HECKE ALGEBRAS, GENERATING SERIES AND APPLICATIONS

Kirill Vankov

▶ **To cite this version:**

Kirill Vankov. HECKE ALGEBRAS, GENERATING SERIES AND APPLICATIONS. Mathematics [math]. Université Joseph-Fourier - Grenoble I, 2008. English. NNT : . tel-00349767

HAL Id: tel-00349767

https://theses.hal.science/tel-00349767

Submitted on 4 Jan 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THÈSE DE DOCTORAT DE MATHÉMATIQUES
DE L'UNIVERSITÉ JOSEPH FOURIER (GRENOBLE I)

préparée à l'Institut Fourier
Laboratoire de mathématiques
UMR 5582 CNRS - UJF

Hecke algebras, generating series and applications

Kirill VANKOV

Soutenance à Grenoble le 27 novembre 2008 devant le jury :

Siegfried BÖCHERER (Professeur, Université de Mannheim)
Roland GILLARD (Professeur, Université Joseph Fourier)
Alexei PANTCHICHKINE (Professeur, Université Joseph Fourier)
Emmanuel ROYER (Professeur, Université Blaise Pascal)
Serge VLADUT (Professeur, Université de la Méditerranée)
Wadim ZUDILIN (Senior Researcher, Steklov Mathematical Institute, RAS)

Au vu des rapports de Serge VLADUT et Wadim ZUDILIN

Acknowledgements

I would like to thank my adviser, Professor Alexei Panchishkin, for all his assistance and patience during the three years of research and preparation of this thesis. It has been a privilege and a pleasure working under his expert guidance.

I thank the members of my Committee, especially Serge Vladut and Wadim Zudilin for their valuable reports on my manuscript. I thank Siegfried Böcherer for helpful discussions during the conferences and his visits to Grenoble. I thank Roland Gillard for his role in establishing my learning ground in cryptography. I thank Emmanuel Royer for inviting me to give a talk at Grenoble-Clermont meeting.

During the last year of my studies I learned a lot from Francesco Chiera. He played an important part in assisting with one chapter of this thesis. I thank colleagues from the Institute Fourier who helped me in learning French, particularly Nicolas Juillet and Luc Guyot who provided corrections and useful suggestions for the Introduction. I appreciate the valuable discussions with Roland Bacher. Many thanks to Gilles Robert for his cooperation at the earlier stage of my work.

I am greatful for the comfortable working environment and the financial support for travelling provided by the Institute Fourier.

Many thanks go to all my friends from Grenoble and from all around the world (Olga, Vlad, Lena, Misha, Dina, Jan and many others) for their friendship and many good times we shared together during the years of my study.

Finally, I would like to express my sincere gratitude to my family for their continuous encouragement and support.

Contents

Appendix

Introduction

Version française

Les objets centraux de la thèse sont les formes modulaires de Siegel et les algèbres de Hecke opérant sur eux. Les objectifs principaux sont notamment la mise au point de calculs explicites en utilisant les séries génératrices des opérateurs de Hecke et le calcul des valeurs spéciales des fonctions L (certains produits d'Euler, attachés aux formes modulaires). Ma thèse s'attache également à étudier l'application aux projets cryptologiques de certaines structures algébriques attachées aux algèbres de Hecke (comme les ensembles finis de classes à gauche et les variétés projectives sur les corps finis). Enfin, le but de la thèse consiste encore à étudier les avancées algorithmiques en matière de cryptologie (en particulier l'utilisation des modules de Drinfeld en cryptologie selon les schémas de Gillard, Leprevost, Pantchichkine et Roblot [GLPR03]).

Le résultat principal dans le travail présenté est le calcul explicite de la série génératrice des opérateurs de Hecke dans l'algèbre de Hecke locale pour les groupes symplectiques de genre 3 et 4. L'algorithme est basé sur l'isomorphisme de Satake, qui permet de réaliser toutes les opérations dans l'algèbre des polynômes à plusieurs variables. À l'origine, Shimura a conjecturé en 1963 la rationalité de la série de Hecke des groupes symplectiques. Il est à noter que dans les cas des genres 1 et 2, la forme explicite de la fraction rationnelle était déjà connue. La conjecture de Shimura a été prouvée par Andrianov pour un genre arbitraire dans sa série de travaux à la fin des années 1960. Dans la présente thèse, le *théorème sur la série génératrice pour le genre 4* fournit la forme explicite des polynômes rationnels pour la somme de la série génératrice de Hecke dans le groupe Sp_4. C'est la première fois que cette expression est calculée pour le genre 4. Le résultat est publié dans « Mathematical Notes » (vol. 81, 2007) [Van07] et « Mathematical Research Letters » (vol. 14, 2007) [PV07].

Pour obtenir le résultat principal, une méthode de calcul symbolique a été développée. Cette approche algorithmique s'applique à d'autres types de séries de Hecke. En particulier, nous formulons et prouvons un analogue du Lemme de Rankin pour le genre 2. Nous avons aussi calculé les séries

génératrices des carrés symétriques et des cubes symétriques. Ces résultats seront publiés dans « Progress in Mathematics » (vol. 269-270, 2009) [PV09].

Se basant sur nos résultats nous formulons une conjecture de modularité pour les convolutions des fonctions L-spineurs associées aux formes modulaires de Siegel. Nous considérons d'autres conjectures importantes liées aux formes modulaires de Siegel et à leurs fonctions L. En particulier, nous traitons de F_{12}, une forme parabolique de Siegel de degré 3 et de poids 12, qui a été construite par Miyawaki. Miyawaki a calculé certains facteurs d'Euler locaux des fonctions L associées et il a formulé des conjectures très intéressantes du relèvement de ces fonctions. Une partie de ces conjectures a été prouvée récemment par Ikeda et Heim. Nous utilisons ces constructions pour calculer les facteurs algébriques rationnels aux valeurs critiques de la fonction L-spineur attachée à F_{12}. A notre connaissance c'est le premier exemple d'une fonction L-spineur de forme parabolique de Siegel de degré 3, dont certaines valeurs spéciales peuvent être calculées explicitement. Le résultat est vérifié numériquement de façon indépendante en utilisant le script de PARI « ComputeL » créé par Dokchitser (inclus dans le logiciel mathématique SAGE).

Finalement, nous appliquons la théorie des algèbres de Hecke exposée au cours des deux premiers chapitres pour construire des cryptosystèmes algébriques sur ensembles finis de classes à gauches dans l'algèbre de Hecke. Nous utilisons une relation entre les classes à gauches et les points sur certains variétés algébriques projectives.

La thèse contient quatre chapitres. Dans le premier chapitre sont énoncé des généralités sur les algèbres de Hecke et les formes modulaires de Siegel. Nous définissons l'algèbre de Hecke pour le groupe symplectique GSp_n et pour le groupe général linéaire GL_n. Ensuite nous décrivons l'application sphérique de Satake, qui fournit une correspondance entre l'algèbre locale de Hecke et une certaine algèbre de polynômes. Une introduction courte sur les fonctions symétriques est incluse dans le premier chapitre. Les formes modulaires de Siegel et les formes modulaires classiques, ainsi que leurs fonctions L associées sont discutées à la fin de ce chapitre.

Dans le deuxième chapitre nous étudions la série génératrice des opérateurs de Hecke. Soit p un nombre premier. L'opérateur de Hecke $\mathbf{T}(p^\delta)$ est défini comme la somme formelle des classes doubles

$$\Gamma M \Gamma \subset \mathrm{GSp}_n^+(\mathbb{Q}) = \{ M \in M_{2n}(\mathbb{Q}) : M\, J\, {}^tM = \mu(M) J\,,\ \mu(M) > 0 \}$$

avec le facteur scalaire fixé $\mu(M) = p^\delta$. Ici J est une matrice antisymétrique de taille $2n$: $J_n = \left(\begin{smallmatrix} 0_n & I_n \\ -I_n & 0_n \end{smallmatrix} \right)$ et ${}^tM$ est la matrice transposée de M. Le groupe

Γ est le groupe modulaire de Siegel de genre n :

$$\Gamma = \mathrm{Sp}_n(\mathbb{Z}) = \{M \in \mathrm{GSp}_n(\mathbb{Q}) \cap M_{2n}(\mathbb{Z}) : \mu(M) = 1\}\,.$$

Le théorème principal de la thèse donne l'expression rationnelle polynomiale pour la somme de la série génératrice des opérateurs de Hecke du groupe Sp_4.

Théorème sur une solution explicite de la Conjecture de Shimura en genre 4 (théorème 2.1, page 53) :

$$\mathbf{D}_p^{(4)}(X) = \sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) X^\delta = \frac{\mathbf{E}_4(X)}{\mathbf{F}_4(X)}\,,$$

où $\mathbf{E}_4(X) = \sum_{k=0}^{14} \mathbf{e}_k X^k$ *est le polynôme de degré* 14 *et* $\mathbf{F}_4(X) = \sum_{k=0}^{16} \mathbf{f}_k X^k$ *est le polynôme de degré* 16 *dont les coefficients* $\mathbf{e}_k$ *et* $\mathbf{f}_k$ *sont décrits au théorème 2.1.*

La preuve du théorème 2.1 est obtenue en utilisant l'application sphérique de Satake injective

$$\Omega : \mathbb{Q}[T(p), T_1(p^2), \ldots, T_n(p^2)] \to \mathbb{Q}[x_0, x_1, \ldots, x_n]\,,$$

où $\{T(p), T_1(p^2), \ldots, T_n(p^2)\}$ est la base canonique de l'algèbre de Hecke.

Comme une conséquence facile de la preuve du théorème 2.1 nous obtenons une relation entre les coefficients polynomiaux K_k de l'image du numérateur sous l'application sphérique de Satake :

théorème sur l'équation fonctionelle des coefficients de l'image sphérique $\Omega(\mathbf{E}_4(X))$ (théorème 2.2, page 61) :

$$\begin{aligned} &K_{14-k}(p, x_0, x_1, x_2, x_3, x_4) = \\ &\quad = -p^{-6}(x_0^2 x_1 x_2 x_3 x_4)^{7-k}\, K_k\left(\frac{1}{p}, x_0x_1x_2x_3x_4, \frac{1}{x_1}, \frac{1}{x_2}, \frac{1}{x_3}, \frac{1}{x_4}\right)\,, \\ &\quad k = 0, \ldots, 14\,. \end{aligned}$$

Plus généralement, l'équation fonctionnelle vérifiée par l'image du numérateur $E(x_0, x_1, \ldots, x_n, X) = \Omega(\mathbf{E}_n(X))$ pour un genre arbitraire n est formulée dans la **Conjecture 2.3** (page 61) :

$$E(x_0, x_1, \ldots, x_n, X) = (-1)^{n-1} \frac{(x_0^2 x_1 \cdots x_n X^2)^{2^{n-1}-1}}{p^{n(n-1)/2}}\, E\left(\frac{1}{x_0}, \ldots, \frac{1}{x_n}, \frac{p}{X}\right)\,.$$

Grâce aux théorème précédent, cette égalité est donc satisfaite pour $n = 4$. De là on peut montrer que c'est aussi le cas pour $n \in \{1, 2, 3\}$.

Nous pouvons simplifier et factoriser le polynôme $\Omega(\mathbf{E}_n(X))$ en appliquant à ses coefficients l'homomorphisme « du degré » ν. L'homomorphisme ν correspond au choix des paramètres de Satake $(x_0, x_1, \ldots, x_n) = (1, p, \ldots, p^n)$ (cet homomorphisme décompte le nombre des classes à gauche dans une classe double). Pour le genre 4 nous énonçons la **Proposition 2.6 sur la factorisation du numérateur dans le cas spécial du Théorème 2.1** (page 63) :

$$\begin{aligned}\Omega|_\nu(\mathbf{E}_4(X)) &= (1-pX)\,(1-p^2X)\,(1-p^3X)^2\,(1-p^4X)\\ &\quad\times(1+p^5X)\,(1-p^5X)^2\,(1-p^6X)^2\,(1-p^7X)\,(1-p^8X)\\ &\quad\times(1+pX+p^2X+2p^3X+p^4X+p^5X+2p^6X+p^7X+p^8X+p^9X^2)\,.\end{aligned}$$

Il est plus simple d'obtenir des résultats de ce type dans le cas de genres inférieurs. En particulier, la **Proposition 2.7** (page 63) formule la proposition précédente pour le genre 3. Nous considérons l'homomorphisme ν correspondant aux paramètres de Satake $(x_0, x_1, x_2, x_3) = (1, p, p^2, p^3)$. Alors le polynôme $\Omega(\mathbf{E}_3)$ prend la forme suivante :

$$\begin{aligned}\Omega|_\nu(\mathbf{E}_3(X)) &= (1-pX)\,(1-p^2X)\,(1-p^3X)\,(1-p^4X)\\ &\quad\times(1+pX+p^2X+p^3X+p^4X+p^5X^2)\,.\end{aligned}$$

Il faut noter que cette méthode de calcul est applicable pour n'importe quel genre fixé. En utilisant cette approche nous calculons la série génératrice des opérateurs de Hecke pour le groupe Sp_3. Le **théorème sur la conjecture explicite de Shimura pour le genre 3** [PV07, théorème 2.1, page 178] présente ce résultat. Ainsi nous avons retrouvé par une méthode différente la formule de Miyawaki et de Andrianov :

$$\mathbf{D}_p^{(3)}(X) = \frac{\mathbf{E}_3(X)}{\mathbf{F}_3(X)}\,,$$

où

$$\begin{aligned}&\mathbf{E}_3(X) =\\ &\quad 1 - p^2\left(\mathbf{T}_2(p^2) + (p^2-p+1)(p^2+p+1)[\mathbf{p}]_3\right)X^2 + p^4(p+1)[\mathbf{p}]_3\mathbf{T}(p)X^3\\ &\quad - p^7[\mathbf{p}]_3\left(\mathbf{T}_2(p^2) + (p^2-p+1)(p^2+p+1)[\mathbf{p}]_3\right)X^4 + p^{15}[\mathbf{p}]_3^3X^6\,,\end{aligned}$$

$$\begin{aligned}\mathbf{F}_3(X) &= 1 - \mathbf{T}(p)X \\ &\quad + p\left(\mathbf{T}_1(p^2) + (p^2+1)\mathbf{T}_2(p^2) + (p^2+1)^2[\mathbf{p}]_3\right)X^2 \\ &\quad - p^3\left(\mathbf{T}_2(p^2) + [\mathbf{p}]_3\right)\mathbf{T}(p)X^3 \\ &\quad + p^6\big(\mathbf{T}_2(p^2) + [\mathbf{p}]_3(\mathbf{T}(p)^2 - 2p\mathbf{T}_1(p^2) - 2(p-1)\mathbf{T}_2(p^2) \\ &\qquad - (p^2+2p-1)(p^2-p+1)(p^2+p+1)[\mathbf{p}]_3)\big)X^4 \\ &\quad - p^9[\mathbf{p}]_3\left(\mathbf{T}_2(p^2) + [\mathbf{p}]_3\right)\mathbf{T}(p)X^5 \\ &\quad + p^{13}[\mathbf{p}]_3^2\left(\mathbf{T}_1(p^2) + (p^2+1)\mathbf{T}_2(p^2) + (p^2+1)^2[\mathbf{p}]_3\right)X^6 \\ &\quad - p^{18}[\mathbf{p}]^3\mathbf{T}(p)X^7 + p^{24}[\mathbf{p}]^4X^8\,.\end{aligned}$$

Ce résultat concorde avec celui obtenu pour le genre $n = 4$ après l'application de la projection $x_4 = 0$, autrement dit, après l'action de l'opérateur de Siegel de Sp_4 vers Sp_3.

La méthode développée s'applique aussi à une plus grande gamme de séries génératrices. Le **théorème sur l'analogue du Lemme de Rankin en genre 2** (théorème 2.8, page 64) fournit pour le genre 2 la résolution des séries génératrices des convolutions des opérateurs de Hecke. Le résultat prend la forme d'une fraction rationnelle de polynômes :

$$\sum_{\delta=0}^{\infty}\mathbf{T}(p^\delta)\otimes\mathbf{T}(p^\delta)\,X^\delta = \frac{(1-p^6[\mathbf{p}]\otimes[\mathbf{p}]X^2)\,\mathbf{R}(X)}{\mathbf{S}(X)}\,;$$

où $\mathbf{R}(X) = 1+\mathbf{r}_1X+\cdots+\mathbf{r}_{12}X^{12}$ et $\mathbf{S}(X) = 1+\mathbf{s}_1X+\cdots+\mathbf{s}_{16}X^{16}$ sont des polynômes de degré 12 et 16 dont les coefficients sont donnés aux théorème 2.8. Notez que $\mathbf{r}_1 = \mathbf{r}_{11} = 0$. Ce résultat répond à la question de Proffeseur S. Friedberg posée en septembre 2006 lors du colloque « Fonctions zêta » à Moscou.

Dans la preuve du théorème 2.8 une étape intermédiaire consiste à établir l'expression de $\Omega_x^{(2)}(\mathbf{T}(p^\delta))$, l'image sphérique de l'opérateur de Hecke $\mathbf{T}(p^\delta)$. **Proposition sur l'image de l'opérateur de Hecke $\mathbf{T}(p^\delta)$** (proposition 2.9, page 69) :

$$\begin{aligned}\Omega_x^{(2)}(\mathbf{T}(p^\delta)) &= -\Big((1-x_1\,x_2)\,(p\,x_1-x_2)\,x_1^{(\delta+1)} + (1-x_1\,x_2)\,(x_1-p\,x_2)\,x_2^{(\delta+1)} \\ &\quad - (x_1-x_2)\,(1-p\,x_1\,x_2)\,(x_1\,x_2)^{(\delta+1)} - (x_1-x_2)\,(p-x_1\,x_2)\Big)\,p^{-1}\,x_0^\delta \\ &\quad \times\Big((1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(x_1-x_2)\Big)^{-1}.\end{aligned}$$

A l'aide de la proposition ci-dessus nous déduisons le **Théorème sur l'image sphérique du produit des séries génératrices** (théorème 2.10,

page 72), qui donne le résultat correspondant de la convolution suivante :

$$\sum_{\delta=0}^{\infty} \Omega_x^{(2)}(\mathbf{T}(p^\delta)) \cdot \Omega_y^{(2)}(\mathbf{T}(p^\delta))\, X^\delta\,.$$

S'ensuivent quelques remarques concernant la forme explicite de la convolution des séries génératrices. Tout d'abord vient la **remarque sur le dénominateur** (remarque 2.11, page 73) : le dénominateur commun du théorème 2.10 est un polynôme de degré 16 dont la forme factorisée particulièrement élégante :

$$\begin{aligned}
&(1 - x_0\, y_0 X)\,(1 - x_0\, y_0\, x_1\, X)\,(1 - x_0\, y_0\, y_1\, X)\,(1 - x_0\, y_0\, x_2\, X)\\
&\times (1 - x_0\, y_0\, y_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, X)\,(1 - x_0\, y_0\, x_1\, x_2\, X)\\
&\times (1 - x_0\, y_0\, x_1\, y_2\, X)\,(1 - x_0\, y_0\, y_1\, x_2\, X)\,(1 - x_0\, y_0\, y_1\, y_2\, X)\\
&\times (1 - x_0\, y_0\, x_2\, y_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, x_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, y_2\, X)\\
&\times (1 - x_0\, y_0\, x_1\, x_2\, y_2\, X)\,(1 - x_0\, y_0\, y_1\, x_2\, y_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, x_2\, y_2\, X).
\end{aligned}$$

Vient ensuite la **remarque sur la comparaison avec le genre 1** (remarque 2.12, page 73). Pour le genre 1, l'expression rationnelle est similaire à celle du genre 2. Le numérateur de genre 2 contient le facteur $1 - x_0^2 y_0^2\, x_1 y_1 x_2 y_2 X^2$ de degré deux et il est similaire structurellement au numérateur de genre 1. Les deux dénominateurs son similaires structurellement :

$$\begin{aligned}
&\sum_{\delta=0}^{\infty} \Omega_x^{(1)}(\mathbf{T}(p^\delta)) \cdot \Omega_y^{(1)}(\mathbf{T}(p^\delta))\, X^\delta\\
&\qquad = \frac{1 - x_0^2\, y_0^2\, x_1\, y_1\, X^2}{(1 - x_0 y_0 X)\,(1 - x_0 y_0 x_1 X)\,(1 - x_0 y_0 y_1 X)\,(1 - x_0 y_0 x_1 y_1 X)}\,.
\end{aligned}$$

La troisième remarque concerne **l'équation fonctionelle du dénominateur au théorème 2.8** (remarque 2.13, page 74) qui établit un lien entre les coefficients $\mathbf{s}_i$ du dénominateur $\mathbf{S}(X)$:

$$\mathbf{s}_{16-i} = (p^6\,[\mathbf{p}] \otimes [\mathbf{p}])^{8-i}\,\mathbf{s}_i\,.$$

Finalement, vient la **remarque sur la comparaison avec le genre 1 où nous utilisons directement des opérateurs de Hecke** (remarque 2.14, page 74). Dans le cas du genre 1, la convolution des séries génératrices peut s'écrire de la façon suivante en utilisant directement des opérateurs de

Hecke :

$$\begin{aligned}
&\sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) \otimes \mathbf{T}(p^\delta)\, X^\delta \\
&\quad = \Big(1 - p^2\, \mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\, X^2\Big) \Big(1 - \mathbf{T}(p) \otimes \mathbf{T}(p)\, X + \\
&\quad \big(p\, \mathbf{T}(p)^2 \otimes \mathbf{T}_1(p^2) + p\, \mathbf{T}_1(p^2) \otimes \mathbf{T}(p)^2 - 2p^2\, \mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\big) X^2 \\
&\quad - p^2\, \mathbf{T}(p)\mathbf{T}_1(p^2) \otimes \mathbf{T}(p)\mathbf{T}_1(p^2) X^3 + p^4\, \mathbf{T}_1(p^2)^2 \otimes \mathbf{T}_1(p^2)^2 X^4\Big)^{-1}.
\end{aligned}$$

A la fin du chapitre 2 nous présentons les résultats sur le calcul des images sphériques des séries carrés et cubiques des opérateurs de Hecke de genre 2.

Le troisième chapitre présente des exemples explicites de formes modulaires de Siegel et de fonctions L qui leur sont associées. Le demi-espace de Siegel de genre n est l'ensemble des matrices complexes symétriques de tailles $n \times n$ dont la partie imaginaire est définie positive :

$$\mathfrak{H}^n = \big\{ Z = {}^tZ = X + iY : X, Y \in M_n(\mathbb{R}),\, Y > 0 \big\}\ .$$

Le groupe symplectique $\mathrm{Sp}_n(\mathbb{Z})$ agit sur l'espace $\mathfrak{H}^n$ de la façon suivante :

$$\gamma(Z) = (AZ + B)\,(CZ + D)^{-1}\,,$$

où $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_n(\mathbb{Z})$ et $Z \in \mathfrak{H}^n$. Une fonction holomorphe $F : \mathfrak{H}^n \to \mathbb{C}$ s'appelle une *forme modulaire de Siegel de genre n et de poids k* sur $\mathrm{Sp}_n(\mathbb{Z})$ si F satisfait

$$\det(CZ + D)^{-k} F(\gamma(Z)) = F(Z)\,, \quad \forall \gamma \in \mathrm{Sp}_n(\mathbb{Z})\,.$$

Dans le cas où $n = 1$, on exige de plus que la fonction F soit holomorphe en ∞. On peut considérer les formes modulaires de Siegel comme des formes à plusieurs variables, c'est-à-dire comme des fonctions spéciales de plusieurs variables complexes. Remarquons que les formes modulaires de Siegel de genre 1 sont les formes modulaires classiques du demi-plan de Poincaré pour le groupe $\mathrm{SL}_2(\mathbb{Z}) = \mathrm{Sp}_1(\mathbb{Z})$ et ses sous-groupes de congruence.

Un exemple de sources de formes modulaires de genre $n > 1$ est le relèvement des formes modulaires classiques. Nous discutons de quelques constructions des relèvements modulaires et de certaines conjectures. En particulier, le *relèvement de Saito-Kurokawa* associe aux formes modulaires de genre 1 et de poids $2k - 2$, des formes modulaires de genre 2 et de poids k.

Le *relèvement d'Ikeda* donne une méthode de construction des formes modulaires de genre $2n$ et de poids $k + n$ à partir des forme modulaires

de poids $2k$, de niveau 1 et de genre 1 (à condition que k et n soient de même parité). La méthode d'Ikeda fournit une formule pour les coefficients de Fourier de ces formes. Les formes relevées peuvent alors être étudiées explicitement.

Les résultats des Sections 2.2 et 2.3 nous permettent de comparer la série génératrice de Hecke de genre 4 (dans les cordonnés sphériques u_0, u_1, u_2, u_3, u_4) avec le produit de Rankin de deux séries de Hecke de genre 2 (dans les coordonnées sphériques x_0, x_1, x_2, y_0, y_1, y_2). Il découle de nos calculs que les dénominateurs de deux séries coïncident. Se basant sur cette égalité, nous formulons la conjecture suivante :

Conjecture sur un relèvement de $\mathrm{GSp}_2 \times \mathrm{GSp}_2$ **vers** GSp_4 (Conjecture 3.6, page 82) : soient f et g deux formes modulaires de Siegel de genre 2 et de poids $k > 4$ et $l = k - 2$. Alors il existe une forme modulaire F de Siegel de genre 4 et de poids k avec les paramètres de Satake

$$\gamma_0 = \alpha_0\beta_0,\ \gamma_1 = \alpha_1,\ \gamma_2 = \alpha_2,\ \gamma_3 = \beta_1,\ \gamma_4 = \beta_2,$$

pour un choix approprié des paramètres de Satake $\{\alpha_0, \alpha_1, \alpha_2\}$ et $\{\beta_0, \beta_1, \beta_2\}$ de f et de g respectivement.

De plus, cette conjecture peut être généralisée de la manière suivante :

Conjecture sur un relèvement de $\mathrm{GSp}_{2m} \times \mathrm{GSp}_{2m}$ **vers** GSp_{4m} (Conjecture 3.7, page 83) : soient f et g deux formes modulaires de Siegel de genre $2m$ et de poids $k > 2m$ et $l = k - 2m$. Alors il existe une forme modulaire F de Siegel de genre $4m$ et de poids k avec les paramètres de Satake

$$\gamma_0 = \alpha_0\beta_0,\ \gamma_1 = \alpha_1, \ldots, \gamma_{2m} = \alpha_{2m},\ \gamma_{2m+1} = \beta_1, \ldots, \gamma_{4m} = \beta_{2m},$$

pour un choix approprié des paramètres de Satake $\{\alpha_0, \alpha_1, \ldots, \alpha_{2m}\}$ de f et $\{\beta_0, \beta_1, \ldots, \beta_{2m}\}$ de g.

Une conjecture importante a été formulé par Miyawaki en 1992. Il a considéré certaines formes modulaires de Siegel de degré 3. Sur la base de calculs numériques il a conjecturé l'existence du relèvement de certaines formes modulaires de Siegel de degré r pour obtenir des formes modulaires de Siegel de degré $r + 2n$ et il a donné une formule pour les fonctions L attachées à ses formes.

Le résultat principal du troisième chapitre est le calcul de valeurs spéciales pour l'exemple de Miyawaki :

Théorème sur l'algébricité des valeurs spéciales de fonction $L(s, F_{12}, spin)$ (théorème 3.9, page, 100). Pour chaque point critique $s \in \{12, \ldots, 19\}$ la fonction L-spineur associée à forme modulaire F_{12} de Miyawaki a l'expression algébrique suivante :

$$L(s, F_{12}, spin) = R(s)\,\pi^{\alpha}\ \langle \Delta, \Delta \rangle\ \langle g_{20}, g_{20} \rangle\ ,$$

où le facteur rationnel R et l'exposant α de π sont présentés dans le tableau 3.4.

Les valeurs critiques de la fonction L-spineur $L(s, F_{12}, spin)$ associée à F_{12} sont aussi calculées numériquement de façon indépendante en utilisant le script de PARI « Computel » créé par T. Dokchitser. Les valeurs numériques obtenues par les deux méthodes coïncident dans les limites de la précision du calcul.

Dans la partie finale de la thèse nous donnons des applications de la théorie exposée au cours des deux premiers chapitres où nous avons construit des cryptosystèmes algébriques sur les ensembles finis de classes à gauches dans l'algèbre de Hecke. Pour la construction de ces cryptosystèmes nous utilisons la relation entre les classes à gauches de certaines classes doubles avec les points de certaines variétés algébriques. Un exemple d'une telle variété est une variété de drapeau sur un corps fini. Dans la construction pratique de cette correspondance on utilise la forme normale de Smith et la forme normale d'Hermite des représentantes de classes.

Nous présentons la version projective du cryptosystème basé sur les modules de Drinfeld, proposé par Gillard, Leprevost, Panchishkin et Roblot. Les propriétés projectives assurent une plus grande sécurité pour ce cryptosystème.

La base théorique essentielle de ce travail est présentée dans des ouvrages fondamentaux tels quels

- Andrianov et Zhuravlev « Modular forms and Hecke operators » [AZ95],
- Martin et Royer « Formes modulaires et périodes » [MR05],
- Miyake « Modular forms » [Miy06],
- Serre « Cours d'arithmétique » [Ser77],
- Shimura « Introduction to the arithmetic theory of automorphic functions » [Shi71],
- van der Geer « Siegel modular forms and their applications » [vdG08],

ainsi que dans quelques articles de Andrianov, Heim, Ikeda, Miyawaki, Panchishkin, Rankin, Shimura, Zagier.

Les résultats principaux de cette thèse sont publiés dans

- Math. Res. Lett., 14(2), 2007 (cf. [PV07]),
- Math. Notes 81 (2007), no. 5–6 (cf. [Van07]),
- arXiv :0805.2114v1 [math.NT] (cf. [CV08]),
- Progress in Mathematics, vol. 269/270 (cf. [PV09]).

Ces résultats ont été présentés au cour de séminaires, dont :

– à l'Institut Fourier (Grenoble), mai 2006, et
– à l'Institut de Mathématiques de Bordeaux, mars 2007 ;

et au cour de conférences, dont :

– au Colloque International « Diophantine and Analytic Problems in Number Theory » en l'honneur du centième anniversaire de Gelfond a l'Université Lomonossov de Moscou, février 2007,
– au Colloque International « Formes de Jacobi et Applications » (CIRM, Luminy), mai 2007,
– à la conférence « Grenoble – Clermont 2008 » à l'Université Blaise Pascal (Clermont-Ferrand), juin 2008 et
– au Colloque « Weekend de rentrée de l'Institut Fourier 2008 » (Autrans), septembre 2008.

English version

The central objects of the thesis are Siegel modular forms and Hecke algebras acting on them. Our main objectives are an explicit computation with generating series of Hecke operators, L-functions (certain Euler products attached to modular forms) and application to cryptology schemes using certain algebraic structures related to Hecke algebras: finite sets of double cosets and related projective varieties over finite fields.

The main result in presented work consists of explicit computation of the generating power series of Hecke operators in local Hecke algebra for the symplectic groups of genus 3 and 4. The computation algorithm is based on the Satake isomorphism allowing to carry out all operations in the algebra of polynomials in multiple variables. Originally, Shimura conjectured in 1963 the rationality of Hecke series of symplectic groups. The explicit form of polynomials in numerator and denominator was known for two cases of smallest genus 1 and 2. Shimura's conjecture was proved by Andrianov in the series of works at the end of 1960s for an arbitrary genus. In the present thesis, *Theorem on generating series in genus 4* provides the explicit form of the rational polynomial expression for the summation of Hecke power series in group Sp_4. This is the first time when this expression was computed in genus 4. The result is published in "Mathematical Notes" (vol. 81, 2007) [Van07] and "Mathematical Research Letters" (vol. 14, 2007) [PV07].

In order to obtain the main result, the method of symbolic computation was developed. This algorithmic approach is also applied to other types of Hecke series. In particular, we formulate and prove the analog of Rankin's Lemma in higher genus. We also computed the symmetric squares and symmetric cubes generating series. These results are published in "Progress in Mathematics" (vol. 269-270, 2009) [PV09].

Based on our computational results we formulate a modularity lifting conjecture for convolutions of L-functions attached to Siegel modular forms. We review other important conjectures related to Siegel modular forms and their L-functions. Namely, a Siegel cusp form F_{12} of degree 3 and weight 12, which was constructed by Miyawaki, is considered. Miyawaki computed some local Euler factors of associated L-functions and he formulated some remarkable lifting conjectures. Parts of conjectures were proved recently by Ikeda and Heim. We use these constructions to compute the rational algebraic factors in critical values of the spinor L-function attached to F_{12}. To our knowledge this is the first example of a spinor L-function of Siegel cusp forms of degree 3, when the special values can be computed explicitly. The result is verified numerically and independently by using Dokchitser's ComputeL PARI script within the mathematics software package SAGE.

Finally, we apply the theory of Hecke algebras to constructions of algebraic cryptosystems on some finite sets of left cosets in Hecke algebra. We use a relation between left cosets and points on certain projective algebraic varieties.

The thesis contains four chapters. In the first chapter we give the general information on Hecke algebras and Siegel modular forms. We define the Hecke algebra for the symplectic group GSp_n and the general linear group GL_n. Then we describe the Satake spherical map, which provides a correspondence of local Hecke algebra to certain polynomial algebra. A short introduction on symmetric functions is included into the first chapter. Siegel modular forms and classical modular forms together with associated L-functions are discussed at the end of this chapter.

We study the generating power series of Hecke operators in the second chapter. Let p be a prime. The Hecke operator $\mathbf{T}(p^\delta)$ is defined as the formal sum of all double cosets

$$\Gamma M \Gamma \subset \mathrm{GSp}_n^+(\mathbb{Q}) = \{ M \in M_{2n}(\mathbb{Q}) : M\, J\, {}^tM = \mu(M) J\,,\ \mu(M) > 0 \}$$

with fixed scalar factor $\mu(M) = p^\delta$. Here J is the antisymmetric matrix of order $2n$: $J_n = \left(\begin{smallmatrix} 0_n & I_n \\ -I_n & 0_n \end{smallmatrix} \right)$ and ${}^tM$ is the transpose of the matrix M. The group Γ is the Siegel modular group

$$\Gamma = \mathrm{Sp}_n(\mathbb{Z}) = \{ M \in \mathrm{GSp}_n(\mathbb{Q}) \cap M_{2n}(\mathbb{Z}) : \mu(M) = 1 \}\,.$$

The main theorem of the dissertation provides the rational polynomial expression for the summation of Hecke power series in group Sp_4.

Theorem on explicit Shimura's conjecture for genus 4 (Theorem 2.1, page 53):

$$\mathbf{D}_p^{(4)}(X) = \sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) X^\delta = \frac{\mathbf{E}_4(X)}{\mathbf{F}_4(X)}\,,$$

where $\mathbf{E}_4(X) = \sum_{k=0}^{14} \mathbf{e}_k X^k$ *is the polynomial of degree* 14 *and* $\mathbf{F}_4(X) = \sum_{k=0}^{16} \mathbf{f}_k X^k$ *is the polynomial of degree* 16 *with the coefficients* $\mathbf{e}_k$ *and* $\mathbf{f}_k$ *listed in the theorem.*

The proof of the theorem 2.1 is obtained with the use of injective spherical mapping

$$\Omega : \mathbb{Q}[T(p), T_1(p^2), \ldots, T_n(p^2)] \to \mathbb{Q}[x_0, x_1, \ldots, x_n]\,,$$

where $\{T(p), T_1(p^2), \ldots, T_n(p^2)\}$ is the basis of the Hecke algebra.

From the theorem 2.1, the relation follows establishing connection between polynomial coefficients K_k of the numerator under the spherical map: **Theorem on a functional equation for coefficients of the Satake map image** $\Omega(\mathbf{E}_4(X))$ (Theorem 2.2, page 61):

$$K_{14-k}(p, x_0, x_1, x_2, x_3, x_4) = \\ = -p^{-6}(x_0^2 x_1 x_2 x_3 x_4)^{7-k}\, K_k\left(\frac{1}{p}, x_0x_1x_2x_3x_4, \frac{1}{x_1}, \frac{1}{x_2}, \frac{1}{x_3}, \frac{1}{x_4}\right), \\ k = 0, \ldots, 14\,.$$

More generally, the functional equation for the image of the numerator $\Omega(\mathbf{E}_n(X)) = E(x_0, x_1, \ldots, x_n, X)$ corresponding to an arbitrary genus n is formulated in the **Conjecture 2.3** (page 61):

$$E(x_0, x_1, \ldots, x_n, X) = (-1)^{n-1} \frac{(x_0^2 x_1 \cdots x_n X^2)^{2^{n-1}-1}}{p^{n(n-1)/2}}\, E\left(\frac{1}{x_0}, \ldots, \frac{1}{x_n}, \frac{p}{X}\right).$$

According to the previous theorem, this conjecture is valid in the case when genus $n = 4$, and also for $n = 1, 2, 3$.

The polynomial $\Omega(\mathbf{E}_n(X))$ is considerably simplified after applying "the degree" homomorphism ν to its coefficients. The homomorphism ν corresponds to the choice of the Satake parameters $(x_0, x_1, \ldots, x_n) = (1, p, \ldots, p^n)$, and it counts the number of left cosets in a given double coset. In the case of the genus 4 we state the following **Proposition 2.6 on special case of Theorem 2.1** (page 63):

$$\Omega|_\nu(\mathbf{E}_4(X)) = (1 - pX)\,(1 - p^2X)\,(1 - p^3X)^2\,(1 - p^4X) \\ \times (1 + p^5X)\,(1 - p^5X)^2\,(1 - p^6X)^2\,(1 - p^7X)\,(1 - p^8X) \\ \times (1 + pX + p^2X + 2p^3X + p^4X + p^5X + 2p^6X + p^7X + p^8X + p^9X^2)\,.$$

It is more simple to obtain the related results for the lower genus. In particular, the **Proposition 2.7** (page 63) formulates the previous proposition for the genus 3. Consider the degree homomorphism ν corresponding the Satake parameters $(x_0, x_1, x_2, x_3) = (1, p, p^2, p^3)$. Then the polynomial $\Omega(\mathbf{E}_3)$ takes the form

$$\Omega|_\nu(\mathbf{E}_3(X)) = (1 - pX)\,(1 - p^2X)\,(1 - p^3X)\,(1 - p^4X) \\ \times (1 + pX + p^2X + p^3X + p^4X + p^5X^2)\,.$$

It is worth noting that the developed computation method is applicable to any fixed genus. Using this method we computed the Hecke power series for the group Sp_3. The **Theorem on explicit Shimura's conjecture for genus 3** [PV07, theorem 2.1, page 178] formulates the result. Therefore, we computed alternatively the result of Miyawaki and Andrianov:

$$\mathbf{D}_p^{(3)}(X) = \frac{\mathbf{E}_3(X)}{\mathbf{F}_3(X)}\,,$$

where

$$\begin{aligned}
&\mathbf{E}_3(X) = \\
&\quad 1 - p^2\left(\mathbf{T}_2(p^2) + (p^2-p+1)(p^2+p+1)[\mathbf{p}]_3\right)X^2 + p^4(p+1)[\mathbf{p}]_3\mathbf{T}(p)X^3 \\
&\quad - p^7[\mathbf{p}]_3\left(\mathbf{T}_2(p^2) + (p^2-p+1)(p^2+p+1)[\mathbf{p}]_3\right)X^4 + p^{15}[\mathbf{p}]_3^3\,X^6\,,
\end{aligned}$$

$$\begin{aligned}
&\mathbf{F}_3(X) = 1 - \mathbf{T}(p)X \\
&\quad + p\left(\mathbf{T}_1(p^2) + (p^2+1)\mathbf{T}_2(p^2) + (p^2+1)^2[\mathbf{p}]_3\right)X^2 \\
&\quad - p^3\left(\mathbf{T}_2(p^2) + [\mathbf{p}]_3\right)\mathbf{T}(p)X^3 \\
&\quad + p^6\big(\mathbf{T}_2(p^2) + [\mathbf{p}]_3(\mathbf{T}(p)^2 - 2p\mathbf{T}_1(p^2) - 2(p-1)\mathbf{T}_2(p^2) \\
&\qquad - (p^2+2p-1)(p^2-p+1)(p^2+p+1)[\mathbf{p}]_3)\big)X^4 \\
&\quad - p^9[\mathbf{p}]_3\left(\mathbf{T}_2(p^2) + [\mathbf{p}]_3\right)\mathbf{T}(p)X^5 \\
&\quad + p^{13}[\mathbf{p}]_3^2\left(\mathbf{T}_1(p^2) + (p^2+1)\mathbf{T}_2(p^2) + (p^2+1)^2[\mathbf{p}]_3\right)X^6 \\
&\quad - p^{18}[\mathbf{p}]^3\mathbf{T}(p)X^7 + p^{24}[\mathbf{p}]^4X^8\,.
\end{aligned}$$

This result agrees with the result for genus $n = 4$ after applying the projection $x_4 = 0$ (corresponding to the action of the Siegel operator from Sp_4 to Sp_3).

The developed method is also applicable to a wider range of generating series. The **Theorem on analog of Rankin's Lemma for genus 2** (Theorem 2.8, page 64) provides the resolution of generating series of convolutions of Hecke operators in genus 2. The result is formulated in terms of the rational polynomial fraction:

$$\sum_{\delta=0}^{\infty}\mathbf{T}(p^\delta)\otimes\mathbf{T}(p^\delta)\,X^\delta = \frac{(1-p^6[\mathbf{p}]\otimes[\mathbf{p}]X^2)\,\mathbf{R}(X)}{\mathbf{S}(X)}\,,$$

where $\mathbf{R}(X) = 1 + \mathbf{r}_1X + \cdots + \mathbf{r}_{12}X^{12}$ is the polynomial of degree 12 and $\mathbf{S}(X) = 1 + \mathbf{s}_1X + \cdots + \mathbf{s}_{16}X^{16}$ is the polynomial of degree 16 with the coefficients $\mathbf{r}_k$ and $\mathbf{s}_k$ given in the Theorem. Note, that $\mathbf{r}_1 = \mathbf{r}_{11} = 0$. This result

responds to the question raised by Prof. S. Friedberg during the conference "Zeta Functions" in September 2006 in Moscow.

As an intermediate step to prove the Theorem 2.8, the expression for the spherical image of Hecke operator $\mathbf{T}(p^\delta)$ is derived.
Proposition on the image of the Hecke operator $\mathbf{T}(p^\delta)$ (2.9, page 69):

$$\begin{aligned}\Omega_x^{(2)}(\mathbf{T}(p^\delta)) = -\Big((1-x_1\,x_2)\,(p\,x_1-x_2)\,x_1^{(\delta+1)} + (1-x_1\,x_2)\,(x_1-p\,x_2)\,x_2^{(\delta+1)} \\ -(x_1-x_2)\,(1-p\,x_1\,x_2)\,(x_1\,x_2)^{(\delta+1)} - (x_1-x_2)\,(p-x_1\,x_2)\Big)\,p^{-1}\,x_0^\delta \\ \times\Big((1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(x_1-x_2)\Big)^{-1}.\end{aligned}$$

With the help of the above proposition we derive the **Theorem on spherical image of generating series product** (Theorem 2.10, page 72), which gives the related result for the following convolution:

$$\sum_{\delta=0}^{\infty} \Omega_x^{(2)}(\mathbf{T}(p^\delta))\cdot\Omega_y^{(2)}(\mathbf{T}(p^\delta))\,X^\delta\,.$$

There are few remarks related to the explicit form of the power series convolution. First, **Remark on the denominator** (Remark 2.11, page 73): the common denominator in the theorem 2.10 has a clear and simple factored form of the following polynomial of degree 16:

$$\begin{aligned}&(1-x_0\,y_0X)\,(1-x_0\,y_0\,x_1\,X)\,(1-x_0\,y_0\,y_1\,X)\,(1-x_0\,y_0\,x_2\,X)\\ &\times(1-x_0\,y_0\,y_2\,X)\,(1-x_0\,y_0\,x_1\,y_1\,X)\,(1-x_0\,y_0\,x_1\,x_2\,X)\\ &\times(1-x_0\,y_0\,x_1\,y_2\,X)\,(1-x_0\,y_0\,y_1\,x_2\,X)\,(1-x_0\,y_0\,y_1\,y_2\,X)\\ &\times(1-x_0\,y_0\,x_2\,y_2\,X)\,(1-x_0\,y_0\,x_1\,y_1\,x_2\,X)\,(1-x_0\,y_0\,x_1\,y_1\,y_2\,X)\\ &\times(1-x_0\,y_0\,x_1\,x_2\,y_2\,X)\,(1-x_0\,y_0\,y_1\,x_2\,y_2\,X)\,(1-x_0\,y_0\,x_1\,y_1\,x_2\,y_2\,X).\end{aligned}$$

Second, **Remark on comparison with genus 1** (Remark 2.12, page 73). In the case of genus 1, the rational expression is similar to the genus 2. The numerator of genus 2 contains the factor of degree two $(1-x_0^2y_0^2\,x_1y_1x_2y_2X^2)$, which is structurally similar to the numerator of the genus 1. Both denominators are structurally similar:

$$\begin{aligned}&\sum_{\delta=0}^{\infty}\Omega_x^{(1)}(\mathbf{T}(p^\delta))\cdot\Omega_y^{(1)}(\mathbf{T}(p^\delta))\,X^\delta\\ &\quad=\frac{1-x_0^2\,y_0^2\,x_1\,y_1\,X^2}{(1-x_0y_0X)\,(1-x_0y_0x_1X)\,(1-x_0y_0y_1X)\,(1-x_0y_0x_1y_1X)}\,.\end{aligned}$$

Third, **Remark on the functional equation for denominator of Th.2.8** (Remark 2.13, page 74). There is an obvious functional equation for the coefficients $\mathbf{s}_i$ of the denominator $\mathbf{S}(X)$:

$$\mathbf{s}_{16-i} = \left(p^6\,[\mathbf{p}] \otimes [\mathbf{p}]\right)^{8-i} \mathbf{s}_i\,.$$

Finally, **Remark on comparison with genus 1 in terms of Hecke operators** (Remark 2.14, page 74). In the case of genus 1, the Hecke power series convolution is written in terms of Hecke operators as following:

$$\begin{aligned}
&\sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) \otimes \mathbf{T}(p^\delta)\, X^\delta \\
&\quad = \Big(1 - p^2\,\mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\, X^2\Big) \Big(1 - \mathbf{T}(p) \otimes \mathbf{T}(p)\, X + \\
&\quad \big(p\,\mathbf{T}(p)^2 \otimes \mathbf{T}_1(p^2) + p\,\mathbf{T}_1(p^2) \otimes \mathbf{T}(p)^2 - 2p^2\,\mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\big) X^2 \\
&\quad - p^2\,\mathbf{T}(p)\mathbf{T}_1(p^2) \otimes \mathbf{T}(p)\mathbf{T}_1(p^2) X^3 + p^4\,\mathbf{T}_1(p^2)^2 \otimes \mathbf{T}_1(p^2)^2 X^4\Big)^{-1}\,.
\end{aligned}$$

At the end of the chapter 2 we present the results of computing the spherical images of symmetric squares and cubes of the Hecke operators in genus 2.

