quadric hypersurface of dimension $2m$ is always a special linear subspace (cf. Corollary 2.17). Therefore we are allowed to replace the Fermat hypersurface by any nonsingular p-quadric hypersurface. In Section 3, we investigate the configuration of special linear subspaces on a nonsingular p-quadric hypersurface X_J of dimension $2m$ defined by the equation

$$\sum_{i=0}^{m}(x_i y_i^q - x_i^q y_i) = 0.$$

We show that, when $p = q = 2$, each m-dimensional linear subspace contained in X_J is labeled in a one-to-one way by a pair of a k-rational linear subspace of $\mathbb{P}^m$ and a Hermitian hypersurface on it (cf. Corollary 3.11). In Section 4, we prove Theorem 1.1 by writing down explicitly an embedding of $NL^m(X_J)$ into an $\mathbb{R}$-vector space of dimension $b_{2m}(X_J)$ equipped with a symmetric bilinear form of signature $(b_{2m}(X_J), 0)$ or $(1, b_{2m}(X_J)-1)$, according to the parity of m. In Section 5, we prove Theorem 1.4. Using the labeling obtained in Section 3, we assign to each generator of $\mathcal{L}^m(X_J)$ a vector of $\widetilde{L}^m$, and show that this assignment yields an isomorphism of lattices between $\mathcal{L}^m(X_J)$ and $\widetilde{L}^m$. In Section 6, we show that the linear code $\mathcal{H}_2$ of length 21 is related to a certain subcode of the Golay code $\mathcal{C}_{24}$, and construct an embedding of $\widetilde{L}^2$ into the Leech lattice, whose image is the laminated lattice Λ_{22}. This proves Theorem 1.5. In Section 7, we evaluate the discriminant, the minimal norm and the kissing number of the lattice $\widetilde{L}^3$. In the last section, we give a geometric explanation for the kissing number of $\widetilde{L}^m \cong \mathcal{L}^m(X)$ for $m = 1, 2, 3$, and present a conjectural formula of the kissing number of $\widetilde{L}^m$ for general m.

After the first version of this paper was finished, the author was informed that Dummigan and Tiep [3] have also considered the lattices $N^m_{\mathrm{prim}}(X)$ from a group-theoretic point of view using an idea of Gross [8].

Acknowledgment. Part of this work was done during the author's stay at the Max-Planck-Institute für Mathematik in Bonn from June to July in 1998. The author would like to thank the Max-Planck-Institute for giving him a stimulating research environment. He also would like to thank Professors Eiichi Bannai, Yoichi Miyaoka, Tetsuji Shioda and Tomohide Terasoma for many helpful discussions and comments.

Conventions.

(1) We fix a prime integer p and its power $q = p^\nu$, where ν is a positive integer. (From Section 5 onwards, we put $p = q = 2$.) Let k be the finite field $\mathbb{F}_{q^2}$, and $\bar{k}$ its algebraic closure.

(2) For an algebraic variety V defined over a field K, we denote by $V(K)$ the set of K-rational points of V.

(3) The homogeneous coordinates of a projective space $\mathbb{P}^n$ are expressed as a *column* vector ${}^t(x_0, \dots, x_n)$, so that the group $GL(n+1)$ of $(n+1) \times (n+1)$ invertible matrices acts on $\mathbb{P}^n$ from the left.

(4) We consider the empty set $\emptyset$ as a linear subspace of $\mathbb{P}^n$ with dimension -1, and understand that every subvariety of $\mathbb{P}^n$ contains $\emptyset$.

(5) Let $r = p^\mu$ be a power of p, where $\mu \in \mathbb{Z}$. For a matrix $\Gamma = (\gamma_{ij})$ with coefficients in $\bar{k}$, we denote by $\Gamma^{(r)}$ the matrix (γ_{ij}^r). Then we have $(\Gamma_1 \cdot \Gamma_2)^{(r)} = \Gamma_1^{(r)} \cdot \Gamma_2^{(r)}$. The transpose of a matrix Γ is denoted by ${}^t\Gamma$.

(6) For a set S, the cardinality of S is denoted by $|S|$. For an abelian group A, the A-module of A-valued functions on S is denoted by A^S. The power set 2^S is identified with $\mathbb{F}_2^S$ in such a way that the addition of subsets of S is defined by the

symmetric difference. The disjoint union of two disjoint sets S_1 and S_2 is written by $S_1 \sqcup S_2$.

2. Projective geometry of p-quadric hypersurfaces

Let n be a positive integer. We denote by $M(n+1, K)$ the set of square matrices of size $n+1$ with coefficients in a field K, where K is k or $\bar{k}$.

First we work over $\bar{k}$. We consider the projective space $\mathbb{P}^n$ of dimension n defined over $\bar{k}$ with homogeneous coordinates $x = {}^t(x_0, \dots, x_n)$. For a non-zero square matrix $A = (a_{ij}) \in M(n+1, \bar{k})$, we define a homogeneous polynomial f_A of $2n+2$ variables by

$$f_A(x, y) := {}^t x \cdot A \cdot y^{(q)} = \sum_{i,j=0}^{n} a_{ij} x_i y_j^q,$$

where $x = {}^t(x_0, \dots, x_n)$ and $y = {}^t(y_0, \dots, y_n)$. We denote by X_A the hypersurface of degree $q+1$ defined in $\mathbb{P}^n$ by the homogeneous equation

$$f_A(x, x) = 0.$$

When A is the identity matrix I, the hypersurface X_I is nothing but the Fermat hypersurface of degree $q+1$.

Definition 2.1. We say that a hypersurface of $\mathbb{P}^n$ is a *p-quadric hypersurface* if it is written as X_A by some non-zero matrix $A \in M(n+1, \bar{k})$.

Note that the definition of p-quadric hypersurfaces does not depend on the choice of homogeneous coordinates of $\mathbb{P}^n$, because we have $g^{-1}(X_A) = X_{A'}$ for any $g \in GL(n+1, \bar{k})$, where $A' = {}^t g A g^{(q)}$. We define an action ρ of the group $GL(n+1, \bar{k})$ on $M(n+1, \bar{k})$ from the left by

$$\rho(g^{-1})(A) := {}^t g A g^{(q)}, \tag{2.1}$$

so that $g(X_A) = X_{\rho(g)(A)}$ holds for any $g \in GL(n+1, \bar{k})$. The following lemma will be used frequently throughout this paper.

Lemma 2.2. *Let Z be a reduced irreducible locally closed subvariety of $GL(n+1, \bar{k})$, and let H be a connected reduced algebraic subgroup of $GL(n+1, \bar{k})$. Suppose that $\rho(h)(Z) \subseteq Z$ holds for any $h \in H$. If $\dim Z \leq \dim H$, then the action of $H(\bar{k})$ on the set $Z(\bar{k})$ by ρ is transitive.*

Proof. For a point $A \in Z(\bar{k})$, we define a morphism $\psi_A : H \to GL(n+1, \bar{k})$ by $\psi_A(h) := \rho(h)(A)$. Let ϵ be the dual number; $\epsilon^2 = 0$. Then we have

$$\psi_A(I + \epsilon a) - \psi_A(I) = -\epsilon\, {}^t a A$$

for all $a \in \mathrm{Lie}(H) \subseteq M(n+1, \bar{k})$ because $(I + \epsilon a)^{-1} = I - \epsilon a$ and $(I - \epsilon a)^{(q)} = I$. Since A is invertible, we see that ψ_A is an immersion locally at $I \in H$. On the other hand, the image of ψ_A is in Z by assumption. Hence $\dim Z \leq \dim H$ implies that $\dim Z = \dim H$, and that ψ_A is dominant onto Z. In particular, for any two points A and A' of $Z(\bar{k})$, we have $\mathrm{Im}\, \psi_A \cap \mathrm{Im}\, \psi_{A'} \neq \emptyset$, which means that there exist elements $h, h' \in H(\bar{k})$ such that $\rho(h)(A) = \rho(h')(A')$. Hence we have $\rho(h'^{-1} h)(A) = A'$. *q.e.d.*

Note that X_A is nonsingular if and only if $\det A \neq 0$. Applying Lemma 2.2 to $Z = GL(n+1, \bar{k})$ and $H = GL(n+1, \bar{k})$, we obtain the following proposition, which is a small part of the main result of Beauville [1].

Proposition 2.3. *A nonsingular hypersurface of degree $q+1$ is p-quadric if and only if it is projectively isomorphic over $\bar{k}$ to the Fermat hypersurface X_I of degree $q+1$.*

By virtue of this proposition, we are allowed to replace the Fermat hypersurface of degree $q+1$ by an arbitrary nonsingular p-quadric hypersurface in the proof of our main results.

Next we recall the definition of Hermitian hypersurfaces, which is a notion over the finite field k of q^2 elements.

Definition 2.4. Suppose that $\mathbb{P}^n$ is defined over the finite field k. A p-quadric hypersurface X_A is said to be *Hermitian* if ${}^tA = A^{(q)}$ holds. In this case, we have $A^{(q^2)} = A$, and hence X_A is defined over k. We define the rank of a Hermitian hypersurface X_A to be the rank of A. By abuse of language, we define a Hermitian hypersurface of rank 0 to be the whole projective space $\mathbb{P}^n$.

Let $H(n+1, r)$ be the set of matrices $A \in M(n+1, k)$ satisfying ${}^tA = A^{(q)}$ and $\operatorname{rank} A = r$. Note that, if $A \in H(n+1, r)$, then ${}^tgAg^{(q)}$ is also an element of $H(n+1, r)$ for any linear transformation $g \in GL(n+1, k)$ with coefficients in k. Hence the finite group $GL(n+1, k)$ acts on the set $H(n+1, r)$ by ρ. Let $GU(r, k)$ be the finite group $\{g \in GL(r, k) \,:\, {}^tgg^{(q)} = I\}$. We understand that $GL(0, k)$ and $GU(0, k)$ are the group of order 1. We have

$$|GL(r,k)| = \prod_{j=0}^{r-1}(q^{2r} - q^{2j}) \quad \text{and} \quad |GU(r,k)| = q^{(r-1)r/2} \cdot \prod_{j=1}^{r}(q^j - (-1)^j).$$

The following is due to Segre [11, n. 3].

Proposition 2.5. (1) *The action of $GL(n+1, k)$ on $H(n+1, r)$ by ρ is transitive for each r.*

(2) *The stabilizer subgroup of an element of $H(n+1, r)$ in $GL(n+1, k)$ is of order $|GU(r, k)| \cdot |GL(n+1-r, k)| \cdot q^{2r(n+1-r)}$.*

Proof. Suppose that $r \neq 0$. Let A be an element of $H(n+1, r)$. Then there exist vectors $v, w \in k^{n+1}$ such that $f_A(v, w) \neq 0$. Because the homomorphism $k \to \mathbb{F}_q$ of additive groups given by $z \mapsto z + z^q$ is surjective, there is a linear combination $u = \lambda v + \mu w$ ($\lambda, \mu \in k$) such that $f_A(u, u) \neq 0$. Because the homomorphism $N : k^\times \to \mathbb{F}_q^\times$ of multiplicative groups given by $z \mapsto z^{q+1}$ is also surjective, there is a multiplicative constant $\gamma \in k^\times$ such that $u_0 := \gamma u$ satisfies $f_A(u_0, u_0) = 1$. The k-rational linear subspace $(u_0)^\perp := \{x \in k^{n+1} \,:\, f_A(u_0, x) = f_A(x, u_0) = 0\}$ of k^{n+1} is of codimension 1, and the restriction of f_A to $(u_0)^\perp$ is of rank $r-1$. Hence the assertion (1) is proved by induction on n. The assertion (2) is obvious. *q.e.d.*

Let H_{n+1} be the set of matrices $A \in M(n+1, k)$ satisfying ${}^tA = A^{(q)}$. Then H_{n+1} carries a natural structure of the vector space over the subfield $\mathbb{F}_q$ of k such that $\dim_{\mathbb{F}_q} H_{n+1} = (n+1)^2$. The set of Hermitian hypersurfaces in $\mathbb{P}^n$ is then identified with $H_{n+1}/\mathbb{F}_q^\times$.

Corollary 2.6. (1) *The group $GL(n+1,k)$ acts on the set of Hermitian hypersurfaces of rank r transitively for each r.*

(2) *The number $h(n,r)$ of Hermitian hypersurfaces of rank r in $\mathbb{P}^n$ is*

$$\frac{1}{q-1}\cdot q^{(r-1)r/2}\cdot\prod_{j=1}^{r}\Big(\frac{q^{2(n+1-r)+2j}-1}{q^j-(-1)^j}\Big)$$

if $r>0$, while it is 1 if $r=0$.

We shall study the set $X_A(k)$ of k-rational points of a Hermitian hypersurface X_A. The following is also due to Segre [11, n. 30].

Proposition 2.7. *Suppose that X_A is a Hermitian hypersurface of rank r. Then $|X_A(k)|$ is equal to $F(n,r)$, where*

$$F(n,r):=\frac{q^{2n-2r+2}-1}{q^2-1}+q^{2n-2r+1}\cdot\Big(\frac{q^{2r}-1}{q^2-1}+\frac{(-q)^r-1}{q+1}\Big).$$

Proof. When $r=0$, we have $X_A(k)=\mathbb{P}^n(k)$, and hence the assertion holds obviously. Suppose that $r>0$. By Corollary 2.6, the hypersurface X_A is projectively isomorphic over k to the hypersurface defined by

$$x_0^{q+1}+\cdots+x_{r-1}^{q+1}=0,$$

which is a cone over the Fermat hypersurface Y of degree $q+1$ in $\mathbb{P}^{r-1}$ with vertex being a k-rational linear subspace of dimension $n-r$. Therefore we have

$$|X_A(k)|=|Y(k)|\cdot|\mathbb{A}^{n-r+1}(k)|+|\mathbb{P}^{n-r}(k)|,$$

where $\mathbb{A}^{n-r+1}$ is the affine space of dimension $n-r+1$ defined over k. The number of k-rational points of the Fermat hypersurface is classically known. We use Edge's argument (Edge [4]) to calculate $|Y(k)|$. Let $\nu(t)$ be the number of t-tuples $(\zeta_1,\dots,\zeta_t)$ of elements of $\mathbb{F}_q^\times$ satisfying $\zeta_1+\cdots+\zeta_t=0$, which is determined by the initial condition $\nu(0)=1$ and the recursive relation

$$q^{t-1}=\sum_{s=0}^{t}\binom{t}{s}\nu(s).$$

Because each fiber of the norm map $N: k^\times\to\mathbb{F}_q^\times$ consists of $q+1$ elements, we have

$$|Y(k)|=\frac{1}{q^2-1}\sum_{s=1}^{r}\binom{r}{s}(q+1)^s\nu(s)=\frac{1}{q}\Big(\frac{q^{2r}-1}{q^2-1}+\frac{(-q)^r-1}{q+1}\Big).$$

Thus we obtain the formula for $|X_A(k)|$. *q.e.d.*

Proposition 2.8. *Let X_A and X_B be two Hermitian hypersurfaces in $\mathbb{P}^n$. If $X_A(k)=X_B(k)$, then there is a non-zero scalar $\lambda\in\mathbb{F}_q^\times$ such that $A=\lambda B$. In other words, the Hermitian hypersurface is determined by the set of its k-rational points.*

Proof. Suppose that $n=1$. Using Proposition 2.7, we can check that $|X_A(k)|=|X_B(k)|$ implies $\operatorname{rank}A=\operatorname{rank}B$. In particular, the assertion is proved when $\operatorname{rank}A=0$. Suppose that A is of positive rank. By Corollary 2.6, the defining equation of X_A can be written as either $x_0^{q+1}=0$ or $x_0^{q+1}+x_1^{q+1}=0$, if we choose appropriate k-rational homogeneous coordinates ${}^t(x_0,x_1)$ of $\mathbb{P}^1$. It follows that $X_A(k)=X_A(\bar{k})$. (Note that the equation $x^{q+1}+1=0$ has $q+1$ distinct roots in the finite field k.) Hence we have $X_A(\bar{k}) = X_B(\bar{k})$. Therefore f_A and f_B are proportional over $\bar{k}$. Because A and B are Hermitian, this implies that A and B are proportional over $\mathbb{F}_q$. When $n \geq 2$, the restrictions of f_A and f_B to any k-rational linear subspace of k^{n+1} of dimension 2 are proportional over $\mathbb{F}_q$ by the above observation, whence so are A and B. *q.e.d.*

Next we introduce a notion of special linear subspaces of nonsingular p-quadric hypersurfaces. From now to the end of this section, we always assume that A is invertible, so that X_A is nonsingular. We will work over $\bar{k}$ unless otherwise stated.

Let a be a $\bar{k}$-rational point of a nonsingular p-quadric hypersurface X_A (not necessarily Hermitian). It is easy to see that the tangent space $T(a, X_A)$ to X_A at a is given by the linear equation $f_A(x, a) = 0$.

Definition 2.9. The *q-tangent space* $qT(a, X_A)$ to X_A at a is the reduced part of the subvariety defined by $f_A(a, x) = 0$. Because $f_A(a, x)$ is the q th power of the linear form $f_{{}^tA^{(1/q)}}(x, a^{(1/q^2)})$, the q-tangent space $qT(a, X_A)$ is a hyperplane for any a.

It is easy to check that the definition of the q-tangent space does not depend on the choice of homogeneous coordinates of $\mathbb{P}^n$; that is, we have

$$g(qT(a, X_A)) = qT(g(a), g(X_A)) = qT(g(a), X_{\rho(g)(A)})$$

for all $g \in GL(n+1, \bar{k})$.

Proposition 2.10. *Let L be a linear subspace of $\mathbb{P}^n$ contained in X_A, and let a be a $\bar{k}$-rational point of L. Then L is contained in $T(a, X_A) \cap qT(a, X_A)$.*

Proof. We choose homogeneous coordinates ${}^t(x_0, \dots, x_n)$ of $\mathbb{P}^n$ such that the point a is ${}^t(1, 0, \dots, 0)$. Let $\sum_{i,j=0}^n a_{ij} x_i x_j^q = 0$ be the defining equation of X_A. We have $a_{00} = 0$ because $a \in X_A(\bar{k})$. In terms of the affine coordinates $u_i := x_i/x_0$ $(i = 1, \dots, n)$, the defining equation of X_A is written as follows:

$$\sum_{i=1}^n a_{i0} u_i + \Big(\sum_{j=1}^n a_{0j}^{1/q} u_j\Big)^q + \sum_{i,j=1}^n a_{ij} u_i u_j^q = 0.$$

It is easy to see that $T(a, X_A)$ is defined by $\sum_{i=1}^n a_{i0} u_i = 0$, and that $qT(a, X_A)$ is defined by $\sum_{j=1}^n a_{0j}^{1/q} u_j = 0$. On the other hand, each of the homogeneous parts

$$\sum_{i=1}^n a_{i0} u_i, \quad (\sum_{j=1}^n a_{0j}^{1/q} u_j)^q \quad \text{and} \quad \sum_{i,j=1}^n a_{ij} u_i u_j^q$$

of the defining equation of X_A must vanish on L, because the linear subspace L is contained in X_A and contains the origin a. *q.e.d.*

Definition 2.11. A $\bar{k}$-rational point s of a nonsingular p-quadric hypersurface X_A is said to be *a special point* if $T(s, X_A) = qT(s, X_A)$ holds. A linear subspace L contained in X_A is said to be *a special linear subspace* of X_A if L is spanned by special points of X_A. We denote by $\Sigma^l(X_A)$ the set of special linear subspaces of X_A with dimension l. We consider the empty set $\emptyset$ as a special linear subspace of X_A so that $\Sigma^{-1}(X_A) = \{\emptyset\}$. (See Convention (4).) We denote by $\Sigma(X_A)$ the disjoint union of $\Sigma^l(X_A)$ for all $l \geq -1$, and define a structure of the poset on $\Sigma(X_A)$ by

$$L_1 \leq L_2 \Longleftrightarrow L_1 \subseteq L_2.$$

Remark again that the definition of special linear subspaces does not depend on the choice of homogeneous coordinates of $\mathbb{P}^n$. If $L \in \Sigma^l(X_A)$, then $g(L) \in \Sigma^l(X_{\rho(g)(A)})$ holds for any $g \in GL(n+1, \bar{k})$. The map $L \mapsto g(L)$ induces an isomorphism of posets between $\Sigma(X_A)$ and $\Sigma(X_{\rho(g)(A)})$. Hence, by Proposition 2.3, the isomorphism class of the poset $\Sigma(X_A)$ depends only on q and n, and is independent of the choice of the invertible matrix A.

