AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **59(1)** (2014), Pages 161–181

The graphs of Hoffman-Singleton, Higman-Sims and McLaughlin, and the Hermitian curve of degree 6 in characteristic 5*

Ichiro Shimada

Department of Mathematics, Graduate School of Science
Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526
Japan
shimada@math.sci.hiroshima-u.ac.jp

Abstract

We construct the graphs of Hoffman-Singleton, Higman-Sims and McLaughlin from certain relations on the set of non-singular conics totally tangent to the Hermitian curve of degree 6 in characteristic 5. We then interpret this geometric construction in terms of the subgroup structure of the automorphism group of this Hermitian curve.

1 Introduction

The Hoffman-Singleton graph [17] is the unique strongly regular graph of parameters $(v, k, \lambda, \mu) = (50, 7, 0, 1)$. Its automorphism group contains $\mathrm{PSU}_3(\mathbb{F}_{25})$ as a subgroup of index 2. The Higman-Sims graph [14] is the unique strongly regular graph of parameters $(v, k, \lambda, \mu) = (100, 22, 0, 6)$. See [9] for the uniqueness. Its automorphism group contains the Higman-Sims group as a subgroup of index 2. The McLaughlin graph [21] is the unique strongly regular graph of parameters $(v, k, \lambda, \mu) = (275, 112, 30, 56)$. See [10] for the uniqueness. Its automorphism group contains the McLaughlin group as a subgroup of index 2. Many constructions of these beautiful graphs are known (see, for example, [4]).

These three graphs are closely related. The Higman-Sims graph has been constructed from the set of 15-cocliques in the Hoffman-Singleton graph (see Hafner [13]). Recently, the McLaughlin graph has been constructed from the Hoffman-Singleton graph by Inoue [18].

On the other hand, looking at the automorphism group, one naturally expects a relation of the Hoffman-Singleton graph with the classical unital in $\mathbb{P}^2(\mathbb{F}_{25})$. 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. They constructed a

* Partially supported by JSPS Grants-in-Aid for Scientific Research (C) No. 25400042

bijection between the set of claws in the graph and the set of polar triangles on the plane compatible with the natural action of $\mathrm{PSU}_3(\mathbb{F}_{25})$.

In this paper, we give a unified geometric construction (Theorems 1.8 and 1.10) of the Hoffman-Singleton graph and the Higman-Sims graph by means of non-singular conics totally tangent to the Hermitian curve Γ_5 of degree 6 in characteristic 5. Using this result, we recast Inoue's construction [18] of the McLaughlin graph in a simpler form (Theorem 1.12). We then translate this construction to a group-theoretic construction in terms of the subgroup structure of the automorphism group $\mathrm{PGU}_3(\mathbb{F}_{25})$ of the curve Γ_5 (Theorems 1.14, 1.15 and 1.16). In fact, it turns out at the final stage that we can construct the graphs without mentioning any geometry (Theorem 5.6).

1.1 Geometric construction

In order to emphasize the algebro-geometric character of our construction, we work, not over $\mathbb{F}_{25}$, but over an algebraically closed field k of characteristic 5. A projective plane curve Γ of degree 6 is said to be a *k-Hermitian curve* if Γ is projectively isomorphic to the Fermat curve

$$\Gamma_5 \quad : \quad x^6 + y^6 + z^6 = 0$$

of degree 6. Several characterizations of k-Hermitian curves are known; for example, see [1] for a characterization by reflexivity. Geometric properties of k-Hermitian curves that will be used in the following can be found in [3], [23], or [15, Chap. 23]. Let Γ be a k-Hermitian curve. Its automorphism group

$$\mathrm{Aut}(\Gamma) = \{ \, g \in \mathrm{PGL}_3(k) \;\mid\; g(\Gamma) = \Gamma \, \}$$

is conjugate to $\mathrm{Aut}(\Gamma_5) = \mathrm{PGU}_3(\mathbb{F}_{25})$ in $\mathrm{Aut}(\mathbb{P}^2) = \mathrm{PGL}_3(k)$. In particular, its order is 378000, and it contains a subgroup of index 3 isomorphic to the simple group $\mathrm{PSU}_3(\mathbb{F}_{25})$. Let P be a point of Γ. Then the tangent line l_P to Γ at P intersects Γ at P with intersection multiplicity ≥ 5. When $\Gamma = \Gamma_5$, the line l_P intersects Γ at P with intersection multiplicity 6 if and only if P is an $\mathbb{F}_{25}$-rational point. Combining this fact with the result of [8] and [20], we see that a point P of Γ is a Weierstrass point of Γ if and only if l_P intersects Γ at P with intersection multiplicity 6. Let $\mathcal{P}$ denote the set of Weierstrass points of Γ. Then we have $|\mathcal{P}| = 126$. The group $\mathrm{Aut}(\Gamma)$ acts on $\mathcal{P}$ doubly transitively.

Definition 1.1 A line L of $\mathbb{P}^2$ is a *special secant line of* Γ if L passes through two distinct points of $\mathcal{P}$.

Let $\mathcal{S}$ denote the set of special secant lines of Γ. Then we have $|\mathcal{S}| = 525$. The group $\mathrm{Aut}(\Gamma)$ acts on $\mathcal{S}$ transitively. If $L \in \mathcal{S}$, then we have $|L \cap \Gamma| = 6$ and

$$L \cap \Gamma \subset \mathcal{P}.$$

The incidence structure on the set of Weierstrass points of a Hermitian curve (over an arbitrary finite field) induced by special secant lines has been studied by many authors. See [16] for these works.

Definition 1.2 A non-singular conic Q on $\mathbb{P}^2$ is said to be *totally tangent to* Γ if Q intersects Γ at six distinct points with intersection multiplicity 2.

Let $\mathcal{Q}$ denote the set of non-singular conics totally tangent to Γ. Then we have $|\mathcal{Q}| = 3150$. The group $\mathrm{Aut}(\Gamma)$ acts on $\mathcal{Q}$ transitively. For each $Q \in \mathcal{Q}$, we have

$$Q \cap \Gamma \subset \mathcal{P}.$$

A special secant line L of Γ is said to be a *special secant line of* $Q \in \mathcal{Q}$ if L passes through two distinct points of $Q \cap \Gamma$. We denote by $\mathcal{S}(Q)$ the set of special secant lines of Q. Since $|Q \cap \Gamma| = 6$, we obviously have $|\mathcal{S}(Q)| = 15$.

Non-singular conics totally tangent to a Hermitian curve were investigated by B. Segre [23, n. 81]. See also [24] for a simple proof of a higher dimensional analogue of Segre's results.

A *triangular graph* $T(m)$ is defined to be the graph whose set of vertices is the set of unordered pairs of distinct elements of $\{1, 2, \dots, m\}$ and whose set of edges is the set of pairs $\{\{i, j\}, \{i', j'\}\}$ such that $\{i, j\} \cap \{i', j'\}$ is non-empty (see [5]). It is easy to see that $T(m)$ is a strongly regular graph of parameters $(v, k, \lambda, \mu) = (\, m(m-1)/2,\, 2(m-2),\, m-2,\, 4\,)$.

Our construction proceeds as follows.

Proposition 1.3 *Let G be the graph whose set of vertices is $\mathcal{Q}$ and whose set of edges is the set of pairs $\{Q, Q'\}$ of distinct conics in $\mathcal{Q}$ 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 D is isomorphic to the triangular graph $T(7)$.*

Let $\mathcal{D}$ denote the set of connected components of the graph G. Each $D \in \mathcal{D}$ is a collection of 21 conics in $\mathcal{Q}$ that satisfy the following property:

Proposition 1.4 *Let $D \in \mathcal{D}$ be a connected component of G. Then we have*

$$|Q \cap Q' \cap \Gamma| = 0$$

for any distinct conics Q, Q' in D. Since $|D| \times 6 = |\mathcal{P}|$, each connected component D of G gives rise to a decomposition of $\mathcal{P}$ into a disjoint union of 21 *sets $Q \cap \Gamma$ of six points, where Q runs through D.*

Using $\mathcal{D}$ as the set of vertices, we construct two graphs H and H' that contain the Hoffman-Singleton graph and the Higman-Sims graph, respectively.

