THE GRAPHS OF HOFFMAN-SINGLETON, HIGMAN-SIMS, MCLAUGHLIN, AND THE HERMITIAN CURVE OF DEGREE 6 IN CHARACTERISTIC 5

ICHIRO SHIMADA (HIROSHIMA UNIVERSITY)

ABSTRACT. We present algebro-geometric constructions of the graphs of Hoffman-Singleton, Higman-Sims, and McLaughlin by means of the configuration of 3150 smooth conics totally tangent to the Hermitian curve of degree 6 in characteristic 5, and the Néron–Severi lattice of the supersingular $K3$ surface in characteristic 5 with Artin invariant 1.

1. Introduction

The graphs of Hoffman-Singleton, Higman-Sims, and McLaughlin are important examples of strongly regular graphs. These three graphs are closely related. Indeed, the Higman-Sims graph is constructed from the set of 15-cocliques in the Hoffman-Singleton graph (see Hafner [10]), and the McLaughlin graph has been constructed from the Hoffman-Singleton graph by Inoue [14] recently.

The fact that the automorphism group of the Hoffman-Singleton graph contains the simple group $\mathrm{PSU}_3(\mathbb{F}_{25})$ as a subgroup of index 2 suggests that there is a relation between these three graphs and the Hermitian curve of degree 6 over $\mathbb{F}_{25}$. In fact, Benson and Losey [2] constructed the Hoffman-Singleton graph by means of the geometry of $\mathbb{P}^2(\mathbb{F}_{25})$ equipped with a Hermitian polarity.

In this talk, we present two algebro-geometric constructions of these three graphs. The one uses the set of smooth conics totally tangent to the Hermitian curve of degree 6 in characteristic 5, and the other uses the Néron–Severi lattice of the supersingular $K3$ surface in characteristic 5 with Artin invariant 1. See [25] for the first construction, and [15] for the second construction.

2. Strongly regular graphs

Let $\Gamma = (V, E)$ be a graph, where V is the set of vertices and $E \subset \binom{V}{2}$ is the set of edges. We assume that V is finite. For $p \in V$, we put

$$L(p) := \{\ p' \in V \ \mid\ pp' \in E\ \}.$$

2000 *Mathematics Subject Classification.* 51E20, 05C25.

This work is supported JSPS Grants-in-Aid for Scientific Research (C) No.25400042 .

We say that Γ is *regular* of degree k if $k := |L(p)|$ does not depend on $p \in V$, and that Γ is *strongly regular* with the parameter (v, k, λ, μ) if Γ is regular of degree k with $|V| = v$ such that, for distinct vertices $p, p' \in V$, we have

$$|L(p) \cap L(p')| = \begin{cases} \lambda & \text{if } pp' \in E, \\ \mu & \text{otherwise.} \end{cases}$$

Definition-Example 2.1. A *triangular graph* $T(m)$ is defined to be the graph (V, E) such that $V = \binom{[m]}{2}$, where $[m] := \{1, 2, \ldots, m\}$, and E is the set of pairs $\{\{i, j\}, \{i', j'\}\}$ such that $\{i, j\} \cap \{i', j'\} \neq \emptyset$. Then $T(m)$ is a strongly regular graph of parameters $(v, k, \lambda, \mu) = (\,m(m-1)/2,\ 2(m-2),\ m-2,\ 4\,)$.

Definition-Theorem 2.1. (1) *The Hoffman-Singleton graph is the unique strongly regular graph of parameters* $(v, k, \lambda, \mu) = (50, 7, 0, 1)$.

(2) *The Higman-Sims graph is the unique strongly regular graph of parameters* $(v, k, \lambda, \mu) = (100, 22, 0, 6)$.

(3) *The McLaughlin graph is the unique strongly regular graph of parameters* $(v, k, \lambda, \mu) = (275, 112, 30, 56)$.

Theorem 2.1. (1) *The automorphism group of the Hoffman-Singleton graph contains* $\mathrm{PSU}_3(\mathbb{F}_{25})$ *as a subgroup of index* 2.

(2) *The automorphism group of the Higman-Sims graph contains the Higman-Sims group as a subgroup of index* 2.