Proposition 2.12. *Suppose that $\mathbb{P}^n$ is defined over k and that X_A is Hermitian. Then a linear subspace L contained in X_A is special if and only if L is k-rational.*

Proof. It is enough to prove the assertion when $\dim L = 0$. A $\bar{k}$-rational point a of X_A is special if and only if the two linear forms $f_A(x, a)$ and $f_{{}^tA^{(1/q)}}(x, a^{(1/q^2)})$ are linearly dependent. When ${}^tA = A^{(q)}$, this is equivalent to saying that $Aa^{(q)}$ and $Aa^{(1/q)}$ are linearly dependent. Because $\det A \neq 0$, this is equivalent to saying that a and $a^{(1/q^2)}$ are linearly dependent; that is, the point a is k-rational. *q.e.d.*

Remark 2.13. There is another characterization of special points of a nonsingular p-quadric hypersurface (not necessarily Hermitian). It is known that the dual hypersurface $X_A^\vee$ of X_A is again a nonsingular p-quadric hypersurface. Let $\delta : X_A \to X_A^\vee$ and $\delta^\vee : X_A^\vee \to X_A$ be the natural morphisms. Then a point $a \in X_A(\bar{k})$ is a special point if and only if $\delta^\vee(\delta(a)) = a$.

If X_A is Hermitian and s is a k-rational point of X_A, then the hyperplane $T(s, X_A)$ is also k-rational. Using this, we get the following.

Corollary 2.14. *Let X_A be a nonsingular p-quadric hypersurface.*
(1) *If $L_1, L_2 \in \Sigma(X_A)$, then $L_1 \cap L_2 \in \Sigma(X_A)$.*
(2) *If $L \in \Sigma(X_A)$ and $s \in \Sigma^0(X_A)$, then $L \cap T(s, X_A) \in \Sigma(X_A)$.*
(3) *If $L \in \Sigma^l(X_A)$, then the number of special points of X_A contained in L is $(q^{2(l+1)} - 1)/(q^2 - 1)$. In particular, if $L_1, L_2 \in \Sigma(X_A)$ and $L_1 \setminus (L_2 \cap L_1) \neq \emptyset$, then there is at least one special point of X_A on $L_1 \setminus (L_2 \cap L_1)$.*

The assertion (1) of Corollary 2.14 implies that any two elements L_1 and L_2 of the poset $\Sigma(X_A)$ have the greatest common lower bound

$$L_1 \wedge L_2 := L_1 \cap L_2.$$

Proposition 2.15. *Let L_0 be the linear subspace of dimension $l \geq 0$ defined by $x_{l+1} = \cdots = x_n = 0$, and let X_A be a nonsingular p-quadric hypersurface associated with a matrix*

$$A := \left(\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right),$$

where A_{11} is a square matrix of size $l+1$. Then X_A contains L_0 as a special linear subspace if and only if the following hold:

- (i) *the submatrix A_{11} is the zero matrix, and*
- (ii) *there is an invertible square matrix Γ of size $l+1$ such that $A_{12} = \Gamma\, {}^tA_{21}^{(q)}$.*

Proof. The condition (i) is equivalent to saying that $L_0 \subset X_A$. We assume that L_0 is contained in X_A. If $a = {}^t(a_0, \ldots, a_l, 0, \ldots, 0)$ is a $\bar{k}$-rational point of L_0, then $T(a, X_A)$ is defined by the linear equation

$$(x_{l+1}, \ldots, x_n) \cdot A_{21} \cdot a' = 0,$$

and $qT(a, X_A)$ is defined by by the linear equation

$$(x_{l+1}, \dots, x_n) \cdot {}^tA_{12}^{(1/q)} \cdot a'^{(1/q)} = 0,$$

where $a' = {}^t(a_0, \dots, a_l)$. Suppose that L_0 is special with respect to X_A. Then there are special points $s_0, \dots, s_l$ of X_A spanning L_0. Let s'_i be the vector of the first $l+1$ components of s_i. Then $A_{21}s'_i$ and ${}^tA_{12}^{(1/q)} s'^{(1/q)}_i$ are linearly dependent, and hence there is $\lambda_i \in \bar{k}^\times$ such that $\lambda_i A_{21} s'_i = {}^tA_{12}^{(1/q)} s'^{(1/q)}_i$. Because the points s_i span L_0, the square matrix $\sigma := (s'_0, \dots, s'_l)$ of size $l+1$ is invertible. Let Λ be the diagonal matrix with diagonal entries $\lambda_0, \dots, \lambda_l$. Then we have $A_{12} = \Gamma\, {}^tA_{21}^{(q)}$, where $\Gamma = {}^t(\sigma^{(q)}\Lambda^{(q)}\sigma^{-1})$. Conversely, suppose that $A_{12} = \Gamma\, {}^tA_{21}^{(q)}$ holds for some $\Gamma \in GL(l+1, \bar{k})$. By the same argument as in the proof of Lemma 2.2, we can prove that the action of $GL(l+1, \bar{k})$ on itself given by $(\gamma, \beta) \mapsto {}^t(\gamma^{(q)}\beta\gamma^{-1})$ is transitive. In particular, the morphism $GL(l+1, \bar{k}) \to GL(l+1, \bar{k})$ given by $\gamma \mapsto {}^t(\gamma^{(q)}\gamma^{-1})$ is surjective. Hence there is an invertible matrix $\sigma = (s'_0, \dots, s'_l)$ such that $\Gamma = {}^t(\sigma^{(q)}\sigma^{-1})$. Then we have ${}^tA_{12}^{(1/q)}\sigma^{(1/q)} = A_{21}\sigma$, which means that the $\bar{k}$-rational points s_i of L_0 whose first $l+1$ coordinates form the $(i+1)$ th column vector s'_i of σ are special points of X_A. Because $\det \sigma \neq 0$, these points span L_0. Therefore L_0 is a special linear subspace of X_A. *q.e.d.*

Corollary 2.16.

$$\Sigma^l(X_A) \neq \emptyset \iff -1 \leq l \leq (n-1)/2.$$

If $\dim X_A = 2m$ and $l = m$, then $\det A \neq 0$ and $A_{11} = O$ imply $\det A_{12} \neq 0$ and $\det A_{21} \neq 0$. Hence we obtain the following.

Corollary 2.17. *Suppose that a nonsingular p-quadric hypersurface X_A is of dimension $2m$. Then any linear subspace contained in X_A of dimension m is special with respect to X_A.*

Corollary 2.18. *Every m-dimensional linear subspace contained in the Fermat hypersurface of degree $q+1$ and of dimension $2m$ is k-rational.*

Next we investigate the action of an automorphism group of X_A on the poset $\Sigma(X_A)$. We put

$$G_A := \{\, g \in GL(n+1, \bar{k}) \;:\; \rho(g)(A) = A \,\}.$$

If $g \in G_I$, then $g^{(q^2)} = g$ holds, and hence g is contained in $GL(n+1, k)$. Therefore G_I coincides with the group $GU(n+1, k)$. Then it follows from Proposition 2.3 that, for any $A \in GL(n+1, \bar{k})$, the group G_A is conjugate to $GU(n+1, k)$ in $GL(n+1, \bar{k})$. The group G_A acts on X_A projectively, and hence G_A acts on the poset $\Sigma(X_A)$.

Proposition 2.19. *The action of G_A on $\Sigma^l(X_A)$ is transitive for each l.*

Proof. Let L_0 be the linear subspace of dimension l defined in the statement of Proposition 2.15. We put

$$Z_0 := \{\, A' \in GL(n+1, \bar{k}) \;:\; L_0 \in \Sigma^l(X_{A'}) \,\},$$
$$H_0 := \{\, g \in GL(n+1, \bar{k}) \;:\; g(L_0) = L_0 \,\}.$$

By definition, the group H_0 acts on Z_0 by ρ. Proposition 2.15 implies that Z_0 is irreducible, and that

$$\dim Z_0 = (l+1)(n-l) + (l+1)^2 + (n-l)^2 = \dim H_0.$$

By Lemma 2.2, the action of $H_0(\bar{k})$ on the set $Z_0(\bar{k})$ is transitive. Suppose that two elements L_1 and L_2 of $\Sigma^l(X_A)$ are given. There are elements $g_1, g_2 \in GL(n+1, \bar{k})$ such that $g_1(L_1) = L_0$ and $g_2(L_2) = L_0$. Then both of $\rho(g_1)(A)$ and $\rho(g_2)(A)$ are in $Z_0(\bar{k})$, and hence there is an element $h \in H_0(\bar{k})$ such that $\rho(h)\rho(g_1)(A) = \rho(g_2)(A)$. Then we have $g_2^{-1}hg_1 \in G_A$. Thus we obtain an element $g_2^{-1}hg_1$ of G_A which satisfies $g_2^{-1}hg_1(L_1) = L_2$. *q.e.d.*

Using Proposition 2.12, we can also deduce Proposition 2.19 from Segre's result [11, n. 50].

Next we consider the projection from a special point of a nonsingular p-quadric hypersurface, which enables us to investigate the structure of the poset $\Sigma(X_A)$ by means of induction on $\dim X_A$.

Let s be a special point of X_A. For simplicity, we denote by T_s the hyperplane $T(s, X_A) = qT(s, X_A)$, and by $\mathbb{P}T_s$ the projective space of lines in T_s passing through s. Then we have the projection $T_s \setminus \{s\} \to \mathbb{P}T_s$ with the center s. We put $\widetilde{X}_A[s] := (X_A \cap T_s) \setminus \{s\}$.

Proposition 2.20. *Suppose that* $\dim X_A \geq 2$.

(1) *There is a nonsingular p-quadric hypersurface* $X_A[s]$ *of dimension* $\dim X_A - 2$ *in* $\mathbb{P}T_s$ *such that* $X_A \cap T_s$ *is the cone over* $X_A[s]$ *with the vertex* s.

(2) *Let* $\phi_s : \widetilde{X}_A[s] \to X_A[s]$ *be the projection with the center* s*, every fiber of which is isomorphic to an affine line. If* L *is a special linear subspace of* X_A*, then the image of* $L \cap \widetilde{X}_A[s]$ *by* ϕ_s *is a special linear subspace of* $X_A[s]$.

(3) *If* L' *is a special linear subspace of* $X_A[s]$*, then the union of* $\phi_s^{-1}(L')$ *and* $\{s\}$ *is a special linear subspace of* X_A *passing through* s.

Proof. By Proposition 2.3, we may assume that X_A is a Hermitian hypersurface defined by the equation

$$x_0^q x_1 + x_0 x_1^q + x_2^{q+1} + \cdots + x_n^{q+1} = 0,$$

and by Proposition 2.19, we may assume that s is the k-rational point ${}^t(1, 0, \ldots, 0)$. Let $u_i := x_i/x_0$ $(i = 1, \ldots, n)$ be the affine coordinates of $\mathbb{P}^n$ with the origin s. Then X_A is defined by $u_1 + u_1^q + u_2^{q+1} + \cdots + u_n^{q+1} = 0$, and T_s is defined by $u_1 = 0$. We can consider ${}^t(u_2, \ldots, u_n)$ as homogeneous coordinates of $\mathbb{P}T_s$. Then $X_A \cap T_s$ is the cone over a hypersurface of $\mathbb{P}T_s$ defined by

$$u_2^{q+1} + \cdots + u_n^{q+1} = 0,$$

which is nonsingular and Hermitian. We write this hypersurface in $\mathbb{P}T_s$ by $X_A[s]$. The projection from $T_s \setminus \{s\}$ to $\mathbb{P}T_s$ with the center s is given by

$${}^t(1, 0, a_2, \ldots, a_n) \mapsto {}^t(a_2, \ldots, a_n),$$

which is obviously defined over k. Hence, by Proposition 2.12 and Corollary 2.14, we see that ϕ_s satisfies (2) and (3). (Note that $\phi_s(\emptyset) = \emptyset \in \Sigma^{-1}(X_A[s])$, and that $\phi_s^{-1}(\emptyset) \cup \{s\} = \{s\} \in \Sigma^0(X_A)$.) *q.e.d.*

For a special point s of X_A, we denote by $\Sigma(X_A; \geq s)$ the subset of $\Sigma(X_A)$ consisting of elements L such that $s \in L$. We can define maps

$$\Phi_s : \Sigma(X_A) \to \Sigma(X_A[s]) \quad \text{and} \quad \Psi_s : \Sigma(X_A[s]) \to \Sigma(X_A; \geq s)$$

by

$$\Phi_s(L) := \phi_s(L \cap \widetilde{X}_A[s]) \quad \text{and} \quad \Psi_s(L') := \phi_s^{-1}(L') \cup \{s\}.$$

Note that $s \in L \in \Sigma(X_A)$ implies $L \subset T_s$ by Proposition 2.10. We can easily prove the following from the definitions.

Corollary 2.21. (1) *If $L \in \Sigma(X_A)$ and $L' \in \Sigma(X_A[s])$, then*

$$\dim \Phi_s(\, L\,) = \begin{cases} \dim L & \text{if } L \subset T_s \text{ and } s \notin L, \\ \dim L - 1 & \text{otherwise,} \end{cases}$$

and

$$\dim \Psi_s(L') = \dim L' + 1.$$

(2) *The two maps Φ_s and Ψ_s yield an isomorphism of posets between $\Sigma(X_A; \geq s)$ and $\Sigma(X_A[s])$ which shifts the dimension by* 1.

(3) *Suppose that $s \in L$. Then $\Phi_s(L) \wedge \Phi_s(L') = \Phi_s(L \wedge L')$ holds for any $L' \in \Sigma(X_A)$. In particular, if $s \in L$ and $s \notin L'$, then*

$$\dim(\Phi_s(L) \wedge \Phi_s(L')) = \dim(L \wedge L').$$

Using Corollaries 2.14 (3) and 2.21 (2), we have

$$|\Sigma^l(X_A)| = \frac{|\Sigma^0(X_A)| \cdot |\Sigma^{l-1}(X_A[s])|}{(q^{2l+2} - 1)/(q^2 - 1)}.$$

On the other hand, we have $|\Sigma^0(X_A)| = F(n, n+1)$ by Propositions 2.7 and 2.12. Combining these formulas, we can calculate $|\Sigma^l(X_A)|$ by induction on $\dim X_A$ and l. This result corresponds, via Proposition 2.12, to Segre's formula [11, n. 32] on the number of k-rational linear subspaces on a nonsingular Hermitian hypersurface. In particular, we obtain the following neat formula.

Corollary 2.22. *If $\dim X_A = 2m$, then $|\Sigma^m(X_A)| = \prod_{\nu=0}^{m}(q^{2\nu+1} + 1)$.*

3. Configuration of special linear subspaces

From now to the end of the paper, we assume that the dimension $n - 1$ of the p-quadric hypersurfaces is even. We put $n := 2m + 1$ where $m > 0$, and consider the configuration of m-dimensional linear subspaces contained in a nonsingular p-quadric hypersurface X_A of dimension $2m$. Recall that every linear subspace of dimension m contained in X_A is special with respect to X_A (cf. Corollary 2.17).

Suppose that X_A is nonsingular. For $H \in \Sigma^{m-1}(X_A)$, we put

$$B_A(H) := \{\, \Pi \in \Sigma^m(X_A) \;:\; \Pi > H \,\};$$

that is, the set $B_A(H)$ consists of $\Pi \in \Sigma^m(X_A)$ that contains H.

Proposition 3.1. (1) *The set $B_A(H)$ consists of $q + 1$ elements for every $H \in \Sigma^{m-1}(X_A)$.*

(2) *For any couple of $\Pi \in \Sigma^m(X_A)$ and $H \in \Sigma^{m-1}(X_A)$, there is a unique element $\beta_A(H, \Pi)$ of $B_A(H)$ such that, for any $\Pi' \in B_A(H)$, the following holds*:

$$\dim(\Pi' \wedge \Pi) = \begin{cases} \dim(H \wedge \Pi) & \text{if } \Pi' \neq \beta_A(H, \Pi), \\ \dim(H \wedge \Pi) + 1 & \text{if } \Pi' = \beta_A(H, \Pi). \end{cases} \tag{3.1}$$

(3) *For each $H \in \Sigma^{m-1}(X_A)$, there is a linear subspace P_H of $\mathbb{P}^{2m+1}$ with $\dim P_H = m + 1$ such that $P_H \cap X_A$ is the union of the $q + 1$ elements of $B_A(H)$.*

Proof. We proceed by induction on m. Suppose that $m = 1$. Then H is a special point s of X_A. Hence $X_A \cap T_s$ is a union of distinct $q+1$ lines passing through s by Proposition 2.20 (1), and the set $B_A(s)$ consists of these lines by Proposition 2.10. Therefore we can take T_s as P_s. Let Π be an arbitrary line on X_A. If Π is contained in T_s, then Π is an element of $B_A(s)$ and hence, with $\beta_A(s, \Pi) = \Pi$, the formula (3.1) holds. If Π is not contained in T_s, then the intersection $T_s \cap \Pi$ of a line and a plane consists of a single point t, which is not s because of Proposition 2.10. There exists exactly one line among $B_A(s)$ that passes through t. Then, with $\beta_A(s, \Pi)$ being this line, the formula (3.1) holds. Suppose that $m > 1$. We choose a special point s of X_A that is on H and make the projection $\widetilde{X}_A[s] \to X_A[s]$ defined in the previous section. We denote $X_A[s]$ by $X_{A'}$, where A' is a certain matrix in $GL(2m, \bar{k})$. Note that $\Phi_s(H)$ is an element of $\Sigma^{m-2}(X_{A'})$. By Corollary 2.21 (2), the map Φ_s induces a bijection

$$B_A(H) \cong B_{A'}(\Phi_s(H)). \tag{3.2}$$

Using the induction hypothesis, we obtain $|B_A(H)| = q+1$. For P_H, we can choose the closure of the pull-back of $P_{\Phi_s(H)} \subset \mathbb{P}T_s$ by the projection $T_s \setminus \{s\} \to \mathbb{P}T_s$ with the center s. Let Π be an arbitrary element of $\Sigma^m(X_A)$. If Π contains H, then we have $\Pi \in B_A(H)$, and (3.1) holds if we put $\beta_A(H, \Pi) = \Pi$. Suppose that Π does not contain H. We can choose the special point s from $H \setminus (H \cap \Pi)$ by virtue of Corollary 2.14 (3). Then we have $\Phi_s(\Pi) \in \Sigma^{m-1}(X_{A'})$ by Corollary 2.21 (1). Moreover we have

$$\dim(H \wedge \Pi) = \dim(\Phi_s(H) \wedge \Phi_s(\Pi)) \quad \text{and} \quad \dim(\Pi' \wedge \Pi) = \dim(\Phi_s(\Pi') \wedge \Phi_s(\Pi))$$

for any $\Pi' \in B_A(H)$ by Corollary 2.21 (3). The element $\beta_{A'}(\Phi_s(H), \Phi_s(\Pi))$ is given uniquely by the induction hypothesis. We set $\beta_A(H, \Pi)$ to be the unique element of $B_A(H)$ that corresponds to $\beta_{A'}(\Phi_s(H), \Phi_s(\Pi))$ by the bijection (3.2). Then (3.1) holds. *q.e.d.*

Corollary 3.2. *Let* Π_0, Π_1 *and* Π_2 *be mutually distinct elements of* $\Sigma^m(X_A)$ *such that* $\dim(\Pi_0 \wedge \Pi_1) = \dim(\Pi_0 \wedge \Pi_2) = m-1$. *Then*

$$\dim(\Pi_1 \wedge \Pi_2) = \begin{cases} m-2 & \textit{if } \Pi_0 \wedge \Pi_1 \neq \Pi_0 \wedge \Pi_2, \\ m-1 & \textit{if } \Pi_0 \wedge \Pi_1 = \Pi_0 \wedge \Pi_2. \end{cases}$$

Proof. It is obvious that $\dim(\Pi_1 \wedge \Pi_2) = m-1$ if $\Pi_0 \wedge \Pi_1 = \Pi_0 \wedge \Pi_2$. Suppose that $\Pi_0 \wedge \Pi_1 \neq \Pi_0 \wedge \Pi_2$. We put $H_1 := \Pi_0 \wedge \Pi_1$ and $H_2 := \Pi_0 \wedge \Pi_2$, both of which are hyperplanes of Π_0. Note that Π_0 and Π_1 are distinct elements of $B_A(H_1)$. Since $\Pi_0 \wedge \Pi_1 \neq \Pi_0 \wedge \Pi_2$, we have $\dim(H_1 \wedge \Pi_2) = \dim(H_1 \wedge H_2) = m-2$ and hence $\dim(\Pi_0 \wedge \Pi_2) = \dim(H_1 \wedge \Pi_2) + 1$. The uniqueness of $\beta_A(H_1, \Pi_2)$ implies that $\beta_A(H_1, \Pi_2) = \Pi_0$. Since $\Pi_1 \neq \Pi_0$, we have $\dim(\Pi_1 \wedge \Pi_2) = \dim(H_1 \wedge \Pi_2) = m-2$. *q.e.d.*

Recall that $h \in N^m(X_A)$ is the numerical equivalence class of the intersection of X_A with a general linear subspace of dimension $m+1$ in $\mathbb{P}^{2m+1}$. For $\Pi \in \Sigma^m(X_A)$, let $[\Pi] \in N^m(X_A)$ denote the numerical equivalence class of Π. From Proposition 3.1 (3), we obtain the following.