Proposition 1.5 *Suppose that $Q \in \mathcal{Q}$ and $D' \in \mathcal{D}$ satisfy $Q \notin D'$. Then one of the following holds:*

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

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

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

For $Q \in \mathcal{Q}$ 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 1.5.

Proposition 1.6 *Suppose that $D, D' \in \mathcal{D}$ are distinct, and hence disjoint as subsets of $\mathcal{Q}$. Then one of the following holds:*

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

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

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

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

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 1.6.

Proposition 1.7 *For distinct $D, D' \in \mathcal{D}$, we have $T(D, D') = T(D', D)$. For a fixed $D \in \mathcal{D}$, the number of $D' \in \mathcal{D}$ such that $T(D, D') = \tau$ is*

$$\begin{cases} 30 & \textit{if } \tau = \beta^{21}, \\ 42 & \textit{if } \tau = \gamma^{21}, \\ 7 & \textit{if } \tau = \alpha^{15}\gamma^{6}, \\ 70 & \textit{if } \tau = \alpha^{3}\gamma^{18}. \end{cases}$$

Our main results are as follows.

Theorem 1.8 *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. We have $|\mathcal{C}_1| = |\mathcal{C}_2| = |\mathcal{C}_3| = 50$ and $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 = \mathcal{D}$.

Proposition 1.9 *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 1.10 *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 $\alpha^{15}\gamma^{6}$. Then H' is a connected regular graph of valency 37. 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.*

The number of 15-cocliques in the Hoffman-Singleton graph is 100. Connecting two distinct 15-cocliques when they have 0 or 8 common vertices, we obtain the Higman-Sims graph. Starting from Robertson's pentagon-pentagram construction [22] (see also [12]) of the Hoffman-Singleton graph and using this 15-coclique method, Hafner [13] gave an elementary construction of the Higman-Sims graph.

Our construction is related to this construction via the following:

Proposition 1.11 *Suppose that $i \neq j \neq k \neq i$. Then the map*

$$g_k \;:\; D \in \mathcal{C}_i \cup \mathcal{C}_j \;\mapsto\; \{\, D' \in \mathcal{C}_k \;|\; T(D, D') = \beta^{21} \,\}$$

induces a bijection from $\mathcal{C}_i \cup \mathcal{C}_j$ to the set of 15-cocliques in the Hoffman-Singleton graph $H|\mathcal{C}_k$. For distinct $D, D' \in \mathcal{C}_i \cup \mathcal{C}_j$, we have

$$|g_k(D) \cap g_k(D')| = \begin{cases} 0 & \text{if } T(D, D') = \alpha^{15}\gamma^{6}, \\ 3 & \text{if } T(D, D') = \alpha^{3}\gamma^{18}, \\ 5 & \text{if } T(D, D') = \gamma^{21}, \\ 8 & \text{if } T(D, D') = \beta^{21}. \end{cases}$$

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

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

We define a symmetric relation $\sim$ on $\mathcal{E}_1$ by $\{D_1, D_2\} \sim \{D'_1, D'_2\}$ 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 $\{D'_1, D'_2\}$. By Haemers [11], the graph $(\mathcal{E}_1, \sim)$ is a strongly regular graph of parameters $(v, k, \lambda, \mu) = (175, 72, 20, 36)$.

Combining our results with the construction of the McLaughlin graph due to Inoue [18], we obtain the following:

Theorem 1.12 *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.*

Since each vertex $D \in \mathcal{D}$ of H and H' is not a single point but a rather complicated geometric object (a collection of 21 conics), we can describe edges of H and H' by various geometric properties other than $T(D, D')$. Or conversely, we can find interesting configurations of conics and lines from the graphs H and H'. In Section 2, we present a few examples.

Remark 1.13 The graph H' of 150 vertices has been constructed in [4] and [13].

1.2 Group-theoretic construction

We consider the construction of the previous subsection in the case $\Gamma = \Gamma_5$. The automorphism group $\mathrm{PGU}_3(\mathbb{F}_{25})$ of the Fermat curve Γ_5 of degree 6 in characteristic 5 acts transitively on the sets $\mathcal{Q}$ and $\mathcal{D}$ of vertices of the graphs G and H or H'. Using this fact, we can define the edges of G, H and H' by means of the structure of stabilizer subgroups in $\mathrm{PGU}_3(\mathbb{F}_{25})$. For an element x of a set X on which $\mathrm{PGU}_3(\mathbb{F}_{25})$ acts, we denote by $\mathrm{stab}(x)$ the stabilizer subgroup in $\mathrm{PGU}_3(\mathbb{F}_{25})$ of x. 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 $\mathcal{Q}$. Then $\mathrm{stab}(Q)$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ (see [23, n. 81], [24] or Proposition 3.1). A rather mysterious definition of the graph G in Proposition 1.3 can be replaced by the following:

Theorem 1.14 *Let* Q *and* Q' *be distinct elements of* $\mathcal{Q}$. *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* $\mathrm{PGU}_3(\mathbb{F}_{25})$ *generated by the union of* $\mathrm{stab}(Q)$ *and* $\mathrm{stab}(Q')$ *is isomorphic to* $\mathfrak{A}_7$.

It is known that, in the automorphism group of the Hoffmann-Singleton graph, the stabilizer subgroup of a vertex is isomorphic to $\mathfrak{S}_7$. Proposition 1.3 gives us a geometric interpretation of this isomorphism. Note that the automorphism group $\mathrm{Aut}(T(m))$ of the triangular graph $T(m)$ is isomorphic to $\mathfrak{S}_m$ by definition.

Theorem 1.15 *For each element* D *of* $\mathcal{D}$, *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* $\mathrm{Aut}(T(7)) \cong \mathfrak{S}_7$.

In order to define the type $T(D, D')$ by means of the structure of $\mathrm{stab}(D) \cong \mathfrak{A}_7$, we define the following subgroups of $\mathfrak{A}_7$. See [7, pages 4 and 10] for details. Note that the full automorphism group of $\mathfrak{A}_7$ is $\mathfrak{S}_7$. For a subgroup Σ of $\mathfrak{A}_7$, we put

$$\mathrm{Conj}_{\mathfrak{A}}(\Sigma) := \{g^{-1}\Sigma g \mid g \in \mathfrak{A}_7\}, \quad \mathrm{Conj}_{\mathfrak{S}}(\Sigma) := \{g^{-1}\Sigma g \mid g \in \mathfrak{S}_7\}.$$

(a) We put

$$\Sigma_a := \{ \, g \in \mathfrak{A}_7 \ \mid \ g(7) = 7 \, \}.$$

Then Σ_a is isomorphic to $\mathfrak{A}_6$, and is maximal in $\mathfrak{A}_7$. Moreover we have $\mathrm{Conj}_{\mathfrak{A}}(\Sigma_a) = \mathrm{Conj}_{\mathfrak{S}}(\Sigma_a)$.

(b) We define a bijection $\rho : \mathbb{P}^2(\mathbb{F}_2) \xrightarrow{\sim} \{1, \dots, 7\}$ by

$$(a : b : c) \mapsto 4a + 2b + c \quad (a, b \in \{0, 1\}),$$

and let $\rho' : \mathbb{P}^2(\mathbb{F}_2) \xrightarrow{\sim} \{1, \dots, 7\}$ be the composite of ρ and the transposition (67). Then the action of $\mathrm{PSL}_3(\mathbb{F}_2)$ on $\mathbb{P}^2(\mathbb{F}_2)$ induces two faithful permutation representations $\mathrm{PSL}_3(\mathbb{F}_2) \hookrightarrow \mathfrak{S}_7$ corresponding to ρ and ρ', and the images Σ_b and Σ_b' of these representations are contained in $\mathfrak{A}_7$. These subgroups Σ_b and Σ_b' are of order 168, and are maximal in $\mathfrak{A}_7$. (Note that $\mathrm{PSL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$.) We also have

$$\mathrm{Conj}_{\mathfrak{S}}(\Sigma_b) = \mathrm{Conj}_{\mathfrak{S}}(\Sigma_b') = \mathrm{Conj}_{\mathfrak{A}}(\Sigma_b) \cup \mathrm{Conj}_{\mathfrak{A}}(\Sigma_b'), \quad \mathrm{Conj}_{\mathfrak{A}}(\Sigma_b) \cap \mathrm{Conj}_{\mathfrak{A}}(\Sigma_b') = \emptyset.$$

(c) We put

$$\Sigma_c := \{\ g \in \mathfrak{A}_7 \ \mid\ \{g(5), g(6), g(7)\} = \{5, 6, 7\}\ \}.$$

Then Σ_c is isomorphic to the group $(\mathfrak{A}_4 \times 3) : 2$ of order 72, and is maximal in $\mathfrak{A}_7$. Moreover we have $\mathrm{Conj}_{\mathfrak{A}}(\Sigma_c) = \mathrm{Conj}_{\mathfrak{S}}(\Sigma_c)$.

