THÈSE DE DOCTORAT D'AIX MARSEILLE UNIVERSITÉ

UFR Sciences
Spécialité
Mathématiques

École doctorale Mathématiques et Informatique d'Aix-Marseille (ED184).

Présentée et soutenue publiquement par
Yih-Dar SHIEH
le mardi 15 décembre 2015

Sujet :

Arithmetic Aspects of Point Counting and Frobenius Distributions

Directeur de thèse : David KOHEL

Rapporteurs :

M. Xavier CARUSO	CR-HDR Univ Rennes I
M. Tim DOKCHITSER	Prof Univ Bristol

Composition du jury :

M. David KOHEL	Prof Univ Aix-Marseille	Directeur de thèse
M. Gilles LACHAUD	DR CNRS Univ Aix-Marseille	Co-directeur
M. Xavier CARUSO	CR-HDR Univ Rennes I	Rapporteur
M. Tim DOKCHITSER	Prof Univ Bristol	Rapporteur
M. Florent JOUVE	MCF-HDR Univ Paris-Sud	Examinateur
M. Enric NART	Prof Univ Autònoma Barcelona	Examinateur
M. François RODIER	DR CNRS Univ Aix-Marseille	Examinateur
M. Peter STEVENHAGEN	Prof Univ Leiden	Examinateur

Remerciements

First and foremost, I would like to offer my sincerest gratitude to my thesis advisor, Professor David R. Kohel. From finding appropriate subjects, his patience with my questions even sometimes they are just silly, to the help during the writing process of this thesis, his words often provide insights that I had not thought in those ways. However, this is by no means the whole story : His encouragement and understanding in some difficult times I encountered during my PhD in France are also very important to the completion of this thesis.

The co-advisor, Mr. Gilles Lachaud, also helped a lot, in particular for the second part of my thesis. Moreover, his suggestion about the French administration, and his encouragement with David, bring the writing process to completion.

I thank also the jury members : Xavier Caruso, Tim Dokchitser, Florent Jouve, Enric Nart, François Rodier and Peter Stevenhagen, for their suggestions and acceptances to be part of this committee.

The people I know in the campus de Luminy of Institut de Mathématiques de Marseille are very nice, enthusiastic and passionate, not only in mathematics but also in their life. Especially, I would like to mention my former colleague, Virgile Ducet, who shared the same office with me. Everytime there was a party or a soirée for the doctorants, which I believed that it was every night, and sometimes more than one in the same evening, he never forgot inviting me to attend. Beside him, Christophe Arène and Florent Rovetta also helped me a lot on the administration things in the university. Aurelia Lozingot, Eric Lozingot and Corinne Roux are always affable to me, even sometimes I had no idea how to proceed for a mission or for extending my carte de séjour. It is a pleasure for me to complete the thesis at Luminy.

It would be difficult to start my thesis without the scholarship from L'École Doctorale en Mathématiques et Informatique de Marseille. I deliver my gratitude to all the people who helped me to obtain this scholarship, and one of them is my advisor.

I am happy to meet some people from my country, Taiwan. Some of them become my friends that we can speak mind to each other, but I won't admit that the main reason are that they are all female. Among them, Cubi is the most closest friend. She also invites me often to diner at her apartment, and I am always being pleased by her cooking talent. It is also pleasant to talk to another friend, Juko, even most of the conversations are of nonsense.

Professor Jungkai Chen at National Taiwan University, and Professor Chia-Fu Yu at Institute of Mathematics Academia Sinica encouraged and helped me to

come to Europe to pursue the research in Mathematics, and I am always grateful for their kindness, and miss those days.

I must also thank my parents for their understanding, especially I rarely come back to Taiwan in these years.

Finally, I am happy to be with my cat, bonbon, who is so cute and so wild at the same time, so I am some kind of experienced with “une française”.

Table des matières

Préface

This thesis consists of two parts. The first part is a general review of point counting, and then a study of Kedlaya's p-adic method (to curves with non-trivial automorphism group). In the second part, I present a new approach to the study of Sato-Tate groups and Galois representations, and analyze its advantages. The study of point counting algorithms, which are used to determine the data of the characteristic polynomial of the geometric Frobenius action, and the analysis of its distribution, are a common thread.

Part I studies the decomposition of cohomology groups induced by automorphisms for a family of non-hyperelliptic genus 3 curves with involution, and I investigate the benefit of such decomposition in the computation of Frobenius action using Kedlaya's algorithm. The involution of a curve C in this family induces a degree 2 map to an elliptic E, which gives a decomposition of the Jacobian $\mathrm{Jac}(C)$ into E and an abelian surface A. The components in the decomposition $H^1_{MW}(E) \oplus V$ of the cohomology group $H^1_{MW}(C)$ give the Frobenius actions on E and A, from which the Frobenius action on C can be recovered. On E, the characteristic polynomial of the Frobenius endomorphism can be computed using a suitable algorithm of Schoof-Elkies-Atkin, Satoh or Kedlaya, which are efficient and fast in practice. By working with the cohomology subgroup V of $H^1_{MW}(C)$, we get a constant speed-up over a straightforward application of Kedlaya's method to C. To my knowledge, this is the first use of decomposition of the cohomology induced by an isogeny decomposition of the Jacobian in Kedlaya's algorithm. In general, since the complexity of Kedlaya's algorithm in the genus g is at least g^4, a decomposition of the cohomological group into k subgroups of almost equal dimensions will give a speed-up by a factor of k^3. Since we work with smaller dimensional groups, the precision required to recovery the character polynomial is also reduced, which gives a further reduce of complexity.

In Part II, I propose a new approach to Frobenius distributions and Sato-Tate groups, which uses the orthogonality relations of the irreducible characters of the compact Lie group $\mathrm{USp}(2g)$ and its subgroups.

For the application to Sato-Tate groups, I first present a simple method to compute the irreducible characters of $\mathrm{USp}(2g)$. This work provides a set of invariants and strategy which can be used in higher genus. Although the idea behind this algorithm is simple, and it works well for small g, it is of theoretical interest to develop a more efficient algorithm. In Section 4.6, I develop an algorithm (Algorithm 1) based on the Brauer-Klimyk formula. Although applied in practice for small d, the average complexity per character for this algorithm to compute all

the irreducible characters of $\mathrm{USp}(2g)$ up to a unweighted degree $d \gg g$ is $O(\frac{d}{g})$.

The advantages of the new approach to Sato-Tate groups are examined in several aspects : I study the error behaviour in the genus g, in the unweighted degree d and in the sample size n. The results show that the error grows slowly with respect to all these three factors, as far as the Sato-Tate group of the curve has a small index in $\mathrm{USp}(2g)$. Moreover, I compared it with the classical use of moment sequences. I also use the family of genus 3 curves studied in Part I as a case study. This example demonstrates the principle that, for non-generic curves, one should work with the character theory of the smallest group that is known to contain the Sato-Tate group. The analyses and comparisons show that the character theory approach is a more intrinsic and very promising tool for studying Sato-Tate groups. Using this new approach, we need many fewer data points of Frobenius (as character polynomials) to identify a Sato-Tate group. This provides further research topics. For example, extend Algorithm 1 to other compact connected Lie groups. It is also interesting to study more exotic Sato-Tate groups, e.g. the five exceptional simple Lie groups. A complete study of Sato-Tate groups requires the additional analysis of the group of connected components, not treated in this thesis. In many cases the splitting field for this (finite) Galois group can be inferred from the geometric context, but in general requires a study of the character theory of finite groups.

Première partie

Kedlaya's Method

Chapitre 1

Introduction

The zeta functions of algebraic varieties over finite fields, in particular, those of algebraic curves, are the main subject of this thesis, playing a central role in the development of the modern algebraic geometry. The reason for the interest in computing zeta functions comes from both theoretical considerations and practical applications to coding theory and cryptography, particularly elliptic curve cryptography.

In this chapter we give a brief introduction to zeta functions. We first recall their history then introduce their basic definitions and properties before concluding with an overview of point counting algorithms.

1.1 History of zeta function

The study of zeta functions in the setting of function fields (and varieties over finite fields) dates back to Artin's thesis in 1921 [Art21] [Art24]. He considered quadratic function fields, i.e., degree 2 extensions of the rational function field $K(x)$ with K being a finite field. Although the main theme of Artin's thesis is not to focus on the zeta function but on the arithmetic of quadratic function fields (decomposition of ideals, ramification, unit theorem, class number and reciprocity law), but on the second part of thesis, Artin introduced the zeta function and proved that it is rational, which is different from the zeta function in the number field case. Artin also tried to prove the analogue of the Riemann hypothesis, which says the non-trivial zeros of the L-function lie on the line $s = 1/2$ in the complex plane.

In 1933 [Has33], Hasse proved the Riemann hypothesis for elliptic function fields. One of the essential step is to show that the endomorphism of an elliptic curve over a finite field is quadratic imaginary. Thereafter, the study of zeta functions, especially the efforts to prove the Riemann hypothesis, became more and more active. André Weil [Wei48] proved the Riemann hypothesis holds for all function fields in 1948. Bombieri [Bom74] gave a very short and elegant proof in 1974, which can be found in the book of Moreno [Mor91]. This was based on an idea of Stepanov of constructions of functions with prescribed numbers of zeros at finitely many given points, which is a weak form of the Riemann-Roch

theorem. Another part in Bombieri's proof is the use of Galois theory to deduce the lower bound for the number of points from the upper bound.

The proof of Weil involved higher dimensional algebraic geometry and leads to the theory of abelian varieties. In 1949, he proposed the *Weil conjectures* about zeta functions of algebraic varieties over finite fields [Wei49]. This led to a very active development in modern algebraic geometry, especial in 1960's and 1970's. This includes Dwork's proof of the rationality of zeta functions [Dwo60], Grothendieck's proof of the functional equation [Gro95], and finally Deligne proved the Riemann hypothesis in 1974 [Del73] [Del75] and [Del80].

1.2 Zeta functions of curves over finite fields

By a *curve* over a field K, we mean a geometrically integral smooth projective algebraic curve defined over K. In this section, K will ba a finite field. We give a brief review of the zeta function of algebraic curves over finite fields. We refer to [Mor91] and [Sti09] for the details and a more thorough presentation.

Definition 1.1. Let C be a curve over $\mathbb{F}_q$. The zeta function of $C/\mathbb{F}_q$ is

$$Z(T) = \sum_D T^{\deg(D)} \in \mathbb{C}[[T]], \tag{1.2.1}$$

where the sum is taken over all effective divisors D in $\mathrm{Div}(C)$, the divisor group of $C/\mathbb{F}_q$.

Remark 1.2. We have a (formal) Euler product formula for the zeta function :

$$Z(T) = \prod_{P \in C} \frac{1}{1 - T^{\deg(P)}} \cdot \tag{1.2.2}$$

Proposition 1.3. The zeta function $Z(T)$ of $C/\mathbb{F}_q$ converges absolutely on $|T| < 1/q$ in $\mathbb{C}$.

Remark 1.4. For $|T| < 1/q$, the Euler product in 1.2 is absolutely convergent, and its value is $Z(T)$.

Proposition 1.5 (Rationality of $Z(T)$)**.** $Z(T)$ can be extended to a rational function on $\mathbb{C}$ which has simple poles at $T = 1$ and $T = \frac{1}{q}$.

Definition 1.6. The *L-polynomial* of $C/\mathbb{F}_q$ is $L(T) = (1 - T)(1 - qt)Z(T)$.

Proposition 1.7 (Functional Equation of $Z(T)$)**.** Let g be the genus of the curve C. The zeta function $Z(T)$ of C satisfies the function equation

$$Z(T) = q^{g-1}T^{2g-2}Z\left(\frac{1}{qT}\right) \cdot \tag{1.2.3}$$

Proposition 1.8. We have

(1) $Z(T) = \frac{L(T)}{(1-T)(1-qT)}$.

(2) $L(T) \in \mathbb{Z}[T]$.

(3) $L(1) = h(C)$, the class number of $C/\mathbb{F}_q$.

(4) $L(T) = q^g T^{2g} L(\frac{1}{qT})$.

(5) $L(T)$ is of degree $2g$. We write $L(T) = a_0 + a_1 T + \cdots + a_{2g} T^{2g}$.

(6) $L(0) = a_0 = 1$ and $a_{2g} = q^g$.

(7) $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$.

(8) Let $\alpha_1, \cdots, \alpha_{2g}$ be the reciprocals roots of $L(T)$, in other words,

$$L(T) = \prod_{i=1}^{2g} (1 - \alpha_i T). \tag{1.2.4}$$

Then we can renumber α_i such that $\alpha_i \alpha_{g+i} = q$ for $i = 1, \cdots, g$.

(9) Let $C_n = C \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ and $L_n(T)$ be the L-polynomial of $C_n/\mathbb{F}_{q^n}$. Then $\alpha_1^n, \cdots, \alpha_{2g}^n$ are the reciprocals roots of $L_n(T)$.