Corollary 3.3. *For any* $H \in \Sigma^{m-1}(X_A)$, *the numerical equivalence class* h *is equal to the sum of* $[\Pi]$, *where* Π *runs through the set* $B_A(H)$.

We choose homogeneous coordinates ${}^t(x_0, \dots, x_m, y_0, \dots, y_m)$ of $\mathbb{P}^{2m+1}$ defined over k, and put

$$M_0 := \{\, y_0 = \dots = y_m = 0 \,\} \quad \text{and} \quad M_\infty := \{\, x_0 = \dots = x_m = 0 \,\}.$$

We also put

$$J := \left(\begin{array}{c|c} O & I_{m+1} \\ \hline -I_{m+1} & O \end{array} \right).$$

Then the hypersurface X_J defined by the homogeneous equation

$$\sum_{i=0}^{m} (x_i y_i^q - x_i^q y_i) = 0$$

is a nonsingular Hermitian hypersurface containing M_0 and M_∞.

Remark 3.4. Using Lemma 2.2, we can prove the following. Suppose that a pair (Π_0, Π_∞) of elements of $\Sigma^m(X_A)$ such that $\Pi_0 \wedge \Pi_\infty = \emptyset$ is given, where A is an element of $GL(2m+2, \bar{k})$. Then there is a linear transformation $g \in GL(2m+2, \bar{k})$ such that $g(X_A) = X_J$, $g(\Pi_0) = M_0$ and $g(\Pi_\infty) = M_\infty$.

We define a subgroup $G_J^{0\infty}$ of $G_J = \{g \in GL(2m+2, \bar{k}) \;:\; \rho(g)(J) = J\}$ by

$$G_J^{0\infty} := \{\, g \in G_J \;:\; g(M_0) = M_0,\; g(M_\infty) = M_\infty \,\},$$

which acts on the triple (X_J, M_0, M_∞) projectively.

Proposition 3.5. *In terms of the coordinates ${}^t(x_0, \dots, x_m, y_0, \dots, y_m)$, the group $G_J^{0\infty}$ is expressed as follows*:

$$G_J^{0\infty} = \left\{ \left(\begin{array}{c|c} \gamma & O \\ \hline O & ({}^t\gamma^{-1})^{(q)} \end{array} \right) \;:\; \gamma \in GL(m+1, k) \right\}.$$

Proof. We decompose $g \in GL(2m+2, \bar{k})$ as follows:

$$g = \left(\begin{array}{c|c} g_{11} & g_{12} \\ \hline g_{21} & g_{22} \end{array} \right),$$

where g_{ij} are square matrices of size $m+1$. Then $g(M_0) = M_0$ and $g(M_\infty) = M_\infty$ hold if and only if $g_{12} = g_{21} = O$. Suppose that $g_{12} = g_{21} = O$. Then g is contained in G_J if and only if ${}^t g_{11} g_{22}^{(q)} = {}^t g_{22} g_{11}^{(q)} = I_{m+1}$ holds, which is equivalent to $g_{22} = ({}^t g_{11}^{-1})^{(q)}$ and $g_{11}^{(q^2)} = g_{11}$. The latter holds if and only if $g_{11} \in GL(m+1, k)$. *q.e.d.*

We fix an identification

$$G_J^{0\infty} \cong GL(m+1, k) \tag{3.3}$$

given by

$$\left(\begin{array}{c|c} \gamma & O \\ \hline O & ({}^t\gamma^{-1})^{(q)} \end{array} \right) \mapsto \gamma.$$

Then the action of $G_J^{0\infty}$ on the projective space M_0 factors through this isomorphism; that is, the group $G_J^{0\infty}$ acts on M_0 over k as the full linear transformation group.

Let a and b be integers such that $-1 \le a, b \le m$. We put

$$\Sigma^m(X_J)^{(a,b)} := \{\, \Pi \in \Sigma^m(X_J) \;:\; \dim(\Pi \wedge M_0) = a,\; \dim(\Pi \wedge M_\infty) = b \,\}.$$

Because $M_0 \wedge M_\infty = \emptyset$, this set $\Sigma^m(X_J)^{(a,b)}$ is empty when $a+b > m-1$. Suppose that $a+b \le m-1$. We define a linear subspace $M_1^{(a,b)}$ of dimension m in $\mathbb{P}^{2m+1}$ by the equations

$$x_\lambda = 0 \quad (a+1 \le \lambda \le a+b+1), \qquad y_\mu = 0 \quad (0 \le \mu \le a), \quad \text{and}$$
$$x_\nu - y_\nu = 0 \quad (a+b+2 \le \nu \le m).$$

For example, we have $M_1^{(-1,m)} = M_\infty$ and $M_1^{(m,-1)} = M_0$. The linear subspace $M_1^{(a,b)}$ is contained in $\Sigma^m(X_J)^{(a,b)}$, and hence $\Sigma^m(X_J)^{(a,b)}$ is non-empty if and only if $a+b \le m-1$. Note that $G_J^{0\infty}$ acts on the set $\Sigma^m(X_J)^{(a,b)}$.

Proposition 3.6. (1) *For each (a,b), the action of $G_J^{0\infty}$ on $\Sigma^m(X_J)^{(a,b)}$ is transitive.*

(2) *We put $c := m-1-a-b$. The number $|\Sigma^m(X_J)^{(a,b)}|$ is equal to*

$$|GL(m+1,k)| \,/\, (\,|GU(c,k)| \cdot |GL(a+1,k)| \cdot |GL(b+1,k)| \cdot q^{2n(a,b)}\,),$$

where $n(a,b) := (a+1)(b+1) + c(a+b+2)$. Here we understand that $|GU(0,k)| = |GL(0,k)| = 1$.

Proof. We decompose matrices $g \in GL(2m+2,\bar{k})$ and $A \in GL(2m+2,\bar{k})$ as follows:

$$g = \left[\begin{array}{c|c} \begin{array}{c|c|c} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \hline \gamma_{21} & \gamma_{22} & \gamma_{23} \\ \hline \gamma_{31} & \gamma_{32} & \gamma_{33} \end{array} & g_{12} \\ \hline g_{21} & \begin{array}{c|c|c} \gamma'_{11} & \gamma'_{12} & \gamma'_{13} \\ \hline \gamma'_{21} & \gamma'_{22} & \gamma'_{23} \\ \hline \gamma'_{31} & \gamma'_{32} & \gamma'_{33} \end{array} \end{array}\right]$$

and

$$A = \left[\begin{array}{c|c} A_{11} & \begin{array}{c|c|c} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \hline \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \hline \alpha_{31} & \alpha_{32} & \alpha_{33} \end{array} \\ \hline \begin{array}{c|c|c} \alpha'_{11} & \alpha'_{12} & \alpha'_{13} \\ \hline \alpha'_{21} & \alpha'_{22} & \alpha'_{23} \\ \hline \alpha'_{31} & \alpha'_{32} & \alpha'_{33} \end{array} & A_{22} \end{array}\right].$$

Here g_{ij} and A_{ij} are square matrices of size $m+1$, and $\gamma_{\mu\nu}$, $\gamma'_{\mu\nu}$, $\alpha_{\mu\nu}$, and $\alpha'_{\mu\nu}$ are matrices of shape $s(\mu) \times s(\nu)$, where $s(1) := a+1$, $s(2) := b+1$ and $s(3) := c$. We define a subgroup $H^{(a,b)}$ of $GL(2m+2,\bar{k})$ and a closed subvariety $Z^{(a,b)}$ of $GL(2m+2,\bar{k})$ as follows:

$$H^{(a,b)} := \{\, g \in GL(2m+2,\bar{k}) \;:\; g(M_0) = M_0,\ g(M_\infty) = M_\infty,\ g(M_1^{(a,b)}) = M_1^{(a,b)} \,\},$$
$$Z^{(a,b)} := \{\, A \in GL(2m+2,\bar{k}) \;:\; M_0 \cup M_\infty \cup M_1^{(a,b)} \subset X_A \,\}.$$

By definition, the group $H^{(a,b)}$ acts on $Z^{(a,b)}$ by ρ. It is easy to see that

$g \in H^{(a,b)} \iff g_{12},\ g_{21},\ \gamma'_{12},\ \gamma_{21},\ \gamma'_{32},\ \gamma_{23},\ \gamma'_{13},\ \gamma_{31}$ are zero matrices, and $\gamma_{33} = \gamma'_{33}$,

$A \in Z^{(a,b)} \iff A_{11},\ A_{22},\ \alpha'_{21},\ \alpha_{12},\ \alpha'_{23},\ \alpha_{32},\ \alpha'_{31},\ \alpha_{13}$ and $\alpha_{33} + \alpha'_{33}$ are zero matrices.

This implies that both of $H^{(a,b)}$ and $Z^{(a,b)}$ are irreducible, and that $\dim H^{(a,b)}$ is equal to $\dim Z^{(a,b)}$. By Lemma 2.2, the action of $H^{(a,b)}(\bar{k})$ on the set $Z^{(a,b)}(\bar{k})$ is transitive. Let Π be an arbitrary element of $\Sigma^m(X_J)^{(a,b)}$. By looking at the action of the group $\{g \in GL(2m+2,\bar{k}) \ : \ g(M_0) = M_0,\ g(M_\infty) = M_\infty\}$ on the Grassmannian variety of m-dimensional linear subspaces in $\mathbb{P}^{2m+1}$, we see that there exists a linear transformation $g \in GL(2m+2,\bar{k})$ such that $g(M_0) = M_0$, $g(M_\infty) = M_\infty$ and $g(\Pi) = M_1^{(a,b)}$. Then we have $\rho(g)(J) \in Z^{(a,b)}(\bar{k})$. By the above argument, there exists an element $g' \in H^{(a,b)}(\bar{k})$ such that $\rho(g')\rho(g)(J) = J$. Then we have $g'g \in G_J^{0\infty}$ and $g'g(\Pi) = M_1^{(a,b)}$. Thus the first assertion is proved.

The stabilizer subgroup of $M_1^{(a,b)} \in \Sigma^m(X_J)^{(a,b)}$ in $G_J^{0\infty}$ is given by $H^{(a,b)} \cap G_J$. An element

$$g = \left(\begin{array}{c|c} \gamma & O \\ \hline O & \gamma' \end{array}\right) \quad \text{with} \quad \gamma = \left[\begin{array}{c|c|c} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \hline O & \gamma_{22} & O \\ \hline O & \gamma_{32} & \gamma_{33} \end{array}\right], \quad \gamma' = \left[\begin{array}{c|c|c} \gamma'_{11} & O & O \\ \hline \gamma'_{21} & \gamma'_{22} & \gamma'_{23} \\ \hline \gamma'_{31} & O & \gamma_{33} \end{array}\right]$$

of $H^{(a,b)}$ is contained in G_J if and only if γ is contained in $GL(m+1,k)$ and ${}^t\gamma'\gamma^{(q)}$ is the identity matrix by Proposition 3.5. If ${}^t\gamma'\gamma^{(q)} = I_{m+1}$, then γ_{33} must be an element of the group $GU(c,k)$. Hence the map $g \mapsto \gamma$ yields a homomorphism from $H^{(a,b)} \cap G_J$ to the group

$$H_J^{(a,b)} := \left\{ \left[\begin{array}{c|c|c} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \hline O & \gamma_{22} & O \\ \hline O & \gamma_{32} & \gamma_{33} \end{array}\right] \in GL(m+1,k) \quad ; \quad \gamma_{33} \in GU(c,k) \right\}.$$

We can check that the order of $H_J^{(a,b)}$ is equal to the denominator of the formula given in the assertion (2). The map $g \mapsto \gamma$ is an isomorphism between $H^{(a,b)} \cap G_J$ and $H_J^{(a,b)}$. Indeed, if $\gamma \in H_J^{(a,b)}$, then $\gamma' := ({}^t\gamma^{-1})^{(q)}$ satisfies $\gamma'_{12} = O$, $\gamma'_{32} = O$, $\gamma'_{13} = O$, and $\gamma_{33} = \gamma'_{33}$, and thus

$$\gamma \mapsto \left(\begin{array}{c|c} \gamma & O \\ \hline O & ({}^t\gamma^{-1})^{(q)} \end{array}\right)$$

yields the inverse homomorphism. Combining this with (3.3), we proved the assertion (2). *q.e.d.*

Because X_J is Hermitian, the set of $H \in \Sigma^{m-1}(X_J)$ satisfying $H \subset M_0$ is identified with the set $M_0^\vee(k)$ of k-rational points of the dual projective space of M_0 by Proposition 2.12. For $H \in M_0^\vee(k)$, we put

$$\Pi_H^+ := \beta_J(H, M_\infty).$$

Because $H \wedge M_\infty = \emptyset$, the definition means that Π_H^+ is the unique element of $B_J(H)$ such that $M_\infty \wedge \Pi_H^+ \neq \emptyset$. Thus $B_J(H)$ has two distinguished elements M_0 and Π_H^+. Therefore, for each $\Pi \in \Sigma^m(X_J)$, we can decompose $M_0^\vee(k)$ into the disjoint union of the following subsets:

$$\begin{aligned} C_0(\Pi) &:= \{\, H \in M_0^\vee(k) \ : \ \beta_J(H,\Pi) = M_0 \,\}, \\ C_\infty(\Pi) &:= \{\, H \in M_0^\vee(k) \ : \ \beta_J(H,\Pi) = \Pi_H^+ \,\}, \\ C_1(\Pi) &:= \{\, H \in M_0^\vee(k) \ : \ \beta_J(H,\Pi) \in B_J(H) \setminus \{M_0, \Pi_H^+\} \ \}. \end{aligned}$$

Table 3.1. $C_0(\Pi), C_\infty(\Pi)$ and $C_1(\Pi)$.

$\setminus\ \Pi$	M_0	M_∞	Π_H^+	Π_H^-
$C_0(\Pi)$	$M_0^\vee(k)$	$\emptyset$	$M_0^\vee(k)\setminus\{H\}$	$M_0^\vee(k)\setminus\{H\}$
$C_\infty(\Pi)$	$\emptyset$	$M_0^\vee(k)$	$\{H\}$	$\emptyset$
$C_1(\Pi)$	$\emptyset$	$\emptyset$	$\emptyset$	$\{H\}$

By the definition of $\beta_J(H,\Pi)$, we have

$$\begin{aligned} H\in C_0(\Pi) &\iff \dim(\Pi\wedge M_0)-1=\dim(\Pi\wedge H)=\dim(\Pi\wedge\Pi_H^+),\\ H\in C_\infty(\Pi) &\iff \dim(\Pi\wedge \Pi_H^+)-1=\dim(\Pi\wedge H)=\dim(\Pi\wedge M_0),\\ H\in C_1(\Pi) &\iff \dim(\Pi\wedge M_0)=\dim(\Pi\wedge\Pi_H^+)=\dim(\Pi\wedge H). \end{aligned} \tag{3.4}$$

For example, we have Table 3.1, where Π_H^- denotes an arbitrary element of $B_J(H)\setminus\{M_0,\Pi_H^+\}$.

Our aim is to describe the decomposition $M_0^\vee(k)=C_0(\Pi)\sqcup C_\infty(\Pi)\sqcup C_1(\Pi)$ for each $\Pi\in\Sigma^m(X_J)$. Let R be a k-rational linear subspace of M_0. We denote by $(M_0/R)^\vee$ the k-rational linear subspace of $M_0^\vee$ consisting of hyperplanes of M_0 containing R. Then we have

$$\dim R+\dim(M_0/R)^\vee+1=m.$$

When R is the empty set (that is, the linear subspace of dimension -1), we have $(M_0/\emptyset)^\vee=M_0^\vee$. (See Convention (4).)

Proposition 3.7. *Let Π be an element of $\Sigma^m(X_J)$, and R the intersection $\Pi\wedge M_0$. Then $C_\infty(\Pi)\sqcup C_1(\Pi)$ coincides with $(M_0/R)^\vee(k)$.*

Proof. We have $\Pi\wedge H=R\wedge H$ for any $H\in M_0^\vee(k)$. Hence $\dim(\Pi\wedge M_0)>\dim(\Pi\wedge H)$ holds if and only if $R\neq R\wedge H$; that is, if and only if $R\not\subset H$. *q.e.d.*

Definition 3.8. We define $\mathcal{P}$ to be the set of pairs (Γ_∞,Γ_1) of mutually disjoint subsets of $M_0^\vee(k)$. We have a map $\zeta:\Sigma^m(X_J)\to\mathcal{P}$ defined by

$$\zeta(\Pi):=(C_\infty(\Pi),C_1(\Pi)).$$

For integers a and b satisfying $-1\le a,b\le m$ and $a+b\le m-1$, we define $\mathcal{R}^{(a,b)}$ to be the set of couples (R,Y) such that

(i) R is a k-rational linear subspace of M_0 with $\dim R=a$, and
(ii) Y is a Hermitian hypersurface in $(M_0/R)^\vee$ with $\operatorname{rank}(Y)=m-1-a-b$.