The third chapter presents the explicit examples of Siegel modular forms and L-functions attached to them. The Siegel upper half space in genus n is the set of all $n \times n$ complex symmetric matrices with positive-definite imaginary part:

$$\mathfrak{H}^n = \left\{Z = {}^tZ = X + iY : X, Y \in M_n(\mathbb{R}),\, Y > 0\right\}\,.$$

The symplectic group $\mathrm{Sp}_n(\mathbb{Z})$ acts on the space $\mathfrak{H}^n$ as

$$\gamma(Z) = (AZ + B)\,(CZ + D)^{-1}\,,$$

where $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_n(\mathbb{Z})$ and $Z \in \mathfrak{H}^n$. A holomorphic function $F : \mathfrak{H}^n \to \mathbb{C}$ is called a *genus n Siegel modular form of weight k* on $\mathrm{Sp}_n(\mathbb{Z})$ if F satisfies

$$\det(CZ + D)^{-k} F(\gamma(Z)) = F(Z)\,, \quad \forall \gamma \in \mathrm{Sp}_n(\mathbb{Z})\,.$$

In the case of $n = 1$, it is also required that F is holomorphic at ∞. Siegel modular forms can be thought of as multivariate modular forms, i.e. as special functions of several complex variables. On the other hand, Siegel modular forms of genus 1 are classical modular forms on the upper half plane for the group $\mathrm{SL}_2(\mathbb{Z}) = \mathrm{Sp}_1(\mathbb{Z})$ and its congruence subgroups.

One source of modular forms of higher genus is lifting from classical modular forms (of genus 1). We discuss several modular lifting constructions and conjectures. In particular, the *Saito-Kurokawa lifting* provides the source of modular form of degree 2 and weight k, which are lifted from genus 1 modular forms of weight $2k-2$.

The *Ikeda lifting* provides the constructive source of degree $2n$ modular forms of weight $k+n$, where $2k$ is the weight of some classical modular form (with condition of the same parity k and n). Ikeda's method gives a formula for the Fourier coefficients, therefore the lifted form can be studied explicitly.

Our results from Sections 2.2 and 2.3 make it possible to compare the Hecke series of genus 4 (in spherical coordinates u_0, u_1, u_2, u_3, u_4) with the Rankin product of two Hecke series of genus 2 (in spherical coordinates x_0, x_1, x_2, y_0, y_1, y_2). It follows from our computation that the denominator of one series coincides with the denominator of the other one. On the basis of this equality we formulate the following conjecture:
Conjecture on a lifting from $\mathrm{GSp}_2 \times \mathrm{GSp}_2$ **to** GSp_4 (Conjecture 3.6, page 82): Let f and g be two Siegel modular forms of genus 2 and of weights $k > 4$ and $l = k-2$. Then there exists a Siegel modular form F of genus 4 and of weight k with the Satake parameters

$$\gamma_0 = \alpha_0\beta_0,\ \gamma_1 = \alpha_1,\ \gamma_2 = \alpha_2,\ \gamma_3 = \beta_1,\ \gamma_4 = \beta_2,$$

for a suitable choice of Satake parameters $\{\alpha_0, \alpha_1, \alpha_2\}$ and $\{\beta_0, \beta_1, \beta_2\}$ of f and g correspondingly.

Moreover, this conjecture can be generalized as follows:
Conjecture on a lifting from $\mathrm{GSp}_{2m} \times \mathrm{GSp}_{2m}$ **to** GSp_{4m} (Conjecture 3.7, page 83): Let f and g be two Siegel modular forms of genus $2m$ and of weights $k > 2m$ and $l = k-2m$. Then there exists a Siegel modular form F of genus $4m$ and of weight k with the Satake parameters

$$\gamma_0 = \alpha_0\beta_0,\ \gamma_1 = \alpha_1, \ldots, \gamma_{2m} = \alpha_{2m},\ \gamma_{2m+1} = \beta_1, \ldots, \gamma_{4m} = \beta_{2m},$$

for a suitable choice of Satake parameters $\{\alpha_0, \alpha_1, \ldots, \alpha_{2m}\}$ of the modular form f and $\{\beta_0, \beta_1, \ldots, \beta_{2m}\}$ of the form g.

The important conjecture was made by Miyawaki in 1992. He considered certain Siegel modular forms of degree 3, and on the basis of some numerical calculations, he suggested the lifting from Siegel modular forms of degree r to Siegel modular forms of degree $r+2n$ and provided formulae for L-functions attached to such forms.

The main result of this chapter is related to the computation of special values for Miyawaki's example.

Theorem on algebraic expression for $L(s, F_{12}, spin)$ (Theorem 3.9, page 100). For each critical point $s \in \{12, \ldots, 19\}$ the value of the spinor L-function associated to Miyawaki's modular form F_{12} is given by the following algebraic expression

$$L(s, F_{12}, spin) = R(s)\, \pi^{\alpha}\ \langle \Delta, \Delta \rangle\ \langle g_{20}, g_{20} \rangle\ ,$$

where the rational factor R and the corresponding power α of π are listed in the Table 3.4, page 101.

The critical values of $L(s, F_{12}, spin)$ are also computed numerically and independently using Dokchitser's PARI scrip ComputeL within the mathematics software package SAGE. The numerical values in both methods coincide within the computing precision.

The final part of the dissertation is devoted to applications of the first two chapters to the construction of algebraic cryptosystems based on the finite sets of left cosets in Hecke algebra. In order to construct this cryptosystems we use the relation between the left cosets of certain double cosets with the points on some algebraic varieties, such as a flag varieties over final fields. For the practical construction of this correspondence, one has to use the Smith normal form and the Hermite normal form of the matices representing the cosets.

We provide a projective version of the cryptosystem based on Drinfeld modules, which was proposed by Gillard, Leprevost, Panchishkin and Roblot [GLPR03]. The projective properties provide an additional security to the cryptosystem.

The essential theoretical background for the presented work is given by the fundamental books

- Andrianov and Zhuravlev "Modular forms and Hecke operators" [AZ95],
- Martin and Royer "Formes modulaires et périodes" [MR05],
- Miyake "Modular forms" [Miy06],
- Serre "Cours d'arithmétique" [Ser77],
- Shimura "Introduction to the arithmetic theory of automorphic functions" [Shi71],
- van der Geer "Siegel modular forms and their applications" [vdG08],

as well as by the several articles by Andrianov, Heim, Ikeda, Miyawaki, Panchishkin, Rankin, Shimura, Zagier.

Main results of the Thesis are published in

- Math. Res. Lett., 14(2), 2007 (cf. [PV07]),
- Math. Notes 81 (2007), no. 5–6 (cf. [Van07]) and in
- arXiv:0805.2114v1 [math.NT] (cf. [CV08]),
- Progress in Mathematics, vol. 269/270 (cf. [PV09]).

These results were presented at several seminars and conferences:

- seminar of the Fourier Institute in Grenoble in May 2006,
- seminar of the Institute of Mathematics in Bordeaux in March 2007,
- International Conference "Diophantine and Analytic Problems in Number Theory" for the 100th anniversary of Gelfond at Moscow State University in February 2007,
- International conference "Jacobi forms and Applications" in CIRM, Luminy, in May 2007,
- Workshop "Grenoble–Clermont–2008" at the University Blaise Pascal in Clermont-Ferrand in June 2008 and
- the conference in Autrans "Weekend de rentrée de l'Institut Fourier 2008" in September 2008.

Notations

$\mathbb{N} = \{1, 2, \dots\}$ is the set of natural numbers;

$\mathbb{Z}$ is the ring of rational integers;

$\mathbb{Q}$ is the field of rational numbers;

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$;

$\mathbb{R}$ is the field of real numbers;

$\mathbb{C}$ is the field of complex numbers;

$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$;

I_n is the identity matrix of order n;

J_n is the antisymmetric matrix of order $2n$: $J_n = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}$;

${}^tM$ is the transpose of the matrix M;

$\mathsf{Tr}(M)$ is the trace of the matrix M;

$M > 0$ means that M is a positive definite matrix;

$M_n(K)$ is the set of $n \times n$-matrices with entries in K;

The group of positive symplectic similitudes:
$\mathrm{GSp}_n^+(\mathbb{Q}) = \{M \in M_{2n}(\mathbb{Q}) : M\, J\, {}^tM = \mu(M) J\ ,\ \mu(M) > 0\ \}$;

Siegel modular group of genus n:
$\mathrm{Sp}_n(\mathbb{Z}) = \{M \in M_{2n}(\mathbb{Z}) : M\, J\, {}^tM = J\}$;

The general linear group of degree n over K:
$\mathrm{GL}_n(K)$ is the group of $n \times n$ invertible matrices with entries in K;

The special linear group of degree n over K:
$\mathrm{SL}_n(K) = \{M \in \mathrm{GL}_n(K) : \det(M) = 1\}$;

$\big(M\big) = \Gamma M \Gamma$ is the double coset modulo the group Γ;

The upper half plane:
$\mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$;

The Siegel upper half space:
$\mathfrak{H}^n = \{Z = {}^tZ = X + iY : X, Y \in M_n(\mathbb{R}),\ Y > 0\}$;

Chapter 1

Preliminaries on Hecke algebras and Siegel modular forms

1.1 Hecke algebras

For any subgroup Γ of a semigroup S consider the $\mathbb{Q}$-vector space formally generated by all left cosets ΓM of $M \in \mathrm{S}$

$$L_{\mathbb{Q}}(\Gamma, \mathrm{S}) = \Big\{ \sum_j a_j(\Gamma M_j) : M_j \in \mathrm{S},\, a_j \in \mathbb{Q} \Big\} . \tag{1.1}$$

Let us assume, that any double coset $\big(M\big) = \Gamma M \Gamma \subset \mathrm{S}$ consists of a *finite* union of left cosets of elements M_j of $\Gamma M \Gamma$, modulo Γ

$$\big(M\big) = \bigcup_{j=1}^{K(M)} \Gamma M_j \quad (K(M) = \#\{\Gamma \backslash \Gamma M \Gamma\}) , \tag{1.2}$$

also we write

$$\big(M\big) = \sum_{M_j \in \Gamma \backslash \Gamma M \Gamma} \Gamma M_j . \tag{1.3}$$

We define the abstract Hecke algebra $\mathcal{L}_{\mathbb{Q}}(\Gamma, \mathrm{S}) = L_{\mathbb{Q}}(\Gamma, \mathrm{S})^{\Gamma}$ as $\mathbb{Q}$-vector space of elements of $L_{\mathbb{Q}}(\Gamma, \mathrm{S})$ fixed by the action of Γ to the right. Double cosets $\big(M\big)$ representing $\Gamma \backslash \mathrm{S} / \Gamma$, form the basis of $\mathcal{L}_{\mathbb{Q}}$; we define their product as

$$\big(M\big) \cdot \big(N\big) = \sum_{i=1}^{K(M)} (\Gamma M_i) \sum_{j=1}^{K(N)} (\Gamma N_j) = \sum_{i,j} (\Gamma M_i N_j) , \tag{1.4}$$

which can be written as $\sum_{k=1}^{K(M,N)} a_k \big(T_k\big)$ for suitable double cosets $\big(T_k\big)$, coefficients a_k are integer numbers $\geqslant 1$. Due to bilinearity this product belongs to $\mathcal{L}_{\mathbb{Q}}(\Gamma, \mathrm{S})$.

1.1.1 Hecke algebra for Sp_n

We denote by I_n the identity matrix of order n, and by J_n the antisymmetric matrix of order $2n$

$$J_n = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}. \tag{1.5}$$

Let us consider the group of positive symplectic similitudes

$$\mathrm{S} = \mathrm{GSp}_n^+(\mathbb{Q}) = \{M \in M_{2n}(\mathbb{Q}) : {}^tMJ_nM = \mu(M)J_n\,,\ \mu(M) > 0\,\}\,, \tag{1.6}$$

where ${}^tM$ is a transpose matrix of M. The rational number $\mu(M) > 0$ is called the scalar factor of the similitude M.

Let

$$\Gamma = \mathrm{Sp}_n(\mathbb{Z}) = \{M \in \mathrm{S} \cap M_{2n}(\mathbb{Z}) : \mu(M) = 1\,\} \tag{1.7}$$

be the Siegel modular group of genus n. We denote double cosets by

$$\big(M\big) = \Gamma M \Gamma \subset \mathrm{S}\ (\text{for } M \in \mathrm{S})\,. \tag{1.8}$$

The following proposition allows us to introduce a useful parametrization of the symplectic factors.

Proposition 1.1 (Lemma 3.6 [AZ95]) *Each double coset $\big(M\big) = \Gamma M \Gamma$, where $M \in \mathrm{S}$ contains a unique representative of the following diagonal matrix form*

$$\begin{aligned} &\mathrm{sd}(M) = \mathrm{diag}(d_1, \ldots, d_n; e_1, \ldots, e_n)\,, \\ \textit{and}\ \ &d_i, e_j \in \mathbb{Z}_+,\ d_ie_i = \mu(M)\ (i, j = 1, \ldots, n)\,,\ d_1|\cdots|d_n|e_n|\cdots|e_1\,. \end{aligned}$$

We call the object $\mathrm{sd}(M)$ *the matrix symplectic factor* of the matrix M and the numbers $d_i = d_i(M)$ and $e_i = e_i(M)$ for all $i = 1, \ldots, n$ *the symplectic factors* of the matrix M.

For each scalar factor μ (which is a strictly positive integer), we define the ensemble $\mathrm{SD}_n(\mu)$ of the following integer positive marices

$$\mathrm{SD}_n(\mu) = \{\mathrm{diag}(d_1, \ldots, d_n; e_1, \ldots, e_n)\} \tag{1.9}$$

where $d_1|\cdots|d_n|e_n|\cdots|e_1$, $d_i, e_j \in \mathbb{Z}_+$, such that $d_ie_i = \mu$ $(i, j = 1, \ldots, n)$.

We denote by $T(\mu)$ the Hecke operator

$$T(\mu) := \sum_{M \in \mathrm{SD}_n(\mu)} \big(M\big)\,. \tag{1.10}$$

PROPOSITION 1.2 (LEMMA 3.10 [AZ95]) *The operator $T(\mu)$ can be presented as a finite union of the left cosets*

$$T(\mu) = \sum_{\substack{M\in\Gamma\backslash \mathrm{S}\\ \mu(M)=\mu}} \big(\Gamma M\big)\,.$$

The following proposition gives a practical form for explicit computation of the sum, which appears in the Proposition 1.2 (one can factor the number μ by the powers of primes; then for each factor the sum of elements of the corresponding local algebra can be written).

PROPOSITION 1.3 (LEMMA 3.11 [AZ95]) *Each left coset ΓM, where $M \in \mathrm{S}$ contains a unique representative of the form*

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \begin{pmatrix} \mu(M)\,{}^tD^{-1} & B \\ 0 & D \end{pmatrix},$$

where the left coset of D modulo GL_n depends only on the double coset $\big(M\big) = \Gamma M\Gamma$ and B belongs to the fixed residue class of D

$$\begin{aligned} &B(D) = \{B \in M_n(\mathbb{Z}) \ : \ {}^tBD = {}^tDB\} \\ &B \equiv B' \pmod{D} \Leftrightarrow (B-B')D^{-1} \in M_n(\mathbb{Z})\,. \end{aligned} \tag{1.11}$$

The double coset with the fixed representative $\mathrm{diag}(d_1,\ldots,d_n;e_1,\ldots,e_n) = \mathrm{sd}(M)$ we denote by

$$T(d_1,\ldots,d_n;e_1,\ldots,e_n) = \big(\mathrm{diag}(d_1,\ldots,d_n;e_1,\ldots,e_n)\big) = \big(\mathrm{sd}(M)\big)\,, \tag{1.12}$$

as the particular Hecke operator.

Let p be a prime. The local Hecke algebra over $\mathbb{Z}$ (a commutative ring)

$$\mathcal{L}_{n,\mathbb{Z}} = \mathbb{Z}[\mathbf{T}(p), \mathbf{T}_1(p^2), \ldots, \mathbf{T}_n(p^2)] \tag{1.13}$$

is defined by the following $n+1$ Hecke operators

$$\begin{aligned} &\mathbf{T}(p) := T(\underbrace{1,\ldots,1}_{n},\underbrace{p,\ldots,p}_{n})\,, \\ &\mathbf{T}_i(p^2) := T(\underbrace{1,\ldots,1}_{n-i},\underbrace{p,\ldots,p}_{i},\underbrace{p^2,\ldots,p^2}_{n-i},\underbrace{p,\ldots,p}_{i})\,,\ i=1,\ldots,n\,, \end{aligned} \tag{1.14}$$

which form the basis of the algebra. We use the common notation $[\mathbf{p}]_n$ (or just $[\mathbf{p}]$ if the context of n is clear) for the scalar Hecke operator $\mathbf{T}_n(p^2)$ $[\mathbf{p}] = [\mathbf{p}]_n = \mathbf{T}_n(p^2) = \big(pI_{2n}\big)$.

For the above introduced basis Hecke operators the matrix representations are as follows:

$$\mathbf{T}(p) = \Gamma \begin{pmatrix} I_n & 0 \\ 0 & pI_n \end{pmatrix} \Gamma\,, \tag{1.15}$$

and for $i = 1, \ldots, n$

$$\mathbf{T}_i(p^2) = \Gamma \begin{pmatrix} I_{n-i} & 0 & 0 & 0 \\ 0 & pI_i & 0 & 0 \\ 0 & 0 & p^2 I_{n-i} & 0 \\ 0 & 0 & 0 & pI_i \end{pmatrix} \Gamma\,. \tag{1.16}$$

1.1.2 Hecke algebra for GL_n.

Let $G = \mathrm{GL}_n(\mathbb{Q})$ and $\Lambda = \mathrm{GL}_n(\mathbb{Z})$. We define the correspondent local Hecke algebra for general linear group $\mathcal{H}_{\mathbb{Q}}(\Lambda, G) = L_{\mathbb{Q}}(\Lambda, G)^{\Lambda}$. This algebra is generated by n basis operators:

$$\pi_i = \pi_i(p) = \big(\mathrm{diag}(\underbrace{1, \ldots, 1}_{n-i}, \underbrace{p, \ldots, p}_{i})\big)\,,\ 1 \leqslant i \leqslant n\,. \tag{1.17}$$

Proposition 1.4 (Lemma 2.7 and equation (2.36) [AZ95]) *Each left coset Λg ($g \in G$) contains a unique representative of the form*

$$\begin{pmatrix} p^{\delta_1} & c_{12} & \cdots & c_{1n} \\ 0 & p^{\delta_2} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & p^{\delta_n} \end{pmatrix}\,, \quad \textit{where } \delta_1, \ldots, \delta_n \in \mathbb{Z} \textit{ and } 0 \leqslant c_{ij} < p^{\delta_j}\,. \tag{1.18}$$

Here it is necessary to introduce other elements of the algabra $\mathcal{H}_{\mathbb{Q}}(\Lambda, G)$, in relation to the product of generators $\pi_i(p)$, and which we use (cf. §1.2.2) in the definition of the spherical mapping below for Sp_n; these elements appear in the formula for the product of generators π_i.

$$\pi_{\alpha\beta} = \pi^n_{\alpha\beta}(p) = \left(\begin{pmatrix} I_{n-\alpha-\beta} & 0 & 0 \\ 0 & p\, I_\alpha & 0 \\ 0 & 0 & p^2 I_\beta \end{pmatrix} \right)\,. \tag{1.19}$$

Actually, the development in the Hecke algebra for GL_n the product of two generators π_i and π_j, where $1 \leqslant i, j \leqslant n$, is written as:

$$\pi_i \pi_j = \sum_{\substack{0 \leqslant a \leqslant n-j \\ 0 \leqslant b \leqslant j \\ a+b=i}} \frac{\varphi_{a+j-b}(p)}{\varphi_a(p)\varphi_{j-b}(p)} \pi_{a+j-b,b}\,, \tag{1.20}$$

where

$$\varphi_r(v) = (v-1)(v^2-1)\cdots(v^r-1) \quad \text{for } r \geqslant 1 \qquad (1.21)$$
$$\text{and } \varphi_0(v) = 1\ .$$

1.2 Spherical map

There are several methods for constructing the map of the Hecke algebra to the polynomial ring. Here, we refer to the classical and fundamental book by Andrianov and Zhuravlev [AZ95] (or its first edition [And87]), where the Hecke algebra is represented in terms of double cosets and their decomposition to the left cosets. The spherical map is a very effective research tool in the Hecke algebras. It allows us to perform the copmutation in the polynomial ring, where the operation of multiplication is much simpler in realization than in the ring of the matrix double cosets.

1.2.1 The case of the general linear group

In the case of the group GL_n the spherical map

$$\omega \ : \ \mathcal{H}_{\mathbb{Q}}(\Lambda, G) \to \mathbb{Q}[x_1, \ldots, x_n] \qquad (1.22)$$

is defined for the representatives of the left cosets of the form (1.18) as

$$\omega(\Lambda g) = \prod_{i=1}^{n} (x_i p^{-i})^{\delta_i}\ , \qquad (1.23)$$

so the image of an arbitrary element $t = \sum_j^{K(t)} a_j\big(\Lambda g_j\big) \in \mathcal{H}_{\mathbb{Q}}(\Lambda, G)$ is given in the form of finite linear combination of the left cosets Λg_j which is written as

$$\omega(t) = \sum_j a_j \omega(\Lambda g_j) = \sum_j a_j \prod_{i=1}^{n} (x_i p^{-i})^{\delta_i}\ . \qquad (1.24)$$

This map is injecting since the diagonal $(p^{\delta_1}, \ldots, p^{\delta_n})$ of the matrix (1.18) is defined uniquely by the left coset due to the Proposition 1.4.

The Lemma 2.21, Chapter 3 in [AZ95] gives explicit formule for the images of basis elements (1.17) under the spherical map in the case of the Hecke algebra for GL_n:

$$\omega(\pi_i(p)) = p^{-\frac{i(i+1)}{2}} e_i(x_1, \ldots, x_n) \quad (1 \leqslant i \leqslant n), \qquad (1.25)$$

where

$$e_i(x_1,\dots,x_n)=\sum_{1\leqslant\alpha_1<\dots<\alpha_i\leqslant n} x_{\alpha_1}\cdots x_{\alpha_i} \tag{1.26}$$

is the i-th elementary symmetrical polynomial (see the section 1.3).

1.2.2 The case of the symplectic group

The definition of the spherical map in the case of the symplectic Hecke algebra Sp_n is based on the definition of the spherical map in the case of the group GL_n. Let us consider an arbitrary element (a double coset) $T\in\mathcal{L}_{n,\mathbb{Z}}$ as a finite linear combination of the left cosets:

$$T=\sum_j b_j\big(\Gamma M_j\big)\,,\quad\text{with}\quad \mu(M_j)=p^{\delta_j}\,. \tag{1.27}$$

We can choose the representatives for the left cosets according to the Proposition 1.3:

$$\Gamma M_j=\begin{pmatrix} p^{\delta_j}D_j^* & B\\ 0 & D_j\end{pmatrix}, \tag{1.28}$$

where $D_j^*={}^tD_j^{-1}$ and the matrix D_j is an upper triangular:

$$D_j=\begin{pmatrix} p^{\gamma_{1j}} & * & \cdots & \cdots\\ 0 & p^{\gamma_{2j}} & * & \cdots\\ \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 0 & p^{\gamma_{nj}}\end{pmatrix}. \tag{1.29}$$

The spherical map Ω is defined as follows:

$$\Omega(T)=\sum_j b_j x_0^{\delta_j}\omega(\Lambda D_j)\,. \tag{1.30}$$

Using Andrianov's method (see page 146 of [AZ95]) one can obtain the principal formulae for spherical images of basis Hecke operators::

$$\begin{aligned}\Omega(\mathbf{T}(p))&=\sum_{i=0}^{n} x_0e_i(x_1,\dots,x_n)=x_0\prod_{i=1}^{n}(1+x_i)\,,\\ \Omega(\mathbf{T}_i(p^2))&=\sum_{\substack{a+b\leqslant n\\ a\geqslant i}} p^{b(a+b+1)}l_p(a-i,a)x_0^2\omega(\pi_{a,b}(p))\,,\end{aligned} \tag{1.31}$$

where the coefficient $l_p(r,a)$ gives the number of symmetrical marices of the size $a\times a$ and rank r over the field of p elements. This coefficient can be

computed using the recursive formula (6.79) in [AZ95] (page 214, Chapter 3, §6):

$$l_p(r,a) = l_p(r,r)\frac{\varphi_a(p)}{\varphi_r(p)\varphi_{a-r}(p)}\,, \tag{1.32}$$

(the function $\varphi_r(v)$ is given by the formula (1.21)).

1.3 Symmetric polynomials

Due to the spherical map, manipulations with elements of the Hecke algebra can be carried out in the polynomial ring. Here we recall the basic definitions and properties of symmetric functions. The theory of symmetric functions of several variables is described in the book "Symmetric functions and Hall polynomials" by Macdonald [Mac95]. Most of the definitions were taken from there. In the theory of symmetric functions, the number of variables is usually irrelevant, provided only that it is large enough, and it is often more convenient to work with symmetric functions in infinitely many variables.

The symmetric group S_n is a group of $n!$ permutations of the final set of integers $\{1, 2, \ldots, n\}$. For all $n > 0$, the group S_n can be injected into S_m for any $m > n$ since one can consider S_n as a subgroup of S_m by adding to all parmutations $\pi \in \mathrm{S}_n$ fixed points $n+1, n+2, \ldots, m$. Bearing in mind this injection $\mathrm{S}_n \hookrightarrow \mathrm{S}_m$, one can define the group S_∞ of all permutations of the set of all positive integers, which permutes the finite number of them:

$$\mathrm{S}_\infty := \bigcup_{i>0} \mathrm{S}_i\,.$$

Let us consider the ring of polynomials $\mathbb{Z}[x_1, \ldots, x_n]$ of n independent variables with integer coefficients. The symmetric group S_n acts on polynomials of n variables $f \in \mathbb{Z}[x_1, \ldots, x_n]$ by permuting the variables $x_1, \ldots, x_n$: $\sigma f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, where $\sigma \in \mathrm{S}_n$.

The polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is *symmetric* if f is an invariant under the action of the group S_n, or $\forall \pi \in \mathrm{S}_n \;\Rightarrow\; \pi f = f$.

The symmetric polynomials form the subring $\Lambda_n = \mathbb{Z}[x_1, \ldots, x_n]^{\mathrm{S}_n}$.

Let $\mathbf{x} = \{x_1, x_2, \ldots\}$ be a set of commutative variables, which we call an alphabyte.

1.3.1 Elementary symmetric polynomials

The *elementary symmetric functions* $e_r(\mathbf{x})$ are defined via the following generating series (t being another variable):

$$E_t(\mathbf{x}) := \sum_{r\geqslant 0} t^r e_r(\mathbf{x}) = \prod_{i\geqslant 1}(1+x_i t)\,. \tag{1.33}$$

If the number of variables is finite, say n, then e_r is zero for all $r > n$, and the previous formula takes the form

$$\sum_{r=0}^{n} t^r e_r(\mathbf{x}) = \prod_{i=1}^{n}(1+x_i t)\,. \tag{1.34}$$

Similar remarks will obviously apply to many subsequent formulae and will be omitted. For example, if $\mathbf{x} = \{x_1, x_2, x_3\}$ one has

$$\begin{aligned} e_1(\mathbf{x}) &= x_1 + x_2 + x_3\,,\\ e_2(\mathbf{x}) &= x_1x_2 + x_1x_3 + x_2x_3\,,\\ e_3(\mathbf{x}) &= x_1x_2x_3\,,\\ e_4(\mathbf{x}) &= 0\,. \end{aligned}$$

1.3.2 Complete symmetric functions

The *complete symmetric functions* $h_r(\mathbf{x})$ are defined via the generating series:

$$H_t(\mathbf{x}) := \sum_{r\geqslant 0} t^r h_r(\mathbf{x}) = \prod_{i\geqslant 1}(1-x_i t)^{-1}\,. \tag{1.35}$$

For example, if $\mathbf{x} = \{x_1, x_2, x_3\}$, one has

$$\begin{aligned} h_1(\mathbf{x}) &= x_1 + x_2 + x_3\,,\\ h_2(\mathbf{x}) &= x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3\,,\\ h_3(\mathbf{x}) &= x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2 + x_1x_2x_3\,. \end{aligned}$$

In particular, $h_0 = 1$, $h_1 = e_1$.

1.3.3 Power sums

The *power sums* $p_r(\mathbf{x})$ are defined via the generating series:

$$P_t(\mathbf{x}) := \sum_{r\geqslant 0} t^{r-1} p_r(\mathbf{x}) = \sum_{i\geqslant 1} x_i(1-x_i t)^{-1}\,. \tag{1.36}$$

For example, if $\mathbf{x} = \{x_1, x_2, x_3\}$, one has

$$p_1(\mathbf{x}) = x_1 + x_2 + x_3\,,$$
$$p_2(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2\,.$$

A *partition* is a sequence of ordered positive integers (called "parts of the partition") $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_r : \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_r\}$. We also write $\lambda = (1^{\alpha_1} 2^{\alpha_2} \ldots)$, where α_i is a number of parts λ_k, which are equal to i. The *weight* of λ is $|\lambda| := \sum_k \lambda_k$ and its *length* is the total number of the parts $\ell(\lambda) := r$.

With each partition $\lambda = (1^{\alpha_1} 2^{\alpha_2} \ldots)$ we associate the following elements:

$$e_\lambda = e_1^{\alpha_1} e_2^{\alpha_2} \ldots\,,$$
$$h_\lambda = h_1^{\alpha_1} h_2^{\alpha_2} \ldots\,,$$
$$p_\lambda = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\,.$$

1.3.4 Monomial symmetric functions

For each $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ we denote the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by $\mathbf{x}^\alpha$. If $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ is a partition of the length n, the *monomial symmetric function* $m_\lambda(\mathbf{x})$ is defined as the sum of all permutations of monomial variables $\mathbf{x}^\lambda = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$:

$$m_\lambda(\mathbf{x}) := \sum_{\pi \in \mathrm{S}_n} \mathbf{x}^{\pi(\lambda)}\,. \tag{1.37}$$

For example, if $\mathbf{x} = \{x_1, x_2, x_3\}$,

$$m_{1,1}(\mathbf{x}) = x_1x_2 + x_1x_3 + x_2x_3\,,$$
$$m_2(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2\,,$$
$$m_{2,1}(\mathbf{x}) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2\,.$$

1.3.5 Schur functions

Let us consider a finite number n of variables, $\mathbf{x} = (x_1, \ldots, x_n)$. Let $\lambda = (\lambda_1, \ldots, \lambda_r) \in \mathbb{Z}^r$ be any (not necessary a partition) r-tuple of nonnegative integers. Consider the monomial $\mathbf{x}^\lambda = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$, and the polynomial a_α, which is obtained by antisymmetrizing $\mathbf{x}^\lambda$, that is:

$$a_\alpha = a_\alpha(x_1, \ldots, x_n) = \sum_{\omega \in \mathrm{S}_n} \varepsilon(\omega) \cdot \omega(\mathbf{x}^\alpha)\,, \tag{1.38}$$

where $\varepsilon(\omega)$ is the *sign* (± 1) of the permutation ω. The polynomial a_α is skew-symmetric, i.e. $\omega(a_\alpha) = \varepsilon(\omega)a_\alpha$ for any $\omega \in \mathrm{S}_n$; in particular, therefore a_α vanishes if there are two $\alpha_i = \alpha_j$ ($i \neq j$). Hence, we may also assume that $\alpha_1 > \alpha_2 > \ldots > \alpha_n \geqslant 0$. Then $\alpha = \lambda + \delta$, where λ is a partition of length not greater then n, and $\delta = (n-1, n-2, \ldots, 1, 0)$. Finally, $a_\alpha = a_{\lambda+\delta}$ can be written as a determinant:

$$a_{\lambda+\delta} = \sum_{\omega \in \mathrm{S}} \varepsilon(\omega) \cdot \omega(\mathbf{x}^{\lambda+\delta}) = \det(x_i^{\lambda_j+n-j}), \quad \text{where } 1 \leqslant i, j \leqslant n. \tag{1.39}$$

Since a_α changes sign when the variables x_i and x_j are interchanged, a_α vanishes at $x_i = x_j$ and is therefore divisible by $x_i - x_j$ for all $i \neq j$. Therefore a_α is divisible by the Vandermonde determinant

$$\prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) = \det(x_i^{n-j}) = a_\delta. \tag{1.40}$$

So a_α is divisible by a_δ, and the quotient

$$s_\lambda = s_\lambda(x_1, \ldots, x_n) := a_{\lambda+\delta}/a_\delta \tag{1.41}$$

is *symmetric* and is called the *symmetric Schur function.*

Each Schur function s_λ can be expressed as a polynomial in the elementary symmetric functions e_r, and as a polynomial in the complete symmetric functions h_r:

$$s_\lambda = \det(e_{\lambda'_i - i + j})_{1 \leqslant i,j \leqslant m}, \tag{1.42}$$

where $m \geqslant \ell(\lambda')$, and

$$s_\lambda = \det(h_{\lambda_i - i + j})_{1 \leqslant i,j \leqslant n}, \tag{1.43}$$

where $m \geqslant \ell(\lambda)$, $h_k = 0$ for $k < 0$.

1.4 Siegel modular forms

1.4.1 Classical modular forms

First, we recall the basic definitions. The complex upper half-plane is denoted by

$$\mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\}. \tag{1.44}$$

The *modular group*

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\} \tag{1.45}$$

acts on the upper half plane $\mathfrak{H}$ via linear fractional transformations as follows. Consider $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. For any $z \in \mathfrak{H}$ we put

$$\gamma(z) = \frac{az+b}{cz+d} \in \mathfrak{H}\,. \tag{1.46}$$

Now consider a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Congruence subgroups play an important role in the theory of modular forms. A congruence subgroup of a matrix group with integer entries is a subgroup with congruence conditions on the matrix entries.

Definition 1.5 (principal congruence subgroup of level N)
Let N be a positive integer. The ***principal congruence subgroup*** *of level N is*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition 1.6 (congruence subgroup of level N)
A ***congruence subgroup*** Γ *of* $\mathrm{SL}_2(\mathbb{Z})$ *is any subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *that contains* $\Gamma(N)$ *for some positive* $N \in \mathbb{Z}$*, in which case* Γ *is a congruence subgroup* ***of level*** N*.*

The most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}, \tag{1.47}$$

where $*$ means any integer, and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}. \tag{1.48}$$

Obviously,

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})\,. \tag{1.49}$$

Let k be an integer. Define the *weight k right action* of $\mathrm{SL}_2(\mathbb{Z})$ on the set of all functions $f : \mathfrak{H} \to \mathbb{C}$ as

$$(f|_k\gamma)(z) = (cz+d)^{-k} f(\gamma(z)), \text{ where } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})\,. \tag{1.50}$$

Definition 1.7 (modular form) *A* ***modular form*** *of integer weight k of level N for a congruence subgroup Γ is a holomorphic on $\mathfrak{H} \cup \infty$ as well as at all cusps of Γ function $f : \mathfrak{H} \to \mathbb{C}$ such that $f|_k\gamma = f$ for all $\gamma \in \Gamma$.*

We denote the *space of modular forms* of weight k for Γ by $\mathcal{M}_k(\Gamma)$. Every element f of $\mathcal{M}_k(\Gamma)$ has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n \, e^{2\pi i n z} \tag{1.51}$$

with complex coefficients a_n. Often it is more convenient to write these series in terms of "q-expansion" with $q = e^{2\pi i z}$

$$f(z) = \sum_{n=0}^{\infty} a_n \, q^n \, . \tag{1.52}$$

DEFINITION 1.8 (CUSP FORM) *A **cusp form** is a modular form that vanishes at ∞, i.e. the Fourier coefficient $a_0 = 0$.*

We denote the *space of cusp forms* of weight k for Γ by $\mathcal{S}_k(\Gamma)$.

More generally, for a positive integer k and a Dirichlet character χ modulo a positive integer N such that $\chi(-1) = (-1)^k$, the holomorphic modular form $f(z)$ satisfy

$$f(\gamma(z)) = \chi(d) \, (cz + d)^k \, f(z) \tag{1.53}$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. We denote the space of such forms by $\mathcal{M}_k(\Gamma, \chi)$.

1.4.2 Siegel Modular Forms

We turn now to the case of higher genus. The Siegel upper half space in genus n is the set of all $n \times n$ complex symmetric matrices with positive-definite imaginary part:

$$\mathfrak{H}^n = \left\{ Z = {}^tZ = X + iY : X, Y \in M_n(\mathbb{R}),\, Y > 0 \right\} . \tag{1.54}$$

The symplectic group (1.7)

$$\mathrm{Sp}_n(\mathbb{Z}) = \{ M \in M_{2n}(\mathbb{Z}) : M \, J \, {}^tM = J \} \text{ for } J_n = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix} \tag{1.55}$$

acts on the space $\mathfrak{H}^n$ as

$$\gamma(Z) = (AZ + B) \, (CZ + D)^{-1} \, , \tag{1.56}$$

where $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_n(\mathbb{Z})$ and $Z \in \mathfrak{H}^n$. For such γ we define the *weight* $k \in \mathbb{Z}$ *right action* of $\mathrm{Sp}_n(\mathbb{Z})$ on the set of all functions $F : \mathfrak{H}^n \to \mathbb{C}$ similarly to (1.50) as

$$(F|_k\gamma)(Z) = \det(CZ + D)^{-k} F(\gamma(Z)) \, . \tag{1.57}$$

Definition 1.9 (Siegel modular form)
A holomorphic function $F : \mathfrak{H}^n \to \mathbb{C}$ is called a ***genus*** *n* ***Siegel modular form of weight*** *k on $\mathrm{Sp}_n(\mathbb{Z})$ if F satisfies*

$$(F|_k\gamma)(Z) = F(Z)\,, \quad \forall \gamma \in \mathrm{Sp}_n(\mathbb{Z})\,. \tag{1.58}$$

In the case of $n = 1$, we also require that F is holomorphic at ∞.

Remark 1.10 *The holomorphy condition is required only for forms of genus $n = 1$, since for $n \geqslant 2$, this condition is a consequence of the definition due to the Koecher principle [vdG08, Theorem 2]. The theorem states that if F is a Siegel modular form of weight k and degree $n > 1$, then F is bounded on subsets of $\mathfrak{H}^n$ of the form $\{Z \in \mathfrak{H}^n : \Im(Z) > \epsilon I_n\}$, where $\epsilon > 0$. Corollary to this theorem is that Siegel modular forms of degree $n > 1$ have Fourier expansions and are thus holomorphic at infinity.*

We denote the vector space of Siegel modular forms of weight k with genus n on $\mathrm{Sp}_n(\mathbb{Z})$ by $\mathcal{M}_k(\mathrm{Sp}_n(\mathbb{Z}))$.

Siegel modular forms can be thought of as multivariate modular forms, i.e. as special functions of several complex variables. On the other hand, Siegel modular forms of genus 1 are classical modular forms on the upper half plane which transform under $\mathrm{SL}_2(\mathbb{Z})$.

In the formal Fourier expansion of a Siegel modular form

$$F(Z) = \sum_{N \in \mathcal{B}} a(N)\, q^N \tag{1.59}$$

the symbol

$$q^N = e^{2\,\pi\, i\, \mathsf{Tr}(NZ)} \tag{1.60}$$

is used, where

$$\mathcal{B} = \left\{M \in M_n(\mathbb{Q}) : M = {}^tM,\ M \geqslant 0,\ M \text{ half-integral}\right\} \tag{1.61}$$

and $\mathsf{Tr}(M)$ means the trace of the matrix M; a symmetric $n \times n$-matrix $M \in \mathrm{GL}_n(\mathbb{Q})$ is called half-integral if $2M$ is an integral matrix with the even diagonal entries.

1.5 Satake parameters, L-functions

1.5.1 Hecke L-functions

The space of modular forms $\mathcal{M}_k(\Gamma)$ is a finite dimensional vector space over $\mathbb{C}$ upon which various linear operators act. In terms of characterizing modular

forms, the Hecke operators are an important family of such operators. In the genus 1 case, the Hecke algebra consists of operators $T(n)$ for all positive $n \in \mathbb{Z}$.

Suppose that $f(z) = \sum_{m=0}^{\infty} a(m)\, q^m \in \mathcal{M}_k$ is an eigenvector of all the Hecke operators $T(n)$, i.e.

$$f|_k T(n) = \lambda_n\, f \quad \forall n \tag{1.62}$$

for some complex numbers λ_n. Then this modular form f can be normalized in such a way, that its Fourier coefficient $a(1) = 1$. We call a modular form satisfying this condition a *Hecke form*, or a *normalized Hecke eigenform*. The important property for such modular forms is that the sequence of Fourier coefficients $\{a(n)\}$ is multiplicative, i.e. $a(1) = 1$ and $a(nm) = a(n)\, a(m)$ whenever n and m are coprime.

The natural way to investigate a multiplicative function $n \mapsto a(n)$ is to form the Dirichlet series $\sum_{m=1}^{\infty} a(m)\, m^{-s}$, the point is that the multiplicative property implies that $a(p_1^{r_1} \cdots p_l^{r_l}) = a(p_1^{r_1}) \cdots a(p_l^{r_l})$ and hence that this Dirichlet series has an Euler product $\prod_{p \text{ prime}} \left(\sum_{r \geqslant 0} a(p^r)\, p^{-rs} \right)$.

Definition 1.11 *The Hecke* ***L*-series** *of a modular form f with Fourier expansion $f(z) = \sum_{m=0}^{\infty} a(m)\, q^m \in \mathcal{M}_k$ is*

$$L(s, f) = \sum_{m=0}^{\infty} \frac{a(m)}{m^s}\,. \tag{1.63}$$

If f is a Hecke eigenform we have an Euler product

$$L(s, f) = \prod_{p \text{ prime}} \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots \right) \tag{1.64}$$

because the coefficients $a(m)$ are multiplicative. In the section 2.1 below we shall see that the summation $\sum_{r \geqslant 0} a(p^r)\, p^{-rs}$ resolves into the polynomial fraction, therefore the Euler product for the Hecke eigenform of weight k takes the following form:

$$L(s, f) = \prod_{p \text{ prime}} \frac{1}{1 - a(p)\, p^{-s} + p^{k-1-2s}}\,. \tag{1.65}$$

L-series converge in a half plane and define functions with useful analytic properties, such as functional equation and growth estimation of the coefficients.

For Siegel modular forms of genus $n = 1$ (classical modular forms on $\mathrm{SL}_2(\mathbb{Z})$) which are simultaneous eigenforms of all the Hecke operators, the associated L-function determines the form up to a constant multiple. It is unknown if such an L-function exists for similar forms of genus $n \geqslant 2$.