(d) Because of the extra outer automorphism of $\mathfrak{S}_6$, the group $\mathfrak{A}_6$ has two maximal subgroups isomorphic to $\mathfrak{A}_5$ up to inner automorphisms. One is a point stabilizer, while the other is the stabilizer subgroup of a *total* (a set of five synthemes containing all duads). We fix a total

$$\begin{aligned} t_0 \ := \ & \{\{\{1,2\},\{3,4\},\{5,6\}\},\{\{1,3\},\{2,5\},\{4,6\}\},\{\{1,4\},\{2,6\},\{3,5\}\}, \\ & \{\{1,5\},\{2,4\},\{3,6\}\},\{\{1,6\},\{2,3\},\{4,5\}\}\}, \end{aligned}$$

and put

$$\Sigma_d := \{\ g \in \mathfrak{A}_7 \ \mid\ g(7) = 7,\ \ g(t_0) = t_0\ \}.$$

Then Σ_d is isomorphic to $\mathfrak{A}_5$, and $\mathrm{Conj}_{\mathfrak{A}}(\Sigma_d) = \mathrm{Conj}_{\mathfrak{S}}(\Sigma_d)$ holds.

Now we have the following:

Theorem 1.16 *Let D and D' be distinct elements of $\mathcal{D}$. We identify* $\mathrm{stab}(D)$ *with* $\mathfrak{A}_7$ *by Theorem 1.15. Then $T(D, D')$ is*

$$\begin{cases} \beta^{21} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \textit{ is conjugate to } \Sigma_b \textit{ or } \Sigma_b', \\ \gamma^{21} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \textit{ is conjugate to } \Sigma_d, \\ \alpha^{15}\gamma^{6} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \textit{ is conjugate to } \Sigma_a, \\ \alpha^{3}\gamma^{18} & \textit{if and only if } \mathrm{stab}(D) \cap \mathrm{stab}(D') \textit{ is conjugate to } \Sigma_c. \end{cases}$$

Note that the statement of Theorem 1.16 does not depend on the choice of the isomorphism $\mathrm{stab}(D) \cong \mathfrak{A}_7$, which is not unique up to conjugations by elements of $\mathfrak{A}_7$, but is unique up to conjugations by elements of $\mathfrak{S}_7$.

Theorem 1.16 implies that $T(D, D')$ is determined simply by the order of the group $\mathrm{stab}(D) \cap \mathrm{stab}(D')$. Combining this fact with Theorems 1.8, 1.10 and 1.12, we have obtained constructions of the three graphs in the title by the subgroup structure of $\mathrm{PGU}_3(\mathbb{F}_{25})$. (See also Theorem 5.6.)

We fix $D \in \mathcal{D}$. Let $\mathcal{C}_i$ be the connected component of H containing D, and let $\mathcal{C}_j$ and $\mathcal{C}_k$ be the other two connected components. The set

$$\mathcal{N}_D := \{ D' \in \mathcal{D} \mid T(D, D') = \beta^{21} \}$$

of vertices that are adjacent to D in H' but are not adjacent to D in H decomposes into the disjoint union of two subsets $\mathcal{N}_D \cap \mathcal{C}_j$ and $\mathcal{N}_D \cap \mathcal{C}_k$.

Proposition 1.17 *Fixing* $\mathrm{stab}(D) \cong \mathfrak{A}_7$ *and interchanging* j *and* k *if necessary, we have the following; for any* $D' \in \mathcal{N}_D$,

$$\begin{aligned} D' \in \mathcal{N}_D \cap \mathcal{C}_j &\iff \mathrm{stab}(D) \cap \mathrm{stab}(D') \text{ is conjugate to } \Sigma_b, \\ D' \in \mathcal{N}_D \cap \mathcal{C}_k &\iff \mathrm{stab}(D) \cap \mathrm{stab}(D') \text{ is conjugate to } \Sigma_b'. \end{aligned}$$

Remark 1.18 We have

$$|\mathrm{Conj}_{\mathfrak{A}}(\Sigma)| = \begin{cases} 7 & \text{if } \Sigma = \Sigma_a, \\ 15 & \text{if } \Sigma = \Sigma_b \text{ or } \Sigma_b', \\ 35 & \text{if } \Sigma = \Sigma_c, \\ 42 & \text{if } \Sigma = \Sigma_d. \end{cases}$$

Compare this result with Proposition 1.7.

1.3 Plan of the paper

Suppose that an adjacency matrix of a graph Γ is given. If the number of vertices is not very large, it is a simple task for a computer to calculate the adjacency matrices of connected components of Γ. Moreover, when Γ is connected, it is also easy to determine whether Γ is strongly regular or not, and in the case when Γ is strongly regular, to compute its parameters (v, k, λ, μ). Since the three graphs we are concerned with are strongly regular graphs uniquely determined by the parameters, Theorems 1.8, 1.10 and 1.12 can be verified if we calculate the adjacency matrices of H, H' and H''. These adjacency matrices are computed from the list $\mathcal{Q}$ of conics by a simple geometry. On the other hand, it seems to be a non-trivial computational task to calculate the list $\mathcal{Q}$. Therefore, in Section 3, we give a method to calculate the list $\mathcal{Q}$. This list and other auxiliary computational data are on the author's web page

`http://www.math.sci.hiroshima-u.ac.jp/~shimada/HSgraphs.html` .

In Sections 4 and 5, we indicate how to prove our results by these computational data. In Section 2, we discuss other geometric methods of defining edges of the graphs H and H'.

This work stems from the author's joint work [19] with Professors T. Katsura and S. Kondo on the geometry of a supersingular $K3$ surface in characteristic 5. The author expresses his gratitude to them for many discussions and comments. He also thanks the referees for their many useful comments and suggestions on the first version of this paper.

2 Other methods of defining edges of H and H'

In this section, we present various ways of defining edges of H and H'.

2.1 Definition of the edges of H by 6-cliques

By the assertion $D \cong T(7)$ of Proposition 1.3, each $D \in \mathcal{D}$ contains exactly seven 6-cliques of G. Let $\mathcal{K}$ denote the set of 6-cliques in G. We have $|\mathcal{K}| = 1050$, and, for each $K \in \mathcal{K}$, we have

$$|\bigcup_{Q \in K} (Q \cap \Gamma)| = 36.$$

Proposition 2.1 *Let K be a 6-clique of G. Then there exists a unique 6-clique K' of G disjoint from K as a subset of $\mathcal{Q}$ such that*

$$\bigcup_{Q \in K} (Q \cap \Gamma) = \bigcup_{Q' \in K'} (Q' \cap \Gamma). \tag{2.1}$$

We denote by $\mathcal{PK}$ the set of pairs $\{K, K'\}$ of disjoint 6-cliques of G satisfying (2.1). The edges of the graph H can be defined as follows:

Proposition 2.2 *Two distinct vertices D and D' of H are adjacent in H if and only if there exists $\{K, K'\} \in \mathcal{PK}$ such that D contains K and D' contains K'.*

In other words, the set $\mathcal{PK}$ can be identified with the set of edges of H. Each pair in $\mathcal{PK}$ has the following remarkable geometric property:

Proposition 2.3 *Let $\{K, K'\}$ be an element of $\mathcal{PK}$. Then any $Q \in K$ and any $Q' \in K'$ intersect at one point with intersection multiplicity 4.*

2.2 Definition of the edges of H by special secant lines

For $D \in \mathcal{D}$, we put

$$\mathcal{S}_D := \bigcup_{Q \in D} \mathcal{S}(Q).$$

Proposition 2.4 *We have $|\mathcal{S}_D| = 105$ for any $D \in \mathcal{D}$.*

Proposition 2.5 *Let D and D' be distinct vertices of H. Then we have*

$$|\mathcal{S}_D \cap \mathcal{S}_{D'}| = \begin{cases} 45 & \text{if } D \text{ and } D' \text{ are adjacent in } H, \\ 15 & \text{if } D \text{ and } D' \text{ are not adjacent} \\ & \qquad \text{but in the same connected component of } H, \\ 21 & \text{if } D \text{ and } D' \text{ are in different connected components of } H. \end{cases}$$

If D and D' are in different connected components of H, then $\mathcal{P}$ is a disjoint union of 21 sets of six points $L \cap \Gamma$, where L runs through $\mathcal{S}_D \cap \mathcal{S}_{D'}$.