(3) *The automorphism group of the McLaughlin graph contains the McLaughlin group as a subgroup of index* 2.

See [9], [11], [13], and [17]. See also [4] for constructions for these graphs.

Remark 2.2. Constructions of these graphs by the Leech lattice are known. Below is a part of Table 10.4 of Conway-Sloane's book [7]. See also Borcherds' paper [3].

Name	Order	Structure
$\cdot 533$	$2^4 \cdot 3^2 \cdot 5^3 \cdot 7$	$\mathrm{PSU}_3(\mathbb{F}_{25})$
$\cdot 7$	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	HS
$\cdot 10_{33}$	$2^{10} \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	$HS.2$
$\cdot 332$	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	HS
$\cdot 5$	$2^8 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	$McL.2$
$\cdot 8_{32}$	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McL
$\cdot 322$	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McL
$\cdot 522$	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	$McL.2$

3. Hermitian varieties

In this and the next sections, we fix a power $q := p^\nu$ of a prime integer p. Let k denote an algebraic closure of the finite field $\mathbb{F}_{q^2}$. Every algebraic variety will be defined over k.

Let n be an integer ≥ 2. We define the *Hermitian variety* X to be the hypersurface of $\mathbb{P}^n$ defined by

$$x_0^{q+1} + \cdots + x_n^{q+1} = 0.$$

The automorphism group $\mathrm{Aut}(X) \subset \mathrm{Aut}(\mathbb{P}^n) = \mathrm{PGL}_{n+1}(k)$ of this hypersurface X is equal to $\mathrm{PGU}_{n+1}(\mathbb{F}_{q^2})$.

We say that a point P of X is a *special point* if P satisfies the following equivalent conditions. Let $T_P \subset \mathbb{P}^n$ be the hyperplane tangent to X at P.

(i) P is an $\mathbb{F}_{q^2}$-rational point of X.

(ii) $T_P \cap X$ is a cone.

We denote by $\mathcal{P}_X$ the set of special points of X. Then we have

$$|\mathcal{P}_X| = \frac{1}{q}\left(\frac{q^{2(n+1)}-1}{q^2-1} + \frac{(-q)^{n+1}-1}{q+1}\right),$$

and $\mathrm{Aut}(X) = \mathrm{PGU}_{n+1}(\mathbb{F}_{q^2})$ acts on $\mathcal{P}_X$ transitively. See [12, Chapter 23] or [23], for example.

A curve $C \subset \mathbb{P}^n$ is said to be a *rational normal curve* if C is projectively equivalent to the image of the morphism $\mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ given by

$$[x : y] \mapsto [x^{n+1} : x^n y : \cdots : xy^n : y^{n+1}].$$

It is known that a curve $C \subset \mathbb{P}^n$ is a rational normal curve if and only if C is non-degenerate (that is, there exist no hyperplanes of $\mathbb{P}^n$ containing C), and $\deg(C) = n + 1$.

We say that a rational normal curve C is *totally tangent* to the Hermitian variety X if C is tangent to X at distinct $q + 1$ points and the intersection multiplicity at each intersection point is n.

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

Theorem 3.1 ([24]). *Suppose that $n \not\equiv 0 \pmod p$ and $2n \leq q$. Let $\mathcal{Q}_X$ denote the set of rational normal curves totally tangent to X.*

(1) *The set $\mathcal{Q}_X$ is non-empty, and $\mathrm{Aut}(X)$ acts on $\mathcal{Q}_X$ transitively with the stabilizer subgroup isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$. In particular, we have*

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

(2) *For any* $C \in \mathcal{Q}_X$*, the points in* $C \cap X$ *form a Baer subset of* C*.*
(3) *Every* $C \in \mathcal{Q}_X$ *is defined over* $\mathbb{F}_{q^2}$*, and we have* $C \cap X \subset \mathcal{P}_X$*.*

Remark 3.2. B. Segre obtained Theorem 3.1 for the case $n = 2$ in [22, n. 81].

4. Hermitian curves

In this section, we put $n = 2$ and consider the Hermitian curve

$$x^{q+1} + y^{q+1} + z^{q+1} = 0$$

of degree $q + 1$ in characteristic p. Then the condition (ii) above for $P \in X$ to be a special point of X is equivalent to $T_P \cap X = \{P\}$, and, by [8] and [16], it is further equivalent to the condition

(iii) P is a Weierstrass point of the curve X.

