Models of $X_0(N)$ and beyond via modular forms and some applications (joint with I. Kodrnja) Representation theory XVII Dubrovnik 03-08.10.2022.

Goran Muić

October 5, 2022

Notation

Notation

$SL_2(\mathbb{R})$ is defined by

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane:

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ;\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az + b}{cz + d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az + b}{cz + d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az+b}{cz+d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

$\mathbb{H}$ can be regarded as a model for the hyperbolic plane with (invariant under $SL_2(\mathbb{R})$)

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az + b}{cz + d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

$\mathbb{H}$ can be regarded as a model for the hyperbolic plane with (invariant under $SL_2(\mathbb{R})$)

hyperbolic volume: $\frac{dxdy}{y^2}$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ;\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az+b}{cz+d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

$\mathbb{H}$ can be regarded as a model for the hyperbolic plane with (invariant under $SL_2(\mathbb{R})$)

hyperbolic volume: $\frac{dxdy}{y^2}$

hyperbolic distance: $ds^2 = \frac{dx^2+dy^2}{y^2}$

Fuchsian groups of the first kind

we are interested in discrete subgroups Γ of $SL_2(\mathbb{R})$

Fuchsian groups of the first kind

we are interested in discrete subgroups Γ of $SL_2(\mathbb{R})$ traditionally called **Fuchsian groups**

Fuchsian groups of the first kind

we are interested in discrete subgroups Γ of $SL_2(\mathbb{R})$ traditionally called **Fuchsian groups**

the hyperbolic geometry can be used to construct nice fundamental domains $\mathcal{F}_\Gamma$ for the action of Γ on $\mathbb{H}$

Fuchsian groups of the first kind

we are interested in discrete subgroups Γ of $SL_2(\mathbb{R})$ traditionally called **Fuchsian groups**

the hyperbolic geometry can be used to construct nice fundamental domains $\mathcal{F}_\Gamma$ for the action of Γ on $\mathbb{H}$
Main interest:

Fuchsian groups of the first kind

we are interested in discrete subgroups Γ of $SL_2(\mathbb{R})$ traditionally called **Fuchsian groups**

the hyperbolic geometry can be used to construct nice fundamental domains $\mathcal{F}_\Gamma$ for the action of Γ on $\mathbb{H}$
Main interest:
Γ is a **Fuchsian group of the first kind** if $\iint_{\mathcal{F}_\Gamma} \frac{dxdy}{y^2} < \infty$

Fuchsian groups of the first kind

$$\overset{Siegel}{\Longrightarrow}$$

$\overset{\textit{Siegel}}{\Longrightarrow}$ $\mathcal{F}_\Gamma$ is a polygon in the hyperbolic plane $\mathbb{H}$ with finitely many vertices: some of them might be at infinity

$\stackrel{Siegel}{\Longrightarrow}$ $\mathcal{F}_\Gamma$ is a polygon in the hyperbolic plane $\mathbb{H}$ with finitely many vertices: some of them might be at infinity $= \mathbb{R} \cup \{\infty\}$

Fuchsian groups of the first kind

$\overset{Siegel}{\Longrightarrow}$ $\mathcal{F}_\Gamma$ is a polygon in the hyperbolic plane $\mathbb{H}$ with finitely many vertices: some of them might be at infinity $= \mathbb{R} \cup \{\infty\}$

a Γ–conjugate of a vertex at infinity is **called cusp** for Γ

In what follows Γ always denotes a Fuchsian group of the first kind

Fuchsian groups of the first kind

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ
the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ
the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ
the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)=

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ
the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)=
complete (projective) non–singular irreducible algebraic curve over $\mathbb{C}$ (algebraic geometry)

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ
the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)$=$
complete (projective) non–singular irreducible algebraic curve over $\mathbb{C}$ (algebraic geometry) **Because:**

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)= complete (projective) non–singular irreducible algebraic curve over $\mathbb{C}$ (algebraic geometry) **Because:**

- a compact Riemann surface $\mathfrak{R}$ can be embedded in a complex projective space $\mathbb{P}^n$ for some n using suitable meromorphic functions;

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)=
complete (projective) non–singular irreducible algebraic curve over $\mathbb{C}$ (algebraic geometry)   **Because:**

- a compact Riemann surface $\mathfrak{R}$ can be embedded in a complex projective space $\mathbb{P}^n$ for some n using suitable meromorphic functions; **particular case is less analytic:**

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)$=$
complete (projective) non–singular irreducible algebraic curve over $\mathbb{C}$ (algebraic geometry)   **Because:**

- a compact Riemann surface $\mathfrak{R}$ can be embedded in a complex projective space $\mathbb{P}^n$ for some n using suitable meromorphic functions; **particular case is less analytic:** **modular forms are used to make this step explicit for $\mathfrak{R}_\Gamma$**

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)=
complete (projective) non–singular irreducible algebraic curve over $\mathbb{C}$ (algebraic geometry) **Because:**

- a compact Riemann surface $\mathfrak{R}$ can be embedded in a complex projective space $\mathbb{P}^n$ for some n using suitable meromorphic functions; **particular case is less analytic:**
  modular forms are used to make this step explicit for $\mathfrak{R}_\Gamma$
- Chow's theorem: the image is a complex irreducible smooth projective curve

Fuchsian groups of the first kind

Let $\mathbb{H}^*$ be the union of $\mathbb{H}$ and the set of all cusps for Γ the space $\mathfrak{R}_\Gamma$ of Γ–orbits for $\mathbb{H}^*$ has a structure of compact Riemann surface

compact Riemann surface (analysis)= complete (projective) non–singular irreducible algebraic curve over $\mathbb{C}$ (algebraic geometry) **Because:**

- a compact Riemann surface $\mathfrak{R}$ can be embedded in a complex projective space $\mathbb{P}^n$ for some n using suitable meromorphic functions; **particular case is less analytic:** **modular forms are used to make this step explicit for $\mathfrak{R}_\Gamma$**
- Chow's theorem: the image is a complex irreducible smooth projective curve $\Longrightarrow$ given by homogeneous polynomial equations

Examples Fuchsian groups of the first kind (Number theory)

Principal congruence subgroups:

Examples Fuchsian groups of the first kind (Number theory)

Principal congruence subgroups: let $N \geq 1$, we define

Examples Fuchsian groups of the first kind (Number theory)

Principal congruence subgroups: let $N \geq 1$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ a, d \equiv 1 \ (mod \ N),\ b, c \equiv 0 \ (mod \ N) \right\}$$

Examples Fuchsian groups of the first kind (Number theory)

Principal congruence subgroups: let $N \geq 1$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ a, d \equiv 1 \ (mod \ \ N),\ b, c \equiv 0 \ (mod \ \ N) \right\}$$

a congruence subgroup is a subgroup Γ of $SL_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$ for some $N \geq 1$.