1.5.2 Satake parameters

A study of spinor and standard zeta functions naturally leads to a study of Satake p-parameters, an invariant related to Siegel modular forms. There are several important facts related to the definition of the Satake parameters, see [And77] for details:

- ▷ The Hecke algebra for symplectic group (see Section 1.1.1) can be presented as a direct product of local p algebras $\mathcal{L}_n$ over all primes p.
- ▷ There is an isomorphism $\mathrm{Hom}_{\mathbb{C}}(\mathcal{L}_n, \mathbb{C}) \cong (\mathbb{C}^*)^{n+1}/W$, where W is the Weyl group.
- ▷ The Weyl group W has an action on $(n+1)$-tuples $(x_0, x_1, \ldots, x_n) \in (\mathbb{C}^*)^{n+1}$ which is generated by all permutations of n elements $x_1, \ldots, x_n$ and by maps $(x_0, x_1, \ldots, x_i, \ldots, x_n) \mapsto (x_0 x_i, x_1, \ldots, x_i^{-1}, \ldots, x_n)$ for $i = 1$ to n.
- ▷ For a given simultaneous eigenform f of all Hecke operators $T \in \mathcal{L}_n$ with respective eigenvalues $\lambda_f(T)$, the map $T \mapsto \lambda_f(T)$ is an element of $\mathrm{Hom}_{\mathbb{C}}(\mathcal{L}_n, \mathbb{C})$.

Definition 1.12 (Satake parameters)
*The **Satake p-parameters** associated to the eigenform $f \in \mathcal{M}_k(\mathrm{Sp}_n(\mathbb{Z}))$ are the elements of the $(n+1)$-tuple, $(\alpha_0, \alpha_1, \ldots, \alpha_n) \in (\mathbb{C}^*)^{n+1}/W$, which is the image of the map $T \mapsto \lambda_f(T)$ under the isomorphism $\mathrm{Hom}_{\mathbb{C}}(\mathcal{L}_n, \mathbb{C}) \cong (\mathbb{C}^*)^{n+1}/W$.*

Note, these parameters depend on prime p but in order to simplify the notations we do not express this relation directly (by placing p as an indice, for example) since in most cases we will fix the prime p and consider the local factor.

The Satake parameters satisfy the relation

$$\alpha_0^2 \alpha_1 \cdots \alpha_n = p^{nk - n(n+1)/2}\,. \tag{1.66}$$

Examples:

1. If f is the Siegel-Eisenstein series of weight k genus n then the Satake p-parameters are: $\alpha_0 = 1$, $\alpha_i = p^{k-i}$ for $i = 1, \ldots, n$.

2. If $f = \sum_{n=1}^{\infty} a(n)\, q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a normalized Hecke eigenform and if we write $a(p) = \beta + \overline{\beta}$ with $\beta\overline{\beta} = p^{k-1}$ then the choice of Satake parameters could be $\alpha_0 = \beta$, $\alpha_1 = \overline{\beta}/\beta$ or $\alpha_0 = \overline{\beta}$, $\alpha_1 = \beta/\overline{\beta}$.

1.5.3 L-functions of Siegel modular forms

For Siegel modular forms of genus $n \geqslant 2$, many complications arise concerning the Hecke theory and L-functions. Specifically, the basis of the Hecke algebra grows; the analogous $T(p)$ operators are no longer sufficient to generate the associated Hecke algebra. Thus, it is unclear if the Hecke eigenvalues $\lambda_F(p)$ will characterize the associated eigenform for genus $n \geqslant 2$. Instead, we examine the Satake parameters because they contain information about all the Hecke eigenvalues. In particular, the Satake p-parameters completely determine the eigenvalues $\lambda_F(p)$. Moreover, for eigenforms of genus 1, knowing the Satake p-parameters is equivalent to knowing the eigenvalues $\lambda_F(p)$. Therefore, genus 1 eigenforms are determined up to a constant multiple by their Satake p-parameters for almost all primes p.

Our comments on L-functions of Siegel modular forms of arbitrary genus are, as next. Primarily, the Fourier coefficients of Siegel modular forms of genus $n \geqslant 2$ are attached to matrices (rather than integers) making it difficult to embed the Fourier coefficients into an L-function. Thus, there are spinor zeta function and standard zeta function that are defined by an Euler product construction instead of a Fourier coefficient construction. While in general it is difficult to determine if these L-functions characterize the associated eigenform, we do know that the spinor and standard zeta function in genus 1 determine the associated eigenform up to the normalization.

Let $F \in \mathcal{M}_k(\mathrm{Sp}_n(\mathbb{Z}))$ be a simultaneous eigenform for all Hecke operators in $\mathcal{L}_n$, and $\{\alpha_0, \ldots, \alpha_n\}$ be the Satake p-parameters of F. Define

$$Q_{F,\,p}(X) = (1 - \alpha_0\, X) \prod_{r=1}^{n} \prod_{1 \leqslant i_1 < \cdots < i_r \leqslant n} (1 - \alpha_0 \alpha_{i_1} \cdots \alpha_{i_r} X)\,. \tag{1.67}$$

The *spinor L-function* attached to the Siegel modular form F is

$$L(s, F, spin) = \prod_{p \text{ prime}} \left(Q_{F,\,p}(p^{-s}) \right)^{-1}. \tag{1.68}$$

For simultaneous eigenforms f of genus 1, the spinor L-function is the usual

Hecke L-series:

$$\begin{aligned} L(s,f) &= \prod_p \left((1-\alpha_{p,0}p^{-s})(1-\alpha_{p,0}\alpha_{p,1}p^{-s})\right)^{-1} \\ &= a(1)\prod_p \left(1-\lambda_F(p)\,p^{-s}+p^{k-1}\,p^{-2s}\right)^{-1} \\ &= \sum_{n=1}^{\infty}\frac{a(n)}{n^s}\,. \end{aligned} \tag{1.69}$$

Thus, we may consider the spinor L-function as generalized factored form of the Euler product of the genus 1 L-function. The analytic continuation of the spinor zeta function is only known for the cases of genus 1 and 2.

There is also a *standard L-function* which is given by

$$L(s,F,stnd) = \prod_{p\text{ prime}} \Big(R_{F,p}(p^{-s})\Big)^{-1}, \tag{1.70}$$

where

$$R_{F,p}(X) = (1-X)\prod_{i=1}^{n}(1-\alpha_i X)(1-\alpha_i^{-1}X)\,. \tag{1.71}$$

In the case of genus 1, the standard L-function is not equal to $\sum a(n)\,n^{-s}$, but is related to the Rankin zeta function $L(s,F,stnd) = D(s,F)$, that is to the Fourier coefficients $a(m^2)$. Indeed, for the normalized Hecke eigenform $f \in \mathcal{M}_k$ of genus 1 one has (see [And77, (3.3)]):

$$D(s-k+1,f) = \prod_p (1+\frac{1}{p^{\,s-k+1}})^{-1}\sum_{n=1}^{\infty}\frac{a(n^2)}{n^s}\,. \tag{1.72}$$

The standard zeta function is also related to the symmetric square L-function.

Many properties are proved for the standard L-function, including the analytic continuation for any genus, see [AK79, Böc85]. However, the standard L-function does not contain the α_0 parameter in its definition. As a consequence, the standard zeta function may not carry the full information about the attached modular form.

Chapter 2

Generating series in Hecke algebras

In this chapter we study the following generating series of operators $\mathbf{T}(p^\delta)$

$$\mathbf{D}_p(X) = \sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) X^\delta \in \mathcal{L}_{n,\mathbb{Z}}[\![X]\!]\,. \tag{2.1}$$

Shimura stated in 1963 (see [Shi63], p. 825) the following conjecture:

> "In general, it is plausible that $\mathbf{D}_p(X) = \mathbf{E}(X)/\mathbf{F}(X)$ with polynomials $\mathbf{E}(X)$ and $\mathbf{F}(X)$ in X with integral coefficients of degree $2^n - 2$ and 2^n, respectively"

(*i.e. with coefficients of both polynomials* $\mathbf{E}(X)$ *and* $\mathbf{F}$ *in the Hecke algebra* $\mathcal{L}_{\mathbb{Z}} = \mathbb{Z}[\mathbf{T}(p), \mathbf{T}_1(p^2), \ldots, \mathbf{T}_{n-1}(p^2), [\mathbf{p}]_n]$).

The existence of such rational polynomial representation $\mathbf{E}(X)/\mathbf{F}(X)$ was proved by Andrianov in the series of works [And67, And68, And69] for an arbitrary genus n. However, the explicit form for the numerator polynomial was not known for the genus $n > 3$. We present the algorithm for computing these polynomials. It was applied in order to obtain the new explicit result for the case of genus $n = 4$.

2.1 Generating series in genus 1 and 2

For genus 1 and genus 2 the results were given by Hecke and Shimura (see [Hec37], [Shi63, Theorem 2]):

$$\mathbf{D}_p^{(1)}(X) = \frac{1}{1 - \mathbf{T}(p)\, X + p\, [\mathbf{p}]_1\, X^2} \tag{2.2}$$

and

$$\mathbf{D}_p^{(2)}(X) = \frac{1 - p^2\,[\mathbf{p}]_2\,X^2}{1 - q_1\,X + q_2\,X^2 - q_3\,X^3 + q_4\,X^4}\,, \tag{2.3}$$

where

$$\begin{aligned} q_1 &= \mathbf{T}(p)\,,\\ q_2 &= p\,\mathbf{T}_1(p^2) + p\,(p^2+1)\,[\mathbf{p}]_2\,,\\ q_3 &= p^3\,[\mathbf{p}]_2\,\mathbf{T}(p)\,,\\ q_4 &= p^6\,[\mathbf{p}]_2^2\,. \end{aligned} \tag{2.4}$$

Indeed, in the case of genus 1 the operators $T(n)$ act on the spaces of modular forms $\mathcal{M}_k$ of the weight k, and the following relations hold:

$$T(m)\,T(n) = T(mn), \quad \text{if } (m,n) = 1, \tag{2.5}$$

$$T(p)\,T(p^n) = T(p^{n+1}) + p^{k-1}\,T(p^{n-1}), \quad \text{for prime } p \text{ and } n \geqslant 1. \tag{2.6}$$

Consider the product $P(X) = \left(\sum_{n=0}^{\infty} T(p^n)\,X^n\right) \times \left(1 - T(p)\,X + p^{k-1}\,X^2\right)$. The coefficient of X is $T(p) - T(p) = 0$; the coefficient of X^{n+1} for $n \geqslant 1$ is $T(p^{n+1}) - T(p)\,T(p^n) + p^{k-1}\,T(p^{n-1}) = 0$ due to (2.6). Therefore, $P(X) = 1$, which verifies (2.2).

In the case of genus 2 we compute the generating series (2.3) by demonstrating the method of Andrianov without the use of computer. From the definition of the Hecke operator (1.10) and the Proposition 1.2 and 1.3, we have the expression for each term in the summation series $\mathbf{D}_p$ (2.1) of genus n

$$\mathbf{T}(p^\delta) = \sum_{D,B} \left(\Gamma \begin{pmatrix} p^\delta\,D^* & B \\ 0 & D \end{pmatrix}\right),$$

where $D \in \Lambda\backslash\Lambda\mathrm{diag}(p^{\delta_1},\ldots,p^{\delta_n})\Lambda$ and $0 \leqslant \delta_1 \leqslant \cdots \leqslant \delta_n \leqslant \delta$, $B \in B(D)/\mathrm{mod}\ D$ (1.11), $\Lambda = \mathrm{GL}_n(\mathbb{Z})$. The number of elements of the set $B \in B(D)/\mathrm{mod}\ D$ for a matrix D with elementary divisors $d_1,\ldots,d_n$ depends only on the elementary divisors and is equal to $d_1^n d_2^{n-1}\cdots d_n$. Therefore, by the definition of the spherical map Ω, we obtain the formal identity:

$$\begin{aligned} \Omega(\mathbf{D}_p(X)) &= \sum_{\delta=0}^{\infty} \Omega(\mathbf{T}(p^\delta))X^\delta \\ &= \sum_{\delta=0}^{\infty} \sum_{0\leqslant\delta_1\leqslant\cdots\leqslant\delta_n\leqslant\delta} p^{n\delta_1+(n-1)\delta_2+\cdots+\delta_n}\,\omega(t(p^{\delta_1},\ldots,p^{\delta_n}))\,(x_0X)^\delta\,, \end{aligned} \tag{2.7}$$

where

$$t(p^{\delta_1},\dots,p^{\delta_n}) = \big(\mathrm{diag}(p^{\delta_1},\dots,p^{\delta_n})\big) \in \mathcal{H}_{\mathbb{Q}} \tag{2.8}$$

is an element of the Hecke algebra for the group GL_n.

In particular, for genus $n = 2$, we have

$$\Omega(\mathbf{D}_p^{(2)}(X)) = \sum_{0\leqslant\delta_1\leqslant\delta_2\leqslant\delta} p^{2\delta_1+\delta_2}\,\omega(t(p^{\delta_1},p^{\delta_2}))\,(x_0X)^{\delta}\,. \tag{2.9}$$

Using the multiplicative properties of the Hecke operators we write $t(p^{\delta_1},p^{\delta_2}) = (\pi_2(p))^{\delta_1}\cdot t(1,p^{\delta_2-\delta_1})$, since the double coset $\pi_2(p)$ consits of the single left coset. Therefore,

$$\begin{aligned}\omega(t(p^{\delta_1},p^{\delta_2})) &= \omega\big((\pi_2(p))^{\delta_1}\cdot t(1,p^{\delta_2-\delta_1})\big)\\ &= (p^{-3}x_1x_2)^{\delta_1}\,\omega(t(1,p^{\delta_2-\delta_1}))\,.\end{aligned} \tag{2.10}$$

With the substitutions $\delta_2 = \delta_1+\alpha$ and $\delta = \delta_2+\beta = \delta_1+\alpha+\beta$, the sum (2.9) can be rewritten in the form

$$\begin{aligned}&\Omega(\mathbf{D}_p^{(2)}(X))\\ &\quad= \sum_{\alpha,\beta,\delta_1\geqslant 0} p^{2\delta_1+\delta_1+\alpha}\,(p^{-3}x_1x_2)^{\delta_1}\,\omega(t(1,p^{\alpha}))\,(x_0X)^{\delta_1+\alpha+\beta}\\ &\quad= \sum_{\beta\geqslant 0}(x_0X)^{\beta}\sum_{\delta_1\geqslant 0}(x_0x_1x_2X)^{\delta_1}\sum_{\alpha\geqslant 0}\omega(t(1,p^{\alpha}))\,(px_0X)^{\alpha}\\ &\quad= (1-x_0X)^{-1}\,(1-x_0x_1x_2X)^{-1}\sum_{\alpha\geqslant 0}\omega(t(1,p^{\alpha}))\,(px_0X)^{\alpha}\,.\end{aligned} \tag{2.11}$$

The last sum can be computed with the help of the Proposition 1.3 by taking the set of the form

$$\left\{\begin{pmatrix}p^{\alpha}&0\\0&1\end{pmatrix},\begin{pmatrix}1&a\\0&p^{\alpha}\end{pmatrix}\text{ with }a \bmod p^{\alpha},\begin{pmatrix}p^{\alpha-\beta}&b\\0&p^{\beta}\end{pmatrix}\text{ with }b \bmod p^{\beta}\text{ and }p\nmid b\right\} \tag{2.12}$$

as a set of representatives of the left cosets modulo Λ contained in the double

coset $\Lambda \begin{pmatrix} 1 & 0 \\ 0 & p^\alpha \end{pmatrix} \Lambda$. Hence, by definition of ω, we obtain

$$\begin{aligned}
\sum_{\alpha \geqslant 0} \omega(t(1,p^\alpha))\,(px_0X)^\alpha &= \sum_{\alpha \geqslant 0} \Big((x_1p^{-1})^\alpha + p^\alpha (x_2p^{-2})^\alpha \\
&\quad + \sum_{0<\beta<\alpha} (p^\beta - p^{\beta-1})(x_1p^{-1})^{\alpha-\beta}(x_2p^{-2})^\beta \Big)\,(px_0X)^\alpha \\
&= \sum_{\beta,\gamma \geqslant 0} p^\beta\,(x_1p^{-1})^\gamma\,(x_2p^{-2})^\beta\,(px_0X)^{\beta+\gamma} \\
&\quad - p^{-1} \sum_{\beta,\gamma \geqslant 1} p^\beta\,(x_1p^{-1})^\gamma\,(x_2p^{-2})^\beta\,(px_0X)^{\beta+\gamma} \\
&= (1 - x_0x_1X)^{-1}\,(1 - x_0x_2X)^{-1}\,(1 - p^{-1}x_0^2x_1x_2X^2)\,.
\end{aligned} \tag{2.13}$$

Thus

$$\Omega(\mathbf{D}_p^{(2)}(X)) = \frac{1 - p^{-1}x_0^2x_1x_2X^2}{(1 - x_0X)\,(1 - x_0x_1X)\,(1 - x_0x_2X)\,(1 - x_0x_1x_2X)}\,. \tag{2.14}$$

The result (2.3) can be easily verified now by computing the spherical images of the basis Hecke operators and substituting them into coefficients $q_i(p)$ (2.4):

$$\begin{aligned}
&\Omega(\mathbf{T}(p)) = x_0\,(1 + x_1)\,(1 + x_2) \\
&\Omega(\mathbf{T}_1(p^2)) = p^{-3}\,x_0^2\,x_1\,x_2\,(p^2 - 1) + p^{-1}\,x_0^2\,(x_1 + x_2)\,(1 + x_1x_2) \\
&\Omega([\mathbf{p}]) = p^{-3}\,x_0^2\,x_1\,x_2\,.
\end{aligned} \tag{2.15}$$

2.2 Explicit solution to Shimura's conjecture for Sp_3 and Sp_4

It is practically impossible to conduct computations on the paper by hands, similarly to the case of genus 2, because the explicit decomposition of the double cosets into the sum of left cosets becomes very large. Andrianov obtained the expression for genus 3 using the multiplication table of Hecke operators in [And67]. This result was recomputed by Miyawaki in [Miy92] in order to find some local factors in Euler product for an L-function associated to some explicit Siegel modular form (see Section 3.1.3). No explicit results for higher genus were known due to an enormous complexity of the Hecke algebra manipulations. Recently the author together with Panchishkin developed a formal calculus approach using a computer. We were able to compute more directly the generating series in Shimura's conjecture for genus 3 (see

[PV07]), and then to explore the case of genus 4. Below is the result for genus 3, where coefficients in p are factorized into irreducible polynomials:

$$\mathbf{D}_p^{(3)}(X) = \frac{\mathbf{E}_3(X)}{\mathbf{F}_3(X)}\,, \tag{2.16}$$

where $\mathbf{E}_3(X), \mathbf{F}_3(X) \in \mathcal{L}_{\mathbb{Z}[X]}$ and

$$\begin{aligned}
&\mathbf{E}_3(X) = \\
&\quad 1 - p^2\left(\mathbf{T}_2(p^2) + (p^2-p+1)(p^2+p+1)[\mathbf{p}]_3\right)X^2 + p^4(p+1)[\mathbf{p}]_3\mathbf{T}(p)X^3 \\
&\quad - p^7[\mathbf{p}]_3\left(\mathbf{T}_2(p^2) + (p^2-p+1)(p^2+p+1)[\mathbf{p}]_3\right)X^4 + p^{15}[\mathbf{p}]_3^3\,X^6\,,
\end{aligned}$$

$$\begin{aligned}
&\mathbf{F}_3(X) = 1 - \mathbf{T}(p)X \\
&\quad + p\left(\mathbf{T}_1(p^2) + (p^2+1)\mathbf{T}_2(p^2) + (p^2+1)^2[\mathbf{p}]_3\right)X^2 \\
&\quad - p^3\left(\mathbf{T}_2(p^2) + [\mathbf{p}]_3\right)\mathbf{T}(p)X^3 \\
&\quad + p^6\big(\mathbf{T}_2(p^2) + [\mathbf{p}]_3(\mathbf{T}(p)^2 - 2p\mathbf{T}_1(p^2) - 2(p-1)\mathbf{T}_2(p^2) \\
&\qquad - (p^2+2p-1)(p^2-p+1)(p^2+p+1)[\mathbf{p}]_3)\big)X^4 \\
&\quad - p^9[\mathbf{p}]_3\left(\mathbf{T}_2(p^2) + [\mathbf{p}]_3\right)\mathbf{T}(p)X^5 \\
&\quad + p^{13}[\mathbf{p}]_3^2\left(\mathbf{T}_1(p^2) + (p^2+1)\mathbf{T}_2(p^2) + (p^2+1)^2[\mathbf{p}]_3\right)X^6 \\
&\quad - p^{18}[\mathbf{p}]^3\mathbf{T}(p)X^7 + p^{24}[\mathbf{p}]^4X^8\,.
\end{aligned}$$

The formal calculus algorithm for a given genus g was developed based on Andrianov's theory of spherical map and the new explicit result for the genus 4 was obtained.

2.2.1 Explicit expression for genus 4

Theorem 2.1 (Explicit Shimura's conjecture for genus 4) *For genus $g = 4$ the summation of Hecke power series $\mathbf{D}_p(X)$ resolves explicitly to the following rational polynomial presentation:*

$$\mathbf{D}_p^{(4)}(X) = \sum_{\delta=0}^{\infty}\mathbf{T}(p^\delta)X^\delta = \frac{\mathbf{E}_4(X)}{\mathbf{F}_4(X)}\,,$$

where $\mathbf{E}_4(X) = \sum_{k=0}^{14}\mathbf{e}_kX^k$ is the polynomial of degree 14 and $\mathbf{F}_4(X) = \sum_{k=0}^{16}\mathbf{f}_kX^k$ is the polynomial of degree 16 with the coefficients $\mathbf{e}_k$ and $\mathbf{f}_k$ listed below:

$$
\begin{aligned}
\mathbf{e}_0 &= 1\,,\\
\mathbf{e}_1 &= 0\,,\\
\mathbf{e}_2 &= -p^2((p^8+p^6+2p^4+2p^2+1)[\mathbf{p}]+(p^2+p+1)(p^2-p+1)\mathbf{T}_3(p^2)\\
&\quad +\mathbf{T}_2(p^2))\,,\\
\mathbf{e}_3 &= p^4(p+1)((p^2+1)(p^3-p^2+1)[\mathbf{p}]+\mathbf{T}_3(p^2))\mathbf{T}(p)\,,\\
\mathbf{e}_4 &= p^7((p^2+p+1)(p^2-p+1)(p^8+3p^7+p^5+2p^3+p-1)[\mathbf{p}]^2\\
&\quad +(p^2+p+1)(p^2-p+1)(2p^3+p-2)\mathbf{T}_3(p^2)[\mathbf{p}]\\
&\quad -(p^2+p+1)(p^2-p+1)\mathbf{T}_3(p^2)^2+(2p^5+2p^3+p^2+p-1)\mathbf{T}_2(p^2)[\mathbf{p}]\\
&\quad -\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)+p(p^2+p+1)\mathbf{T}_1(p^2)[\mathbf{p}]-(p^2+p+1)\mathbf{T}(p)^2[\mathbf{p}])\,,\\
\mathbf{e}_5 &= -p^{10}(p+1)((p^2+1)(p^7-p^6-p^2-1)[\mathbf{p}]-(p^2+1)\mathbf{T}_3(p^2)\\
&\quad -\mathbf{T}_2(p^2))\mathbf{T}(p)[\mathbf{p}]\,,\\
\mathbf{e}_6 &= p^{14}((p^{16}-p^{15}-2p^{14}-3p^{12}-5p^{10}-8p^8+p^7-8p^6-5p^4-4p^2-1)[\mathbf{p}]^3\\
&\quad +(p^{12}-p^{10}-p^9-5p^8+2p^7-7p^6-6p^4-8p^2+p-2)\mathbf{T}_3(p^2)[\mathbf{p}]^2\\
&\quad +(p^7-p^4-4p^2+2p-1)\mathbf{T}_3(p^2)^2[\mathbf{p}]+p\mathbf{T}_3(p^2)^3\\
&\quad -(2p^8+3p^6+p^4-p^3+3p^2+p+1)\mathbf{T}_2(p^2)[\mathbf{p}]^2\\
&\quad -(3p^2+p+1)\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]-(p^6-p^3+1)\mathbf{T}_1(p^2)[\mathbf{p}]^2\\
&\quad -\mathbf{T}_1(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]+p^2(p^3+p-1)\mathbf{T}(p)^2[\mathbf{p}]^2)\,,\\
\mathbf{e}_7 &= -p^{19}(p-1)(p+1)((p^2+p+1)(p^2-p+1)(p^2+1)[\mathbf{p}]\\
&\quad +(p^2+p+1)(p^2-p+1)\mathbf{T}_3(p^2)+\mathbf{T}_2(p^2))\mathbf{T}(p)[\mathbf{p}]^2\,,\\
\mathbf{e}_8 &= -p^{24}((p^{16}-3p^{12}-3p^{10}-p^9-9p^8-8p^6-7p^4-5p^2+p-1)[\mathbf{p}]^3\\
&\quad +(p^{10}-p^9-4p^8-6p^6-8p^4-9p^2+3p-2)\mathbf{T}_3(p^2)[\mathbf{p}]^2\\
&\quad -(p^4+4p^2-3p+1)\mathbf{T}_3(p^2)^2[\mathbf{p}]+p\mathbf{T}_3(p^2)^3\\
&\quad -(p^8+2p^6-p^5+2p^4+p^3+4p^2+1)\mathbf{T}_2(p^2)[\mathbf{p}]^2\\
&\quad -(p^3+3p^2+1)\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]+(p^5-p^2-1)\mathbf{T}_1(p^2)[\mathbf{p}]^2\\
&\quad -\mathbf{T}_1(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]-p(p^3-p^2-1)\mathbf{T}(p)^2[\mathbf{p}]^2)[\mathbf{p}]\,,\\
\mathbf{e}_9 &= p^{29}(p+1)((p^2+1)(p^5-2p^4-1)[\mathbf{p}]-(p^4+1)\mathbf{T}_3(p^2)-\mathbf{T}_2(p^2))\mathbf{T}(p)[\mathbf{p}]^3\,,\\
\mathbf{e}_{10} &= -p^{35}((p^2-p+1)(p^2+p+1)(p^8+2p^7+p^5+3p^3+p-1)[\mathbf{p}]^2\\
&\quad -(p^2-p+1)(p^2+p+1)(p^5-3p^3-p+2)\mathbf{T}_3(p^2)[\mathbf{p}]\\
&\quad -(p^2-p+1)(p^2+p+1)\mathbf{T}_3(p^2)^2+(p^5+3p^3+p^2+p-1)\mathbf{T}_2(p^2)[\mathbf{p}]\\
&\quad -\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)+p(p^2+p+1)\mathbf{T}_1(p^2)[\mathbf{p}]-(p^2+p+1)\mathbf{T}(p)^2[\mathbf{p}])[\mathbf{p}]^3\,,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{e}_{11} &= -p^{41}(p+1)((p^2+1)(p^3-p^2+1)[\mathbf{p}]+\mathbf{T}_3(p^2))\mathbf{T}(p)[\mathbf{p}]^4\,,\\
\mathbf{e}_{12} &= p^{48}((2p^6+2p^4+2p^2+1)[\mathbf{p}]+(p^2-p+1)(p^2+p+1)\mathbf{T}_3(p^2)\\
&\quad +\mathbf{T}_2(p^2))[\mathbf{p}]^5\,,\\
\mathbf{e}_{13} &= 0\,,\\
\mathbf{e}_{14} &= -p^{64}[\mathbf{p}]^7\,,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{f}_0 &= 1\,,\\
\mathbf{f}_1 &= -\mathbf{T}(p)\,,\\
\mathbf{f}_2 &= p((p^8+2p^6+2p^4+2p^2+1)[\mathbf{p}]+(p^4+2p^2+1)\mathbf{T}_3(p^2)\\
&\quad +(p^2+1)\mathbf{T}_2(p^2)+\mathbf{T}_1(p^2))\,,\\
\mathbf{f}_3 &= p^3((p^7-p^6-p^4-p^2-1)[\mathbf{p}]-\mathbf{T}_3(p^2)-\mathbf{T}_2(p^2))\mathbf{T}(p)\,,\\
\mathbf{f}_4 &= -p^6((p^4+1)^2(p^6-p^4+2p^3-2p^2+2p-1)[\mathbf{p}]^2\\
&\quad +2(p^2-p+1)(p^4+1)(p^4+2p^3+p^2+p-1)\mathbf{T}_3(p^2)[\mathbf{p}]\\
&\quad +(p^2-p+1)(p^2+p+1)(p^2+2p-1)\mathbf{T}_3(p^2)^2\\
&\quad -2(p^2-p+1)(p^4+1)\mathbf{T}_2(p^2)[\mathbf{p}]+2(p-1)\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)\\
&\quad -\mathbf{T}_2(p^2)^2+2p(p^4+1)\mathbf{T}_1(p^2)[\mathbf{p}]+2p\mathbf{T}_1(p^2)\mathbf{T}_3(p^2)-\mathbf{T}(p)^2[\mathbf{p}]\\
&\quad -\mathbf{T}(p)^2\mathbf{T}_3(p^2))\,,\\
\mathbf{f}_5 &= p^9((p^{11}+p^{10}+4p^8+2p^7+3p^6+3p^4+2p^2-1)[\mathbf{p}]^2\\
&\quad +(2p^7+2p^6+3p^4+2p^2-2)\mathbf{T}_3(p^2)[\mathbf{p}]-\mathbf{T}_3(p^2)^2+(p^4+3p^2-1)\mathbf{T}_2(p^2)[\mathbf{p}]\\
&\quad -\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)+3p^2\mathbf{T}_1(p^2)[\mathbf{p}]-p\mathbf{T}(p)^2[\mathbf{p}])\mathbf{T}(p)\,,\\
\mathbf{f}_6 &= -p^{13}((p^4+1)(p^2+1)^2(2p^8+2p^7+2p^5+2p^3+2p-1)[\mathbf{p}]^3\\
&\quad +(p^2+1)^2(2p^8+2p^7+4p^5-2p^4+2p^3+4p-3)\mathbf{T}_3(p^2)[\mathbf{p}]^2\\
&\quad -(p^2+1)^2(p^4-2p+3)\mathbf{T}_3(p^2)^2[\mathbf{p}]-(p^2+1)^2\mathbf{T}_3(p^2)^3\\
&\quad +(p^2+1)(2p^8+4p^7+4p^5+4p^3+4p-1)\mathbf{T}_2(p^2)[\mathbf{p}]^2\\
&\quad +2(p^2+1)(p^3+2p-1)\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]-(p^2+1)\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)^2\\
&\quad +2p(p^2+1)\mathbf{T}_2(p^2)^2[\mathbf{p}]+(2p^8+2p^7+2p^5+2p^3+2p-1)\mathbf{T}_1(p^2)[\mathbf{p}]^2\\
&\quad +2(p-1)\mathbf{T}_1(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]-\mathbf{T}_1(p^2)\mathbf{T}_3(p^2)^2+2p\mathbf{T}_1(p^2)\mathbf{T}_2(p^2)[\mathbf{p}]\\
&\quad -(p^2+1)(p^5+p^4-p^3+1)\mathbf{T}(p)^2[\mathbf{p}]^2+(p-1)(p^2+p+1)\mathbf{T}(p)^2\mathbf{T}_3(p^2)[\mathbf{p}]\\
&\quad -\mathbf{T}(p)^2\mathbf{T}_2(p^2)[\mathbf{p}])\,,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{f}_7 = &-p^{17}((2p^{13}+p^{12}+3p^{10}+p^9+p^8+2p^6-p^5+p^4-p^2+p+1)[\mathbf{p}]^3\\
&+(p^9+2p^6-2p^5+2p^4-2p^2+3p+2)\mathbf{T}_3(p^2)[\mathbf{p}]^2\\
&-(p^5-p^4+p^2-3p-1)\mathbf{T}_3(p^2)^2[\mathbf{p}]+p\mathbf{T}_3(p^2)^3\\
&+(p^6+2p^4-2p^2+1)\mathbf{T}_2(p^2)[\mathbf{p}]^2-(2p^2-1)\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]\\
&+(2p^4+1)\mathbf{T}_1(p^2)[\mathbf{p}]^2+\mathbf{T}_1(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]-p^3\mathbf{T}(p)^2[\mathbf{p}]^2)\mathbf{T}(p)\,,\\
\mathbf{f}_8 = &\,p^{22}((p^{18}+4p^{17}+3p^{16}+8p^{15}+12p^{14}+8p^{13}+14p^{12}+12p^{11}+20p^{10}\\
&\quad+4p^9+20p^8+16p^6+10p^4-4p^3+5p^2+1)[\mathbf{p}]^4\\
&+2(2p^{10}+2p^9+p^8+6p^7+4p^6+8p^4-6p^3+6p^2+1)(p^4+1)\mathbf{T}_3(p^2)[\mathbf{p}]^3\\
&+(p^8+4p^6+8p^4-12p^3+10p^2+1)\mathbf{T}_3(p^2)^2[\mathbf{p}]^2\\
&-4p^2(p-1)\mathbf{T}_3(p^2)^3[\mathbf{p}]+p^2\mathbf{T}_3(p^2)^4\\
&+2(2p^7+3p^6+2p^5+5p^4-2p^3+3p^2+1)(p^4+1)\mathbf{T}_2(p^2)[\mathbf{p}]^3\\
&+(2p^6+4p^5+10p^4-8p^3+6p^2+2)\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]^2\\
&-4p^3\mathbf{T}_2(p^2)\mathbf{T}_3(p^2)^2[\mathbf{p}]+(3p^4+2p^2+1)\mathbf{T}_2(p^2)^2[\mathbf{p}]^2\\
&+2(2p^5+p^4+2p^2+1)(p^4+1)\mathbf{T}_1(p^2)[\mathbf{p}]^3\\
&+(4p^5+2p^4+4p^2+2)\mathbf{T}_1(p^2)\mathbf{T}_3(p^2)[\mathbf{p}]^2+2(p^2+1)\mathbf{T}_1(p^2)\mathbf{T}_2(p^2)[\mathbf{p}]^2\\
&+\mathbf{T}_1(p^2)^2[\mathbf{p}]^2-(p^8+2p^7+2p^5+2p^4+2p^3+2p-1)\mathbf{T}(p)^2[\mathbf{p}]^3\\
&-2(p^4+p-1)\mathbf{T}(p)^2\mathbf{T}_3(p^2)[\mathbf{p}]^2+\mathbf{T}(p)^2\mathbf{T}_3(p^2)^2[\mathbf{p}]-2p\mathbf{T}(p)^2\mathbf{T}_2(p^2)[\mathbf{p}]^2)
\end{aligned}
$$

and the higher degree coefficients $\mathbf{f}_i$ *are obtained from the following relations:*

$$
\begin{aligned}
&\mathbf{f}_9=\mathbf{f}_7\cdot p^{10}[\mathbf{p}],\quad \mathbf{f}_{10}=\mathbf{f}_6\cdot p^{20}[\mathbf{p}]^2,\quad \mathbf{f}_{11}=\mathbf{f}_5\cdot p^{30}[\mathbf{p}]^3,\quad \mathbf{f}_{12}=\mathbf{f}_4\cdot p^{40}[\mathbf{p}]^4,\\
&\mathbf{f}_{13}=\mathbf{f}_3\cdot p^{50}[\mathbf{p}]^5,\quad \mathbf{f}_{14}=\mathbf{f}_2\cdot p^{60}[\mathbf{p}]^6,\quad \mathbf{f}_{15}=\mathbf{f}_1\cdot p^{70}[\mathbf{p}]^7,\quad \mathbf{f}_{16}=\mathbf{f}_0\cdot p^{80}[\mathbf{p}]^8.
\end{aligned}
$$

This expression was obtained in two steps. First, the spherical image of the generating series (2.1) was computed as well as the images of all basis Hecke operators. Then, at the second step, the inverted spherical image was found using the method of undetermined coefficients.

2.2.2 Practical implementation

The algorithm was programmed and the results were computed using the Maple system. We found more practical and suitable for direct programming the formulae for spherical mapping in the article [And70]. Notice that the notation Ω in that article indicates the spherical mapping of the Hecke algebra for general linear group. It corresponds to our mapping ω defined above with substitution of all x_i by x_i/p for $i=1,\dots,n$. Therefore we used the

formula (1.7) on page 432 of [And70] and then performed the substitution. This formula gives a direct expression for images of elements t of type (2.8) including images of $\pi_{\alpha\beta}(p)$ (1.19). In our notation it can be written as

$$\omega(t(p^{(\delta)}) = p^{-\sum_i (n-i)\delta_i} \frac{Q(x)}{P^{(k)}(p^{-1})}\,, \tag{2.17}$$

where

$$\begin{aligned} Q(x) &= \sum_{w\in \mathrm{S}_n} (wx)^{(\delta)} c\,(wx)\,, \\ c\,(x) &= \prod_{\alpha\in\Sigma} \frac{1-p^{-1}(x)^{(\alpha)}}{1-(x)^{(\alpha)}}\,, \\ P^{(k)}(v) &= \frac{\varphi_{k_1}(v)\dots\varphi_{k_t}(v)}{\varphi_1(v)^n}\,, \end{aligned}$$

the function $\varphi_r(v)$ was defined in (1.21), the notation (x) is used for the n-tuple $(x_1, x_2, \dots, x_n)$, then $(x)^{(\alpha)} \equiv x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, and the action of a permutation ω is $(wx)^{(\delta)} \equiv x_{w(1)}^{\delta_1} x_{w(2)}^{\delta_2} \cdots x_{w(n)}^{\delta_n}$. The set $\Sigma = \{(\alpha)\} = \{(\alpha_1, \alpha_2, \dots, \alpha_n)\} = \{\alpha_{ij}, 1 \leqslant i < j \leqslant n\}$, where α_{ij} is defined with putting of 1 and -1 within the set of n zeros $\alpha_{ij} \equiv (\dots, 0, 1_i, 0, \dots, 0, -1_j, 0, \dots) \in \mathbb{Z}^n$:

$$\alpha_{ij} = (\overset{1}{0}, \dots, \overset{i-1}{0}, \overset{i}{1}, \overset{i+1}{0}, \dots, \overset{j-1}{0}, \overset{j}{-1}, \overset{j+1}{0}, \dots, \overset{n}{0})\,.$$

The element of Hecke algebra for the general linear group is denoted by $t(p^{(\delta)})$ is $t(p^{\delta_1}, \dots, p^{\delta_n})$. Numbers $(k) \equiv (k_1, \dots, k_t)$ denote the quantities of t distinct elements in the set of integers $(\delta) = (\delta_1, \dots, \delta_n)$, that is, the number δ_1 occurs in (δ) exactly k_1 times, the next number following δ_1 in the ordering of (δ) and distinct from δ_1 appears there k_2 times, etc. Note, that all $k_i > 0$ and $k_1 + \dots + k_t = n$.

Let $n = 4$. In this case, the set Σ consists of 6 elements:

$$\Sigma = \{(1,-1,0,0), (1,0,-1,0), (1,0,0,-1), \tag{2.18}$$
$$(0,1,-1,0), (0,1,0,-1), (0,0,1,-1)\}\,. \tag{2.19}$$

Then the expression for $c(x)$ takes the following explicit form

$$c(x) = \frac{(px_2-x_1)(px_3-x_1)(px_4-x_1)(px_3-x_2)(px_4-x_2)(px_4-x_3)}{p^6(x_2-x_1)(x_3-x_1)(x_4-x_1)(x_3-x_2)(x_4-x_2)(x_4-x_3)}\,. \tag{2.20}$$

Recall the formula (1.31) for the spherical images of base Hecke operators. The elements $\pi_{a,b}(p)$ correspond to $t(p^\delta)$ with values δ_i from 0 to 2. More precisely,

$$\{(\delta)\} = \{(0,0,0,1),(0,0,1,1),(0,0,1,2),(0,1,1,1),(0,1,1,2),\\ (0,1,2,2),(1,1,1,1),(1,1,1,2),(1,1,2,2),(1,2,2,2)\}.$$

Further, we shall see that in order to compute the series (2.7) we need an expanded set $\{(\delta)\}$ with components $\delta_i \leqslant 14$. Fortunately, we can drastically reduce the amount of different $t(p^\delta)$ elements by normalizing double classes by the common multiplier p^{δ_1} and placing it outside of the matrix. Therefore, we need to compute 680 primitive elements of the form $t(1, p^{\delta_2}, p^{\delta_3}, p^{\delta_4})$ eliminating the variable δ_1, where $0 \leqslant \delta_2 \leqslant \delta_3 \leqslant \delta_4 \leqslant 14$. Note, that in the case $n = 3$ it is necessary to compute just 28 images $\omega(t(1, p^{\delta_2}, p^{\delta_3}))$.