The number of special points of X is equal to $q^3 + 1$, and $\mathrm{Aut}(X)$ acts on $\mathcal{P}_X$ double-transitively.

A line $L \subset \mathbb{P}^2$ is a *special secant line* of X if L contains distinct two points of $\mathcal{P}_X$. If L is a special secant line, then L intersects X transversely, and we have $L \cap X \subset \mathcal{P}_X$. Let $\mathcal{S}_X$ denote the set of special secant lines of X. We have

$$|\mathcal{S}_X| = q^4 - q^3 + q^2.$$

Suppose that p is odd and $q \geq 5$. Then we have $|\mathcal{Q}_X| = q^2(q^3 + 1)$. Let $Q \in \mathcal{Q}_X$ be a conic totally tangent to X. A special secant line L of X is said to be a *special secant line of* Q if L passes through two distinct points of $Q \cap X$. We denote by $\mathcal{S}(Q)$ the set of special secant lines of Q. Since $|Q \cap \Gamma| = q + 1$, we obviously have $|\mathcal{S}(Q)| = q(q + 1)/2$.

5. Geometric construction by the Hermitian curve

In this section, we consider the Hermitian curve

$$X : x^6 + y^6 + z^6 = 0$$

of degree 6 in characteristic 5. We have

$$|\mathrm{Aut}(X)| = 378000, \quad |\mathcal{P}_X| = 126, \quad |\mathcal{Q}_X| = 3150, \quad |\mathcal{S}_X| = 525,$$

and for $Q \in \mathcal{Q}_X$, we have $|Q \cap X| = 6$ and $|\mathcal{S}(Q)| = 15$.

Our construction proceeds as follows.

Proposition 5.1. *Let* G *be the graph whose set of vertices is* $\mathcal{Q}_X$ *and whose set of edges is the set of pairs* $\{Q, Q'\}$ *of distinct conics in* $\mathcal{Q}_X$ *such that* Q *and* Q' *intersect transversely (that is,* $|Q \cap Q'| = 4$*) and* $|\mathcal{S}(Q) \cap \mathcal{S}(Q')| = 3$*. Then* G *has exactly* 150 *connected components, and each connected component is isomorphic to the triangular graph* $T(7)$*.*

Let $\mathcal{D}$ denote the set of connected components of the graph G.

Proposition 5.2. *Let $D \in \mathcal{D}$ be a connected component of the graph G. Then $Q \cap Q' \cap X = \emptyset$ for any distinct conics Q, Q' in D. Since $|D| \times |Q \cap X| = |\mathcal{P}_X|$, each $D \in \mathcal{D}$ gives rise to a decomposition of $\mathcal{P}_X$ into a disjoint union of 21 sets $Q \cap X$ of six points, where Q runs through D.*

Proposition 5.3. *Suppose that $Q \in \mathcal{Q}_X$ and $D' \in \mathcal{D}$ satisfy $Q \notin D'$. Then one of the following holds:*

$$(\alpha) \qquad |Q \cap Q' \cap X| = \begin{cases} 2 & \text{for } 3 \text{ conics } Q' \in D', \\ 0 & \text{for } 18 \text{ conics } Q' \in D'. \end{cases}$$

$$(\beta) \qquad |Q \cap Q' \cap X| = \begin{cases} 2 & \text{for } 1 \text{ conic } Q' \in D', \\ 1 & \text{for } 4 \text{ conics } Q' \in D', \\ 0 & \text{for } 16 \text{ conics } Q' \in D'. \end{cases}$$

$$(\gamma) \qquad |Q \cap Q' \cap X| = \begin{cases} 1 & \text{for } 6 \text{ conics } Q' \in D', \\ 0 & \text{for } 15 \text{ conics } Q' \in D'. \end{cases}$$

For $Q \in \mathcal{Q}_X$ and $D' \in \mathcal{D}$ satisfying $Q \notin D'$, we define $t(Q, D')$ to be α, β or γ according to the cases in Proposition 5.3.