The zeta function $Z(T)$ has a very close relation with the number of points on a curve :

Proposition 1.9. Let $N_n = \#C(\mathbb{F}_{q^n})$, i.e. the number of $\mathbb{F}_{q^n}$-rational points of $C/\mathbb{F}_q$. We have

$$Z(T) = \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n} \right). \tag{1.2.5}$$

and

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n. \tag{1.2.6}$$

Proof. We have

$$\begin{aligned} \log(Z(T)) &= \log\left(\prod_{P \in C} \frac{1}{1 - T^{\deg(P)}} \right) \\ &= \sum_{n=1}^{\infty} \sum_{P \in C} \frac{T^{n \cdot \deg(P)}}{n} \\ &= \sum_{n=1}^{\infty} \sum_{P} \frac{\deg(P) \cdot T^{n \cdot \deg(P)}}{\deg(P) \cdot n} \\ &= \sum_{m=1}^{\infty} \left(\sum_{\deg(P) | m} \deg(P) \right) \frac{T^m}{m} \\ &= \sum_{m=1}^{\infty} \tilde{N}_m \frac{T^m}{m}. \end{aligned} \tag{1.2.7}$$

where $\tilde{N}_m = \sum_{\deg(P)|m} \deg(P)$. Hence

$$Z(T) = \exp\left(\sum_{m=1}^{\infty} \tilde{N}_m \frac{T^m}{m}\right). \tag{1.2.8}$$

For $m = 1$, $\tilde{N}_1$ equals to the number of closed points of C of degree 1, so $\tilde{N}_1 = N_1$. For any positive integer n, let $Z(T, C_n)$ be the zeta function of $C_n = C \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$. As in 1.2.8, we write

$$Z(T, C_n) = \exp\left(\sum_{m=1}^{\infty} M_m \frac{T^m}{m}\right). \tag{1.2.9}$$

The above argument shows $M_1 = N_n$. Combine 1.2.9 with the equality

$$Z(T^n, C_n) = \prod_{\zeta^n=1} Z(\zeta T, C), \tag{1.2.10}$$

see [Sti09, §5.3, Prop. 5.1.10], we obtain

$$\exp\left(\sum_{m=1}^{\infty} M_m \frac{T^{nm}}{m}\right) = Z(T^n, C_n) = \exp\left(\sum_{m=1}^{\infty} \left(\sum_{\zeta^n=1} \zeta^m\right) \tilde{N}_m \frac{T^m}{m}\right). \tag{1.2.11}$$

Compare the coefficients of T^n, we find that M_1, which equals to N_n as seen above, equals to $\tilde{N}_n$. This shows $\tilde{N}_n = N_n$ for all n, and we complete the proof for 1.2.5. For the proof for 1.2.6, consider the zeta function of C_n in 1.2.9 and we have

$$\begin{aligned} \exp\left(\sum_{m=1}^{\infty} M_m \frac{T^m}{m}\right) &= Z(T, C_n) \\ &= \frac{L_n(T)}{(1-T)(1-q^nT)} \\ &= \frac{\prod_{i=1}^{2g}(1-\alpha_i^n T)}{(1-T)(1-q^nT)} \\ &= \exp\left(\sum_{n=1}^{\infty}\left(q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n\right)\frac{T^n}{n}\right). \end{aligned} \tag{1.2.12}$$

Here we use the notations and results in (8) and (9) in 1.8. This implies

$$q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n = M_1 = N_n.$$

□

The following theorem is important, which is an analogue of the (classical) Riemann hypothesis.

Theorem 1.10 (Hasse-Weil)**.** Let $L(T)$ be the L-polynomial of a curve $C/\mathbb{F}_q$. Let $\alpha_1, \cdots, \alpha_{2g}$ be the reciprocals roots of $L(T)$. Then

$$|\alpha_i| = q^{1/2} \text{ for } i = 1, \ldots, 2g. \tag{1.2.13}$$

Proof. See [Mor91, §3.4] or [Sti09, §5.2]. □

Corollary 1.11 (Hasse-Weil Bound)**.** We have a bound on the number of rational points on a curve $C/\mathbb{F}_q$:

$$|N_n - (q^n + 1)| \leq 2g\, q^{n/2}. \tag{1.2.14}$$

Proof. It is from 1.2.6 and 1.2.13. □

1.3 Point Counting

In this section, we review a few point counting algorithms. It is impossible to introduce all algorithms, and we refer to [Coh+06] for a more comprehensive introduction. We begin with naive algorithms.

Naive enumeration

Given an equation $f = 0$ with $f(x, y) \in \mathbb{F}_q[x, y]$ which defines a curve C. The most direct way to know the number of points $|C(\mathbb{F}_q)|$ is to check if $f(\alpha, \beta)$ is zero for all $(\alpha, \beta) \in \mathbb{F}_q^2$. Since $|\mathbb{F}_q^2| = q^2$, the time required is $\tilde{O}(q^2)$, where the time for evaluate the polynomial $f(x, y)$ is negligible comparing to the size of the field $\mathbb{F}_q$.

Enumeration

Let $C : y^2 = f(x)$ with $f \in \mathbb{F}_p[x]$ a squarefree polynomial of degree $2g+1$ be a hyperelliptic curve over the prime field $\mathbb{F}_p$. For each $\alpha \in \mathbb{F}_p$, there are $1 + \left(\frac{f(\alpha)}{p}\right)$ solutions of the equation $y^2 - f(\alpha) = 0$ for y in $\mathbb{F}_p$, where we use the Legendre symbol. Hence the number of $\mathbb{F}_p$ rational points on C is given by

$$|C(\mathbb{F}_p)| = \sum_{\alpha=0}^{p-1} \left(1 + \left(\frac{f(\alpha)}{p}\right)\right) + 1,$$

where the last 1 corresponds to the unique point at infinity of C. For any $a \in \mathbb{F}_p$, the Legendre symbol $\left(\frac{a}{p}\right)$ can be computed in time $O((\log p)^2)$, or using the

fast multiplication and Jacobi symbol algorithms, in time $\tilde{O}(\log p\,(\log\log p)^2)$. Since $|\mathbb{F}_p| = p$, this enumeration algorithm runs in time $\tilde{O}(p\log p\,(\log\log p)^2)$. This method can be generalized to extension field $\mathbb{F}_q$ directly. The difference between running times of this method and the naive enumeration is that the latter one has running time quadratic in q. However, this method works only for hyperelliptic curves.

Schoof's algorithm

Consider an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$. We focus on the case that q is a large integer. Let t be the trace of the Frobenius action $\phi = F_q$ on E. We have $\#E(\mathbb{F}_q) = q + 1 - t$. Hence for elliptic curves, determining the number of points of E is equivalent to determining the trace t. The Hasse-Weil bound says that $|t| \leq 2\sqrt{q}$. If we can determining t mod N for some positive integer $N > 4\sqrt{q}$, then t equals to the unique integer t' in $\left[-2\sqrt{q}, 2\sqrt{q}\right]$ with $t' \equiv t \bmod N$. Unfortunately $N > 4\sqrt{q}$ is a large integer, and we don't have an efficient way to compute t mod N directly. However, the Chinese remainder theorem make this possible if we can compute t mod ℓ_i for distinct small primes ℓ_i such that $N := \prod_{i=1}^{r} > 4\sqrt{q}$. It is clear that the number r of such primes is no more than $\log_2(4q^{1/2}) + 1$, and we can just choose the first r primes.

Given a small prime number ℓ, we need to compute t mod ℓ. The Frobenius action ϕ satisfy the equation $\phi^2 - t\phi + q = 0$, which means $\phi^2(P) - t\,\phi(P) + qP = O$ for all $P = (x, y) \in E(\overline{\mathbb{F}}_q)$, where we use the addition and scalar multiplication on the group $E(\overline{\mathbb{F}}_q)$. Again, since t and q are large integers, the generic points $t\,\phi(P)$ and qP are impossible to compute.

Schoof's idea is to work out this computation with the ℓ-torsion subgroup $E[\ell]$. On this (small) subgroup, we have $\phi^2(P) - \bar{t}\,\phi(P) + \bar{q}P = O$ for all $P \in E[\ell]$ and any integers $\bar{t} \equiv t$ and $\bar{q} \equiv q$ mod ℓ. Moreover, if for $\ell \neq p$ and an integer $\bar{t}$ which satisfies $\phi^2(P) + \bar{t}\,\phi(P) - \bar{q}P = O$ for all $P \in E[\ell]$, we have $t \equiv \bar{t}$ mod ℓ, since the restriction of ϕ on $E[\ell]$ is invertible. So in order to determine t mode ℓ for $\ell \neq p$, we only need to determine $\bar{t}$ for which $\phi^2 + \bar{q} = \bar{t}\,\phi$ holds on $E[\ell]$. Of course, we can consider only $\bar{q}$ and $\bar{t}$ in the range $\left[-\frac{(\ell-1)}{2}, \frac{(\ell-1)}{2}\right]$.

Finally, the relation $\phi^2 + \bar{q} = \bar{t}\,\phi$ on $E[\ell]$ can be tested using the ℓ-division polynomial $\psi_\ell[x, y] \in \mathbb{F}_q[x, y]$, which vanishes exactly at the nontrivial ℓ-torsion points $P = (x, y)$. This leads to the computation being done modulo a polynomial in $\mathbb{F}_q[x]$ of degree $\frac{\ell^2-1}{2}$, see [Sch85] for more details.

The complexity is $\tilde{O}((\log q)^5)$ using fast algorithms for integer arithmetic and polynomials. The improved algorithm by Noam Elkies and A. O. L. Atkin, which is called Schoof–Elkies–Atkin algorithm (SEA), is probabilistic and has expected running time $\tilde{O}((\log q)^4)$, see [Atk92].

Satoh's algorithm

The p-adic method is used in the study of zeta functions of algebraic varieties by Dwork in 1960 to show that the rationality of the zeta function, see [Dwo60]. Kato and Lubkin [KL82] developed a p-adic algorithm to count points on elliptic curves, however it has never been implemented.

In 1999, Satoh [Sat00] designed an p-adic algorithm based on the canonical lifts of elliptic curves. For an elliptic curve $E/\mathbb{F}_q$, a canonical lift of E is an elliptic curve $\mathcal{E}/\mathbb{Q}_q$ defined over $\mathbb{Z}_q$ such that the ring homomorphism $\mathrm{End}\mathbb{Q}_q(\mathcal{E}) \to \mathrm{End}_{\mathbb{F}_q}(E)$ induced by reduction modulo p is a ring isomorphism. If E is ordinary, Deuring [Deu41a] showed the existence and uniqueness (up to isomorphism) of the canonical lift. Lubin, Serre and Tate [LST64] proved that the j-invariant of $\mathcal{E}$ is the unique solution in $\mathbb{Z}_q$ of the equation

$$\Phi_p(X, \Sigma(X)) = 0 \text{ and } X \equiv j(E) \bmod p,$$

where $\Sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ is the lift of the p-th power Frobenius on $\mathbb{F}_q$ to $\mathbb{Z}_q$, and $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$ is the p-th modular polynomial. This provides a way to compute $j(\mathcal{E})$ using a generalized Newton's method, and thus an equation of the canonical lift $\mathcal{E}$. Let $\mathcal{F}_q$ be the lifted Frobenius to $\mathcal{E}$ of the Frobenius F_q on E, and ω be a holomorphic differential on $\mathcal{E}$, e.g. the invariant differential. Satoh proved that the trace of Frobenius is given by $c + \frac{q}{c}$ where $c \in \mathbb{Z}_q$ is determined by $\mathcal{F}_q^*(\omega) = c\omega$. Satoh then found a way to compute c and turned the above ideas into an effective algorithm. For a fixed prime p, the running time for $E/\mathbb{F}_q$ with $q = p^n$ is $\tilde{O}(n^3)$ and it requires $O(n^3)$ space.

Kedlaya's algorithm

In 2001, Kedlaya designed a point counting algorithm for hyperelliptic curves using the Monsky-Washnitzer cohomology. We will devote to this method in Chapter 2, but our target is the family of genus 3 curves with automorphism groups $\mathbb{Z}/2\mathbb{Z}$. Hence we give an overview of Kedlaya's algorithm in its original form.

Let $\overline{C}$ be a hyperelliptic curve of genus g over $\mathbb{F}_q$, $q = p^n$, defined the equation $y^2 = \overline{f}(x)$ with $\overline{f} \in \mathbb{F}_q[x]$ a squarefree polynomial of degree $2g + 1$. We lift $\overline{f}$ to a monic polynomial $f \in \mathbb{Z}_q$, the unramified extension of $\mathbb{Z}_p$ of degree n. The equation $y^2 = f(x)$ defines a hyperelliptic curve C over $\mathbb{Q}_q$ whose reduction modulo p is $\overline{C}$.

It can be shown that $x^1dy, x^2dy, \ldots, x^{2g}dy$ form a basis of the Monsky-Washnizter cohomology of the affine scheme $C\backslash\{\infty\}$ whose associated dagger algebra is $\mathbb{Q}_q\langle x, y\rangle^\dagger / (y^2 - f(x))$, see Section 2.2 for more information. One can use this basis and a lift of Frobenius on this dagger ring to compute the zeta function of $\overline{C}$. However, Kedlaya work with the curve obtained from C by removing the point at infinity and the locus of $y = 0$. The corresponding dagger ring is then

$A^\dagger = \mathbb{Q}_q\langle x, y, y^{-1}\rangle^\dagger / (y^2 - f(x))$. The advantage of using this larger ring is that it admits a lift of Frobenius with a simpler form and can be computed very fast, which is given by $F_p(x) = x^p$ and

$$F_p(y) = y^p \left(1 + \frac{F_p\left(f(x)\right) - f(x)^p}{y^{2p}}\right).$$

Note that we invert y in this formula, which is the reason for which we work with $A^\dagger$. This gives us a cohomology group whose dimension is bigger, however we only need to work with a subspace for which $\{x^i/y\,dx\}_{i=0}^{2g-1}$ forms a basis.

From the above formula, it is easy to see that the lifted Frobenius converges p-adically in linear rate, see the definition of overconvergent series and dagger ring in Section 2.2. Another important parts in Kedlaya's work are explicit reductions of differential forms and an upper bound of the lost of precision during the reductions, see Section 2.3.2 and 2.3.3 respectively. This upper bound provides an upper bound for the required precision to compute the lifted Frobenius.

The running time of Kedlaya's algorithm for a hyperelliptic curve of genus g over $\mathbb{F}_{p^n}$ is $\tilde{O}(g^4n^3)$ and it uses $O(g^3n^3)$ space for a fixed p. Its dependence on p is $\tilde{O}(p)$. In 2006, David Harvey improved this complexity to $\tilde{O}(\sqrt{p})$, see [Har07]. In 2012, he also gives an average polynomial time algorithm to compute the zeta functions for the reductions of any hyperelliptic curve defined over $\mathbb{Q}$, see [Har14].

1.4 Conclusion

The naive methods with clever use of Pollard rho or the baby-step, giant-step algorithm in the group structure of the Jacobian play an important role in determining the zeta function in small to moderate characteristic (and low genus).