Below are some examples of the values of these images:

$$\begin{aligned}
&\omega(t(1,1,1,1)) = 1\,,\\
&\omega(t(1,1,1,p)) = p^{-1}(x_1+x_2+x_3+x_4)\,,\\
&\omega(t(1,1,p,p)) = p^{-3}(x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4)\,,\\
&\omega(t(1,p,p,p)) = p^{-3}(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)\,,\\
&\omega(t(1,p,p,p^3)) = p^{-9}(px_1^3x_2x_3+px_1^3x_2x_4+px_1^3x_3x_4-x_1^2x_2^2x_3+px_1^2x_2^2x_3\\
&\quad -x_1^2x_2^2x_4+px_1^2x_2^2x_4+px_1^2x_2x_3^2-x_1^2x_2x_3^2-3x_1^2x_2x_3x_4+3px_1^2x_2x_3x_4\\
&\quad +px_1^2x_2x_4^2-x_1^2x_2x_4^2-x_1^2x_3^2x_4+px_1^2x_3^2x_4+px_1^2x_3x_4^2-x_1^2x_3x_4^2\\
&\quad +px_1x_2^3x_3+px_1x_2^3x_4-x_1x_2^2x_3^2+px_1x_2^2x_3^2+3px_1x_2^2x_3x_4-3x_1x_2^2x_3x_4\\
&\quad +px_1x_2^2x_4^2-x_1x_2^2x_4^2+px_1x_2x_3^3-3x_1x_2x_3^2x_4+3px_1x_2x_3^2x_4+3px_1x_2x_3x_4^2\\
&\quad -3x_1x_2x_3x_4^2+px_1x_2x_4^3+px_1x_3^3x_4+px_1x_3^2x_4^2-x_1x_3^2x_4^2+px_1x_3x_4^3\\
&\quad +px_2^3x_3x_4+px_2^2x_3^2x_4-x_2^2x_3^2x_4-x_2^2x_3x_4^2+px_2^2x_3x_4^2+px_2x_3^3x_4\\
&\quad +px_2x_3^2x_4^2-x_2x_3^2x_4^2+px_2x_3x_4^3)\,.
\end{aligned}$$

These expressions are symmetrical polynomials as expected. The written form becomes very long when the degree of p increases. In order to present intermediate results preserving the structure of these polynomials we use the monomial symmetrical polynomial of four variables $m_{i_1i_2i_3i_4}$ (see the Section 1.3.4), namely

$$m_{i_1i_2i_3i_4} = \sum_{w\in S_4/\,\mathrm{Stab}(x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4})} w(x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4})\,,$$

where the sum is normalized by $\mathrm{Stab}(x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4})$ so the resulting coefficient

is equal to 1 and $i_1 \geqslant i_2 \geqslant i_3 \geqslant i_4 \geqslant 0$. For example,

$$\begin{aligned}
m_{1000} &= x_1 + x_2 + x_3 + x_4\,,\\
m_{1100} &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4\,,\\
m_{2110} &= x_1^2x_2x_3 + x_1^2x_2x_4 + x_1^2x_3x_4 + x_1x_2^2x_3 + x_1x_2^2x_4 + x_1x_2x_3^2\\
&\quad + x_1x_2x_4^2 + x_1x_3^2x_4 + x_1x_3x_4^2 + x_2^2x_3x_4 + x_2x_3^2x_4 + x_2x_3x_4^2\,,\\
m_{3333} &= x_1^3x_2^3x_3^3x_4^3\,.
\end{aligned}$$

Using this notation the previously listed examples of $\omega(\cdot)$ images become the short expressions:

$$\begin{aligned}
&\omega(t(1,1,1,1)) = 1 = m_{0000}\,,\\
&\omega(t(1,1,1,p)) = p^{-1}m_{1000}\,,\\
&\omega(t(1,1,p,p)) = p^{-3}m_{1100}\,,\\
&\omega(t(1,p,p,p)) = p^{-3}m_{1110}\,,\\
&\omega(t(1,p,p,p^3)) = p^{-9}(p\,m_{3110} + (p-1)m_{2210} + 3(p-1)\,m_{2111})\,.
\end{aligned}$$

Finally, using formulae (1.31) and (2.17) we obtain the images of basis Hecke operators for the symplectic group (1.14), which we present here in terms of $m_{i_1i_2i_3i_4}$:

$$\Omega(\mathbf{T}(p)) = x_0\,(m_{1111} + m_{1110} + m_{1100} + m_{1000} + 1)\,,$$

$$\begin{aligned}
\Omega(\mathbf{T}_1(p^2)) &= x_0^2p^{-8}((p-1)^2(p+1)(4p^4+3p^3+3p^2+p+1)\,m_{1111}\\
&\quad + p^4(p-1)(3p^2+2p+1)(m_{2111}+m_{1110})\\
&\quad + p^5(p-1)(p+1)(m_{2211}+m_{2110}+m_{1100})\\
&\quad + p^7(m_{2221}+m_{2210}+m_{2100}+m_{1000}))\,,
\end{aligned}$$

$$\begin{aligned}
\Omega(\mathbf{T}_2(p^2)) &= x_0^2p^{-8}((p-1)(4p^4+3p^3+3p^2+p+1)\,m_{1111}\\
&\quad + p^2(p-1)(p^2+p+1)(m_{2111}+m_{1110})\\
&\quad + p^5(m_{2211}+m_{2110}+m_{1100}))\,,
\end{aligned} \tag{2.21}$$

$$\begin{aligned}
\Omega(\mathbf{T}_3(p^2)) &= x_0^2p^{-10}((p-1)(p+1)(p^2+1)\,m_{1111}\\
&\quad + p^4(m_{2111}+m_{1110}))\,,
\end{aligned}$$

$$\Omega([\mathbf{p}]) = x_0^2p^{-10}\,m_{1111}\,.$$

2.2.3 Spherical image of Hecke power series

Similarly to manipulations with the series in the Section 2.1 we introduce the following substitutions:

$$\begin{aligned} \delta_2 &= \delta_1 + \delta_2' \,, \\ \delta_3 &= \delta_1 + \delta_3' \,, \\ \delta_4 &= \delta_1 + \delta_4' \,, \\ \delta &= \delta_1 + \delta_4' + \beta \,, \end{aligned} \tag{2.22}$$

where $0 \leqslant \delta_2' \leqslant \delta_3' \leqslant \delta_4' \leqslant \delta'$ and $\beta \geqslant 0$. Continuing the formula (2.7) with the use of the above substitutions we obtain for $n = 4$

$$\begin{aligned} \Omega(\mathbf{D}_p(X)) &= \sum_{\delta=0}^{\infty} \Omega(\mathbf{T}(p^\delta)) X^\delta \\ &= \sum_{\delta=0}^{\infty} \sum_{0 \leqslant \delta_1 \leqslant \delta_2 \leqslant \delta_3 \leqslant \delta_4 \leqslant \delta} p^{4\delta_1 + 3\delta_2 + 2\delta_3 + \delta_4} \, \omega(t(p^{\delta_1}, p^{\delta_2}, p^{\delta_3}, p^{\delta_4})) \, (x_0 X)^\delta \\ &= \sum_{\substack{\delta_1 \geqslant 0, \, \beta \geqslant 0 \\ 0 \leqslant \delta_2' \leqslant \delta_3' \leqslant \delta_4'}} (x_0 X)^{\delta_1 + \beta + \delta_4'} p^{10\delta_1 + 3\delta_2' + 2\delta_3' + \delta_4'} \left(\frac{x_1 x_2 x_3 x_4}{p^{10}} \right)^{\delta_1} \omega(t(1, p^{\delta_2'}, p^{\delta_3'}, p^{\delta_4'})) \\ &= \sum_{\substack{\delta_1 \geqslant 0, \, \beta \geqslant 0 \\ 0 \leqslant \delta_2' \leqslant \delta_3' \leqslant \delta_4'}} (x_0 x_1 x_2 x_3 x_4 X)^{\delta_1} (x_0 X)^\beta \omega(t(1, p^{\delta_2'}, p^{\delta_3'}, p^{\delta_4'})) p^{3\delta_2' + 2\delta_3' + \delta_4'} (x_0 X)^{\delta_4'} \,. \end{aligned} \tag{2.23}$$

In the last formula we can separate the terms containing δ_1 and β variables and perform an independent summation. These two series result in

$$\sum_{\delta_1 \geqslant 0} (x_0 x_1 x_2 x_3 x_4 X)^{\delta_1} = \frac{1}{1 - x_0 x_1 x_2 x_3 x_4 X} \tag{2.24}$$

and

$$\sum_{\beta \geqslant 0} (x_0 X)^\beta = \frac{1}{1 - x_0 X} \,. \tag{2.25}$$

In the rational representation of series $\mathbf{D}_p(X) = \mathbf{E}(X)/\mathbf{F}(X)$ the degree of the numerator $\mathbf{E}_4(X)$ for $n = 4$ is equal to 14. Moreover, the spherical image of the denominator $\mathbf{F}_4(X)$ is explicitly known

$$\begin{aligned} \Omega(\mathbf{F}_4(X)) = {} & (1 - x_0 X) \, (1 - x_0 x_1 X) \, (1 - x_0 x_2 X) \, (1 - x_0 x_3 X) \\ & \times (1 - x_0 x_4 X) \, (1 - x_0 x_1 x_2 X) \, (1 - x_0 x_1 x_3 X) \\ & \times (1 - x_0 x_1 x_4 X) \, (1 - x_0 x_2 x_3 X) \, (1 - x_0 x_2 x_4 X) \\ & \times (1 - x_0 x_3 x_4 X) \, (1 - x_0 x_1 x_2 x_3 X) \, (1 - x_0 x_1 x_2 x_4 X) \\ & \times (1 - x_0 x_1 x_3 x_4 X) \, (1 - x_0 x_2 x_3 x_4 X) \, (1 - x_0 x_1 x_2 x_3 x_4 X) \,. \end{aligned} \tag{2.26}$$

Therefore we obtain

$$\begin{aligned}\Omega(\mathbf{E}_4(X)) = &\left(\sum_{0\leqslant\delta_2'\leqslant\delta_3'\leqslant\delta_4'} \omega(t(1,p^{\delta_2'},p^{\delta_3'},p^{\delta_4'}))p^{3\delta_2'+2\delta_3'+\delta_4'}(x_0X)^{\delta_4'}\right)\\ &\times(1-x_0x_1X)\,(1-x_0x_2X)\,(1-x_0x_3X)\,(1-x_0x_4X)\\ &\times(1-x_0x_1x_2X)\,(1-x_0x_1x_3X)\,(1-x_0x_1x_4X)\,(1-x_0x_2x_3X)\\ &\times(1-x_0x_2x_4X)\,(1-x_0x_3x_4X)\,(1-x_0x_1x_2x_3X)\\ &\times(1-x_0x_1x_2x_4X)(1-x_0x_1x_3x_4X)(1-x_0x_2x_3x_4X)\,.\end{aligned} \tag{2.27}$$

In order to obtain an explicit expression for the image of the numerator $\mathbf{E}_4(X)$ we compute all $\left(\omega(t(1,p^{\delta_2'},p^{\delta_3'},p^{\delta_4'}))p^{3\delta_2'+2\delta_3'+\delta_4'}(x_0X)^{\delta_4'}\right)$ up to $\delta_4' \leqslant 14$, add them together and perform the multiplication of terms in (2.27) considering only resulting powers of X up to 14. These expressions are very long, it took days and hours of processor time to compute all sums and products. Intermediate results fill hundreds of pages of paper. However, the final result is quite short (see Appendix A and [Van07]), showing some interesting properties of this polynomial (e.g. a functional equation). Namely, we noticed a very interesting symmetry property of the coefficients K_k. Knowing this relation in advance, one can limit computation of coefficients just up to degree 7, skipping the most time consuming higher degree coefficients.

THEOREM 2.2 (FUNCTIONAL EQUATION FOR COEFFICIENTS OF $\Omega(\mathbf{E}_4(X))$)
Polynomial $\Omega(\mathbf{E}_4(X))$ has the following functional relation between its coefficients K_k, $k = 0,\dots,14$:

$$\begin{aligned}&K_{14-k}(p,x_0,x_1,x_2,x_3,x_4) =\\ &\quad = -p^{-6}(x_0^2x_1x_2x_3x_4)^{7-k}\,K_k\left(\frac{1}{p},x_0x_1x_2x_3x_4,\frac{1}{x_1},\frac{1}{x_2},\frac{1}{x_3},\frac{1}{x_4}\right)\end{aligned}$$

CONJECTURE 2.3 (FUNCTIONAL EQUATION FOR $\Omega(\mathbf{E}_n(X))$)
Let $\Omega(\mathbf{E}_n(X)) = E(x_0,x_1,\dots,x_n,X)$. It is suggested that this functional relation is true for all n in the following form:

$$E(x_0,x_1,\dots,x_n,X) = (-1)^{n-1}\frac{(x_0^2x_1\cdots x_nX^2)^{2^{n-1}-1}}{p^{n(n-1)/2}}\,E\left(\frac{1}{x_0},\dots,\frac{1}{x_n},\frac{p}{X}\right).$$

REMARK 2.4 *The obtained result for genus $n = 4$ is in a full agreement with the result of the earlier work [PV07] for $n = 3$ after applying the projection $x_4 = 0$ (corresponding to Siegel operator acting from Sp_4 to Sp_3).*

2.2.4 Inverting the spherical image

In order to obtain the result of the theorem 2.1 we apply the method of undetermined coefficients to each coefficient of $\Omega(\mathbf{E}_4(X))$ and $\Omega(\mathbf{F}_4(X))$. Let us take, as a reference, the variable x_0. In expressions for $\Omega(\mathbf{E}_4(X))$ and $\Omega(\mathbf{F}_4(X))$ this variable has the same degree as X for each summand. The expression for $\Omega(\mathbf{T}(p))$ (see (2.21)) includes the variable x_0 of degree 1, other images of basis Hecke operators $\Omega(\mathbf{T}_i(p))$ include x_0 of degree 2. Therefore, to reconstruct the particularly given coefficient of degree k of the polynomial $\mathbf{E}_4(X)$ or $\mathbf{F}_4(X)$ we need to construct all possible products of $\mathbf{T}(p)$, $\mathbf{T}_1(p^2)$, $\mathbf{T}_2(p^2)$, $\mathbf{T}_3(p^2)$ and $\mathbf{T}(p)$, so that the resulting degree of x_0 in the spherical image will be equal to k. For example, consider the coefficient of degree 3 in polynomial $\mathbf{E}_4(X)$. Its image was computed in [Van07]:

$$\begin{aligned}\Omega(\mathbf{e}_3) = x_0^3 p^{-3}(p+1)\big(p\,(&m_{3222} + m_{3221} + m_{3211} \\ &+ m_{3111} + m_{2220} + m_{2210} + m_{2110} + m_{1110}) \\ &+ (p^2+4p+1)(m_{2222} + m_{2221} + m_{2211} + m_{2111} + m_{1111})\big)\,.\end{aligned}$$

All possible products of generators of the Hecke ring with x_0 of degree 3 under the spherical mapping are: $\mathbf{T}(p)\mathbf{T}_1(p^2)$, $\mathbf{T}(p)\mathbf{T}_2(p^2)$, $\mathbf{T}(p)\mathbf{T}_3(p^2)$ and $[\mathbf{p}]\mathbf{T}(p)$. Then

$$\begin{aligned}\Omega(\mathbf{e}_3) = K_1\Omega(\mathbf{T}(p))\Omega(\mathbf{T}_1(p^2)) + K_2\Omega(\mathbf{T}(p))\Omega(\mathbf{T}_2(p^2)) \\ + K_3\Omega(\mathbf{T}(p))\Omega(\mathbf{T}_3(p^2)) + K_4\Omega(\mathbf{T}(p))\Omega([\mathbf{p}])\,.\end{aligned}$$

Expanding these products we can construct a linear system of K_j variables by comparing the coefficients of appropriate monomial symmetric functions (or $x_i x_j \cdots$ monomials). This system resolves uniquely due to the fact that the spherical mapping constructed on basis Hecke operators is an isomorphism. In the above example we find that $K_1 = 0$, $K_2 = 0$, $K_3 = p^4(p+1)$ and $K_4 = p^4(p+1)(p^2+1)(p^3-p^2+1)$. In practice, for higher degree there exist many choices of products of generators and the expansion of them becomes not a trivial task. In the most complicated case, it took almost 80 hours of the processor time to construct and resolve the linear system for the coefficient of degree 8 of the denominator. Fortunately, there is a functional equation for coefficients of the denominator $\mathbf{F}_4(X)$ due to the symmetric structure of the spherical image polynomial:

$$\mathbf{f}_i = \mathbf{f}_{16-i} \cdot (p^{10}[\mathbf{p}])^{i-8}\,, \quad i = 0, \ldots, 16\,.$$

Therefore, we used the approach of undetermined coefficient for only lower degree $\mathbf{f}_i$, where $i = 0, \ldots, 8$. The same computational problem exists for

the higher degree coefficient of the numerator. To avoid the unnecessary manipulations and blind guessing of the $\mathbf{T}$–product combination we take advantage of the fact that it is possible to lower the degree of the equation for the particular coefficient $\mathbf{e}_i$ for $i > 7$ by dividing this equation by the factor $\Omega([\mathbf{p}]) = x_0^2 p^{-10} x_1 x_2 x_3 x_4$ in appropriate degree and using the same products (with non zero coefficients) of $\mathbf{T}(p)^{i_1}\mathbf{T}(p)^{i_2}\mathbf{T}(p)^{i_3}\mathbf{T}(p)^{i_4}\mathbf{T}(p)^{i_5}$ as in already computed $\mathbf{e}_{14-i}$.

This final step complets the computation.

2.2.5 Remarks

Remark 2.5 *The result of the Theorem 2.1 is fully compatible with the result of the earlier work [PV07], where the same method was applied for the case of genus $g = 3$. Considering the projection from genus $g = 4$ to $g = 3$ corresponding to Siegel operator acting from Sp_4 to Sp_3 in Hecke algebra by taking $[\mathbf{p}]_4$ to zero, $\mathbf{T}^{(4)}(p)$ to $\mathbf{T}^{(3)}(p)$, and $\mathbf{T}_i^{(4)}(p^2)$ to $\mathbf{T}_i^{(3)}(p^2)$ for $i = 1, 2, 3$, we obtain the exact formula of generating power series (2.16). All formulae (1.14) for the images of basis Hecke operators transform to the exact formulae for lower genus as well. The spherical image $\Omega(\mathbf{D}_p^{(4)})$ under a projection $x_4 = 0$ transforms into $\Omega(\mathbf{D}_p^{(3)})$. This genus lowering procedure is valid for $g = 2$ and $g = 1$ as well.*

For the special choice of the Satake parameters x_i, the spherical image of the numerator $\mathbf{E}(X)$ can be considerably simplified.

Proposition 2.6 (Special case of Theorem 2.1)
Let genus $n = 4$. Consider "the degree" homomorphism ν corresponding the Satake parameters $(x_0, x_1, x_2, x_3, x_4) = (1, p, p^2, p^3, p^4)$. Then the polynomial $\Omega(\mathbf{E}_4)$ takes the form

$$\begin{aligned}\Omega|_\nu(\mathbf{E}_4(X)) &= (1 - pX)\,(1 - p^2X)\,(1 - p^3X)^2\,(1 - p^4X)\\ &\times (1 + p^5X)\,(1 - p^5X)^2\,(1 - p^6X)^2\,(1 - p^7X)\,(1 - p^8X)\\ &\times (1 + pX + p^2X + 2p^3X + p^4X + p^5X + 2p^6X + p^7X + p^8X + p^9X^2)\,.\end{aligned}$$

Proposition 2.7 ([PV07], Section 5) *In the case of genus $n = 3$, the similar to the Proposition 2.6 statement holds. Namely, consider the homomorphism ν corresponding the Satake parameters $(x_0, x_1, x_2, x_3) = (1, p, p^2, p^3)$. Then the polynomial $\Omega(\mathbf{E}_3)$ takes the form*

$$\begin{aligned}\Omega|_\nu(\mathbf{E}_3(X)) &= (1 - pX)\,(1 - p^2X)\,(1 - p^3X)\,(1 - p^4X)\\ &\times (1 + pX + p^2X + p^3X + p^4X + p^5X^2)\,.\end{aligned}$$

2.3 Rankin's Lemma for higher genus and tensor products

2.3.1 Statement of the result

The theory of spherical mapping allows one to compute explicitly some other series in the Hecke algebra. In particular, we formulate and prove the analog of Rankin's lemma (see Remark 2.12 on page 73 and Lemma 3.8 on page 86) in genus two for generating series with coefficients in a tensor product of local Hecke algebras.

THEOREM 2.8 (RANKIN'S LEMMA FOR GENUS 2) *For genus $n = 2$ the following equality holds:*

$$\sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) \otimes \mathbf{T}(p^\delta)\, X^\delta = \frac{(1 - p^6[\mathbf{p}] \otimes [\mathbf{p}]X^2)\, \mathbf{R}(X)}{\mathbf{S}(X)}\,, \tag{2.28}$$

where $\mathbf{R}(X) = 1 + \mathbf{r}_1 X + \cdots + \mathbf{r}_{12}X^{12}$ is the polynomial of degree 12 and $\mathbf{S}(X) = 1 + \mathbf{s}_1 X + \cdots + \mathbf{s}_{16}X^{16}$ is the polynomial of degree 16 with the coefficients $\mathbf{r}_k$ (note, that $\mathbf{r}_1 = \mathbf{r}_{11} = 0$) and $\mathbf{s}_k \in \mathcal{L}_{2,\mathbb{Z}} \otimes \mathcal{L}_{2,\mathbb{Z}}$ presented below:

$$\begin{aligned}
\mathbf{r}_1 &= 0\,,\\
\mathbf{r}_2 &= p^2\,((2p-1)(p^2+1)\,[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad - (p^2-p+1)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}] + [\mathbf{p}]\otimes\mathbf{T}_1(p^2))\\
&\quad - (\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2) + \mathbf{T}(p)^2\otimes[\mathbf{p}] + [\mathbf{p}]\otimes\mathbf{T}(p)^2)\,,\\
\mathbf{r}_3 &= p^3\,(p+1)\,(2\,[\mathbf{p}]\otimes[\mathbf{p}] + \mathbf{T}_1(p^2)\otimes[\mathbf{p}] + [\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}(p)\otimes\mathbf{T}(p)\,,\\
\mathbf{r}_4 &= -p^5\,((p^7+2p^6-2p^5+6p^4+p^3+6p^2+p+2)[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&\quad - (p^2+1)(p^3-3p^2-p-3)(\mathbf{T}_1(p^2)\otimes[\mathbf{p}] + [\mathbf{p}]\otimes\mathbf{T}_1(p^2))[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad + (p+4)(p^2+1)\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}_1(p^2)[\mathbf{p}]\\
&\quad - (p^3-p^2-1)(\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2 + [\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)\\
&\quad + (\mathbf{T}_1(p^2)\otimes[\mathbf{p}] + [\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2)\\
&\quad - p(p^3+2p^2-p+2)(\mathbf{T}(p)^2\otimes[\mathbf{p}] + [\mathbf{p}]\otimes\mathbf{T}(p)^2)[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad - 2p(\mathbf{T}(p)^2\otimes\mathbf{T}_1(p^2) + \mathbf{T}_1(p^2)\otimes\mathbf{T}(p)^2)[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad + p^2(\mathbf{T}(p)^2\mathbf{T}_1(p^2)\otimes[\mathbf{p}]^2 + [\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2))\\
&\quad + (p+2)\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}(p)^2[\mathbf{p}])\,,
\end{aligned}$$

$$
\begin{aligned}
\mathbf{r}_5 &= -p^7\,(2(p+1)(2p^4-p^3+p^2-1)[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad+(p+1)(p-2)(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\\
&\quad-2\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2)\\
&\quad-p(p+1)(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2))\mathbf{T}(p)[\mathbf{p}]\otimes\mathbf{T}(p)[\mathbf{p}]\,,\\
\mathbf{r}_6 &= -p^{10}\,(p\,(p^2+1)(p^5-2p^3-8p^2-p-4)[\mathbf{p}]^3\otimes[\mathbf{p}]^3\\
&\quad-p\,(p^5+4p^4+2p^3+12p^2+p+6)(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&\quad+p\,(p-4)(p^2+1)\mathbf{T}_1(p^2)[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)[\mathbf{p}]^2\\
&\quad-p\,(p+4)(p^2+1)(\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad-p\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}_1(p^2)[\mathbf{p}]\\
&\quad-p\,(\mathbf{T}_1(p^2)^3\otimes[\mathbf{p}]^3+[\mathbf{p}]^3\otimes\mathbf{T}_1(p^2)^3)\\
&\quad-(p^5-4p^2-p-2)(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&\quad+(p^2+3)(\mathbf{T}(p)^2\otimes\mathbf{T}_1(p^2)+\mathbf{T}_1(p^2)\otimes\mathbf{T}(p)^2)[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&\quad+(\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}_1(p^2)^2+\mathbf{T}_1(p^2)^2\otimes\mathbf{T}(p)^2[\mathbf{p}])[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad+(p^3+3p^2+p+1)(\mathbf{T}(p)^2\mathbf{T}_1(p^2)\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2))[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad+(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}_1(p^2)[\mathbf{p}]\\
&\quad+(p^2+1)\mathbf{T}(p)^2[\mathbf{p}]^2\otimes\mathbf{T}(p)^2[\mathbf{p}]^2)\,,\\
\mathbf{r}_7 &= -p^{13}\,(2(p+1)(p^3+p-1)[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad-(p+1)(p^2-2p+2)(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\\
&\quad-2\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2)\\
&\quad-(p+1)(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2))\mathbf{T}(p)[\mathbf{p}]^2\otimes\mathbf{T}(p)[\mathbf{p}]^2\,,\\
\mathbf{r}_8 &= -p^{16}\,(p\,(2p^6+3p^5+6p^4-p^3+6p^2-p+2)[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&\quad+p\,(p^2+1)(p^3+3p^2-p+3)(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad+p\,(p+4)(p^2+1)\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}_1(p^2)[\mathbf{p}]\\
&\quad+p\,(p^2-p+1)(\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)\\
&\quad+p\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2)\\
&\quad-p\,(2p^3+p^2+2p-1)(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad-2p^2(\mathbf{T}(p)^2\otimes\mathbf{T}_1(p^2)+\mathbf{T}_1(p^2)\otimes\mathbf{T}(p)^2)[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad+p\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2)\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2))\\
&\quad+(2p+1)\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}(p)^2[\mathbf{p}])[\mathbf{p}]^2\otimes[\mathbf{p}]^2\,,\\
\mathbf{r}_9 &= p^{20}\,(p+1)\,(2\,[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad+\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}(p)[\mathbf{p}]^3\otimes\mathbf{T}(p)[\mathbf{p}]^3\\
\mathbf{r}_{10} &= p^{24}\,((p^2+1)(p^4+2p^3-p^2-1)\,[\mathbf{p}]\otimes[\mathbf{p}]\\
&\quad+(p^3-p^2-1)(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))-\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2)\\
&\quad-p^2\,(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2))\,[\mathbf{p}]^4\otimes[\mathbf{p}]^4\,,
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{r}_{11} = 0\,,\\
&\mathbf{r}_{12} = p^{34}\,[\mathbf{p}]^6 \otimes [\mathbf{p}]^6\,.
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{s}_1 &= -\,\mathbf{T}(p) \otimes \mathbf{T}(p)\,,\\
\mathbf{s}_2 &= -p\,(2\,p\,(p^2+1)^2\,[\mathbf{p}] \otimes [\mathbf{p}] + 2\,p\,(p^2+1)\,(\mathbf{T}_1(p^2) \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}_1(p^2))\\
&\quad + 2\,p\,\mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2) - (p^2+1)\,(\mathbf{T}(p)^2 \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}(p)^2)\\
&\quad - (\mathbf{T}(p)^2 \otimes \mathbf{T}_1(p^2) + \mathbf{T}_1(p^2) \otimes \mathbf{T}(p)^2))\,,\\
\mathbf{s}_3 &= p^2\,((2p^4+4p^2-1)\,[\mathbf{p}] \otimes [\mathbf{p}] + (2p^2-1)\,(\mathbf{T}_1(p^2) \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}_1(p^2))\\
&\quad - \mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2) - p\,(\mathbf{T}(p)^2 \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}(p)^2))\,\mathbf{T}(p) \otimes \mathbf{T}(p)\,,\\
\mathbf{s}_4 &= p^4\,((p^8+12p^6+10p^4+4p^2+1)\,[\mathbf{p}]^2 \otimes [\mathbf{p}]^2\\
&\quad + 2(3p^6+5p^4+3p^2+1)\,(\mathbf{T}_1(p^2) \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}_1(p^2))[\mathbf{p}] \otimes [\mathbf{p}]\\
&\quad + 4(p^2+1)^2\,\mathbf{T}_1(p^2)[\mathbf{p}] \otimes \mathbf{T}_1(p^2)[\mathbf{p}]\\
&\quad + (3p^4+2p^2+1)\,(\mathbf{T}_1(p^2)^2 \otimes [\mathbf{p}]^2 + [\mathbf{p}]^2 \otimes \mathbf{T}_1(p^2)^2)\\
&\quad + 2(p^2+1)\,(\mathbf{T}_1(p^2) \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}_1(p^2))\mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\\
&\quad + \mathbf{T}_1(p^2)^2 \otimes \mathbf{T}_1(p^2)^2\\
&\quad - 2p(p^4+4p^2+1)\,(\mathbf{T}(p)^2 \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}(p)^2)[\mathbf{p}] \otimes [\mathbf{p}]\\
&\quad - 4p(p^2+1)\,(\mathbf{T}(p)^2 \otimes \mathbf{T}_1(p^2) + \mathbf{T}_1(p^2) \otimes \mathbf{T}(p)^2)[\mathbf{p}] \otimes [\mathbf{p}]\\
&\quad - 2p\,(\mathbf{T}(p)^2[\mathbf{p}] \otimes \mathbf{T}_1(p^2)^2 + \mathbf{T}_1(p^2)^2 \otimes \mathbf{T}(p)^2[\mathbf{p}])\\
&\quad - 4p^3\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2) \otimes [\mathbf{p}]^2 + [\mathbf{p}]^2 \otimes \mathbf{T}(p)^2\mathbf{T}_1(p^2))\\
&\quad + (p^2+2)\,\mathbf{T}(p)^2[\mathbf{p}] \otimes \mathbf{T}(p)^2[\mathbf{p}]\\
&\quad + (\mathbf{T}_1(p^2) \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}_1(p^2))\mathbf{T}(p)^2 \otimes \mathbf{T}(p)^2\\
&\quad + p^2\,(\mathbf{T}(p)^4 \otimes [\mathbf{p}]^2 + [\mathbf{p}]^2 \otimes \mathbf{T}(p)^4))\,,\\
\mathbf{s}_5 &= -p^6\,((6p^6+2p^4-p^2+2)\,[\mathbf{p}]^2 \otimes [\mathbf{p}]^2\\
&\quad + (p^4-p^2+3)\,(\mathbf{T}_1(p^2) \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}_1(p^2))[\mathbf{p}] \otimes [\mathbf{p}]\\
&\quad + (3p^2+4)\,\mathbf{T}_1(p^2)[\mathbf{p}] \otimes \mathbf{T}_1(p^2)[\mathbf{p}]\\
&\quad - (2p^2-1)\,(\mathbf{T}_1(p^2)^2 \otimes [\mathbf{p}]^2 + [\mathbf{p}]^2 \otimes \mathbf{T}_1(p^2)^2)\\
&\quad + (\mathbf{T}_1(p^2) \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}_1(p^2))\mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\\
&\quad - p(2p^2+1)\,(\mathbf{T}(p)^2 \otimes [\mathbf{p}] + [\mathbf{p}] \otimes \mathbf{T}(p)^2)[\mathbf{p}] \otimes [\mathbf{p}]\\
&\quad - 2p\,(\mathbf{T}(p)^2 \otimes \mathbf{T}_1(p^2) + \mathbf{T}_1(p^2) \otimes \mathbf{T}(p)^2)[\mathbf{p}] \otimes [\mathbf{p}]\\
&\quad + p\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2) \otimes [\mathbf{p}]^2 + [\mathbf{p}]^2 \otimes \mathbf{T}(p)^2\mathbf{T}_1(p^2))\\
&\quad + \mathbf{T}(p)^2[\mathbf{p}] \otimes \mathbf{T}(p)^2[\mathbf{p}])\mathbf{T}(p) \otimes \mathbf{T}(p)\,,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{s}_6 = &-p^8\,(2p^2(p^8+6p^6+11p^4+8p^2+2)\,[\mathbf{p}]^3\otimes[\mathbf{p}]^3\\
&+2p^2(5p^4+12p^2+6)\,\mathbf{T}_1(p^2)[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)[\mathbf{p}]^2\\
&+(3p^4+10p^2-1)\,\mathbf{T}(p)^2[\mathbf{p}]^2\otimes\mathbf{T}(p)^2[\mathbf{p}]^2\\
&-\mathbf{T}(p)^2\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2)[\mathbf{p}]\\
&+2p^2(3p^6+11p^4+12p^2+4)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&+6p^2(p^2+1)^2\,(\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)[\mathbf{p}]\otimes[\mathbf{p}]\\
&+6p^2(p^2+1)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}_1(p^2)[\mathbf{p}]\\
&+2p^2(p^2+1)\,(\mathbf{T}_1(p^2)^3\otimes[\mathbf{p}]^3+[\mathbf{p}]^3\otimes\mathbf{T}_1(p^2)^3)\\
&+2p^2\,(\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2)\\
&-p(5p^6+13p^4+10p^2+2)\,(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&-p(7p^4+12p^2+4)\,(\mathbf{T}(p)^2\otimes\mathbf{T}_1(p^2)+\mathbf{T}_1(p^2)\otimes\mathbf{T}(p)^2)[\mathbf{p}]^2\otimes[\mathbf{p}]^2\\
&-3p(p^2+1)\,(\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}_1(p^2)^2+\mathbf{T}_1(p^2)^2\otimes\mathbf{T}(p)^2[\mathbf{p}])[\mathbf{p}]\otimes[\mathbf{p}]\\
&-p\,(\mathbf{T}(p)^2[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^3+\mathbf{T}_1(p^2)^3\otimes\mathbf{T}(p)^2[\mathbf{p}]^2)\\
&-2p(3p^4+4p^2+1)\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2)\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2))[\mathbf{p}]\otimes[\mathbf{p}]\\
&-2p(3p^2+1)\,(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}_1(p^2)[\mathbf{p}]\\
&-p(p^2+1)\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^3+[\mathbf{p}]^3\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2)^2)\\
&-p\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2)\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2))\mathbf{T}_1(p^2)\otimes\mathbf{T}_1(p^2)\\
&+(5p^2-1)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}(p)^2[\mathbf{p}]\\
&+2p^2(p^2+1)\,(\mathbf{T}(p)^4\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^4)[\mathbf{p}]\otimes[\mathbf{p}]\\
&+2p^2\,(\mathbf{T}(p)^4\otimes\mathbf{T}_1(p^2)[\mathbf{p}]+\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}(p)^4)[\mathbf{p}]\otimes[\mathbf{p}]\\
&-p\,(\mathbf{T}(p)^4\otimes\mathbf{T}(p)^4[\mathbf{p}]+\mathbf{T}(p)^4[\mathbf{p}]\otimes\mathbf{T}(p)^4)[\mathbf{p}]\otimes[\mathbf{p}])\,,\\
\mathbf{s}_7 = &\,p^{11}\,(p(5p^6-2p^4+2)\,\mathbf{T}(p)[\mathbf{p}]^3\otimes\mathbf{T}(p)[\mathbf{p}]^3\\
&+8p\,\mathbf{T}(p)\mathbf{T}_1(p^2)[\mathbf{p}]^2\otimes\mathbf{T}(p)\mathbf{T}_1(p^2)[\mathbf{p}]^2\\
&+p\,\mathbf{T}(p)^3[\mathbf{p}]^2\otimes\mathbf{T}(p)^3[\mathbf{p}]^2\\
&-p(p^4-3)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}(p)[\mathbf{p}]^2\otimes\mathbf{T}(p)[\mathbf{p}]^2\\
&-p\,(\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)\mathbf{T}(p)[\mathbf{p}]\otimes\mathbf{T}(p)[\mathbf{p}]\\
&+2p\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}(p)\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}(p)\mathbf{T}_1(p^2)[\mathbf{p}]\\
&-p\,(\mathbf{T}_1(p^2)^3\otimes[\mathbf{p}]^3+[\mathbf{p}]^3\otimes\mathbf{T}_1(p^2)^3)\mathbf{T}(p)\otimes\mathbf{T}(p)\\
&-(3p^4-3p^2+2)\,(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)\mathbf{T}(p)[\mathbf{p}]^2\otimes\mathbf{T}(p)[\mathbf{p}]^2\\
&+(p^2-3)\,(\mathbf{T}(p)^2\otimes\mathbf{T}_1(p^2)+\mathbf{T}_1(p^2)\otimes\mathbf{T}(p)^2)\mathbf{T}(p)[\mathbf{p}]^2\otimes\mathbf{T}(p)[\mathbf{p}]^2\\
&-(\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}_1(p^2)^2+\mathbf{T}_1(p^2)^2\otimes\mathbf{T}(p)^2[\mathbf{p}])\mathbf{T}(p)[\mathbf{p}]\otimes\mathbf{T}(p)[\mathbf{p}]\\
&+(2p^2-1)\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2)\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2))\mathbf{T}(p)[\mathbf{p}]\otimes\mathbf{T}(p)[\mathbf{p}]\\
&-(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)\mathbf{T}(p)\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}(p)\mathbf{T}_1(p^2)[\mathbf{p}])\,,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{s}_8 = {} & p^{14}\,(2p^2(2p^8+4p^6+14p^4+12p^2+3)\,[\mathbf{p}]^4\otimes[\mathbf{p}]^4 \\
& + 4p^2(p^6+7p^4+9p^2+3)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))[\mathbf{p}]^3\otimes[\mathbf{p}]^3 \\
& + 16p^2(p^2+1)^2\,\mathbf{T}_1(p^2)[\mathbf{p}]^3\otimes\mathbf{T}_1(p^2)[\mathbf{p}]^3 \\
& + 2p^2(3p^4+10p^2+5)\,(\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)[\mathbf{p}]^2\otimes[\mathbf{p}]^2 \\
& + 8p^2(p^2+1)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}_1(p^2)[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)[\mathbf{p}]^2 \\
& + 4p^2\,\mathbf{T}_1(p^2)^2[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2[\mathbf{p}]^2 \\
& + 4p^2(p^2+1)\,(\mathbf{T}_1(p^2)^3\otimes[\mathbf{p}]^3+[\mathbf{p}]^3\otimes\mathbf{T}_1(p^2)^3)[\mathbf{p}]\otimes[\mathbf{p}] \\
& + p^2\,(\mathbf{T}_1(p^2)^4\otimes[\mathbf{p}]^4+[\mathbf{p}]^4\otimes\mathbf{T}_1(p^2)^4) \\
& - 4p(2p^6+3p^4+4p^2+1)\,(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)[\mathbf{p}]^3\otimes[\mathbf{p}]^3 \\
& - 8p(p^2+1)^2\,(\mathbf{T}(p)^2\otimes\mathbf{T}_1(p^2)+\mathbf{T}_1(p^2)\otimes\mathbf{T}(p)^2)[\mathbf{p}]^3\otimes[\mathbf{p}]^3 \\
& - 4p(p^2+1)\,(\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}_1(p^2)^2+\mathbf{T}_1(p^2)^2\otimes\mathbf{T}(p)^2[\mathbf{p}])[\mathbf{p}]^2\otimes[\mathbf{p}]^2 \\
& - 4p(p^4+4p^2+1)\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2)\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2))[\mathbf{p}]^2\otimes[\mathbf{p}]^2 \\
& - 8p(p^2+1)\,(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)\mathbf{T}_1(p^2)[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)[\mathbf{p}]^2 \\
& - 4p\,(\mathbf{T}(p)^2\otimes\mathbf{T}_1(p^2)+\mathbf{T}_1(p^2)\otimes\mathbf{T}(p)^2)\mathbf{T}_1(p^2)[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)[\mathbf{p}]^2 \\
& - 4p^3\,(\mathbf{T}(p)^2\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^3+[\mathbf{p}]^3\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2)^2)+[\mathbf{p}]\otimes[\mathbf{p}] \\
& + 2(5p^4+2p^2+2)\,\mathbf{T}(p)^2[\mathbf{p}]^3\otimes\mathbf{T}(p)^2[\mathbf{p}]^3 \\
& + 2(p^2+2)\,(\mathbf{T}_1(p^2)\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}_1(p^2))\mathbf{T}(p)^2[\mathbf{p}]^2\otimes\mathbf{T}(p)^2[\mathbf{p}]^2 \\
& + 2\,\mathbf{T}(p)^2\mathbf{T}_1(p^2)[\mathbf{p}]^2\otimes\mathbf{T}(p)^2\mathbf{T}_1(p^2)[\mathbf{p}]^2 \\
& + (\mathbf{T}_1(p^2)^2\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}_1(p^2)^2)\mathbf{T}(p)^2[\mathbf{p}]\otimes\mathbf{T}(p)^2[\mathbf{p}] \\
& + (3p^4+2p^2+1)\,(\mathbf{T}(p)^4\otimes[\mathbf{p}]^2+[\mathbf{p}]^2\otimes\mathbf{T}(p)^4)[\mathbf{p}]^2\otimes[\mathbf{p}]^2 \\
& + 2(p^2+1)\,(\mathbf{T}(p)^4\otimes\mathbf{T}_1(p^2)[\mathbf{p}]+\mathbf{T}_1(p^2)[\mathbf{p}]\otimes\mathbf{T}(p)^4)[\mathbf{p}]^2\otimes[\mathbf{p}]^2 \\
& + (\mathbf{T}(p)^4\otimes\mathbf{T}_1(p^2)^2+\mathbf{T}_1(p^2)^2\otimes\mathbf{T}(p)^4)[\mathbf{p}]^2\otimes[\mathbf{p}]^2 \\
& - 2p\,(\mathbf{T}(p)^2\otimes[\mathbf{p}]+[\mathbf{p}]\otimes\mathbf{T}(p)^2)\mathbf{T}(p)^2[\mathbf{p}]^2\otimes\mathbf{T}(p)^2[\mathbf{p}]^2)\,.
\end{aligned}
$$

The other coefficients $\mathbf{s}_9,\dots,\mathbf{s}_{16}$ *are determined by the functional equation:*

$$\mathbf{s}_{16-i} = (p^6\,[\mathbf{p}]\otimes[\mathbf{p}])^{8-i}\,\mathbf{s}_i \quad (i=0,\dots,7)\,.$$

2.3.2 Formula for the Hecke operator $\mathbf{T}(p^\delta)$ in genus 2

In computations of various series of Hecke operators it is useful to have an explicit formula for the spherical image of Hecke operator $\mathbf{T}(p^\delta)$, but it could not be found in the literature. Next, we show how derive it.

PROPOSITION 2.9 (SPHERICAL IMAGE OF HECKE OPERATOR $\mathbf{T}(p^\delta)$)
For genus $n = 2$ the Hecke operator $\mathbf{T}(p^\delta)$ is expressed in the spherical coordinates x_0, x_1, x_2 as

$$\begin{aligned}
\Omega_x^{(2)}(\mathbf{T}(p^\delta)) &= p^{-1}\, x_0^\delta \Big(p\, x_1^{(3+\delta)}\, x_2 - p\, x_1^{(2+\delta)} - p\, x_1^{(3+\delta)}\, x_2^{(2+\delta)} \\
&\quad + p\, x_1^{(2+\delta)}\, x_2^{(3+\delta)} - p\, x_1\, x_2^{(3+\delta)} + p\, x_2^{(2+\delta)} + p\, x_1 - p\, x_2 \\
&\quad - x_1^{(2+\delta)}\, x_2^2 + x_1^{(1+\delta)}\, x_2 + x_1^{(2+\delta)}\, x_2^{(1+\delta)} - x_1^{(1+\delta)}\, x_2^{(2+\delta)} \\
&\quad + x_1^2\, x_2^{(2+\delta)} - x_1\, x_2^{(1+\delta)} - x_1^2\, x_2 + x_1\, x_2^2 \Big) \\
&\quad \times \Big((1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(x_1-x_2) \Big)^{-1} \\
&= -\Big((1-x_1\,x_2)\,(p\,x_1-x_2)\, x_1^{(\delta+1)} \\
&\quad + (1-x_1\,x_2)\,(x_1-p\,x_2)\, x_2^{(\delta+1)} \\
&\quad - (x_1-x_2)\,(1-p\,x_1\,x_2)\,(x_1\,x_2)^{(\delta+1)} \\
&\quad - (x_1-x_2)\,(p-x_1\,x_2) \Big)\, p^{-1}\, x_0^\delta \\
&\quad \times \Big((1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(x_1-x_2) \Big)^{-1}.
\end{aligned} \tag{2.29}$$

This expression is obtained with the help of the formula (2.14) after developing and a simplification by a means of change of summation. Recall the expression for spherical image of the generating power series $\Omega(\mathbf{D}_p^{(2)}(X))$ from the page 52:

$$\Omega(\mathbf{D}_p^{(2)}(X)) = \frac{1 - p^{-1} x_0^2 x_1 x_2 X^2}{(1-x_0X)\,(1-x_0x_1X)\,(1-x_0x_2X)\,(1-x_0x_1x_2X)}\,.$$

Consider the geometric progressions

$$\begin{aligned}
\frac{1}{1-x_0\,X} &= \sum_{\delta_1=0}^{\infty} x_0\,X\,, \\
\frac{1}{1-x_0\,x_1\,X} &= \sum_{\delta_2=0}^{\infty} x_0\,x_1\,X\,, \\
\frac{1}{1-x_0\,x_2\,X} &= \sum_{\delta_3=0}^{\infty} x_0\,x_2\,X\,, \\
\frac{1}{1-x_0\,x_1\,x_2\,X} &= \sum_{\delta_4=0}^{\infty} x_0\,x_1\,x_2\,X\,.
\end{aligned} \tag{2.30}$$

The product of all series (2.30) can be rewritten with the use of substitution $\delta = \delta_1 + \delta_2 + \delta_3 + \delta_4$:

$$\begin{aligned}
&\frac{1}{(1-x_0X)\,(1-x_0x_1X)\,(1-x_0x_2X)\,(1-x_0x_1x_2X)} \\
&\quad = \sum_{\delta_1=0}^{\infty} x_0\,X \sum_{\delta_2=0}^{\infty} x_0\,x_1\,X \sum_{\delta_3=0}^{\infty} x_0\,x_2\,X \sum_{\delta_4=0}^{\infty} x_0\,x_1\,x_2\,X \\
&\quad = \sum_{\delta=0}^{\infty} \sum_{\delta_2=0}^{\delta} \sum_{\delta_3=0}^{\delta-\delta_2} \sum_{\delta_4=0}^{\delta-\delta_2-\delta_3} x_0^{\delta}\,x_1^{\delta_2+\delta_4}\,x_2^{\delta_3+\delta_4}\,X^{\delta}\,,
\end{aligned} \tag{2.31}$$

where the summation over δ_4, δ_3 and δ_2 can be done explicitly:

$$\begin{aligned}
B(\delta) &= \sum_{\delta_2=0}^{\delta} \sum_{\delta_3=0}^{\delta-\delta_2} \sum_{\delta_4=0}^{\delta-\delta_2-\delta_3} x_0^{\delta}\,x_1^{\delta_2+\delta_4}\,x_2^{\delta_3+\delta_4}\,X^{\delta} \\
&= \sum_{\delta_2=0}^{\delta} \sum_{\delta_3=0}^{\delta-\delta_2} \frac{x_1^{\delta_2}\,x_2^{\delta_3} - x_1^{\delta-\delta_3+1}\,x_2^{\delta-\delta_2+1}}{1-x_1\,x_2}\,(x_0\,X)^{\delta} \\
&= \sum_{\delta_2=0}^{\delta} \frac{x_1^{\delta_2}(1-x_1) + (x_1^{\delta+2}(1-x_2) - x_1^{\delta_2}(1-x_1x_2))x_2^{\delta-\delta_2+1}}{(1-x_1)\,(1-x_2)\,(1-x_1\,x_2)}\,(x_0\,X)^{\delta} \\
&= \frac{(x_1-x_2)(1-(x_1x_2)^{\delta+2}) - (x_1^{\delta+2}-x_2^{\delta+2})(1-x_1x_2)}{(1-x_1)\,(1-x_2)\,(1-x_1x_2)\,(x_1-x_2)}\,(x_0X)^{\delta}\,.
\end{aligned} \tag{2.32}$$

It is sufficient to compute $B(\delta) - p^{-1}x_0^2x_1x_2X^2\,B(\delta-2)$ using the above formula (2.32) in order to obtain the term of the series $\Omega(\mathbf{D}_p^{(2)}(X))$ with X in power δ, which corresponds to $\Omega_x^{(2)}(\mathbf{T}(p^{\delta}))X^{\delta}$. This step completes the demonstration of the Proposition 2.9.