Examples Fuchsian groups of the first kind (Number theory)

Principal congruence subgroups: let $N \geq 1$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ a, d \equiv 1\ (mod\ \ N),\ b, c \equiv 0\ (mod\ \ N) \right\}$$

a congruence subgroup is a subgroup Γ of $SL_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$ for some $N \geq 1$.
the most important congruence subgroups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ c \equiv 0\ (mod\ \ N) \right\}$$

Examples Fuchsian groups of the first kind (Number theory)

Principal congruence subgroups: let $N \geq 1$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ a, d \equiv 1\ (mod\ \ N),\ b, c \equiv 0\ (mod\ \ N) \right\}$$

a congruence subgroup is a subgroup Γ of $SL_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$ for some $N \geq 1$.
the most important congruence subgroups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ c \equiv 0\ (mod\ \ N) \right\}$$

the set of cusps for congruence subgroups is $\mathbb{Q} \cup \{\infty\}$

Examples Fuchsian groups of the first kind (Algebraic Geometry)

Let $C \subset \mathbb{P}^n$ be a smooth and irreducible projective complex curve of genus $g \geq 2$

Examples Fuchsian groups of the first kind (Algebraic Geometry)

Let $C \subset \mathbb{P}^n$ be a smooth and irreducible projective complex curve of genus $g \geq 2$

Uniformization theory:

Examples Fuchsian groups of the first kind (Algebraic Geometry)

Let $C \subset \mathbb{P}^n$ be a smooth and irreducible projective complex curve of genus $g \geq 2$

Uniformization theory: $C = \mathfrak{R}_\Gamma$, where

Examples Fuchsian groups of the first kind (Algebraic Geometry)

Let $C \subset \mathbb{P}^n$ be a smooth and irreducible projective complex curve of genus $g \geq 2$

Uniformization theory: $C = \mathfrak{R}_\Gamma$, where
$-1 \in \Gamma$ and $\Gamma/\{\pm 1\}$ is isomorphic to the fundamental group of C

Examples Fuchsian groups of the first kind (Algebraic Geometry)

Let $C \subset \mathbb{P}^n$ be a smooth and irreducible projective complex curve of genus $g \geq 2$

Uniformization theory: $C = \mathfrak{R}_\Gamma$, where
$-1 \in \Gamma$ and $\Gamma/\{\pm 1\}$ is isomorphic to the fundamental group of C

Γ has no cups

Examples Fuchsian groups of the first kind (Algebraic Geometry)

Let $C \subset \mathbb{P}^n$ be a smooth and irreducible projective complex curve of genus $g \geq 2$

Uniformization theory: $C = \mathfrak{R}_\Gamma$, where
$-1 \in \Gamma$ and $\Gamma/\{\pm 1\}$ is isomorphic to the fundamental group of C

Γ has no cups

$\mathbb{H}$ is the universal covering space for C:

Examples Fuchsian groups of the first kind (Algebraic Geometry)

Let $C \subset \mathbb{P}^n$ be a smooth and irreducible projective complex curve of genus $g \geq 2$

Uniformization theory: $C = \mathfrak{R}_\Gamma$, where
$-1 \in \Gamma$ and $\Gamma/\{\pm 1\}$ is isomorphic to the fundamental group of C

Γ has no cups

$\mathbb{H}$ is the universal covering space for C: $C = \Gamma \setminus \mathbb{H}$.

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma$, where

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma$, where

$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z), \quad$ for all $\; z \in \mathbb{H}, \; \gamma \in \Gamma$, where

$$j(\gamma, z) \overset{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f is holomorphic in cusps for Γ

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma$, where
$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
2. f is holomorphic in cusps for Γ
3. In addition, if f vanish at all cusps it is called a **cusp form**

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma$, where

$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f is holomorphic in cusps for Γ
3. In addition, if f vanish at all cusps it is called a **cusp form**

condition 2. is a technical condition which for $\Gamma = \Gamma_0(N)$ and the cusp ∞ means that

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma$, where
$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
2. f is holomorphic in cusps for Γ
3. In addition, if f vanish at all cusps it is called a **cusp form**

condition 2. is a technical condition which for $\Gamma = \Gamma_0(N)$ and the cusp ∞ means that f has a Fourier expansion so called q**–expansion**

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma$, where

$$j(\gamma, z) \overset{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f is holomorphic in cusps for Γ
3. In addition, if f vanish at all cusps it is called a **cusp form**

condition 2. is a technical condition which for $\Gamma = \Gamma_0(N)$ and the cusp ∞ means that f has a Fourier expansion so called q**–expansion**

$$f(z) = a_0 + a_1 q + a_2 q^2 + \cdots, \quad q = \exp\left(2\pi\sqrt{-1}z\right),$$

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for Γ of (integral) weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma$, where

$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f is holomorphic in cusps for Γ
3. In addition, if f vanish at all cusps it is called a **cusp form**

condition 2. is a technical condition which for $\Gamma = \Gamma_0(N)$ and the cusp ∞ means that f has a Fourier expansion so called q–**expansion**

$$f(z) = a_0 + a_1 q + a_2 q^2 + \cdots, \quad q = \exp\left(2\pi\sqrt{-1}z\right),$$

and condition 3. f means $a_0 = 0$

Modular forms of one variable

Famous example: Ramanujan Δ function is a cusp form for $SL_2(\mathbb{Z}) = \Gamma_0(1)$ of weight 12:

Famous example: Ramanujan Δ function is a cusp form for $SL_2(\mathbb{Z}) = \Gamma_0(1)$ of weight 12:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - \cdots$$

Famous example: Ramanujan Δ function is a cusp form for $SL_2(\mathbb{Z}) = \Gamma_0(1)$ of weight 12:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - \cdots$$

Coefficients in the q–expansion of modular forms usually carry deep arithmetic information

Cuspidal forms of one variable

Let $S_m(\Gamma)$ be the vector space of all cusp forms for Γ

Let $S_m(\Gamma)$ be the vector space of all cusp forms for Γ

Riemann–Roch theorem for the curve $\mathfrak{R}_\Gamma$

Cuspidal forms of one variable

Let $S_m(\Gamma)$ be the vector space of all cusp forms for Γ

Riemann–Roch theorem for the curve $\mathfrak{R}_\Gamma$

- $\implies$ $\dim S_m(\Gamma)$ is finite dimensional

Cuspidal forms of one variable

Let $S_m(\Gamma)$ be the vector space of all cusp forms for Γ

Riemann–Roch theorem for the curve $\mathfrak{R}_\Gamma$

- $\implies$ $\dim S_m(\Gamma)$ is finite dimensional
- $\implies$ the formula for the dimension of $S_m(\Gamma)$ when $m \geq 2$

Let $S_m(\Gamma)$ be the vector space of all cusp forms for Γ

Riemann–Roch theorem for the curve $\mathfrak{R}_\Gamma$

- $\Longrightarrow$ $\dim S_m(\Gamma)$ is finite dimensional
- $\Longrightarrow$ the formula for the dimension of $S_m(\Gamma)$ when $m \geq 2$

For applications in number theory, there are various ways of construction bases for $S_m(\Gamma)$ especially when $\Gamma = \Gamma_0(N)$

Cuspidal forms of one variable for $\Gamma_0(N)$

Cuspidal forms of one variable for $\Gamma_0(N)$

In fact, there are computer systems such as SAGE or MAGMA for computing with modular forms.

In fact, there are computer systems such as SAGE or MAGMA for computing with modular forms. **For example,** computation of q–expansions of certain bases of $S_m(\Gamma_0(N))$.

In fact, there are computer systems such as SAGE or MAGMA for computing with modular forms. **For example,** computation of q–expansions of certain bases of $S_m(\Gamma_0(N))$.

This is very useful for computing explicit embeddings of curves $\mathfrak{R}_{\Gamma_0(N)}$ in various complex $\mathbb{P}^N$ resulting in explicit equations.

In fact, there are computer systems such as SAGE or MAGMA for computing with modular forms. **For example,** computation of q–expansions of certain bases of $S_m(\Gamma_0(N))$.

This is very useful for computing explicit embeddings of curves $\mathfrak{R}_{\Gamma_0(N)}$ in various complex $\mathbb{P}^N$ resulting in explicit equations.

That was studied by many people (including very recently some of my works joint with Kodrnja). For that computations, the space of weight two cusp forms for $\Gamma_0(N)$ is especially useful since it canonically isomorphic to the space of holomorphic differentials on the curve.

Maps into $\mathbb{P}^2$

Maps into $\mathbb{P}^2$

Assume that Γ has at least one cusp e.g. $\Gamma = \Gamma_0(N)$. Let $g(\Gamma)$ be the genus of $\mathfrak{R}_\Gamma$.

Maps into $\mathbb{P}^2$

Assume that Γ has at least one cusp e.g. $\Gamma = \Gamma_0(N)$. Let $g(\Gamma)$ be the genus of $\mathfrak{R}_\Gamma$.

Let $m \geq 2$ an **even integer**, such that $\dim M_m(\Gamma) \geq 3$.

Maps into $\mathbb{P}^2$

Assume that Γ has at least one cusp e.g. $\Gamma = \Gamma_0(N)$. Let $g(\Gamma)$ be the genus of $\mathfrak{R}_\Gamma$.

Let $m \geq 2$ an **even integer**, such that $\dim M_m(\Gamma) \geq 3$.

Let f, g, h be three linearly independent modular forms in $M_m(\Gamma)$.

Maps into $\mathbb{P}^2$

Assume that Γ has at least one cusp e.g. $\Gamma = \Gamma_0(N)$. Let $g(\Gamma)$ be the genus of $\mathfrak{R}_\Gamma$.

Let $m \geq 2$ an **even integer**, such that $\dim M_m(\Gamma) \geq 3$.

Let f, g, h be three linearly independent modular forms in $M_m(\Gamma)$.

Then, we define a holomorphic (regular) map

$$\mathfrak{R}_\Gamma \to \mathbb{P}^2$$

by

$$\begin{aligned} \Gamma \backslash \mathbb{H} &\longrightarrow \mathbb{P}^2 \\ z &\longmapsto (f(z) : g(z) : h(z)). \end{aligned} \tag{0-1}$$

Maps into $\mathbb{P}^2$

Maps into $\mathbb{P}^2$

Since $\mathfrak{R}_\Gamma$ has a canonical structure of complex projective irreducible algebraic curve, this map can be regarded as a regular map between projective varieties. Consequently, the image is an irreducible projective curve which we denote by $\mathcal{C}(f, g, h)$.

Maps into $\mathbb{P}^2$

Since $\mathfrak{R}_\Gamma$ has a canonical structure of complex projective irreducible algebraic curve, this map can be regarded as a regular map between projective varieties. Consequently, the image is an irreducible projective curve which we denote by $\mathcal{C}(f, g, h)$.

The degree $d(f, g, h)$ of the map (0-1) is by definition the degree of the field extension of the fields of rational functions:

$$\mathbb{C}\left(\mathcal{C}(f, g, h)\right) \subset \mathbb{C}\left(\mathfrak{R}_\Gamma\right).$$

Maps into $\mathbb{P}^2$

Since $\mathfrak{R}_\Gamma$ has a canonical structure of complex projective irreducible algebraic curve, this map can be regarded as a regular map between projective varieties. Consequently, the image is an irreducible projective curve which we denote by $\mathcal{C}(f, g, h)$.