Note that we can consider Y as a subvariety of $M_0^\vee$ because $(M_0/R)^\vee$ is a linear subspace of $M_0^\vee$. Let $\mathcal{R}$ be the disjoint union of the sets $\mathcal{R}^{(a,b)}$. We have a map $\xi:\mathcal{R}\to\mathcal{P}$ defined by

$$\xi(R,Y):=(\ Y(k),\ (M_0/R)^\vee(k)\setminus Y(k)\ ).$$

Recall that the group $G_J^{0\infty}$ acts on M_0 over k, and hence $G_J^{0\infty}$ acts on $\mathcal{P}$. By definition, the map ζ is equivariant under this action. The group $G_J^{0\infty}$ also acts on the set $\mathcal{R}^{(a,b)}$ in a natural way, and the map ξ is obviously equivariant under this action. Hence the subset $\xi(\mathcal{R}^{(a,b)})$ of $\mathcal{P}$ is stable under the action of $G_J^{0\infty}$.

Proposition 3.9. (1) *For each (a,b), the action of $G_J^{0\infty}$ on the set $\mathcal{R}^{(a,b)}$ is transitive.*

(2) *The number $|\mathcal{R}^{(a,b)}|$ is equal to*

$$h(m-a-1, m-1-a-b) \cdot |\operatorname{Grass}(\mathbb{P}^a, M_0)(k)|,$$

where h is the function given in Corollary 2.6 and $\operatorname{Grass}(\mathbb{P}^a, M_0)(k)$ is the set of k-rational linear subspaces of M_0 with dimension a.

Proof. The action of $G_J^{0\infty}$ on M_0 factors through the isomorphism (3.3). Hence $G_J^{0\infty}$ acts on the set $\operatorname{Grass}(\mathbb{P}^a, M_0)(k)$ transitively, and the stabilizer subgroup of a linear subspace $R \in \operatorname{Grass}(\mathbb{P}^a, M_0)(k)$ acts on the set of Hermitian hypersurfaces of rank $m-1-a-b$ in $(M_0/R)^\vee$ transitively by Proposition 1.2 (1). Thus the assertion (1) is proved. The assertion (2) is obvious. *q.e.d.*

Proposition 3.10. *For each (a,b), the map $\zeta : \Sigma^m(X_J) \to \mathcal{P}$ induces a surjective map from $\Sigma^m(X_J)^{(a,b)}$ to $\xi(\mathcal{R}^{(a,b)})$ such that each fiber consists of a single element if $a+b = m-1$, while it consists of $q-1$ elements if $a+b \neq m-1$.*

Proof. The map ξ is injective because of Proposition 2.8. Hence $|\xi(\mathcal{R}^{(a,b)})|$ is equal to $|\mathcal{R}^{(a,b)}|$. By Propositions 3.6 (2) and 3.9 (2), we have

$$|\Sigma^m(X_J)^{(a,b)}| \;/\; |\xi(\mathcal{R}^{(a,b)})| = \begin{cases} q-1 & \text{if } a+b \neq m-1, \\ 1 & \text{if } a+b = m-1. \end{cases}$$

Because ζ and ξ are equivariant under the action of $G_J^{0\infty}$, and because the actions are transitive both on $\Sigma^m(X_J)^{(a,b)}$ and $\xi(\mathcal{R}^{(a,b)})$ by Propositions 3.6 (1) and 3.9 (1), it is enough to show that an element of $\Sigma^m(X_J)^{(a,b)}$ is mapped to an element of $\xi(\mathcal{R}^{(a,b)})$ by ζ. Consider the element $M_1^{(a,b)} \in \Sigma^m(X_J)^{(a,b)}$. We put

$$R^a := M_1^{(a,b)} \cap M_0 = \{\, x_{a+1} = \cdots = x_m = y_0 = \cdots = y_m = 0 \,\}.$$

By Proposition 3.7, we have $C_\infty(M_1^{(a,b)}) \sqcup C_1(M_1^{(a,b)}) = (M_0/R^a)^\vee(k)$. We consider ${}^t(x_0, \dots, x_m)$ as homogeneous coordinates of M_0. Let $(\xi_0, \dots, \xi_m)$ be the homogeneous coordinates of $M_0^\vee$ dual to ${}^t(x_0, \dots, x_m)$. Then we have

$$(M_0/R^a)^\vee = \{\, \xi_0 = \cdots = \xi_a = 0 \,\}.$$

We fix an element H of $(M_0/R^a)^\vee(k)$. Let the defining equation of H in M_0 be

$$\alpha_{a+1}x_{a+1} + \cdots + \alpha_m x_m = 0,$$

where $\alpha_i \in k$ $(i = a+1, \dots, m)$. We will show that the linear subspace Π_H^+ is spanned by H and the point

$$\delta(H) := {}^t(\overbrace{0, \dots, 0,}^{m+a+2 \text{ times}}\ \alpha_{a+1}^q, \dots, \alpha_m^q) \in M_\infty.$$

Because Π_H^+ is the unique element of $\Sigma^m(X_J)$ that contains H and intersects M_∞, it is enough to show that the m-dimensional linear subspace spanned by H and $\delta(H)$ is contained in X_J. For a point $u := {}^t(u_0, \dots, u_m)$ of H, the line connecting $\delta(H)$ and u is given by

$$\{\, {}^t(\lambda u_0, \dots, \lambda u_m, 0, \dots, 0, \alpha_{a+1}^q, \dots, \alpha_m^q) \;:\; \lambda \in \mathbb{P}^1 \,\}.$$

Using $\alpha_{a+1}u_{a+1} + \cdots + \alpha_m u_m = 0$ and $\alpha_i^{q^2} = \alpha_i$, we can easily check that this line is contained in X_J. Thus the claim is proved.

By (3.4), the element H of $(M_0/R^a)^\vee(k)$ is contained in $C_\infty(M_1^{(a,b)})$ if and only if $\dim(\Pi_H^+ \wedge M_1^{(a,b)}) = a+1$ holds. Because R^a is contained in $\Pi_H^+ \wedge M_1^{(a,b)}$, this is equivalent to the existence of a point of $\Pi_H^+ \wedge M_1^{(a,b)}$ that is not contained in R^a. A point

$$^t(\lambda u_0, \dots, \lambda u_m, 0, \dots, 0, \alpha_{a+1}^q, \dots, \alpha_m^q)$$

of Π_H^+ is not contained in M_0 if and only if $\lambda \neq \infty$, and this point is contained in $M_1^{(a,b)}$ if and only if

$$\lambda u_{a+1} = \cdots = \lambda u_{a+b+1} = 0 \text{ and } \lambda u_j = \alpha_j^q \text{ for } j = a+b+2, \dots, m \tag{3.5}$$

hold. In order for a point $u \in H$ and $\lambda \in \mathbb{P}^1 \setminus \{\infty\}$ satisfying (3.5) to exist, it is necessary and sufficient that $\alpha_{a+b+2}^{q+1} + \cdots + \alpha_m^{q+1} = 0$ holds. Therefore $H \in C_\infty(M_1^{(a,b)})$ if and only if H is a k-rational point of the Hermitian hypersurface in $(M_0/R^a)^\vee$ defined by

$$\xi_{a+b+2}^{q+1} + \cdots + \xi_m^{q+1} = 0.$$

The rank of this Hermitian hypersurface is $m-1-a-b$. *q.e.d.*

Corollary 3.11. *Suppose that $q=2$. Then ζ induces a bijection from $\Sigma^m(X_J)^{(a,b)}$ to $\xi(\mathcal{R}^{(a,b)})$ for every (a,b).*

Corollary 3.12. *Suppose that Π is an element of $\Sigma^m(X_J)^{(a,b)}$. Then we have*

$$\begin{aligned} |C_0(\Pi)| &= |\mathbb{P}^m(k)| - |\mathbb{P}^{m-a-1}(k)|, \\ |C_\infty(\Pi)| &= F(m-a-1, m-1-a-b), \\ |C_1(\Pi)| &= |\mathbb{P}^{m-a-1}(k)| - F(m-a-1, m-1-a-b), \end{aligned}$$

where F is the function given in Proposition 2.7.

4. The signature and the discriminant of the lattice

In this section, we prove Theorem 1.1.

Let (X_J, M_0, M_∞) be the triple defined in the previous section. The intersection number of two elements Π, Π' of $\Sigma^m(X_J)$ on X_J is given by

$$\Pi.\Pi' = \theta(\nu) := \frac{1-(-q)^{\nu+1}}{1+q}, \quad \text{where } \nu := \dim(\Pi \wedge \Pi'). \tag{4.1}$$

(See, for example, Fulton [7, p. 102, Excess Intersection Formula].) Note that this formula holds even when Π and Π' are disjoint, because we have defined $\dim \emptyset$ to be -1. (See Convention (4).) For simplicity, we put

$$\Omega := \Sigma^m(X_J)^{(m-1,-1)} \quad \text{and} \quad \Xi := \Sigma^m(X_J)^{(m-1,0)}.$$

Recall that the set of $H \in \Sigma^{m-1}(X_J)$ lying on M_0 is identified with $M_0^\vee(k)$. We denote by

$$\tau : \Omega \sqcup \Xi \longrightarrow M_0^\vee(k)$$

the map $\Pi \mapsto \Pi \wedge M_0$. By Proposition 3.1, the fiber $\tau^{-1}(H)$ of τ over an element H of $M_0^\vee(k)$ coincides with the set $B_J(H) \setminus \{M_0\}$ consisting of q elements, and $\tau^{-1}(H) \cap \Xi$ consists of a single element $\Pi_H^+ = \beta_J(H, M_\infty)$. Thus we have $|\Omega| =$

$(q-1)\cdot|M_0^\vee(k)|$. On the other hand, the middle Betti number $b_{2m}(S_d^{2m})$ of a nonsingular hypersurface S_d^{2m} of dimension $2m$ and degree d is well-known:

$$b_{2m}(S_d^{2m}) = 2 + (\ (d-1)^{2m+2} - 1\ )\ /\ d.$$

Applying this formula to our case $d = q+1$, we obtain

$$|\Omega| = b_{2m}(X_J) - 2. \tag{4.2}$$

We put

$$\overline{\Omega} := \Omega \sqcup \{\eta, \omega\},$$

where η and ω are formal elements. We denote by E the real vector space $\mathbb{R}^{\overline{\Omega}}$ of $\mathbb{R}$-valued functions on $\overline{\Omega}$, and define a symmetric bilinear form $(\ ,\ )_E$ on E by

$$(f,g)_E := f(\omega)g(\omega) + (-1)^m\big[f(\eta)g(\eta) + \sum_{\Pi\in\Omega} f(\Pi)g(\Pi)\big].$$

Note that we have $\dim E = b_{2m}(X_J)$ by (4.2), and that the signature of E is $(1, b_{2m}(X_J)-1)$ when m is odd, while it is $(b_{2m}(X_J), 0)$ when m is even.

Let M' be an element of Ξ. We put $\Omega' := \Omega \sqcup \{M_0, M'\}$. We will show that there exists a map $v : \Omega' \to E$ with the following two properties:

(i) for any $\Pi, \Pi' \in \Omega'$, we have $\Pi.\Pi' = (v(\Pi), v(\Pi'))_E$, and

(ii) the determinant of the square matrix

$$\Gamma := (v(\Pi)(x)\ ;\ \Pi\in\Omega',\ x\in\overline{\Omega})$$

of size $b_{2m}(X_J)$ is a power of $\sqrt{q}$ up to sign.

First we assume that such a map v is constructed, and deduce Theorem 1.1. Because $\det\Gamma \neq 0$ and $|\Omega'| = \dim E$, the set of vectors $\{v(\Pi) : \Pi\in\Omega'\}$ constitutes a basis of E over $\mathbb{R}$. Combining this with the property (i), we see that v induces an isometry

$$NL^m(X_J)' \otimes_{\mathbb{Z}} \mathbb{R} \cong E,$$

where $NL^m(X_J)'$ is the sublattice of $NL^m(X_J)$ generated by the numerical equivalence classes $[\Pi]$ of $\Pi\in\Omega'$. It follows that the rank of $NL^m(X_J)'$ is equal to $b_{2m}(X_J)$, that the set of classes $\{[\Pi] : \Pi\in\Omega'\}$ becomes a $\mathbb{Z}$-basis of $NL^m(X_J)'$, and that the signature of $NL^m(X_J)'$ is the same with that of E. In particular, we recover the result of Tate [16] that X_J is supersingular, and hence $N^m(X_J)$ is of finite rank with $\mathrm{rank}(N^m(X_J)) = b_{2m}(X_J)$. By the property (i), the intersection matrix of $NL^m(X_J)'$ with respect to the basis $\{[\Pi] : \Pi\in\Omega'\}$ is given by ${}^t\Gamma\cdot\mathrm{Gram}(E)\cdot\Gamma$, where $\mathrm{Gram}(E)$ is the Gram matrix of E with respect to the standard basis. In particular, we have $\mathrm{disc}(NL^m(X_J)') = (\det\Gamma)^2$. By the property (ii), we see that $\mathrm{disc}(NL^m(X_J)')$ is a power of q. We know that the rank of $NL^m(X_J)$ is at most $\mathrm{rank}(N^m(X_J)) = b_{2m}(X_J)$. Thus $NL^m(X_J)'$ is of finite index in $NL^m(X_J)$. Therefore the signature of $NL^m(X_J)$ is equal to that of E, and the discriminant of $NL^m(X_J)$ divides that of $NL^m(X_J)'$. Thus Theorem 1.1 is proved.

Now we proceed to the construction of the map v. We will construct a map

$$v' : \Omega\sqcup\Xi\sqcup\{M_0, M_\infty\} \longrightarrow E$$

such that

$$\Pi.\Pi' = (v'(\Pi), v'(\Pi'))_E \tag{4.3}$$

Table 4.1. $\dim(\Pi \wedge \Pi')$.

<table>
<tr><th>$\Pi' \ \backslash \ \Pi$</th><th>M_0</th><th>M_∞</th><th>in Ω</th><th>in Ξ</th></tr>
<tr><td>M_0</td><td>m</td><td>-1</td><td>$m-1$</td><td>$m-1$</td></tr>
<tr><td>M_∞</td><td>-1</td><td>m</td><td>-1</td><td>0</td></tr>
<tr><td>in Ω</td><td>$m-1$</td><td>-1</td><td colspan="2" rowspan="2">$\begin{cases} m & \text{if } \Pi = \Pi' \\ m-1 & \text{if } \Pi \neq \Pi' \text{ and } \tau(\Pi) = \tau(\Pi') \\ m-2 & \text{if } \tau(\Pi) \neq \tau(\Pi') \end{cases}$</td></tr>
<tr><td>in Ξ</td><td>$m-1$</td><td>0</td></tr>
</table>

Table 4.2. The intersection number $A.B$.

<table>
<tr><th>$A \ \backslash \ B$</th><th>M_0</th><th>$M_\infty - M_0$</th><th>$\Pi - M_0 \ \ (\Pi \in \Omega)$</th><th>$\Pi - M_0 \ \ (\Pi \in \Xi)$</th></tr>
<tr><td>M_0</td><td>$\theta(m)$</td><td>$-\theta(m)$</td><td>$-(-q)^m$</td><td>$-(-q)^m$</td></tr>
<tr><td>$M_\infty - M_0$</td><td>$-\theta(m)$</td><td>$2\theta(m)$</td><td>$(-q)^m$</td><td>$1+(-q)^m$</td></tr>
<tr><td colspan="5">and, for $\Pi, \Pi' \in \Omega \sqcup \Xi$, we have $$(\Pi - M_0).(\Pi' - M_0) = \begin{cases} 2(-q)^m & \text{if } \Pi = \Pi' \\ (-q)^m & \text{if } \Pi \neq \Pi' \text{ and } \tau(\Pi) = \tau(\Pi') \\ -(q+1)(-q)^{m-1} & \text{if } \tau(\Pi) \neq \tau(\Pi') \end{cases}$$</td></tr>
</table>

holds for any $\Pi, \Pi' \in \Omega \sqcup \Xi \sqcup \{M_0, M_\infty\}$, and show that the restriction of v' to Ω' possesses the property (ii) for an arbitrary choice of $M' \in \Xi$.

By Corollary 3.2, the dimensions of $\Pi \wedge \Pi'$ are as in Table 4.1. Using the formula (4.1), we can calculate the intersection numbers $A.B$ as in Table 4.2, where A and B are M_0, $M_\infty - M_0$ or $\Pi - M_0$ ($\Pi \in \Omega \sqcup \Xi$). Here we have used the equalities

$$\theta(m) - \theta(m-1) = (-q)^m \quad \text{and} \quad \theta(m) - 2\,\theta(m-1) + \theta(m-2) = -(q+1)(-q)^{m-1}.$$

For simplicity, we put

$$\alpha_0 := \frac{1}{\sqrt{q+1}}, \quad \alpha_\infty := -\frac{\sqrt{q^{m+1}}}{\sqrt{q+1}}, \qquad \beta_1 := \frac{1}{\sqrt{q^{m+1}}}, \quad \beta_\infty := \frac{q^{m+1}+(-1)^m}{\sqrt{q+1}\sqrt{q^{m+1}}},$$

$$\gamma_\infty := \sqrt{q^{m-1}(q+1)}, \quad \gamma_1 := \frac{\sqrt{q^m}}{q-1}\left(1 - \frac{(-1)^m}{\sqrt{q}}\right), \quad \gamma_2 := \frac{\sqrt{q^m}}{q-1}\left((2-q) - \frac{(-1)^m}{\sqrt{q}}\right),$$

$$Q := (-1)^m \sqrt{q^{m-1}}.$$

We define the map v' by Table 4.3, which indicates the value of the function $v'(A)$ at $x \in \overline{\Omega}$. Here $v'(\Pi - M_0)$ means $v'(\Pi) - v'(M_0)$. Recall that, for a given $H \in M_0^\vee(k)$, there are exactly $q-1$ elements of Ω that are mapped to H by τ. Hence the values $(v'(A), v'(B))_E$ are calculated as in Table 4.4. We can easily check that Tables 4.2 and 4.4 coincide. Thus the map v' satisfies (4.3).

TABLE 4.3. $v'(A)(x)$.

$x \setminus A$	M_0	$M_\infty - M_0$	$\Pi - M_0$ $(\Pi \in \Omega)$	$\Pi - M_0$ $(\Pi \in \Xi)$
ω	α_0	0	0	0
η	α_∞	β_∞	γ_∞	γ_∞
in Ω	0	β_1	$\diamondsuit$	$\heartsuit$

where

$$\diamondsuit = \begin{cases} \gamma_2 & \text{if } x = \Pi \\ \gamma_1 & \text{if } x \neq \Pi \text{ and } \tau(x) = \tau(\Pi) \\ 0 & \text{if } \tau(x) \neq \tau(\Pi) \end{cases} \qquad \text{and} \qquad \heartsuit = \begin{cases} Q & \text{if } \tau(x) = \tau(\Pi) \\ 0 & \text{if } \tau(x) \neq \tau(\Pi) \end{cases}$$

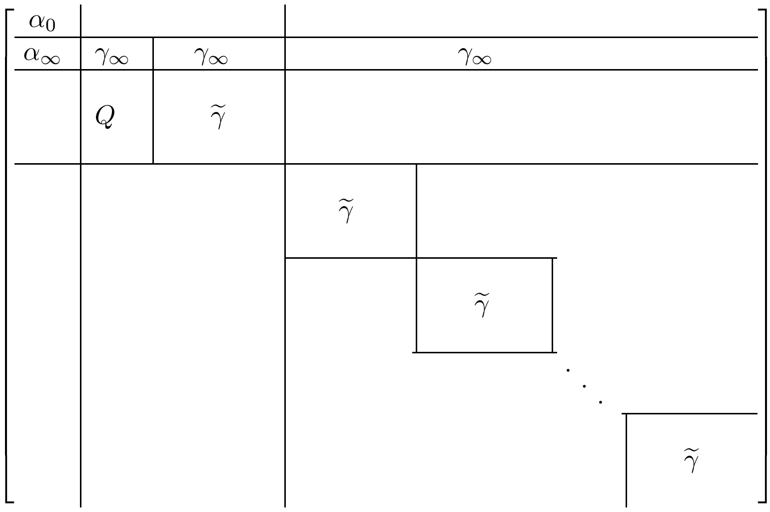
TABLE 4.4. $(v'(A), v'(B))_E$.