2.3 Definition of the edges of H' by doubly tangential pairs of conics

Suppose that $Q, Q' \in \mathcal{Q}$ are distinct. Since Q and Q' are tangent at each point of $Q \cap Q' \cap \Gamma$, we have $|Q \cap Q' \cap \Gamma| \le 2$. We say that a pair $\{Q, Q'\}$ of conics is *doubly tangential* if $|Q \cap Q' \cap \Gamma| = 2$ holds. It turns out that, if $\{Q, Q'\}$ is a doubly tangential pair, then $|\mathcal{S}(Q) \cap \mathcal{S}(Q')|$ is either one or three (see Table 4.3). For $Q \in \mathcal{Q}$, we put

$$\mathcal{R}(Q) := \{\, Q' \in \mathcal{Q} \;\mid\; |Q \cap Q' \cap \Gamma| = 2,\ |\mathcal{S}(Q) \cap \mathcal{S}(Q')| = 1 \,\},$$

and for $D \in \mathcal{D}$, we put $\mathcal{R}_D := \bigcup_{Q \in D} \mathcal{R}(Q)$. For each set $\mathcal{C}_i$ of vertices of a connected component of H, we put

$$\widetilde{\mathcal{C}}_i := \bigcup_{D \in \mathcal{C}_i} D \quad \subset \quad \mathcal{Q}.$$

Then we have $|\widetilde{\mathcal{C}}_i| = 1050$ and $\widetilde{\mathcal{C}}_1 \cup \widetilde{\mathcal{C}}_2 \cup \widetilde{\mathcal{C}}_3 = \mathcal{Q}$.

Proposition 2.6 *For any $Q \in \mathcal{Q}$, we have $|\mathcal{R}(Q)| = 45$ and $|\mathcal{R}(Q) \cap \widetilde{\mathcal{C}}_i| = 15$ for $i = 1, 2, 3$. For any $D \in \mathcal{D}$, we have $|\mathcal{R}_D| = 735$ and*

$$|\mathcal{R}_D \cap \widetilde{\mathcal{C}}_i| = \begin{cases} 105 & \text{if } D \in \mathcal{C}_i, \\ 315 & \text{if } D \notin \mathcal{C}_i. \end{cases}$$

The sets $\mathcal{R}_D$ determine the edges of H' by the following:

Proposition 2.7 *Two distinct vertices $D, D' \in \mathcal{D}$ are adjacent in H' if and only if $\mathcal{R}_D$ and D' are not disjoint in $\mathcal{Q}$. More precisely, we have*

$$|\mathcal{R}_D \cap D'| = \begin{cases} 21 & \text{if } T(D, D') = \beta^{21}, \\ 15 & \text{if } T(D, D') = \alpha^{15}\gamma^{6}, \\ 0 & \text{if } T(D, D') = \gamma^{21} \text{ or } \alpha^{3}\gamma^{18}. \end{cases}$$

We can refine Proposition 2.7 for edges of H' not contained in a connected component of H. For a vertex $D \in \mathcal{D}$, we denote by $N'(D)$ the set of vertices adjacent to D in the graph H'. If $D \in \mathcal{C}_i$ and $D' \in N'(D) \cap \mathcal{C}_j$ with $i \ne j$, we have $T(D, D') = \beta^{21}$, and hence, by definition of the type β^{21} and Proposition 1.7, we can define a unique bijection $f_{D,D'} : D \to D'$ by requiring $|Q \cap f_{D,D'}(Q) \cap \Gamma| = 2$ for any $Q \in D$.

Proposition 2.8 *If $D \in \mathcal{C}_i$, $D' \in \mathcal{C}_j$ with $i \ne j$ and $T(D, D') = \beta^{21}$, the conic $f_{D,D'}(Q)$ belongs to $\mathcal{R}(Q)$ for any $Q \in D$.*

Proposition 2.9 *For $D \in \mathcal{C}_i$ and $j \ne i$, the map $(Q, D') \mapsto f_{D,D'}(Q)$ induces a bijection from $D \times (N'(D) \cap \mathcal{C}_j)$ to $\mathcal{R}_D \cap \widetilde{\mathcal{C}}_j$. In other words, if $D \in \mathcal{C}_i$ and $j \ne i$, then $\mathcal{R}_D \cap \widetilde{\mathcal{C}}_j$ is a disjoint union of D', where D' runs through $N'(D) \cap \mathcal{C}_j$.*

3 The list of totally tangent conics

In this section, we give a method to calculate the list of conics totally tangent to a Hermitian curve in odd characteristic, based on the results in [23, n. 81] and [24].

Let p be an odd prime, and q a power of p. We work in characteristic p. Let Γ_q denote the Fermat curve

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

of degree $q+1$. By [8] and [20], we see that, for a point P of Γ_q, the following are equivalent;

(i) the tangent line of Γ_q at P intersects Γ_q at P with multiplicity $q+1$,

(ii) P is an $\mathbb{F}_{q^2}$-rational point of Γ_q, and

(iii) P is a Weierstrass point of Γ_q.

Let $\mathcal{P}_q$ denote the set of points of Γ_q satisfying (i), (ii) and (iii). By (ii), we have $|\mathcal{P}_q| = q^3+1$. A non-singular conic Q is said to be *totally tangent to* Γ_q if Q intersects Γ_q at $q+1$ distinct points with intersection multiplicity 2. Let $\mathcal{Q}_q$ denote the set of non-singular conics totally tangent to Γ_q. In [23, n. 81] and [24], the following was proved:

Proposition 3.1 (1) *The automorphism group* $\mathrm{Aut}(\Gamma_q) = \mathrm{PGU}_3(\mathbb{F}_{q^2})$ *of* Γ_q *acts on* $\mathcal{Q}_q$ *transitively, and the stabilizer subgroup of* $Q \in \mathcal{Q}_q$ *in* $\mathrm{Aut}(\Gamma_q)$ *is isomorphic to* $\mathrm{PGL}_2(\mathbb{F}_q)$. *In particular, we have* $|\mathcal{Q}_q| = q^2(q^3+1)$.

(2) *For any* $Q \in \mathcal{Q}_q$, *we have* $Q \cap \Gamma_q \subset \mathcal{P}_q$.

(3) *Let* P_0, P_1, P_2 *be three distinct points of* $\mathcal{P}_q$. *If there exists a non-singular conic* Q *that is tangent to* Γ_q *at* P_0, P_1, P_2, *then* $Q \in \mathcal{Q}_q$.

A set $\{p_1, \dots, p_m\}$ of m points in $\mathcal{P}_q$ with $m \geq 3$ is said to be a *co-conical set of* m *points* if there exists $Q \in \mathcal{Q}_q$ such that

$$\{p_1, \dots, p_m\} \subset Q \cap \Gamma_q.$$

Then the set $\mathcal{Q}_q$ is identified with the set of co-conical sets of $q+1$ points via $Q \mapsto Q \cap \Gamma_q$. It is obvious that any co-conical set of $q+1$ points $Q \cap \Gamma_q$ is a union of co-conical sets of 3 points contained in $Q \cap \Gamma_q$, and the assertion (3) of Proposition 3.1 implies that any co-conical set of 3 points is contained in a unique co-conical set of $q+1$ points. Therefore the following proposition, which characterizes co-conical sets of 3 points, enables us to calculate $\mathcal{Q}_q$ efficiently.