The degree $d(f, g, h)$ of the map (0-1) is by definition the degree of the field extension of the fields of rational functions:

$$\mathbb{C}\left(\mathcal{C}(f, g, h)\right) \subset \mathbb{C}\left(\mathfrak{R}_\Gamma\right).$$

The degree $\deg \mathcal{C}(f, g, h)$ of the curve $\mathcal{C}(f, g, h)$ is the degree of the reduced homogeneous equation defining $\mathcal{C}(f, g, h)$ in $\mathbb{P}^2$

Description of $d(f, g, h) \cdot \deg \mathcal{C}(f, g, h)$

Description of $d(f, g, h) \cdot \deg \mathcal{C}(f, g, h)$

Any $f \in M_m(\Gamma)$, $f \neq 0$ has a divisor which has the form

$$\mathrm{div}(f) = (\text{the part independent of } f) + \mathfrak{c}'_f,$$

Any $f \in M_m(\Gamma)$, $f \neq 0$ has a divisor which has the form

$$\mathrm{div}(f) = (\text{the part independent of } f) + \mathfrak{c}'_f,$$

$\mathfrak{c}'_f$ is usual divisor on the curve $\mathfrak{R}_\Gamma$

Description of $d(f,g,h) \cdot \deg \mathcal{C}(f,g,h)$

Any $f \in M_m(\Gamma)$, $f \neq 0$ has a divisor which has the form

$$\mathrm{div}(f) = (\text{the part independent of } f) + \mathfrak{c}'_f,$$

$\mathfrak{c}'_f$ is usual divisor on the curve $\mathfrak{R}_\Gamma$

We write

$$\mathfrak{c}'_f = \sum_{\mathfrak{a} \in \mathfrak{R}_\Gamma} \nu_\mathfrak{a}(f)\mathfrak{a} \ \ \text{(a finite sum)}, \ \ \mathfrak{c}'_f(\mathfrak{a}) = \nu_\mathfrak{a}(f)$$

Description of $d(f,g,h)\cdot\deg\mathcal{C}(f,g,h)$

Any $f\in M_m(\Gamma)$, $f\neq 0$ has a divisor which has the form

$$\mathrm{div}(f) = (\text{the part independent of } f) + \mathfrak{c}'_f,$$

$\mathfrak{c}'_f$ is usual divisor on the curve $\mathfrak{R}_\Gamma$

We write

$$\mathfrak{c}'_f = \sum_{\mathfrak{a}\in\mathfrak{R}_\Gamma} \nu_{\mathfrak{a}}(f)\mathfrak{a} \ \ (\text{a finite sum}), \quad \mathfrak{c}'_f(\mathfrak{a}) = \nu_{\mathfrak{a}}(f)$$

When $f\in S_m(\Gamma)$, we define another divisor

$$\mathfrak{c}_f = \mathfrak{c}'_f - \sum_{\substack{\mathfrak{a}\in\mathfrak{R}_\Gamma \\ \mathfrak{a}\ \text{cusp}}} \mathfrak{a}$$

Description of $d(f,g,h) \cdot \deg \mathcal{C}(f,g,h)$

Description of $d(f,g,h)\cdot\deg\mathcal{C}(f,g,h)$

Theorem (M.)

We have the following:

$$d(f,g,h)\cdot\deg\mathcal{C}(f,g,h) =$$
$$\begin{cases}\dim M_m(\Gamma)+g(\Gamma)-1-\sum_{\mathfrak{a}\in\mathfrak{R}_\Gamma}\min\left(\mathfrak{c}'_f(\mathfrak{a}),\mathfrak{c}'_g(\mathfrak{a}),\mathfrak{c}'_h(\mathfrak{a})\right),\\ \dim S_m(\Gamma)+g(\Gamma)-1-\epsilon_m-\sum_{\mathfrak{a}\in\mathfrak{R}_\Gamma}\min\left(\mathfrak{c}_f(\mathfrak{a}),\mathfrak{c}_g(\mathfrak{a}),\mathfrak{c}_h(\mathfrak{a})\right),\\ \qquad \text{if } f,g,h\in S_m(\Gamma),\end{cases}$$

where $\epsilon_2 = 1$ *and* $\epsilon_m = 0$ *for* m *even,* $m \geq 4$.

Models of $\mathfrak{X}_\Gamma$

$\mathcal{C}(f, g, h)$ is a **model of** $\mathfrak{X}_\Gamma$ if the map (0-1) defines birational equivalence, or equivalently $d(f, g, h) = 1$

$\mathcal{C}(f, g, h)$ is a **model of** $\mathfrak{R}_\Gamma$ if the map (0-1) defines birational equivalence, or equivalently $d(f, g, h) = 1$

In this case, the theorem implies

$$\deg \mathcal{C}(f, g, h) = \begin{cases} \dim M_m(\Gamma) + g(\Gamma) - 1 - \sum_{\mathfrak{a} \in \mathfrak{R}_\Gamma} \min\left(\mathfrak{c}'_f(\mathfrak{a}), \mathfrak{c}'_g(\mathfrak{a}), \mathfrak{c}'_h(\mathfrak{a})\right), \\ \dim S_m(\Gamma) + g(\Gamma) - 1 - \epsilon_m - \sum_{\mathfrak{a} \in \mathfrak{R}_\Gamma} \min\left(\mathfrak{c}_f(\mathfrak{a}), \mathfrak{c}_g(\mathfrak{a}), \mathfrak{c}_h(\mathfrak{a})\right), \\ \qquad \text{if } f, g, h \in S_m(\Gamma) \end{cases}$$

Definition

Let $W \subset M_m(\Gamma)$ be a non-zero linear subspace. Then, we say that W determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$ *if* $\dim W \geq 2$, *and there exists a basis $f_0, \ldots, f_{s-1}$ of W, such that $\mathbb{C}(\mathfrak{R}_\Gamma)$ is generated over $\mathbb{C}$ by the quotients f_i/f_0, $1 \leq i \leq s-1$.*

Models of $\mathfrak{R}_\Gamma$

Definition

Let $W \subset M_m(\Gamma)$ be a non-zero linear subspace. Then, we say that W determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$ *if* $\dim W \geq 2$, *and there exists a basis $f_0, \ldots, f_{s-1}$ of W, such that $\mathbb{C}(\mathfrak{R}_\Gamma)$ is generated over $\mathbb{C}$ by the quotients f_i/f_0, $1 \leq i \leq s-1$.*

This notion does not depend on the choice of the basis used. Also, it is equivalent to the fact that the holomorphic map $\mathfrak{R}_\Gamma \longrightarrow \mathbb{P}^{s-1}$ given by $z \mapsto (f_0(z) : \cdots : f_{s-1}(z))$ is birational onto its image in $\mathbb{P}^{s-1}$.