$A \setminus B$	M_0	$M_\infty - M_0$
M_0	$\alpha_0^2 + (-1)^m \alpha_\infty^2$	$(-1)^m \alpha_\infty \beta_\infty$
$M_\infty - M_0$	$(-1)^m \alpha_\infty \beta_\infty$	$(-1)^m (\beta_\infty^2 + \lvert\Omega\rvert\, \beta_1^2)$
$\Pi' - M_0$ $(\Pi' \in \Omega)$	$(-1)^m \alpha_\infty \gamma_\infty$	$(-1)^m \{\beta_\infty \gamma_\infty + \beta_1(\gamma_2 + (q-2)\gamma_1)\}$
$\Pi' - M_0$ $(\Pi' \in \Xi)$	$(-1)^m \alpha_\infty \gamma_\infty$	$(-1)^m \{\beta_\infty \gamma_\infty + (q-1)\beta_1 Q\}$

$A \setminus B$	$\Pi - M_0$ $(\Pi \in \Omega)$
$\Pi' - M_0$ $(\Pi' \in \Omega)$	$\begin{cases} (-1)^m \{\gamma_\infty^2 + \gamma_2^2 + (q-2)\gamma_1^2\} & \text{if } \Pi = \Pi' \\ (-1)^m \{\gamma_\infty^2 + (q-3)\gamma_1^2 + 2\gamma_1\gamma_2\} & \text{if } \Pi \neq \Pi' \text{ and } \tau(\Pi) = \tau(\Pi') \\ (-1)^m \gamma_\infty^2 & \text{if } \tau(\Pi) \neq \tau(\Pi') \end{cases}$
$\Pi' - M_0$ $(\Pi' \in \Xi)$	$\begin{cases} (-1)^m \{\gamma_\infty^2 + Q(\gamma_2 + (q-2)\gamma_1)\} & \text{if } \tau(\Pi) = \tau(\Pi') \\ (-1)^m \gamma_\infty^2 & \text{if } \tau(\Pi) \neq \tau(\Pi') \end{cases}$

$A \setminus B$	$\Pi - M_0$ $(\Pi \in \Xi)$
$\Pi' - M_0$ $(\Pi' \in \Xi)$	$\begin{cases} (-1)^m \{\gamma_\infty^2 + (q-1)Q^2\} & \text{if } \tau(\Pi) = \tau(\Pi') \\ (-1)^m \gamma_\infty^2 & \text{if } \tau(\Pi) \neq \tau(\Pi') \end{cases}$

FIGURE 4.1. The matrix Γ'.



,

We define a square matrix $\widetilde{\gamma} = (\gamma_{ij})$ of size $q-1$ by

$$\gamma_{ij} := \begin{cases} \gamma_2 & \text{if } i = j \\ \gamma_1 & \text{if } i \neq j. \end{cases}$$

We also put

$$\Omega'' := \{\, M_0, M' - M_0 \} \ \sqcup \ \{ \Pi - M_0 \ : \ \Pi \in \Omega \,\},$$

where M' is an arbitrary element of Ξ. By ordering elements of $\overline{\Omega}$ and Ω'' in a suitable way, the square matrix

$$\Gamma' := (v(A)(x) \ : \ A \in \Omega'',\ x \in \overline{\Omega})$$

of size $b_{2m}(X_J)$ is written in the form as in Figure 4.1, in which blank parts are zero matrices. Because we have

$$\det \widetilde{\gamma} = (\gamma_2 - \gamma_1)^{q-2} \cdot (\gamma_2 + (q-2)\gamma_1) = \pm \sqrt{q}^{mq-m-1}$$

and

$$\det \left(\begin{array}{c|c} \gamma_\infty & \gamma_\infty \\ \hline Q & \widetilde{\gamma} \end{array} \right) = \gamma_\infty \cdot (\gamma_2 - \gamma_1)^{q-2} \cdot (\gamma_2 + (q-2)\gamma_1 - (q-1)Q) = \pm \frac{1}{\alpha_0} \sqrt{q}^{mq},$$

it follows that $|\det \Gamma\,| = |\det \Gamma'\,|$ is a power of $\sqrt{q}$. *q.e.d.*

Because Ω' is contained in $\Omega \sqcup \Xi \sqcup \{M_0\}$, we have also proved the following.

Corollary 4.1. *The vector space* $NL^m(X_J) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is generated by the classes* $[\Pi]$, *where* Π *runs through the set* $\Omega \sqcup \Xi \sqcup \{M_0\}$.

The map v induces an isometry $\tilde{v}$ from $N^m(X_J) \otimes_{\mathbb{Z}} \mathbb{R}$ to E. Let us calculate the vector $\tilde{v}(h) \in E$, where $h \in N^m(X_J)$ is the numerical equivalence class of the intersection of X_J with a general linear subspace of $\mathbb{P}^{2m+1}$ with dimension $m+1$.

We choose H from $M_0^\vee(k)$. By Corollary 3.3, the vector $\tilde{v}(h)$ is the sum of $\tilde{v}([\Pi])$, where Π runs through the set $B_J(H)$. Because

$$(q+1)\alpha_\infty + q\gamma_\infty = 0 \quad \text{and} \quad \gamma_2 + (q-2)\gamma_1 + Q = 0,$$

we see that

$$\tilde{v}(h)(x) = \begin{cases} \alpha_0 & \text{if } x = \omega, \\ 0 & \text{if } x \in \overline{\Omega} \setminus \{\omega\}. \end{cases}$$

In particular, the primitive part $N^m_{\mathrm{prim}}(X_J) = (h)^\perp$ is mapped by $\tilde{v}$ to the subspace $\{f \in E \,:\, f(\omega) = 0\}$ of E, on which $(\ ,\ )_E$ multiplied by $(-1)^m$ is positive definite.

5. The structure of the lattice in the case $q = 2$

From now to the end of the paper, we put $p = q = 2$. In particular, the finite field k is $\mathbb{F}_4$, and X_J is projectively isomorphic to the cubic Fermat hypersurface.

Let (X_J, M_0, M_∞) be the triple defined in Section 2. We put $T := M_0^\vee(k)$, and let $\widetilde{L}^m$ be the lattice constructed from this T by the procedure described in the Introduction. Our aim in this section is to prove Theorem 1.4; that is, to construct an isomorphism $\mathcal{L}^m(X_J) \cong \widetilde{L}^m$ of lattices.

The lattice $\mathcal{L}^m(X_J)$ is generated by the numerical equivalence classes

$$[\![\Pi]\!] := [\Pi] - [M_0] \quad (\Pi \in \Sigma^m(X_J) \setminus \{M_0\}).$$

The symmetric bilinear form $(\ ,\ )_\mathcal{L}$ on $\mathcal{L}^m(X_J)$ is the intersection form multiplied by $(-1)^m$, and hence it is given by

$$([\![\Pi]\!], [\![\Pi']\!])_\mathcal{L} = (-1)^m(\theta(\dim(\Pi \wedge \Pi')) - \theta(\dim(\Pi \wedge M_0)) - \theta(\dim(\Pi' \wedge M_0)) + \theta(m)), \tag{5.1}$$

where θ is defined by (4.1). Recall that $\widetilde{T}$ is the set $T \sqcup \{\varphi\}$, where φ is a formal element, and that $\mathbb{Z}^{\widetilde{T}}$ is equipped with a $\mathbb{Q}$-valued bilinear symmetric form $(\ ,\ )_T$ given by (1.1). First we define a map $u : \Sigma^m(X_J) \to \mathbb{Z}^{\widetilde{T}}$ such that

$$([\![\Pi]\!], [\![\Pi']\!])_\mathcal{L} = (u(\Pi), u(\Pi'))_T \tag{5.2}$$

holds for any $\Pi, \Pi' \in \Sigma^m(X_J)$.

Suppose that $\dim(\Pi \wedge M_0) = a$. We define $u(\Pi) \in \mathbb{Z}^{\widetilde{T}}$ by

$$u(\Pi)(H) := \begin{cases} 0 & \text{if } H \in C_0(\Pi), \\ (-2)^{a+1} & \text{if } H \in C_\infty(\Pi), , \\ -(-2)^{a+1} & \text{if } H \in C_1(\Pi) \end{cases}$$

and

$$u(\Pi)(\varphi) := -(-2)^{a+1}\,\theta(m-a-1).$$

Then Table 3.1 implies that $u(M_0) = 0$. Because $q = 2$, the map $\tau : \Omega \sqcup \Xi \to T$ defined in Section 4 induces bijections $\Omega \cong T$ and $\Xi \cong T$ of sets. For $H \in T$, we denote by $\Pi_H^- \in \Omega$ and $\Pi_H^+ \in \Xi$ the unique elements such that $\tau(\Pi_H^-) = \tau(\Pi_H^+) = H$. Then $B_J(H)$ consists of the three elements M_0, Π_H^+ and Π_H^- for any $H \in T$. If $\Pi \in \Omega \sqcup \Xi$, then $\dim(\Pi \wedge M_0) = m - 1$ and hence $u(\Pi)(\varphi) = -(-2)^m$. Using Table 3.1, we can calculate $(u(\Pi), u(\Pi'))_T$ for $\Pi, \Pi' \in \Omega \sqcup \Xi$ as in Table 5.1. On the other hand, from Corollary 3.2, the dimensions $\dim(\Pi \wedge \Pi')$ are given by Table 5.2. We put

Table 5.1. $(u(\Pi^{\pm}_H), u(\Pi^{\pm}_{H'}))_T$.

$\Pi' \setminus \Pi$	Π^+_H	Π^-_H
$\Pi^+_{H'}$	$\begin{cases} 3\cdot 2^{m-1} & \text{if } H\ne H' \\ 4\cdot 2^{m-1} & \text{if } H=H' \end{cases}$	$\begin{cases} 3\cdot 2^{m-1} & \text{if } H\ne H' \\ 2\cdot 2^{m-1} & \text{if } H=H' \end{cases}$
$\Pi^-_{H'}$	$\begin{cases} 3\cdot 2^{m-1} & \text{if } H\ne H' \\ 2\cdot 2^{m-1} & \text{if } H=H' \end{cases}$	$\begin{cases} 3\cdot 2^{m-1} & \text{if } H\ne H' \\ 4\cdot 2^{m-1} & \text{if } H=H' \end{cases}$

Table 5.2. $\dim(\Pi^{\pm}_H \wedge \Pi^{\pm}_{H'})$.

$\Pi' \setminus \Pi$	Π^+_H	Π^-_H
$\Pi^+_{H'}$	$\begin{cases} m-2 & \text{if } H\ne H' \\ m & \text{if } H=H' \end{cases}$	$\begin{cases} m-2 & \text{if } H\ne H' \\ m-1 & \text{if } H=H' \end{cases}$
$\Pi^-_{H'}$	$\begin{cases} m-2 & \text{if } H\ne H' \\ m-1 & \text{if } H=H' \end{cases}$	$\begin{cases} m-2 & \text{if } H\ne H' \\ m & \text{if } H=H' \end{cases}$

$$\Theta_a(\nu) := (-1)^m(\theta(\nu) - \theta(a) - \theta(m-1) + \theta(m)).$$

If $\Pi, \Pi' \in \Omega \sqcup \Xi$, then $([\![\Pi]\!], [\![\Pi']\!])_{\mathcal{L}} = \Theta_{m-1}(\dim(\Pi \wedge \Pi'))$ by (5.1). It is easy to check that the equalities

$$\Theta_{m-1}(m-2) = 3\cdot 2^{m-1}, \quad \Theta_{m-1}(m-1) = 2\cdot 2^{m-1} \quad \text{and} \quad \Theta_{m-1}(m) = 4\cdot 2^{m-1}$$

hold. Hence (5.2) is satisfied when Π and Π' are elements of $\Omega \sqcup \Xi$. By Corollary 4.1, the vector space $\mathcal{L}^m(X_J) \otimes_{\mathbb{Z}} \mathbb{Q}$ is generated by the numerical equivalence classes $[\![\Pi]\!]$ of $\Pi \in \Omega \sqcup \Xi$. Hence the map $u|_{\Omega\sqcup\Xi} : \Omega \sqcup \Xi \to \mathbb{Z}^{\widetilde{T}}$ induces an isomorphism of $\mathbb{Q}$-lattices

$$\mathcal{L}^m(X_J) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Z}^{\widetilde{T}} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Therefore, in order to check (5.2), it is enough to show that

$$([\![\Pi]\!], [\![\Pi^+_H]\!])_{\mathcal{L}} = (u(\Pi), u(\Pi^+_H))_T \quad \text{and} \quad ([\![\Pi]\!], [\![\Pi^-_H]\!])_{\mathcal{L}} = (u(\Pi), u(\Pi^-_H))_T \tag{5.3}$$

hold for any couple of $\Pi \in \Sigma^m(X_J) \setminus (\Omega \sqcup \Xi \sqcup \{M_0\})$ and $H \in T$. Note that the set $\Sigma^m(X_J) \setminus (\Omega \sqcup \Xi \sqcup \{M_0\})$ is the disjoint union of $\Sigma^m(X_J)^{(a,b)}$ with $a \le m-2$. Let Π be an element of $\Sigma^m(X_J)^{(a,b)}$ with $a \le m-2$. We put

$$\Phi_a := \frac{1}{2^{m+1}}(3\cdot u(\Pi)(\varphi)\cdot u(\Pi^{\pm}_H)(\varphi)) = 3\cdot(-1)^{m+1}\cdot(-2)^a\cdot\theta(m-a-1).$$

From the definition of u and Table 3.1, we can calculate $(u(\Pi), u(\Pi^{\pm}_H))_T$ as in Table 5.3. On the other hand, from the definitions of $\beta_J(H,\Pi)$ and $C_0(\Pi)$, $C_\infty(\Pi)$, $C_1(\Pi)$, we obtain Table 5.4. (See (3.4).) Because

$$([\![\Pi]\!], [\![\Pi^+_H]\!])_{\mathcal{L}} = \Theta_a(\dim(\Pi \wedge \Pi^+_H)), \qquad ([\![\Pi]\!], [\![\Pi^-_H]\!])_{\mathcal{L}} = \Theta_a(\dim(\Pi \wedge \Pi^-_H))$$

and

$$\Theta_a(a-1) = \Phi_a, \quad \Theta_a(a+1) = \Phi_a + (-1)^{m+1}(-2)^a \quad \text{and} \quad \Theta_a(a) = \Phi_a - (-1)^{m+1}(-2)^a,$$

we see that the map u satisfies (5.3) and hence (5.2).

TABLE 5.3. $(u(\Pi), u(\Pi_H^{\pm}))_T$.

	$(u(\Pi), u(\Pi_H^{+}))_T$	$(u(\Pi), u(\Pi_H^{-}))_T$
$H \in C_0(\Pi)$	Φ_a	Φ_a
$H \in C_\infty(\Pi)$	$\Phi_a + (-1)^{m+1}(-2)^a$	$\Phi_a - (-1)^{m+1}(-2)^a$
$H \in C_1(\Pi)$	$\Phi_a - (-1)^{m+1}(-2)^a$	$\Phi_a + (-1)^{m+1}(-2)^a$

TABLE 5.4. $\dim(\Pi \wedge X)$ for $X = H, M_0, \Pi_H^{\pm}$.

	$\dim(\Pi \wedge H)$	$\dim(\Pi \wedge M_0)$	$\dim(\Pi \wedge \Pi_H^{+})$	$\dim(\Pi \wedge \Pi_H^{-})$
$H \in C_0(\Pi)$	$a-1$	a	$a-1$	$a-1$
$H \in C_\infty(\Pi)$	a	a	$a+1$	a
$H \in C_1(\Pi)$	a	a	a	$a+1$

The map u induces an embedding $\tilde{u} : \mathcal{L}^m(X_J) \hookrightarrow \mathbb{Z}^{\widetilde{T}}$ of the lattice $\mathcal{L}^m(X_J)$ into $\mathbb{Z}^{\widetilde{T}}$. Next we show that the image of $\tilde{u}$ coincides with $\widetilde{L}^m$. First note that the vectors $u(\Pi_H^+) - u(\Pi_H^-)$ and $u(\Pi_H^+) + u(\Pi_H^-)$, where H runs through T, generate the kernel of the natural projection $\widetilde{\mathrm{pr}} : \mathbb{Z}^{\widetilde{T}} \to R^{\widetilde{T}}$, where $R = \mathbb{Z}/(2^{m+1})$. Hence we have $\operatorname{Ker} \widetilde{\mathrm{pr}} \subset \operatorname{Im} \tilde{u}$. Second, using Corollary 3.12, we can check that

$$\begin{aligned} -u(\Pi)(\varphi) + \sum_{H \in T} u(\Pi)(H) &= (-2)^{a+1}\theta(m-a-1) + (|C_\infty(\Pi)| - |C_1(\Pi)|) \cdot (-2)^{a+1} \\ &= (-2)^{m+1} \cdot (-1 + (-2)^{b+1}) \,/\, 3 \end{aligned}$$

is 0 modulo 2^{m+1} for any $\Pi \in \Sigma^m(X_J)$. This means that $\widetilde{\mathrm{pr}}(u(\Pi)) \in R^{\widetilde{T}}$ is the extension of its restriction $\widetilde{\mathrm{pr}}(u(\Pi))|_T \in R^T$ to T. Therefore, it is enough to show that the restriction $\widetilde{\mathrm{pr}}(\operatorname{Im} \tilde{u})|_T \subset R^T$ of the R-submodule $\widetilde{\mathrm{pr}}(\operatorname{Im} \tilde{u})$ of $R^{\widetilde{T}}$ to $T \subset \widetilde{T}$ coincides with the R-submodule $\overline{L}^m$ of R^T.

First we prepare several lemmas. Recall that $\overline{L}^m$ is generated by $\overline{V}_T$ and $2\,\overline{V}_S$, where S runs through the linear subspace $\mathcal{H}_m$ of $\mathbb{F}_2^T$ generated by the sets of k-rational points of Hermitian hypersurfaces in $M_0^\vee$. Here we identify $\mathbb{F}_2^T$ with the power set 2^T of T. (See Convention (6).) Let H_{m+1} be the vector space over $\mathbb{F}_2$ of Hermitian matrices of size $m+1$. Let $\xi = (\xi_0, \dots, \xi_m)$ be k-rational homogeneous coordinates of $M_0^\vee$. For $A \in H_{m+1}$, let $f_A(\xi, \xi)$ be the cubic homogeneous polynomial $\xi \cdot A \cdot {}^t\xi^{(2)}$, and let Y_A be the Hermitian hypersurface of $M_0^\vee$ defined by $f_A(\xi, \xi) = 0$.