Proposition 5.4. *Suppose that $D, D' \in \mathcal{D}$ are distinct, and hence disjoint as subsets of $\mathcal{Q}_X$. Then one of the following holds:*

$$(\beta^{21}) \qquad t(Q, D') = \beta \quad \text{for all } Q \in D.$$

$$(\gamma^{21}) \qquad t(Q, D') = \gamma \quad \text{for all } Q \in D.$$

$$(\alpha^{15}\gamma^{6}) \qquad t(Q, D') = \begin{cases} \alpha & \text{for } 15 \text{ conics } Q \in D, \\ \gamma & \text{for } 6 \text{ conics } Q \in D. \end{cases}$$

$$(\alpha^{3}\gamma^{18}) \qquad t(Q, D') = \begin{cases} \alpha & \text{for } 3 \text{ conics } Q \in D, \\ \gamma & \text{for } 18 \text{ conics } Q \in D. \end{cases}$$

For distinct $D, D' \in \mathcal{D}$, we define $T(D, D')$ to be β^{21}, γ^{21}, $\alpha^{15}\gamma^{6}$ or $\alpha^{3}\gamma^{18}$ according to the cases in Proposition 5.4.

Our main results are as follows.

Theorem 5.5. *Let H be the graph whose set of vertices is $\mathcal{D}$, and whose set of edges is the set of pairs $\{D, D'\}$ such that $D \neq D'$ and $T(D, D') = \alpha^{15}\gamma^{6}$. Then H has exactly three connected components, and each connected component is the Hoffman-Singleton graph.*

We denote by $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ the set of vertices of the connected components of H. The orbit of an element $D \in \mathcal{D}$ by the subgroup $\mathrm{PSU}_3(\mathbb{F}_{25}) \subset \mathrm{Aut}(X)$ of index 3 is one of the connected component $\mathcal{C}_i$ of H.

Proposition 5.6. *If D and D' are in the same connected component of H, then $T(D, D')$ is either γ^{21} or $\alpha^{15}\gamma^{6}$. If D and D' are in different connected components of H, then $T(D, D')$ is either β^{21} or $\alpha^{3}\gamma^{18}$.*

Theorem 5.7. *Let H' be the graph whose set of vertices is $\mathcal{D}$, and whose set of edges is the set of pairs $\{D, D'\}$ such that $D \neq D'$ and $T(D, D')$ is either β^{21} or $\alpha^{15}\gamma^{6}$. For any i and j with $i \neq j$, the restriction $H'|(\mathcal{C}_i \cup \mathcal{C}_j)$ of H' to $\mathcal{C}_i \cup \mathcal{C}_j$ is the Higman-Sims graph.*

Using our results, we can recast the construction of the McLaughlin graph by Inoue [14] into a simpler form.

Let $\mathcal{E}_1$ denote the set of edges of the Hoffman-Singleton graph $H|\mathcal{C}_1$; that is,

$$\mathcal{E}_1 := \{ \{D_1, D_2\} \mid D_1, D_2 \in \mathcal{C}_1, \;\; T(D_1, D_2) = \alpha^{15}\gamma^{6} \}.$$

We define a symmetric relation $\sim$ on $\mathcal{E}_1$ by setting $\{D_1, D_2\} \sim \{D'_1, D'_2\}$ if and only if $\{D_1, D_2\}$ and $\{D'_1, D'_2\}$ are disjoint and there exists an edge $\{D''_1, D''_2\} \in \mathcal{E}_1$ that has a common vertex with each of the edges $\{D_1, D_2\}$ and $\{D'_1, D'_2\}$.

Theorem 5.8. *Let H'' be the graph whose set of vertices is $\mathcal{E}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$, and whose set of edges consists of*

- *$\{E, E'\}$, where $E, E' \in \mathcal{E}_1$ are distinct and satisfy $E \sim E'$,*
- *$\{E, D\}$, where $E = \{D_1, D_2\} \in \mathcal{E}_1$, $D \in \mathcal{C}_2 \cup \mathcal{C}_3$, and both of $T(D_1, D)$ and $T(D_2, D)$ are $\alpha^{3}\gamma^{18}$, and*
- *$\{D, D'\}$, where $D, D' \in \mathcal{C}_2 \cup \mathcal{C}_3$ are distinct and satisfy and $T(D, D') = \alpha^{15}\gamma^{6}$ or $\alpha^{3}\gamma^{18}$.*

Then H'' is the McLaughlin graph.

