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

Ichiro Shimada

Hiroshima University

2014.06. Tohoku

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

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

We say that Γ is *regular* of degree k if $k := |L(p)|$ does not depend on $p \in V$.
We say that Γ is a *strongly regular* graph with the parameter (v, k, λ, μ) $(\mathrm{srg}(v, k, \lambda, \mu))$ 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

We put $[m] := \{1, 2, \ldots, m\}$.
The *triangular graph* $T(m)$ is defined to be the graph (V, E) such that

- $V = \binom{[m]}{2}$, and
- $E = \{ \{\{i, j\}, \{i', j'\}\} \mid \{i, j\} \cap \{i', j'\} \neq \emptyset \}$.

Then $T(m)$ is

$$\mathrm{srg}(\, m(m-1)/2,\ 2(m-2),\ m-2,\ 4\,).$$

Definition-Theorem

- *The Hoffman-Singleton* (**HfSg**) *graph is the unique* $\mathrm{srg}(50, 7, 0, 1)$.
- *The Higman-Sims graph* (**HgSm**) *is the unique* $\mathrm{srg}(100, 22, 0, 6)$.
- *The McLaughlin graph* (**McL**) *is the unique* $\mathrm{srg}(275, 112, 30, 56)$.

Theorem

- $\mathrm{Aut}(\mathbf{HfSg}) \supset \mathrm{PSU}_3(\mathbb{F}_{25})$ *as index* 2 *subgroup.*
- $\mathrm{Aut}(\mathbf{HgSm}) \supset$ *HS as index* 2 *subgroup.*
- $\mathrm{Aut}(\mathbf{McL}) \supset$ *McL as index* 2 *subgroup.*

These graphs are related to the Leech lattice.
A part of Table 10.4 of Conway-Sloane's book:

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
$\cdot 522$	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	$McL.2$

Constructions of these graphs by the Leech lattice are known.

The aim of this talk:
We present **algebro-geometric** constructions of these graphs.

Hermitian curve

We fix a power $q := p^\nu$ of an *odd* prime integer p,
and work over an algebraically closed field of characteristic p.
We consider the Hermitian curve

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

of degree $q + 1$.
We say that a point P of X is *special* if P satisfies the following equivalent conditions.

(i) P is an $\mathbb{F}_{q^2}$-rational point of X.
(ii) $T_P \cap X = \{P\}$, where $T_P \subset \mathbb{P}^2$ is the tan. line to X at P.
(iii) P is a Weierstrass point of the curve X.

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

$$|\mathcal{P}_X| = q^3 + 1,$$

and $\mathrm{Aut}(X) = \mathrm{PGU}_3(\mathbb{F}_{q^2})$ acts on $\mathcal{P}_X$ double-transitively.

Definition

A smooth conic $C \subset \mathbb{P}^2$ is *totally tangent* to X if C is tangent to X at distinct $q+1$ points. Let $\mathcal{Q}_X$ denote the set of smooth conics totally tangent to X.

Since the conic $x^2 + y^2 + z^2 = 0$ is a member of $\mathcal{Q}_X$, we have $\mathcal{Q}_X \neq \emptyset$.

Theorem (Segre, S.-)

Suppose that and $q \geq 5$. Then $\mathrm{Aut}(X)$ acts on $\mathcal{Q}_X$ transitively with the stab. subgr. isom. to $\mathrm{PGL}_2(\mathbb{F}_q)$. Hence

$$|\mathcal{Q}_X| = q^2(q^3 + 1).$$

Moreover, every $C \in \mathcal{Q}_X$ is defined over $\mathbb{F}_{q^2}$ and satisfies $C \cap X \subset \mathcal{P}_X$.

Definition

A line $L \subset \mathbb{P}^n$ is a *special secant line* of X if L contains distinct two points of $\mathcal{P}_X$.
We denote by $\mathcal{S}_X$ the set of special secant lines of X.

We have

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

Every $L \in \mathcal{S}_X$ intersects X transversely, and satisfies $L \cap X \subset \mathcal{P}_X$.

Definition

A special secant line L of X is said to be a *special secant line of* $Q \in \mathcal{Q}_X$ 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.

We obviously have $|\mathcal{S}(Q)| = q(q+1)/2$.

Construction I

We work over an algebraically closed field of characteristic 5, and consider the Hermitian curve

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

of degree 6. We have

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

We define a graph $G = (V, E)$ by

- $V := \mathcal{Q}_X$, and
- $E := \{QQ' \mid \ |Q \cap Q'| = 4 \text{ and } |\mathcal{S}(Q) \cap \mathcal{S}(Q')| = 3 \ \}$.

Proposition

The graph G has exactly 150 connected components, and each connected component is isomorphic to the triangular graph $T(7)$, which is $\mathrm{srg}(21, 10, 5, 4)$.