Lemma 5.1. *If $A, A' \in H_{m+1}$, then the subset $Y_A(k) + Y_{A'}(k)$ of T coincides with $T + Y_{A+A'}(k) = T \setminus Y_{A+A'}(k)$. In particular, the map $A \mapsto T + Y_A(k)$ yields a homomorphism $\alpha : H_{m+1} \to \mathbb{F}_2^T$ of vector spaces over $\mathbb{F}_2$.*

Proof. If $a = (a_0, \dots, a_m)$ is a vector with $a_i \in k$, then $f_A(a, a)$ satisfies $f_A(a, a)^2 = f_A(a, a)$, because ${}^tA^{(2)} = A$ and $a^{(4)} = a$. Hence $f_A(a, a)$ is in $\mathbb{F}_2$. Then we have

$$\begin{aligned} a \notin Y_{A+A'}(k) &\iff f_A(a, a) + f_{A'}(a, a) = 1 \iff \\ &(f_A(a, a), f_{A'}(a, a)) = (1, 0) \;\text{ or }\; (0, 1) \iff a \in Y_A(k) + Y_{A'}(k). \end{aligned}$$

Thus the first assertion is proved. The second assertion is now obvious. *q.e.d.*

Lemma 5.2. *Suppose that S is an element of $\mathcal{H}_m$. Then one and only one of the following holds*;

(i) *there is a Hermitian hypersurface Y of $M_0^\vee$ such that $S = Y(k)$, or*
(ii) *there is a Hermitian hypersurface Y of $M_0^\vee$ such that $S = T + Y(k)$.*

Proof. First note that $\mathcal{H}_m$ is stable under the involution $S \mapsto T + S$ of the power set $\mathbb{F}_2^T$, because $T \in \mathcal{H}_m$. Let S be an element of $\mathcal{H}_m$. Then there are Hermitian matrices $A_1, \dots, A_l \in H_{m+1}$ such that $S = Y_{A_1}(k) + \cdots + Y_{A_l}(k)$. By Lemma 5.1, we have

$$(T + Y_{A_1}(k)) + \cdots + (T + Y_{A_l}(k)) = T + Y_{A_1+\cdots+A_l}(k).$$

Thus S is $Y_{A_1+\cdots+A_l}(k)$ if l is odd, while it is $T + Y_{A_1+\cdots+A_l}(k)$ if l is even. Assume that there were two Hermitian matrices $A, A' \in H_{m+1}$ such that $Y_A(k) = T + Y_{A'}(k)$. By Lemma 5.1, it would follow that $Y_{A+A'}(k) = \emptyset$. However any Hermitian hypersurface has at least one k-rational point. Hence we get a contradiction. *q.e.d.*

Lemma 5.3. *Let $A_1, \dots, A_d$ be a basis of H_{m+1} over $\mathbb{F}_2$, where $d = (m+1)^2$. Then T, $Y_{A_1}(k), \dots, Y_{A_d}(k)$ form a basis of $\mathcal{H}_m$.*

Proof. Because $\mathbb{F}_2^\times = \{1\}$, Proposition 2.8 implies that the homomorphism α defined in Lemma 5.1 is injective. The subspace $\mathcal{H}_m$ of $\mathbb{F}_2^T$ is generated by the image of α and T. Because there are no Hermitian matrices $A \in H_{m+1}$ such that $Y_A(k) = \emptyset$, we have $T \notin \operatorname{Im} \alpha$. *q.e.d.*

For a linear code $\mathcal{H} \subseteq \mathbb{F}_2^T$, its weight enumerator is defined as follows:

$$\operatorname{we}(\mathcal{H}) := \sum_{S \in \mathcal{H}} z^{|S|},$$

where z is a formal variable. By Lemma 5.2 combined with Propositions 2.7 and 2.8 and Corollary 2.6, we obtain the following formula.

Corollary 5.4.

$$\operatorname{we}(\mathcal{H}_m) = \sum_{r=0}^{m+1} h(m,r) \cdot (z^{F(m,r)} + z^{|T| - F(m,r)}).$$

Lemma 5.5. *Let $S_1, \dots, S_l$ be elements of $\mathcal{H}_m$. We put $W := S_1 \cap \cdots \cap S_l$. Then $2^l\, \overline{V}_W$ is contained in $\overline{L}^m$.*

Proof. We put $I := \{1, \dots, l\}$. For a positive integer λ with $\lambda \le l$, let $I^{[\lambda]}$ be the set of non-ordered λ-tuples of distinct elements of I. For $\mathbf{i} = \{i_1, \dots, i_\lambda\} \in I^{[\lambda]}$, we put

$$S_{\mathbf{i}} := S_{i_1} + \cdots + S_{i_\lambda}.$$

Note that $2\,\overline{V}_{S_{\mathbf{i}}}$ is an element of $\overline{L}^m$ for any λ and any $\mathbf{i} \in I^{[\lambda]}$. On the other hand, it is easy to see that

$$\sum_{\lambda=1}^{l} (-1)^{\lambda+1} \sum_{\mathbf{i} \in I^{[\lambda]}} \overline{V}_{S_{\mathbf{i}}} = 2^{l-1}\, \overline{V}_W.$$

Thus $2^l\, \overline{V}_W$ is an element of $\overline{L}^m$. *q.e.d.*

Table 6.1. MOG.

μ_1	μ_5	μ_9	μ_{13}	μ_{17}	μ_{21}
μ_2	μ_6	μ_{10}	μ_{14}	μ_{18}	μ_{22}
μ_3	μ_7	μ_{11}	μ_{15}	μ_{19}	μ_{23}
μ_4	μ_8	μ_{12}	μ_{16}	μ_{20}	μ_{24}

We are now ready to prove $\widetilde{\mathrm{pr}}\,(\operatorname{Im}\tilde{u})|_T = \overline{L}^m$. For simplicity, we put

$$\overline{\mathcal{L}}^m(X_J) := \widetilde{\mathrm{pr}}\,(\operatorname{Im}\tilde{u})|_T, \quad \text{and} \quad \bar{u}(\Pi) := \widetilde{\mathrm{pr}}\,(u(\Pi))|_T \in R^T.$$

Then $\overline{\mathcal{L}}^m(X_J)$ is the R-submodule of R^T generated by $\bar{u}(\Pi)$, where Π runs through $\Sigma^m(X_J)$. First we will show that $\overline{\mathcal{L}}^m(X_J)$ contains $\overline{L}^m$. By Table 3.1, we have

$$\bar{u}(M_\infty) = \overline{V}_T.$$

Let Y be a Hermitian hypersurface of rank r in $M_0^\vee$. By Corollary 3.11, there is an element $\Pi \in \Sigma^m(X_J)^{(-1,m-r)}$ such that $C_\infty(\Pi) = Y(k)$ and $C_1(\Pi) = T \setminus Y(k)$. Then we have

$$\bar{u}(M_\infty) + \bar{u}(\Pi) = 2\,\overline{V}_{Y(k)}, \quad \text{and} \quad \bar{u}(M_\infty) - \bar{u}(\Pi) = 2\,\overline{V}_{T+Y(k)}.$$

Using these identities and Lemma 5.2, we see that $\overline{\mathcal{L}}^m(X_J)$ contains all generators of $\overline{L}^m$. Next we show that $\overline{\mathcal{L}}^m(X_J)$ is contained in $\overline{L}^m$. It is enough to show that $\bar{u}(\Pi) \in \overline{L}^m$ for any $\Pi \in \Sigma^m(X_J)$. Note that a k-rational hyperplane K of $M_0^\vee$ is a Hermitian hypersurface of $M_0^\vee$ with rank 1, and hence $K(k) \in \mathcal{H}_m$. Let Π be an element of $\Sigma^m(X_J)^{(a,b)}$. By Corollary 3.11, there is a couple (R, Y) of a k-rational linear subspace R of M_0 with $\dim R = a$, and a Hermitian hypersurface Y in $(M_0/R)^\vee$ such that $C_\infty(\Pi) \sqcup C_1(\Pi) = (M_0/R)^\vee(k)$ and $C_\infty(\Pi) = Y(k)$. Then we have

$$\begin{aligned}\bar{u}(\Pi) &= (-2)^{a+1}\,\overline{V}_{C_\infty(\Pi)} - (-2)^{a+1}\,\overline{V}_{C_1(\Pi)} \\ &= -(-1)^{a+1} \cdot (2^{a+1}\,\overline{V}_{(M_0/R)^\vee(k)} - 2^{a+2}\,\overline{V}_{Y(k)}).\end{aligned}$$

On the other hand, there are k-rational hyperplanes $K_1, \ldots, K_{a+1}$ of $M_0^\vee$ and a Hermitian hypersurface $\tilde{Y}$ of $M_0^\vee$ such that $(M_0/R)^\vee = K_1 \cap \cdots \cap K_{a+1}$ and $Y = K_1 \cap \cdots \cap K_{a+1} \cap \tilde{Y}$. Lemma 5.5 implies that $2^{a+1}\,\overline{V}_{(M_0/R)^\vee(k)}$ and $2^{a+2}\,\overline{V}_{Y(k)}$ are elements of $\overline{L}^m$. Hence $\bar{u}(\Pi)$ is an element of $\overline{L}^m$.

Thus the proof of Theorem 1.4 is completed. *q.e.d.*

Corollary 5.6. *The lattice $\widetilde{L}^m$ is an even lattice with minimal norm at most 2^m.*

Proof. The generators $[\Pi] - [\Pi']$ of $\mathcal{L}^m(X_J)$ have even norms. When $\dim(\Pi \wedge \Pi') = m - 2$, the norm of $[\Pi] - [\Pi']$ is equal to 2^m. *q.e.d.*

6. Edge-Jónsson-McKay correspondence

In this section, we put $m = 2$ and prove Theorem 1.5.

First let us recall the construction of the Leech lattice Λ_{24} and the laminated lattice Λ_{22}. For details, see Conway and Sloane's book [2]. We label the positions of the Miracle Octad Generator (MOG) as in Table 6.1, and put $M := \{\mu_1, \ldots, \mu_{24}\}$. Let $\mathcal{C}_{24} \subset \mathbb{F}_2^M$ be the Golay code. (See [2, Chapter 11, Section 5] for the MOG and the Golay code.) A subset S of M is said to be a $\mathcal{C}$-set if S is an element of $\mathcal{C}_{24}$

Table 6.2. Definition of γ.

$(1:\omega:0)$ $(1:\omega:1)$	$(1:\bar{\omega}:0)$ $(1:\bar{\omega}:1)$	$(1:1:0)$ $(1:1:1)$	$(1:0:0)$ $(1:0:1)$	$(0:1:0)$ $(0:1:1)$	$(0:0:1)$ φ
$(1:\omega:\omega)$ $(1:\omega:\bar{\omega})$	$(1:\bar{\omega}:\omega)$ $(1:\bar{\omega}:\bar{\omega})$	$(1:1:\omega)$ $(1:1:\bar{\omega})$	$(1:0:\omega)$ $(1:0:\bar{\omega})$	$(0:1:\omega)$ $(0:1:\bar{\omega})$	φ φ

under the identification $\mathbb{F}_2^M = 2^M$. We equip $\mathbb{Z}^M$ with a positive definite symmetric bilinear form $(\ ,\ )_M$ defined by

$$(v, w)_M := \frac{1}{8} \sum_{\mu \in M} v(\mu) w(\mu). \tag{6.1}$$

We use [2, Chapter 10, Theorem 25] as a definition of the Leech lattice.

Definition 6.1. The Leech lattice Λ_{24} is the sublattice of $\mathbb{Z}^M$ consisting of vectors $x \in \mathbb{Z}^M$ satisfying the following:

(i) the coordinates $x(\mu_i)$ are all even or all odd,
(ii) for any $\alpha \in \mathbb{Z}/(4)$, the set $\{\mu_i \in M \,:\, x(\mu_i) \bmod 4 = \alpha\}$ is a $\mathcal{C}$-set, and
(iii) if $x(\mu_i)$ are even, then $\sum_{i=1}^{24} x(\mu_i) \bmod 8 = 0$ holds, while if $x(\mu_i)$ are odd, then $\sum_{i=1}^{24} x(\mu_i) \bmod 8 = 4$ holds.

For an abelian group A, we write by $(A^M)_{22}$ the submodule of A^M consisting of functions $a : M \to A$ satisfying $a(\mu_{22}) = a(\mu_{23}) = a(\mu_{24})$. We use [2, Chapter 6, Figure 6.2] as the definition of laminated lattices.

Definition 6.2. The laminated lattice Λ_{22} is defined to be $\Lambda_{24} \cap (\mathbb{Z}^M)_{22}$.

The minimal norm of Λ_{22} is 4 and the kissing number is 49896.

We will construct an isomorphism of lattices between $\widetilde{L}^2$ and Λ_{22}. In the present case $m = 2$, the set $\widetilde{T} = M_0^\vee(k) \sqcup \{\varphi\}$ consists of 22 elements. We define a map $\gamma : M \to \widetilde{T}$ by the MOG diagram given in Table 6.2, where $\omega \in k = \mathbb{F}_4$ is a root of the equation $x^2 + x + 1 = 0$ and $\bar{\omega} = \omega^2$. Then the natural homomorphism $\gamma^* : \mathbb{Z}^{\widetilde{T}} \to \mathbb{Z}^M$ induced by γ yields an isomorphism of $\mathbb{Q}$-lattices $\mathbb{Z}^{\widetilde{T}} \cong (\mathbb{Z}^M)_{22}$, where the symmetric bilinear forms on $\mathbb{Z}^{\widetilde{T}}$ and $\mathbb{Z}^M$ are defined by (1.1) and (6.1), respectively. It is enough to show that $\gamma^*(\widetilde{L}^2)$ coincides with Λ_{22}.

By Corollary 5.4, the weight distribution of the linear code $\mathcal{H}_2 \subset \mathbb{F}_2^T$ is

$$0^1 5^{21} 8^{210} 9^{280} 12^{280} 13^{210} 16^{21} 21^1. \tag{6.2}$$

In particular, we see that $|S| \bmod 4$ is either 0 or 1 for any $S \in \mathcal{H}_2$. By definition, the subspace $(\mathbb{F}_2^M)_{22} \subset \mathbb{F}_2^M$ consists of the subsets $S \subseteq T$ satisfying either $\{\mu_{22}, \mu_{23}, \mu_{24}\} \cap S = \emptyset$ or $\{\mu_{22}, \mu_{23}, \mu_{24}\} \subseteq S$. We define a map $\tilde{\gamma}^* : \mathcal{H}_2 \to (\mathbb{F}_2^M)_{22}$ as follows:

$$\tilde{\gamma}^*(S) := \begin{cases} \gamma^{-1}(S) & \text{if } |S| \bmod 4 = 0, \\ \gamma^{-1}(S) \sqcup \{\mu_{22}, \mu_{23}, \mu_{24}\} & \text{if } |S| \bmod 4 = 1. \end{cases}$$

We put

$$\mathcal{C}_{22} := \mathcal{C}_{24} \cap (\mathbb{F}_2^M)_{22}.$$

The map γ is defined in such a way that the following holds.

The map $\tilde{\gamma}^*$ induces an isomorphism $\mathcal{H}_2 \cong \mathcal{C}_{22}$ of vector spaces over $\mathbb{F}_2$. (6.3)

This claim is proved as follows. We see that $F(2, r) \bmod 4 = 1$ holds for $r = 0, \dots, 3$, where F is the function given in Proposition 2.7. Hence Lemma 5.2 implies that a code word S of $\mathcal{H}_2$ satisfies $|S| \bmod 4 = 0$ if and only if S is of the form $T + Y_A(k)$ for some Hermitian matrix A. Then Lemma 5.1 implies that, for $S_1, S_2 \in \mathcal{H}_2$, we have

$$|S_1 + S_2| \bmod 4 = 0 \quad \Longleftrightarrow \quad (\,|S_1| \bmod 4\ ,\ |S_2| \bmod 4\,) = (0, 0) \text{ or } (1, 1).$$

Hence the map $\tilde{\gamma}^*$ is a linear homomorphism over $\mathbb{F}_2$. We can write down a basis $S_1, \dots, S_{10}$ of $\mathcal{H}_2$ by Lemma 5.3. Using the method described in [2, Chapter 11, Section 5], we can check that $\tilde{\gamma}^*(S_i)$ is a $\mathcal{C}$-set for each S_i. Hence the image of $\tilde{\gamma}^*$ is in $\mathcal{C}_{22}$. It is obvious that $\tilde{\gamma}^*$ is injective. Hence it suffices to show that $\dim_{\mathbb{F}_2} \mathcal{C}_{22}$ is equal to $\dim_{\mathbb{F}_2} \mathcal{H}_2 = 10$. Let N be the subset $\{\mu_1, \dots, \mu_{21}\}$ of M, and $\mathrm{res}^M : (\mathbb{F}_2^M)_{22} \to \mathbb{F}_2^N$ the restriction homomorphism. The kernel of res^M intersects $\mathcal{C}_{22}$ only at the zero vector (that is, the empty set), because there are no non-empty $\mathcal{C}$-sets consisting of three or fewer elements. Therefore $\mathcal{C}_{22}$ and $\mathrm{res}^M(\mathcal{C}_{22})$ are isomorphic as vector spaces over $\mathbb{F}_2$. The weight distribution of the linear code $\mathrm{res}^M(\mathcal{C}_{22})$ can be read from [2, Chapter 10, Tables 10.1 and 10.2], and it coincides with (6.2). Hence we have $\dim_{\mathbb{F}_2} \mathcal{C}_{22} = \dim_{\mathbb{F}_2} \mathrm{res}^M(\mathcal{C}_{22}) = 10$. Thus (6.3) is proved.

Let us consider the following commutative diagram:

$$\begin{array}{ccc}
\mathbb{Z}^{\widetilde{T}} & \xrightarrow[\gamma^*]{\sim} & (\mathbb{Z}^M)_{22} \\
{\scriptstyle \widetilde{\mathrm{pr}}^{\,T}}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{pr}^M} \\
R^{\widetilde{T}} & \xrightarrow[\gamma_R^*]{\sim} & (R^M)_{22},
\end{array}$$

where R is the finite ring $\mathbb{Z}/(8)$ and the vertical arrows are the natural projections. It is easy to see that $\mathrm{Ker}(\mathrm{pr}^M)$ is contained in Λ_{22}. Hence, in order to prove $\gamma^*(\widetilde{L}^2) = \Lambda_{22}$, it is enough to show that $\gamma_R^*((\overline{L}^2)\tilde{\ })$ coincides with $\mathrm{pr}^M(\Lambda_{22})$.