Schoof's algorithm can be generalized to higher dimensional abelian varieties over finite fields. However the complexity in g is exponential, and it is impractical for genus > 2. Satoh's algorithm is also theoretically general, but it requires the computation of (an ideal of) modular relations, which limits both the genus and the characteristic. Kedlaya's algorithm is generalized to a wide class of curves. In Section 1.3, we use this method for non-hyperelliptic genus 3 curves whose automorphism group contains $\mathbb{Z}/2\mathbb{Z}$. The limitation of Kedlaya's algorithm is the complexity in the characteristic p is $\tilde{O}(p)$, but this is reduced to $\tilde{O}(\sqrt{p})$ after Harvey.

In the application to the Sato-Tate conjectures, the simultaneous computation modulo many primes can be optimized by work of Harvey [Har14], and Harvey and Sutherland [HS16].

Chapitre 2

Point Counting for Non-Hyperelliptic Genus 3 Curves

2.1 Introduction

Henn [Hen76] gave the table of the possible non-trivial groups which appear as automorphism groups of a non-hyperelliptic genus 3 curves, which can be found in Vermeulen's thesis [Ver83]. The dimension of the set of moduli points of non-hyperelliptic genus 3 curves whose automorphism group contain $\mathbb{Z}/2\mathbb{Z}$ is 4 inside the moduli of genus 3 curves $\mathcal{M}_3$ of dimension 6. We thus obtain an algorithm to compute the zeta function of a large family of genus 3 curves.

In [Ked01], Kedlaya used Monsky-Washnitzer cohomology to compute the zeta functions of hyperelliptic curves over finite fields. This method could be applied to general varieties, and there are already generalizations to superelliptic curves, $C_{a,b}$ curves and non-degenerate curves, see [GG01], [DV06] and [Cas06].

In this chapter, we use Monsky-Washnitzer cohomology for non-hyperelliptic genus 3 curves with an involution (double covers of elliptic curves), but focuses on a smaller dimensional space associated to an abelian surface in the jacobian of C.

This chapter is organized as follows : Section 2.2 recalls the definition of Monsky-Washnitzer cohomology and results in this theory. In Section 2.3, we compute a basis of the cohomology and describe a way to do the reduction of a differential form. Reduction means to write a differential form as a linear combination of the basis. In particular, we give an upper bound of the denominator after a differential form is reduced. This bound makes the algorithm practical since it establishes a finite precision bound for the computation. Section 2.4 describes a way to compute a lift of Frobenius and Section 2.5 explains why the computation splits into 2 eigenspaces. Finally, Section 2.6 gives the algorithm and an analysis of its complexity.

2.2 Monsky-Washnitzer cohomology

In this section, we recall the definition of Monsky-Washnitzer cohomology which is introduced by Monsky and Washnitzer in [MW68] and Monsky [Mon68], [Mon71].

Monsky-Washnitzer cohomology is a p-adic cohomology theory defined for smooth affine varieties over finite fields. Let X be a smooth affine variety defined over a finite field $k := \mathbb{F}_q$ of characteristic p with coordinate ring $\overline{A}$ which is a finitely generated k-algebra. In [Elk73], Elkik showed that there exists a finitely generated smooth $\mathbb{Z}_q$-algebra A such that $A/pA \cong \overline{A}$, here $\mathbb{Z}_q$ is the valuation ring of $\mathbb{Q}_q$, the degree $n := \log_p q$ unramified extension of $\mathbb{Q}_p$.

In general, A does not admit a lift of the Frobenius endomorphism $\overline{F}$ on $\overline{A}$, but its p-adic completion A^∞ does. However, the dimension of the de Rham cohomology of A^∞ may be too big. For example, if $A = \mathbb{Z}_p[x]$, then $\sum_{n=0}^{\infty} p^n x^{p^n-1} dx$ is not an exact differential form since $\sum_{n=0}^{\infty} x^{p^n}$ is not in A^∞, but each term of this sum is exact. The problem is that this differential form does not converge fast enough for its integral to converge as well.

Monsky and Washnitzer work with a subalgebra $A^\dagger$ of A^∞ consisting of series which converge fast enough to solve the above problem. For

$$A = \mathbb{Z}_q[x_1, x_2, \cdots, x_d]/(f_1, f_2, \cdots, f_r),$$

the weak completion or dagger ring of A is

$$A^\dagger := \mathbb{Z}_q\langle x_1, x_2, \cdots, x_d\rangle/(f_1, f_2, \cdots, f_r)$$

where $\mathbb{Z}_q\langle x_1, x_2, \cdots, x_d\rangle$ is the subring of A^∞ which consists of overconvergent power series

$$\left\{ \sum_\alpha a_\alpha x^\alpha \in \mathbb{Z}_q[[x_1, x_2, \cdots, x_d]] \;\middle|\; \liminf_{|\alpha|\to\infty} \frac{v_p(a_\alpha)}{|\alpha|} > 0 \right\}$$

with $\alpha := (\alpha_1, \cdots, \alpha_d)$, $x^\alpha := x_1^{\alpha_1} \cdots x_d^{\alpha_d}$, $|\alpha| = \sum_{i=1}^d \alpha_i$ and v_p is the usual p-adic valuation on $\mathbb{Z}_q$.

Definition 2.1. The Monsky-Washnitizer cohomology of $X/\mathbb{F}_q$ is the de Rham cohomology of $A^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$. More precisely, let $D^0(A^\dagger) := A^\dagger$, $D^1(A^\dagger)$ be its universal module of differentials

$$D^1(A^\dagger) := \left(A^\dagger\, dx_1 + \cdots + A^\dagger\, dx_d\right) / \left(\sum_{j=1}^{r} A^\dagger \left(\frac{\partial f_i}{\partial x_1} dx_1 + \cdots + \frac{\partial f_i}{\partial x_d} dx_d\right)\right)$$

and $D^i(A^\dagger)$ be the i-th exterior product of $D^1(A^\dagger)$. Let $H^i(\overline{A}, \mathbb{Z}_q)$ be the i-th

cohomology group of the complex

$$0 \to D^0(A^\dagger) \xrightarrow{d_0} D^1(A^\dagger) \xrightarrow{d_1} D^2(A^\dagger) \xrightarrow{d_2} D^3(A^\dagger) \xrightarrow{d_3} \cdots$$

where d_i is the usual differentiation. Then the i-th Monsky-Washnitzer cohomology group of X (or of $\overline{A}$) is $H^i(\overline{A}, \mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$, which is denoted by $H^i_{MW}(X/\mathbb{F}_q)$ (or $H^i(\overline{A}, \mathbb{Q}_q)$).

The Monsky-Washnitzer cohomology has the following properties, see van der Put [Put86].

Theorem 2.2. For a smooth finitely generated $\mathbb{F}_q$-algebra $\overline{A}$, we have

(a) The map $\overline{A} \mapsto H^i(\overline{A}, \mathbb{Q}_q)$ is well defined and functorial.

(b) There exists a $\mathbb{Z}_q$-algebra homomorphism $F_q : A^\dagger \to A^\dagger$ which lifts the Frobenius endomorphism of $\overline{A}$. Furthermore, any two lifts induce homotopic maps on the complex $D^i(A^\dagger)$. Hence they induce the same map $F_{q,*} : H^i(\overline{A}, \mathbb{Q}_q) \to H^i(\overline{A}, \mathbb{Q}_q)$ on the Monsky-Washnitzer cohomology.

The following Lefschetz fixed point formula allows us to compute the zeta function of $X = \mathrm{Spec}(\overline{A})$ using Monsky-Washnitzer cohomology.

Theorem 2.3 (Lefschetz fixed point formula)**.** Let $X/\mathbb{F}_q$ be a smooth affine variety of dimension d. Then we have

$$X(\mathbb{F}_q) = \sum_{i=0}^{d} (-1)^i \mathrm{Tr}\left(q^d F_{q,*}^{-1} \middle| H^i_{MW}(X/\mathbb{F}_q) \right).$$

2.3 Cohomology of non-hyperelliptic genus 3 plane curves with automorphism group $\mathbb{Z}/2\mathbb{Z}$

In this section, we consider non-hyperelliptic smooth projective plane curves C of genus 3 whose automorphism group contains $\mathbb{Z}/2\mathbb{Z}$ over a finite field $\mathbb{F}_q$ of characteristic $p \neq 2$. Such curves can be written (up to isomorphism) as

$$C : \overline{F} := Y^4 + \overline{G}(X, Z)X^2 + \overline{H}(X, Z) = 0,$$

with $\overline{G}(X, Z)$ and $\overline{H}(X, Z) \in \mathbb{F}_q[X, Z]$ which are homogeneous of degree 2 and 4 respectly. We assume that C is smooth. Since the Monsky-Washnitzer cohomology is defined for smooth affine varieties, we also consider the affine part of C

$$C_{\text{aff}} : \overline{f} := y^4 + \overline{g}(x)y^2 + \overline{h}(x) = 0,$$

where $\overline{g}(x) = \overline{G}(x, 1)$ and $\overline{h}(x) = \overline{H}(x, 1)$ are the dehomogenizations of $\overline{G}(X, Z)$ and $\overline{H}(X, Z)$ with respect to Z. In this section, we compute the Monsky-Washnitzer

cohomology $H^i_{MW}(C_{\text{aff}}/\mathbb{F}_q)$ of C_{aff} and relate the zeta function of $C/\mathbb{F}_q$ to the characteristic polynomial of the Frobenius action $F_{q,*}$ on $H^i_{MW}(C_{\text{aff}}/\mathbb{F}_q)$.

Choose arbitrary lifts $G(X,Z)$ and $H(X,Z) \in \mathbb{Z}_q[X,Z]$ of $\overline{G}(X,Z)$ and $\overline{H}(X,Z)$ such that $\deg_X G = \deg_X \overline{G}$ and $\deg_X H = \deg_X \overline{H}$. Let $g(x) := G(x,1)$ and $h(x) := H(X,1)$ be the dehomogenizations. Consider the following two curves

$$\tilde{C} : F := Y^4 + G(X,Z)Y^2 + H(X,Z) = 0,$$

and

$$\tilde{C}_{\text{aff}} : f := y^4 + g(x)y^2 + h(x) = 0 \tag{2.3.1}$$

Since the reduction of F modulo the maximal ideal (p) of $\mathbb{Z}_q$ is $\overline{F}$ which defines a smooth projective curve C, the generic fiber $\tilde{C}_\xi := \tilde{C} \times_{\mathbb{Z}_q} \mathbb{Q}_q$ of $\tilde{C}$ is also smooth. Using the three facts that the reduction of f modulo the maximal ideal (p) of $\mathbb{Z}_q$ equals to $\overline{f}$ which is not zero in $\mathbb{F}_q[x,y]$, that $\overline{A} := \mathbb{F}_q[x,y]/(\overline{f}(x,y))$ is an integral domain and that p is a prime element in the unique factorization domain $\mathbb{Z}_q[x,y]$, one sees that A is an integral domain and hence it is flat over $\mathbb{Z}_q$. This shows that A is a finitely generated smooth $\mathbb{Z}_q$-algebra, so we can work with A to apply the theory of Monsky-Washnitzer cohomology. The above arguments also show that the generic fiber $\tilde{C}_\xi$ of $\tilde{C}$ is a geometrically integral smooth projective curve over $\mathbb{Q}_q$.

Although we can compute the Monsky-Washnitzer cohomology of the affine curve $C_{\text{aff}}/\mathbb{F}_q$ by explicit reduction algorithms and the control of denominators, we use the following theorem instead, see [Ked04], and compute the algebraic de Rham cohomology $H^i_{dR}(\tilde{C}_{\xi,\text{aff}}/\mathbb{Q}_q)$ of the curve $\tilde{C}_{\xi,\text{aff}}/\mathbb{Q}_q$, the affine part of the generical fiber $\tilde{C}_\xi$. Note that we are concerned with curves, hence the divisors are always normal crossings.

Theorem 2.4. Let $Y/\mathbb{Z}_q$ be a smooth proper scheme, Z be a relative normal crossings divisor and $X := Y \backslash Z$ is affine. Then there is a canonical isomorphism

$$H^i_{dR}(X_\xi/\mathbb{Q}_q) \to H^i_{MW}(X_p/\mathbb{F}_q),$$

where X_ξ is the generic fiber and X_p is the special fiber of $X/\mathbb{Z}_q$, namely, the fibers of X at the closed point (p) of $\text{Spec}(\mathbb{Z}_q)$.

2.3.1 Geometry

Before we compute the algebraic de Rham cohomology of the affine curve $\tilde{C}_{\xi,\text{aff}}$, we need to study its geometry. The coordinate ring of $\tilde{C}_{\xi,\text{aff}}$ is

$$A := \mathbb{Q}_q[x,y]/(f(x,y)),$$

where $f(x,y) = y^4 + g(x)y^2 + h(x) \in \mathbb{Z}_q[x,y]$ with $\deg(g) \leq 2$ and $\deg(h) \leq 4$.

We write $g(x)$ and $h(x)$ as following

$$\begin{aligned} g(x) &= a_2x^2 + a_1x + a_0,\ a_i \in \mathbb{Z}_q \\ h(x) &= b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0,\ b_i \in \mathbb{Z}_q \end{aligned} \tag{2.3.2}$$

There are four cases to consider :

Case 1. $b_4 = 0$ and $a_2 = 0$
There is only one point at infinity which is $P_\infty := (1 : 0 : 0)$. Using the fact that $\tilde{C}_\xi$ is smooth at P_∞, one shows that $b_3 \neq 0$. The dimension of the first algebraic de Rham cohomology of $\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q$ is $2g + N_\infty - 1 = 2 \cdot 3 + 1 - 1 = 6$, here g is the genus of $\tilde{C}_\xi$, which equals to the genus of C, and N_∞ is the number of points at infinity. We have $v_{P_\infty}(x) = -4$ and $v_{P_\infty}(y) = -3$. The local parameter at P_∞ is $t := b_3x^2/y^3$. The expansions of x and y as Laurent series of the local parameter t are $x = -b_3/t^4 + \cdots$ and $y = b_3/t^3 + \cdots$.