Models of $\mathfrak{R}_\Gamma$

Definition

Let $W \subset M_m(\Gamma)$ be a non-zero linear subspace. Then, we say that W determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$ *if* $\dim W \geq 2$, *and there exists a basis $f_0, \ldots, f_{s-1}$ of W, such that $\mathbb{C}(\mathfrak{R}_\Gamma)$ is generated over $\mathbb{C}$ by the quotients f_i/f_0, $1 \leq i \leq s-1$.*

This notion does not depend on the choice of the basis used. Also, it is equivalent to the fact that the holomorphic map $\mathfrak{R}_\Gamma \longrightarrow \mathbb{P}^{s-1}$ given by $z \mapsto (f_0(z) : \cdots : f_{s-1}(z))$ is birational onto its image in $\mathbb{P}^{s-1}$.

For example, if $\dim S_m(\Gamma) \geq \max(g(\Gamma)+2, 3)$, then we can take $W = S_m(\Gamma)$ by general theory of algebraic curves

Models of $\mathfrak{R}_\Gamma$

Definition

Let $W \subset M_m(\Gamma)$ be a non-zero linear subspace. Then, we say that W determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$ *if* $\dim W \geq 2$, *and there exists a basis $f_0, \ldots, f_{s-1}$ of W, such that $\mathbb{C}(\mathfrak{R}_\Gamma)$ is generated over $\mathbb{C}$ by the quotients f_i/f_0, $1 \leq i \leq s-1$.*

This notion does not depend on the choice of the basis used. Also, it is equivalent to the fact that the holomorphic map $\mathfrak{R}_\Gamma \longrightarrow \mathbb{P}^{s-1}$ given by $z \mapsto (f_0(z) : \cdots : f_{s-1}(z))$ is birational onto its image in $\mathbb{P}^{s-1}$.

For example, if $\dim S_m(\Gamma) \geq \max(g(\Gamma)+2, 3)$, then we can take $W = S_m(\Gamma)$ by general theory of algebraic curves

We recall that $\mathfrak{R}_\Gamma$ is hyperelliptic if $g(\Gamma) \geq 2$, and there is a degree two map onto $\mathbb{P}^1$. If $\mathfrak{R}_\Gamma$ is not hyperelliptic, then $\dim S_2(\Gamma) = g(\Gamma) \geq 3$, and we can take $W = S_2(\Gamma)$

Models of $\mathfrak{R}_\Gamma$

We recall that $g(\Gamma_0(N)) \geq 2$ unless

$$\begin{cases} N \in \{1-10, 12, 13, 16, 18, 25\} & \text{when } g(\Gamma_0(N)) = 0, \text{ and} \\ N \in \{11, 14, 15, 17, 19-21, 24, 27, 32, 36, 49\} & \text{when } g(\Gamma_0(N)) = 1. \end{cases}$$

Let $g(\Gamma_0(N)) \geq 2$. Ogg has determined all $X_0(N)$ which are hyperelliptic curves. In view of Ogg's paper, we see that $X_0(N)$ is not hyperelliptic for $N \in \{34, 38, 42, 43, 44, 45, 51-58, 60-70\}$ or $N \geq 72$. This implies $g(\Gamma_0(N)) \geq 3$.

Simple example: Models of $\mathfrak{X}_\Gamma$

Proposition

Consider three linearly independent forms from the four dimensional space $S_4(\Gamma_0(14))$ of cusp forms of weight four for $\Gamma_0(14)$:

$$f = q^2 - 2q^5 - 2q^6 + q^7 - 6q^8 + 12q^{10} + 4q^{11} + 2q^{13} + \cdots,$$
$$g = q^3 - q^5 - 2q^6 - q^7 - 4q^8 + 6q^9 + 10q^{10} - 6q^{11} + \cdots,$$
$$h = q^4 - 2q^5 + q^7 + q^8 - 4q^{10} + 4q^{11} - 2q^{12} + 2q^{13} + \cdots.$$

Then, the map (0-1) is a birational equivalence of $X_0(14)$ and $\mathcal{C}(f,g,h)$. Moreover, $\deg \mathcal{C}(f,g,h) = 3$.

Simple example: Models of $\mathfrak{R}_\Gamma$

Proposition

Consider three linearly independent forms from the four dimensional space $S_4(\Gamma_0(14))$ of cusp forms of weight four for $\Gamma_0(14)$:

$$f = q^2 - 2q^5 - 2q^6 + q^7 - 6q^8 + 12q^{10} + 4q^{11} + 2q^{13} + \cdots,$$
$$g = q^3 - q^5 - 2q^6 - q^7 - 4q^8 + 6q^9 + 10q^{10} - 6q^{11} + \cdots,$$
$$h = q^4 - 2q^5 + q^7 + q^8 - 4q^{10} + 4q^{11} - 2q^{12} + 2q^{13} + \cdots.$$

Then, the map (0-1) is a birational equivalence of $X_0(14)$ and $\mathcal{C}(f,g,h)$. Moreover, $\deg \mathcal{C}(f,g,h) = 3$.