2.3.3 Computation in spherical coordinates

In order to state the analogous of Rankin's lemma for multiplicative convolution of two series in genus two, we write the corresponding formulae (2.29) for the Hecke operators $\mathbf{T}(p^{\delta})$ in two sets of spherical variables $\{x_0, x_1, x_2\}$ and $\{y_0, y_1, y_2\}$ of two copies of Ω_x and Ω_y of the spherical map. It allows us

to treat the tensor product of two local Hecke algebras, as follows:

$$\begin{aligned}\Omega_y^{(2)}(\mathbf{T}(p^\delta)) = p^{-1}\, y_0^\delta \Big(& p\, y_1^{(3+\delta)}\, y_2 - p\, y_1^{(2+\delta)} - p\, y_1^{(3+\delta)}\, y_2^{(2+\delta)} \\ & + p\, y_1^{(2+\delta)}\, y_2^{(3+\delta)} - p\, y_1\, y_2^{(3+\delta)} + p\, y_2^{(2+\delta)} + p\, y_1 - p\, y_2 \\ & - y_1^{(2+\delta)}\, y_2^2 + y_1^{(1+\delta)}\, y_2 + y_1^{(2+\delta)}\, y_2^{(1+\delta)} - y_1^{(1+\delta)}\, y_2^{(2+\delta)} \\ & + y_1^2\, y_2^{(2+\delta)} - y_1\, y_2^{(1+\delta)} - y_1^2\, y_2 + y_1\, y_2^2 \Big) \\ \times & \Big((1-y_1)\,(1-y_2)\,(1-y_1\,y_2)\,(y_1-y_2) \Big)^{-1}. \end{aligned} \tag{2.33}$$

The product of the above polynomials (2.29) and (2.33) is given by

$$\begin{aligned}\Omega_x^{(2)}(\mathbf{T}(p^\delta)) \cdot \Omega_y^{(2)}(\mathbf{T}(p^\delta)) = & \\ p^{-2}\, x_0^\delta\, y_0^\delta \Big(& p\, x_1^{(3+\delta)}\, x_2 - p\, x_1^{(2+\delta)} - p\, x_1^{(3+\delta)}\, x_2^{(2+\delta)} \\ & + p\, x_1^{(2+\delta)}\, x_2^{(3+\delta)} - p\, x_1\, x_2^{(3+\delta)} + p\, x_2^{(2+\delta)} + p\, x_1 - p\, x_2 \\ & - x_1^{(2+\delta)}\, x_2^2 + x_1^{(1+\delta)}\, x_2 + x_1^{(2+\delta)}\, x_2^{(1+\delta)} - x_1^{(1+\delta)}\, x_2^{(2+\delta)} \\ & + x_1^2\, x_2^{(2+\delta)} - x_1\, x_2^{(1+\delta)} - x_1^2\, x_2 + x_1\, x_2^2 \Big) \\ \times & \Big(p\, y_1^{(3+\delta)}\, y_2 - p\, y_1^{(2+\delta)} - p\, y_1^{(3+\delta)}\, y_2^{(2+\delta)} \\ & + p\, y_1^{(2+\delta)}\, y_2^{(3+\delta)} - p\, y_1\, y_2^{(3+\delta)} + p\, y_2^{(2+\delta)} + p\, y_1 - p\, y_2 \\ & - y_1^{(2+\delta)}\, y_2^2 + y_1^{(1+\delta)}\, y_2 + y_1^{(2+\delta)}\, y_2^{(1+\delta)} - y_1^{(1+\delta)}\, y_2^{(2+\delta)} \\ & + y_1^2\, y_2^{(2+\delta)} - y_1\, y_2^{(1+\delta)} - y_1^2\, y_2 + y_1\, y_2^2 \Big) \\ \times & \Big((1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(x_1-x_2) \Big)^{-1} \\ \times & \Big((1-y_1)\,(1-y_2)\,(1-y_1\,y_2)\,(y_1-y_2) \Big)^{-1}. \end{aligned} \tag{2.34}$$

Next, in order to carry out the summation of the series with obtained in (2.34) terms $\Omega_x^{(2)}(\mathbf{T}(p^\delta)) \cdot \Omega_y^{(2)}(\mathbf{T}(p^\delta))$ multiplied by X^δ, we use a subdivision of each summand (over δ) into smaller parts. These parts correspond to symbolic monomials in x_1^δ, y_1^δ, x_2^δ, y_2^δ, $(x_1x_2)^\delta$, $(y_1y_2)^\delta$; there are 16 different terms in the numerator after the simplification of the result of multiplication. Therefore, we have the following theorem:

THEOREM 2.10 (SPHERICAL IMAGE OF GENERATING SERIES PRODUCT)
In genus 2 *the following equality holds*

$$\sum_{\delta=0}^{\infty} \Omega_x^{(2)}(\mathbf{T}(p^\delta)) \cdot \Omega_y^{(2)}(\mathbf{T}(p^\delta))\, X^\delta = \tag{2.35}$$

$$
\begin{aligned}
&- \frac{(p\,x_1 - x_2)\,(1 - p\,y_1\,y_2)\,x_1\,y_1\,y_2}{p^2\,(1-x_1)(1-x_2)(x_1-x_2)(1-y_1)(1-y_2)(1-y_1y_2)(1-x_0x_1y_0y_1y_2\,X)} \\
&+ \frac{x_2\,y_1\,(x_1 - p\,x_2)\,(p\,y_1 - y_2)}{p^2\,(1-x_1)(1-x_2)(x_1-x_2)(1-y_1)(1-y_2)(y_1-y_2)(1-x_0\,x_2\,y_0\,y_1\,X)} \\
&+ \frac{x_2\,y_2\,(x_1 - p\,x_2)(y_1 - p\,y_2)}{p^2\,(1-x_1)(1-x_2)(x_1-x_1)(1-y_1)(1-y_2)(y1-y_2)(1-x_0\,y_0\,x_2\,y_2\,X)} \\
&- \frac{x_2\,y_1\,y_2\,(x_1 - p\,x_2)\,(1 - p\,y_1\,y_2)}{p^2\,(1-x_1)(1-x_2)(x_1-x_2)(1-y_1)(1-y_2)(1-y_1y_2)(1-x_0x_2y_0y_1y_2X)} \\
&- \frac{x_1\,(p\,x_1 - x_2)\,(p - y_1\,y_2)}{p^2\,(1-x_1)\,(1-x_2)\,(x_1-x_2)\,(1-y_1)\,(1-y_2)\,(1-y_1\,y_2)\,(1-x_0\,x_1\,y_0\,X)} \\
&- \frac{x_1\,x_2\,y_1(1 - p\,x_1\,x_2)\,(p\,y_1 - y_2)}{p^2\,(1-x_1)(1-x_2)(1-x_1x_2)(1-y_1)(1-y_2)(y_1-y_2)(1-x_0x_1x_2y_0y_1X)} \\
&- \frac{x_1\,x_2\,y_2\,(1 - p\,x_1\,x_2)\,(y_1 - p\,y_2)}{p^2\,(1-x_1)(1-x_2)(1-x_1x_2)(1-y_1)(1-y_2)(y_1-y_2)(1-x_0x_1x_2y_0y_2X)} \\
&+ \frac{y_1\,y_2\,(p - x_1\,x_2)\,(1 - p\,y_1\,y_2)}{p^2\,(1-x_1)(1-x_2)(1-x_1x_2)(1-y_1)(1-y_2)(1-y_1y_2)(1-x_0y_0y_1y_2X)} \\
&+ \frac{x_1\,x_2\,(1 - p\,x_1\,x_2)\,(p - y_1\,y_2)}{p^2\,(1-x_1)(1-x_2)(1-x_1x_2)(1-y_1)(1-y_2)(1-y_1y_2)(1-x_0x_1x_2y_0X)} \\
&- \frac{x_1\,y_1\,(p\,x_1 - x_2)\,(p\,y_1 - y_2)}{p^2\,(1-x_1)\,(1-x_2)\,(x_1-x_2)\,(1-y_1)\,(1-y_2)\,(y_1-y_2)\,(1-x_0\,x_1\,y_0\,y_1\,X)} \\
&+ \frac{x_1\,y_2\,(p\,x_1 - x_2)\,(y_1 - p\,y_2)}{p^2\,(1-x_1)\,(1-x_2)\,(x_1-x_2)\,(1-y_1)\,(1-y_2)\,(y_1-y_2)\,(1-x_0\,x_1\,y_0\,y_2\,X)} \\
&- \frac{x_2\,(x_1 - p\,x_2)\,(p - y_1\,y_2)}{p^2\,(1-x_1)\,(1-x_2)\,(x_1-x_2)\,(1-y_1)\,(1-y_2)\,(1-y_1\,y_2)\,(1-x_0\,x_2\,y_0\,X)} \\
&+ \frac{x_1\,x_2\,y_1\,y_2\,(1 - p\,x_1\,x_2)\,(1 - p\,y_1\,y_2)}{p^2\,(1-x_1)(1-x_2)(1-x_1x_2)(1-y_1)(1-y_2)(1-y_1y_2)(1-x_0\,x_1\,x_2\,y_0\,y_1\,y_2\,X)} \\
&+ \frac{(p - x_1\,x_2)\,(p - y_1\,y_2)}{p^2\,(1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(1-y_1)\,(1-y_2)\,(1-y_1\,y_2)\,(1-x_0\,y_0\,X)} \\
&- \frac{y_1\,(p - x_1\,x_2)\,(p\,y_1 - y_2)}{p^2\,(1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(1-y_1)\,(1-y_2)\,(y_1-y_2)\,(1-x_0\,y_0\,y_1\,X)} \\
&- \frac{y_2\,(p - x_1\,x_2)\,(y_1 - p\,y_2)}{p^2\,(1-x_1)\,(1-x_2)\,(1-x_1\,x_2)\,(1-y_1)\,(1-y_2)\,(y_1-y_2)\,(1-x_0\,y_0\,y_2\,X)}
\end{aligned}
$$

Remark 2.11 (On the denominator of (2.35)) *With the help of computer, one finds that the polynomial factors, which not dependent on X in the denominators of (2.35) dropped after the simplification in the ring $\mathbb{Q}[x_0, x_1, x_2, y_0, y_1, y_2][\![X]\!]$, so that the common denominator becomes*

$$\begin{aligned}
&(1 - x_0\, y_0 X)\,(1 - x_0\, y_0\, x_1\, X)\,(1 - x_0\, y_0\, y_1\, X)\,(1 - x_0\, y_0\, x_2\, X)\\
&(1 - x_0\, y_0\, y_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, X)\,(1 - x_0\, y_0\, x_1\, x_2\, X)\\
&(1 - x_0\, y_0\, x_1\, y_2\, X)\,(1 - x_0\, y_0\, y_1\, x_2\, X)\,(1 - x_0\, y_0\, y_1\, y_2\, X)\\
&(1 - x_0\, y_0\, x_2\, y_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, x_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, y_2\, X)\\
&(1 - x_0\, y_0\, x_1\, x_2\, y_2\, X)\,(1 - x_0\, y_0\, y_1\, x_2\, y_2\, X)\,(1 - x_0\, y_0\, x_1\, y_1\, x_2\, y_2\, X).
\end{aligned} \tag{2.36}$$

Remark 2.12 (Comparison with genus 1) *From direct computations, it is seen that the numerator of rational fraction (2.35) is the product of $1 - x_0^2 y_0^2\, x_1 y_1 x_2 y_2 X^2$ and the polynomial of degree 12 in X with coefficients in $\mathbb{Q}[x_0, x_1, x_2, y_0, y_1, y_2]$, which constant term is equal to 1, while the leading term is:*

$$\frac{x_0^{12}\, y_0^{12}\, x_1^6\, x_2^6\, y_1^6\, y_2^6}{p^2}\, X^{12}.$$

It is also seen that the factor of degree 12 does not contain terms of degree 1 and 11 in X. The factor of degree 2 in X is similar to that in the case of genus 1 (this series was studied and used in [MP77]):

$$\begin{aligned}
&\sum_{\delta=0}^{\infty} \Omega_x^{(1)}(\mathbf{T}(p^\delta)) \cdot \Omega_y^{(1)}(\mathbf{T}(p^\delta))\, X^\delta\\
&\quad = \sum_{\delta=0}^{\infty} \frac{x_0^\delta\,(1 - x_1^{(1+\delta)})}{1 - x_1} \cdot \frac{y_0^\delta\,(1 - y_1^{(1+\delta)})}{1 - y_1}\, X^\delta\\
&\quad = \frac{1}{(1 - x_1)\,(1 - y_1)\,(1 - x_0\, y_0\, X)}\\
&\qquad - \frac{y_1}{(1 - x_1)\,(1 - y_1)\,(1 - x_0\, y_0\, y_1\, X)}\\
&\qquad - \frac{x_1}{(1 - x_1)\,(1 - y_1)\,(1 - x_0\, y_0\, x_1\, X)}\\
&\qquad + \frac{x_1\, y_1}{(1 - x_1)\,(1 - y_1)\,(1 - x_0\, y_0\, x_1\, y_1\, X)}\\
&\quad = \frac{1 - x_0^2\, y_0^2\, x_1\, y_1\, X^2}{(1 - x_0 y_0 x_1 y_1 X)(1 - x_0 y_0 x_1 X)(1 - x_0 y_0 y_1 X)(1 - x_0 y_0 X)}\,.
\end{aligned} \tag{2.37}$$

Also see Lemma 3.8 on page 86.

2.3.4 Inverting the spherical image

The statement of Theorem 2.8 in terms of Hecke operators is obtained by the inversion of the spherical image (2.35) with the help of method of undetermined coefficients, which was described in the Section 2.2.4. The formulae for the basis Hecke operators are given in (2.15).

Remark 2.13 (Functional equation for denominator of Th.2.8) *There is an obvious functional equation for the coefficients* $\mathbf{s}_i$ *of the denominator of* (2.28) *(similar to [And87, (3.3.79), page 164]):*

$$\mathbf{s}_{16-i} = (p^6\,[\mathbf{p}] \otimes [\mathbf{p}])^{8-i}\,\mathbf{s}_i\,. \tag{2.38}$$

Remark 2.14 (Comparison with genus 1 in terms of Hecke operators) *It follows directly from the Remark 2.12 that the result obtained in case of genus* 1 *can be written in terms of Hecke operators as next:*

$$\begin{aligned}
&\sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) \otimes \mathbf{T}(p^\delta)\, X^\delta \\
&\quad = \Big(1 - p^2\,\mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\, X^2\Big)\,\Big(1 - \mathbf{T}(p) \otimes \mathbf{T}(p)\, X + \\
&\quad \big(p\,\mathbf{T}(p)^2 \otimes \mathbf{T}_1(p^2) + p\,\mathbf{T}_1(p^2) \otimes \mathbf{T}(p)^2 - 2p^2\,\mathbf{T}_1(p^2) \otimes \mathbf{T}_1(p^2)\big) X^2 \\
&\quad - p^2\,\mathbf{T}(p)\mathbf{T}_1(p^2) \otimes \mathbf{T}(p)\mathbf{T}_1(p^2) X^3 + p^4\,\mathbf{T}_1(p^2)^2 \otimes \mathbf{T}_1(p^2)^2 X^4\Big)^{-1}\,.
\end{aligned} \tag{2.39}$$

2.4 Generating series for symmetric squares and cubes

Using the formula (2.29), one can also evaluate the symmetric square generating series and the cubic generating series of higher genus. Note that this series, written here in spherical coordinates x_0, x_1, x_2 is different from the one studied by Andrianov and Kalinin in [AK79], and has the form:

$$\begin{aligned}
&\sum_{\delta=0}^{\infty} \Omega_x^{(2)}(\mathbf{T}(p^{2\delta}))X^\delta \\
&\quad = \Big(1 - \frac{x_0^2 x_1 x_2}{p} X\Big) \\
&\quad \times \frac{1 + x_0^2(x_1 + x_2 + 2x_1x_2 + x_1^2x_2 + x_1x_2^2)X + x_0^4\,x_1^2\,x_2^2\,X^2}{(1 - x_0^2\,X)\,(1 - x_0^2\,x_1^2\,X)\,(1 - x_0^2\,x_2^2\,X)\,(1 - x_0^2\,x_1^2\,x_2^2\,X)}\,.
\end{aligned} \tag{2.40}$$

The cubic generating series of higher genus, written in spherical variables x_0, x_1, x_2 has the form:

$$\begin{aligned}
&\sum_{\delta=0}^{\infty} \Omega_x^{(2)}(\mathbf{T}(p^{3\delta}))X^\delta = \\
&\quad p^{-1}\Big(-p - x_0^3(x_1+1)(x_2+1)(p(x_1+x_2+x_1^2x_2+x_1x_2^2)-x_1x_2)X \\
&\quad + x_0^6((x_1x_2^3+x_1^3x_2)+(1-p)x_1^2x_2^2+(2-p)(x_1^2x_2^3+x_1^3x_2^2) \\
&\qquad + (1-p)(x_1^2x_2^4+x_1^4x_2^2)+(3-2p)x_1^3x_2^3+(2-p)(x_1^3x_2^4+x_1^4x_2^3) \\
&\qquad + (x_1^3x_2^5+x_1^5x_2^3)+(1-p)x_1^4x_2^4)X^2 \\
&\quad + x_0^9x_1^4x_2^4(x_1+1)(x_2+1)X^3\Big) \\
&\quad \times \Big((1-x_0^3X)(1-x_0^3x_1^3X)(1-x_0^3x_2^3X)(1-x_0^3x_1^3x_2^3X)\Big)^{-1}.
\end{aligned} \tag{2.41}$$

Chapter 3

Computation with Siegel modular forms and L-functions

3.1 Explicit examples of Siegel modular forms

3.1.1 Saito-Kurokawa conjecture

In 1978 Kurokawa computed explicit examples of Siegel modular forms of genus 2 [Kur78]. These examples led to the Saito-Kurokawa conjecture, proving of which required focusing much attention on Jacobi forms. The latter were first studied by Eichler and Zagier [EZ85]. Jacobi forms provide a powerful tool in study of Siegel modular forms. Using modern technique, Skoruppa [Sko92] demonstrated the computational approach to the study of Siegel modular forms. He computed the Siegel cusp Hecke eigenforms of even weight on the group $\mathrm{Sp}_2(\mathbb{Z})$, which do not belong to the Maaß space, and observed some interesting new phenomena.

At the time of Kurokawa's paper, much effort has been made by mathematicians to give explicit examples of Siegel modular forms. In particular, Kurokawa constructed the degree 2 cusp form χ_{10} of weight 10. On the basis of explicit calculations, he guessed that

$$L(s, \chi_{10}, spin) = \zeta(s-9)\,\zeta(s-8)\,L(s, f_{18})\,, \tag{3.1}$$

where f_{18} is the normalized cusp form of weight 18 on $\mathrm{SL}_2(\mathbb{Z})$. His examples suggested that is some cases

$$L(s, F_k, spin) = \zeta(s-k+1)\,\zeta(s-k+2)\,L(s, f_{2k-2}) \tag{3.2}$$

with $f_{2k-2} \in \mathcal{S}_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$ a normalized cusp form and F_k a corresponding Siegel modular form of weight k, which is an eigenform of the Hecke algebra.

He conjectured the existence of a lifting

$$\mathcal{S}_{2k-2}(\mathrm{SL}_2(\mathbb{Z})) \longrightarrow \mathcal{S}_k(\mathrm{Sp}_2(\mathbb{Z}))\,, \quad f_{2k-2} \mapsto F_k \tag{3.3}$$

with the relation (3.2). More precisely, now we have the following theorem:

THEOREM 3.1 (SAITO-KUROKAWA) *The Maaß subspace $\mathcal{S}_k^*(\mathrm{Sp}_2(\mathbb{Z}))$ is invariant under the action of the Hecke algebra and there is one-to-one correspondence between eigenspaces in $\mathcal{S}_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$ and Hecke eigenspaces in $\mathcal{S}_k^*(\mathrm{Sp}_2(\mathbb{Z}))$ given by*

$$f \leftrightarrow F \Leftrightarrow L(s, F, spin) = \zeta(s-k+1)\,\zeta(s-k+2)\,L(s, f)\,. \tag{3.4}$$

This theorem is due to Maaß [Maa79a, Maa79b, Maa79c], Andrianov [And79] and Zagier [Zag81].

It is worth mentioning that forms in the Maaß space are, strictly speaking, not "pure" Siegel modular forms in the sense that they are obtained by means of a lifting from GL_2. Thus many properties can be derived from corresponding properties of forms on GL_2. In particular, squared Fourier coefficients of the cusp Siegel eigenform are essentially equal to the central special values of the L-function associated to the elliptic cusp form.

3.1.2 Ikeda lifting

Duke and Imamoḡlu [DI96] presented another proof of the isomorphic lifting from the Kohnen space to the Maaß space in the Saito-Kurokawa correspondence. The interesting fact is that their proof bypasses the use of Jacobi forms. They also conjectured that for the same parity k and n there exists a Hecke eigenform $F(Z) \in \mathcal{S}_{k+n}(\mathrm{Sp}_{2n}(\mathbb{Z}))$ of degree $2n$, whose standard L-function is essentially equal to the product of shifted Hecke L-series of a normalized Hecke eigenform $f(z) \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$. The evidences were given by Breulmann and Kuss [BK00].

Ikeda [Ike01] showed that the conjecture by Duke and Imamoḡlu is true. Moreover, he obtained a simple formula for the Fourier coefficients of such Siegel form $F(Z)$. His work was a generalization of the Saito-Kurokawa lifting to the higher degree. In particular, for k being an arbitrary positive integer such that $k \equiv n \pmod 2$ for some positive integer n, choose a normalized Hecke eigenform

$$f(z) = \sum_{m=1}^{\infty} a_m\, q^m \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z})), \quad a_1 = 1\,. \tag{3.5}$$

Then there is an explicit expression for the Fourier coefficients of a Siegel cusp form $F(Z)$, which is a Hecke eigenform whose standard L-function is equal to

$$L(s, F, stnd) = \zeta(s) \prod_{i=1}^{2n} L(s + k + n - i, f)\,. \tag{3.6}$$

Murakawa [Mur02, Lemma 4.1] determined the local Satake p-parameters $\{\beta_0, \beta_1, \ldots, \beta_{2n}\}$ for $F(Z)$:

$$\begin{aligned} \beta_0 &= p^{nk - n(n+1)/2}\,, \\ \beta_i &= \alpha\, p^{i-1/2}\,, \\ \beta_{n+i} &= \alpha^{-1}\, p^{i-1/2}\,, \quad i = 1, \ldots, n\,, \end{aligned} \tag{3.7}$$

where $\{\alpha, \alpha^{-1}\}$ are the local Satake p-parameters of $f(z) = \sum a_n\, q^n$, i.e.

$$(1 - \alpha\, p^{k-1/2}\, X)\,(1 - \alpha^{-1}\, p^{k-1/2}\, X) = 1 - a_p\, X + p^{2k-1}\, X^2\,. \tag{3.8}$$

When $n = 1$, the lifted form $F(Z)$ is equal to the Saito-Kurokawa lift of $f(z)$.

3.1.3 Miyawaki's constructions

In the remarkable paper [Miy92] Miyawaki considered certain Siegel cusp forms of degree 3, and on the basis of some numerical calculations, he made interesting conjectures about the degeneration of the standard and spinor L-functions associated to such cusp forms. Several years later Ikeda proved a part of the Miyawaki's conjecture related to the standard L-function (see [Ike06]). Basically he was able to construct an explicit lifting from Siegel cusp forms of degree r to Siegel cusp forms of degree $r + 2n$. In particular, it turns out that the only cusp form of degree 3 and weight 12 is a basic example of this lifting (for $r = 1$, $n = 1$).

Ikeda refined Miyawaki's idea to the following result:

Theorem 3.2 (Miyawaki-Ikeda) *Let k and n be natural numbers with $k - n$ even. Furthermore, let $f \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ be a normalized Hecke eigenform. Then, under non-vanishing conditions, there exists for every eigenform $g \in \mathcal{S}_{k+n+r}(\mathrm{Sp}_r(\mathbb{Z}))$ with $n, r \geqslant 1$ a Siegel modular eigenform $F_{f,g} \in \mathcal{S}_{k+n+r}(\mathrm{Sp}_{2n+r}(\mathbb{Z}))$ such that*

$$L(s, F_{f,g}, stnd) = L(s, g, stnd) \prod_{j=1}^{2n} L(s + k + n - j, f)\,. \tag{3.9}$$

Recall that Miyawaki constructed his numerical examples by means of theta functions with spherical functions. Namely, let E_8 be a unique even unimodular lattice of rank 8 i.e.,

$$E_8 = \left\{ {}^t(x_1, \ldots, x_8) \in \mathbb{R}^8 \;\middle|\; \begin{array}{l} 2x_i \in \mathbb{Z} (i = 1, \ldots, 8), \\ x_1 + \cdots + x_8 \in 2\mathbb{Z}, \\ x_i - x_j \in \mathbb{Z} \end{array} \right\}, \tag{3.10}$$

and

$$Q = \begin{pmatrix} 1 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & i & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & i & 0 & 0 \end{pmatrix} \tag{3.11}$$

be 3×8 matrix. Then the theta series

$$F_{12}(Z) = \sum_{v_1, v_2, v_3 \in E_8} \Re(\det(Q \cdot (v_1, v_2, v_3))^8) \exp(\pi i \, \mathsf{Tr}((\langle v_i, v_j \rangle) Z)) \tag{3.12}$$

is a cusp form of weight 12 with respect to $\mathrm{Sp}_3(\mathbb{Z})$, where $Z \in \mathfrak{H}^3$,

$$\mathrm{Sp}_3(\mathbb{Z}) = \left\{ M \in M_6 : M \, J \, {}^t M = J \right\}, \; J = \left(\begin{smallmatrix} 0 & \mathrm{I}_3 \\ -\mathrm{I}_3 & 0 \end{smallmatrix} \right), \tag{3.13}$$

$$\mathfrak{H}^3 = \left\{ Z = {}^t Z = X + iY : X, Y \in M_3(\mathbb{R}), \, Y > 0 \right\}. \tag{3.14}$$

In the recent work [Hei07] Heim proved Miyawaki's conjecture relevant to the spinor L-function for the specific case of the cusp form F_{12}. In fact, Heim showed that the following equality holds:

$$L(s, F_{12}, spin) = L(s - 9, \Delta) \, L(s - 10, \Delta) \, L(s, \Delta \otimes g_{20}), \tag{3.15}$$

where Δ is Ramanujan's discriminant cusp form and g_{20} is the cusp form of weight 20 of level 1. In Section 3.2 we show that one can provide the explicit rational numbers R_s and powers of π such that for each critical value $s = 12, \ldots, 19$

$$L(s, F_{12}, spin) = R_s \, \pi^{\alpha_s} \, \langle \Delta, \Delta \rangle \, \langle g_{20}, g_{20} \rangle. \tag{3.16}$$

We also compute the values numerically using the SAGE software [SAG] and Dokchitser's ComputeL PARI package [Dok, Dok04].

To our knowledge, this is the first example of a spinor L-function of Siegel cusp forms of degree 3, when the special values can be computed explicitly. The spinor L-function $L(s, F_{12}, spin)$ has a holomorphic continuation to the whole complex plane and is the first example of a spinor L-function of a Siegel cusp forms of degree 3 which satisfies a functional equation.

It is possible to apply the same technique to compute the critical values of the spinor L-functions for non cuspidal modular forms; but there exist direct (and more simple) methods in this case. For example, due to Zharkovskaya [Žar74, Theorem 1] there is the famous equality for non cuspidal forms

$$L(s, F, spin) = L(s, \Phi(F), spin)\, L(s - k + n, \Phi(F), spin)\,, \tag{3.17}$$

where Φ is the Siegel operator. We could also use our approach to compute the conjectural special values of the spinor L-function $L(s, F_{14}, spin)$ for the unique Siegel cusp for of degree 3 and weight 14.

3.1.4 Other conjectures

The proof of Miyawaki's conjecture related to F_{12} cannot be extended to F_{14}. In fact, Heim indicated [Hei08] two types of Miyawaki's constructions and related conjectures:

Conjecture 3.3 (Miyawaki conjecture type I) *There exists a map $\mathcal{S}_k \times \mathcal{S}_{2k-2} \longrightarrow \mathcal{S}_k^3$ such that for pairs of Hecke eigenforms (f, g) the image F is a Hecke eigenform and the eigenvalues of F are expressed in terms of the eigenvalues of f and g.*

Conjecture 3.4 (Miyawaki conjecture type II) *There exists a map $\mathcal{S}_{k-2} \times \mathcal{S}_{2k-2} \longrightarrow \mathcal{S}_k^3$ such that for pairs of Hecke eigenforms (f, g) the image F is a Hecke eigenform and the eigenvalues of F are expressed in terms of the eigenvalues of f and g.*

The conjecture of type II is still open. Heim performed the careful analysis of Miyawaki's constructions and several other examples. The observations led him to the following statement.

Conjecture 3.5 (Heim, [Hei08]) *Let k be a positive integer.*

1. *Let $G \in \mathcal{M}_k^2$ be a Hecke eigenform. Then $G \boxtimes E_{k-2} \in \mathcal{M}_k^3$.*
2. *Let $G \in \mathcal{S}_k^2$ and $h \in \mathcal{S}_{k-2}$ be Hecke eigenforms. Then $L(s, G \otimes h)$ is modular and $G \boxtimes h \in \mathcal{S}_k^3$, i.e. $L(s, G \otimes h) = L(s, G \boxtimes h, spin)$.*

Heim also suggested the asymptotic dimension formula for the space of cusp forms of weight k of degree 3. The notation $G \boxtimes h$ corresponds to a Siegel Hecke eigenform $F = G \boxtimes h$ such that $L(s, F, spin) = L(s, G \otimes h)$, and $L(s, G \otimes h)$ means the Rankin L-function defined by the product of the local Euler factors of corresponding L-functions of G and h, E_k is Eisenstein series.

Our results from Sections 2.2 and 2.3 make it possible to compare the spinor Hecke series of genus 4 (in spherical coordinates u_0, u_1, u_2, u_3, u_4) with the Rankin product of two Hecke series of genus 2 (in spherical coordinates x_0, x_1, x_2, y_0, y_1, y_2). It follows from our computation that if we make the substitution $u_0 = x_0\, y_0$, $u_1 = x_1$, $u_2 = x_2$, $u_3 = y_1$, $u_4 = y_2$, then the denominator of the series (2.23)

$$\sum_{\delta=0}^{\infty} \Omega_u^{(4)}(T(p^\delta))\, X^\delta \tag{3.18}$$

coincides with the denominator of the Rankin product (2.35)

$$\sum_{\delta=0}^{\infty} \Omega_x^{(2)}(\mathbf{T}(p^\delta)) \cdot \Omega_y^{(2)}(\mathbf{T}(p^\delta))\, X^\delta\,. \tag{3.19}$$

On the basis of this equality we formulate the following conjecture (see [PV09]):

Conjecture 3.6 (on a lifting from $\mathrm{GSp}_2 \times \mathrm{GSp}_2$ to GSp_4) *Let f and g be two Siegel modular forms of genus 2 and of weights $k > 4$ and $l = k-2$. Then there exists a Siegel modular form F of genus 4 and of weight k with the Satake parameters*

$$\gamma_0 = \alpha_0\beta_0,\ \gamma_1 = \alpha_1,\ \gamma_2 = \alpha_2,\ \gamma_3 = \beta_1,\ \gamma_4 = \beta_2,$$

for a suitable choice of Satake parameters α_0, α_1, α_2 and β_0, β_1, β_2 of f and g.

An evidence for the conjecture comes from Ikeda-Miyawaki constructions ([Ike01], [Mur02], [Ike06]). For an even positive integer k let $h \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ be a normalized Hecke eigenform of weight $2k$. Let $f \in \mathcal{S}_{k+n+r}(\mathrm{Sp}_r(\mathbb{Z}))$ be an arbitrary Siegel cusp eigenform of genus r and weight $k+n+r$, with $n, r \geqslant 1$. Then, according to Ikeda-Miyawaki (see [Ike06, Theorem 1.1]) there exists a Siegel eigenform $\mathcal{F}_{h,f} \in \mathcal{S}_{k+n+r}(\mathrm{Sp}_{2n+r}(\mathbb{Z}))$ such that

$$L(s, \mathcal{F}_{h,f}, stnd) = L(s, f, stnd) \prod_{j=1}^{2n} L(s+k+n-j, h) \tag{3.20}$$

(under a non-vanishing condition). The form $\mathcal{F}_{h,f}$ is given by the integral

$$\mathcal{F}_{h,f}(Z) = \langle F_{2n+2r} \left(\begin{smallmatrix} Z & 0 \\ 0 & Z' \end{smallmatrix}\right), f(Z') \rangle_{Z'}\,, \tag{3.21}$$

where $F_{2n} \in \mathcal{S}_{k+n}(\mathrm{Sp}_{2n}(\mathbb{Z}))$ is the Ikeda lift of h, in assumption that $k \equiv n \pmod 2$; for $n = 1$ it corresponds to the Maass lift $F_2 = Maass(h) \in \mathcal{S}_{k+1}(\mathrm{Sp}_2(\mathbb{Z}))$. The valid example of the conjecture is given by $n = 1$, $r = 2$, $k := k + 1$, $g = F_2$,

$$\begin{aligned} &(f, g) = (f, F_2) \mapsto \mathcal{F}_{f,h} \in \mathcal{S}_{k+3}(\mathrm{Sp}_4(\mathbb{Z}))\,, \\ &(f, g) = (f, F_2) \in \mathcal{S}_{k+3}(\mathrm{Sp}_2(\mathbb{Z})) \times \mathcal{S}_{k+1}(\mathrm{Sp}_2(\mathbb{Z}))\,. \end{aligned} \tag{3.22}$$

The L-function of degree 16 in Conjecture 3.6 is related to the tensor product L-function in [Jia96]. In the above example it coincides with the product of two shifted L-functions of degree 8 of Böcherer-Heim [BH06].

The conjecture 3.6 can be generalized as follows:

Conjecture 3.7 (on a lifting from $\mathrm{GSp}_{2m} \times \mathrm{GSp}_{2m}$ to GSp_{4m}) *Let f and g be two Siegel modular forms of genus $2m$ and of weights $k > 2m$ and $l = k - 2m$. Then there exists a Siegel modular form F of genus $4m$ and of weight k with the Satake parameters*

$$\gamma_0 = \alpha_0\beta_0,\ \gamma_1 = \alpha_1, \ldots, \gamma_{2m} = \alpha_{2m},\ \gamma_{2m+1} = \beta_1, \ldots, \gamma_{4m} = \beta_{2m},$$

for a suitable choice of Satake parameters α_0, α_1, …, α_{2m} and β_0, β_1, …, β_{2m} of f and g.

Once again, the evidence for this version of the conjecture comes from Ikeda-Miyawaki constructions. Let k be an even positive integer, $h \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ be a normalized Hecke eigenform of weight $2k$, $F_{2n} \in \mathcal{S}_{k+n}(\mathrm{Sp}_{2n}(\mathbb{Z}))$ be the Ikeda lift of h of genus $2n$ (we assume $k \equiv n \pmod 2$, $n \geqslant 1$). Consider an arbitrary Siegel cusp eigenform $f \in \mathcal{S}_{k+n+r}(\mathrm{Sp}_r(\mathbb{Z}))$ of genus r and weight $k + n + r$, with $r \geqslant 1$. If we take in (3.20) $n = m$, $r = 2m$, $k := k + m$, $k + n + r := k + 3m$, then a valid example of this version of the conjecture is given by

$$\begin{aligned} &(f, g) = (f, F_{2m}(h)) \mapsto \mathcal{F}_{h,f} \in \mathcal{S}_{k+3m}(\mathrm{Sp}_{4m}(\mathbb{Z}))\,, \\ &(f, g) = (f, F_{2m}(h)) \in \mathcal{S}_{k+3m}(\mathrm{Sp}_{2m}(\mathbb{Z})) \times \mathcal{S}_{k+m}(\mathrm{Sp}_{2m}(\mathbb{Z}))\,. \end{aligned} \tag{3.23}$$

Another evidence comes from the Siegel-Eisenstein series

$$f = E_k^{2m}\,, \quad g = E_{k-2m}^{2m} \tag{3.24}$$

of even genus $2m$ and weights k and $k-2m$. Their corresponding local Satake parameters are:

$$\begin{aligned} &\alpha_0 = 1,\ \alpha_1 = p^{k-2m},\ \ldots,\ \alpha_{2m} = p^{k-1}, \\ &\beta_0 = 1,\ \beta_1 = p^{k-4m},\ \ldots,\ \beta_{2m} = p^{k-2m-1}. \end{aligned} \tag{3.25}$$

The Siegel-Eisenstein series E_k^{4m} with Satake parameters

$$\gamma_0 = 1,\ \gamma_1 = p^{k-4m},\ \ldots,\ \gamma_{2m} = p^{k-1}, \tag{3.26}$$

will be the right choice of the form F in the conjecture.

3.2 Computing critical values for $L(s, F_{12}, spin)$

3.2.1 Preliminaries

We recall the basic definitions. Let $\mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$ be the upper half-plane. For a positive integer k and a Dirichlet character χ modulo a positive integer N such that $\chi(-1) = (-1)^k$, we denote by $\mathcal{M}_k(\Gamma_0(N), \chi)$ the vector space of all holomorphic modular forms $f(z)$ of weight k satisfying

$$f(\gamma(z)) = \chi(d)(cz+d)^k f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)\,, \tag{3.27}$$

where the variable $z \in \mathfrak{H}$, $\gamma(z) = \dfrac{az+b}{cz+d}$, and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}. \tag{3.28}$$

We denote by $\mathcal{S}_k(N, \chi)$ the subspace of $\mathcal{M}_k(\Gamma_0(N), \chi)$ consisting of all cusp forms. Every element f of $\mathcal{M}_k(\Gamma_0(N), \chi)$ has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a(n)\, q^n\,, \tag{3.29}$$

where $q = \exp(2\pi i z)$ and $a(n)$ are complex numbers in general.

The L-function associated to f is defined as $L(s, f) = \sum_{n=1}^{\infty} a(n)\, n^{-s}$. More generally, with an arbitrary Dirichlet character ω, the twisted L-function is defined as $L(s, f, \omega) = \sum_{n=1}^{\infty} a(n)\,\omega(n)\, n^{-s}$. These L-functions can be also written in the form of Euler product:

$$L(s, f) = \prod_{p \text{ prime}} (1 - a(p)\, p^{-s} + \chi(p)\, p^{k-1-2s})^{-1}\,, \tag{3.30}$$

$$L(s, f, \omega) = \prod_{p \text{ prime}} (1 - a(p)\,\omega(p)\, p^{-s} + \chi(p)\,\omega(p)^2\, p^{k-1-2s})^{-1}\,. \tag{3.31}$$

Next, the Dirichlet L-series for any character χ of conductor N is given by

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)\, n^{-s} \tag{3.32}$$

and its Euler product

$$L(s,\chi) = \prod_{p \nmid N} \frac{1}{1-\chi(p)\, p^{-s}}\,. \tag{3.33}$$

In the case, when χ is the identity Dirichlet character, the latter series is Riemann's zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Let $g(z) = \sum_{n=0}^{\infty} b(n)\, q^n \in \mathcal{M}_l(\Gamma_0(N), \xi)$ be another modular form of weight l with Fourier coefficients $b(n)$. The L function associated to two modular forms f and g is given by the additive convolution

$$L(s,f,g) = \sum_{n=1}^{\infty} a(n)\, b(n)\, n^{-s}\,. \tag{3.34}$$

Another type of L-functions associated to two modular forms is Rankin's product L-function (multiplicative convolution). It is denoted by $L(s, f \otimes g)$ and defined as (see [Shi76, page 786]):

$$L(s, f\otimes g) = L_N(2s+2-k-l, \chi\xi)\, L(s,f,g)\,, \tag{3.35}$$

where $L_N(s,\omega)$ with a Dirichlet character ω modulo N is defined, as usual, in (3.32) with $\omega(n) = 0$ for $(n,N) \neq 1$, and the Euler factors in (3.33), corresponding to the prime divisors of a number N, have been omitted. Note, that in the case, when f and g are cusp eigenforms, the lefthand side of (3.35) is an Euler product of degree 4.

For two elements $f, h \in \mathcal{M}_k(\Gamma_0(N))$ such that fh is a cusp form, the Petersson inner product $\langle f, h\rangle$ is defined as

$$\langle f,h\rangle = \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]} \int_{\Phi_N} \overline{f(z)}\, h(z)\, y^k\, \frac{dx\, dy}{y^2}\,, \tag{3.36}$$

where $z = x + iy$, Φ_N is a fundamental domain for $\mathfrak{H}$ modulo $\Gamma_0(N)$ and the bar denotes the complex conjugate. We also define $\langle f, h\rangle$ by (3.36) for nearly holomorphic modular forms f and h on $\mathfrak{H}$ whenever the integral is convergent (see [Shi07, section 8.2] for definition and properties of the nearly holomorphic modular forms).

We conduct a computation of (3.15) separately for two components $L(s-9, \Delta)\, L(s-10, \Delta)$ and $L(s, \Delta \otimes g_{20})$ each time applying the Rankin-Selberg method.

3.2.2 Rankin-Selberg method

To compute the special values of L-functions we use the "unfolding method" invented by Rankin and Selberg in their papers of 1939-40 [Ran39, Sel40]. There are three principal steps in the application of this method:

▷ Rankin's Euler product of degree 4:

$$L(s, f \otimes g) = L_N(2s + 2 - k - l, \chi\xi)\, L(s, f, g)\,;$$

▷ Integral convolution:

$$(4\pi)^{-s}\,\Gamma(s)\, L(s, f, g) = \int_0^\infty \int_{-1/2}^{1/2} \overline{f_\rho}\, g\, y^{s-1}\, dx\, dy\,;$$

▷ Passage to the fundamental domain:

$$(4\pi)^{-s}\,\Gamma(s)\, L(s, f, g) = \int_{\Phi_N} \overline{f_\rho}\, g\, E^*_{k-l,N}(z, s + 1 - k, \chi\xi)\, y^{s-1}\, dx\, dy\,,$$

where

$z = x + iy$, $\quad k > l$ are the weights of f and g,

$f_\rho(z) = \overline{f(-\overline{z})} = \sum \overline{a_n}\, q^n\,,$

$E^*_{\lambda,N}(z, s, \omega) = \displaystyle\sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} \omega(d)\,(cz + d)^{-\lambda}\,|cz + d|^{-2s}, \quad \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\,,$

Φ_N is a fundamental domain for $\Gamma_0(N)\backslash\mathfrak{H}$ and $\Gamma_\infty = \{\pm \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) : m \in \mathbb{Z}\}\,,$

ω is a Dirichlet character modulo N such that $\omega(-1) = (-1)^\lambda\,.$

The Rankin's convolution L-function $L(s, f \otimes g) = L_N(2s + 2 - k - l, \chi\xi)\, L(s, f, g)$ has the Euler product of degree 4 in the view of the following lemma:

Lemma 3.8 (Lemma 1, [Shi76]) *Suppose we have formally*

$$\sum_{n=1}^{\infty} A(n)\, n^{-s} = \prod_p \left[(1 - \alpha_p\, p^{-s})(1 - \alpha'_p\, p^{-s})\right]^{-1}$$

and

$$\sum_{n=1}^{\infty} B(n)\, n^{-s} = \prod_p \left[(1 - \beta_p\, p^{-s})(1 - \beta'_p\, p^{-s})\right]^{-1}\,.$$

Then

$$\sum_{n=1}^{\infty} A(n)\, B(n)\, n^{-s} = \prod_p \frac{1 - \alpha\alpha'\beta\beta' p^{-2s}}{(1 - \alpha\beta p^{-s})(1 - \alpha\beta' p^{-s})(1 - \alpha'\beta p^{-s})(1 - \alpha'\beta' p^{-s})}\,.$$

The integral representation is actually reduced to the multiplication by Γ-function:

$$\begin{aligned}
&\int_0^\infty \int_{-1/2}^{1/2} \overline{f_\rho}\, g\, y^{s-1}\, dx\, dy \\
&\quad = \int_0^\infty \int_{-1/2}^{1/2} y^{s-1} \sum_{n_1} a_{n_1} \mathrm{e}^{-2\pi i n_1 \overline{z}} \sum_{n_2} b_{n_2} \mathrm{e}^{2\pi i n_2 z}\, dx\, dy \\
&\quad = \int_0^\infty \int_{-1/2}^{1/2} y^{s-1} \sum_{n_1, n_2} a_{n_1}\, b_{n_2}\, \mathrm{e}^{2\pi i(-n_1+n_2)x}\, \mathrm{e}^{-2\pi i(n_1+n_2)y}\, dx\, dy \\
&\quad = \sum_n a_n\, b_n \int_0^\infty y^{s-1}\, \mathrm{e}^{-4\pi i n y}\, dy \\
&\quad = \sum_n a_n\, b_n\, (4\pi n)^{-s} \int_0^\infty (4\pi n y)^{s-1}\, \mathrm{e}^{-4\pi i n y}\, d(4\pi n y) \\
&\quad = (4\pi)^{-s}\, \Gamma(s) \sum_n a_n\, b_n\, n^{-s} \;=\; (4\pi)^{-s}\, \Gamma(s)\, L(s, f, g)\,.
\end{aligned} \tag{3.37}$$

Finally, the integration in the rectangular $\left\{|x| \leqslant \frac{1}{2},\, y > 0\right\}$ area is based on the explicit definition of Eisenstein series and interchange of summations and integration. The invariance of $(y^{-2}\, dx\, dy)$ with respect to modular substitutions is used to unfold the fundamental domain.