First we show that $\gamma_R^*((\overline{L}^2)\tilde{\ })$ is contained in $\mathrm{pr}^M(\Lambda_{22})$. The R-module $\gamma_R^*((\overline{L}^2)\tilde{\ })$ is generated by $\gamma_R^*((\overline{V}_T)\tilde{\ })$ and $\gamma_R^*(2\,(\overline{V}_S)\tilde{\ })$, where S runs through $\mathcal{H}_2$. The vector $\gamma_R^*((\overline{V}_T)\tilde{\ }) \in (R^M)_{22}$ is given by

$$\gamma_R^*((\overline{V}_T)\tilde{\ })(\mu_i) = \begin{cases} 1 & \text{if } i \le 21, \\ 5 & \text{if } 22 \le i \le 24, \end{cases}$$

which is an element of $\mathrm{pr}^M(\Lambda_{22})$. Suppose that $S \in \mathcal{H}_2$. The value of $2\,(\overline{V}_S)\tilde{\ }$ at the formal element φ is 0 if $|S| \bmod 4 = 0$, while it is 2 if $|S| \bmod 4 = 1$. Hence the set $\{\mu_i \in M\ :\ \gamma_R^*(2\,(\overline{V}_S)\tilde{\ })(\mu_i) \bmod 8 = 2\}$ coincides with $\tilde{\gamma}^*(S)$, which is an element of $\mathcal{C}_{22}$ by (6.3). Hence the vector $v'_S \in (\mathbb{Z}^M)_{22}$ defined by

$$v'_S(\mu_i) := \begin{cases} 0 & \text{if } \mu_i \notin \tilde{\gamma}^*(S), \\ 2 & \text{if } \mu_i \in \tilde{\gamma}^*(S) \end{cases}$$

is a vector of Λ_{22}, which is mapped to $\gamma_R^*(2\,(\overline{V}_S)\tilde{\ })$ by pr^M. Therefore $\gamma_R^*(2\,(\overline{V}_S)\tilde{\ })$ is also an element of $\mathrm{pr}^M(\Lambda_{22})$. Next we show that an arbitrary element $\bar{w}$ of $\mathrm{pr}^M(\Lambda_{22})$ is contained in $\gamma_R^*((\overline{L}^2)\tilde{\ })$. If $\bar{w}(\mu_i) \bmod 2 = 1$, then we replace $\bar{w}$ by

$\bar{w} - \gamma_R^*((\overline{V}_T)\tilde{\ })$ so that we can assume $\bar{w}(\mu_i) \mod 2 = 0$ for any $\mu_i \in M$. The set $\{\mu_i \in M \ :\ \bar{w}(\mu_i) \bmod 4 = 2\}$ is an element of $\mathcal{C}_{22}$. By (6.3), it coincides with $\tilde{\gamma}^*(S)$ for some $S \in \mathcal{H}_2$. Then the element $\bar{w} + \gamma_R^*(2\,(\overline{V}_S)\tilde{\ })$ is contained in the R-submodule

$$\{\ \bar{w}' \in \mathrm{pr}^M(\Lambda_{22}) \ :\ \bar{w}'(\mu_i) \bmod 4 = 0 \ \text{ for all } \ \mu_i \in M\ \}$$

of $(R^M)_{22}$. This submodule is generated by elements $\bar{w}_i$ $(i = 1, \dots, 21)$ defined by

$$\bar{w}_i(\mu_j) := \begin{cases} 4 \bmod 8 & \text{if } j = i \text{ or } j \in \{22, 23, 24\}, \\ 0 \bmod 8 & \text{otherwise.} \end{cases}$$

Hence it suffices to show that these $\bar{w}_i$ belong to $\gamma_R^*((\overline{L}^2)\tilde{\ })$. Let $p_i \in T$ be the k-rational point of $M_0^\vee$ such that $\gamma(\mu_i) = p_i$. There are k-rational lines l and l' on $M_0^\vee$ such that $l \cap l' = \{p_i\}$. Because $l(k)$, $l'(k)$ and $l(k) + l'(k)$ are elements of $\mathcal{H}_2$, and because $\bar{w}_i$ is written as

$$\bar{w}_i = \gamma_R^*(2\,(\overline{V}_{l(k)})\tilde{\ } + 2\,(\overline{V}_{l'(k)})\tilde{\ } - 2\,(\overline{V}_{l(k)+l'(k)})\tilde{\ }),$$

we have $\bar{w}_i \in \gamma_R^*((\overline{L}^2)\tilde{\ })$. *q.e.d.*

7. Discriminant, minimal norm and kissing number of $\widetilde{L}^3$

In this section, we prove Theorem 1.6.

First we will present a method for estimating $\mathrm{disc}(\widetilde{L}^m)$ from above. This method yields $\mathrm{disc}(\widetilde{L}^3) = 2^{16} \cdot 3$ stated in Theorem 1.6.

The discriminant of the $\mathbb{Q}$-lattice $\mathbb{Z}^{\widetilde{T}}$ with the symmetric bilinear form $(\ ,\ )_T$ given by (1.1) is $2^{-(m+1)(|T|+1)} \cdot 3$. The index of $\widetilde{L}^m$ in $\mathbb{Z}^{\widetilde{T}}$ is

$$|R^{\widetilde{T}}/(\overline{L}^m)\tilde{\ }| = 2^{(m+1)(|T|+1)}/\,|\overline{L}^m|,$$

because $(\overline{L}^m)\tilde{\ }$ and $\overline{L}^m$ are isomorphic as R-modules. Hence we have

$$\mathrm{disc}(\widetilde{L}^m) = \mathrm{disc}(\mathbb{Z}^{\widetilde{T}}) \cdot [\mathbb{Z}^{\widetilde{T}} : \widetilde{L}^m]^2 = 3 \cdot 2^{(m+1)(|T|+1)}/\,|\overline{L}^m|^2. \tag{7.1}$$

For a non-negative integer n with $n \le m+1$, let ϕ^n be the natural projection from $R^T = (\mathbb{Z}/(2^{m+1}))^T$ to $(\mathbb{Z}/(2^n))^T$. We put

$$(\overline{L}^m)^n := \mathrm{Ker}\,\phi^n \cap \overline{L}^m.$$

Then we obtain a decreasing filtration

$$\overline{L}^m = (\overline{L}^m)^0 \supseteq (\overline{L}^m)^1 \supseteq (\overline{L}^m)^2 \supseteq \cdots \supseteq (\overline{L}^m)^m \supseteq (\overline{L}^m)^{m+1} = 0$$

of $\overline{L}^m$. There is a natural identification of $\mathrm{Ker}\,\phi^n/\,\mathrm{Ker}\,\phi^{n+1}$ with $\mathbb{F}_2^T$. Using this identification, we define a linear code $\mathcal{C}^{\,m}(n) \subseteq \mathbb{F}_2^T$ by

$$\mathcal{C}^{\,m}(n) := (\overline{L}^m)^n/(\overline{L}^m)^{n+1}.$$

Then we have

$$|\,\overline{L}^m\,| = \prod_{n=0}^{m} |\,\mathcal{C}^{\,m}(n)|. \tag{7.2}$$

An element α of R is uniquely written in the form

$$\alpha = r_0(\alpha) + 2\,r_1(\alpha) + 4\,r_2(\alpha) + \cdots + 2^m\,r_m(\alpha),$$

TABLE 7.1. $\dim_{\mathbb{F}_2} \mathcal{H}_m(n)$.

$m \setminus n$	0	1	2	3	4	5
3	1	17	61	85		
4	1	26	146	296	341	
5	1	37	302	882	1289	1365

where $r_i(\alpha) \in \{0,1\}$. Hence, for any vector $\bar{v} \in R^T$, there is a unique sequence $U_0(\bar{v}), U_1(\bar{v}), \dots, U_m(\bar{v})$ of subsets of T such that

$$\bar{v} = \overline{V}_{U_0(\bar{v})} + 2\,\overline{V}_{U_1(\bar{v})} + 4\,\overline{V}_{U_2(\bar{v})} + \cdots + 2^m\,\overline{V}_{U_m(\bar{v})}. \tag{7.3}$$

Note that a vector $\bar{v}$ of $\overline{L}^m$ is contained in $(\overline{L}^m)^n$ if and only if $U_0(\bar{v}) = \cdots = U_{n-1}(\bar{v}) = \emptyset$, and that, if $\bar{v} \in (\overline{L}^m)^n$, then the image of $\bar{v}$ in $\mathcal{C}^m(n)$ by the natural projection $(\overline{L}^m)^n \to \mathcal{C}^m(n)$ is $U_n(\bar{v})$. It is easy to see from the definition of $\overline{L}^m$ that $\mathcal{C}^m(0) = \{\emptyset, T\}$. For a positive integer l, let $\mathcal{H}_m(l) \subseteq \mathbb{F}_2^T$ be the linear code generated by the subsets

$$S_1 \cap \cdots \cap S_l \qquad (S_1, \dots, S_l \in \mathcal{H}_m)$$

of T. We have $\mathcal{H}_m(1) = \mathcal{H}_m$. We put $\mathcal{H}_m(0) := \mathcal{C}^m(0) = \{\emptyset, T\}$.

Lemma 7.1. *If $\bar{v} \in \overline{L}^m$, then $U_i(\bar{v})$ is a member of $\mathcal{H}_m(2^{i-1})$ for each i.*

Proof. A vector $\bar{v}$ of $\overline{L}^m$ is written in the form

$$\bar{v} = \overline{V}_{U_0(\bar{v})} + 2\,\overline{V}_{S_1} + \cdots + 2\,\overline{V}_{S_N}, \tag{7.4}$$

where $U_0(\bar{v}) \in \mathcal{C}^m(0) = \{\emptyset, T\}$ and $S_1, \dots, S_N \in \mathcal{H}_m$. Using the formula

$$2^l\,\overline{V}_S + 2^l\,\overline{V}_{S'} = 2^l\,\overline{V}_{S+S'} + 2^{l+1}\,\overline{V}_{S\cap S'}$$

and

$$(S + S') \cap S'' = (S \cap S'') + (S' \cap S'') \tag{7.5}$$

recursively, we can rewrite (7.4) into the form (7.3), where $U_i(\bar{v}) \in \mathcal{H}_m(2^{i-1})$. *q.e.d.*

Lemma 7.2. *For a positive integer n with $n \le m$, we have $\mathcal{H}_m(n) \subseteq \mathcal{C}^m(n) \subseteq \mathcal{H}_m(2^{n-1})$. In particular, the subcode $\mathcal{H}_m(1)$ coincides with $\mathcal{C}^m(1)$ and the subcode $\mathcal{H}_m(2)$ coincides with $\mathcal{C}^m(2)$. Moreover, we have $\mathcal{H}_m(m) = \mathcal{C}^m(m) = \mathbb{F}_2^T$.*

Proof. The inclusion $\mathcal{H}_m(n) \subseteq \mathcal{C}^m(n)$ follows from Lemma 5.5. The inclusion $\mathcal{C}^m(n) \subseteq \mathcal{H}_m(2^{n-1})$ follows from Lemma 7.1. If K is a k-rational hyperplane of $M_0^\vee$, then the subset $K(k)$ of T is a member of $\mathcal{H}_m$. Any k-rational point of $M_0^\vee$ is expressed as the intersection of k-rational hyperplanes $K_1, \dots, K_m$ of $M_0^\vee$. Hence $\{H\}$ is a code word of $\mathcal{H}_m(m)$ for any $H \in T$, which implies that $\mathcal{H}_m(m) = \mathbb{F}_2^T$. *q.e.d.*

By Lemma 5.3, we can write down a basis of $\mathcal{H}_m(1)$, which consists of N subsets $B_1, \dots, B_N$ of T, where $N := (m+1)^2 + 1$. Suppose that a basis $B'_1, \dots, B'_M$ of $\mathcal{H}_m(n)$ is given. Because of the formula (7.5), we see that $\mathcal{H}_m(n+1)$ is generated by the subsets $B_i \cap B'_j$, where $i = 1, \dots, N$ and $j = 1, \dots, M$. Hence we can pick up a basis of $\mathcal{H}_m(n+1)$ from these NM subsets using a simple linear algebra over $\mathbb{F}_2$. By this inductive method, we obtain Table 7.1 of $\dim_{\mathbb{F}_2} \mathcal{H}_m(n)$ for $m \le 5$. Combining Table 7.1 with (7.1), (7.2) and Lemma 7.2, we obtain the following:

$$\begin{aligned}
\operatorname{disc}(\widetilde{L}^3) &= 2^{16}\cdot 3,\\
\operatorname{disc}(\widetilde{L}^4) &= 2^{\nu(4)}\cdot 3 \quad\text{with}\quad \nu(4)\le 90,\\
\operatorname{disc}(\widetilde{L}^5) &= 2^{\nu(5)}\cdot 3 \quad\text{with}\quad \nu(5)\le 444.
\end{aligned}$$

Next we consider the minimal norm and the kissing number of $\widetilde{L}^3$. We put $m = 3$ and $R = \mathbb{Z}/(16)$. Let $\operatorname{ws}(\mathcal{H}_3(n))$ be the set $\{|S| : S \in \mathcal{H}_3(n)\}$ of weights of the code words of $\mathcal{H}_3(n)$. By Corollary 5.4, the weight enumerator $\operatorname{we}(\mathcal{H}_3(1))$ and hence the weight set $\operatorname{ws}(\mathcal{H}_3(1))$ are easily calculated:

$$\begin{aligned}
\operatorname{we}(\mathcal{H}_3(1)) =& z^{85} + 85\, z^{64} + 3570\, z^{53} + 23800\, z^{48} + 38080\, z^{45} +\\
&+ 38080\, z^{40} + 23800\, z^{37} + 3570\, z^{32} + 85\, z^{21} + 1,\\
\operatorname{ws}(\mathcal{H}_3(1)) =& \{0, 21, 32, 37, 40, 45, 48, 53, 64, 85\}.
\end{aligned}$$

We can calculate $\operatorname{ws}(\mathcal{H}_3(2))$ as follows. Let $\mathbb{F}_2^T$ be equipped with a non-degenerate symmetric bilinear form $(S, S') := |S \cap S'| \bmod 2$. The orthogonal complement $\mathcal{H}_3(2)^\perp$ of $\mathcal{H}_3(2)$ in $\mathbb{F}_2^T$ is of dimension $85 - 61 = 24$. Because we have calculated a basis of $\mathcal{H}_3(2)$, it is easy to obtain a basis of $\mathcal{H}_3(2)^\perp$. The weight enumerator of $\mathcal{H}_3(2)^\perp$ can be calculated by brute strength using a computer, because it has relatively small dimension. The weight enumerator of $\mathcal{H}_3(2)$ is related to that of $\mathcal{H}_3(2)^\perp$ via the MacWilliams formula. (See, for example, van Lint [17, p. 39, Theorem 3.5.3].) The result is as follows:

$$\begin{gathered}
\operatorname{we}(\mathcal{H}_3(2)) := z^{85} + 357\, z^{80} + 17850\, z^{77} + 23800\, z^{76} + 45696\, z^{75} + 1142400\, z^{74} +\\
\cdots\\
19007943360\, z^{17} + 4668633585\, z^{16} + 1074247680\, z^{15} + 229785600\, z^{14} + 44666650\, z^{13} +\\
8020600\, z^{12} + 1142400\, z^{11} + 45696\, z^{10} + 23800\, z^{9} + 17850\, z^{8} + 357\, z^{5} + 1.
\end{gathered}$$

In particular, we have

$$\operatorname{ws}(\mathcal{H}_3(2)) = \{0, 1, 2, \dots, 85\} \setminus \{1, 2, 3, 4, 6, 7, 78, 79, 81, 82, 83, 84\}.$$

The group $G_J^{0\infty} \cong GL(4, k)$ acts on $M_0^\vee$ projectively over k, and hence on the codes $\mathcal{H}_3(1)$ and $\mathcal{H}_3(2)$. Recall that every code word of $\mathcal{H}_3 \cong \mathcal{H}_3(1)$ is either the set of k-rational points of a Hermitian surface in $M_0^\vee \cong \mathbb{P}^3$ or its complement. (Lemma 5.2.) By Corollary 2.6, the action is transitive on the set of code words of a given weight in $\mathcal{H}_3(1)$. The upper half of Table 7.2 shows the number of Hermitian surfaces S of each rank and the weight of corresponding code words $S(k)$ and $M_0^\vee(k) \setminus S(k)$.

Note that the number 357 of the code words of weight 5 in $\mathcal{H}_3(2)$ is equal to the number of k-rational lines in $M_0^\vee$. Because any k-rational line ℓ can be expressed as an intersection of two k-rational planes and $\ell(k)$ has five points, a code word of weight 5 is a member of $\mathcal{H}_3(2)$ if and only if it is the set of k-rational points of a k-rational line. The lower half of Table 7.2 shows the number of k-rational lines ℓ that intersect at distinct points of a given number with a Hermitian surface S of a fixed rank.

Suppose that a non-zero vector v of $\widetilde{L}^3$ contained in the kernel of the natural projection $\widetilde{\mathrm{pr}} : \widetilde{L}^3 \to \widetilde{R^T}$ is given. Then we have $(v, v)_T \ge 16$, and hence v cannot be a minimal non-zero vector.

TABLE 7.2. Number of Hermitian surfaces and lines.

rank of S	0	1	2	3	4
$\lvert S(k)\rvert$	85	21	53	37	45
$\lvert M_0^{\vee}(k) \setminus S(k)\rvert$	0	64	32	48	40
number of S	1	85	3570	23800	38080
$\lvert S(k) \cap \ell(k)\rvert$	number of ℓ				
0	0	0	0	0	0
1	0	336	40	156	90
2	0	0	0	0	0
3	0	0	256	192	240
4	0	0	0	0	0
5	357	21	61	9	27

For an element α of R, let $\langle \alpha \rangle$ be the unique integer such that $-8 < \langle \alpha \rangle \le 8$ and $\langle \alpha \rangle \bmod 16 = \alpha$. For an element $\bar{w} \in \overline{L}^3$, let $\langle \bar{w}^{\sim} \rangle \in \widetilde{L}^3$ be the vector defined by

$$\langle \bar{w}^{\sim} \rangle(H) := \langle \bar{w}(H) \rangle \quad \text{for} \quad H \in T \quad \text{and} \qquad \langle \bar{w}^{\sim} \rangle(\varphi) := \Big\langle \sum_{H \in T} \bar{w}(H) \Big\rangle.$$

It is obvious that $\langle \bar{w}^{\sim} \rangle$ is one of the vectors of minimal norm in $\widetilde{\mathrm{pr}}^{-1}(\bar{w}^{\sim})$. (If the number of $H \in \widetilde{T}$ such that $\bar{w}(H) = 8$ is ν, then the set of the vectors of minimal norm in $\widetilde{\mathrm{pr}}^{-1}(\bar{w}^{\sim})$ consists of 2^{ν} elements.) The vector $\bar{w}$ is written in one of the following forms:

$$\begin{aligned} \bar{w} &= \overline{V}_T + 2\,\overline{V}_{U_1(\bar{w})} + 4\,\overline{V}_{U_2(\bar{w})} + 8\,\overline{V}_{U_3(\bar{w})} \quad \text{or} \\ \bar{w} &= 2\,\overline{V}_{U_1(\bar{w})} + 4\,\overline{V}_{U_2(\bar{w})} + 8\,\overline{V}_{U_3(\bar{w})}, \end{aligned}$$

where $U_i(\bar{w}) \in \mathcal{H}_3(2^{i-1})$ for $i = 1, 2, 3$ are the code words given by Lemma 7.1. We say that $\bar{w}$ is *odd* or *even* according to whether $\bar{w}$ is written in the first form or in the second form. Because $\overline{V}_T \in \overline{L}^3$, if $\bar{w} \in \overline{L}^3$ is odd, then the even vector

$$\bar{w} + \overline{V}_T = 2\,\overline{V}_{T+U_1(\bar{w})} + 4\,\overline{V}_{U_1(\bar{w})+U_2(\bar{w})} + 8\,\overline{V}_{U_3(\bar{w})+U_1(\bar{w})\cap U_2(\bar{w})}$$

is also contained in $\overline{L}^3$, while if $\bar{w} \in \overline{L}^3$ is even, then the even vector

$$\bar{w} + 2\,\overline{V}_T = 2\,\overline{V}_{T+U_1(\bar{w})} + 4\,\overline{V}_{U_1(\bar{w})+U_2(\bar{w})} + 8\,\overline{V}_{U_3(\bar{w})+U_1(\bar{w})\cap U_2(\bar{w})}$$

is also contained in $\overline{L}^3$. We define the function $\delta_{\bar{w}} : R \to \mathbb{Z}_{\ge 0}$ by

$$\delta_{\bar{w}}(\alpha) := |\{ H \in T \;:\; \bar{w}(H) = \alpha \}|.$$

For any function $\delta : R \to \mathbb{Z}_{\ge 0}$, we put

$$N(\delta) := \frac{1}{16} \Big(\sum_{\alpha \in R} \langle \alpha \rangle^2 \delta(\alpha) + 3 \Big\langle \sum_{\alpha \in R} \alpha\, \delta(\alpha) \Big\rangle^2 \Big).$$

Then the norm of $\langle \bar{w}^{\sim} \rangle \in \widetilde{L}^3$ is equal to $N(\delta_{\bar{w}})$.

Suppose that a function $\delta : R \to \mathbb{Z}_{\ge 0}$ is equal to $\delta_{\bar{w}}$ for some non-zero element $\bar{w} \in \overline{L}^3$. Then δ must satisfy the following conditions.

(1) The sum $\sum_{\alpha\in R}\delta(\alpha)$ is equal to 85, and $\delta(0) < 85$. Moreover, we have $\delta(\alpha) = 0$ for all even α if $\bar{w}$ is odd, while $\delta(\alpha) = 0$ for all odd α if $\bar{w}$ is even.