Proof of Theorems. We make the list of defining equations of the conics in $\mathcal{Q}_X$, and calculate the adjacency matrices of G, H, H' and H''. We then show that $H|\mathcal{C}_i$ is strongly regular of parameters $(50, 7, 0, 1)$, $H'|(\mathcal{C}_i \cup \mathcal{C}_j)$ is strongly regular of parameters $(100, 22, 0, 6)$, and H'' is strongly regular of parameters $(275, 112, 30, 56)$.

Remark 5.9. There are many other ways to define the edges of H and H'. For example, the classical 15-coclique construction of the Higman-Sims graph from the Hoffman-Singleton graph can be rephrased neatly in terms of the geometry of $\mathcal{Q}_X$.

6. Group theoretic interpretation

The above construction can be expressed in terms of the structure of subgroups of $\mathrm{Aut}(X) = \mathrm{PGU}_3(\mathbb{F}_{25})$.

For an element a of a set A on which $\mathrm{PGU}_3(\mathbb{F}_{25})$ acts, we denote by $\mathrm{stab}(a)$ the stabilizer subgroup in $\mathrm{PGU}_3(\mathbb{F}_{25})$ of a. By $\mathfrak{S}_m$ and $\mathfrak{A}_m$, we denote the symmetric group and the alternating group of degree m, respectively.

Let Q be an element of $\mathcal{Q}_X$. Then $\mathrm{stab}(Q)$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$.

Theorem 6.1. *Let Q and Q' be distinct elements of $\mathcal{Q}_X$. Then Q and Q' are adjacent in the graph G if and only if $\mathrm{stab}(Q) \cap \mathrm{stab}(Q')$ is isomorphic to $\mathfrak{A}_4$. Moreover, Q and Q' are in the same connected component of G if and only if the subgroup $\langle \mathrm{stab}(Q), \mathrm{stab}(Q') \rangle$ of $\mathrm{PGU}_3(\mathbb{F}_{25})$ is isomorphic to $\mathfrak{A}_7$.*

Proposition 6.2. *For each $D \in \mathcal{D}$, the action of $\mathrm{stab}(D)$ on the triangular graph $D \cong T(7)$ identifies $\mathrm{stab}(D)$ with the subgroup $\mathfrak{A}_7$ of $\mathrm{Aut}(T(7)) \cong \mathfrak{S}_7$.*

Theorem 6.3. *Let D and D' be distinct elements of $\mathcal{D}$. We identify $\mathrm{stab}(D)$ with $\mathfrak{A}_7$ by Proposition 6.2. Then $T(D, D')$ is*

$$\begin{cases} \beta^{21} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \cong \mathrm{PSL}_2(\mathbb{F}_7), \\ \gamma^{21} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \cong \mathfrak{A}_5, \\ \alpha^{15}\gamma^{6} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \cong \mathfrak{A}_6, \\ \alpha^{3}\gamma^{18} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \cong (\mathfrak{A}_4 \times 3) : 2. \end{cases}$$

Remark 6.4. By ATLAS [6], we see that the maximal subgroups of $\mathfrak{A}_7$ are

$$\mathfrak{A}_6, \quad \mathrm{PSL}_2(\mathbb{F}_7), \quad \mathrm{PSL}_2(\mathbb{F}_7), \quad \mathfrak{S}_5, \quad (\mathfrak{A}_4 \times 3) : 2.$$

7. Supersingular $K3$ surface

First we recall the definition of the Néron–Severi lattice of a smooth projective surface Y defined over an algebraically closed field. A divisor D on Y is *numerically equivalent to zero* if

$$D \cdot C = 0 \quad \text{for any curve } C \text{ on } Y,$$

where $D \cdot C$ is the intersection number of D and C on Y. Let S_Y be the $\mathbb{Z}$-module of numerical equivalence classes of divisors on Y. Then S_Y with the symmetric bilinear form $\langle \cdot, \cdot \rangle$ induced by the intersection pairing becomes a lattice, which is called the *Néron–Severi lattice* of Y.