Case 2. $b_4 = 0$ and $a_2 \neq 0$
There are 3 points at infinity : $P_\infty := (1 : 0 : 0)$ and $P_{\infty,\pm} := (1 : \pm\alpha : 0)$ with $\alpha^2 = -a_2$. Using the fact that $\tilde{C}_\xi$ is smooth at P_∞, one shows that $b_3 \neq 0$. (The condition $a_2 \neq 0$ implies the smoothness at $P_{\infty,+}$ and $P_{\infty,-}$.) We have $\dim_{\mathbb{Q}_q} H^1_{dR}(\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q) = 2 \cdot 3 + 3 - 1 = 8$, $v_{P_{\infty,\pm}}(x) = v_{P_{\infty,\pm}}(y) = -1$, $v_{P_\infty}(x) = -2$ and $v_{P_\infty}(y) = -1$. The local parameters at P_∞ and $P_{\infty,\pm}$ are $t := 1/y$ and $t_\pm := 1/x$. The expansions of x and y at P_∞ and $P_{\infty,\pm}$ as Laurent series of the local parameters are $x = \beta/t^2 + \gamma + \delta t^2 + \cdots$ with $\beta = -a_2/b_3$, $y = 1/t$, and $x = 1/t_\pm$, $y = \pm\alpha/t + \cdots$.

Case 3. $b_4 \neq 0$ and $a_2^2 - 4b_4 = 0$
There are 2 points at infinity : $P_{\infty,\pm} := (1 : \pm\alpha : 0)$ with $\alpha = (-a_2/2)^{1/2}$. Using the fact that $\tilde{C}_\xi$ is smooth at $P_{\infty,+}$, one shows that $a_1a_2 - 2b_3 \neq 0$. We have $\dim_{\mathbb{Q}_q} H^1_{dR}(\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q) = 2 \cdot 3 + 2 - 1 = 7$ and $v_{P_{\infty,\pm}}(x) = v_{P_{\infty,\pm}}(y) = -2$. The local parameters are $t_\pm := y/x \mp \alpha$. The expansions of x and y as Laurent series of the local parameters are $x = \beta/t_\pm^2 + \gamma/t_\pm + \cdots$ and $y = \pm\alpha\beta/t_\pm^2 + (\beta \pm \alpha\gamma)/t_\pm + \cdots$ with $\beta = -(a_1a_2 - 2b_3)/4a_2$ and $\gamma = \alpha(a_1a_2 + 2b_3)/2a_2^2$.

Case 4. $b_4 \neq 0$ and $a_2^2 - 4b_4 \neq 0$
There are 4 points at infinity which are $P_{\infty,i,\pm} := (1 : \pm\alpha_i : 0)$ with $\pm\alpha_1$ and $\pm\alpha_2$ are the four roots of $y^4 + a_2y^2 + b_4 = 0$. We have $\dim_{\mathbb{Q}_q} H^1_{dR}(\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q) = 2 \cdot 3 + 4 - 1 = 9$ and $v_{P_{\infty,i,\pm}}(x) = v_{P_{\infty,i,\pm}}(y) = -1$. The local parameters are $t := 1/x$. The expansions of x and y as Laurent series of t are $x = 1/t$ and $y = \pm\alpha_i/t + \cdots$.

In order to analyze the control of denominators later, we need to impose further assumptions on the choice of the lift $F(X, Y, Z)$.

Assumption 2.5. The coefficients a_i and b_j of $g(x)$ and $h(x)$ in (2.3.2) are either 0 or units in $\mathbb{Z}_q$. Furthermore, $a_2^2 - 4b_4$ is either 0 or a unit in $\mathbb{Z}_q$.

Remark 2.6. A lift which satisfies the above assumptions could be constructed by using Teichmüller lift. The choice of such a lift is to preserve the geometric structure. Under these assumptions, we introduce some facts which will be used later. The expansions of x and y as Laurent series of the local parameters have integral coefficients. [1] This means that x and y are in $\mathcal{O}((t))$, here $\mathcal{O}$ is the integral closure of $\mathbb{Z}_q$ in a finite extension $\mathbb{Q}_q(\alpha)$ ($\mathbb{Q}_q(\alpha_1, \alpha_2)$ in Case 4) of $\mathbb{Q}_q$ and α is the Y-coordinate of the points at infinity discussed above. Furthermore, the coefficients of the lowest terms [2] in these Laurent series are units in $\mathcal{O}$. (In Case 3, one shows that $a_1a_2 - 2b_3$ is a unit in $\mathbb{Z}_q$ by using C is smooth.) $\tilde{C}_\xi$ and $\overline{C}$ have the same geometry. In Case 4, $\sqrt{a_2^2 - 4b_4}$ is a unit in $\mathcal{O}$.

2.3.2 The reduction algorithm and algebraic de Rham cohomology

In this subsection, we present the reduction algorithm and use it to compute $H^1_{dR}(\tilde{C}_{\xi,\text{aff}}/\mathbb{Q}_q)$. First of all, since $(i+1)x^jy^idy = d(x^jy^{i+1}) - jx^{j-1}y^{i+1}dx$ for all $i \geq 0$, the universal module of differential Ω^1 of $\tilde{C}_{\xi,\text{aff}}/\mathbb{Q}_q$ is generated by $\{x^jy^idx \mid i \geq 0, j \geq 0\}$. From the defining equation (2.3.1), Ω^1 is generated by $\{x^jy^idx \mid 1 \leq i \leq 3, j \geq 0\}$. Since

$$0 = df = d\left(y^4 + g(x)y^2 + h(x)\right) = \left(g'(x)y^2 + h'(x)\right)dx + \left(4y^3 + 2g(x)y\right)dy,$$

we have

$$x^k\left(g'(x)y^2 + h'(x)\right)y^ldx + x^k\left(4y^3 + 2g(x)y\right)y^ldy = 0.$$

Combine with the following equation

$$\begin{aligned} &d\left(x^k\left(\frac{4}{l+4}y^{l+4} + \frac{2}{l+2}g(x)y^{l+2}\right)\right) - x^k\left(4y^3 + 2g(x)y\right)y^ldy \\ &= \left(\frac{4}{l+4}kx^{k-1}y^{l+4} + \frac{2}{l+2}\left(kx^{k-1}g(x) + x^kg'(x)\right)y^{l+2}\right)dx, \end{aligned}$$

one gets

$$\begin{aligned} &x^k\left(\frac{l}{l+2}g'(x)y^2 + h'(x)\right)y^ldx - kx^{k-1}\left(\frac{4}{l+4}y^4 + \frac{2}{l+2}g(x)y^2\right)y^ldx \\ &= d(S_{l,k}), \text{ where } S_{l,k} := -x^k\left(\frac{4}{l+4}y^{l+4} + \frac{2}{l+2}g(x)y^{l+2}\right) \end{aligned}$$

1. Use Hensel's lemma. For Case 1, one needs a 2-variable version of Hensel's lemma.
2. In particular, $\alpha, \beta \in \mathcal{O}^*$ if we use the notations in the above classification.

Using $y^4 = -(g(x)y^2 + h(x))$ and the explicit description of $g(x)$ and $h(x)$ in (2.3.2), the above equation becomes

$$\left(\sum_{j=-1}^{3} \Gamma_{k,l,0,j}\, x^{k+j} y^l + \sum_{j=-1}^{1} \Gamma_{k,l,2,j}\, x^{k+j} y^{l+2} \right) dx = d(S_{l,k}), \tag{2.3.3}$$

here the coefficients $\Gamma_{k,l,0,j}$ and $\Gamma_{k,l,2,j}$ are defined as following

$$\Gamma_{k,l,0,j} := (j+1+\frac{4k}{l+4})\, b_{j+1}, \quad \Gamma_{k,l,2,j} := \frac{l}{l+2}(j+1+\frac{2k}{l+4}) a_{j+1}.$$

In order to make things more clear, we use the following notation :

Definition 2.7. A family of matrices M_k of size $m \times n$ with entries $(M_k)_{i,j} = m_{k,i,j} \in \mathbb{Q}_q$ is called *a family of reduction matrices* if

$$\left(\sum_{i=1}^{m} \sum_{j=1}^{n} m_{k,i,j}\, x^{k+j-3} y^{i-1} \right) dx \equiv 0 \text{ in } \Omega^1, \text{ for all } k.$$

For reduction matrices M_k, we define $M_k\, dx$ to be

$$\left(\sum_{i=1}^{m} \sum_{j=1}^{n} m_{k,i,j}\, x^{k+j-3} y^{i-1} \right) dx.$$

For example, from (2.3.3), we have reduction matrices of size $(l+3) \times 6$ which has non-zero entries only at the $(l+1)$-th and $(l+3)$-th rows

$$M^0_{l,k} := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \Gamma_{l,k,0,-1} & \Gamma_{l,k,0,0} & \Gamma_{l,k,0,1} & \Gamma_{l,k,0,2} & \Gamma_{l,k,0,3} \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \Gamma_{l,k,2,-1} & \Gamma_{l,k,2,0} & \Gamma_{l,k,2,1} & 0 & 0 \end{pmatrix}$$

and $M^0_{l,k} dx = d(S_{l,k})$. The superscript 0 that appears in $M^0_{l,k}$ means that it is obtained from (2.3.3), without further reduction.

We have to consider $l = 1, 2$ and 3, which give the reductions of $x^{k+3}y^2 dx$ or $x^{k+2}y^2 dx$:

$\boldsymbol{l = 1}$.
As mentioned above, we have reduction matrices of size 4×6

$$M_{1,k} = \frac{1}{15} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 12kb_0 & (12k+15)b_1 & (12k+30)b_2 & (12k+45)b_3 & (12k+60)b_4 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2ka_0 & (2k+5)a_1 & (2k+10)a_2 & 0 & 0 \end{pmatrix}$$

From Section 2.3.1, we know that one of b_4 and b_3 is non-zero. Hence $x^{k+3}ydx$ or $x^{k+2}ydx$ can be reduced to a linear combination of $\{x^j y^i dx\}$ with $i = 1$ or 3 and $j \leq k+2$ (if $b_4 \neq 0$) or $j \leq k+1$ (if $b_4 = 0$), which have smaller degree in x.

$l = 2$.

From (Section 2.3.2), we have reduction matrices of size 5×6, so y^4 is involved. Using the defining equation (2.3.1) to reduce the degree in y, one gets a reduction matrix $M_{2,k}$ whose transpose is

$$M_{2,k}^t = -\frac{1}{6} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & k(a_0^2 - 4b_0) & 0 \\ 0 & 0 & (2k+3)(a_0a_1 - 2b_1) & 0 \\ 0 & 0 & (k+3)(a_1^2 + 2a_0a_2 - 4b_2) & 0 \\ 0 & 0 & (2k+9)(a_1a_2 - 2b_3) & 0 \\ 0 & 0 & (k+6)(a_2^2 - 4b_4) & 0 \end{pmatrix}$$

This gives us the reductions of $x^{k+3}y^2dx$ or $x^{k+2}y^2dx$ depending on the nullity of $a_2^2 - 4b_4$.

$l = 3$.

As at the start of $l = 2$ (dealing with y^5), one gets $M_{3,k}^1$ whose transpose is

$$-\frac{1}{35} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 6ka_0b_0 & 0 & k(6a_0^2 - 20b_0) \\ 0 & 6k(a_1b_0 + a_0b_1) + 21a_1b_0 & 0 & (4k+7)(3a_0a_1 - 5b_1) \\ 0 & 6k(a_2b_0 + a_1b_1 + a_0b_2) + 21a_1b_1 + 42a_2b_0 & 0 & (2k+7)(3a_1^2 + 6a_0a_2 - 10b_2) \\ 0 & 6k(a_2b_1 + a_1b_2 + a_0b_3) + 21a_1b_2 + 42a_2b_1 & 0 & (4k+21)(3a_1a_2 - 5b_3) \\ 0 & 6k(a_2b_2 + a_1b_3 + a_0b_4) + 21a_1b_3 + 42a_2b_2 & 0 & (2k+14)(3a_2^2 - 10b_4) \\ 0 & (6k+21)(a_2b_3 + a_1b_4) + 21a_2b_3 & 0 & 0 \\ 0 & (6k+42)a_2b_4 & 0 & 0 \end{pmatrix}$$

Since we want to reduce $x^j y^3 dx$ to those with smaller degree in x, $M_{3,k}^1$ is not suitable since it has (possible) non-zero entries which correspond to $x^{k+5}y^1$, $x^{k+4}y^1$ and $x^{k+3}y^1$. We use $l = 1$ to reduce $x^{k+3}ydx$ to $\{x^{j_1}ydx, x^{j_2}y^3dx \,|\, j_1 \leq k+2, j_2 \leq k+1\}$ if $b_4 \neq 0$, or reduce $x^{k+2}ydx$ to $\{x^{j_1}ydx, x^{j_2}y^3dx \,|\, j_1 \leq k+1, j_2 \leq k+1\}$) if $b_4 = 0$. Then use this result to reduce $x^{k+3}ydx$ (if $b_4 = 0$), $x^{k+4}ydx$ and $x^{k+5}ydx$ (if $b_4 \neq 0$) iteratively to $\{x^{j_1}ydx, x^{j_2}y^3dx \,|\, j_1 \leq k+2, j_2 \leq k+3\}$, depending the nullity of b_4. Finally, use these reductions in $M_{3,k}^1$, we get reduction matrices in

Case 3 and Case 4 : $b_4 \neq 0$

$$M'_{3,k} = c \cdot \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & * & * & * & *_{2,5} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & * & * & * & *_{4,5} & 384(k+4)(k+5)(k+6)(k+7)b_4^3(a_2^2 - 4b_4) \end{pmatrix}$$

with $c = -1/\left(2688(k+4)(k+5)(k+6)b_4^3\right)$ and

$$*_{4,5} = 96b_4^2(k+4)(k+5)(k+6)\left((8k+44)a_1a_2b_4 - a_2^2b_3 - (16k+84)b_3b_4\right)$$

which equals to $384b_4^3(k+4)(k+5)(k+6)(2k+11)(a_1a_2-2b_3)$ if $a_2^2-4b_4=0$, and

$$*_{2,5}=36(k+4)b_4\left((6k^2+136k+285)a_2b_3^3-8(6k^2+56k+125)a_2b_2b_3\right.$$
$$+48(k^2+11k+30)a_2b_1b_4^2+16(k^2+6k)a_0b_3b_4^2$$
$$\left.-2(8k^2+58k+105)a_1b_3^2b_4+16(2k^2+17k+35)a_1b_2b_4^2\right)$$

Notice that $*_{2,5}$ may be non-zero, but it corresponds to $x^{k+2}y$ and since $b_4\neq 0$, one can use $M_{1,k-1}$ in the case $l=1$ to reduce $x^{k+2}ydx$ and get a new reduction matrices

$$M_{3,k}=c\cdot\begin{pmatrix}0&0&0&0&0&0\\ *&*&*&*&0&0\\ 0&0&0&0&0&0\\ *&*&*&*&*_{4,5}&384(k+4)(k+5)(k+6)(k+7)b_4^3(a_2^2-4b_4)\end{pmatrix}$$

Notice that the reduction of $x^{k+2}ydx$ using $M_{1,k-1}$ only involve x^jydx with $k-2\leq j\leq k+1$ and x^jy^3 with $k-2\leq j\leq k$, the last two columns of $M_{3,k}$ and $M_{3,k}^2$ are the same except the $(2,5)$-entry, and $M_{3,k}$ satisfies the condition in Definition Definition 2.7, so they are indeed reduction matrices. The reduction involves division by $12(k+4)b_4$, hence $c^{-1}M_{3,k}$ has integral coefficients.