Proof: Let $\mathfrak{a}_\infty$ be the $\Gamma_0(14)$–orbit of the cusp ∞. Since the forms have at least double zero at $\mathfrak{a}_\infty$, and f has exactly double zero, we have

Simple example: Models of $\mathfrak{R}_\Gamma$

$$\sum_{\mathfrak{a} \in X_0(14)} \min\left(\mathfrak{c}_f(\mathfrak{a}), \mathfrak{c}_g(\mathfrak{a}), \mathfrak{c}_h(\mathfrak{a})\right) \geq \min\left(\mathfrak{c}_f(\mathfrak{a}_\infty), \mathfrak{c}_g(\mathfrak{a}_\infty), \mathfrak{c}_h(\mathfrak{a}_\infty)\right) = 1.$$

$$\implies 1 \leq d(f,g,h) \cdot \deg \mathcal{C}(f,g,h) \leq$$
$$\leq \dim S_4(\Gamma_0(14)) + g(\Gamma_0(14)) - 1 - \epsilon_4 - 1 = 3$$

$$\implies g(\Gamma_0(14)) = 1 \implies \deg \mathcal{C}(f,g,h) \in \{1,2,3\}.$$

But $\deg \mathcal{C}(f,g,h) = 1$ means that $\mathcal{C}(f,g,h)$ is a line which is clearly impossible since f, g, and h are linearly independent. The case $\deg \mathcal{C}(f,g,h) = 2$ means that $\mathcal{C}(f,g,h)$ is an irreducible conic. Using

$$2d(f,g,h) = d(f,g,h) \cdot \deg \mathcal{C}(f,g,h) \leq 3,$$

we must have

$$d(f,g,h) = 1$$

This means that $X_0(14)$ is birationally equivalent to the conic $\mathcal{C}(f,g,h)$. But irreducible conic is non-singular. This means that $X_0(14)$ isomorphic to a conic. This is a contradiction since conic has genus 0 while $X_0(14)$ has genus 1.
Thus, $\deg \mathcal{C}(f,g,h) = 3$. Consequently, $d(f,g,h) = 1$ proving the proposition.

Models of $\mathfrak{R}_\Gamma$

Theorem (Kodrnja-M.)

Assume that $m \geq 2$ is an even integer. Let $W \subset M_m(\Gamma)$, $\dim W \geq 3$, be a subspace which determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$ (see Definition 0-3). Let $f, g \in W$ be linearly independent. Then there exists a non-empty Zariski open set $\mathcal{U} \subset W$ such that for any $h \in \mathcal{U}$ we have the following:

(i) *f, g, and h are linearly independent;*

(ii) *$\mathfrak{R}_\Gamma$ is birationally equivalent to $\mathcal{C}(f, g, h)$ via the map (0-1).*

Theorem (Kodrnja-M.)

Assume that $m \geq 2$ is an even integer. Let $W \subset M_m(\Gamma)$, $\dim W \geq 3$, be a subspace which determines the field of rational functions $\mathbb{C}(\mathfrak{X}_\Gamma)$ (see Definition 0-3). Let $f, g \in W$ be linearly independent. Then there exists a non-empty Zariski open set $\mathcal{U} \subset W$ such that for any $h \in \mathcal{U}$ we have the following:

(i) *f, g, and h are linearly independent;*

(ii) *$\mathfrak{X}_\Gamma$ is birationally equivalent to $\mathcal{C}(f, g, h)$ via the map (0-1).*

Problem: Given f, g, determine h such that $\mathcal{C}(f, g, h)$ is a model of $\mathfrak{X}_\Gamma$

Corollary

Let $m \geq 2$ be an even integer. Assume that one of the following holds:

(A) $g(\Gamma_0(N)) \geq 1$, *and* $m \geq 4$ *(if* $N \neq 11$*) or* $m \geq 6$ *(if* $N = 11$*);*

(B) $X_0(N)$ *is not hyperelliptic, and* $m = 2$.

(In either case, $\dim S_m(\Gamma_0(N)) \geq 3$.*) Let* $f, g \in S_m(\Gamma_0(N))$ *be linearly independent with integral q-expansions. Then, there exists infinitely many* $h \in S_m(\Gamma_0(N))$ *with integral q–expansion such that we have the following:*

(i) $X_0(N) \stackrel{def}{=} \mathfrak{X}_{\Gamma_0(N)}$ *is birationally equivalent to* $\mathcal{C}(f, g, h)$ *via the map (0-1), and*

(ii) *the reduced equation of* $\mathcal{C}(f, g, h)$ *has integral coefficients up to a multiplication by a non-zero constant in* $\mathbb{C}$.

Some methods for explicit determination of h

Some methods for explicit determination of h

Problem: Given f, g (subject to the condition of the theorem), determine h such that $\mathcal{C}(f, g, h)$ is a model of $\mathfrak{R}_\Gamma$

Problem: Given f, g (subject to the condition of the theorem), determine h such that $\mathcal{C}(f, g, h)$ is a model of $\mathfrak{R}_\Gamma$

We offer two solutions:

Problem: Given f, g (subject to the condition of the theorem), determine h such that $\mathcal{C}(f, g, h)$ is a model of $\mathfrak{R}_\Gamma$

We offer two solutions:

1) the method of estimates for Primitive Elements in finite extensions of algebriac function fields

Some methods for explicit determination of h

Problem: Given f, g (subject to the condition of the theorem), determine h such that $\mathcal{C}(f, g, h)$ is a model of $\mathfrak{R}_\Gamma$

We offer two solutions:

1) the method of estimates for Primitive Elements in finite extensions of algebriac function fields

2) the trial method for determining primitive element in finite extensions of algebriac function fields , commonly used in the cases of algebraic number fields

Proposition

Assume that $m \geq 2$ is an even integer. Let $W \subset M_m(\Gamma)$, $\dim W = 4$, be a subspace which determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$ (see Definition 0-3). Select a basis $\{f = f_0, g = f_1, f_2, f_3\}$ of W. We assume that all f_i has integral q–expansions. Then, there exists an explicitly computable *$c_0 \in \mathbb{Z}$ such that for all $c \in \mathbb{Z}$, $|c| \geq c_0$, $\mathfrak{R}_\Gamma$ is birationally equivalent to $\mathcal{C}(f, g, h_c)$ via the map (0-1) with $h = h_c$, where $h_c \overset{def}{=} f_2 + cf_3$.*