Let

$$R = \Gamma_\infty \backslash \Gamma_0(N) = \begin{pmatrix} * & * \\ N m_1 & n_1 \end{pmatrix},$$

where

$$\begin{array}{ll} (m_1, n_1) = 1 & \text{if } m_1 > 0, \\ n_1 = 1 & \text{if } m_1 = 0. \end{array}$$

Consider the area $\mathfrak{S} = \left\{|x| \leqslant \frac{1}{2},\, y > 0\right\} = \Gamma_\infty \backslash \mathfrak{H}$ and $\Phi_N = \Gamma_0(N) \backslash \mathfrak{H}$. Then $\mathfrak{S} = \bigcup_{\gamma \in R} \gamma \Phi_N$. The integration in the area $\mathfrak{S}$ can be performed as follows:

$$
\begin{aligned}
&\int_0^\infty \int_{-1/2}^{1/2} \overline{f_\rho(z)}\, g(z)\, y^{s-1}\, dx\, dy \\
&\quad = \int_0^\infty \int_{-1/2}^{1/2} \overline{f_\rho(z)}\, g(z)\, y^{s+1}\, \frac{dx\, dy}{y^2} \\
&\quad = \sum_{\gamma\in R} \int_{\gamma\Phi_N} \overline{f_\rho(z)}\, g(z)\, y^{s+1}\, (y^{-2}\, dx\, dy) \\
&\quad = \int_{\Phi_N} \sum_{\gamma\in R} \overline{f_\rho(\gamma z)}\, g(\gamma z)\, y(\gamma z)^{s+1}\, \frac{dx\, dy}{y^2} \\
&\quad = \int_{\Phi_N} \sum_{\gamma\in R} \overline{f_\rho(z)}\, g(z)\, \chi\xi(d)\, (cz+d)^{-k+l} |cz+d|^{-2s-2+2k}\, y^{s+1}\, \frac{dx\, dy}{y^2} \\
&\quad = \int_{\Phi_N} \overline{f_\rho(z)}\, g(z) \left[\sum_{\gamma\in R} \chi\xi(d)\, (cz+d)^{-(k-l)} |cz+d|^{-2(s+1-k)} \right] y^{s-1}\, dx\, dy \\
&\quad = \int_{\Phi_N} \overline{f_\rho(z)}\, g(z)\, E_{k-l,N}(z, s+1-k, \chi\xi)\, y^{s-1}\, dx\, dy\,.
\end{aligned}
\tag{3.38}
$$

Also

$$
\begin{aligned}
E_{\lambda,N}(z,s,\omega) &= {\sum_{(n,m)}}' \omega(n)\, (mNz+n)^{-\lambda} |mNz+n|^{-2s} \\
&= \sum_{d=1}^\infty \sum_{(n_1,m_1)=1} \omega(dn_1)\, (dm_1Nz+dn_1)^{-\lambda} |dm_1Nz+dn_1|^{-2s} \\
&= \sum_{d=1}^\infty \omega(d)\, d^{-\lambda-2s} \sum_{(n_1,m_1)=1} \omega(n_1)\, (m_1Nz+n_1)^{-\lambda} |m_1Nz+n_1|^{-2s} \\
&= 2\, L_N(2s+\lambda,\omega)\, E^*_{\lambda,N}(z,s,\omega)\,,
\end{aligned}
\tag{3.39}
$$

where $m = dm_1$ and $n = dn_1$. Hence, comparing (3.37) and (3.38), we have (see also [Shi76, (2.4)])

$$
2\,(4\pi)^{-s}\,\Gamma(s)\, L(s, f\otimes g) = \int_{\Phi_N} \overline{f_\rho}\, g\, E_{k-l,N}(z, s+1-k, \chi\xi)\, y^{s-1}\, dx\, dy\,. \tag{3.40}
$$

3.2.3 The expression for $L(s,\Delta)\,L(s-1,\Delta)$

Let $f=\Delta$ be Ramanujan's discriminant modular form of weight $k=12$:

$$\begin{aligned} f(z)=\Delta(z)&=\sum_{n=1}^{\infty}\tau(n)\,q^n=q\prod_{n=1}^{\infty}(1-q^n)^{24}\\ &=q-24\,q^2+252\,q^3-1472\,q^4+4830\,q^5-6048\,q^6+\cdots\,, \end{aligned} \tag{3.41}$$

where $\tau(n)$ is Ramanujan's tau function. The associated L-function is

$$L(s,f)=\sum_{n=1}^{\infty}\tau(n)\,n^{-s}=\prod_{p}\left(1-\tau(p)\,p^{-s}+p^{11-2s}\right)^{-1}\,. \tag{3.42}$$

Let $G_2(z)=-\dfrac{1}{24}+\sum_{n=1}^{\infty}\sigma_1(n)\,q^n=-\dfrac{1}{24}+q+3\,q^2+4\,q^3+7\,q^4+\cdots$, where $\sigma_1(n)=\sum_{d|n}d$ is the divisor function defined as the sum of the divisors of n. Consider the Eisenstein series (see [Miy06, Lemma 7.2.19, (2)])

$$g(z)=G_{2,p}(z)=G_2(z)-p\,G_2(pz)=\frac{p-1}{24}+\sum_{n=1}^{\infty}\sum_{\substack{d|n\\ p\nmid d}}d\,q^n\,, \tag{3.43}$$

of weight 2 for $\Gamma_0(p)$ and the corresponding L series

$$\begin{aligned} L(s,g)&=\sum_{n=1}^{\infty}\sum_{\substack{d|n\\ p\nmid d}}d\,n^{-s}=\sum_{\substack{d,d_1\geqslant 1\\ p\nmid d}}d\,(d\,d_1)^{-s}=\sum_{\substack{d\geqslant 1\\ p\nmid d}}d^{1-s}\sum_{d_1\geqslant 1}d_1^{-s}\\ &=(1-p^{1-s})\,\zeta(s-1)\,\zeta(s)\,. \end{aligned} \tag{3.44}$$

Put $p=2$, then

$$\begin{aligned} g(z)=G_{2,2}(z)&=G_2(z)-2\,G_2(2z)\\ &=\frac{1}{24}+q+q^2+4\,q^3+q^4+6\,q^5+4\,q^6+\cdots\,, \end{aligned} \tag{3.45}$$

and

$$L(s,g)=(1-2^{1-s})\,\zeta(s-1)\,\zeta(s)\,. \tag{3.46}$$

For $f=\Delta=\sum\tau(n)\,q^n\in S_{12}(2)$ and $g=G_{2,2}=\sum b(n)\,q^n\in\mathcal{M}_2(\Gamma_0(2),\xi)$ we have $k=12$ and $l=2$. Put $N=2$, $\chi=1$ and

$$\xi(n)=(1 \bmod N)(n)=\begin{cases}1, & \text{if } n \text{ odd;}\\ 0, & \text{if } n \text{ even.}\end{cases} \tag{3.47}$$

Assume $1-\tau(p)\,X+p^{11}\,X^2=(1-\alpha_p\,X)(1-\alpha'_p\,X)$, then $\alpha_p+\alpha'_p=\tau(p)$, $\alpha_p\,\alpha'_p=p^{11}$, and

$$L(s,f)=\prod_p\left((1-\alpha_p\,p^{-s})(1-\alpha'_p\,p^{-s})\right)^{-1}\,. \tag{3.48}$$

Similarly, consider

$$\begin{aligned}L(s,g)&=\sum_{n=1}^{\infty}b(n)\,n^{-s}=(1-2^{1-s})\,\zeta(s-1)\,\zeta(s)\\&=(1-2^{1-s})\prod_p\left((1-p^{1-s})\,(1-p^{-s})\right)^{-1}\\&=\prod_p\left((1-\beta_p\,p^{-s})\,(1-\beta'_p\,p^{-s})\right)^{-1}\,,\end{aligned} \tag{3.49}$$

where $\beta(p)=1$ for all p, $\beta'(2)=0$ and $\beta'(p)=p$ for all odd primes. By definition and using Lemma 3.8

$$\begin{aligned}&L(s,\Delta\otimes G_{2,2})=L_2(2s+2-12-2,\psi)\,L(s,f,g)\\&=\prod_{p\neq2}(1-p^{12-2s})^{-1}\,\cdot\sum_{n=1}^{\infty}\tau(n)\,b(n)\,n^{-s}\\&=\prod_{p\neq2}(1-p^{12-2s})^{-1}\times\\&\quad\times\prod_p\frac{1-\alpha_p\,\alpha'_p\,\beta_p\,\beta'_p\,p^{-2s}}{(1-\alpha_p\,\beta_p\,p^{-s})\,(1-\alpha'_p\,\beta_p\,p^{-s})\,(1-\alpha_p\,\beta'_p\,p^{-s})\,(1-\alpha'_p\,\beta'_p\,p^{-s})}\\&=\frac{1}{(1-\alpha_2\,2^{-s})\,(1-\alpha'_2\,2^{-s})}\times\\&\quad\times\prod_{p\neq2}\frac{(1-p^{12-2s})^{-1}\,(1-p^{11}\,p\,p^{-2s})}{(1-\alpha_p\,p^{-s})\,(1-\alpha'_p\,p^{-s})\,(1-\alpha_p\,p\,p^{-s})\,(1-\alpha'_p\,p\,p^{-s})}\\&=\frac{1}{(1-\alpha_2\,2^{-s})\,(1-\alpha'_2\,2^{-s})}\times\\&\quad\times\prod_{p\neq2}\frac{1}{\left((1-\alpha_p\,p^{-s})\,(1-\alpha'_p\,p^{-s})\right)\,\left((1-\alpha_p\,p^{1-s})\,(1-\alpha'_p\,p^{1-s})\right)}\\&=\prod_p\frac{1}{(1-\alpha_p\,p^{-s})\,(1-\alpha'_p\,p^{-s})}\prod_{p\neq2}\frac{1}{(1-\alpha_p\,p^{1-s})\,(1-\alpha'_p\,p^{1-s})}\\&=L(s,\Delta)\,L(s-1,\Delta)\,(1-\tau(2)\,2^{1-s}+2^{11}\,2^{2-2s})\\&=(1+3\cdot2^{4-s}+2^{13-2s})\,L(s,\Delta)\,L(s-1,\Delta)\,.\end{aligned} \tag{3.50}$$

Finally, we obtain the following identity

$$L(s,\Delta)\,L(s-1,\Delta) = \frac{L(s,\Delta\otimes G_{2,2})}{(1+3\cdot 2^{4-s}+2^{13-2s})}\,. \tag{3.51}$$

3.2.4 Computation of $L(s, \Delta \otimes G_{2,2})$

Now we express $L(s,\Delta\otimes G_{2,2})$ (at integral points $s=3,\dots,10$) as a multiple of Petersson inner product $\langle\Delta,\Delta\rangle$. Using (3.40),

$$\begin{aligned}
&L(s,\Delta\otimes G_{2,2})\\
&=\frac{(4\,\pi)^s}{2\,\Gamma(s)}\int_{\Phi_2}\overline{\Delta(z)}\,G_{2,2}(z)\,E_{10,2}(z,s-11,\xi)\,y^{s-1}\,dx\,dy\\
&=\frac{(4\,\pi)^s}{2\,\Gamma(s)}\int_{\Phi_2}\overline{\Delta(z)}\,G_{2,2}(z)\,E_{10,2}(z,s-11,\xi)\,y^{s-11}\,y^{10}\,dx\,dy\\
&=\frac{(4\,\pi)^s\,[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(2)]}{2\,\Gamma(s)}\left\langle\Delta(z),G_{2,2}(z)\,y^{s-11}\,E_{10,2}(z,s-11,\xi)\right\rangle\\
&=\frac{3}{2}\frac{(4\,\pi)^s}{\Gamma(s)}\left\langle\Delta(z),\mathcal{H}ol\left(G_{2,2}(z)\,y^{s-11}\,E_{10,2}(z,s-11,\xi)\right)\right\rangle\\
&=\frac{3}{2}\frac{(4\,\pi)^{11}}{\Gamma(s)}\left\langle\Delta(z),\mathcal{H}ol\left(G_{2,2}(z)\,(4\pi y)^{s-11}\,E_{10,2}(z,s-11,\xi)\right)\right\rangle\,,
\end{aligned} \tag{3.52}$$

where $\langle f,g\rangle$ is the Petersson inner product (3.36), Φ_2 denotes a fundamental domain for $\Gamma_0(2)\backslash\mathfrak{H}$, $z=x+iy$,

$$E_{\lambda,N}(z,s,\xi)=\sum_{(m,n)}{}'\,\xi(n)\,(mNz+n)^{-\lambda}|mNz+n|^{-2s}\,, \tag{3.53}$$

$\sum'$ denotes the summation over all $(m,n)\in\mathbb{Z}^2$, $(m,n)\neq(0,0)$, $\mathcal{H}ol(F)$ is the operator of holomorphic projection (see [Stu80] and [CP04, (2.148)]). It is defined so, that $\langle f,F\rangle=\langle f,\mathcal{H}ol(F)\rangle$ for all $f\in\mathcal{S}_k(N,\psi)$.

In order to compute the holomorphic projection of the product in the last identity of (3.52) $\mathcal{H}ol\left(G_{2,2}(z)\,(4\pi y)^{s-11}\,E_{10,2}(z,s-11,\xi)\right)$ we write the Fourier expansion for $E_{10,2}(z,s-11,\xi)$ in the convenient form using the Whittaker functions by applying the Proposition 2.2 of [Pan03], where in

notations of that proposition

$$\begin{aligned}
&s \in \{3, \dots, 10\}\,, \quad s-11<0\,, \quad s-11+10 = s-1>0\,,\\
&a=0\,, \quad b=1\,, \quad \delta(\frac{a}{N})=1\,,\\
&\mathbf{E}_{10,2}(z, s-11, 0, 1) = E_{10,2}(z, s-11, \xi)\,,\\
&\zeta(s;0,2) = \sum_{0<n\equiv 0(2)} n^{-s} = \sum_{n=1}^{\infty}(2n)^{-s} = 2^{-s}\zeta(s)\,,\\
&\zeta(s;1,2) = \sum_{0<n\equiv 1(2)} n^{-s} = \zeta(s)-\zeta(s;0,2) = (1-2^{-s})\zeta(s)\,.
\end{aligned}$$

The Whittaker function $W(y,\alpha,\beta)$ (see [Pan03, (2.4)], for example) is defined as

$$W(y,\alpha,\beta) = \Gamma(\beta)^{-1}\int_0^{+\infty}(u+1)^{\alpha-1}\,u^{\beta-1}\,\mathrm{e}^{-yu}\,du \tag{3.54}$$

for $y>0$, $\alpha,\beta\in\mathbb{C}$ with $\Re(\beta)>0$ and for arbitrary α and β this function is defined by the analytic continuation and the functional equation:

$$W(y,\alpha,\beta) = y^{1-\alpha-\beta}\,W(y,1-\beta,1-\alpha)\,. \tag{3.55}$$

For a non negative integer r, we have

$$W(y,\alpha,-r) = \sum_{i=0}^{r}\frac{(-1)^i\binom{r}{i}\Gamma(\alpha)}{\Gamma(\alpha-i)}\,y^{r-i}\,. \tag{3.56}$$

Therefore,

$$\begin{aligned}
&(4\pi y)^{s-11}\,E_{10,2}(z,s-11,\xi)\\
&= (4\pi y)^{s-11}\,2\,\zeta(2s-12;1,2)\\
&\quad + (4\pi y)^{s-11}\,\frac{(-2\pi i)^{2s-12}\,(-1)^{s-11}\Gamma(2s-13)}{(4\pi y)^{2s-13}\,2\,\Gamma(s-1)\,\Gamma(s-11)}\,2\,\zeta(2s-13;0,2)\\
&\quad + (4\pi y)^{s-11}\,\frac{(-2\pi i)^{2s-12}\,(-1)^{s-11}}{2^{2s-12}\Gamma(s-1)}\times\\
&\qquad \times\sum_{n=1}^{\infty}\sum_{\pm d|n}\mathrm{sgn}(d)\,d^{\,2s-13}\,\mathrm{e}^{\pi i d}\,W(4\pi n y, s-1, s-11)\,q^n\\
&= 2\,(4\pi y)^{s-11}\,(1-2^{12-2s})\,\zeta(2s-12)\\
&\quad - (4\pi y)^{2-s}\frac{2\pi^{2s-12}\,\Gamma(2s-13)\,\zeta(2s-13)}{\Gamma(s-11)\,\Gamma(s-1)}\\
&\quad - (4\pi y)^{s-11}\frac{2\pi^{2s-12}}{\Gamma(s-1)}\sum_{n=1}^{\infty}\sum_{d|n}(-1)^d d^{\,2s-13}\,W(4\pi n y, s-1, s-11)\,q^n\,.
\end{aligned} \tag{3.57}$$

Let

$$\begin{aligned} C_0' &= C_0'(s) = (-1)\frac{2\,\pi^{2s-12}\,\Gamma(2s-13)\,\zeta(2s-13)}{\Gamma(s-11)\,\Gamma(s-1)}\,, \\ C_0'' &= C_0''(s) = (2-2^{13-2s})\,\zeta(2s-12)\,, \\ C_1 &= C_1(s) = 2\,\pi^{2s-12}\,, \\ C_2 &= C_2(s) = (2-2^{2s-12})\,\pi^{2s-12}\,, \end{aligned} \tag{3.58}$$

then

$$\begin{aligned} &(4\pi y)^{s-11}\,E_{10,2}(z, s-11, \xi) \\ &\quad = C_0'\,(4\pi y)^{2-s} + C_0''\,(4\pi y)^{s-11} \\ &\qquad + C_1\,\frac{W(4\pi y, s-1, s-11)}{\Gamma(s-1)}(4\pi y)^{s-11}\,q \\ &\qquad + C_2\,\frac{W(8\pi y, s-1, s-11)}{\Gamma(s-1)}(4\pi y)^{s-11}\,q^2 + \cdots\,. \end{aligned} \tag{3.59}$$

Recall that $G_{2,2}(z) = 1/24 + q + q^2 + \cdots$ by (3.45). We write the Fourier coefficients $\widetilde{A}_i(s,y)$ for the product $F = G_{2,2}(z)\,(4\pi y)^{s-11}\,E_{10,2}(z, s-11, \xi) = \sum \widetilde{A}_n(s,y)q^n$ in order to apply the Holomorphic Projection Lemma [GZ86, Proposition (5.1)] to find the image of the projection operator $\mathcal{H}ol(F) = \sum A_n(s)q^n$ (the Lemma is originally due to Sturm [Stu80]). It should be noted, that the relevant polynomial decay hypotheses of the Lemma are satisfied for all actions $E_{10,2}(z, s-11, \xi)|\gamma$ of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and at each critical point s, see [Pan03, (2.3)].

We need to compute just two coefficients $A_1 = A_1(s)$ and $A_2 = A_2(s)$ since the result of the holomorphic projection belongs to the space of cusp forms for the subgroup $\Gamma_0(2)$, which has the dimension 2. Then we find the linear combination representing $\mathcal{H}ol(F)$ in the basis $\{\Delta(z), \Delta(2z)\}$:

$$\mathcal{H}ol(F) = \alpha \cdot \Delta(z) + \beta \cdot \Delta(2z)\,. \tag{3.60}$$

Namely, the computation of A_1 and A_2 gives:

$$\begin{aligned}
A_1 &= \frac{C_0'}{10!}\int_0^{+\infty}(4\pi y)^{2-s}\,\mathrm{e}^{-4\pi y}\,(4\pi y)^{10}\,d(4\pi y)\\
&\quad+\frac{C_0''}{10!}\int_0^{+\infty}(4\pi y)^{s-11}\,\mathrm{e}^{-4\pi y}\,(4\pi y)^{10}\,d(4\pi y)\\
&\quad+\frac{C_1}{24\cdot 10!}\int_0^{+\infty}\frac{W(4\pi y,s-1,s-11)}{\Gamma(s-1)}(4\pi y)^{s-11}\,\mathrm{e}^{-4\pi y}\,(4\pi y)^{10}\,d(4\pi y)\\
&=\frac{\Gamma(13-s)}{10!}\,C_0'+\frac{\Gamma(s)}{10!}\,C_0''\\
&\quad+\frac{C_1}{24\cdot 10!}\int_0^{+\infty}\sum_{i=0}^{11-s}\frac{(-1)^i\binom{11-s}{i}(4\pi y)^{10-i}}{\Gamma(s-1-i)}\,\mathrm{e}^{-4\pi y}\,d(4\pi y)\\
&=\frac{\Gamma(13-s)}{10!}\,C_0'+\frac{\Gamma(s)}{10!}\,C_0''+\frac{C_1}{24\cdot 10!}\sum_{i=0}^{11-s}\frac{(-1)^i\binom{11-s}{i}\Gamma(11-i)}{\Gamma(s-1-i)}\,,
\end{aligned}\tag{3.61}$$

$$\begin{aligned}
A_2 &= \frac{C_0'}{10!}\int_0^{+\infty}(4\pi y)^{2-s}\,\mathrm{e}^{-8\pi y}\,(8\pi y)^{10}\,d(8\pi y)\\
&\quad+\frac{C_0''}{10!}\int_0^{+\infty}(4\pi y)^{s-11}\,\mathrm{e}^{-8\pi y}\,(8\pi y)^{10}\,d(8\pi y)\\
&\quad+\frac{C_1}{10!}\int_0^{+\infty}\frac{W(4\pi y,s-1,s-11)}{\Gamma(s-1)}(4\pi y)^{s-11}\,\mathrm{e}^{-8\pi y}\,(8\pi y)^{10}\,d(8\pi y)\\
&\quad+\frac{C_2}{24\cdot 10!}\int_0^{+\infty}\frac{W(8\pi y,s-1,s-11)}{\Gamma(s-1)}(4\pi y)^{s-11}\,\mathrm{e}^{-8\pi y}\,(8\pi y)^{10}\,d(8\pi y)\\
&=\frac{C_0'}{10!}\,2^{s-2}\int_0^{+\infty}(8\pi y)^{12-s}\,\mathrm{e}^{-8\pi y}\,d(8\pi y)+\frac{C_0''}{10!}\,2^{11-s}\int_0^{+\infty}(8\pi y)^{s-1}\,\mathrm{e}^{-8\pi y}\,d(8\pi y)\\
&\quad+\frac{C_1}{10!}\int_0^{+\infty}\sum_{i=0}^{11-s}\frac{(-1)^i\binom{11-s}{i}(4\pi y)^{11-s-i}}{\Gamma(s-1-i)}\,(4\pi y)^{s-11}\,\mathrm{e}^{-8\pi y}\,(8\pi y)^{10}\,d(8\pi y)\\
&\quad+\frac{C_2}{24\cdot 10!}\int_0^{+\infty}\sum_{i=0}^{11-s}\frac{(-1)^i\binom{11-s}{i}(8\pi y)^{11-s-i}}{\Gamma(s-1-i)}\,(4\pi y)^{s-11}\,\mathrm{e}^{-8\pi y}\,(8\pi y)^{10}\,d(8\pi y)\\
&=\frac{\Gamma(13-s)}{10!}\,2^{s-2}\,C_0'+\frac{\Gamma(s)}{10!}\,2^{11-s}\,C_0''+\frac{C_1}{10!}\sum_{i=0}^{11-s}2^i\,\frac{(-1)^i\binom{11-s}{i}\Gamma(11-i)}{\Gamma(s-1-i)}\\
&\quad+\frac{C_2}{24\cdot 10!}\,2^{11-s}\sum_{i=0}^{11-s}\frac{(-1)^i\binom{11-s}{i}\Gamma(11-i)}{\Gamma(s-1-i)}\,.
\end{aligned}\tag{3.62}$$

These Fourier coefficients are rational numbers up to the factor π^{2s-12} for each $s \in \{3, \ldots, 10\}$, see Table 3.1.

Next, we compute α and β in the linear combination (3.60) by comparing the coefficients A_1 and A_2 corresponding to terms q and q^2 with the equivalent linear combination of coefficients of our basis functions $\Delta(z) = q - 24q^2 + \ldots$ and $\Delta(2z) = q^2 + \ldots$:

$$\begin{cases} A_1 = \alpha \cdot 1 + \beta \cdot 0 \\ A_2 = \alpha \cdot (-24) + \beta \cdot 1 \end{cases} \tag{3.63}$$

Upon resolving this system of linear equations, we have

$$\begin{aligned} \alpha &= A_1 \\ \beta &= 24\, A_1 + A_2\,, \end{aligned} \tag{3.64}$$

therefore, we obtain the following identity for the Rankin's convolution of Δ and $G_{2,2}$ (3.52):

$$\begin{aligned} &L(s, \Delta \otimes G_{2,2}) \\ &\quad = \frac{3}{2} \frac{(4\pi)^{11}}{\Gamma(s)} \left(A_1(s) \left\langle \Delta(z), \Delta(z) \right\rangle + \left(24\, A_1(s) + A_2(s)\right) \left\langle \Delta(z), \Delta(2z) \right\rangle \right). \end{aligned} \tag{3.65}$$

Table 3.1: Fourier coefficient of $\mathcal{H}ol\left(G_{2,2}(z)\,(4\pi y)^{s-11}\, E_{10,2}(z, s-11, \xi)\right)$

s	π-factor	$A_1(s)$	$A_2(s)$
3	π^{-6}	$\frac{1}{50}$	$\frac{76}{25}$
4	π^{-4}	$\frac{1}{270}$	$\frac{56}{135}$
5	π^{-2}	$\frac{1}{1440}$	$\frac{1}{20}$
6	π^{0}	$\frac{1}{6048}$	$\frac{5}{756}$
7	π^{2}	$\frac{1}{16800}$	$\frac{1}{900}$
8	π^{4}	$\frac{17}{518400}$	$\frac{13}{64800}$
9	π^{6}	$\frac{11}{453600}$	$\frac{-1}{56700}$
10	π^{8}	$\frac{13}{604800}$	$\frac{-1}{10800}$

We simplify the obtained expression even further. Recall that

$$\Delta(2z) = 2^{-k/2}\,\Delta(z)|_k \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) , \tag{3.66}$$

where $k = 12$ is the weight of Δ. Then

$$\langle \Delta(z), \Delta(2z) \rangle = 2^{-6} \left\langle \Delta(z), \Delta(z)|_k \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle . \tag{3.67}$$

Consider $\gamma \in \Gamma_0(2)\backslash\Gamma$, $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. The summation over all γ gives

$$\begin{aligned} \langle \Delta(z), \Delta(2z) \rangle &= 2^{-6}[\Gamma : \Gamma_0(2)]^{-1} \sum_{\gamma} \left\langle \Delta(z)|\gamma, \Delta(z)|_k \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \gamma \right\rangle \\ &= 2^{-6} 3^{-1} \left\langle \Delta(z), \mathsf{Tr}^{(2)} \left(\Delta(z)|_k \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) \right\rangle . \end{aligned} \tag{3.68}$$

The trace operator $\mathsf{Tr}^{(N)} : \mathcal{M}_k(\Gamma_0(N)) \to \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ is defined as the action $f \to \sum_{\gamma \in \Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})} f|_k\gamma$. We have (see [Ser73])

$$\mathsf{Tr}^{(2)} \left(\Delta(z)|_k \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) = 2^{-5}\, T_2(\Delta) \tag{3.69}$$

where T_2 is the Hecke operator, therefore,

$$\begin{aligned} \langle \Delta(z), \Delta(2z) \rangle &= 2^{-6} 3^{-1} \left\langle \Delta(z), 2^{-5}\, T_2\left(\Delta(z)\right) \right\rangle \\ &= 2^{-11} 3^{-1} \left\langle \Delta(z), \tau(2)\, \Delta(z) \right\rangle \\ &= -\frac{1}{256} \left\langle \Delta(z), \Delta(z) \right\rangle . \end{aligned} \tag{3.70}$$

Substituting the last identity into (3.65), we obtain the final expression:

$$L(s, \Delta \otimes G_{2,2}) = \frac{3}{2} \frac{(4\pi)^{11}}{\Gamma(s)} \frac{(232\, A_1(s) - A_2(s))}{256} \langle \Delta, \Delta \rangle . \tag{3.71}$$

3.2.5 Result for $L(s-9, \Delta)\, L(s-10, \Delta)$

Combining together (3.51) and (3.71) we obtain the expression for the product $L(s-9, \Delta)\, L(s-10, \Delta)$:

$$L(s-9, \Delta)\, L(s-10, \Delta) = \frac{3 \cdot 2^{13} \pi^{11} (232\, A_1(s-9) - A_2(s-9))}{(1 + 3 \cdot 2^{13-s} + 2^{31-2s})\, \Gamma(s-9)} \langle \Delta, \Delta \rangle . \tag{3.72}$$

Now we evaluate this result in the form $L(s-9, \Delta)\, L(s-10, \Delta) = R_\Delta(s)\, P_\Delta(s)\, \langle \Delta, \Delta \rangle$ for each $s \in \{12, \ldots, 19\}$ computing the rational coefficient R_Δ and the corresponding power of π, see Table 3.2. The numerical value of the Petersson inner product

$$\langle \Delta, \Delta \rangle = 0.000001035362056 \tag{3.73}$$

is computed in the section 3.2.8.

Table 3.2: $L(s-9,\Delta)\,L(s-10,\Delta)$

s	R_Δ	P_Δ	$L(s-9,\Delta)\,L(s-10,\Delta)$
12	$\frac{32768}{225} = \frac{2^{15}}{3^2\cdot 5^2}$	π^5	0.046143339818118
13	$\frac{4096}{81} = \frac{2^{12}}{3^4}$	π^7	0.158130732552033
14	$\frac{2048}{189} = \frac{2^{11}}{3^3\cdot 7}$	π^9	0.334433094416363
15	$\frac{8192}{4725} = \frac{2^{13}}{3^3\cdot 5^2\cdot 7}$	π^{11}	0.528115574483468
16	$\frac{16384}{70875} = \frac{2^{14}}{3^4\cdot 5^3\cdot 7}$	π^{13}	0.694972239760782
17	$\frac{8192}{297675} = \frac{2^{13}}{3^5\cdot 5^2\cdot 7^2}$	π^{15}	0.816559651925946
18	$\frac{8192}{2679075} = \frac{2^{13}}{3^7\cdot 5^2\cdot 7^2}$	π^{17}	0.895457859377812
19	$\frac{65536}{200930625} = \frac{2^{16}}{3^8\cdot 5^4\cdot 7^2}$	π^{19}	0.942700248523234

3.2.6 Computation of $L(s, \Delta\otimes g_{20})$

We apply once again (3.40) similarly to as in section 3.2.4. The main difference is that the Petersson inner product is taken for both modular forms being cusp forms and for the full modular group $\mathrm{SL}_2(\mathbb{Z})$:

$$\begin{aligned} L(s,\Delta\otimes g_{20}) &= \frac{(4\pi)^s}{2\,\Gamma(s)}\int_{\Phi_1}\overline{g_{20}}\,\Delta\,E_{8,1}(z,s-19)\,y^{s-1}\,dx\,dy \\ &= \frac{(4\pi)^s}{2\,\Gamma(s)}\int_{\Phi_1}\overline{g_{20}}\,\Delta\,E_{8,1}(z,s-19)\,y^{18}\,y^{s-19}\,dx\,dy \\ &= \frac{(4\pi)^s}{2\,\Gamma(s)}\left\langle g_{20},\Delta\,y^{s-19}\,E_{8,1}(z,s-19)\right\rangle \\ &= \frac{(4\pi)^s}{2\,\Gamma(s)}\left\langle g_{20},\mathcal{H}ol\left(\Delta\,y^{s-19}\,E_{8,1}(z,s-19)\right)\right\rangle \\ &= \frac{(4\pi)^{19}}{2\,\Gamma(s)}\left\langle g_{20},\mathcal{H}ol\left(\Delta\,(4\pi y)^{s-19}\,E_{8,1}(z,s-19)\right)\right\rangle\,, \end{aligned} \tag{3.74}$$

In this case the critical values of s are $12,\ldots,19$. We verify that $s-19\leqslant 0$, $s-19+8=s-11>0$, then the series $E_{8,1}(z,s-19)$ is a nearly holomorphic

modular form for all these $s \in \{12, \ldots, 19\}$. We write the Fourier expansion of $E_{8,1}(z, s-19)$ using [Pan03, Proposition 2.2]:

$$\begin{aligned}
&(4\pi y)^{s-19}\, E_{8,1}(z, s-19) \\
&\quad = (4\pi y)^{s-19} \Big[2\zeta(2s-30) \\
&\qquad + \frac{(-2\pi i)^{2s-30}\,(-1)^{s-19}\Gamma(2s-31)}{(4\pi y)^{2s-31}\,\Gamma(s-11)\,\Gamma(s-19)}\, 2\zeta(2s-31) \\
&\qquad + \frac{2(-2\pi i)^{2s-30}(-1)^{s-19}}{\Gamma(s-11)} \times \\
&\qquad\quad \times \sum_{n=1}^{\infty} \sum_{d|n} d^{2s-31}\, W(4\pi n y, s-11, s-19)\, q^n \Big] \\
&\quad = 2\zeta(2s-30)(4\pi y)^{s-19} + 2(2\pi)^{2s-30} \frac{\zeta(2s-31)\,\Gamma(2s-31)}{\Gamma(s-11)\,\Gamma(s-19)}\, (4\pi y)^{12-s} \\
&\qquad + (4\pi y)^{s-19} \frac{2(2\pi)^{2s-30}}{\Gamma(s-11)} \sum_{n=1}^{\infty} \sum_{d|n} d^{2s-31}\, W(4\pi n y, s-11, s-19)\, q^n \\
&\quad = D_0'\,(4\pi y)^{12-s} + D_0''\,(4\pi y)^{s-19} \\
&\qquad + \sum_{n=1}^{\infty} 2\,(2\pi)^{2s-30} \sum_{d|n} d^{2s-31}\, \frac{W(4\pi n y, s-11, s-19)}{\Gamma(s-11)} (4\pi y)^{s-11}\, q^n\,,
\end{aligned} \tag{3.75}$$

where

$$\begin{aligned}
D_0' &= D_0'(s) = 2\,(2\pi)^{2s-30} \frac{\Gamma(2s-31)\,\zeta(2s-31)}{\Gamma(s-11)\,\Gamma(s-19)}\,, \\
D_0'' &= D_0''(s) = 2\,\zeta(2s-30)\,.
\end{aligned} \tag{3.76}$$

Since the result of the holomorphic projection in this case belongs to the one-dimensional space spanned by g_{20}, we need to compute just the first Fourier coefficient $B_1(s)$ of $\mathcal{H}ol(\cdot) = \sum_{n=1}^{\infty} B_n(s) q^n$ in order to express it as a multiple of g_{20}. We compute it as the integral given by the Holomorphic Projection Lemma:

$$\begin{aligned}
B_1(s) &= \frac{1}{18!} \int_0^{+\infty} D_0''\,(4\pi y)^{s-19}\, \mathrm{e}^{-4\pi y}\, (4\pi y)^{18}\, d(4\pi y) \\
&\quad + \frac{1}{18!} \int_0^{+\infty} D_0'\,(4\pi y)^{12-s}\, \mathrm{e}^{-4\pi y}\, (4\pi y)^{18}\, d(4\pi y) \\
&= \frac{\Gamma(s)}{18!}\, D_0'' + \frac{\Gamma(31-s)}{18!}\, D_0'
\end{aligned} \tag{3.77}$$

Table 3.3: $L(s, \Delta \otimes g_{20})$

s	$R_{g_{20}}$	$P_{g_{20}}$	$L(s, \Delta \otimes g_{20})$
12	$\frac{524288}{2338875} = \frac{2^{19}}{3^5 \cdot 5^3 \cdot 7 \cdot 11}$	π^{13}	5.380003562880315
13	$\frac{2097152}{88409475} = \frac{2^{21}}{3^8 \cdot 5^2 \cdot 7^2 \cdot 11}$	π^{15}	5.618889612918517
14	$\frac{4194304}{2791213425} = \frac{2^{22}}{3^8 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17}$	π^{17}	3.513063561721911
15	$\frac{8388608}{97692469875} = \frac{2^{23}}{3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17}$	π^{19}	1.981288433718698
16	$\frac{8388608}{1465387048125} = \frac{2^{23}}{3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17}$	π^{21}	1.303635536350500
17	$\frac{2097152}{4396161144375} = \frac{2^{21}}{3^{10} \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17}$	π^{23}	1.072197252248449
18	$\frac{4194304}{92319384031875} = \frac{2^{22}}{3^{11} \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17}$	π^{25}	1.007825020916877
19	$\frac{2097152}{461596920159375} = \frac{2^{21}}{3^{11} \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17}$	π^{27}	0.994683426196918

The final expression is, as follows:

$$\begin{aligned} L(s, \Delta \otimes g_{20}) &= B_1(s) \, \frac{(4\pi)^{19}}{2\,\Gamma(s)} \, \langle g_{20}, g_{20} \rangle \\ &= \left(\frac{\Gamma(s)}{18!} \, D_0'' + \frac{\Gamma(31-s)}{18!} \, D_0' \right) \, \frac{(4\pi)^{19}}{2\,\Gamma(s)} \, \langle g_{20}, g_{20} \rangle \\ &= \frac{(4\pi)^{19}}{2 \cdot 18!} \, \left(D_0'' + \frac{\Gamma(31-s)}{\Gamma(s)} \, D_0' \right) \, \langle g_{20}, g_{20} \rangle \ . \end{aligned} \tag{3.78}$$

Now we evaluate this result for each $s \in \{12, \ldots, 19\}$ in the form $L(s, \Delta \otimes g_{20}) = R_{g_{20}}(s) \, P_{g_{20}}(s) \, \langle g_{20}, g_{20} \rangle$ computing the rational coefficient $R_{g_{20}}$ and the corresponding power of π, see Table 3.3. The numerical value of the Petersson inner product

$$\langle g_{20}, g_{20} \rangle = 0.00000826554153165970 \tag{3.79}$$

is computed in the section 3.2.8.

3.2.7 The main identity

Combining (3.72) and (3.78) into the original expression (3.15) we get the following:

THEOREM 3.9 (ALGEBRAIC EXPRESSION FOR $L(s, F_{12}, spin)$)

$$\begin{aligned} L(s, F_{12}, spin) &= L(s-9, \Delta)\, L(s-10, \Delta)\, L(s, \Delta \otimes g_{20}) \\ &= \frac{3 \cdot 2^{13} \pi^{11}}{\Gamma(s-9)} \frac{(232\, A_1(s-9) - A_2(s-9))}{(1 + 3 \cdot 2^{13-s} + 2^{31-2s})} \langle \Delta, \Delta \rangle \times \\ &\quad \times \frac{(4\pi)^{19}}{2 \cdot 18!} \left(D_0''(s) + \frac{\Gamma(31-s)}{\Gamma(s)} D_0'(s) \right) \langle g_{20}, g_{20} \rangle \\ &= \frac{3 \cdot 2^{50}\, \pi^{30}\, (232\, A_1(s-9) - A_2(s-9))}{18!\, \Gamma(s-9)\, (1 + 3 \cdot 2^{13-s} + 2^{31-2s})} \times \\ &\quad \times \left(D_0''(s) + \frac{\Gamma(31-s)}{\Gamma(s)} D_0'(s) \right) \langle \Delta, \Delta \rangle \, \langle g_{20}, g_{20} \rangle \, , \end{aligned} \tag{3.80}$$

where $A_1(s)$ is given by (3.61)*, $A_2(s)$ is given by* (3.62)*, D_0' and D_0'' are given by* (3.76)*. For each critical value at point $s \in \{12, \ldots, 19\}$ we evaluate this expression in the form $L(s, F_{12}, spin) = R(s)\, P(s)\, \langle \Delta, \Delta \rangle \, \langle g_{20}, g_{20} \rangle$ computing the rational coefficient R and the corresponding power of π, see Table 3.4.*

3.2.8 Numerical computation of Petersson product

To compute numerically the Petersson inner product of Δ by itself and g_{20} by itself we use the classical result by Rankin [Ran52, Theorem 5]:

$$\langle f_k, f_k \rangle = \frac{(4\pi)^{1-k}\, (k-2)!}{\zeta(l)} \frac{\alpha_r}{\alpha_l + \alpha_r - \alpha_k} L(k-1, f_k)\, L(l, f_k)\, , \tag{3.81}$$

where f_k is the cusp form of weight $k = \{12, 16, 18, 20, 22, 26\}$ of the form

$$f_k(z) = E_{k-12}(z)\, \Delta(z) \tag{3.82}$$

and

$$\begin{aligned} &4 \leqslant r \leqslant k/2 - 2\, , \\ &l = k - r\, ; \end{aligned} \tag{3.83}$$

Table 3.4: $L(s, F_{12}, spin)$

s	R	P	$L(s, F_{12}, spin)$
12	$\frac{17179869184}{526246875} = \frac{2^{34}}{3^7 \cdot 5^5 \cdot 7 \cdot 11}$	π^{18}	0.248251332624670
13	$\frac{8589934592}{7161167475} = \frac{2^{33}}{3^{12} \cdot 5^2 \cdot 7^2 \cdot 11}$	π^{22}	0.888519130619814
14	$\frac{8589934592}{527539337325} = \frac{2^{33}}{3^{11} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17}$	π^{26}	1.174884717828030
15	$\frac{68719476736}{461596920159375} = \frac{2^{36}}{3^{11} \cdot 5^3 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17}$	π^{30}	1.046349279390801
16	$\frac{137438953472}{103859307035859375} = \frac{2^{37}}{3^{13} \cdot 5^7 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17}$	π^{34}	0.905990508529256
17	$\frac{17179869184}{1308627268651828125} = \frac{2^{24}}{3^{15} \cdot 5^6 \cdot 7^4 \cdot 11 \cdot 13 \cdot 17}$	π^{38}	0.875513015091950
18	$\frac{34359738368}{247330553775195515625} = \frac{2^{35}}{3^{18} \cdot 5^6 \cdot 7^5 \cdot 11 \cdot 13 \cdot 17}$	π^{42}	0.902464835857626
19	$\frac{137438953472}{92748957665698318359375} = \frac{2^{37}}{3^{19} \cdot 5^9 \cdot 7^5 \cdot 11 \cdot 13 \cdot 17}$	π^{46}	0.937688313077777

E_k denotes normalized Eisenstein series

$$\begin{aligned} E_k(z) &= \sum_{n=0}^{\infty} \alpha_k(n)\, q^n\,, \\ \alpha_k(0) &= 1\,, \\ \alpha_k &= \alpha_k(1) = -\frac{2k}{B_k}\,, \end{aligned} \tag{3.84}$$

B_k is a Bernoulli number ($B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0, \ldots$).

For $f_k = \Delta$ we are able to use only one choice of critical value $l = 8$. To compute the numerical values $L(11, \Delta)$ and $L(8, \Delta)$ we used Dokchitser's L-functions Calculator [Dok]. In order to achieve the default precision (53 machine bits, which satisfies the functional equation to `1E-21`), it is necessary to input 12 Fourier coefficients in this case. The obtained value is

$$\langle \Delta, \Delta \rangle = 0.00000103536205680432094820959680 4\,, \tag{3.85}$$

which coincides with the value given by Zagier in [Zag77, page 116] up to 11 digit (his method exploits the direct summation of 250 first terms in L-series).

We used again Rankin's theorem to compute the Petersson inner product of g_{20} by itself. For the modular form of weight 20 there are three choices $l = 12, 14, 16$. For each choice of l we computed the special value of $L(l, g_{20})$ using Dokchitser's L-functions Calculator. It required to input 14 Fourier coefficients of g_{20} in order to achieve the default precision. The obtained values are

$$\begin{aligned}
\langle g_{20}, g_{20}\rangle &= 0.000008265541531659702744699575969 \text{ for } l = 12,\\
\langle g_{20}, g_{20}\rangle &= 0.000008265541531659703390644766954 \text{ for } l = 14,\\
\langle g_{20}, g_{20}\rangle &= 0.000008265541531659703069998511729 \text{ for } l = 16.
\end{aligned} \tag{3.86}$$

3.2.9 Numerical verification

The obtained values of $L(s, F_{12}, spin)$ in section 3.2.7 can be numerically verified by using Dokchitser's L-functions Calculator and computing each term of the product in the righthand side of the identity (3.15). The computation of $L(s, \Delta)$ was already described in the previous section.

To compute values of $L(s, \Delta \otimes g_{20})$ for $s \in \{12, \ldots, 19\}$ we have to determine the coefficients of this Dirichlet series first. Using the identity (3.35) for $f = \Delta = \sum \tau(n) n^{-s}$ and $g = g_{20} = \sum b(n) n^{-s} \in \mathcal{S}_{20}$ we get

$$\begin{aligned}
L(s, \Delta \otimes g_{20}) &= \sum_{n=1}^{\infty} A(n) n^{-s}\\
&= \sum_{d=1}^{\infty} d^{30-2s} \sum_{d_1=1}^{\infty} \tau(d_1) b(d_1) d_1^{-s}\\
&= \sum_{d, d_1 \geqslant 1} d^{30} \tau(d_1) b(d_1)\, (d^2 d_1)^{-s}\\
&= \sum_{n=1}^{\infty} \sum_{d : d^2 | n} d^{30} \tau(\frac{n}{d^2}) b(\frac{n}{d^2})\, n^{-s}\,.
\end{aligned} \tag{3.87}$$

Therefore we obtain

$$A(n) = \sum_{d : d^2 | n} d^{30}\, \tau(\frac{n}{d^2})\, b(\frac{n}{d^2})\,. \tag{3.88}$$

The ComputeL program requires some functional equation parameters such as Γ-factors and the weight. The functional equation for $L(s, f \otimes g)$ is known, see [Li79]. Therefore, the parameters that are used by ComputeL are

$$\Gamma_{\mathbb{C}}(s)\, \Gamma_{\mathbb{C}}(s - l + 1) \text{ and } s \mapsto k + l - 1 - s\,,$$

where $k = 20 > l = 12$ are the weights of g_{20} and Δ. In our case (using the Gauss Duplication formula) we have four gamma factors $\Gamma_{\mathbb{R}}(s)\,\Gamma_{\mathbb{R}}(s+1)\,\Gamma_{\mathbb{R}}(s-11)\,\Gamma_{\mathbb{R}}(s-10)$ and the "motivic weight" is 31.