Case 1 and Case 2 : $b_4=0$

$$M_{3,k}=c\cdot\begin{pmatrix}0&0&0&0&0&0\\ 0&*&*&*&0&0\\ 0&0&0&0&0&0\\ 0&*&*&*&*_{4,5}&2(k+7)(2k+11)(4k+15)(4k+19)b_3^2a_2^2\end{pmatrix}$$

with $c=-1/\left(7(4k+15)(4k+19)(4k+23)b_3^2\right)$ and

$$*_{4,5}=(4k+15)b_3\left((32k^3+504k^2+2648k+4641)a_1a_2b_3-(4k^2+52k+168)a_2^2b_2\right.$$
$$\left.-(64k^3+1008k^2+5276k+9177)b_3^2\right)$$

which equals to $-(4k+15)(4k+19)(4k+21)(4k+23)b_3^3$ if $a_2=0$.

Now we can compute the algebraic de Rham cohomology $H^1_{dR}(\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q)$ of $\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q$.

Proposition 2.8. The algebraic de Rham cohomology $H^1_{dR}(\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q)$ has a basis

(1) $\{ydx,y^2dx,y^3dx,xydx,xy^2dx,xy^3dx\}$, if $b_4=0$ and $a_2=0$.
(2) $\{ydx,y^2dx,y^3dx,xydx,xy^2dx,xy^3dx,x^2y^2dx,x^2y^3dx\}$, if $b_4=0$ and $a_2\neq 0$.

(3) $\{ydx, y^2dx, y^3dx, xydx, xy^2dx, xy^3dx, x^2ydx\}$, if $b_4 \neq 0$ and $a_2^2 - 4b_4 = 0$.

(4) $\{ydx, y^2dx, y^3dx, xydx, xy^2dx, xy^3dx, x^2ydx, x^2y^2dx, x^2y^3dx\}$, if $b_4 \neq 0$ and $a_2^2 - 4b_4 \neq 0$.

Proof. We give the proof for (c). For other parts, the proofs are all similar. Suppose $b_4 \neq 0$ and $a_2^2 - 4b_4 = 0$. The reduction matrices $M_{1,k}$ shows that $x^{k+3}ydx$ is a linear combination of $\{x^{j_1}ydx, x^{j_2}y^3dx \mid k-1 \leq j_1 \leq k+2, k-1 \leq j_2 \leq k+1\}$, since $b_4 \neq 0$. So each x^jydx with $j \geq 3$ can be reduced. The $(3,6)$-entry of the reduction matrix $M_{2,k}$ is $(k+6)(a_2^2-4b_4) = 0$, but its $(3,5)$-entry is $(2k+9)(a_1a_2-2b_3)$ which is non-zero by Case 3 in Section 2.3.1. So $x^{k+2}y^2dx$ is a linear combination of $\{x^jy^2 \mid k-1 \leq j \leq k+1\}$ and hence each x^jy^2dx with $j \geq 2$ can be reduced. The reduction matrix $M_{3,k}$ in Case 3 has $(k+7)(a_2^2 - 4b_4) = 0$ at the $(4,6)$-entry, but its $(4,5)$-entry is $*_{4,5} = (2k+11)(a_1a_2 - 2b_3) \neq 0$. So $x^{k+2}y^3dx$ is a linear combination of $\{x^{j_1}ydx, x^{j_2}y^3dx \mid k-2 \leq j_1 \leq k+1, k-2 \leq j_2 \leq k+1\}$ and hence each x^jy^3 with $j \geq 2$ can be reduced. This completes the proof for (c). □

The following table give a more clear description of these basis.

dx	1	x	x^2
y	•	•	×
y^2	•	•	×
y^3	•	•	×

(2.1.a) Case 1

dx	1	x	x^2
y	•	•	×
y^2	•	•	•
y^3	•	•	•

(2.1.b) Case 2

dx	1	x	x^2
y	•	•	•
y^2	•	•	×
y^3	•	•	×

(2.1.c) Case 3

dx	1	x	x^2
y	•	•	•
y^2	•	•	•
y^3	•	•	•

(2.1.d) Case 4

Table 2.1 – Basis of $H^1_{dR}(\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q)$

2.3.3 Control of the denominators in the reduction algorithm and Monsky-Washnitzer cohomology

The reduction algorithm in Section 2.3.2 allows us to obtain a basis of the cohomology $H^1_{dR}(\tilde{C}_{\xi,\mathrm{aff}}/\mathbb{Q}_q)$ of $\tilde{C}_{\xi,\mathrm{aff}}$. By Theorem 2.4, this basis also forms a basis of the Monsky-Washnitzer cohomology $H^1_{MW}(C_{\mathrm{aff}}/\mathbb{F}_q)$. One can also prove this by the following upper bound on the denominators that appear during the reduction process. This bound provides the precision necessary for our algorithm.

Before stating the main result of this subsection, we fix some notations. For a local parameter t at a point at infinity P_∞, we write the Laurent series expansion of x, y and x^jy^i with respect to t as following :

$$x = \sum_{s=v_p(x)}^{\infty} \delta_s^{0,1}\, t^s, \quad y = \sum_{s=v_p(y)}^{\infty} \delta_s^{1,0}\, t^s \text{ and } x^jy^i = \sum_{s=v_p(x^jy^i)}^{\infty} \delta_s^{i,j}\, t^s. \tag{2.3.4}$$

If a subscript is used to denote a local parameter at some point, we use this subscript in the coefficients of the above expansion. For example, in Case 3, we write $x^jy^i = \sum_s^\infty \delta_{s,+}^{i,j}\, t_+^s$ at $P_{\infty,+}$ and $x^jy^i = \sum_s^\infty \delta_{s,-}^{i,j}\, t_-^s$ at $P_{\infty,-}$. Recall that all the coefficents $\delta_s^{i,j}$ are in $\mathcal{O}$ in all cases that we are concerned, see Remark 2.6.

Proposition 2.9. Write

$$x^k y^l dx = \sum_{i=1}^{3}\sum_{j=0}^{2} a_{i,j}x^jy^i dx + dS, \text{ where } S = \sum_{i=0}^{3}\sum_{j\geq 0} b_{i,j}x^jy^i \tag{2.3.5}$$

with $a_{i,j}$ and $b_{i,j} \in \mathbb{Q}_q$, $a_{i,j} = 0$ if x^jy^i is not in the basis in Proposition 2.8, $1 \leq l \leq 3$ and $k \in \mathbb{N}$. Then

(a) One can choose S with the property that $b_{i,j} = 0$ if $i - l \neq 0 \pmod 2$.

(b) For any S in (2.3.5) which satisfies the property in (a), we have $b_{i,j-i} = 0$ for all $0 \leq i \leq 3$ and $j \geq k+5$. Furthermore $p^m b_{i,j-i} \in \mathcal{O}$ for all $0 \leq i \leq 3$ and $j \geq 7$, where $m = \lfloor \log_p(4k+8) \rfloor$.

(c) $p^{m+\Delta+1}a_{i,j} \in \mathbb{Z}_q$, where $\Delta := 11\left(\lfloor \log_p(63)\rfloor + \tau(p)\right)$ with $\tau(3) = 5, \tau(5) = 3, \tau(p) = 1$ for $p = 7, 11, 13$ and $\tau(p) = 0$ if $p > 13$.

Proof. (a) Using the automorphism $y \to -y$, or by a direct analysis on the reduction process discussed in the previous subsection. (b) We prove this for Case 4, proofs for other cases are all similar. From the expansions in Case 4, one obtains

$$x^jy^i = \sum_{s=-(i+j)}^{\infty} \delta_{s,\mu,\pm}^{i,j} t_{\mu,\pm}^s \tag{2.3.6}$$

with $\delta_{-(i+j),\mu,\pm}^{i,j} = (\pm\alpha_\mu)^i$ and $\mu = 1, 2$. There is an integer $M > 0$ such that $b_{i,j} = 0$ for all $j > M$. Hence

$$\begin{aligned} S &= \sum_{i=0}^{3}\sum_{j\geq 0}^{M} b_{i,j}x^jy^i = \sum_{i=0}^{3}\sum_{j\geq 0}^{M} b_{i,j} \sum_{s=-(i+j)}^{\infty} \delta_{s,\mu,\pm}^{i,j} t_{\mu,\pm}^s \\ &= \sum_{j=0}^{M+3}\left(\sum_{i=0}^{3} b_{i,j-i}\delta_{-j,\mu,\pm}^{i,j-i} + \sum_{j'>j}^{M+3}\left(\sum_{i=0}^{3} b_{i,j'-i}\delta_{-j,\mu,\pm}^{i,j'-i}\right)\right) t_{\mu,\pm}^{-j} \end{aligned}$$

Since $\upsilon_{p_{\infty,\mu,\pm}}(a_{i,j}x^jy^idx) \geq 7$ and $\upsilon_{p_{\infty,\mu,\pm}}(x^ky^ldx) \geq -(k+5)$ and the expansions of x^ky^ldx have integral coefficients, we have

$$j \cdot \left(\sum_{i=0}^{3} b_{i,j-i}\delta_{-j,\mu,\pm}^{i,j-i} + \sum_{j'>j}^{M+3}\left(\sum_{i=0}^{3} b_{i,j'-i}\delta_{-j,\mu,\pm}^{i,j'-i}\right)\right) \in \mathcal{O} \tag{2.3.7}$$

for all $j \geq 7$ and it is zero if $j \geq k+5$. Combine (2.3.7) with the property in (a)

and the fact that α_1 and α_2 are units in $\mathcal{O}$ (Remark 2.6), we get

$$j \cdot \left(1 \cdot b_{i,j-i} + \alpha_\mu^2 \cdot b_{i+2,j-i-2} + \sum_{j'>j}^{M+3} \sum_{i=0}^{3} * \right) \in \mathcal{O}$$

for $i = 0, 1$, $j \geq 7$ and $\mu = 1, 2$, and it is zero if $j \geq k + 5$. Since $\alpha_1^2 - \alpha_2^2 = \sqrt{D}$, here $D = a_2^2 - 4b_4 \neq 0$, one obtains

$$j \cdot \left(1 \cdot b_{i,j-i} + \sqrt{D} \cdot b_{i+2,j-i-2} + \sum_{j'>j}^{M+3} \sum_{i=0}^{3} * \right) \in \mathcal{O} \tag{2.3.8}$$

for $i = 0, 1$, $j \geq 7$, and it is zero if $j \geq k+5$, here $*$ involves only $b_{i,j'-i}$ with $j' > j$ and elements in $\mathcal{O}$. Remember that $\sqrt{D} \in \mathcal{O}^*$. Apply $j = M + 3$ to (2.3.8), we know that $b_{i,M+3-i} = 0$ for all $0 \leq i \leq 3$. Repeat the same argument, one shows that $b_{i,j-i} = 0$ for all $0 \leq i \leq 3$ and $j \geq k + 5$. Now apply $j = k + 4$ to (2.3.8), we get $p^m b_{i,k+4-i} \in \mathcal{O}$ for all $0 \leq i \leq 3$. Repeat the same argument and notice that the terms $*$ in (2.3.8) are in $\mathcal{O}$ in each step (since all the $\delta_s^{\bullet,\bullet}$ and $b_{i,j'-i} \in \mathcal{O}$ if $j' > j$ in each step),one proves that $p^m b_{i,j-i} \in \mathcal{O}$ for all $0 \leq i \leq 3$ and $j \geq 7$. So $p^m b_{i,j-i} \in \mathcal{O} \cap \mathbb{Q}_q = \mathbb{Z}_q$ for all $0 \leq i \leq 3$ and $j \geq 7$.
(c) Consider

$$\omega := p^m \left(x^k y^l dx - d \left(\sum_{i=0}^{3} \sum_{j \geq 7-i}^{k+5} b_{i,j} x^j y^i \right) \right) \tag{2.3.9a}$$

$$= p^m \left(\sum_{i=1}^{3} \sum_{j=0}^{2} a_{i,j} x^j y^i dx + d \left(\sum_{i=0}^{3} \sum_{j=0}^{6-i} b_{i,j} x^j y^i \right) \right) \tag{2.3.9b}$$

From (b) and (2.3.9a), one knows that ω has integral coefficients, so we can choose $\varphi_1(x, y)$ and $\psi_1(x, y)$ in $\mathbb{Z}_q[x, y]$ such that $\omega = \psi_1\, dx + \varphi_1\, dy$. On the other hand, from (2.3.9b), one knows that $\omega = \psi_2\, dx + \varphi_2\, dy$ for some φ_2 and ψ_2 in $\mathbb{Q}_q[x, y]$ with $\deg(\varphi_2) \leq 5$, $\deg(\psi_2) \leq 5$. Consider

$$\begin{aligned} f_y\, \omega &= f_y\, (\psi_i\, dx + \varphi_i\, dy) = (\psi_i f_y - \varphi_i f_x)\, dx \\ f_x\, \omega &= f_x\, (\psi_i\, dx + \varphi_i\, dy) = (\varphi_i f_x - \psi_i f_y)\, dy \end{aligned} \tag{2.3.10}$$