A $K3$ surface Y is said to be *supersingular* if the rank of S_Y attains the possible maximum 22. Supersingular $K3$ surfaces exist only in positive characteristics. Suppose that Y is a supersingular $K3$ surface in characteristic $p > 0$.

Let $S_Y^\vee := \mathrm{Hom}(S_Y, \mathbb{Z})$ denote the dual lattice of S_Y. Artin [1] proved that $S_Y^\vee/S_Y$ is a p-elementary abelian group of rank 2σ, where σ is an integer such that $1 \le \sigma \le 10$. This integer σ is called the *Artin invariant* of Y. It is known that the isomorphism class of the lattice S_Y depends only on p and σ (Rudakov and Shafarevich [21]), and that a supersingular $K3$ surface with Artin invariant 1 in characteristic p exists and is unique up to isomorphisms (Ogus [19, 20], Rudakov and Shafarevich [21]).

We work over an algebraically closed field of characteristic 5, and consider the smooth surface Y defined by

$$w^2 = x^6 + y^6 + z^6$$

in the weighted projective space $\mathbb{P}(3, 1, 1, 1)$. Then Y is a double cover of $\mathbb{P}^2$ branched along the Hermitian curve $X \subset \mathbb{P}^2$ of degree 6.

Proposition 7.1. *The surface Y is a supersingular $K3$ surface with Artin invariant 1. In particular, its Néron–Severi lattice S_Y is isomorphic to the unique lattice characterized by the following properties:*

- *S_Y is even and of signature $(1, 21)$,*
- *$S_Y^\vee/S_Y \cong (\mathbb{Z}/5\mathbb{Z})^2$.*

In fact, we can give a basis of S_Y explicitly. Let P be a special point of X. Then the tangent line T_P to X at P intersects X at P with multiplicity 6. Hence the pullback of T_P by the double covering $Y \to \mathbb{P}^2$ splits into two smooth rational curves meeting at one point with multiplicity 3. Since the number of $\mathbb{F}_{25}$-rational points of X is 126, we obtain 252 smooth rational curves on Y. There exist 22 curves among these 252 curves such that their numerical equivalence classes form a lattice of rank 22 and discriminant -25. Therefore they generate S_Y.

The class of the pull-back of a line of $\mathbb{P}^2$ is denoted by $h_0 \in S_Y$. We have $h_0^2 = 2$. Then the automorphism group

$$\mathrm{Aut}(Y, h_0) := \{g \in \mathrm{Aut}(Y) \mid h_0^g = h_0\}$$

of the polarized $K3$ surface (Y, h_0) is isomorphic to $\mathrm{PGU}_3(\mathbb{F}_{25}).2$ of order 756000, where the extra involution comes from $\mathrm{Gal}(Y/\mathbb{P}^2)$.

8. Construction by the Néron–Severi lattice

This construction stems from [15]. In an attempt to calculate the full automorphism group $\mathrm{Aut}(Y)$ by Borcherds method [3], we embedded S_Y into an even unimodular lattice L_{26} of signature $(1, 25)$. Note that the lattice L_{26} is unique up to isomorphisms. From the lattice data (S_Y, h_0), the Hoffman-Singleton graph and Higman-Sims graph can be constructed.

Let U be the hyperbolic plane

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and let Λ be the *negative definite* Leech lattice. As L_{26}, we use $U \oplus \Lambda$. Vectors of L_{26} are written as (a, b, λ), where $a, b \in \mathbb{Z}$, $(a, b) \in U$ and $\lambda \in \Lambda$. Let $\mathcal{P}(L_{26})$ be the connected component of $\{v \in L_{26} \otimes \mathbb{R} \mid v^2 > 0\}$ that contains

$$w_0 := (1, 0, 0)$$

on its boundary. Each vector $r \in L_{26}$ with $r^2 = -2$ defines a reflection

$$s_r \colon x \mapsto x + \langle x, r \rangle r.$$

Let $W(L_{26})$ denote the subgroup of $\mathrm{O}(L_{26})$ generated by these s_r. Then $W(L_{26})$ acts on $\mathcal{P}(L_{26})$. We put

$$\begin{aligned} \mathcal{R}_0 &:= \{\, r \in L_{26} \mid r^2 = -2,\ \langle r, w_0 \rangle = 1 \,\}, \\ \mathcal{D}_0 &:= \{\, x \in \mathcal{P}(L_{26}) \mid \langle x, r \rangle \geq 0 \text{ for any } r \in \mathcal{R}_0 \,\}. \end{aligned}$$