Proposition 3.2 *Let* P_0, P_1, P_2 *be non-collinear three points of* $\mathcal{P}_q$, *and let*

$$P_i = (a_i : b_i : c_i)$$

be the homogeneous coordinates of P_i *with* $a_i, b_i, c_i \in \mathbb{F}_{q^2}$. *We put*

$$\kappa_{ij} := a_i \bar{a}_j + b_i \bar{b}_j + c_i \bar{c}_j \in \mathbb{F}_{q^2},$$

where $\bar{x} := x^q$ *for* $x \in \mathbb{F}_{q^2}$. *Then there exists a non-singular conic* Q *that is tangent to* Γ_q *at* P_i *for* $i = 0, 1, 2$ *if and only if* $\kappa_{12}\kappa_{23}\kappa_{31}$ *is a non-zero element of* $\mathbb{F}_q$.

For the proof of Proposition 3.2, we recall a classical result of elementary geometry. Let (L_0, L_1, L_2) be an ordered triple of non-concurrent lines on $\mathbb{P}^2$, and let P_0, P_1, P_2 be points of $\mathbb{P}^2$ such that $P_i \in L_i$ and $P_i \notin L_j$ for $i \neq j$. We denote by V_i the intersection point of L_j and L_k, where $i \neq j \neq k \neq i$. We put

$$\Delta := (L_0, L_1, L_2 \,|\, P_0, P_1, P_2).$$

Let T be the intersection point of the lines V_1P_1 and V_2P_2, and let R be the intersection point of L_0 and V_0T. We denote by $\gamma(\Delta)$ the cross-ratio of the ordered four points V_1, V_2, R, P_0 on L_0; that is, if z is an affine parameter of L_0, then

$$\gamma(\Delta) := \frac{(z(V_1) - z(R))(z(V_2) - z(P_0))}{(z(V_1) - z(P_0))(z(V_2) - z(R))}.$$

It is easy to see that there exists a non-singular conic that is tangent to L_i at P_i for $i = 0, 1, 2$ if and only if $\gamma(\Delta) = 1$.

Proof of Proposition 3.2. Let L_i denote the tangent line of Γ_q at P_i, which is defined by $\bar{a}_i x + \bar{b}_i y + \bar{c}_i z = 0$. Since P_0, P_1, P_2 are not collinear, the lines L_0, L_1, L_2 are not concurrent. Since $L_i \cap \Gamma_q = \{P_i\}$, we can consider $\gamma(\Delta)$, where $\Delta = (L_0, L_1, L_2 | P_0, P_1, P_2)$. Since $\kappa_{ij} = \bar{\kappa}_{ji}$, it is enough to show that

$$\gamma(\Delta) = \frac{\kappa_{12}\kappa_{23}\kappa_{31}}{\kappa_{21}\kappa_{32}\kappa_{13}}. \tag{3.1}$$

Let $\mathbf{p}_i$ denote the column vector ${}^t[a_i, b_i, c_i]$, and we put $\bar{\mathbf{p}}_j := {}^t[\bar{a}_j, \bar{b}_j, \bar{c}_j]$. We consider the unique linear transformation g of $\mathbb{P}^2$ that maps L_0 to $x = 0$, L_1 to $y = 0$, L_2 to $z = 0$, and P_1 to $(1 : 0 : 1)$, P_2 to $(1 : 1 : 0)$. Then g maps P_0 to $[0 : \gamma(\Delta) : 1]$. Suppose that g is given by the left multiplication of a 3×3 matrix M. Then there exist non-zero constants τ_0, τ_1, τ_2 and s, t, u such that

$$M\mathbf{P} = \begin{bmatrix} 0 & t & u \\ s\gamma(\Delta) & 0 & u \\ s & t & 0 \end{bmatrix}, \quad {}^tM^{-1}\bar{\mathbf{P}} = \begin{bmatrix} \tau_0 & 0 & 0 \\ 0 & \tau_1 & 0 \\ 0 & 0 & \tau_2 \end{bmatrix}, \quad \text{where } \mathbf{P} := [\mathbf{p}_0, \mathbf{p}_1, \mathbf{p}_2].$$

On the other hand, we have

$${}^t\mathbf{P}\bar{\mathbf{P}} = \begin{bmatrix} 0 & \kappa_{12} & \kappa_{13} \\ \kappa_{21} & 0 & \kappa_{23} \\ \kappa_{31} & \kappa_{32} & 0 \end{bmatrix}.$$

Combining these equations, we obtain (3.1). □

Remark 3.3 By Chevalley-Warning theorem, the non-singular conic Q_1 defined by $x^2 + y^2 + z^2 = 0$ has $q + 1$ rational points over $\mathbb{F}_q$, and it intersects Γ_q at each of these $\mathbb{F}_q$-rational points with intersection multiplicity 2. Hence we can also make the list $\mathcal{Q}_q$ from Q_1 by the action of $\mathrm{Aut}(\Gamma_q) = \mathrm{PGU}_3(\mathbb{F}_{q^2})$ on $\mathbb{P}^2$.

4 Geometric construction

In this section, we work in characteristic 5. By a *list*, we mean an ordered finite set. We put

$$\alpha := \sqrt{2} \;\in\; \mathbb{F}_{25} = \mathbb{F}_5(\alpha).$$

With the help of Proposition 3.2, we construct the following lists. They are available from the web page given at the end of Introduction.

- The list `P` of the Weierstrass points of Γ_5; that is, the list of $\mathbb{F}_{25}$-rational points of Γ_5.
- The list `S` of sets of collinear six points in `P`, which is regarded as the list $\mathcal{S}_5$ of special secant lines L of Γ_5 by $L \mapsto L \cap \Gamma_5$.
- The list `Q` of co-conical sets of six points in `P`, which is regarded as the list $\mathcal{Q}_5$ of totally tangent conics Q by $Q \mapsto Q \cap \Gamma_5$.

In the following, conics in $\mathcal{Q}_5$ are numbered as $Q_1, \dots, Q_{3150}$ according to the order of the list `Q`. For example, the first member of `Q` is

$$\{\, (0:1:\pm 2),\;\; (1:0:\pm 2),\;\; (1:\pm 2:0)\,\},$$

and hence the conic Q_1 is defined by $\phi_1 : x^2 + y^2 + z^2 = 0$. From the lists `P`, `S` and `Q`, we obtain the following lists:

- The list `SQ` $= [\mathcal{S}(Q_1), \dots, \mathcal{S}(Q_{3150})]$ of the sets $\mathcal{S}(Q_i)$ of special secant lines of conics Q_i.
- The list `EQ` $= [\phi_1, \dots, \phi_{3150}]$ of the defining equations ϕ_i of conics Q_i.

From the list `Q`, we compute a 3150×3150 matrix M_0 whose (i, j) entry is equal to $|Q_i \cap Q_j \cap \Gamma_5|$. From the list `SQ`, we compute a 3150×3150 matrix M_1 whose (i, j) entry is equal to $|\mathcal{S}(Q_i) \cap \mathcal{S}(Q_j)|$.

Suppose that a non-singular conic C is defined by an equation ${}^t\mathbf{x}\, F_C\, \mathbf{x} = 0$, where F_C is a 3×3 symmetric matrix. Then two non-singular conics C and C' intersect at four distinct points transversely if and only if the cubic polynomial

$$f := \det(F_C + tF_{C'})$$

of t has no multiple roots. From the list `EQ`, we calculate the discriminant of the polynomials f for $Q_i, Q_j \in \mathcal{Q}_5$, and compute a 3150×3150 matrix M_2 whose (i, j) entry is 1 if $|Q_i \cap Q_j| = 4$ and is 0 if $i = j$ or $|Q_i \cap Q_j| < 4$.