The modern interpretation of the functional equation can be obtained by using the Hodge theory. The mentioned parameters can be deduced from the Hodge structures (see [Sch90]) of Δ and g_{20}, namely

$$\begin{aligned} \Delta &\longrightarrow (0,11)+(11,0)\,, \quad H(M(\Delta)) = H^{0,11} \oplus H^{11,0} \\ g_{20} &\longrightarrow (0,19)+(19,0)\,, \quad H(M(g_{20})) = H^{0,19} \oplus H^{19,0}\,. \end{aligned} \tag{3.89}$$

Therefore the Hodge structure of their tensor product (see [Yos01]) is

$$\begin{aligned} &\Delta \otimes g_{20} \longrightarrow (0,30)+(11,19)+(19,11)+(30,0)\,, \\ &H(M(g_{20}) \otimes M(\Delta)) = H^{0,30} \oplus H^{11,19} \oplus H^{19,11} \oplus H^{30,0}\,. \end{aligned} \tag{3.90}$$

The Deligne's rule gives [Del79, page 329] in our case two Serre's Γ-factors: $\Gamma_{\mathbb{C}}(s)$ and $\Gamma_{\mathbb{C}}(s-11)$. Once again one can use the Gauss Duplication formula, which gives in our case the same four factors $\Gamma_{\mathbb{R}}(s)\,\Gamma_{\mathbb{R}}(s+1)\,\Gamma_{\mathbb{R}}(s-11)\,\Gamma_{\mathbb{R}}(s-10)$. By Deligne's description, the weight k of the symmetry $s \mapsto k-s$ that appears in the functional equation coincides with the motivic weight of the tensor product of two motives plus 1, which gives us $11+19+1=31$.

We need about 150 coefficients of L-series to obtain the default precision (the functional equation is satisfied with `1E-27` precision). Coefficient of Δ and g_{20} are readily available in SAGE. First few coefficients $A(n)$ are given in Table B.1 in the Appendix B.

Finally, we are able to compare the result in Table 3.4 and both of its parts in Tables 3.2, 3.3 with the direct numerical computation. These values and the absolute values of the difference with theoretical rational computation results are presented in Table 3.5 and Table 3.6.

Table 3.5: Numerical computation and comparison

s	$L(s-9,\Delta)\,L(s-10,\Delta)$	variation from Table 3.2	$L(s,\Delta\otimes g_{20})$	variation from Table 3.3
12	0.046143339853964	3.58E-11	5.38000356288032	4.95E-15
13	0.158130732674877	1.23E-10	5.61888961291852	2.39E-15
14	0.334433094676168	2.60E-10	3.51306356172191	1.44E-15
15	0.528115574893734	4.10E-10	1.98128843371870	1.36E-15
16	0.694972240300672	5.40E-10	1.30363553635050	7.99E-16
17	0.816559652560290	6.34E-10	1.07219725224845	7.40E-16
18	0.895457860073449	6.96E-10	1.00782502091688	2.75E-15
19	0.942700249255570	7.32E-10	0.99468342619692	4.22E-16

Table 3.6: Numerical computation and comparison (final)

s	$L(s,F_{12},spin)$	variation from Table 3.4
12	0.24825133281752	1.98E-10
13	0.88851913131006	6.90E-10
14	1.17488471874074	9.13E-10
15	1.04634928020366	8.13E-10
16	0.90599050923308	7.04E-10
17	0.87551301577209	6.80E-10
18	0.90246483655871	7.01E-10
19	0.93768831380622	7.28E-10

Chapter 4

Cryptography aspects, relations to the Hecke algebra over $\mathbb{F}_q$

4.1 Review on algebraic cryptosystems

The term *cryptography* refers to a wide range of security issues in the transmission and storage of information. The number theory takes nowadays the leading role in continuous development of this domain.

A cryptosystem is a map from units of plaintext (ordinary information) to units of ciphertext (coded text). For example, a primitive coding algorithm of an addition modulo N, where N is a number of letters in the alphabet, is known for centuries. It can be also viewed as a cyclic permutation of the alphabet. Since then, numerous complicated algorithms were developed with the use of a *private key* (see the next paragraph). The important mathematical result in early stage cryptography is the famous theorem of Shannon [Sha49] stating that the only way to obtain perfect security is to use a *one-time keypad*. Even so, a safety of the cryptographic message transmission depended on the secured key transmission (e.g., using a trusted courier).

In 1976 Whitfield Diffie and Martin Hellman [DH76] invented an entirely new type of cryptography. They used the idea of a one-way function for encryption. Roughly speaking, we say that a one-to-one function $f : X \to Y$ is *one-way* if it is easy to compute $f(x)$ for any $x \in X$, but it is hard to compute $f^{-1}(y)$ for most randomly selected y in the range of f. Sometimes it could be even a stronger statement, that it is hard to compute any partial information about $f^{-1}(y)$ for most randomly selected y. With the use of such a one-way function (as a *public key*), one can encrypt the plaintext. However, only those, who have an additional information (private key) can compute an inverse function in a reasonable amount of time.

The most common purposes for the public key cryptography are:

- confidential information transmission;
- authentication (using hash functions, digital signatures, passwords, etc.);
- key exchange (to agree on a secret key for some private key cryptosystem);
- secret sharing (a method for distributing a secret).

The most known and commonly used public key cryptosystems are RSA (based on a problem of factoring integers) and Diffie-Hellman (based on discrete logarithm problem).

4.1.1 Encryption using RSA

RSA was introduced by Rivest, Shamir, and Adleman in 1977. This is the most popular public-key cryptosystem in use today. Its security rests on the fact that it is hard to factor a product of two large primes. However, the statement that there is no efficient algorithm exist to factorize a number has not been proved. The idea of RSA is simple:

1. Choose two distinct large prime numbers p and q.
2. Compute $n = pq$, n is used as the modulus for both the public and private keys.
3. Compute the Euler function: $\varphi(n) = (p-1)(q-1)$.
4. Choose an integer e such that $1 < e < \varphi(n)$, and e and $\varphi(n)$ are coprime; e is released as the public key exponent.
5. Compute d to satisfy the congruence relation $de \equiv 1 \pmod{\varphi(n)}$; d is kept as the private key exponent.

Here is the example. Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M (a number smaller than n) to Alice. He computes the ciphertext C corresponding to $C = M^e \pmod{n}$. This can be done quickly using the method of exponentiation by squaring. Bob then transmits C to Alice. Alice can recover M from C by using her private key exponent d by computing $M = C^d \pmod{n}$. The above decryption procedure works because $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M \pmod{n}$.

Recent advancements in computing algorithms and the Number Theory itself led to the increase of the size of primes used in practice. The most of

public-key cryptosystems today use RSA with a binary key length of 512-bit, the business community is already turning to 768-bit RSA or 1024-bit RSA in order to enhance a security against possible attacks with the use of advanced algorithms in future.

The problem with large key lengths is that they are not applicable in constrained conditions, such as limited memory capacity of smart cards. That is why, the business community seeks for alternatives.

4.1.2 Diffie-Hellman (discrete logarithm problem)

In a general case, let us consider G be a finite cyclic group with n elements. We assume that the group is the multiplicative one. Then every element h of G can be written in the form $h = g^k$ for some integer k, where g is the generator of G. Furthermore, any two such integers representing h will be congruent modulo n. We can thus define a function $\log_g : G \rightarrow \mathbb{Z}_n$ by assigning to h the congruence class of k modulo n. This function is a group isomorphism, called the discrete logarithm to base g.

While the problem of computing discrete logarithms and the problem of integer factorization are different problems they share some properties:

* both problems are difficult (no efficient algorithms are known),
* algorithms related to one problem are often adapted to the other,
* both problems has been exploited to construct various cryptographic systems.

In application to cryptography the inverse problem of discrete exponentiation is not difficult (it can be computed efficiently with the use of the exponentiation by squaring, for example). This asymmetry is analogous to that in the factorization and the multiplication.

The key-exchange protocol is simple:

1. Alice and Bob agree on a finite cyclic group G and a generating element g in G.
2. Alice picks up a random natural number a and sends g^a to Bob.
3. Bob picks up a random natural number b and sends g^b to Alice.
4. Alice computes $(g^b)^a$.
5. Bob computes $(g^a)^b$.

Both Alice and Bob are now in possession of the group element g^{ab}, which can serve as the shared secret key. The values of $(g^b)^a$ and $(g^a)^b$ are the same because groups are power associative.

Based on the Diffie-Hellman key agreement protocol, one can encrypt the message with the use of the ElGamal encryption system. ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

The key generator works as follows:

1. Alice generates an efficient description of a multiplicative cyclic group G, of order q with generator g.
2. Alice chooses a random x from $\{0, \ldots, q-1\}$.
3. Alice computes $h = g^x$.
4. Alice publishes h, along with the description of G, q, g as her public key. Alice retains x as her private key which must be kept secret.

The encryption algorithm works as follows: to encrypt a message $m \in G$ to Alice under her public key (G, q, g, h),

1. Bob chooses a random y from $\{0, \ldots, q-1\}$, then calculates $c_1 = g^y$ and $c_2 = m \cdot h^y$.
2. Bob sends the ciphertext (c_1, c_2) to Alice.

The decryption algorithm works as follows: to decrypt a ciphertext (c_1, c_2) with her private key x,

Alice computes c_2/c_1^x as the plaintext message.

The decryption algorithm produces the intended message, since

$$\frac{c_2}{c_1^x} = \frac{m \cdot h^y}{g^{xy}} = \frac{m \cdot g^{xy}}{g^{xy}} = m.$$

4.1.3 Alternatives

The most popular current alternatives to RSA and ElGamal are the elliptic curve cryptosystems invented by Neal Koblitz and Victor Miller in 1985 independently. The security of elliptic curve cryptography depends on our inability to solve the elliptic curve discrete logarithm problem in subexponential time. The set of points on elliptic curve (i.e., all solutions to the equation together with a point at infinity) can be shown to form an abelian

group (with the point at infinity as the identity element). If the coordinates x and y are chosen from a large finite field, the solutions form a finite abelian group. It is believed that the discrete logarithm problem on such elliptic curve groups is more difficult than the corresponding problem in the underlying finite field. Thus, keys in elliptic curve cryptography can be chosen much shorter for a comparable degree of security.

4.2 Cryptosystems on a projective space

The projective coordinates can be efficiently used for increasing of a cryptosystem security level. We demonstrate this transition on the cryptosystem based on Drinfeld modules [GLPR03]. First, recall the underlying theory.

4.2.1 Cryptosystem based on Drinfeld modules

Denote by $\mathcal{A} = \mathbb{F}_p[T]$ the polynomial ring in variable T with coefficients from the finite field $\mathbb{F}_p$. Consider the polynomial ring $\mathcal{A}\{\tau\} = \mathbb{F}_p[T]\{\tau\}$ in variable τ with coefficients from $\mathcal{A}$ with the following multiplicative commutation rule:

$$\tau^k \times \alpha = \alpha^{p^k} \times \tau^k \,, \tag{4.1}$$

where $k \geq 1$ and $\alpha \in \mathcal{A}$. The addition operation in $\mathcal{A}\{\tau\}$ is a usual one.

EXAMPLE 4.1 *Let* $p = 3$.

$$\begin{aligned}(\tau + T)^2 &= (\tau + T) \times (\tau + T) \\ &= \tau^2 + \tau \times T + T \times \tau + T^2 \\ &= \tau^2 + T^3\tau + T\tau + T^2 \\ &= \tau^2 + (T^3 + T)\tau + T^2 \,.\end{aligned}$$

Each element of $\mathcal{A}\{\tau\}$ defines a map from $\mathcal{A}$ to itself by associating

1) with each $\alpha \in \mathcal{A} \subset \mathcal{A}\{\tau\}$ an element resulting by left multiplication $z \mapsto \alpha z$

2) and with τ — the Frobenius map $z \mapsto z^p$.

Therefore, the multiplication in $\mathcal{A}\{\tau\}$ corresponds to the composition of functions. The ring $\mathcal{A}$ has a natural structure of $\mathcal{A}\{\tau\}$-module where for each $\alpha = \sum_{i=0}^{m} a_i \tau^i \in \mathcal{A}\{\tau\}$ and $z \in \mathcal{A}$ one has:

$$\alpha z = \sum_{i=0}^{m} a_i z^{p^i} \,. \tag{4.2}$$

DEFINITION 4.2 *A Drinfeld module is a morphism ϕ of $\mathbb{F}_p$-algebra of $\mathcal{A}$ to $\mathcal{A}\{\tau\}$ such that $\phi(T)$ is a non-constant polynomial in variable τ with constant term is equal to T.*

Since the Drinfeld module is a morphism, it is defined as far as the value of $\phi(T)$ is fixed.

EXAMPLE 4.3 *A simple example of Drinfeld module is the Carlitz module, defined by $\phi(T) = \tau + T$. For $p = 3$ one has*

$$\begin{aligned}\phi(T^2+T+1) &= (\tau+T)^2 + (\tau+T) + 1 \\ &= \tau^2 + (T^3+T)\tau + T^2 + \tau + T + 1 \\ &= \tau^2 + (T^3+T+1)\tau + (T^2+T+1)\,.\end{aligned}$$

DEFINITION 4.4 *We denote by ϕ_α the mapping of $\mathcal{A}$ to itself defined by the polynomial $\phi(\alpha) \in \mathcal{A}\{\tau\}$, where $\alpha \in \mathcal{A}$. The map ϕ_1 is the identity map in $\mathcal{A}$.*

EXAMPLE 4.5 *The map defined by Example 4.3 is*

$$\begin{aligned}\phi_{T^2+T+1}(z) &= \left(\tau^2 + (T^3+T+1)\tau + (T^2+T+1)\right)(z) \\ &= z^9 + (T^3+T+1)z^3 + (T^2+T+1)z\,.\end{aligned}$$

Let us denote by $\mathcal{B} = \mathcal{A}/f(T)$ the quotient of $\mathcal{A}$ by an irreducible polynomial $f(T) \in \mathcal{A}$ of degree $d > 1$. Since $\mathcal{A}$ can be viewed as a morphism, $\mathcal{B}$ can be considered as a morphism of a finite field of p^d elements. This field can be easily provided with a natural structure of $\mathcal{A}$-module by passage to the quotient. For $\alpha \in \mathcal{A}$, we denote by $\overline{\alpha}$ the class of α in $\mathcal{B}$. Therefore,

$$\alpha \times \beta = \overline{\alpha b} \tag{4.3}$$

for $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{B}$ such that $\beta = \overline{b}$ for a corresponding $b \in \mathcal{A}$.

DEFINITION 4.6 *Similarly to Definition 4.4 we denote by $\overline{\phi_\alpha}$ the map from $\mathcal{B}$ to $\mathcal{B}$ corresponding to $\alpha \in \mathcal{A}$:*

$$\overline{\phi_\alpha} \;:\; \beta \mapsto \overline{\phi_\alpha(b)} \tag{4.4}$$

for $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{B}$ such that $\beta = \overline{b}$ for a corresponding $b \in \mathcal{A}$.

Therefore, we introduce the following structure of $\mathcal{A}$-module, which is associated to the Drinfeld module ϕ:

$$\alpha \times_\phi \beta = \overline{\phi_\alpha}(\beta) \tag{4.5}$$

EXAMPLE 4.7 *Let $p = 3$, $d = 2$, $\phi(T) = \tau + T$, $f(T) = T^2 + 1$. We continue Example 4.5 and obtain*

$$\overline{\phi_{T^2+T+1}}(z) = z^9 + z^3 + \overline{T}z\,.$$

If we denote by $\mathcal{B}_\phi$ the set $\mathcal{B}$ with $\mathcal{A}$-module structure defined in (4.5), then for some polynomial $\mathsf{f}_\phi \in \mathcal{A}$ of degree d we have $\mathcal{B}_\phi \simeq \mathcal{A}/(\mathsf{f}_\phi)$.

PROPOSITION 4.8 ([GLPR03])

(*i*) *Two elements α_1 and α_2 of $\mathcal{A}$ define the same mapping $\overline{\phi_{\alpha_1}} = \overline{\phi_{\alpha_2}}$ if and only if $\alpha_1 \equiv \alpha_2 \pmod{\mathsf{f}_\phi}$.*

(*ii*) *The map $\overline{\phi_\alpha}$ is bijective if and only if α is prime to f_ϕ. In this case, the inverse mapping $\overline{\phi_{\alpha'}}$ is defined by α' such that $\alpha\alpha' \equiv 1 \pmod{\mathsf{f}_\phi}$.*

This proposition is important for defining the one-way function ψ. The idea of R. Gillard, F. Leprevost, A. Panchishkin and X.-F. Roblot is to construct a public key in the following form:

$$\psi(z) = \left(\overline{\phi_{c_1}} \circ \sigma \circ \overline{\phi_{c_2}}\right)(z)\,, \tag{4.6}$$

where c_1 and c_2 are prime to f_ϕ (such that both functions ϕ_{c_1} and ϕ_{c_2} are invertible) and σ is a bijective function from $\mathcal{B}$ to itself, which is easy to inverse, in particular, $\sigma : z \mapsto z^e + \delta$ (e is prime with p and with $p^d - 1$, $\delta \in \mathcal{B}$, then $\sigma^{-1}(z) = (z - \delta)^{e'}$, where $ee' \equiv 1 \pmod{p^d - 1}$). The function $\psi(z)$ is a polynomial from $\mathcal{B}[z]$. This function is bijective, its inverse is a combination of inverse components

$$\psi^{-1}(z) = \left(\overline{\phi_{c_2'}} \circ \sigma^{-1} \circ \overline{\phi_{c_1'}}\right)(z) \tag{4.7}$$

with elements c_1' and c_2' from $\mathcal{A}$ such that $c_1c_1' \equiv 1 \pmod{\mathsf{f}_\phi}$ and $c_2c_2' \equiv 1 \pmod{\mathsf{f}_\phi}$. This inverse function is difficult to determine without knowing the secret key (c_1, c_2, σ).

However, in the article [BCG06] the authors proposed an attack on the cryptosystem based on linearization. Their method was efficient for retrieving the secret key and decrypting the message.

4.2.2 Projective version of GLPR

The projective version of GLPR cryptosystem adds the "point" ∞ to an algebraic variety $\mathcal{B}$. Then we can use a linear fractional transformation $\sigma(z) = \dfrac{az + b}{cz + d}$ in the composition of the trap door $\psi(z)$. We always stay in

terms a polynomials replacing $\frac{az+b}{cz+d}$ by projective coordinates $(az+b : cz+d)$. If $z = \frac{x}{y}$, we write $z \mapsto (x : y)$, then $\frac{az+b}{cz+d} \mapsto (ax + by : cx + dy)$. In the same way, if $\phi(z)$ is a polynomial of degree d, then we replace $(\phi(z) : 1)$ with $(y^d\phi(\frac{x}{y}) : y^d)$. The point ∞ corresponds to $(1 : 0)$. The action of $f(z)$ is $(f_x(x : y) : f_y(x : y))$, the composition of f and g then acts by $f \circ g(z) \mapsto \Big(f_x\big(g_x(x : y) : g_y(x : y)\big) : f_y\big(g_x(x : y) : g_y(x : y)\big)\Big)$.

EXAMPLE 4.9 *Let $p = 3$, $d = 2$, $\phi(T) = \tau + T$, $f(T) = T^2 + 1$, $\mathsf{f}_\phi = 2T^2$. Consider*

$$\psi = \overline{\phi_{c_2} \circ \sigma_2 \circ \sigma_1 \circ \phi_{c_1}}\,,$$

where

$$\begin{aligned} c_1 &= T + 1\,, \qquad \text{then } \phi_{c_1}(z) = z^3 + (T+1)z\,,\\ c_2 &= T + 2\,, \qquad \text{then } \phi_{c_2}(z) = z^3 + (T+2)z\,,\\ \sigma_1(z) &= z^5 + T\,,\\ \sigma_2(z) &= \frac{Tz+1}{z+T}\,. \end{aligned}$$

Suppose $z = x/y$, then replace $\psi(z)$ with $\psi(x : y)$ and obtain the following encryption function

$$\begin{aligned} \psi(x : y) = {}& \\ & \big((T+2)y^6x^7 + (2T+1)y^7x^6 + (T+2)x^5 + 2y^8x^5 + yx^4 + \\ & (2T+2)y^2x^3 + (2T+2)y^3x^2 + (2T+1)y^4x : \\ & (2T+1)y^6x^7 + x^5 + y^8x^5 + (T+1)y^2x^3 + y^4Tx + Ty^5\big)\,. \end{aligned}$$

Therefore, for example, the encoding of $(1 : 1)$, $(1 : 0)$ and $(T : 1)$ is given by:
$\psi(1 : 1) = (T + 1 : 2T + 1) = (T : 1)$,
$\psi(1 : 0) = (T + 2 : 1)$,
$\psi(T : 1) = (1 : T + 2) = (T + 1 : 1)$, ...
The decoding procedure consists in sequence of inverse maps $\phi_{c_2}^{-1}$, σ_2^{-1}, σ_1^{-1}, $\phi_{c_1}^{-1}$, where

$$\begin{aligned} \phi_{c_1}^{-1}(z) &= 2z^3 + (2T+1)z\,,\\ \phi_{c_2}^{-1}(z) &= 2z^3 + (2T+2)z\,,\\ \sigma_1^{-1}(z) &= (z-T)^5\,,\\ \sigma_2(z)^{-1} &= \frac{Tz+2}{2z+T}\,, \end{aligned}$$

which immediately gives $\phi_{c_1}^{-1}(\sigma_1^{-1}(\sigma_2^{-1}(\phi_{c_2}^{-1}(T + 1 : 1)))) = (T : 1)$.

The simple way to experiment with different models of cryptosystem is to use the interactive interface of SAGE. The listing related to given examples and further generalizations can be found in the Appendix C.

A reasonable option for further development of the presented approach is to consider the projective space of higher degree. For the projective plane $\mathbb{P}^2$ of the type $(* : * : *)$ we compose the bijections in a similar way

$$\psi : \mathbb{A}^2 \xrightarrow{\sigma_a} \mathbb{A}^2 \xrightarrow{\phi_{c_{i,j}}} \mathbb{A}^2 \xrightarrow{\sigma_b} \mathbb{P}^2 , \tag{4.8}$$

where $\mathbb{A}^2$ is an affine chart of the type $(* : * : 1)$.

4.2.3 Generalization to $\mathbb{P}^n$

In a general case, the Frobenius map can be defined on affine chart as

$$(1 : z_1 : \ldots : z_n) \overset{\sigma_p}{\mapsto} (1 : z_1^{e_1} : \ldots : z_n^{e_n}) \tag{4.9}$$

for all $e_i \nmid p^d - 1$. In projective coordinates we have to keep them homogeneous, so

$$(x_0 : x_1 : \ldots : x_n) \overset{\sigma_p}{\mapsto} (x_0^{e_0} : x_0^{e_0-e_1} x_1^{e_1} : \ldots : x_0^{e_0-e_n} x_n^{e_n}) , \tag{4.10}$$

where $e_0 = \max\{e_1, \ldots, e_n\}$.

Similarly, the bijection defined by the Drinfeld module polynomials $\phi_c(z) = \alpha_0 z + \alpha_1 z p + \cdots + \alpha_r z^{p^r}$ acts on affine chart as

$$(1 : z_1 : \ldots : z_n) \overset{\phi_c}{\mapsto} (1 : \phi_{c_1}(z_1) : \ldots : \phi_{c_n}(z_n)) . \tag{4.11}$$

In projective coordinates

$$(x_0 : x_1 : \ldots : x_n) \overset{\phi_c}{\mapsto} (x_0^{p^{r_0}} : x_0^{p^{r_0}} \phi_{c_1}(\tfrac{x_1}{x_0}) : \ldots : x_0^{p^{r_0}} \phi_{c_n}(\tfrac{x_n}{x_0})) , \tag{4.12}$$

where $r_0 = \max\{r_1, \ldots, r_n\}$.

These functions are easy to program in a similar way as in the previous section. The Frobenius map is realized in the procedure myexp(pp,pe) on page 130 of the Appendix C. The bijection defined by the Drinfeld module is realized in the procedure phi_c(pp,pc) on page 132.

In addition to the described bijections, we use an invertible matrix action. The corresponding listing is presented on page 133.

4.2.4 Rational points of flag varieties

Flag varieties are examples of varieties having a large number of points over a finite field and can therefore be used for constructing efficient cryptosystems. First, we give a definition of a flag variety.

DEFINITION 4.10 *A **flag** over a finite field $\mathbb{F}_q$ is a sequence X of strictly embedded subspaces $V_{i_1} \subset V_{i_2} \subset \cdots \subset V_{i_s}$ of dimension i_1, i_2, ..., i_s of an m-dimensional vector space $V = (\mathbb{F}_q)^m$. A **flag variety** of type $(i_1, i_2, \ldots, i_s)$ is the variety of all flags $\mathcal{F} = \{(V_{i_1}, V_{i_2}, \ldots, V_{i_s})\}$ with $(i_1, i_2, \ldots, i_s)$ given.*

The flag variety can be also described as the set G/P, where $G = \mathrm{GL}_n(\mathbb{F}_q)$ and P is a parabolic subgroup of G. In this case the parabolic group P consits of upper triangular matrices in blocks or of conjugates of such a matrix:

$$P = \begin{pmatrix} M_1 & * & \cdots & * \\ 0 & M_2 & \cdots & * \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & M_{s+1} \end{pmatrix}$$

where $M_r \in \mathrm{GL}_{i_r - i_{r-1}}(\mathbb{F}_q)$ for $2 \leqslant r \leqslant s+1$ with $V_{s+1} = V = (\mathbb{F}_q)^m$. Since the group G acts transitively on the set of flags $\mathcal{F} = \{(V_{i_1}, V_{i_2}, \ldots, V_{i_s})\}$, the group P is the stabilizer of the flag

$$\{(\langle e_1, e_2, \ldots, e_{i_1}\rangle, \langle e_{i_1+1}, e_{i_1+2}, \ldots, e_{i_2}\rangle, \ldots, \langle e_{i_s+1}, e_{i_s+2}, \ldots, e_m\rangle)\},$$

where $\{e_1, e_2, \ldots, e_m\}$ is the canonical basis of the vector space V.

The principal idea of the cryptosystem design is the interpretation of points on flag varieties over a finite field in terms of finite sets of left cosets $\{\Gamma g_1, \cdots, \Gamma g_m\}$, which come up into a double coset $\Gamma g \Gamma = \bigcup_{j=1}^{m} \Gamma g_j$. We can use automorphisms and bijections on the $\mathbb{F}_q$-rational points of G and of $X = G/P$.

There is an alternative description of this set as a double coset

$$\Gamma g_j \longleftrightarrow \{\Gamma_{(g)} \backslash \Gamma\}, \tag{4.13}$$

where $\Gamma_{(g)} = g^{-1}\Gamma g \cap \Gamma \subset \mathrm{GL}_n(\mathrm{K})$ (or more general $\subset M_n(\mathrm{A})$), and $\Gamma = \mathrm{GL}_n(\mathrm{A})$, $\mathrm{A} = \mathbb{F}_q[T]$ (or $\mathbb{Z}$), $\mathrm{K} = \mathrm{Quotient}(\mathrm{A})\{\mathbb{F}_p[T],\ \text{or}\ \mathbb{Q}\}$.

The explicit description of the bijection (4.13) can be found in [Shi71], for example. It is given by notion of HNF (Hermite Normal Form) and SNF (Smith Normal Form). More precisely, $\Gamma_{(g)}$ is a stabilizer of the element Γg for the right action of Γ on the set of left cosets $\{\Gamma g_j\}$:

$$\Gamma g\, \gamma = \Gamma g \quad \Leftrightarrow \quad g\gamma = xg \quad \Leftrightarrow \quad \gamma = g^{-1}xg \in g^{-1}\Gamma g \cap \Gamma.$$

Consider the module $\mathrm{A}^n \supset (f\mathrm{A})^n$, where f is an irreducible polynomial. Let us describe the elements γ. Note, that γ acts on $\mathrm{A}^n/(f\mathrm{A})^n \cong (\mathrm{A}/f\mathrm{A})^n$. This action is trivial if and only if $\gamma \equiv I_n \pmod f$, i.e. γ belongs to the main congruence subgroup $\Gamma(f) = \{\gamma \in \Gamma : \gamma \equiv I_n \pmod f\}$, moreover, $\Gamma(f) \lhd \Gamma$, therefore, $\Gamma/\Gamma(f) \cong \mathrm{GL}_n(\mathrm{A}/f\mathrm{A})$.

For any intermediate subgroup $\widetilde{\Gamma}$, such that $\Gamma(f) \subset \widetilde{\Gamma} \subset \Gamma$, the quotient $\widetilde{\Gamma}/\Gamma(f)$ is a subgroup of $\mathrm{GL}_n(\mathrm{A}/f\mathrm{A})$. Let $\mathrm{V} = (\mathrm{A}/f\mathrm{A})^n$. The group $\widetilde{\Gamma}$ acts on V. Consider a flag $\mathcal{F} \equiv (0 \neq \mathrm{V}_1 \subset \cdots \subset \mathrm{V}_k \subsetneq (\mathrm{A}/f\mathrm{A})^n = \mathrm{V})$ of a type $(n_1, \ldots, n_k)$, $n_i = \dim \mathrm{V}_i$. Define $\Gamma_{\mathcal{F}} = \{\gamma : \gamma(\mathcal{F}) \subset \mathcal{F}\}$, that is for all i we have $\gamma(\mathrm{V}_i) \subset \mathrm{V}_i$. $\{\mathcal{F}\}$ can be described as an algebraic variety over $\mathbb{F}_q = \mathrm{A}/f\mathrm{A} : \mathcal{D}(n_1, \ldots, n_k)$. The group Γ acts on $\mathcal{D}(n_1, \ldots, n_k)$ and $\mathrm{Stab}_{\mathcal{F}} = \Gamma_{\mathcal{F}}$, $\Gamma/\Gamma_{\mathcal{F}} \cong$ Orbit of $\mathcal{F}$.

Example 4.11 (general linear group) *Let* $k = 1$, $n_1 = 1$, $\mathcal{D}(1) \cong \mathbb{P}^{n-1}(\mathbb{F}_q)$, $\gamma(e_1) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. $\gamma(\langle e_1 \rangle) = \langle e_1 \rangle$, *therefore* $\gamma = \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & & \vdots & \\ 0 & * & \cdots & * \end{pmatrix} \bmod f$.

Example 4.12 (symplectic group) *Let* $p \neq 2$, $n = 2m$, $\mathrm{V} = (\mathrm{A}/f\mathrm{A})^{2m}$. *Let* $B(x, y) = \langle (x_1, \ldots, x_{2m}), (y_1, \ldots, y_{2m}) \rangle = -x_1 y_{m+1} - \cdots - x_m y_{2m} + x_{m+1} y_1 + \cdots + x_{2m} y_m$, $B(x, y) = -B(y, x)$. *Let* $W = \langle e_1, \ldots, e_m \rangle$ *is a maximal isotropic subgroup, such that for any* u *and* $v \in W$ $B(u, v) = 0$. *Let* $\Gamma_B = \{\gamma : \forall u, v \, B(\gamma u, \gamma v) = B(u, v)\}$.

4.2.5 Bijection between left cosets and points on algebraic variety

We start with two simple examples providing the evident correspondence between decomposition of the double cosets into left cosets and the projective points.

Example 4.13 ($\mathrm{GL}_2(\mathbb{Z})$) *Let's take an element* $g = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. *The corresponding variety is* $\mathcal{X}_g = \mathbb{P}^1(\mathbb{F}_p)$. *The double coset* $\Gamma g \Gamma$ *consits of* $p + 1$ *left cosets:*

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & p \end{pmatrix}, \ldots, \begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix}, \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right\},$$

corresponding to $p + 1$ *points of* $\mathcal{X}_g$*:*

$$\{(0, 1), (1, 1), \ldots, (p-1, 1), (1, 0)\}.$$

EXAMPLE 4.14 ($\mathrm{GL}_3(\mathbb{Z})$) *Consider the Hecke operator* $t(1,1,p)$ *in the case of* $\mathrm{GL}_3(\mathbb{Z})$. *Three types of matices are associated to this class :*

$$\left\{ \begin{pmatrix} p & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & * & 0 \\ 0 & p & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & p \end{pmatrix} \right\}.$$

There are $1 + p + p^2 = \dfrac{p^3 - 1}{p - 1}$ *elements in this set. The projective space* $\mathbb{P}^2$ *has the same number of elements, which correspond to*

$$\left\{ \textit{point at } \infty, p \textit{ projective lines}, p^2 \textit{ projective planes} \right\}.$$

The list of left cosets for the basis Hecke operators π_i (recall the definition (1.17) on page 34) can be constructed using [AZ95, Lemma 2.18, page 114]. It was mentioned above, that there is a bijection between left cosets g_i that are contained into double coset $\Gamma g \Gamma$ and the elements δ_i from the presentation $\Gamma = \bigcup \Gamma_{(g)} \delta_i$. The canonical form of the double coset is represented by the Smith normal form of the matrix. Therefore, $\delta_i = V^{-1}$, where V is the transition matrix in Smith normal form presentation of g_j: $g = U g_j V$. The map to the opposite direction is given by the Hermite normal form of the product $g\delta_i$.

Let us establish a correspondence between the classes of the decomposition $\Gamma = \bigcup \Gamma_{(g)} \delta_i$ and the points of the projective space $\mathbb{P}^{n-1}(\mathbb{F}_q)$. We choose the SNF form to be the diagonal matrix with the largest element at the end of the diagonal (as implemented in mathematical computer program Magma). Therefore, the matrix $\alpha = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & f \end{smallmatrix}\right)$ is in Smith normal form. Note, that the SNF presentation with the largest element at the top left corner of the matrix is also widely used, for example, in PARI and SAGE software.

Notice that for the vector $v = \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right)$ the group $\Gamma_{(\alpha)} = \alpha^{-1} \Gamma \alpha \cap \Gamma$ preseves its linear shell $\Gamma_{(\alpha)} \langle v \rangle = \langle v \rangle$, that is $\Gamma_{(\alpha)}$ is a stabilizer of the vector v. It follows that the orbit of Γ is $\mathbb{P}^{n-1}(\mathbb{F}_q)$ and the correspondence between elements is bijective.

Let $x_0 = \langle v \rangle$. Then $\mathrm{Orbit}(x_0) = \Gamma / \mathrm{Stab}(x_0)$, so that $\gamma x_0 \longleftrightarrow \gamma \mathrm{Stab}(x_0)$ and $\Gamma = \bigcup_{\gamma \in \Gamma / \mathrm{Stab}(x_0)} \gamma \mathrm{Stab}(x_0) = \bigcup \mathrm{Stab}(x_0) \gamma^{-1}$. Now we compare this decomposition with $\Gamma = \bigcup \Gamma_{(\alpha)} \delta_i$. It follows that $\mathrm{Stab}(x_0) = \Gamma_{(\alpha)}$ and $\delta_i = \gamma^{-1}$, that is $\gamma = \delta_i^{-1}$ is a system of representatives of the right cosets. On the other hand $\delta_i^{-1} = V_i$, where V_i is the transition matrix of the Smith normal form $\alpha = U_i g_i V_i$. Finally, γx_0 corresponds to the last column of the matrix V_i (which is equals to δ_i^{-1}).

The algorithm in Appendix D outputs the list of left cosets and their corresponding elements δ_i^{-1} together with the projective point. In this algorithm we consider the Hecke algebra over the polynomials with coefficients from the finite field F_p.

EXAMPLE 4.15 *Consider*

$$n = 3,\ p = 3,\ f = T^2 + 2T + 2,\ g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & f \end{pmatrix},$$

then there are 91 left cosets Γg_i *in the decomposition of* $\Gamma g \Gamma$. *There are also 91 points on the projective space* $\mathbb{P}^2(\mathbb{F}_9)$, *which are in one-to-one correspondence with the cosets* Γg_i. *For example, the coset representative* $\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2T+1 \\ 0 & 0 & f \end{pmatrix}$ *corresponds to the point* $(2T : T + 2 : 1)$. *The complete list for this model example is given in the table D.1 in the Appendix D at page 142.*

The one-way function construction in a general case consists of the combination of:

ϕ_c — based on Drinfeld modules;

a mapping of the form σ with a suitable power e for of each affine coordinate like in [GLPR03];

$*g$ — multiplication by a group element.

To increase the security and stability against attacks it is possible to add a "zero"-polynomial of a type $x^{q^d} - x$. A "zero"-function on projective space could be constructed as a product of "zero"-functions of different affine charts.

We plan do develop this topic in details in a future research. We hope that this chapter, including the Appendix C and D, gives a good basis for developing an efficient and highly secured encoding algorithm. The research is not limited by consideration of general linear group, but also can be extended to the symplectic version and general flag varieties over finite fields.

Appendix A

Spherical image of the series $\mathbf{D}_p^{(4)}$

Note by $m_{i_1 i_2 i_3 i_4}$ the monomial symmetric function (see Section 1.3.4). Consider the Hecke power series (2.1) of Section 2.2:

$$\mathbf{D}_p(X) = \sum_{\delta=0}^{\infty} \mathbf{T}(p^\delta) X^\delta$$

For genus $n = 4$ there is the following explicit polynomial presentation for the spherical image of the above series:

$$\Omega(\mathbf{D}_p(X)) = \frac{E_4(X)}{F_4(X)} \ ,$$

where

$$\begin{aligned} F_4(X) = {} & (1 - x_0 X)(1 - x_0 x_1 X)(1 - x_0 x_2 X)(1 - x_0 x_3 X)(1 - x_0 x_4 X) \\ & \times (1 - x_0 x_1 x_2 X)(1 - x_0 x_1 x_3 X)(1 - x_0 x_1 x_4 X)(1 - x_0 x_2 x_3 X) \\ & \times (1 - x_0 x_2 x_4 X)(1 - x_0 x_3 x_4 X)(1 - x_0 x_1 x_2 x_3 X)(1 - x_0 x_1 x_2 x_4 X) \\ & \times (1 - x_0 x_1 x_3 x_4 X)(1 - x_0 x_2 x_3 x_4 X)(1 - x_0 x_1 x_2 x_3 x_4 X) \end{aligned}$$

and

$$E_4(X) = \sum_{k=0}^{14} K_k(p, x_0, x_1, x_2, x_3, x_4) X^k$$

with coefficients K_k below:

$$
\begin{aligned}
K_0 &= 1\ ,\\
K_1 &= 0\ ,\\
K_2 &= -x_0^2p^{-2}\big(p\,(m_{2211}+m_{2110}+m_{1100})\\
&\quad +(p^2+p+1)(m_{2111}+m_{1110})+(2p^2+4p+1)\,m_{1111}\big)\ ,\\
K_3 &= x_0^3p^{-3}\big(p\,(p+1)(m_{3222}+m_{3221}+m_{3211}+m_{3111}+m_{2220}\\
&\quad +m_{2210}+m_{2110}+m_{1110})+(p^3+5p^2+5p+1)(m_{2222}\\
&\quad +m_{2221}+m_{2211}+m_{2111}+m_{1111})\big)\ ,\\
K_4 &= -x_0^4p^{-4}\big(p^2(m_{4322}+m_{4221}+m_{3220}+m_{2210})+p\,(p^2+p+1)\\
&\quad \times(m_{4222}+m_{3333}+m_{3331}+m_{3311}+m_{3111}+m_{2220}\\
&\quad +m_{1111})+p\,(p^2+4p+1)(m_{3332}+m_{3321}+m_{3211}+m_{2111})\\
&\quad +p\,(3p^2+6p+4)(m_{3322}+m_{3221}+m_{2211})+(5p^3+15p^2+6p\\
&\quad +1)(m_{3222}+m_{2221})+(12p^3+22p^2+16p+1)\,m_{2222}\big)\ ,\\
K_5 &= x_0^5p^{-4}\big((p^2+p)(m_{4433}+m_{4432}+m_{4422}+m_{4331}+m_{4321}\\
&\quad +m_{4221}+m_{3311}+m_{3211}+m_{2211})+(4p^2+5p+1)(m_{4333}\\
&\quad +m_{4332}+m_{4322}+m_{4222}+m_{3331}+m_{3321}\\
&\quad +m_{3221}+m_{2221})+(-p^4+14p^2+18p+5)(m_{3333}+m_{3332}\\
&\quad +m_{3322}+m_{3222}+m_{2222})\big)\ ,\\
K_6 &= x_0^6p^{-6}\big(p^2(p^3-5p-4)(m_{4432}+m_{4322}+m_{3222}+m_{4443})\\
&\quad +p\,(p^5+5p^4-17p^2-15p-1)(m_{4333}+m_{3332})-p^2(p+1)(m_{4331}\\
&\quad +m_{3321}+m_{5332}+m_{5433})+p\,(3p^4-12p^2-6p-1)(m_{4332}\\
&\quad +m_{3322}+m_{4433})+p^2(p^3-3p-1)(m_{4222}+m_{3331}+m_{2222}\\
&\quad +m_{4422}+m_{4442}+m_{4444}+m_{5333})+p^3(m_{6333}-m_{5443}\\
&\quad -m_{5432}-m_{5322}-m_{4431}-m_{4321}+m_{3330}-m_{3221})\\
&\quad +(2p^6+12p^5-32p^3-22p^2-4p+1)\,m_{3333}\big)\ ,\\
K_7 &= -x_0^7p^{-5}\big(p\,(p^2-1)(m_{5544}+m_{5543}+m_{5533}+m_{5442}+m_{5432}\\
&\quad +m_{5332}+m_{4422}+m_{4322}+m_{3322})+(p^4+4p^3-4p-1)\\
&\quad \times(m_{5444}+m_{5443}+m_{5433}+m_{5333}+m_{4442}+m_{4432}\\
&\quad +m_{4332}+m_{3332})+(5p^4+14p^3-14p-5)(m_{4444}+m_{4443}\\
&\quad +m_{4433}+m_{4333}+m_{3333})\big)\ ,
\end{aligned}
$$

$$
\begin{aligned}
K_8 &= x_0^8 p^{-6}\big((p^5+15p^4+17p^3-5p-1)(m_{5444}+m_{4443})-p^3(m_{7444}\\
&\quad -m_{6554}-m_{6543}-m_{6433}-m_{5542}-m_{5432}+m_{4441}\\
&\quad -m_{4332})+p\,(4p^3+5p^2-1)(m_{5554}+m_{5543}+m_{5433}\\
&\quad +m_{4333})+p^3(p+1)(m_{6544}+m_{6443}+m_{5442}+m_{4432})\\
&\quad +p\,(p^3+3p^2-1)(m_{4442}+m_{5333}+m_{5533}+m_{5555}+m_{6444}\\
&\quad +m_{5553}+m_{3333})-(p^6-4p^5-22p^4-32p^3+12p+2)\,m_{4444}\\
&\quad +p\,(p^4+6p^3+12p^2-3)(m_{5544}+m_{5443}+m_{4433})\big)\ ,\\
K_9 &= -x_0^9 p^{-6}\big(p^2(p+1)(m_{6655}+m_{6654}+m_{6644}+m_{6553}+m_{6543}\\
&\quad +m_{6443}+m_{5533}+m_{5433}+m_{4433})+p^2(p^2+5p+4)(m_{6555}\\
&\quad +m_{6554}+m_{6544}+m_{6444}+m_{5553}+m_{5543}\\
&\quad +m_{5443}+m_{4443})+(5p^4+18p^3+14p^2-1)(m_{5555}+m_{5554}\\
&\quad +m_{5544}+m_{5444}+m_{4444})\big)\ ,\\
K_{10} &= x_0^{10} p^{-5}\big((p^2+p+1)(m_{4444}+m_{5553}+m_{6444}+m_{6644}\\
&\quad +m_{6664}+m_{6666}+m_{7555})+(p^2+4p+1)(m_{5444}+m_{6544}\\
&\quad +m_{6654}+m_{6665})+p\,(m_{5543}+m_{6553}+m_{7554}+m_{7655})\\
&\quad +(4p^2+6p+3)(m_{5544}+m_{6554}+m_{6655})+(p^3+6p^2+15p+5)\\
&\quad \times(m_{5554}+m_{6555})+(p^3+16p^2+22p+12)m_{5555}\big)\ ,\\
K_{11} &= -x_0^{11} p^{-6}\big(p\,(p+1)(m_{7666}+m_{7665}+m_{7655}+m_{7555}+m_{6664}\\
&\quad +m_{6654}+m_{6554}+m_{5554})+(p^3+5p^2+5p+1)(m_{6666}\\
&\quad +m_{6665}+m_{6655}+m_{6555}+m_{5555})\big)\ ,\\
K_{12} &= x_0^{12} p^{-6}\big((p^2+p+1)(m_{6665}+m_{7666})+(p^2+4p+2)\,m_{6666}\\
&\quad +p\,(m_{7665}+m_{7766}+m_{6655})\big)\ ,\\
K_{13} &= 0\ ,\\
K_{14} &= -x_0^{14} p^{-6} m_{7777}\ .
\end{aligned}
$$

Appendix B

Coefficients of $L(s, \Delta \otimes g_{20})$

SAGE listing

```
sage: num = 150
sage: # dq - q-expansion of Delta function
sage: dq=delta_qexp(prec=num+1)
sage: # tau - Ramanujan's tau function
sage: tau = []
sage: tau.append(0)
sage: dc=dq.coefficients()
sage: tau.extend(dc)
sage: b = []
sage: b.append(0)
sage: S20 = CuspForms(1,weight=20)
sage: g20 = S20.0
sage: t=g20.q_expansion(prec=num+1)
sage: b.extend(t.coefficients())
sage: A = []
sage: A.append(0)
sage: for n in range(1,num+1):
...       t = 0
...       for d in range(1,n^(1/2)+1):
...           i = floor(n/(d^2))
...           if i == (n+0.0)/(d^2):
...               t = t + d^30*tau[i]*b[i]
...       A.append(t)
sage: print '%2s %9s %15s %22s'%("n","\Delta","g_{20}","A")
sage: print "--|---------|---------------|----------------------"
sage: for i in range(1,21):
...       print '%2s %9s %15s %22s'%(i, tau[i], b[i], A[i])
```

Table B.1: Coefficients of $L(s, \Delta \otimes g_{20})$

n	τ	g_{20}	A
1	1	1	1
2	−24	456	−10944
3	252	50652	12764304
4	−1472	−316352	1539411968
5	4830	−2377410	−11482890300
6	−6048	23097312	−139692542976
7	−16744	−16917544	283267356736
8	84480	−383331840	−44134904365056
9	−113643	1403363637	46408678295058
10	−115920	−1084098960	125668751443200
11	534612	−16212108	−8667187482096
12	−370944	−16023861504	19649522340790272
13	−577738	50421615062	−29130483042689756
14	401856	−7714400064	−3100077952118784
15	1217160	−120420571320	−146571102587851200
16	987136	−8939761664	1644106253837795328
17	−6905934	225070099506	−1554319252561868604
18	2727432	639933818472	−507896575261114752
19	10661420	−1710278572660	−18233998180128777200
20	−7109760	752098408320	−17676898755051110400

Appendix C

Cryptosystem model in SAGE

The simple way to experiment with different models of cryptosystem is to use the interactive interface of SAGE. The theoretical part of the cryptosystem is presented in the section 4.2.1, page 109.