The map

$$\lambda \mapsto r_\lambda := (-1 - \lambda^2/2, 1, \lambda)$$

gives a bijection from Λ to $\mathcal{R}_0$, and the group $\mathrm{Aut}(\mathcal{D}_0) := \{g \in \mathrm{O}(L_{26}) \mid \mathcal{D}_0^g = \mathcal{D}_0\}$ is isomorphic to the Conway group Co_∞. Conway [5] proved the following:

Theorem 8.1. *The domain $\mathcal{D}_0$ is a standard fundamental domain of the action of $W(L_{26})$ on $\mathcal{P}(L_{26})$.*

By Nikulin [18], we see that there exists a primitive embedding $S_Y \hookrightarrow L_{26}$ unique up to $\mathrm{O}(L_{26})$. The orthogonal complement R of S_Y in L_{26} has a Gram matrix

$$\begin{bmatrix} -2 & -1 & 0 & 1 \\ -1 & -2 & -1 & 0 \\ 0 & -1 & -4 & -2 \\ 1 & 0 & -2 & -4 \end{bmatrix}.$$

We denote by

$$\mathrm{pr}_S : L_{26} \to S_Y^\vee, \quad \mathrm{pr}_R : L_{26} \to R^\vee,$$

the orthogonal projections to $S_Y^\vee$ and $R^\vee$, respectively.

Theorem 8.2 ([15])**.** *There exists a primitive embedding $S_Y \hookrightarrow L_{26}$ such that $\mathrm{pr}_S(w_0) = h_0$.*

In the following, we use this primitive embedding. The set

$$\mathcal{V} := \{\ r_\lambda \in \mathcal{R}_0 \ \mid\ \langle \mathrm{pr}_S(r_\lambda), h_0\rangle = 1,\ \ \langle \mathrm{pr}_S(r_\lambda), \mathrm{pr}_S(r_\lambda)\rangle = -8/5\ \}$$

consists of 300 elements. For each $r_\lambda \in \mathcal{V}$, there exists a unique $r'_\lambda \in \mathcal{V}$ such that $\langle r_\lambda, r'_\lambda\rangle = 3$, and for any vector $r_\mu \in \mathcal{V}$ other than r_λ, r'_λ, we have that $\langle r_\lambda, r_\mu\rangle$ is 0 or 1.

Definition 8.3. Let F be the graph whose set of vertices is $\mathcal{V}$ and whose set of edges is the set of pairs $\{r_\lambda, r_\mu\}$ such that $\langle r_\lambda, r_\mu\rangle = 1$.

The subset $\mathrm{pr}_R(\mathcal{V})$ of $R^\vee$ consists of six elements $\rho_1, \dots, \rho_6$. Their inner-products are given by

$$\frac{1}{5}\begin{bmatrix} -2 & -1 & -1 & 1 & 1 & 2 \\ -1 & -2 & 1 & -1 & 2 & 1 \\ -1 & 1 & -2 & 2 & -1 & 1 \\ 1 & -1 & 2 & -2 & 1 & -1 \\ 1 & 2 & -1 & 1 & -2 & -1 \\ 2 & 1 & 1 & -1 & -1 & -2 \end{bmatrix}.$$

We put

$$\mathcal{V}_i := \mathrm{pr}_R^{-1}(\rho_i) \cap \mathcal{V}.$$

If $r_\lambda \in \mathcal{V}_i$, then the unique vector $r'_\lambda \in \mathcal{V}$ with $\langle r_\lambda, r'_\lambda\rangle = 3$ belongs to $\mathcal{V}_{i'}$, where $\langle \rho_i, \rho_{i'}\rangle = 2/5$.