(using $f_x\, dx + f_y\, dy = df = 0$). Let $\lambda_i(x, y) := \psi_i f_y - \varphi_i f_x$. It is clear that $\lambda_1 \in \mathbb{Z}_q[x, y]$ and $\lambda_2 \in \mathbb{Q}_q[x, y]$ with $\deg(\lambda_2) \leq 8$. Using the defining equation f to reduce the degree of y in λ_i, we get $f_y\, \omega = \tilde{\lambda}_i\, dx$ and $f_x\, \omega = -\tilde{\lambda}_i\, dy$ with $\tilde{\lambda}_1 \in \mathbb{Z}_q[x, y]$, $\deg_y(\tilde{\lambda}_1) \leq 3$, $\tilde{\lambda}_2 \in \mathbb{Q}_q[x, y]$, $\deg(\tilde{\lambda}_2) \leq 8$ and $\deg_y(\tilde{\lambda}_2) \leq 3$. Since $(\tilde{\lambda}_1 - \tilde{\lambda}_2)dx = f_y\, \omega - f_y\, \omega = 0$ and $\deg_y(\tilde{\lambda}_1 - \tilde{\lambda}_2) \leq 3$, we have $\tilde{\lambda}_1 = \tilde{\lambda}_2$. This means that $f_y\, \omega = \tilde{\lambda}\, dx$ and $f_x\, \omega = -\tilde{\lambda}\, dy$ with $\tilde{\lambda} := \tilde{\lambda}_1 = \tilde{\lambda}_2$ which is in $\mathbb{Z}_q[x, y]$ of $\deg(\tilde{\lambda}) \leq 8$. By Corollary 2.12, there exist α and β in $\mathbb{Z}_q[x, y]$ with $\deg(\alpha) \leq 5$ and $\deg(\beta) \leq 5$ such that $\alpha f_y + \beta f_x = 1$ in A. So $\omega = (\alpha f_y + \beta f_x)\, \omega = (\alpha\tilde{\lambda})dx - (\beta\tilde{\lambda})dy$. Notice

that $\omega \equiv \sum_{i=1}^{3}\sum_{j=0}^{2} p^m a_{i,j}\, x^j y^i dx$, we can use the reduction of $(\alpha\tilde{\lambda})dx - (\beta\tilde{\lambda})dy$ to get the denominators of $p^m a_{i,j}$. Since $\deg(\alpha\tilde{\lambda}) \leq 13$ and $\deg(\beta\tilde{\lambda}) \leq 13$, we need only to know the denominators of the final reductions of $x^j y^i dx$ and $x^j y^i dy$ with $0 \leq i+j \leq 13$. Using $x^j y^i dy \equiv -j/(i+1) x^{j-1} y^{i+1} dx$, the defining equation f, and $x^j dx \equiv 0$, we only need to consider the reductions of $x^j y^i dx$ with $1 \leq i \leq 3$ and $i+j \leq 13$, but if $p = 3$, the extra denominator 3 should be counted.

The reduction of $x^k y^l dx$ $(1 \leq l \leq 3)$ using the reduction matrices $M_{i,j}$ in Section 2.3.2 involve divisions by some of the following : $12(k+2)b_4$, $(12k+21)b_3$, $(k+3)(a_2^2 - 4b_4)$, $(2k+5)(a_1a_2 - 2b_3)$, $384(k+1)(k+2)(k+3)(k+4)b_4^3(a_2^2 - 4b_4)$, $384(k+2)(k+3)(k+4)(2k+7)b_4^3(a_1a_2 - 2b_3)$, $2(k+4)(2k+5)(4k+3)(4k+7)b_3^2a_2^2$, $-(4k+7)(4k+11)(4k+13)(4k+15)b_3^3$, depending on each case, and the numbers $2, a_2, b_4, b_3, a_2^2 - 4b_4$ and $a_1a_2 - 2b_3$ that we need to consider (depending on each case) are units of $\mathbb{Z}_q$. So in each step, we get extra denominators which are at most

$$p^{\lfloor \log_p(4j+15) \rfloor + \tau(p)},$$

here $\tau(3) = 5, \tau(5) = 3, \tau(p) = 1$ for $p = 7, 1, 13$ and $\tau(p) = 0$ if $p > 13$. Since we are concerned with $2 \leq j \leq 12$, we need at most 11 reduction steps, so the denominators of the reductions of $x^j y^i dx$ with $1 \leq i \leq 3$ and $i+j \leq 13$ are at most

$$p^{11 \cdot (\lfloor \log_p(63) \rfloor + \tau(p))}.$$

Hence $p^{m+\Delta+1} a_{i,j} \in \mathbb{Z}_q$. □

Remark 2.10. Proposition 2.9 gives an upper bound for the denominators after a differential form (with integral coefficients) is reduced to the linear combination of the basis we found in Proposition 2.8. Along with the rate of convergence of the Frobenius F_p (see Corollary 2.22), one can determine how much p-adic precision we need to work with (and determine an integer N_3 such that one can work with modulo x^{N_3}), see Section 2.6. But one needs an upper bound for all the denominators that will appear during the computation (in the reduction step) in order to know how much precision of the reduction matrices $M_{i,j}$ are required and to have an analysis of the bit complexity. It turns out that one has a similar bound as in Proposition 2.9. The proof is completely similar.

Theorem 2.11. Let R be a field or a discrete valuation ring and $\mathfrak{m}$ be the maximal ideal of R. Let $f_0, \ldots, f_n \in R[x_1, \ldots, x_n]$ with $\deg f_i = d_i$ and define

$$\rho = d_0 + \ldots + d_n - n - 1.$$

Denote the homogenization of f_i by f_i^h for $i = 0, \ldots, n$. Assume that there is no point in $\mathbb{P}^n(\overline{R/\mathfrak{m}})$ satisfies $f_0^h = f_1^h = \ldots = f_n^h = 0$. Then there exist polynomials $g_0, \ldots, g_n \in R[x_1, \ldots, x_n]$ with $\deg g_i \leq \rho + 1 - d_i$ for $i = 0, \ldots, n$ such that

$$\sum_{i=0}^{n} g_i f_i = 1.$$

Proof. This appears as Theorem 2 in Denef-Vercauteren [DV06]. □

Corollary 2.12. There exist α and β in $\mathbb{Z}_q[x, y]$ with $\deg(\alpha) \leq 5$ and $\deg(\beta) \leq 5$ such that $\alpha f_y + \beta f_x = 1$ in A. Furthermore, one can find such α and β such that α has only odd degrees in y and β has only even degrees in y.

Proof. Apply Theorem 2.11 to $R = \mathbb{Z}_q$, $f_0 = f$, $f_1 = f_y$ and $f_2 = f_x$.

Apply Theorem 2.11 to $R = \mathbb{Z}_q$, $f_0 = f$, $f_1 = f_y$ and $f_2 = f_x$. If α and β don't satisfy the last property, consider the equality

$$\alpha(x, -y)f_y(x, -y) + \beta(x, -y)f_x(x, -y) = 1$$

in A. From (2.3.1), it is clear that $f_y(x, -y) = -f_y(x, y)$ and $f_x(x, -y) = f_x(x, y)$. We thus have

$$\left(\frac{\alpha(x, y) - \alpha(x, -y)}{2}\right) f_y + \left(\frac{\beta(x, y) + \beta(x, -y)}{2}\right) f_x = 1,$$

which completes the proof. □

2.4 Lift of Frobenius

In this section, we describe a lift F_p of the absolute Frobeninus endomorphism $\overline{F}_p : \overline{a} \to \overline{a}^p$ on the coordinate ring $\overline{A}$ of $\overline{C}_{\text{aff}}$ to $A^\dagger$. This means that F_p is a $\mathbb{Z}_p$-algebra endomorphism on $A^\dagger$ such that $\pi \circ F_p = \overline{F}_p \circ \pi$, where π is the reduction modulo p. The lift F_q of the q-th Frobenius endomorphism of $\overline{A}$ is F_p^n, hence one can work with F_p for the purpose of computation.

Denote by σ the p-th power Frobenius endomorphism on $\mathbb{F}_p$ and also its lift on $\mathbb{Z}_p$. Any lift F_p satisfies

$$F_p(x) \equiv x^p \bmod p, \quad F_p(y) \equiv y^p \bmod p, \quad F_p(f(x, y)) = 0.$$

From Corollary 2.12, we know that there exist α and β in $\mathbb{Z}_q[x, y]$ such that $\alpha f_y + \beta f_x = 1$. Define $\delta_y := \alpha^p$, $\delta_x := \beta^p$ and consider the equation

$$G(Z) := F_p(f(x, y)) = f^\sigma(x^p + \delta_x Z, y^p + \delta_y Z) = 0 \tag{2.4.1}$$

in $A^\dagger[Z]$. Then $G(0) = f^\sigma(x^p, y^p) \equiv f^\sigma(x^\sigma, y^\sigma) = 0 \bmod p$. We also have $G'(0) = f_y^\sigma(x^p, y^p)\delta_y + f_x^\sigma(x^p, y^p)\delta_x \equiv f_y^\sigma(x^\sigma, y^\sigma)\delta_y + f_x^\sigma(x^\sigma, y^\sigma)\delta_x \equiv f_y^p\delta_y + f_x^p\delta_x = f_y^p\alpha^p + f_x^p\beta^p = (f_y\alpha + f_x\beta)^p = 1 \bmod p$. Hence by Hensel's lemma, there is a unique solution of (2.4.1) in A^∞. We will prove that this solution is in fact in $A^\dagger$. In fact, Corollary 2.22 below gives an explicit lower bound on the rate of convergence, which allows us (together with Proposition 2.8) to work with a finite and explicit p-adic precision.

We start with a series of lemmas. Given the following data of integers :

$$\begin{aligned}
-1 = \Delta_{1,-1} < \Delta_{1,0} < \Delta_{1,1} < \cdots < \Delta_{1,j} < \cdots \\
-1 = \Delta_{2,-1} < \Delta_{2,0} < \Delta_{2,1} < \cdots < \Delta_{2,j} < \cdots \\
\vdots \\
-1 = \Delta_{n,-1} < \Delta_{n,0} < \Delta_{n,1} < \cdots < \Delta_{n,j} < \cdots \\
\vdots
\end{aligned}$$

we can define subsets (for each $n \geq 1$) of the power series ring $\mathbb{Z}_q\langle x\rangle$:

$$S_n := \left\{ \sum_{i=0}^{\infty} a_i x^i \;\middle|\; v_p(a_i) \geq n + j + 1 \;\text{ if }\; i \geq \Delta_{n,j} + 1 \right\}.$$

Lemma 2.13. Let (p) be the ideal of $\mathbb{Z}_q\langle x\rangle$ generated by p, i.e. $(p) = p\,\mathbb{Z}_q\langle x\rangle$. Then $S_n \subseteq (p)^n$.

Proof. Consider $j = -1$ in the definition of S_n. We see $v_p(a_i) \geq n + (-1) + 1 = n$ if $i \geq \Delta_{n,-1} + 1 = (-1) + 1 = 0$. Hence $S_n \subseteq (p)^n$. □

We first study several conditions on $\Delta_{n,j}$ for which the sets S_n satisfy some nice properties.

Lemma 2.14. For any fixed n, we have $S_1\, S_n \subseteq S_{n+1}$ if

$$\Delta_{n+1,j} \geq \max_{0 \leq \ell \leq j} \{\Delta_{1,\ell} + \Delta_{n,j-\ell}\} \;\text{ for all } j. \tag{2.4.2}$$

Proof. Assume the above condition (2.4.2) holds. Given $f_1 = \sum_{i=0}^{\infty} a_i x^i \in S_1$ and $f_2 = \sum_{k=0}^{\infty} b_k x^k \in S_n$, we have

$$f_1\, f_n = \sum_{m=0}^{\infty} c_m x^m, \;\text{ where } c_m := \sum_{i+k=m} a_i\, b_k.$$

Given $m \geq \Delta_{n+1,j} + 1$. Consider each summand $a_i b_k$ with $i + k = m$ in c_m. If $i \geq \Delta_{1,j} + 1$, we have $v_p(a_i) \geq 1 + j + 1$, since $f_1 \in S_1$. We also have $v_p(b_k) \geq n$ for $f_n \in S_n \subseteq (p)^n$, by Lemma 2.13. So $v_p(a_i b_k) \geq (n+1) + j + 1$ if $i \geq \Delta_{1,j} + 1$. For $i \leq \Delta_{1,j}$, we can find some $0 \leq \ell \leq j$ such that $\Delta_{1,\ell-1} + 1 \leq i \leq \Delta_{1,\ell}$. Then we get

$$\begin{aligned}
k = m - i &\geq (\Delta_{n+1,j} + 1) - i \\
&\geq \left(\max_{0 \leq \ell' \leq j} \{\Delta_{1,\ell'} + \Delta_{n,j-\ell'}\} + 1 \right) - \Delta_{1,\ell} \\
&\geq (\Delta_{1,\ell} + \Delta_{n,j-\ell} + 1) - \Delta_{1,\ell} \\
&= \Delta_{n,j-\ell} + 1.
\end{aligned}$$

Hence $v_p(b_k) \geq n + (j - \ell) + 1$ since $f_n \in S_n$. We also have $v_p(a_i) \geq 1 + (\ell - 1) + 1$ since $f_1 \in S_1$ and we are under the assumption $i \geq \Delta_{1,\ell-1} + 1$. This shows that $v_p(a_i b_k) \geq n + (j - \ell) + 1 + 1 + (\ell - 1) + 1 = (n + 1) + j + 1$ for each summand $a_i b_k$ in c_m with $i \leq \Delta_{1,j}$. The about arguments prove that $v_p(c_m) \geq (n+1) + j + 1$ if $m \geq \Delta_{n+1,j} + 1$, and thus $f_1 f_n \in S_{n+1}$. This completes the proof. □

The following lemma gives a condition for which we have $S_n \subseteq S_1$.

Lemma 2.15. Consider any fixed n. If $\Delta_{1,\ell+n-1} \geq \Delta_{n,\ell}$ for all $\ell \geq 0$, then $S_n \subseteq S_1$.