Example for the method of estimates for Primitive Elements

Proposition

Consider the four dimensional space $W \stackrel{def}{=} S_4(\Gamma_0(14))$ *of cusp forms of weight four for* $\Gamma_0(14)$. *It has a basis:*

$$f = f_0 = q - 2q^5 - 4q^6 - q^7 + 8q^8 - 11q^9 - 12q^{10} + 12q^{11} + \cdots,$$
$$g = f_1 = q^2 - 2q^5 - 2q^6 + q^7 - 6q^8 + 12q^{10} + 4q^{11} + 2q^{13} + \cdots,$$
$$f_2 = q^3 - q^5 - 2q^6 - q^7 - 4q^8 + 6q^9 + 10q^{10} - 6q^{11} + \cdots,$$
$$f_3 = q^4 - 2q^5 + q^7 + q^8 - 4q^{10} + 4q^{11} - 2q^{12} + 2q^{13} + \cdots.$$

Put $h_c \stackrel{def}{=} f_2 + cf_3$, $c \in \mathbb{Z}$, *as in the statement of the previous proposition. Then,* $X_0(14)$ *is birationally equivalent to* $\mathcal{C}(f, g, h_c)$ *via the map (0-1) with* $h = h_c$ *for* $|c| \geq 7$.

The trial method

The trial method

Let $W \subset S_m(\Gamma)$, $m \geq 2$, be a non-zero subspace that determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$

The trial method

Let $W \subset S_m(\Gamma)$, $m \geq 2$, be a non-zero subspace that determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$
Assume that $\dim W = s \geq 4$

The trial method

Let $W \subset S_m(\Gamma)$, $m \geq 2$, be a non-zero subspace that determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$

Assume that $\dim W = s \geq 4$

Let $f_0, \ldots, f_{s-1}$ be a basis of W. We let $f = f_0$ and $g = f_1$.

The trial method

Let $W \subset S_m(\Gamma)$, $m \geq 2$, be a non-zero subspace that determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$
Assume that $\dim W = s \geq 4$
Let $f_0, \ldots, f_{s-1}$ be a basis of W. We let $f = f_0$ and $g = f_1$.
Let $K \overset{def}{=} \mathbb{C}(f/g)$, and

$$L \overset{def}{=} \mathbb{C}(\mathfrak{R}_\Gamma) = \mathbb{C}(f_1/f_0,\ f_2/f_0,\ \ldots,\ f_{s-1}/f_0) = \mathbb{C}(f/g,\ f_2/f,\ \ldots,\ f_{s-1}/f)$$

The trial method

Let $W \subset S_m(\Gamma)$, $m \geq 2$, be a non-zero subspace that determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$
Assume that $\dim W = s \geq 4$
Let $f_0, \ldots, f_{s-1}$ be a basis of W. We let $f = f_0$ and $g = f_1$.
Let $K \overset{def}{=} \mathbb{C}(f/g)$, and

$$L \overset{def}{=} \mathbb{C}(\mathfrak{R}_\Gamma) = \mathbb{C}(f_1/f_0,\ f_2/f_0,\ \ldots,\ f_{s-1}/f_0) = \mathbb{C}(f/g,\ f_2/f,\ \ldots,\ f_{s-1}/f)$$

L is a finite algebraic extension of K, and we have the following:

$$L = K(f_2/f_0,\ \ldots,\ f_{s-1}/f_0).$$

The trial method

Let $W \subset S_m(\Gamma)$, $m \geq 2$, be a non-zero subspace that determines the field of rational functions $\mathbb{C}(\mathfrak{R}_\Gamma)$

Assume that $\dim W = s \geq 4$

Let $f_0, \ldots, f_{s-1}$ be a basis of W. We let $f = f_0$ and $g = f_1$.

Let $K \stackrel{def}{=} \mathbb{C}(f/g)$, and

$$L \stackrel{def}{=} \mathbb{C}(\mathfrak{R}_\Gamma) = \mathbb{C}(f_1/f_0,\ f_2/f_0,\ \ldots,\ f_{s-1}/f_0) = \mathbb{C}(f/g,\ f_2/f,\ \ldots,\ f_{s-1}/f)$$

L is a finite algebraic extension of K, and we have the following:

$$L = K(f_2/f_0,\ \ldots,\ f_{s-1}/f_0).$$

interested in finding a primitive element of L over K which has the form of linear combination of the generators $f_2/f_0, \ldots, f_{s-1}/f_0$

The trial method

The trial method

For $a \overset{def}{=} (a_2, a_3, \ldots, a_{s-1}) \in \mathbb{Z}^{s-2}$, we let

$$h \overset{def}{=} h_a \overset{def}{=} a_2 f_2/f_0 + \cdots + a_{s-1} f_{s-1}/f_0 \in L.$$

The trial method

For $a \stackrel{def}{=} (a_2, a_3, \ldots, a_{s-1}) \in \mathbb{Z}^{s-2}$, we let

$$h \stackrel{def}{=} h_a \stackrel{def}{=} a_2 f_2/f_0 + \cdots + a_{s-1} f_{s-1}/f_0 \in L.$$

by the main theorem

$$d(f, g, h) \cdot \deg \mathcal{C}(f, g, h) \leq \dim S_m(\Gamma) + g(\Gamma) - 1 - \epsilon_m,$$

The trial method

For $a \stackrel{def}{=} (a_2, a_3, \ldots, a_{s-1}) \in \mathbb{Z}^{s-2}$, we let

$$h \stackrel{def}{=} h_a \stackrel{def}{=} a_2 f_2/f_0 + \cdots + a_{s-1} f_{s-1}/f_0 \in L.$$

by the main theorem

$$d(f,g,h) \cdot \deg \mathcal{C}(f,g,h) \leq \dim S_m(\Gamma) + g(\Gamma) - 1 - \epsilon_m,$$

Thus, if we have

$$\deg \mathcal{C}(f,g,h) > \frac{\dim S_m(\Gamma) + g(\Gamma) - 1 - \epsilon_m}{2},$$

then $d(f,g,h) = 1$ i.e., $\mathcal{C}(f,g,h)$ is a model of $\mathfrak{R}_\Gamma$.