Theorem 8.4. *For each i, $F|\mathcal{V}_i$ is the Hoffman-Singleton graph.*
If $\langle \rho_i, \rho_{i'}\rangle = -1/5$, then $F|(\mathcal{V}_i \cup \mathcal{V}_{i'})$ is the Higman-Sims graph.

References

[1] M. Artin. Supersingular $K3$ surfaces. *Ann. Sci. École Norm. Sup. (4)*, 7:543–567 (1975), 1974.

[2] C. T. Benson and N. E. Losey. On a graph of Hoffman and Singleton. *J. Combinatorial Theory Ser. B*, 11:67–79, 1971.

[3] Richard Borcherds. Automorphism groups of Lorentzian lattices. *J. Algebra*, 111(1):133–153, 1987.

[4] A. E. Brouwer and J. H. van Lint. Strongly regular graphs and partial geometries. In *Enumeration and design (Waterloo, Ont., 1982)*, pages 85–122. Academic Press, Toronto, ON, 1984.

[5] J. H. Conway. The automorphism group of the 26-dimensional even unimodular Lorentzian lattice. *J. Algebra*, 80(1):159–163, 1983.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[7] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften* . Springer-Verlag, New York, third edition, 1999.

[8] Arnaldo García and Paulo Viana. Weierstrass points on certain nonclassical curves. *Arch. Math. (Basel)*, 46(4):315–322, 1986.

[9] A. Gewirtz. Graphs with maximal even girth. *Canad. J. Math.*, 21:915–934, 1969.

[10] Paul R. Hafner. On the graphs of Hoffman-Singleton and Higman-Sims. *Electron. J. Combin.*, 11(1):Research Paper 77, 33 pp. (electronic), 2004.

[11] Donald G. Higman and Charles C. Sims. A simple group of order $44,352,000$. *Math. Z.*, 105:110–113, 1968.

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

[13] A. J. Hoffman and R. R. Singleton. On Moore graphs with diameters 2 and 3. *IBM J. Res. Develop.*, 4:497–504, 1960.

[14] Koichi Inoue. A construction of the McLaughlin graph from the Hoffman-Singleton graph. *Australas. J. Combin.*, 52:197–204, 2012.

[15] Toshiyuki Katsura, Shigeyuki Kondo, and Ichiro Shimada. On the supersingular $K3$ surface in characteristic 5 with Artin invariant 1, 2013. preprint, arXiv:1312.0687.

[16] Heinrich-Wolfgang Leopoldt. Über die Automorphismengruppe des Fermatkörpers. *J. Number Theory*, 56(2):256–282, 1996.

[17] Jack McLaughlin. A simple group of order $898,128,000$. In *Theory of Finite Groups (Symposium, Harvard Univ., Cambridge, Mass., 1968)*, pages 109–111. Benjamin, New York, 1969.

[18] V. V. Nikulin. Integer symmetric bilinear forms and some of their geometric applications. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(1):111–177, 238, 1979. English translation: Math USSR-Izv. 14 (1979), no. 1, 103–167 (1980).

[19] Arthur Ogus. Supersingular $K3$ crystals. In *Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II*, volume 64 of *Astérisque*, pages 3–86. Soc. Math. France, Paris, 1979.

[20] Arthur Ogus. A crystalline Torelli theorem for supersingular $K3$ surfaces. In *Arithmetic and geometry, Vol. II*, volume 36 of *Progr. Math.*, pages 361–394. Birkhäuser Boston, Boston, MA, 1983.

[21] A. N. Rudakov and I. R. Shafarevich. Surfaces of type $K3$ over fields of finite characteristic. In *Current problems in mathematics, Vol. 18*, pages 115–207. Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1981. Reprinted in I. R. Shafarevich, Collected Mathematical Papers, Springer-Verlag, Berlin, 1989, pp. 657–714.

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

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

[24] Ichiro Shimada. A note on rational normal curves totally tangent to a Hermitian variety. *Des. Codes Cryptogr.*, 69(3):299–303, 2013.

[25] Ichiro Shimada. The graphs of Hoffman-Singleton, Higman-Sims, McLaughlin and the Hermite curve of degree 6 in characteristic 5. *Australas. J. Combin.*, 59:161–181, 2014.

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