Proof. Given $f_n = \sum_{i=0}^{\infty} a_i x^i \in S_n$. From the definition of S_n, for $j \geq n - 1$, we have $v_p(a_i) \geq n + (j - n + 1) + 1 = 1 + j + 1$ if $i \geq \Delta_{n,j-n+1}$. By our condition (for $\ell = j - n + 1$), we have $\Delta_{1,j} \geq \Delta_{n,j-n+1}$, and thus $v_p(a_i) \geq 1 + j + 1$ if $i \geq \Delta_{1,j}$. For $j \leq n - 2$, we have $v_p(a_i) \geq n$ for arbitrary i by Lemma 2.13, thus $v_p(a_i) \geq n \geq j + 2 = 1 + j + 1$ for any i. Hence $f_n \in S_1$. This proves that $S_n \subseteq S_1$. □

Corollary 2.16. If the conditions in Lemma 2.14 and Lemma 2.15 hold for any $n \geq 1$, then we have

$$S_1^n \subseteq S_n \subset S_1.$$

Lemma 2.17. Given a polynomial $g \in \mathbb{Z}_q[x]$ with degree d_0. Assume $g \in (p)$. Then $g \in S_1$ if $\Delta_{1,0} \geq d_0$.

Proof. This is easy. □

Lemma 2.18. Given a polynomial $g \in \mathbb{Z}_q[x]$ with degree d_1, and $f_1 \in S_1$. Assume $g \in (p)$. Then $g f_1 \in S_1$ if $\Delta_{1,j} \geq \Delta_{1,j-1} + d_1$ for all $j \geq 0$.

Proof. The proof is similar to Lemma 2.19 below However, there is a minor difference. In this lemma, we assume $g \in (p)$. However, in Lemma 2.19, we don't assume this condition. □

Lemma 2.19. Let $n \geq 2$ be fixed. Given a polynomial $g \in \mathbb{Z}_q[x]$ with degree d. Then $g S_n \subseteq S_1$ if $\Delta_{1,n-1+\ell} \geq \Delta_{n,\ell} + d$ for all $\ell \geq 0$.

Proof. Assume the condition in the above statement holds. Write $g = \sum_{i=0}^{d} a_i x^i$. Given $f_n = \sum_{k=0}^{\infty} b_k x^k \in S_n$, write

$$g f_n = \sum_{m=0}^{\infty} c_m x^m, \text{ where } c_m := \sum_{i+k=m,\, 0 \leq i \leq d} a_i b_k.$$

Since $f_n \in S_n \subseteq (p)^n$, the values $v_p(b_k) \geq n \geq 1 + j + 1$ for all $0 \leq j \leq n - 2$ and all k, thus $v_p(c_m) \geq 1 + j + 1$ for all $0 \leq j \leq n - 2$ and all m. Now consider the cases where $j \geq n - 1$. If $m \geq \Delta_{1,j} + 1$, then by the condition (for $\ell = j - n + 1$), we have $m \geq \Delta_{1,j} + 1 \geq \Delta_{n,j-n+1} + d + 1$. Since $i + k = m$, $0 \leq i \leq d$ and $m \geq \Delta_{n,j-n+1} + d + 1$, we have $k \geq \Delta_{n,j-n+1} + 1$. Since $f_n \in S_n$, by the definition,

we obtain $v_p(a_i b_k) \geq v_p(b_k) \geq n + (j - n + 1) + 1 = 1 + j + 1$. This implies that $v_p(c_m) \geq 1 + j + 1$ under the condition $m \geq \Delta_{1,j} + 1$ for all $j \geq 0$. The case for $j = -1$ is trivial, and by the definition of S_1, we see $gf_n \in\subset S_1$. This completes the proof. □

Lemma 2.20. Let $H(Z) = \sum h_k(x) Z^k \in \mathbb{Z}_q[x][Z]$ and $d_k := \deg(h_k)$. Assume $h_0(x) \equiv 0 \bmod p$ and $h_1(x) \equiv 1 \bmod p$. Let $-1 = \Delta_{n,-1} < \Delta_{n,0} < \Delta_{n,1} < \cdots < \Delta_{n,j} < \cdots$, for $n \geq 1$ and $j \geq 0$, be integers satisfy the following conditions :

1. $\Delta_{n+1,j} \geq \max\limits_{0 \leq \ell \leq j} \{\Delta_{1,\ell} + \Delta_{n,j-\ell}\}$ for all $n \geq 1$, $j \geq 0$.
2. $\Delta_{1,0} \geq d_0$.
3. $\Delta_{1,j} - \Delta_{1,j-1} \geq d_1$ for all $j \geq 0$.
4. $\Delta_{1,n-1+\ell} \geq \Delta_{n,\ell} + d_n$ for all $n \geq 2, \ell \geq 0$.

Then the unique solution $\alpha = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{Z}_q\langle x \rangle$ of $H(Z) = 0$ has the property : $v_p(a_i) \geq j + 2$ if $i \geq \Delta_{1,j} + 1$. One can always find such $\Delta_{n,j}$.

Proof. In $\mathbb{Z}_q\langle x \rangle$, we can use Newton method to compute α : $\alpha_0 = 0$, $\alpha_1 = -h_0(x)$ and

$$\alpha_{i+1} = \alpha_i - \frac{H(\alpha_i)}{H'(\alpha_i)} = \alpha_i - H(\alpha_i) \left(1 + \sum_{k=1}^{\infty} (1 - H'(\alpha_i))^k\right).$$

The conditions on $\Delta_{n,j}$ ensure that the result α_i in the i-th iteration above is in S_i. We use induction to prove this. It is obviously true for $i = 0$. For $i = 1$, it follows from condition 2 and Lemma 2.17. Assume $\alpha_i \in S_1$ and we want to prove $\alpha_{i+1} \in S_1$. It is sufficient to show : $H(\alpha_i) \in S_1$ and $(1 - H'(\alpha_i))\, S_1 \subset S_1$. $H(\alpha_i) = h_0(x) + h_1(x)\alpha_i + \sum_{n=2}^{\infty} h_n(x)\alpha_i^n$. We have seen $h_0(x) \in S_1$. From condition 3 and Lemma 2.18, we know $(1 - h_1(x))\alpha_i \in S_1$, thus $h_1(x)\alpha_i = \alpha_i - (1 - h_1(x))\, \alpha_i \in S_1$. Similarly for $n \geq 2$, since $\alpha_i^n \in S_1^n \subseteq S_n$, which is from condition 1 and Lemma 2.14, we have $h_n(x)\alpha_i^n \in S_1$, which is from condition 4 and Lemma 2.19. This proves that $H(\alpha_i) \in S_1$.

For the proof of $(1 - H'(\alpha_i))\, S_1 \subset S_1$, we use

$$(1 - H'(\alpha_i)) = \left((1 - h_1(x)) - \sum_{n=2}^{\infty} n h_n(x) \alpha_i^{n-1}\right).$$

The proof is exactly the same as above. We then completed the proof of $\alpha_{i+1} \in S_1$, and this implies that the solution $\alpha \in S_1$.

For the existence of $\Delta_{n,j}$, notice that the conditions 2, 3 and 4 are equivalent to : $\Delta_{1,n+1} \geq \max\{\Delta_{1,n} + d_1, \Delta_{k,n+2-k} + d_k \mid 2 \leq k \leq n + 2\}$ for all $n \geq 0$. Suppose one has determined $\Delta_{n',j'}$ for all $n' + j' \leq n + 1$. Use condition 1, one can determine $\Delta_{k,n+2-k}$ for all $2 \leq k \leq n + 2$ (i.e. for $\Delta_{n',j'}$ with $n' + j' \leq n + 2$ and $n' \geq 2$). Finally, one determines $\Delta_{1,n+1}$. Therefore, one determines all the $\Delta_{n',j'}$ with $n' + j' \leq n + 2$. This shows that one can find $\Delta_{n,j}$ recursively. □

Lemma 2.21. Suppose $\deg(h_k(x)) \leq (k+1)\,d$ in Lemma 2.20. Then $\Delta_{i,j} := (i+4j)\,d$ satisfy the conditions in Lemma 2.20 and all the inequalities are equalities. In particular, $\Delta_{1,j} = (4j+1)\,d$.

Proof. This follows by induction in i and j. □

Corollary 2.22. There exists a lift F_p of the absolute Frobeninus endomorphism $\overline{a} \to \overline{a}^p$ on the coordinate ring $\overline{A}$ of $\overline{C}_{\text{aff}}$ to $A^\dagger$ such that $F_p(x) = x^p + \delta_x Z_0$ and $F_p(y) = y^p + \delta_y Z_0$ with $Z_0 = \sum_{i,j} a_{i,j} x^j y^i$, $a_{i,j} \in \mathbb{Z}_q$ and $\text{ord}_p(a_{i,j}) > \frac{i+j}{16p}$. Also the coefficient of $x^j y^i$ in $F_p(y)$ and $F_p(x)$ has p-adic order $> \frac{i+j}{16p}$ if $i + j \neq p$. Finally, $F_p(x^k y^l dx) = \sum_{i=1}^{3} \sum_j b_{i,j} x^j y^i dx$ with $\text{ord}_p(b_{i,j}) > \frac{i+j}{16p} - 4$.

Proof. Using Corollary 2.12 and Equation (2.4.1), one can apply $d = 4p$ to Lemma 2.21. □

Theorem 2.23. There exists a lift of Frobenius F_p on $A^\dagger$ which commutes with the involution $\tau : y \to -y$ and has the rate of convergence in Corollary Corollary 2.22.

Proof. We choose α and β such that α has only odd degrees in y and β has only even degrees in y as in Corollary 2.12. Since $\delta_y = \alpha^p$ and $\delta_x = \beta^p$, they have the same property as α and β. For solving $G(Z) = 0$ by Newton's method, we use Lemma 2.20 with $H = G = f^\sigma(x^p + \delta_x Z, y^p + \delta_y Z)$. It is clear that G has only even degrees in y, hence so does the solution Z_0. From this, it is clear that the lift of Frobenius $F_p : A^\dagger \to A^\dagger$ commutes with the involution τ. □

2.5 Quotient by automorphism

We have study $H^1_{MW}(C_{\text{aff}}/\mathbb{F}_q)$. In this section, we consider the quotient of C by the automorphism $\tau : Y \to -Y$. We denote the quotient map by $\pi : C \to E := C/\langle\tau\rangle$. One can show that $C/\langle\tau\rangle$ has genus 1 either by Riemann-Hurwitz genus formula or from the affine equation directly, using the fact that C_{aff} is stable under τ and $C_{\text{aff}}/\langle\tau\rangle$ is smooth, hence the notation E is justified. The affine part E_{aff} of E is $C_{\text{aff}}/\langle\tau\rangle$, which has the defining equation : $v^2 + \overline{g}(u)v + \overline{h}(u) = 0$. We have $C_{\text{aff}} \xrightarrow{\pi} E_{\text{aff}}$, $(x, y) \to (x, y^2)$, and the corresponding map on the coordinate ring is $\pi^* : u \to x$, $v \to y^2$.

Our goal is to study the followings : $H^1_{MW}(E_{\text{aff}}/\mathbb{F}_q)$, the induced map $\pi^* : H^i_{MW}(E_{\text{aff}}/\mathbb{F}_q) \to H^i_{MW}(C_{\text{aff}}/\mathbb{F}_q)$ and its interplay with Frobenius endomorphism. Since $\tilde{C}_{\text{aff}} \xrightarrow{\tilde{\pi}} \tilde{E}_{\text{aff}}$, $(x, y) \to (x, y^2)$ lifts π, here $\tilde{E}_{\text{aff}}$ is the lift of E_{aff}, whose defining equation is $v^2 + g(u)v + h(u) = 0$, we can study $H^i_{MW}(E_{\text{aff}}/\mathbb{F}_q) \xrightarrow{\pi^*} H^i_{MW}(C_{\text{aff}}/\mathbb{F}_q)$ by $H^i_{dR}(\tilde{E}_{\text{aff},\xi}/\mathbb{Q}_q) \xrightarrow{\tilde{\pi}^*} H^i_{dR}(\tilde{C}_{\text{aff},\xi}/\mathbb{Q}_q)$. For $i \neq 1$, these are isomorphisms. For $i = 1$, since $\{\tilde{\pi}^*(u^j v du) = x^j y^2 dx\} \mid 0 \leq j \leq 1 \text{ (resp. } 0 \leq j \leq 2)\}$ are linear independent in Case 1 and Case 3 (resp. in Case 2 and Case 4),

one sees that $\{u^j v du \mid 0 \leq j \leq 1 \text{ (resp. } 0 \leq j \leq 2)\}$ are linear independent. Let δ_E be the number of points at infinity of E. We have $\delta_E = 1, 2, 1, 2$ in each case, hence $\dim_{\mathbb{Z}_q} H^1_{dR}(\tilde{E}_{\text{aff},\xi}/\mathbb{Q}_q) = 2 \cdot g_E - 1 + \delta_E = 2, 3, 2, 3$. This shows that $\{u^j v du \mid 0 \leq j \leq 1 \text{ (resp. } 0 \leq j \leq 2)\}$ is the basis of $H^1_{dR}(\tilde{E}_{\text{aff},\xi}/\mathbb{Q}_q)$ which is isomorphic via $\tilde{\pi}^*$ to the subspace V of $H^1_{dR}(\tilde{C}_{\text{aff},\xi}/\mathbb{Q}_q)$ generated by $\{x^j y^2 dx \mid 0 \leq j \leq 1 \text{ (resp. } 0 \leq j \leq 2)\}$.