From the matrices M_1 and M_2, we compute the adjacency matrix A_G of G. From the matrix A_G, we compute the list `D` of the connected components of G. It turns out that `D` consists of 150 members $D_1, \dots, D_{150}$, and that each connected component has 21 vertices. For example, the connected component D_1 of G containing Q_1 consists of the conics given in Table 4.1, and their adjacency relation is given in Table 4.2,

$$
\begin{array}{rcl}
Q_1 & : & x^2+y^2+z^2=0 \\
Q_{309} & : & (2\,\alpha+2)\,x^2+(3\,\alpha+2)\,y^2+z^2=0 \\
Q_{434} & : & (3\,\alpha+2)\,x^2+(2\,\alpha+2)\,y^2+z^2=0 \\
Q_{1454} & : & 2\,z^2+xy=0 \\
Q_{1535} & : & 4\,x^2+4\,y^2+4\,z^2+4\,xy+yz+zx=0 \\
Q_{1628} & : & x^2+y^2+z^2+xy+yz+zx=0 \\
Q_{2063} & : & 3\,z^2+xy=0 \\
Q_{2120} & : & 4\,x^2+4\,y^2+4\,z^2+xy+4\,yz+zx=0 \\
Q_{2187} & : & x^2+y^2+z^2+4\,xy+4\,yz+zx=0 \\
Q_{2445} & : & 2\,y^2+zx=0 \\
Q_{2489} & : & 3\,y^2+zx=0 \\
Q_{2511} & : & (2\,\alpha+2)\,x^2+y^2+(3\,\alpha+2)\,z^2+(3\,\alpha+2)\,xy+(2\,\alpha+2)\,yz+zx=0 \\
Q_{2556} & : & (2\,\alpha+3)\,x^2+4\,y^2+(3\,\alpha+3)\,z^2+(2\,\alpha+2)\,xy+(2\,\alpha+3)\,yz+zx=0 \\
Q_{2592} & : & (3\,\alpha+2)\,x^2+y^2+(2\,\alpha+2)\,z^2+(3\,\alpha+3)\,xy+(2\,\alpha+3)\,yz+zx=0 \\
Q_{2615} & : & (3\,\alpha+3)\,x^2+4\,y^2+(2\,\alpha+3)\,z^2+(2\,\alpha+3)\,xy+(2\,\alpha+2)\,yz+zx=0 \\
Q_{2708} & : & 2\,x^2+yz=0 \\
Q_{2790} & : & 3\,x^2+yz=0 \\
Q_{3082} & : & (2\,\alpha+3)\,x^2+4\,y^2+(3\,\alpha+3)\,z^2+(3\,\alpha+3)\,xy+(3\,\alpha+2)\,yz+zx=0 \\
Q_{3086} & : & (3\,\alpha+2)\,x^2+y^2+(2\,\alpha+2)\,z^2+(2\,\alpha+2)\,xy+(3\,\alpha+2)\,yz+zx=0 \\
Q_{3116} & : & (3\,\alpha+3)\,x^2+4\,y^2+(2\,\alpha+3)\,z^2+(3\,\alpha+2)\,xy+(3\,\alpha+3)\,yz+zx=0 \\
Q_{3122} & : & (2\,\alpha+2)\,x^2+y^2+(3\,\alpha+2)\,z^2+(2\,\alpha+3)\,xy+(3\,\alpha+3)\,yz+zx=0
\end{array}
$$

Table 4.1: Vertices of D_1

where distinct conics Q at the ith row and the jth column and Q' at the i'th row and the j'th column are adjacent if and only if $\{i,j\}\cap\{i',j'\}\neq\emptyset$. Thus an isomorphism $D_1\cong T(7)$ of graphs is established. Using the list `Q`, we confirm

$$\bigcup_{Q\in D_1}(Q\cap\Gamma_5)=\mathcal{P}_5.$$

Since $\mathrm{Aut}(\Gamma_5)$ acts on $\mathcal{Q}_5$ transitively, it acts on $\mathcal{D}$ transitively. Thus we have proved Propositions 1.3 and 1.4.

Using the matrix M_0 and the list `D`, we confirm Proposition 1.5 and 1.6. We then calculate a 3150×150 matrix whose (ν,j) entry is $t(Q_\nu,D_j)$ if $Q_\nu\notin D_j$ and 0 if $Q_\nu\in D_j$. We then calculate a 150×150 matrix $\mathbb{T}$ whose (i,j) entry is $T(D_i,D_j)$ if $i\neq j$ and 0 if $i=j$. Then Proposition 1.7 is confirmed. From the matrix $\mathbb{T}$, we obtain the adjacency matrix A_H of the graph H in Theorem 1.8. It turns out that H has exactly three connected components whose set of vertices are denoted by $\mathcal{C}_1,\mathcal{C}_2,\mathcal{C}_3$. Then it is easy to confirm that each connected component of H is a strongly regular

–	Q_1	Q_{309}	Q_{2615}	Q_{2511}	Q_{3116}	Q_{3122}
	–	Q_{434}	Q_{3082}	Q_{3086}	Q_{2556}	Q_{2592}
		–	Q_{1535}	Q_{1628}	Q_{2120}	Q_{2187}
			–	Q_{1454}	Q_{2489}	Q_{2790}
				–	Q_{2708}	Q_{2445}
					–	Q_{2063}

Table 4.2: Adjacency relation on D_1

graph of parameters $(v, k, \lambda, \mu) = (50, 7, 0, 1)$. Therefore Theorem 1.8 is proved. Using $\mathbb{T}$ and the sets $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, we confirm Proposition 1.9.

We then calculate the adjacency matrix $A_{H'}$ of the graph H' form $\mathbb{T}$. Then it is easy to confirm that, for any i and j with $i \neq j$, $H'|(\mathcal{C}_i \cup \mathcal{C}_j)$ is a strongly regular graph of parameters $(v, k, \lambda, \mu) = (100, 22, 0, 6)$. Thus Theorem 1.10 is proved. Using $\mathbb{T}$, the adjacency matrix of H and the sets $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, we confirm Proposition 1.11. Then Theorem 1.12 follows from [18], or we can compute the adjacency matrix of H'' and confirm Theorem 1.12 directly.

Note that the conic $Q_1 \in \mathcal{Q}_5$ defined by $x^2 + y^2 + z^2 = 0$ has a parametric presentation

$$t \mapsto (t^2 + 4 : 2t : 2\,t^2 + 2).$$

Using the list `EQ` and this parametric presentation, we can calculate

$$n(Q_i) := [\nu_1, \nu_2, \nu_3, \nu_4]$$

for each $i > 1$, where ν_m is the number of points in $Q_1 \cap Q_i$ at which Q_1 and Q_i intersect with intersection multiplicity m. In Table 4.3, we give the number N of conics Q that have an intersection pattern with Q_1 prescribed by $n(Q)$ and

$$a(Q) := |Q_1 \cap Q \cap \Gamma_5|, \quad s(Q) := |\mathcal{S}(Q_1) \cap \mathcal{S}(Q)|.$$

Next we prove results in Section 2.1. By the adjacency matrix A_G of the graph G and the list `D`, we can construct the list `K` of 6-cliques in G. Using `Q`, `D`, `K` and the adjacency matrix of H obtained from $\mathbb{T}$, we confirm Propositions 2.1, 2.2, and construct the list $\mathcal{PK}$. The two 6-cliques containing Q_1 are

$$\begin{aligned} K_a &= \{Q_1, Q_{309}, Q_{2511}, Q_{2615}, Q_{3116}, Q_{3122}\}, \\ K_b &= \{Q_1, Q_{434}, Q_{2556}, Q_{2592}, Q_{3082}, Q_{3086}\}. \end{aligned}$$

Then their partners in $\mathcal{PK}$ are

$$\begin{aligned} K'_a &= \{Q_8, Q_{171}, Q_{827}, Q_{936}, Q_{1973}, Q_{2038}\}, \\ K'_b &= \{Q_{22}, Q_{160}, Q_{816}, Q_{947}, Q_{1984}, Q_{2034}\}, \end{aligned}$$