Let $\mathcal{D}$ denote the set of connected components of G. Each $D \in \mathcal{D}$ is a collection of $3150/150 = 21$ conics in $\mathcal{Q}_X$.

Proposition

Let $D \in \mathcal{D}$ be a connected component of G. Then

$$Q \cap Q' \cap X = \emptyset$$

for any distinct conics $Q, Q' \in D$.

Since

$$|D| \times |Q \cap X| = 126 = |\mathcal{P}_X|,$$

each connected component D of G gives rise to a decomposition of $\mathcal{P}_X$ into a disjoint union of 21 sets of 6 points.

Proposition

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

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

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

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

We define $t(Q, D')$ to be α, β or γ according to the cases.

Proposition

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

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

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

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

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

We define $T(D, D')$ to be β^{21}, γ^{21}, $\alpha^{15}\gamma^{6}$ or $\alpha^{3}\gamma^{18}$ according to the cases. We have $T(D, D') = T(D', D)$.

We define $H = (V, E)$ by

- $V := \mathcal{D}$,
- $E := \{DD' \mid T(D, D') = \alpha^{15}\gamma^{6}\}$.

Theorem

The graph H has exactly three connected components, and each connected component is the Hoffman-Singleton graph.

Proposition

If D and D' are in the same connected component of H, then

$$T(D, D') = \gamma^{21} \ \ or \ \ \alpha^{15}\gamma^{6}.$$

If D and D' are in different connected components of H, then

$$T(D, D') = \beta^{21} \ \ or \ \ \alpha^{3}\gamma^{18}.$$

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 $\mathcal{C}_i$.

We define $H' = (V', E')$ by

- $V' := \mathcal{D}$,
- $E' := \{DD' \mid T(D, D') = \alpha^{15}\gamma^6 \text{ or } \beta^{21}\}$.

Then H' is a connected regular graph of valency 37.

Theorem

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 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 $\{D_1, D_2\} \sim \{D_1', D_2'\}$ 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 $\{D_1, D_2\}$ and $\{D_1', D_2'\}$.

Theorem

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 $\mathrm{srg}(50, 7, 0, 1)$,
$H'|(\mathcal{C}_i \cup \mathcal{C}_j)$ is $\mathrm{srg}(100, 22, 0, 6)$, and
H'' is $\mathrm{srg}(275, 112, 30, 56)$.

Remark

There are many other geometric ways to define the edges of H and H'.

Remark

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

For an element a of a set A on which $\mathrm{Aut}(X) = \mathrm{PGU}_3(\mathbb{F}_{25})$ acts, we denote by $\mathrm{stab}(a)$ the stabilizer subgroup in $\mathrm{PGU}_3(\mathbb{F}_{25})$ of a.

For $Q \in \mathcal{Q}_X$, we have $\mathrm{stab}(Q) \cong \mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$.

Theorem

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 $\mathrm{stab}(Q) \cap \mathrm{stab}(Q') \cong \mathfrak{A}_4$, and

Q and Q' are in the same connected component of G if and only if $\langle \mathrm{stab}(Q), \mathrm{stab}(Q') \rangle \cong \mathfrak{A}_7$.

Proposition

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

Let D and D' be distinct elements of $\mathcal{D}$. Then $T(D, D')$ is

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

Remark

By ATLAS, we see that the maximal subgroups of $\mathfrak{A}_7$ are

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

Construction II

Let Y be a smooth projective surface.

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.

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 over of $\mathbb{P}^2$ branched along the Hermitian curve $X \subset \mathbb{P}^2$.

Proposition

The Néron–Severi lattice S_Y is isomorphic to the unique lattice characterized by the following properties:

- *S_Y is even, hyperbolic, and of rank 22,*
- *$S_Y^{\vee}/S_Y \cong (\mathbb{Z}/5\mathbb{Z})^2$.*

In S_Y, we have the class

$$h_0 \in S_Y$$

of the pull-back of a line of $\mathbb{P}^2$ by the double covering $Y \to \mathbb{P}^2$.

Conway theory

Let U be the hyperbolic plane

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

and let Λ be the *negative definite* Leech lattice.
We put

$$L_{26} = U \oplus \Lambda,$$

which is an even unimodular hyperbolic lattice of rank 26.
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 reflections 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 $\mathcal{R}_0$.
Conway proved the following:

Theorem

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

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 (Katsura, Kondo, S.-)

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

$$\mathcal{V} := \{\ r_\lambda \in \mathcal{R}_0 \ \mid\ \langle \mathrm{pr}_S(r_\lambda), h_0 \rangle = 1,\ \ \mathrm{pr}_S(r_\lambda)^2 = -8/5\ \}$$

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

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 $\rho_1, \ldots, \rho_6$. We put

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

Each $\mathcal{V}_i$ has 50 vertices.

Theorem

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.

Thank you!