The use of projective space provides an additional security for the cryptology system. However, the presented computer program provides just a scheme for the real cryptology model. In order to implement a real cryptosystem it is necessary to program the one-way function with the help of efficient algorithms for sparse polynomials (term by term operation on vectors, representing the polynomial coefficients). It is also possible to adopt the software code developed by Roblot in [GLPR03]. It is also necessary to conduct a thorow cryptanalysis in order to make an appropriate choice of the parameters of the proposed cryptosystem.

First, we define the polynomial rings:

SAGE listing

```
sage: # prime number
sage: p = 3
sage: # mod polynomial degree
sage: d = 2
sage: A.<T>  = PolynomialRing(IntegerModRing(p))
sage: print "A :", A
sage: PA.<t> = PolynomialRing(A)
sage: Pz.<z> = PolynomialRing(A)
sage: print "PA :", PA
sage: # mod polynomial (irreducible in PA[T] degree d)
sage: f = T^2 + 1
sage: print "f =", f
sage: print "is f irreducible?", f.is_irreducible()
sage: # define a quotient B=A/f
```

```
sage: B = A.quo(f)
sage: PB.<s> = PolynomialRing(B)
sage: print "B :", B
A : Univariate Polynomial Ring in T over Ring of integers modulo 3
PA : Univariate Polynomial Ring in t over Univariate Polynomial
  Ring in T over Ring of integers modulo 3
f = T^2 + 1
is f irreducible? True
B : Univariate Quotient Polynomial Ring in Tbar over Ring of
  integers modulo 3 with modulus T^2 + 1
```

Now, we define the multiplication operation in $\mathcal{A}[T]\{\tau\}$ and the exponentiation:

SAGE listing

```
sage: # define multiplication rule in PA[t]
sage: def mul_PA(a,b):
...       a = PA(a)
...       b = PA(b)
...       c = 0
...       for ia in a.dict().items():
...           for ib in b.dict().items():
...               c = c + ia[1]*(ib[1]^(p^ia[0]))*t^(ia[0]+ib[0])
...       return PA(c)
...
sage: # define exponentiation operation in PA[t]
sage: def pow_PA(a,k):
...       a = PA(a)
...       if k==0:
...           return PA(1)
...       if k==1:
...           return a
...       c = a
...       while k>1:
...           c = mul_PA(c,a)
...           k = k-1
...       return c
```

The global variable *dm* is used for defining the Drinfeld module. The procedure $DM(x)$ computes the morphism corresponding to x.

SAGE listing

```
sage: # 'dm' is a global variable defining the Drinfeld module
sage: dm = t+T
```

```
...
sage: # define Drinfeld module morphism
sage: def DM(x):
...       x = A(x)
...       degx = x.degree()
...       coex = x.coeffs()
...       res = 0
...       fac = 1
...       for i in range(degx+1):
...           res = res + coex[i]*fac
...           fac = mul_PA(fac,dm)
...       return PA(res)
...
sage: # define phi_c
sage: def phi_c(c):
...       x = DM(c)
...       y = 0
...       for i in x.dict().items():
...           y = y + i[1]*z^(p^i[0])
...       return Pz(y)
```

Multiplication example.

SAGE listing

```
sage: a = T^2 + 2*T + 1
sage: b = 2*T^2 + T + 1
sage: print "   {T^2 + 2*T + 1} *    {2*T^2 + T + 1} =",a*b
sage: print "bar{T^2 + 2*T + 1} * bar{2*T^2 + T + 1} =",B(a*b)
   {T^2 + 2*T + 1} *    {2*T^2 + T + 1} = 2*T^4 + 2*T^3 + 2*T^2 + 1
bar{T^2 + 2*T + 1} * bar{2*T^2 + T + 1} = Tbar + 1
```

Inverting elements in B:

SAGE listing

```
sage: ### inverting elements in B
sage: x = B(T^2 + T + 1)
sage: print 1/x
2*Tbar
```

Computation of $B(\phi_a(b))$ by two methods: with the use of basis monomials and direct method:

SAGE listing

```
sage: ### a = 2*T^2 + 1
sage: ### b = B(T^2 + T + 1)
```

```
sage: ### goal: compute B(phi_a(b))
sage: a = 2*T^2 + 1
sage: b = B(T^2 + T + 1)
sage: print "a =", a
sage: print "b =", b
sage: print "goal: compute B(phi_a(b))\n"
sage: ### computing phi_1-basis
sage: ph1 = phi_c(1)
sage: print "phi_1(z) =",ph1
sage: ph1_1 = B(ph1(1))
sage: print "bar{phi_1( 1 )} =",ph1_1
sage: ph1_T = B(ph1(T))
sage: print "bar{phi_1( T )} =",ph1_T
sage: ph1_T2 = B(ph1(T^2))
sage: print "bar{phi_1(T^2)} =",ph1_T2
sage: ### computing phi_T-basis
sage: phT = phi_c(T)
sage: print "\nphi_T(z) =",phT
sage: phT_1 = B(phT(1))
sage: print "bar{phi_T( 1 )} =",phT_1
sage: phT_T = B(phT(T))
sage: print "bar{phi_T( T )} =",phT_T
sage: phT_T2 = B(phT(T^2))
sage: print "bar{phi_T(T^2)} =",phT_T2
sage: ### computing phi_{T^2}-basis
sage: phT2_1 = B(phT(lift(phT_1)))
sage: print "\nbar{phi_{T^2}( 1 )} =",phT2_1
sage: phT2_T = B(phT(lift(phT_T)))
sage: print "bar{phi_{T^2}( T )} =",phT2_T
sage: phT2_T2 = B(phT(lift(phT_T2)))
sage: print "bar{phi_{T^2}(T^2)} =",phT2_T2,"\n"
sage: ### finally B(phi_a(b)) = B(2*phi_{T^2}(b)) + B(phi_1(b))
sage: print "computing B(phi_a(b)) using basis  :",
  2*phT2_T2 + 2*phT2_T + 2*phT2_1 + ph1_T2 + ph1_T + ph1_1
sage: print "computing directly by 'phi_c(a)(b)':", phi_c(a)(b)
a = 2*T^2 + 1
b = Tbar
goal: compute B(phi_a(b))

phi_1(z) = z
bar{phi_1( 1 )} = 1
bar{phi_1( T )} = Tbar
bar{phi_1(T^2)} = 2
```

```
phi_T(z) = z^3 + T*z
bar{phi_T( 1 )} = Tbar + 1
bar{phi_T( T )} = 2*Tbar + 2
bar{phi_T(T^2)} = 2*Tbar + 2

bar{phi_{T^2}( 1 )} = 0
bar{phi_{T^2}( T )} = 0
bar{phi_{T^2}(T^2)} = 0

computing B(phi_a(b)) using basis  : Tbar
computing directly by 'phi_c(a)(b)': Tbar
```

The polynomial f_ϕ is a characteristic polynomial:

SAGE listing

```
sage: ### computing characteristic polynomial
sage: phT = phi_c(T)
sage: phT_list = []
sage: for i in range(d):
...       phT_list.append(lift(B(phT(T^i))))
...
sage: C = matrix(d,d,[0 for i in range(d^2)])
sage: for j in range(d):
...       d_max = phT_list[j].degree()
...       coe = phT_list[j].coeffs()
...       for i in range(d_max):
...           C[i,j] = coe[i]
...
sage: f_phi = C.characteristic_polynomial()(T)
sage: print "f_phi =", f_phi
f_phi = T^2 + 2*T
```

Working with a projective plane over finate field, list of elements:

SAGE listing

```
sage: N = 3 # dimension
sage: p = 3 # prime number
sage: d = 2 # degree
sage: # define a polynomial ring over (Z mod p) in variable 's'
sage: P.<s>=PolynomialRing(Integers(p))
sage: # define an irreducible polynomial to generate a finite field
sage: f = s^2+1
sage: # define a finite field
```

```
sage: FF = FiniteField(p^d,'T',modulus=f)
sage: T = FF.gen()
sage: # define a projective space
sage: X = ProjectiveSpace(N-1,FF)
sage: x = gens(X)
sage: X_list = [x for x in X]
sage: X_list.sort()
sage: i = 1
sage: for x in X_list:
...       print '%3s  (%7s : %7s : %1s)'%(i,x[0],x[1],x[2])
...       i+=1
  1  (      0 :       0 : 1)
  2  (      0 :       1 : 0)
  3  (      0 :       1 : 1)
  4  (      0 :       2 : 1)
  5  (      0 :       T : 1)
  6  (      0 :   T + 1 : 1)
  7  (      0 :   T + 2 : 1)
  8  (      0 :     2*T : 1)
  9  (      0 : 2*T + 1 : 1)
 10  (      0 : 2*T + 2 : 1)
 11  (      1 :       0 : 0)
 12  (      1 :       0 : 1)
...
... truncated output
...
 84  (2*T + 2 :       1 : 1)
 85  (2*T + 2 :       2 : 1)
 86  (2*T + 2 :       T : 1)
 87  (2*T + 2 :   T + 1 : 1)
 88  (2*T + 2 :   T + 2 : 1)
 89  (2*T + 2 :     2*T : 1)
 90  (2*T + 2 : 2*T + 1 : 1)
 91  (2*T + 2 : 2*T + 2 : 1)
```

Exponentiation procedure and the result for affine chart of the type $(* : * : 1)$:

SAGE listing

```
sage: ##################################################################
sage: # exponentiation
sage: # input:
sage: #     pp - point in Projective Space
sage: #     pe - exponent vector (list)
```

```
sage: # output:
sage: #     the element of the projective space pp^pe
sage: # global variables:
sage: #     X - projective space
sage: ################################################################
sage: def myexp(pp,pe):
...       res = []
...       e_max = pe[0]
...       i_max = 0
...       n = X.dimension()
...       for i in range(1,n):
...           if e_max < pe[i]:
...               e_max = pe[i]
...               i_max = i
...       for i in range(n):
...           res.append(pp[n]^(pe[i_max]-pe[i])*pp[i]^pe[i])
...       res.append(pp[n]^pe[i_max])
...       return X(res)
sage: pe = [5,7,9]
sage: n = X.dimension()
sage: for x in X_list:
...       if x[n] != 0:
...           print '%25s %25s'%(x,myexp(x,pe))
              (0 : 0 : 1)               (0 : 0 : 1)
              (0 : 1 : 1)               (0 : 1 : 1)
              (0 : 2 : 1)               (0 : 2 : 1)
              (0 : T : 1)             (0 : 2*T : 1)
          (0 : T + 1 : 1)           (0 : T + 2 : 1)
          (0 : T + 2 : 1)           (0 : T + 1 : 1)
            (0 : 2*T : 1)               (0 : T : 1)
        (0 : 2*T + 1 : 1)         (0 : 2*T + 2 : 1)
        (0 : 2*T + 2 : 1)         (0 : 2*T + 1 : 1)
              (1 : 0 : 1)               (1 : 0 : 1)
...
... truncated output
...
        (2*T + 2 : 1 : 1)           (T + 1 : 1 : 1)
        (2*T + 2 : 2 : 1)           (T + 1 : 2 : 1)
        (2*T + 2 : T : 1)         (T + 1 : 2*T : 1)
    (2*T + 2 : T + 1 : 1)       (T + 1 : T + 2 : 1)
    (2*T + 2 : T + 2 : 1)       (T + 1 : T + 1 : 1)
      (2*T + 2 : 2*T : 1)           (T + 1 : T : 1)
  (2*T + 2 : 2*T + 1 : 1)     (T + 1 : 2*T + 2 : 1)
```

```
  (2*T + 2 : 2*T + 2 : 1)     (T + 1 : 2*T + 1 : 1)
```

Procedure for computing ϕ_c in a projective space and an example for $\phi_c = (z^3 + (T+1)\,z, z^3 + (T+2)\,z)$:

SAGE listing

```
sage: ####################################################################
sage: # phi_c
sage: # input:
sage: #     pp - point in Projective Space
sage: #     pc - phi_c[i] polynomials (list)
sage: # output:
sage: #     the element of the projective space phi_c(pp)
sage: # global variables:
sage: #     X - projective space
sage: # note:
sage: #     the last coordinate is always either 0, or 1
sage: ####################################################################
sage: def phi_c(pp,pc):
...       res = []
...       n = X.dimension()
...       d_max = 0
...       for c in pc:
...           if d_max < c.degree():
...               d_max = c.degree()
...       for i in range(n):
...           res.append(pc[i](pp[i]/pp[n])*pp[n]^d_max)
...       res.append(pp[n]^d_max)
...       return X(res)
sage: Pz=PolynomialRing(FF,'z')
sage: z=Pz.gen()
sage: pc=[]
sage: pc.append(z^3+(T+1)*z)
sage: pc.append(z^3+(T+2)*z)
sage: print 'pc = ', pc
sage: n = X.dimension()
sage: res = []
sage: for x in X_list:
...       if x[n] != 0:
...           print '%25s %25s'%(x,phi_c(x,pc))
pc =  [z^3 + (T + 1)*z, z^3 + (T + 2)*z]
              (0 : 0 : 1)               (0 : 0 : 1)
              (0 : 1 : 1)               (0 : T : 1)
              (0 : 2 : 1)            (0 : 2*T : 1)
```

```
             (0 : T : 1)           (0 : T + 2 : 1)
          (0 : T + 1 : 1)         (0 : 2*T + 2 : 1)
          (0 : T + 2 : 1)               (0 : 2 : 1)
            (0 : 2*T : 1)         (0 : 2*T + 1 : 1)
        (0 : 2*T + 1 : 1)               (0 : 1 : 1)
        (0 : 2*T + 2 : 1)           (0 : T + 1 : 1)
             (1 : 0 : 1)            (T + 2 : 0 : 1)
...
... truncated output
...
        (2*T + 2 : 1 : 1)         (2*T + 2 : T : 1)
        (2*T + 2 : 2 : 1)       (2*T + 2 : 2*T : 1)
        (2*T + 2 : T : 1)     (2*T + 2 : T + 2 : 1)
    (2*T + 2 : T + 1 : 1)   (2*T + 2 : 2*T + 2 : 1)
    (2*T + 2 : T + 2 : 1)         (2*T + 2 : 2 : 1)
      (2*T + 2 : 2*T : 1)   (2*T + 2 : 2*T + 1 : 1)
  (2*T + 2 : 2*T + 1 : 1)         (2*T + 2 : 1 : 1)
  (2*T + 2 : 2*T + 2 : 1)     (2*T + 2 : T + 1 : 1)
```

Finally, the matrix action on the projective space:

SAGE listing

```
sage: # construct an invertible matrix
sage: M = MatrixSpace(FF,N)
sage: RU = M([T,2,T,0,T+1,T+2,0,0,2*T])
sage: RL = M([2*T+1,0,0,2*T+2,T+1,0,2,T,T+1])
sage: R = RU*RL
sage: print R, R.det()
[  T + 2 2*T + 1   T + 2]
[      1   T + 2       1]
[      T       1 2*T + 1] T
sage: # example of matrix action on a projective space point
sage: V = VectorSpace(FF,N)
sage: for x in X_list:
...       print '%25s %25s'%(x,X(list( V(list(x))*R.transpose()) ))
             (0 : 0 : 1)           (2 : 2*T + 2 : 1)
             (0 : 1 : 0)       (2*T + 1 : T + 2 : 1)
             (0 : 1 : 1)             (0 : T + 1 : 1)
             (0 : 2 : 1)       (T + 1 : 2*T + 1 : 1)
             (0 : T : 1)             (2*T : 2*T : 1)
          (0 : T + 1 : 1)         (2*T + 2 : 1 : 1)
          (0 : T + 2 : 1)         (2*T + 1 : 1 : 0)
            (0 : 2*T : 1)           (T + 2 : T : 1)
        (0 : 2*T + 1 : 1)               (T : 2 : 1)
```

```
        (0 : 2*T + 2 : 1)              (1 : 0 : 1)
             (1 : 0 : 0)         (T + 1 : 2*T : 1)
             (1 : 0 : 1)         (2*T + 1 : 2 : 1)
...
... truncated output
...
        (2*T + 2 : 1 : 1)              (T : T : 1)
        (2*T + 2 : 2 : 1)            (T + 1 : 1 : 1)
        (2*T + 2 : T : 1)              (1 : 2*T : 1)
    (2*T + 2 : T + 1 : 1)            (2 : T + 1 : 1)
    (2*T + 2 : T + 2 : 1)          (2*T + 2 : 0 : 1)
      (2*T + 2 : 2*T : 1)              (0 : 2 : 1)
  (2*T + 2 : 2*T + 1 : 1)          (2*T + 2 : 1 : 0)
  (2*T + 2 : 2*T + 2 : 1)      (T + 2 : 2*T + 2 : 1)
```

Appendix D

Correspondence between left cosets in the case of the ring $\mathbb{F}_q[T]$

This appendix describes the practical implementation of the theory exposed in the section 4.2.5, page 115.

magma listing

```
> //
> // Lemma 2.18, page 114 for Finite Field F_{p}
> // case \pi_i (\alpha contains exactly "i" "1")
>
> p := 3;
> d := 2;
> q := p^d;
> alpha := [0,0,1];
> n := 3;
>
> // first of all count how many '1' in \alpha
> i := 0;
> for x in alpha do
for>   i := i+x;
for> end for;
>
> // define the finite field
> FFp<a> := FiniteField(p);
>
> // define Polynomial Ring over FFp
> PR<T> := PolynomialRing(FFp);
>
```

```
> // define matrix space over PR
> M := MatrixAlgebra(PR,n);
>
> // define Quotient Ring
> f := T^2+2*T+2;
> PQ<t> := quo<PR|f>;
>
> // list of elements in FFq
> FFq_list := [*0*];
> k := 0;
> for k in [1..q-1] do
for>   Append(~FFq_list,t^k);
for> end for;
>
> // computing function \phi_i_ff
> phiff := func<i, q | &*[q^j - 1 : j in [1..i]] >;
>
> // the quantity of the elements in the class is
> qtt := phiff(n,q)/phiff(i,q)/phiff(n-i,q);
> print "there are",qtt,"left classes in the considered double class";
there are 91 left classes in the considered double class
>
>
> // construct matrix D, corresponding to \pi_i
> // it is diagonal of the form [E_{n-i},fE_i]
> D := M!1; // identity matrix
> for j in [1..n] do
for>   if alpha[j] eq 1 then
for|if>     D[j,j] := f;
for|if>   end if;
for> end for;
>
> // C_list - the list of C_{\alpha,i}
> C_list := [* *];
> V_list := [* *];
>
> // writing down all permutations for alpha as 2^n cycle
> al := [0 : k in [1..n]];
> for ji in [1..2^n-1] do
for>   flag := 1;
for>   for j in [1..n] do
for|for>     if flag eq 1 then
for|for|if>       al[n-j+1] := al[n-j+1]+1;
```

```
for|for|if>       if al[n-j+1] eq 2 then
for|for|if|if>         al[n-j+1] := 0;
for|for|if|if>       else
for|for|if|if>         flag := 0;
for|for|if|if>       end if;
for|for|if>     end if;
for|for>   end for;
for>   ni := 0;
for>   for x in al do
for|for>     if x eq 1 then
for|for|if>       ni := ni+1;
for|for|if>     end if;
for|for>   end for;
for>   if ni eq i then
for|if>   // main cycle
for|if>     pos := [* *]; // create the list of 'positions' of '1'
for|if>     C := M!0;
for|if>     for j in [1..n] do
for|if|for>       // place 'f' on diagonal if a[j]==1
for|if|for>       if al[j] eq 1 then
for|if|for|if>         C[j,j] := f;
for|if|for|if>         // also we note the position of this column
for|if|for|if>         // where to put non zero elements
for|if|for|if>         for k in [1..j-1] do
for|if|for|if|for>           if C[k,k] eq 1 then
for|if|for|if|for|if>             Append(~pos,[k,j]);
for|if|for|if|for|if>           end if;
for|if|for|if|for>         end for;
for|if|for|if>       else
for|if|for|if>         C[j,j] := 1;
for|if|for|if>       end if;
for|if|for>     end for;
for|if>     npos := 0;
for|if>     for j in pos do
for|if|for>       npos := npos+1;
for|if|for>     end for;
for|if>     Append(~C_list,M!C);
for|if>     S,U,V := SmithForm(M!C);
for|if>     Append(~V_list,V);
for|if>     ct := [* 0 : k in [1..npos] *];
for|if>     for k in [1..q^npos-1] do
for|if|for>       flag := 1;
for|if|for>       for j in [0..npos-1] do
```

```
for|if|for|for>         if flag eq 1 then
for|if|for|for|if>           ct[npos-j] := ct[npos-j]+1;
for|if|for|for|if>           if ct[npos-j] eq q then
for|if|for|for|if|if>             ct[npos-j] := 0;
for|if|for|for|if|if>          else
for|if|for|for|if|if>             flag := 0;
for|if|for|for|if|if>          end if;
for|if|for|for|if>          end if;
for|if|for|for>       end for;
for|if|for>       for j in [0..npos-1] do
for|if|for|for>         l := ct[npos-j]+1;
for|if|for|for>         x := (pos[npos-j])[1];
for|if|for|for>         y := (pos[npos-j])[2];
for|if|for|for>         z := FFq_list[l];
for|if|for|for>         C[x,y] := PR!z;
for|if|for|for>       end for;
for|if|for>       Append(~C_list,M!C);
for|if|for>       S,U,V := SmithForm(M!C);
for|if|for>       Append(~V_list,V);
for|if|for>     end for;
for|if>   // end of main cycle
for|if>   end if;
for> end for;
>
> //============================
> // verification of SNF
>
> S1,U,V := SmithForm(C_list[1]);
> i := 0;
> for C in C_list do
for>   i := i+1;
for>   S,U,V := SmithForm(C);
for>   if S1 ne S then
for|if>     print i,"*** something is wrong with SNF...";
for|if>   end if;
for> end for;
>
> //============================
> // testing HNF for V matrices
> for i in [1..91] do
for>   H := HermiteForm(D*(V_list[i]^(-1)));
for>   if H ne C_list[i] then
for|if>     print i,"*** something is wrong with HNF",C_list[i],H;
```

```
for|if>   end if;
for> end for;
>
> //============================
> // verify that all matrices V have different third column
> x := 0;
> for i in [1..91] do
for> for j in [1..91] do
for|for>   if j gt i then
for|for|if>     a := Transpose(V_list[i])[3];
for|for|if>     b := Transpose(V_list[j])[3];
for|for|if>     if a eq b then
for|for|if|if>       x := x+1;
for|for|if|if>       print " the following columns are the same: ",i,j;
for|for|if|if>     end if;
for|for|if>   end if;
for|for> end for;
for> end for;
> print "there are ",x," equal columns";
there are  0  equal columns
>
> //============================
> // output C_list and V_list
> for i in [1..91] do
for>   print i,"===";
for>   print C_list[i];
for>   print "---";
for>   print V_list[i];
for>   print "---";
for>   print Transpose(V_list[i])[3];
for> end for;
1 ===
[            1            0            0]
[            0            1            0]
[            0            0 T^2 + 2*T + 2]
---
[1 0 0]
[0 1 0]
[0 0 1]
---
(0 0 1)
2 ===
[            1            0            0]
```

```
[            0             1             T]
[            0             0 T^2 + 2*T + 2]
---
[  1   0   0]
[  0   1 2*T]
[  0   0   1]
---
(  0 2*T   1)
3 ===
[            1             0             0]
[            0             1         T + 1]
[            0             0 T^2 + 2*T + 2]
---
[      1       0       0]
[      0       1 2*T + 2]
[      0       0       1]
---
(      0 2*T + 2       1)
4 ===
[            1             0             0]
[            0             1       2*T + 1]
[            0             0 T^2 + 2*T + 2]
---
[    1     0     0]
[    0     1 T + 2]
[    0     0     1]
---
(    0 T + 2     1)
5 ===
[            1             0             0]
[            0             1             2]
[            0             0 T^2 + 2*T + 2]
---
[1 0 0]
[0 1 1]
[0 0 1]
---
(0 1 1)
...
... truncated output
...
88 ===
[            1       2*T + 2             0]
```

```
[            0 T^2 + 2*T + 2             0]
[            0             0             1]
---
[    0     1 T + 1]
[    0     0     1]
[    1     0     0]
---
(T + 1     1    0)
89 ===
[            1         T + 2             0]
[            0 T^2 + 2*T + 2             0]
[            0             0             1]
---
[      0       1 2*T + 1]
[      0       0       1]
[      1       0       0]
---
(2*T + 1       1       0)
\\
90 ===
[            1             1             0]
[            0 T^2 + 2*T + 2             0]
[            0             0             1]
---
[0 1 2]
[0 0 1]
[1 0 0]
---
(2 1 0)
91 ===
[T^2 + 2*T + 2             0             0]
[            0             1             0]
[            0             0             1]
---
[0 0 1]
[1 0 0]
[0 1 0]
---
(1 0 0)
>
```

Table D.1: Correspondence between g_i, δ_i and projective points.

	left coset g_i	matrix δ_i^{-1}	point of $\mathbb{P}^3(\mathbb{F}_9)$
1	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(0:0:1)$
2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(0:2T:1)$
3	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(0:2T+2:1)$
4	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(0:T+2:1)$
5	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(0:1:1)$
6	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(0:T:1)$
7	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(0:T+1:1)$
8	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(0:2T+1:1)$
9	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(0:2:1)$
10	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2T \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:0:1)$
11	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:2T:1)$
12	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:2T+2:1)$
13	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:T+2:1)$
14	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:1:1)$
15	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:T:1)$
16	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:T+1:1)$
17	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:2T+1:1)$
18	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T:2:1)$

continue on the next page

	left coset g_i	matrix δ_i^{-1}	point of $\mathbb{P}^3(\mathbb{F}_9)$
19	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2T+2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:0:1)$
20	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:2T:1)$
21	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:2T+2:1)$
22	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:T+2:1)$
23	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:1:1)$
24	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:T:1)$
25	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:T+1:1)$
26	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:2T+1:1)$
27	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+2:2:1)$
28	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & T+2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:0:1)$
29	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:2T:1)$
30	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:2T+2:1)$
31	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:T+2:1)$
32	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:1:1)$
33	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:T:1)$
34	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:T+1:1)$
35	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:2T+1:1)$
36	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+2:2:1)$
37	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(1:0:1)$

continue on the next page

	left coset g_i	matrix δ_i^{-1}	point of $\mathbb{P}^3(\mathbb{F}_9)$
38	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : 2T : 1)$
39	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : 2T + 2 : 1)$
40	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : T + 2 : 1)$
41	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : 1 : 1)$
42	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : T : 1)$
43	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : T + 1 : 1)$
44	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : 2T + 1 : 1)$
45	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(1 : 2 : 1)$
46	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & T \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(T : 0 : 1)$
47	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(T : 2T : 1)$
48	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T : 2T + 2 : 1)$
49	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T : T + 2 : 1)$
50	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T : 1 : 1)$
51	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(T : T : 1)$
52	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T : T + 1 : 1)$
53	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T : 2T + 1 : 1)$
54	$\begin{pmatrix} 1 & 0 & 2T \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T : 2 : 1)$
55	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & T+1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(T + 1 : 0 : 1)$
56	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(T + 1 : 2T : 1)$

continue on the next page

	left coset g_i	matrix δ_i^{-1}	point of $\mathbb{P}^3(\mathbb{F}_9)$
57	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+1 : 2T+2 : 1)$
58	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+1 : T+2 : 1)$
59	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+1 : 1 : 1)$
60	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(T+1 : T : 1)$
61	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+1 : T+1 : 1)$
62	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+1 : 2T+1 : 1)$
63	$\begin{pmatrix} 1 & 0 & 2T+2 \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & T+1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(T+1 : 2 : 1)$
64	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2T+1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : 0 : 1)$
65	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : 2T : 1)$
66	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : 2T+2 : 1)$
67	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : T+2 : 1)$
68	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : 1 : 1)$
69	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : T : 1)$
70	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : T+1 : 1)$
71	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : 2T+1 : 1)$
72	$\begin{pmatrix} 1 & 0 & T+2 \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2T+1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2T+1 : 2 : 1)$
73	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : 0 : 1)$
74	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2T \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : 2T : 1)$
75	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : 2T+2 : 1)$

continue on the next page

	left coset g_i	matrix δ_i^{-1}	point of $\mathbb{P}^3(\mathbb{F}_9)$
76	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2T+1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & T+2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : T+2 : 1)$
77	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : 1 : 1)$
78	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2T \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : T : 1)$
79	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : T+1 : 1)$
80	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & T+2 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2T+1 \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : 2T+1 : 1)$
81	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & T^2+2T+2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$	$(2 : 2 : 1)$
82	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	$(0 : 1 : 0)$
83	$\begin{pmatrix} 1 & T & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2T \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(2T : 1 : 0)$
84	$\begin{pmatrix} 1 & T+1 & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2T+2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(2T+2 : 1 : 0)$
85	$\begin{pmatrix} 1 & 2T+1 & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & T+2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(T+2 : 1 : 0)$
86	$\begin{pmatrix} 1 & 2 & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(1 : 1 : 0)$
87	$\begin{pmatrix} 1 & 2T & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & T \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(T : 1 : 0)$
88	$\begin{pmatrix} 1 & 2T+2 & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & T+1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(T+1 : 1 : 0)$
89	$\begin{pmatrix} 1 & T+2 & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2T+1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(2T+1 : 1 : 0)$
90	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & T^2+2T+2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$(2 : 1 : 0)$
91	$\begin{pmatrix} T^2+2T+2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$(1 : 0 : 0)$

Bibliography

[AK79] A. N. Andrianov and V. L. Kalinin. On analytic properties of standard zeta functions of Siegel modular forms. *Math. USSR Sbornik*, 35(1):323–339, 495, 1979. Translated from Mat. Sbornik 106(148) (1978) no. 3, 1–17.

[And67] A. N. Andrianov. Shimura's conjecture for Siegel's modular group of genus 3. *Dokl. Akad. Nauk SSSR*, 177(3):755–758, 1967. Translated from Soviet Math. Dokl. 8 (1967), 1474–1478.

[And68] A. N. Andrianov. Rationality of multiple Hecke series of the full linear group and Shimura's hypothesis on Hecke series of the symplectic group. *Dokl. Akad. Nauk SSSR*, 183:9–11, 1968. Translated from Soviet Math. Dokl. 9 (1968), 1295–1297.

[And69] A. N. Andrianov. Rationality theorems for Hecke series and Zeta functions of the groups GL_n and Sp_n over local fields. *Izv. Akad. Nauk SSSR Ser. Mat.*, 33:466–505, 1969. Translated from Math. USSR – Izvestija, Vol. 3 (1969), No. 3, 439–476.

[And70] A. N. Andrianov. Spherical functions for GL_n over local fields, and the summation of Hecke series. *Math. USSR Sbornik*, 12 (3):429–452, 1970. Translated from Mat. Sb. (N.S.), 1970, 83(125), 429–451.

[And77] A. N. Andrianov. On zeta-functions of Rankin type associated with Siegel modular forms. In *Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 325–338. Lecture Notes in Math., Vol. 627. Springer, Berlin, 1977.

[And79] A. N. Andrianov. Modular descent and the Saito-Kurokawa conjecture. *Invent. Math.*, 53(3):267–280, 1979.

[And87] A. N. Andrianov. *Quadratic forms and Hecke operators*, volume 286 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1987.

[AZ95] A. N. Andrianov and V. G. Zhuravlëv. *Modular forms and Hecke operators*, volume 145 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1995. Translated from the 1990 Russian original by Neal Koblitz.

[BCG06] Simon R. Blackburn, Carlos F. A. Cid, and Steven D. Galbraith. Cryptanalysis of a cryptosystem based on Drinfeld modules. *IEE Proc. – Inf. Secur*, 153(1):12–14, 2006.

[BH06] Siegfried Böcherer and Bernhard E. Heim. Critical values of L-functions on $\mathrm{GSp}_2 \times \mathrm{GL}_2$. *Math. Z.*, 254(3):485–503, 2006.

[BK00] Stefan Breulmann and Michael Kuss. On a conjecture of Duke-Imamoḡlu. *Proc. Amer. Math. Soc.*, 128(6):1595–1604, 2000.

[Böc85] Siegfried Böcherer. Über die Funktionalgleichung automorpher L-Funktionen zur Siegelschen Modulgruppe. *J. Reine Angew. Math.*, 362:146–168, 1985.

[CP04] Michel Courtieu and Alexei Panchishkin. *Non-Archimedean L-functions and arithmetical Siegel modular forms*, volume 1471 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, second augmented ed. edition, 2004.

[CV08] Francesco Chiera and Kirill Vankov. On special values of spinor L-functions of Siegel cusp eigenforms of genus 3. 2008. arXiv:0805.2114v1 [math.NT].

[Del79] Pierre Deligne. Valeurs de fonctions L et périodes d'intégrales. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 313–346. Amer. Math. Soc., Providence, R.I., 1979. With an appendix by N. Koblitz and A. Ogus.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[DI96] W. Duke and Ö. Imamoḡlu. A converse theorem and the Saito-Kurokawa lift. *Internat. Math. Res. Notices*, (7):347–355, 1996.

[Dok] Tim Dokchitser. *ComputeL – Computing special values of L-functions*. http://www.maths.dur.ac.uk/~dma0td/computel/. v1.3.

[Dok04] Tim Dokchitser. Computing special values of motivic L-functions. *Experiment. Math.*, 13(2):137–149, 2004.

[EZ85] Martin Eichler and Don Zagier. *The theory of Jacobi forms*, volume 55 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1985.

[GLPR03] Roland Gillard, Franck Leprevost, Alexei Panchishkin, and Xavier-François Roblot. Utilisation des modules de Drinfeld en cryptologie. *C. R. Math. Acad. Sci. Paris*, 336(11):879–882, 2003.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Hec37] E. Hecke. Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. I, II. *Math. Ann.*, 114(1):1–28, 316–351, 1937. Mathematische Werke. Göttingen: Vandenhoeck und Ruprecht, 1959, 644-707.

[Hei07] Bernhard Heim. Miyawaki's F_{12} spinor L-function conjecture. 2007. arXiv:0712.1286v1 [math.NT].

[Hei08] Bernhard Heim. On the modularity of the GL_2-twisted spinor L-function. *preprint*, 2008.

[Ike01] Tamotsu Ikeda. On the lifting of elliptic cusp forms to Siegel cusp forms of degree $2n$. *Ann. of Math. (2)*, 154(3):641–681, 2001.

[Ike06] Tamotsu Ikeda. Pullback of the lifting of elliptic cusp forms and Miyawaki's conjecture. *Duke Math. J.*, 131(3):469–497, 2006.

[Jia96] Dihua Jiang. Degree 16 standard L-function of $\mathrm{GSp}(2) \times \mathrm{GSp}(2)$. *Mem. Amer. Math. Soc.*, 123(588):viii+196, 1996.

[Kur78] Nobushige Kurokawa. Examples of eigenvalues of Hecke operators on Siegel cusp forms of degree two. *Invent. Math.*, 49(2):149–165, 1978.

[Li79] Wen Ch'ing Winnie Li. L-series of Rankin type and their functional equations. *Math. Ann.*, 244(2):135–166, 1979.

[Maa79a] Hans Maass. Über eine Spezialschar von Modulformen zweiten Grades. *Invent. Math.*, 52(1):95–104, 1979.

[Maa79b] Hans Maass. Über eine Spezialschar von Modulformen zweiten Grades. II. *Invent. Math.*, 53(3):249–253, 1979.

[Maa79c] Hans Maass. Über eine Spezialschar von Modulformen zweiten Grades. III. *Invent. Math.*, 53(3):255–265, 1979.

[Mac95] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1995. With contributions by A. Zelevinsky, Oxford Science Publications.

[Miy92] Isao Miyawaki. Numerical examples of Siegel cusp forms of degree 3 and their zeta-functions. *Mem. Fac. Sci. Kyushu Univ. Ser. A*, 46(2):307–339, 1992.

[Miy06] Toshitsune Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[MP77] Yu.I. Manin and A.A. Panchishkin. Convolutions of Hecke series and their values at integral points. *Mat. Sbornik*, 104:617–651, 1977. Math. USSR, Sb. 33, 539-571 (1977); Selected Papers of Yu.I.Manin, World Scientific, 1996, 325–357.

[MR05] François Martin and Emmanuel Royer. Formes modulaires et périodes. In *Formes modulaires et transcendance*, volume 12 of *Sémin. Congr.*, pages 1–117. Soc. Math. France, Paris, 2005.

[Mur02] Kenji Murakawa. Relations between symmetric power L-functions and spinor L-functions attached to Ikeda lifts. *Kodai Math. J.*, 25(1):61–71, 2002.

[Pan03] Alexei Panchishkin. Two variable p-adic L functions attached to eigenfamilies of positive slope. *Invent. Math.*, 154(3):551–615, 2003.

[PV07] Alexei Panchishkin and Kirill Vankov. Explicit Shimura's conjecture for Sp_3 on a computer. *Math. Res. Lett.*, 14(2):173–187, 2007.

[PV09] Alexei Panchishkin and Kirill Vankov. Explicit formulas for Hecke operators and Rankin's lemma in higher genus. In *Algebra, Arithmetic and Geometry. In Honor of Yu.I. Manin*, volume 269-270 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 2009.

[Ran39] R. A. Rankin. Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. I. The zeros of the function $\sum_{n=1}^{\infty} \tau(n)/n^s$ on the line $\Re s = 13/2$. II. The order of the Fourier coefficients of integral modular forms. *Proc. Cambridge Philos. Soc.*, 35:351–372, 1939.

[Ran52] R. A. Rankin. The scalar product of modular forms. *Proc. London Math. Soc. (3)*, 2:198–217, 1952.

[SAG] *SAGE Mathematical Software*. http://www.sagemath.org. Ver. 3.1.1.

[Sch90] A. J. Scholl. Motives for modular forms. *Invent. Math.*, 100(2):419–430, 1990.

[Sel40] Atle Selberg. Bemerkungen über eine Dirichletsche Reihe, die mit der Theorie der Modulformen nahe verbunden ist. *Arch. Math. Naturvid.*, 43:47–50, 1940.

[Ser73] Jean-Pierre Serre. Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 191–268. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[Ser77] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[Shi63] Goro Shimura. On modular correspondences for $Sp(n, Z)$ and their congruence relations. *Proc. Nat. Acad. Sci. U.S.A.*, 49:824–828, 1963.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo and Princeton

University Press, Princeton, N.J, 1971. Kanô Memorial Lectures, No. 1.

[Shi76] Goro Shimura. The special values of the zeta functions associated with cusp forms. *Comm. Pure Appl. Math.*, 29(6):783–804, 1976.

[Shi07] Goro Shimura. *Elementary Dirichlet series and modular forms*. Springer Monographs in Mathematics. Springer, New York, 2007.

[Sko92] Nils-Peter Skoruppa. Computations of Siegel modular forms of genus two. *Math. Comp.*, 58(197):381–398, 1992.

[Stu80] Jacob Sturm. Projections of C^∞ automorphic forms. *Bull. Amer. Math. Soc. (N.S.)*, 2(3):435–439, 1980.

[Van07] Kirill Vankov. The image of a local Hecke series of genus four under a spherical mapping. *Mat. Zametki*, 81(5):676–680, 2007.

[vdG08] van der Geer. Siegel modular forms and their applications. In *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*, Universitext, pages 181–246. Springer, Leipzig, Germany, 2008. http://arxiv.org/abs/math/0605346.

[Yos01] Hiroyuki Yoshida. Motives and Siegel modular forms. *Amer. J. Math.*, 123(6):1171–1197, 2001.

[Zag77] Don Zagier. Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields. In *Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 105–169. Lecture Notes in Math., Vol. 627. Springer, Berlin, 1977.

[Zag81] Don Zagier. Sur la conjecture de Saito-Kurokawa (d'après H. Maass). In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progress in Mathematics*, pages 371–394. Birkhäuser Boston, Boston, MA, 1981.

[Žar74] N. A. Žarkovskaja. The Siegel operator and Hecke operators. *Funkcional. Anal. i Priložen.*, 8(2):30–38, 1974. in Russian.

ABSTRACT

The main result of the present work consists of the explicit computation of the generating power series of Hecke operators in local Hecke algebra for the symplectic groups of genus 3 and 4. The computation algorithm is based on the Satake isomorphism, which make it possible to carry out all operations in the algebra of polynomials in multiple variables. This is the first time when this expression was computed in genus 4.

In order to obtain the result, the method of symbolic computation was developed. This algorithmic approach is also applied to other types of Hecke series. In particular, we formulate and prove the analog of Rankin's Lemma in higher genus. We also computed the symmetric squares and symmetric cubes generating series.

Based on our computational results we formulate a modularity lifting conjecture for convolutions of L-functions attached to Siegel modular forms. We review other important conjectures related to Siegel modular forms and their L-functions. We use these constructions to compute the rational algebraic factors in critical values of the spinor L-function attached to F_{12} of Miyawaki. To our knowledge this is the first example of a spinor L-function of Siegel cusp forms of degree 3, when the special values can be computed explicitly.

Finally, we apply the theory of Hecke algebras to constructions of algebraic cryptosystems on some finite sets of left cosets in Hecke algebras. We use a relation between left cosets and points on certain projective algebraic varieties.

RÉSUMÉ

Le résultat principal dans le travail présenté est le calcul explicite de la série génératrice des opérateurs de Hecke dans l'algèbre de Hecke locale pour les groupes symplectiques de genre 3 et 4. L'algorithme est basé sur l'isomorphisme de Satake, qui permet de réaliser toutes les opérations dans l'algèbre des polynômes à plusieurs variables. C'est la première fois que cette expression est calculée pour le genre 4.

Pour obtenir le résultat principal, une méthode de calcul symbolique a été développée. Cette approche algorithmique s'applique à d'autres types de séries de Hecke. En particulier, nous formulons et prouvons un analogue du Lemme de Rankin pour le genre 2. Nous avons aussi calculé les séries génératrices des carrés symétriques et des cubes symétriques.

Se basant sur nos résultats nous formulons une conjecture de modularité pour les convolutions des fonctions L-spineurs associées aux formes modulaires de Siegel. Nous considérons d'autres conjectures importantes liées aux formes modulaires de Siegel et à leurs fonctions L. Nous utilisons ces constructions pour calculer les facteurs algébriques rationnels aux valeurs critiques de la fonction L-spineur attachée à F_{12} de Miyawaki. A notre connaissance c'est le premier exemple d'une fonction L-spineur de forme parabolique de Siegel de degré 3, dont certaines valeurs spéciales peuvent être calculées explicitement.

Finalement, nous appliquons la théorie des algèbres de Hecke pour construire des cryptosystèmes algébriques sur ensembles finis de classes à gauches dans les algèbres de Hecke. Nous utilisons une relation entre les classes à gauches et les points sur certaines variétés algébriques projectives.

MOTS-CLÉS

Hecke algebras, Siegel modular forms, L-functions, special values, algebraic cryptosystems, projective varieties over finite fields

CLASSIFICATION MATHÉMATIQUE

11F46, 11F67, 11G09, 11T71, 14G10