$a(Q)$	$s(Q)$	$n(Q)$	N	an example
6	15	–	1	$x^2+y^2+z^2=0$
0	3	$[4,0,0,0]$	10	$(2\alpha+2)\,x^2+(3\alpha+2)\,y^2+z^2=0$
0	3	$[0,2,0,0]$	20	$(\alpha+2)\,x^2+\alpha y^2+\alpha z^2+yz=0$
1	5	$[0,0,0,1]$	24	$3\alpha x^2+(3\alpha+4)\,y^2+(3\alpha+1)\,z^2+yz=0$
2	3	$[0,2,0,0]$	30	$(3\alpha+2)\,x^2+y^2+z^2=0$
0	0	$[0,2,0,0]$	30	$(2\alpha+1)x^2+(2\alpha+1)y^2+(2\alpha+1)z^2+xy+yz+zx=0$
2	1	$[0,2,0,0]$	45	$(2\alpha+3)\,x^2+y^2+z^2=0$
1	0	$[1,0,1,0]$	120	$3\alpha x^2+(\alpha+2)\,y^2+3z^2+3xy+(2\alpha+3)\,yz+zx=0$
0	1	$[4,0,0,0]$	390	$3\alpha x^2+\alpha\,y^2+\alpha\,z^2+yz=0$
1	1	$[2,1,0,0]$	600	$(4\alpha+2)\,x^2+(3\alpha+4)\,y^2+(3\alpha+1)\,z^2+yz=0$
0	0	$[4,0,0,0]$	1880	$4x^2+4y^2+(2\alpha+4)\,z^2+(4\alpha+4)\,xy+yz+zx=0$

Table 4.3: Classification of conics by intersection pattern with Q_1

$$
\begin{array}{rcl}
Q_{8} & : & 3\,\alpha\,x^2+(3\,\alpha+4)\,y^2+(3\,\alpha+1)\,z^2+yz=0\\
Q_{171} & : & 2\,\alpha\,x^2+(2\,\alpha+1)\,y^2+(2\,\alpha+4)\,z^2+yz=0\\
Q_{827} & : & (2\,\alpha+4)\,x^2+2\,\alpha\,y^2+(2\,\alpha+1)\,z^2+zx=0\\
Q_{936} & : & (3\,\alpha+1)\,x^2+3\,\alpha\,y^2+(3\,\alpha+4)\,z^2+zx=0\\
Q_{1973} & : & (3\,\alpha+4)\,x^2+(3\,\alpha+1)\,y^2+3\,\alpha\,z^2+xy=0\\
Q_{2038} & : & (2\,\alpha+1)\,x^2+(2\,\alpha+4)\,y^2+2\,\alpha\,z^2+xy=0\\
Q_{22} & : & 2\,\alpha\,x^2+(2\,\alpha+4)\,y^2+(2\,\alpha+1)\,z^2+yz=0\\
Q_{160} & : & 3\,\alpha\,x^2+(3\,\alpha+1)\,y^2+(3\,\alpha+4)\,z^2+yz=0\\
Q_{816} & : & (3\,\alpha+4)\,x^2+3\,\alpha\,y^2+(3\,\alpha+1)\,z^2+zx=0\\
Q_{947} & : & (2\,\alpha+1)\,x^2+2\,\alpha\,y^2+(2\,\alpha+4)\,z^2+zx=0\\
Q_{1984} & : & (2\,\alpha+4)\,x^2+(2\,\alpha+1)\,y^2+2\,\alpha\,z^2+xy=0\\
Q_{2034} & : & (3\,\alpha+1)\,x^2+(3\,\alpha+4)\,y^2+3\,\alpha\,z^2+xy=0.
\end{array}
$$

Table 4.4: Conics in K'_a and K'_b

the defining equations of whose members are given in Table 4.4. Each of these conics intersects Q_1 only at one point with intersection multiplicity 4. For example, Q_8 intersects Q_1 only at $(0:3:1)$. Since $\mathrm{Aut}(\Gamma_5)$ acts on $\mathcal{Q}_5$ transitively, Proposition 2.3 is proved.

Remark 4.1 From Table 4.3, we see that there exist exactly 12 conics $Q' \in \mathcal{Q}_5$ that intersect Q_1 only at one point with intersection multiplicity 4 but are not contained in $K'_a \cup K'_b$. An example of such a conic is

$$4\,\alpha\,x^2 + (4\,\alpha + 4)\,y^2 + (4\,\alpha + 1)\,z^2 + yz = 0.$$

These 12 conics are contained in $\widetilde{\mathcal{C}}_1$.

The proofs in Sections 2.2 and 2.3 are analogous and we omit the details.

Remark 4.2 Some families of strongly regular graphs have been constructed from Hermitian varieties in Chakravarti [6].

5 Group-theoretic construction

In order to verify the group-theoretic construction (Theorems 1.14, 1.15, 1.16 and Proposition 1.17), we make the following computational data. Since the order 378000 of $\mathrm{PGU}_3(\mathbb{F}_{25})$ is large, it uses too much memory to make the list of all elements of $\mathrm{PGU}_3(\mathbb{F}_{25})$. Instead we make the lists of elements of

$$\begin{aligned} G_S &:= \mathrm{stab}(p_1), \quad \text{where } p_1 = (0:1:2) \in \mathcal{P}_5, \quad \text{and} \\ G_T &:= \text{a complete set of representatives of } \mathrm{PGU}_3(\mathbb{F}_{25})/G_S. \end{aligned}$$

Then we have $|G_S| = 3000$ and $|G_T| = 126$, and each element of $\mathrm{PGU}_3(\mathbb{F}_{25})$ is uniquely written as $\tau\sigma$, where $\sigma \in G_S$ and $\tau \in G_T$. We then calculate the permutation on the set $\mathcal{P}_5$ induced by each of the $3000 + 126$ elements of G_S and G_T. From this list of permutations, we calculate the permutation on the set $\mathcal{Q}_5$ induced by each element of G_S and G_T, and from this list, we calculate the permutation on the set $\mathcal{D}$ induced by each element of G_S and G_T. Thus we obtain three permutation representations of $\mathrm{PGU}_3(\mathbb{F}_{25})$ on $\mathcal{P}_5$, $\mathcal{Q}_5$ and $\mathcal{D}$, each of which is faithful.

Remark 5.1 In order to determine the structure of subgroups of $\mathrm{PGU}_3(\mathbb{F}_{25})$, it is more convenient to use these permutation representations than to handle 3×3 matrices with components in $\mathbb{F}_{25}$.

Then we calculate $\mathrm{stab}(Q_1)$ and its subgroups

$$\mathrm{stab}(Q_1, Q) := \mathrm{stab}(Q_1) \cap \mathrm{stab}(Q)$$

for each $Q \in \mathcal{Q}_5$. Combining this data with the adjacency matrix A_G of the graph G, we confirm the first-half of Theorem 1.14.

No.	$a(Q)$	$s(Q)$	$n(Q)$	$\mathrm{stab}(Q_1, Q)$	N
1	6	15	–	$\mathfrak{S}_5$	1
2	0	3	$[4, 0, 0, 0]$	$\mathfrak{A}_4$	10
3	0	3	$[0, 2, 0, 0]$	$\mathfrak{D}_{12}$	20
4	1	5	$[0, 0, 0, 1]$	$\mathfrak{D}_{10}$	24
5	2	3	$[0, 2, 0, 0]$	$\mathfrak{D}_8$	30
6	0	0	$[0, 2, 0, 0]$	$\mathfrak{D}_{12}$	30
7	2	1	$[0, 2, 0, 0]$	$\mathfrak{D}_8$	45
8	1	0	$[1, 0, 1, 0]$	0	120
9	0	1	$[4, 0, 0, 0]$	$\mathbb{Z}/2\mathbb{Z}$	180
10	0	1	$[4, 0, 0, 0]$	$(\mathbb{Z}/2\mathbb{Z})^2$	210
11	1	1	$[2, 1, 0, 0]$	$\mathbb{Z}/2\mathbb{Z}$	600
12	0	0	$[4, 0, 0, 0]$	0	720
13	0	0	$[4, 0, 0, 0]$	$\mathbb{Z}/2\mathbb{Z}$	900
14	0	0	$[4, 0, 0, 0]$	$\mathbb{Z}/3\mathbb{Z}$	80
15	0	0	$[4, 0, 0, 0]$	$(\mathbb{Z}/2\mathbb{Z})^2$	180

Table 5.1: $\mathrm{stab}(Q_1, Q)$

If $Q \in \mathcal{Q}_5$ is distinct from Q_1, then $\mathrm{stab}(Q_1, Q)$ is isomorphic to one of the following groups:

$$0, \ \mathbb{Z}/2\mathbb{Z}, \ \mathbb{Z}/3\mathbb{Z}, \ (\mathbb{Z}/2\mathbb{Z})^2, \ \mathfrak{D}_8, \ \mathfrak{D}_{10}, \ \mathfrak{D}_{12}, \ \mathfrak{A}_4,$$

where $\mathfrak{D}_{2n}$ is the dihedral group of order $2n$. Table 4.3 is refined to Table 5.1 by using this new data. The action of $\mathrm{stab}(Q_1) \cong \mathfrak{S}_5$ decomposes $\mathcal{Q}_5$ into 64 orbits, and each row of Table 5.1 contains

$$N \cdot |\mathrm{stab}(Q_1, Q)|/120$$

orbits of size $120/|\mathrm{stab}(Q_1, Q)|$. From each of these orbits other than $\{Q_1\}$, we choose a representative conic Q and confirm the following:

$$Q \in D_1 \implies |\langle \mathrm{stab}(Q_1), \mathrm{stab}(Q) \rangle| = 2520,$$
$$Q \notin D_1 \implies |\langle \mathrm{stab}(Q_1), \mathrm{stab}(Q) \rangle| > 2520.$$

Thus the second-half of Theorem 1.14 is verified.