The trial method

For $a \stackrel{def}{=} (a_2, a_3, \ldots, a_{s-1}) \in \mathbb{Z}^{s-2}$, we let

$$h \stackrel{def}{=} h_a \stackrel{def}{=} a_2 f_2/f_0 + \cdots + a_{s-1} f_{s-1}/f_0 \in L.$$

by the main theorem

$$d(f,g,h) \cdot \deg \mathcal{C}(f,g,h) \leq \dim S_m(\Gamma) + g(\Gamma) - 1 - \epsilon_m,$$

Thus, if we have

$$\deg \mathcal{C}(f,g,h) > \frac{\dim S_m(\Gamma) + g(\Gamma) - 1 - \epsilon_m}{2},$$

then $d(f,g,h) = 1$ i.e., $\mathcal{C}(f,g,h)$ is a model of $\mathfrak{R}_\Gamma$.
We organize $(s-2)$–tuples in $\mathbb{Z}^{s-2}$ as follows:

$$S_M \stackrel{def}{=} \left\{ a_2 f_2/f_0 + \cdots + a_{s-1} f_{s-1}/f_0;\, a_i \in \mathbb{Z}, \sum_{i=2}^{s-1} |a_i| = M \right\},$$

for all $M \in \mathbb{Z}_{\geq 1}$. For $M \geq 1$, we order elements of S_M using the lexicographical order.

The algorithm:

(1) Let $M = 1$. Repeat the following:

(2) For $a \in S_M$, we repeat the following: compute $\deg \mathcal{C}(f, g, h)$ (by means of computing the equation), and check if $\deg \mathcal{C}(f, g, h) > \frac{\dim S_m(\Gamma) + g(\Gamma) - 1 - \epsilon_m}{2}$ for $h = h_a$. If the holds, then the algorithm stops. OUTPUT: h such that h/f is a primitive element for the extension $K \subset L$.

(3) Increase M by one, and return to step (2).

Example: The trial method

Example: The trial method

Let $\Gamma = \Gamma_0(N)$ such that $g(\Gamma_0(N)) \geq 4$, and $X_0(N)$ is not hyperelliptic $\implies$ we may take $W = S_2(\Gamma_0(N))$. In this case we need to test

$$\deg \mathcal{C}(f, g, h) > g(\Gamma_0(N)) - 1.$$

Example: The trial method

Let $\Gamma = \Gamma_0(N)$ such that $g(\Gamma_0(N)) \geq 4$, and $X_0(N)$ is not hyperelliptic $\implies$ we may take $W = S_2(\Gamma_0(N))$. In this case we need to test

$$\deg \mathcal{C}(f, g, h) > g(\Gamma_0(N)) - 1.$$

As an example, we consider the case $N = 72$. Then, $g(\Gamma_0(72)) = 5$, and we may take

$$\begin{aligned} f = f_0 &= q^3 - q^9 - 2q^{15} + q^{27} + 4q^{33} - 2q^{39} + \cdots , \\ g = f_1 &= q^5 - 2q^{11} - q^{17} + 4q^{23} - 3q^{29} + \cdots , \\ f_2 &= q^7 - q^{13} - 3q^{19} + q^{25} + 3q^{31} + 4q^{37} + \cdots , \\ f_3 &= q - 2q^{13} - 4q^{19} - q^{25} + 8q^{31} + 6q^{37} + \cdots , \\ f_4 &= q^2 - 4q^{14} + 2q^{26} + 8q^{38} + \cdots , \end{aligned}$$

Example: The trial method

Example: The trial method

Applying above algorithm, we obtain the following:

(1) For $M = 1$, we have three cases in their lexicographical order $a = (0, 0, 1)$, $(0, 1, 0)$, and $(1, 0, 0)$. We have $\deg \mathcal{C}(f, g, h_a) = 3$, 2, and 3, respectively. In any case, $\deg \mathcal{C}(f, g, h_a) \leq g(\Gamma_0(72)) - 1 = 4$. So, we go to the next step.

(2) For $M = 2$, in the lexicographical order, we have the following:

1. $a = (0, 0, 2)$, $\deg \mathcal{C}(f, g, h_a) = 3 \leq g(\Gamma_0(72)) - 1 = 4$;
2. $a = (0, 1, 1)$, $\deg \mathcal{C}(f, g, h_a) = 3 \leq 4$;
3. $a = (0, 2, 0)$, $\deg \mathcal{C}(f, g, h_a) = 2 \leq 4$;
4. $a = (1, 0, 1)$, $\deg \mathcal{C}(f, g, h_a) = 7 > 4$; STOP.

Example: The trial method

hence, for $h = h_{(1,0,1)}$ is a birational equivalence of $X_0(72)$ and $\mathcal{C}(f, g, h_{(1,0,1)})$. The reduced equation of $\mathcal{C}(f, g, h_{(1,0,1)})$ is given by the irreducible polynomial

$$x_0^7 - 4x_0^6x_1 - 3x_0^4x_1^3 - 8x_0^3x_1^4 - x_0^2x_1^5 - 4x_0x_1^6 - 4x_1^7 - 4x_0^5x_1x_2+ \\ + 2x_0^3x_1^3x_2 - 4x_0^2x_1^4x_2 - x_0^4x_1x_2^2 + 8x_0^3x_1^2x_2^2 - 4x_0x_1^4x_2^2 + 8x_1^5x_2^2+ \\ + 4x_0^2x_1^2x_2^3 - 4x_1^3x_2^4$$

Applications

Applications

I discussed in my talk in Split in June, we use Hilbert's irreducibility to compute certain Galois groups of finite extensions of algebraic function fields (a variant of considerations of Serre)

Applications

I discussed in my talk in Split in June, we use Hilbert's irreducibility to compute certain Galois groups of finite extensions of algebraic function fields (a variant of considerations of Serre)

I am also interested in obtaining explicit results in the theory of complex algebraic curves, "representation theory of curves" instead of the representation theory of reductive Lie groups

Thank you!