(2) The integer $|U_1(\bar{w})|$ appears in $\mathrm{ws}(\mathcal{H}_3(1))$, where

$$|U_1(\bar{w})| = \begin{cases} \delta(3)+\delta(7)+\delta(11)+\delta(15) & \text{if } \bar{w} \text{ is odd,} \\ \delta(2)+\delta(6)+\delta(10)+\delta(14) & \text{if } \bar{w} \text{ is even.} \end{cases}$$

(3) The integer $|U_2(\bar{w})|$ appears in $\mathrm{ws}(\mathcal{H}_3(2))$, where

$$|U_2(\bar{w})| = \begin{cases} \delta(5)+\delta(7)+\delta(13)+\delta(15) & \text{if } \bar{w} \text{ is odd,} \\ \delta(4)+\delta(6)+\delta(12)+\delta(14) & \text{if } \bar{w} \text{ is even.} \end{cases}$$

(4) The following integer appears in $\mathrm{ws}(\mathcal{H}_3(2))$:

$$\begin{cases} |U_2(\bar{w}+\overline{V}_T)| = |U_1(\bar{w})+U_2(\bar{w})| = \delta(3)+\delta(5)+\delta(11)+\delta(13) & \text{if } \bar{w} \text{ is odd,} \\ |U_2(\bar{w}+2\,\overline{V}_T)| = |U_1(\bar{w})+U_2(\bar{w})| = \delta(2)+\delta(4)+\delta(10)+\delta(12) & \text{if } \bar{w} \text{ is even.} \end{cases}$$

(5) The norm $N(\delta) = (\langle \bar{w}\tilde{\ }\rangle, \langle \bar{w}\tilde{\ }\rangle)_T$ is an even integer.

We list up all the functions $\delta : R \to \mathbb{Z}_{\geq 0}$ that satisfy the conditions (1)-(5) and $N(\delta) \leq 8$. There are no such functions δ with $N(\delta) \leq 4$. The list of δ with $N(\delta) = 6$ or $N(\delta) = 8$ is given in Table 7.3, where the function δ is expressed by the concatenation of $\alpha^{\delta(\alpha)}$ ($\alpha \in R$) with $\delta(\alpha) > 0$. The third column of Table 7.3 indicates the number $\nu(\delta)$ of the vectors $w \in \widetilde{L}^3$ such that $\delta_{\bar{w}} = \delta$ and $(w,w)_T = N(\delta)$, where $\bar{w}$ is the restriction of $\widetilde{\mathrm{pr}}\,(w) \in R^{\widetilde{T}}$ to T.

In order to calculate $\nu(\delta)$, we need the following lemma. Let A be a subset of $M_0^\vee(k)$. We define $\mathcal{H}_3(2, A)$ to be the linear subcode of $\mathcal{H}_3(2)$ consisting of all the code words of $\mathcal{H}_3(2)$ that are contained in A.

Lemma 7.3. (1) *Let P be a k-rational plane of $M_0^\vee$, and p and q two distinct points of $M_0^\vee(k) \setminus P(k)$. Then we have*

$$\mathcal{H}_3(2, P(k) \sqcup \{p, q\}) = \mathcal{H}_3(2, P(k)).$$

The weight enumerator of $\mathcal{H}_3(2, P(k))$ is

$$z^{21} + 21\,z^{16} + 210\,z^{13} + 280\,z^{12} + 280\,z^{9} + 210\,z^{8} + 21\,z^{5} + 1.$$

(2) *Let A be a code word of $\mathcal{H}_3(1)$ with weight* 32; *that is, A is $M_0^\vee(k) \setminus S(k)$ where S is a Hermitian surface of rank* 2. *Then the weight enumerator of $\mathcal{H}_3(2, A)$ is*

$$z^{32} + 140\,z^{24} + 3520\,z^{20} + 9062\,z^{16} + 3520\,z^{12} + 140\,z^{8} + 1.$$

Proof. The action of the group $G_J^{0\infty} \cong GL(4, k)$ on $M_0^\vee$ is transitive on the set of k-rational planes of $M_0^\vee$, and the stabilizer subgroup of a k-rational plane P_0 acts 2-transitively on $M_0^\vee(k) \setminus P_0(k)$. Hence it is enough to check the assertion (1) only for one choice of P_0 and p, q. Since we have already obtained a basis of $\mathcal{H}_3(2)$, this checking can be easily done by a computer. In fact, we see that $\mathcal{H}_3(2, P(k))$ is isomorphic to $\mathcal{H}_2(1)$. A similar argument can be applied to the assertion (2). *q.e.d.*

We will demonstrate how to calculate $\nu(\delta)$ on several examples.

Example 1. $\delta = 2^{11}14^{10}$ (No. 0). If $\delta = \delta_{\bar{w}}$, then $|U_1(\bar{w})| = 21$ and hence $U_1(\bar{w})$ should coincide with $P(k)$ for some k-rational plane P. Then $U_2(\bar{w})$ is a code

Table 7.3. Kissing numbers.

Norm 6

No.	δ	$\nu(\delta)$
0	$2^{11}14^{10}$	0
1	$2^{10}14^{11}$	0

Norm 8: even

No.	δ	$\nu(\delta)$
2	$0^{80}14^{32}$	3570
3	$0^{80}12^{5}$	357
4	$0^{77}12^{8}$	17850
5	$0^{83}8^{2}$	14280
6	$0^{64}6^{1}14^{20}$	1785
7	$0^{80}4^{1}12^{4}$	1785
8	$0^{80}4^{2}12^{3}$	3570
9	$0^{77}4^{2}12^{6}$	499800
10	$0^{80}4^{3}12^{2}$	3570
11	$0^{80}4^{4}12^{1}$	1785
12	$0^{77}4^{4}12^{4}$	1249500
13	$0^{80}4^{5}$	357
14	$0^{77}4^{6}12^{2}$	499800
15	$0^{77}4^{8}$	17850
16	$0^{62}2^{3}4^{1}12^{1}14^{18}$	0
17	$0^{64}2^{4}10^{1}14^{16}$	8925
18	$0^{64}2^{5}6^{1}14^{15}$	28560
19	$0^{62}2^{6}4^{1}12^{1}14^{15}$	0
20	$0^{64}2^{7}10^{1}14^{13}$	142800
21	$0^{62}2^{7}4^{1}12^{1}14^{14}$	0
22	$0^{53}2^{8}14^{24}$	499800
23	$0^{62}2^{8}12^{2}14^{13}$	0
24	$0^{64}2^{8}10^{1}14^{12}$	214200
25	$0^{64}2^{8}6^{1}14^{12}$	232050
26	$0^{62}2^{8}4^{2}14^{13}$	0

No.	δ	$\nu(\delta)$
27	$0^{62}2^{9}12^{2}14^{12}$	0
28	$0^{64}2^{9}6^{1}14^{11}$	285600
29	$0^{62}2^{9}4^{2}14^{12}$	0
30	$0^{62}2^{10}4^{1}12^{1}14^{11}$	0
31	$0^{64}2^{11}10^{1}14^{9}$	285600
32	$0^{62}2^{11}4^{1}12^{1}14^{10}$	0
33	$0^{53}2^{12}14^{20}$	12566400
34	$0^{62}2^{12}12^{2}14^{9}$	0
35	$0^{64}2^{12}10^{1}14^{8}$	232050
36	$0^{64}2^{12}6^{1}14^{8}$	214200
37	$0^{62}2^{12}4^{2}14^{9}$	0
38	$0^{62}2^{13}12^{2}14^{8}$	0
39	$0^{64}2^{13}6^{1}14^{7}$	142800
40	$0^{62}2^{13}4^{2}14^{8}$	0
41	$0^{62}2^{14}4^{1}12^{1}14^{7}$	0
42	$0^{64}2^{15}10^{1}14^{5}$	28560
43	$0^{62}2^{15}4^{1}12^{1}14^{6}$	0
44	$0^{53}2^{16}14^{16}$	32351340
45	$0^{64}2^{16}6^{1}14^{4}$	8925
46	$0^{62}2^{18}4^{1}12^{1}14^{3}$	0
47	$0^{53}2^{20}14^{12}$	12566400
48	$0^{64}2^{20}10^{1}$	1785
49	$0^{53}2^{24}14^{8}$	499800
50	$0^{53}2^{32}$	3570

Norm 8: odd

No.	δ	$\nu(\delta)$
51	$3^{5}15^{80}$	357
52	$1^{16}13^{5}15^{64}$	1785
53	$1^{18}3^{2}13^{3}15^{62}$	0
54	$1^{20}3^{4}13^{1}15^{60}$	28560
55	$1^{28}3^{1}13^{4}15^{52}$	142800
56	$1^{30}3^{3}13^{2}15^{50}$	913920
57	$1^{32}13^{5}15^{48}$	214200
58	$1^{32}3^{5}15^{48}$	217770
59	$1^{34}3^{2}13^{3}15^{46}$	4569600
60	$1^{36}3^{1}13^{4}15^{44}$	3427200
61	$1^{36}3^{4}13^{1}15^{44}$	3712800
62	$1^{38}3^{3}13^{2}15^{42}$	9139200
63	$1^{40}13^{5}15^{40}$	1028160

No.	δ	$\nu(\delta)$
64	$1^{40}3^{5}15^{40}$	1028160
65	$1^{42}3^{2}13^{3}15^{38}$	9139200
66	$1^{44}3^{1}13^{4}15^{36}$	3712800
67	$1^{44}3^{4}13^{1}15^{36}$	3427200
68	$1^{46}3^{3}13^{2}15^{34}$	4569600
69	$1^{48}13^{5}15^{32}$	217770
70	$1^{48}3^{5}15^{32}$	214200
71	$1^{50}3^{2}13^{3}15^{30}$	913920
72	$1^{52}3^{4}13^{1}15^{28}$	142800
73	$1^{60}3^{1}13^{4}15^{20}$	28560
74	$1^{62}3^{3}13^{2}15^{18}$	0
75	$1^{64}3^{5}15^{16}$	1785
76	$1^{80}13^{5}$	357

word of $\mathcal{H}_3(2, P(k))$ with weight 10. However there are no such code words by Lemma 7.3, and hence

$$\nu(2^{11}14^{10}) = 0.$$

Example 2. $\delta = 0^{83}8^2$ (No. 5). The code $\mathcal{H}_3(3)$ coincides with $\mathbb{F}_2^T$. Hence there are $\binom{85}{2}$ elements $\bar{w}$ of $\overline{L}^3$ such that $\delta = \delta_{\bar{w}}$. For each such $\bar{w}$, there are four vectors $w \in \widetilde{L}^3$ such that $\widetilde{\mathrm{pr}}\,(w)|_T = \bar{w}$ and $(w, w)_T = 8$, because we can lift $8 \in R$ to either $8 \in \mathbb{Z}$ or $-8 \in \mathbb{Z}$. Hence we have

$$\nu(0^{83}8^2) = \binom{85}{2} \cdot 4 = 14280.$$

Example 3. $\delta = 0^{77}4^4 12^4$ (No. 12). Suppose that $\delta = \delta_{\bar{w}}$. There is only one $w \in \widetilde{L}^3$ such that $\widetilde{\mathrm{pr}}\,(w)|_T = \bar{w}$ and $(w, w)_T = 8$. In such a situation, we say that the lift of $\bar{w}$ is unique. The code word $U_2(\bar{w})$ is one of 17850 code words of weight 8 in $\mathcal{H}_3(2)$ and, for each such code word, there are $\binom{8}{4}$ choices of $U_3(\bar{w}) \subset U_2(\bar{w})$. Hence

$$\nu(0^{77}4^4 12^4) = 17850 \cdot \binom{8}{4} = 1249500.$$

Example 4. $\delta = 0^{62}2^3 4^1 12^1 14^{18}$ (No. 16). Suppose that $\delta = \delta_{\bar{w}}$. The lift of $\bar{w}$ is unique. Since $|U_1(\bar{w})| = 21$, $U_1(\bar{w})$ is equal to $P(k)$ for some k-rational plane P. The code word $U_2(\bar{w})$ of weight 20 must satisfy $|U_2(\bar{w}) \setminus P(k)| = 2$. There are no such code words by Lemma 7.3. Hence

$$\nu(0^{62}2^3 4^1 12^1 14^{18}) = 0.$$

Example 5. $\delta = 0^{53}2^{16}14^{16}$ (No. 44). Suppose that $\delta = \delta_{\bar{w}}$. The lift of $\bar{w}$ is unique. The code word $U_1(\bar{w})$ is one of 3570 code words of weight 32 in $\mathcal{H}_3(1)$. The code word $U_2(\bar{w})$ is an element of $\mathcal{H}_3(2, U_1(\bar{w}))$ with weight 16. There are 9062 such code words by Lemma 7.3. The code word $U_3(\bar{w})$ must be equal to $U_2(\bar{w})$. Hence

$$\nu(0^{53}2^{16}14^{16}) = 3570 \cdot 9062 = 32351340.$$

Example 6. $\delta = 1^{38}3^3 13^2 15^{42}$ (No. 62). Suppose that $\delta = \delta_{\bar{w}}$. The lift of $\bar{w}$ is unique. We put $\bar{v} = \bar{w} + \overline{V}_T$. Then $\delta_{\bar{v}} = 2^{38}4^3 14^2$. The code word $U_1(\bar{v})$ is one of 38080 code words of weight 40 in $\mathcal{H}_3(1)$. The code word $U_2(\bar{v})$ is an element of $\mathcal{H}_3(2)$ with weight 5, and hence there is a k-rational line ℓ such that $U_2(\bar{v}) = \ell(k)$. This line ℓ must intersect with $U_1(\bar{v})$ at distinct two points. There are 240 such lines by Table 7.2. The code word $U_3(\bar{v})$ must be equal to $U_1(\bar{v}) \cap U_2(\bar{v})$. Hence

$$\nu(1^{38}3^3 13^2 15^{42}) = 38080 \cdot 240 = 9139200.$$

Now we see that there are no non-zero vectors $w \in \widetilde{L}^3$ with $(w, w)_T < 8$, and the kissing number of $\widetilde{L}^3$ is

$$\sum \nu(\delta) = 109421928.$$

q.e.d.

8. Concluding remarks

Let X be the cubic Fermat hypersurface of dimension $2m$ in characteristic 2. The lattice $\mathcal{L}^m(X)$ has geometrically natural generators $[\Pi]-[\Pi']$ $(\Pi, \Pi' \in \Sigma^m(X))$. The norm of these generators is at least 2^m, and the minimal value 2^m is attained if and only if $\dim(\Pi \wedge \Pi') = m - 2$. Using induction on m, we see that, for each

$A \in \Sigma^{m-2}(X)$, there are $27 \cdot 16 = 432$ ordered pairs Π, Π' such that $\Pi \wedge \Pi' = A$. Hence there are $27 \cdot 16 \cdot |\Sigma^{m-2}(X)|$ ordered pairs Π, Π' such that

$$([\Pi] - [\Pi'], [\Pi] - [\Pi'])_{\mathcal{L}} = 2^m.$$

For $m = 1, 2, 3$, the number $|\Sigma^{m-2}(X)|$ is equal to 1, 693 and 1519749, respectively. On the other hand, for each vector $v = [\Pi_1] - [\Pi'_1]$ with $(v, v)_{\mathcal{L}} = 2^m$, there are at least six ordered pairs Π_i, Π'_i $(i = 1, \ldots, 6)$ such that $v = [\Pi_i] - [\Pi'_i]$ holds. Indeed, there are five elements $\Xi_2, \ldots, \Xi_6$ of $\Sigma^m(X)$ such that $\dim(\Pi_1 \wedge \Xi_i) = \dim(\Pi'_1 \wedge \Xi_i) = m - 1$. Let Π'_i be the unique element of $\Sigma^m(X)$ that is distinct from Π_1 and Ξ_i and contains $\Pi_1 \wedge \Xi_i$, and Π_i the unique element of $\Sigma^m(X)$ that is distinct from Π'_1 and Ξ_i and contains $\Pi'_1 \wedge \Xi_i$. Both of $[\Pi_1] + [\Pi'_i] + [\Xi_i]$ and $[\Pi'_1] + [\Pi_i] + [\Xi_i]$ are equal to the numerical equivalence class h by Corollary 3.3. Hence we have $v = [\Pi_i] - [\Pi'_i]$ for $i = 1, \ldots, 6$.

We have obtained the following.

Observation. For $m = 1, 2, 3$, the minimal norm of $\mathcal{L}^m(X)$ is 2^m and the kissing number is equal to

$$(27 \cdot 16 \cdot |\Sigma^{m-2}(X)|)/6 = 72 \cdot |\Sigma^{m-2}(X)|.$$

We may therefore expect that the same formulae continue to be valid for $m \geq 4$.

References

[1] A. Beauville, 'Sur les hypersurfaces dont les sections hyperplanes sont à module constant, With an appendix by D. Eisenbud and C. Huneke', *The Grothendieck Festschrift, Vol. I*, (ed. P. Cartier, L. Illusie, N. M. Katz, G. Laumon, Yu. Manin and K. A. Ribet), Progress in Mathematics. 86 (Birkhäuser, Boston, 1990) 121–133.

[2] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups,* Second edition, with additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften, 290 (Springer, Berlin, 1993).

[3] N. Dummigan and Pham Huu Tiep, 'Lower bounds for the minima of certain symplectic and unitary group lattices', *Amer. J. Math.* 121 (1999) 889–918.

[4] W. L. Edge, 'Permutation representations of a group of order 9,196,830,720', *J. London Math. Soc.* (2) 2 (1970) 753–762.

[5] N. D. Elkies, 'Mordell-Weil lattices in characteristic 2. I. Construction and first properties', *Internat. Math. Res. Notices.* (1994) no. 8, 343 ff., approx. 18 pp. (electronic).

[6] N. D. Elkies, 'Mordell-Weil lattices in characteristic 2. II. The Leech lattice as a Mordell-Weil lattice', *Invent. Math.* 128 (1997) 1–8.

[7] W. Fulton, *Intersection theory.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 2 (Springer, Berlin, 1984).

[8] B. H. Gross, 'Group representations and lattices', *J. Amer. Math. Soc.* 3 (1990), 929–960.

[9] W. Jónsson and J. McKay, 'More about the Mathieu group M_{22}', *Canad. J. Math.* 38 (1976) 929–937.

[10] Yu. I. Manin, *Cubic forms* (North-Holland, Amsterdam, 1986).

[11] B. Segre, 'Forme e geometrie hermitiane, con particolare riguardo al caso finito', *Ann. Mat. Pura Appl.* 70 (1965) 1–201.

[12] I. Shimada, 'A generalization of Morin-Predonzan's theorem on the unirationality of complete intersections', *J. Algebraic Geom.* 4 (1995) 597–638.

[13] T. Shioda, 'Some observations on Jacobi sums', *Galois representations and arithmetic algebraic geometry,* Kyoto, 1985/Tokyo, 1986, (ed. Y. Ihara), Advanced Studies in Pure Mathematics 12 (North-Holland, Amsterdam, 1987) 119–135.

[14] T. Shioda, 'Mordell-Weil lattices and sphere packings', *Amer. J. Math.* 113 (1991) 931–948.

[15] T. Shioda and T. Katsura, 'On Fermat varieties', *Tôhoku Math. J.* 31 (1979) 97–115.

[16] J. T. Tate, 'Algebraic cycles and poles of zeta functions', *Arithmetical algebraic geometry* (Proceedings of a conference at Purdue University, 1963), (ed. O. F. G. Schilling, Harper and Row, New York, 1965) 93–110.

[17] J. L. van Lint. *Introduction to coding theory.* Graduate Texts in Mathematics 86 (Springer, Berlin, 1992).

Department of Mathematics, Faculty of Science, Hokkaido University, Sapporo 060-0810, JAPAN

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