Remark 5.2 The conics in $\mathcal{Q}_5$ that are in the connected component D_1 of G but are not adjacent to Q_1 in G form one of the three orbits of size 10 in the 6th row of Table 5.1.

We then calculate $\mathrm{stab}(D_1)$ and its subgroup

$$\mathrm{stab}(D_1, D) := \mathrm{stab}(D_1) \cap \mathrm{stab}(D)$$

for each $D \in \mathcal{D}$. An isomorphism $\kappa : D_1 \xrightarrow{\sim} T(7)$ of graphs is obtained from the triangle in Table 4.2 by putting $\kappa(Q_\nu) = \{i, j\}$ if $Q_\nu \in D_1$ is at the ith row and the jth column of the triangle. This map κ gives rise to a homomorphism

$$\mathrm{stab}(D_1) \to \mathrm{Aut}(T(7)) = \mathfrak{S}_7.$$

We confirm that this homomorphism is injective, and verify Theorem 1.15. Using the matrix $\mathbb{T}$, we also confirm Theorem 1.16 and Proposition 1.17.

Remark 5.3 Each connected component of the graph H is an orbit of the action of the subgroup $\mathrm{PSU}_3(\mathbb{F}_{25})$ of index 3 in $\mathrm{PGU}_3(\mathbb{F}_{25})$ on $\mathcal{D}$.

Combining all the results above, we can construct the Hoffmann-Singleton graph and the Higman-Sims graph from $\mathrm{PGU}_3(\mathbb{F}_{25})$ without using any geometry. We put

$$\Delta := \mathrm{PGU}_3(\mathbb{F}_{25}) \cap \mathrm{PGO}_3(\mathbb{F}_{25}).$$

Remark 5.4 We have $\mathrm{PGO}_3(\mathbb{F}_{25}) = \{M \in \mathrm{PGL}_3(\mathbb{F}_{25}) \mid {}^tMM \text{ is a diagonal matrix}\}$. Since Q_1 is defined by $x^2 + y^2 + z^2 = 0$, we have $\Delta = \mathrm{stab}(Q_1)$.

Consider the following five elements of $\mathrm{PGU}_3(\mathbb{F}_{25})$:

$$g_2 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^{-1} \end{bmatrix} \quad (\omega := 2 + 3\alpha), \qquad g_3 := \begin{bmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix},$$

$$g_4 := \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \quad g_5 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 4 \\ 0 & 4 & 0 \end{bmatrix}, \quad g_6 := \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Remark 5.5 The elements g_i $(i = 2, \dots, 6)$ belong to $\mathrm{stab}(D_1)$, and correspond to $(1, 2)(i, i + 1) \in \mathfrak{A}_7$ by the isomorphism $\mathrm{stab}(D_1) \cong \mathfrak{A}_7$ induced by $\kappa : D_1 \cong T(7)$. Since these five permutations $(1, 2)(i, i + 1)$ generate $\mathfrak{A}_7$, we see that the elements $g_2, \dots, g_6$ generate $\mathrm{stab}(D_1)$.

Theorem 5.6 *Let Γ be the subgroup of $\mathrm{PGU}_3(\mathbb{F}_{25})$ generated by $g_2, \dots, g_6$ above. Then Γ is isomorphic to $\mathfrak{A}_7$. Moreover, if $\gamma \in \mathrm{PGU}_3(\mathbb{F}_{25})$ satisfies $\Delta \cap \gamma^{-1}\Delta\gamma \cong \mathfrak{A}_4$, then Γ is generated by Δ and $\gamma^{-1}\Delta\gamma$.*

Let $\mathcal{V}$ denote the set of subgroups of $\mathrm{PGU}_3(\mathbb{F}_{25})$ conjugate to Γ. Then, we have $|\mathcal{V}| = 150$, and for distinct elements $\Gamma', \Gamma'' \in \mathcal{V}$, the group $\Gamma' \cap \Gamma''$ is isomorphic to one of the following:

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

For $n = 360, 168, 72$ and 60, we define a subset $\mathcal{E}_n$ of the set of unordered pairs of distinct elements of $\mathcal{V}$ by

$$\mathcal{E}_n := \{ \{\Gamma', \Gamma''\} \mid |\Gamma' \cap \Gamma''| = n \}.$$

Then the graph $(\mathcal{V}, \mathcal{E}_{360})$ *has exactly three connected components* $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$*, and each* $\mathcal{C}_i$ *is the Hoffmann-Singleton graph. Moreover the graph* $(\mathcal{V}, \mathcal{E}_{360} \cup \mathcal{E}_{168})|(\mathcal{C}_i \cup \mathcal{C}_j)$ *is the Higman-Sims graph for any* $i \neq j$*.*

We can also construct the McLaughlin graph from $\mathcal{V}$ and $\mathcal{E}_n$ by the recipe of Inoue [18] in the same way as Theorem 1.12.

References

[1] E. Ballico and A. Hefez, Nonreflexive projective curves of low degree, *Manuscripta Math.* 70(4) (1991), 385–396.

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

[3] R.C. Bose and I.M. Chakravarti, Hermitian varieties in a finite projective space PG(N, q^2), *Canad. J. Math.* 18 (1966), 1161–1182.

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

[5] P.J. Cameron and J.H. van Lint, *Graph theory, coding theory and block designs*, Cambridge University Press, Cambridge, 1975, London Math. Soc. Lec. Note Series No. 19.

[6] I.M. Chakravarti, Geometric construction of some families of two-class and three-class association schemes and codes from nondegenerate and degenerate Hermitian varieties, Graph theory and combinatorics (Marseille-Luminy, 1990), *Discrete Math.* 111 (1-3) (1993), 95–103.

[7] 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.

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

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

[10] J.-M. Goethals and J.J. Seidel, The regular two-graph on 276 vertices, *Discrete Math.* 12 (1975), 143–158.

[11] W. Haemers, A new partial geometry constructed from the Hoffman-Singleton graph, In *Finite geometries and designs (Proc. Conf., Chelwood Gate, 1980)*, vol. 49 of *London Math. Soc. Lec. Note Ser.*, pp. 119–127, Cambridge Univ. Press, Cambridge, 1981.

[12] P.R. Hafner, The Hoffman-Singleton graph and its automorphisms, *J. Algebraic Combin.* 18 (1) (2003), 7–12.

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

[14] D.G. Higman and C.C. Sims, A simple group of order $44,352,000$, *Math. Z.* 105 (1968), 110–113.

[15] 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.

[16] G. Hiss, Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups, *Indag. Math. (N.S.)* 15 (2) (2004), 223–243.

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

[18] K. Inoue, A construction of the McLaughlin graph from the Hoffman-Singleton graph, *Australas. J. Combin.* 52 (2012), 197–204.

[19] T. Katsura, S. Kondō and I. Shimada, On the supersingular $K3$ surface in characteristic 5 with Artin invariant 1, (preprint), arXiv:1312.0687.

[20] H.-W. Leopoldt, Über die Automorphismengruppe des Fermatkörpers, *J. Number Theory* 56 (2) (1996), 256–282.

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

[22] N. Robertson, Graphs minimal under girth, valency, and connectivity constraints, PhD thesis, University of Waterloo, 1969.

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

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

(Received 10 Aug 2013; revised 11 Feb 2014)