As in Section 2.4, there is a lift $F_{q,E} : A_E^\dagger \to A_E^\dagger$ of the Frobenius endomorphism $\overline{F}_{q,E}$ on the coordinate ring $\overline{A}_E$ of E. The left diagram below is not necessary commutative, but its reduction mod p is commutative

$$\begin{array}{ccc} A^\dagger & \xleftarrow{\tilde{\pi}^*} & A_E^\dagger \\ \downarrow{\scriptstyle F_q} & & \downarrow{\scriptstyle F_{q,E}} \\ A^\dagger & \xleftarrow[\tilde{\pi}^*]{} & A_E^\dagger \end{array} \qquad \begin{array}{ccc} \overline{A} & \xleftarrow{\pi^*} & \overline{A}_E \\ \downarrow{\scriptstyle \overline{F}_q} & & \downarrow{\scriptstyle \overline{F}_{q,E}} \\ \overline{A} & \xleftarrow[\pi^*]{} & \overline{A}_E \end{array}$$

Here $A^\dagger \xleftarrow{\tilde{\pi}^*} A_E^\dagger$ is the natural lift of homomorphism $A \xleftarrow{\tilde{\pi}^*} A_E$ on the coordinate rings which corresponds to the morphism $\tilde{\pi} : \tilde{C}_{\text{aff},\xi}/\mathbb{Q}_q \to \tilde{E}_{\text{aff},\xi}/\mathbb{Q}_q$, so the reduction of $A^\dagger \xleftarrow{\tilde{\pi}^*} A_E^\dagger$ modulo p is just the natural homomorphism on the coordinate rings of $C_{\text{aff}} \xrightarrow{\pi} E_{\text{aff}}$. Since $\overline{F}_q \circ \pi^* = \pi^* \circ \overline{F}_{q,E}$, we know that

$$\begin{array}{ccc} H^i_{MW}(C_{\text{aff}}/\mathbb{F}_q) & \xleftarrow{\pi^*} & H^i_{MW}(E_{\text{aff}}/\mathbb{F}_q) \\ \downarrow{\scriptstyle F_{q,*}} & & \downarrow{\scriptstyle F_{q,E,*}} \\ H^i_{MW}(C_{\text{aff}}/\mathbb{F}_q) & \xleftarrow[\pi^*]{} & H^i_{MW}(E_{\text{aff}}/\mathbb{F}_q) \end{array}$$

So the point counting on E_{aff} is the same as computing on the subsapce of $H^1_{MW}(C_{\text{aff}}/\mathbb{F}_q)$ generated by $\{x^j y^2 dx \mid 0 \leq j \leq 1 \text{ (resp. } 0 \leq j \leq 2)\}$.

From Lefschetz fixed point formula (Theorem 2.3), we have

$$\begin{aligned} \#C_{\text{aff}}(\mathbb{F}_{q^r}) &= \operatorname{Tr}\left((qF_{q,*}^{-1})^r | H^0_{MW}(C_{\text{aff}})\right) - \operatorname{Tr}\left((qF_{q,*}^{-1})^r | H^1_{MW}(C_{\text{aff}})\right) \\ \#E_{\text{aff}}(\mathbb{F}_{q^r}) &= \operatorname{Tr}\left((qF_{q,*}^{-1})^r | H^0_{MW}(E_{\text{aff}})\right) - \operatorname{Tr}\left((qF_{q,*}^{-1})^r | H^1_{MW}(E_{\text{aff}})\right) \end{aligned}$$

Let $P_E(X) = (X - \beta_1)(X - \beta_2)$ be the Weil polynomial of E and $S_r(E) := \beta_1^r + \beta_2^r$. Then $\#E_{\text{aff}}(\mathbb{F}_{q^r}) = q^r + 1 - S_r(E) - \delta_E$, here δ_E is the number of points at infinity of E. Use $\#C_{\text{aff}}(\mathbb{F}_{q^r}) = \#C(\mathbb{F}_{q^r}) - \delta_C$, we get

$$\#C(\mathbb{F}_{q^r}) = q^r + 1 - S_r(E) - \operatorname{Tr}\left((qF_{q,*}^{-1})^r | V\right) + (\delta_C - \delta_E),$$

here V is the subsapce of $H^1_{MW}(C_{\text{aff}}/\mathbb{F}_q)$ generated by $\{x^j y^2 dx \mid 0 \leq j \leq 1 \text{ (resp. } 0 \leq j \leq 2)\}$, whose dimension is $4 + \delta_C - \delta_E$. This implies that the Weil polynomial $P(X)$ of $C/\mathbb{F}_q$ equals to $P_E(X)Q_V(X)(X-1)^{-(\delta_C-\delta_E)}$, here $Q_V(X)$ is the characteristic polynomial of $qF_{q,*}^{-1}$ acts on V. The characteristic polynomial $P_V(X)$ of $F_{q,*} = q \cdot (qF_{q,*}^{-1})^{-1}$ is $Q_V(X)(X-q)^{\delta_C-\delta_E}(X-1)^{-(\delta_C-\delta_E)}$, so

$$P(X) = P_E(X)P_V(X)(X-q)^{-(\delta_C-\delta_E)}.$$

Summary 2.24. The Weil polynomial $P(X)$ of $C/\mathbb{F}_q$ is equal to

$$P_E(X)P_V(X)(X-q)^{-(\delta_C-\delta_E)},$$

where $P_E(X)$ is the Weil polynomial of $E/\mathbb{F}_q$ and $P_V(X)$ is the characteristic polynomial of $F_{q,*}$ on V.

2.6 The algorithm

In order to compute $P_V(X)$, one needs to compute $P_V(X)$ with a precision $N_1 = \lfloor \log_p 30 + 2n \rfloor + 1$ with $n = \log_p q$, which is determined by the Weil bound. Due to the fact that the matrix M_p of the Frobenius action $F_{p,*}$ may have denominators, we need M_p with a precision $N_2 := N_1 + (6n-1)c$ with $c = \lfloor c_1 + \log_p(c_1 + \log_p(2c_1)) \rfloor + 1$ and $c_1 = 6 + \log_p 80 + \Delta$. From this, we only need to compute (for $1 \leq l \leq 3$ and $0 \leq k \leq 2$) Z_0, $F_p(x)$, $F_p(y)$ and $F_p(y^l x^k dx)$ modulo (x^{N_3}, p^{N_4}) with $N_3 = \lfloor 16p(c_2 + \log_p(2c_2)) \rfloor + 1$, $N_4 = \lfloor N_2 + c_1 + \log_p(c_2 + \log_p(2c_2)) \rfloor + 1$ and $c_2 = 6 + \log_p 80 + \Delta + N_2$. Finally, the above discussion is based on the reduction matrices $M_{i,k}$ $(1 \leq i \leq 3)$ introduced in Section 2.3.2. But since one can only work with an approximation of $M_{i,k}$, one need $M_{i,k}$ modulo p^{N_5} with a slightly higher precision $N_5 = N_4 + 8\lfloor \log_p N_3 \rfloor + 14$. We have $N_3 = O(pn)$, $N_4 = O(n)$ and $N_5 = O(n)$. We work in $\mathbb{Z}_q/p^{N_5}$ [3], whose elements can be stored in $O(n^2 \log p)$ space and the arithmetic on it could be done in $\tilde{O}(n^2 \log p)$ bit operations. This gives the algorithm :

Algorithm

Step 1. Compute α and β in Corollary 2.12 modulo p. [4]

Step 2. Compute Z_0 in Corollary 2.22 using Newton's method, then $F_p(x^k y^l dx)$ for $l = 1, 3$ and $0 \leq k \leq 2$, all of them are modulo (x^{N_3}, p^{N_4}). [5]

3. More precisely, with p-adic precsion N_4 but with denominators at most $p^{(N_5-N_4)}$.

4. In Corollary 2.12, we only need $\alpha f_y + \beta f_x \equiv 1$ modulo p in order to compute the lift of Frobenius.

5. In the proof of Lemma 2.20, we showed that the results during the Newton's iteration all have the same rate of convergence as in Corollary 2.22, so we can work modulo x^{N_3} during the Newton's iteration.

Step 3. Use reduction matrices $M_{i,j}$ $(1 \leq i \leq 3, 2 \leq j \leq N_3)$ to reduce $F_p(x^k y^l dx)$ and get M_p.

Step 4. Compute $M_q = M_p M_p^{\sigma} \cdots M_p^{\sigma^{n-1}}$ by repeated squaring.

Step 5. Finally, compute the characteristic polynomial $P_V(X)$ modulo P^{N_1}.

Theorem 2.25. The above algorithm requires $\tilde{O}(n^3 p)$ bit operations.

Proof. Step 1 consists of solving a system of linear equations over $\mathbb{F}_q$ of size at most 16. Hence it requires $\tilde{O}(n^2 \log p)$ bit operations. Step 2 requires $O(\log N_4)$ Newton's iterations, and each iteration requires $\tilde{O}(N_3 n^2 \log p)$ bit operations. Hence this step requires $\tilde{O}(pn^3)$ bit operations. Step 3 requires $O(N_3)$ operations in $\mathbb{Z}_q/p^{N_5}$, hence $\tilde{O}(pn^3)$ bit operations. Step 4 requires $O(\log n)$ squarings and the application of the lift of the p-th power Frobenius $\sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ modulo p^{N_4} on matrices of size 6×6. Squaring requires $\tilde{O}(n^2 \log p)$ bit operations. For σ, we use Newton's method which needs to evaluate a polynomial of degree n with coefficients in $\mathbb{Z}_q/p^{N_4}$, which requires $O(n)\tilde{O}(n^2 \log p)$ bit operations. Hence we need $\tilde{O}(n^3 \log p)$ bit operations in this step. Step 5 requires $\tilde{O}(n^2 \log p)$ bit operations. Hence the algorithm requires $\tilde{O}(n^3 p)$ bit operations. □

If one works directly on $H^1_{MW}(C_{\text{aff}})$ and denote the precision needed by N_i', then $N_i \approx \frac{2}{3} N_i'$. Also the matrix M_p is of size 6×6 and M_p' is of size 9×9. From these, we give a comparison of speed. Step 2 is reduced by a factor of $(\frac{2}{3})^2 \approx 0.45$. In Step 3, we have 6 differential forms $F_p(x^k y^l dx)$, $l = 1, 3$ and $0 \leq k \leq 2$, to reduce. This contributes a factor of $\frac{4}{5}$. (It is $\frac{4}{5}$ instead of $\frac{2}{3}$ because the reductions of $F_p(x^k y^2 dx)$ involve fewer operations than the reductions of $F_p(x^k y^1 dx)$ and $F_p(x^k y^3 dx)$. See the reduction matrices in Section 2.3.2.) Since each of these $F_p(x^k y^l dx)$ is computed modulo (x^{N_3}, p^{N_4}) in Step 2, we work with smaller powers on x and fewer p-adic precision in Step 3. This means that we have fewer reduction steps and the basic arithmetic operations are faster, which contribute a factor of $(\frac{2}{3})^2$. So Step 3 is reduced by a factor of $\frac{4}{5} \cdot (\frac{2}{3})^2 \approx 0.36$. Step 4 is reduced by a factor at least of $(\frac{2}{3})^3 \approx 0.3$, due to the smaller size of M_p and fewer precision.

Deuxième partie

Frobenius Distributions and Character Theory

Chapitre 3

Sato-Tate Groups

In the chapters of Part I, we study the characteristic polynomial of the Frobenius action for a single algebraic curve over a finite field F_p. In March 1963, the Japanese mathematician Mikio Sato arrived at a conjecture about the distribution of traces [1] of Frobenius actions for a family of elliptic curves E_p over (different) finite fields $\mathbb{F}_p$, obtained from an elliptic curve $E/\mathbb{Q}$ by reduction modulo primes p of good reduction. Sato found this conjectural distribution experimentally based on computational data using computers. In the same year, John Tate also discovered this distribution in his article "*Algebraic cycles and poles of zeta functions*" [Tat65], but he gave a theoretical explanation based on another conjecture. One can find some more historical details about Sato-Tate conjecture in a web page of Ralf Schmidt [Sch] or on a slide of Tetsushi Ito [Ito].

In this chapter, we give a quick introduction to Sato-Tate conjecture. Section 3.3 recalls the notion of moments of a random variable and gives some moment sequences which can be used to distinguish different distributions. In Section 3.4, we give the statement of the generalized Sato-Tate conjecture without details. Finally, we demonstrate the advantage, over the use of moments, of irreducible characters of compact Lie groups to the study of higher dimensional Sato-Tate conjecture in Section 3.5.

3.1 Sato-Tate distributions for elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve with short Weierstrass equation

$$y^2 = x^3 + ax + b,\ a, b \in \mathbb{Q}\,.$$

Let p be a prime of good reduction of E, which means $v_p(\Delta) = 0$, where $\Delta = -16(4a^3 + 27b^2)$ is the discriminant of E. The reduction $\overline{E}_p$ of E module p is again an elliptic curve (over $\mathbb{F}_p$).

1. Sato worked with Frobenius angle $\theta_p = \cos^{-1}\left(\frac{t_p}{2\sqrt{p}}\right) \in [0, \pi]$, rather then the trace t_p of Frobenius.

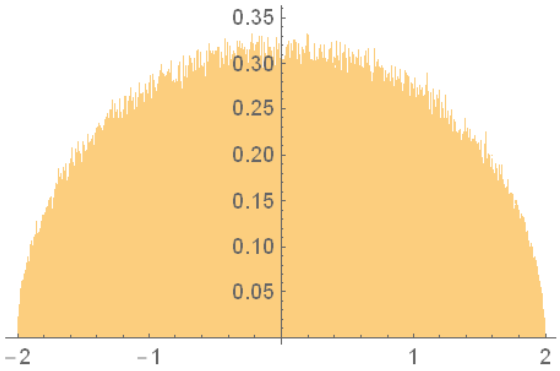
The number of $\mathbb{F}_p$-points on $\overline{E}_p$ is

$$\#\overline{E}_p(\mathbb{F}_p) = p + 1 - t_p\,,$$

where t_p is the trace of Frobenius, which is an integer in the interval $[-2\sqrt{p}, 2\sqrt{p}]$.

The Sato-Tate conjecture is concerned with the limiting distribution of $-t_p/\sqrt{p} \in [-2, 2]$ as p varies over primes of good reduction.

Example 3.1. Consider the elliptic curve $E : y^2 = x^3 + x + 1$ defined over the rational field $\mathbb{Q}$. We compute the normalized trace $-t_p/\sqrt{p}$ for prime of good reduction $p \leq 2^{20}$. The histogram of the probability density of this data is



bin width = $1/2^8$

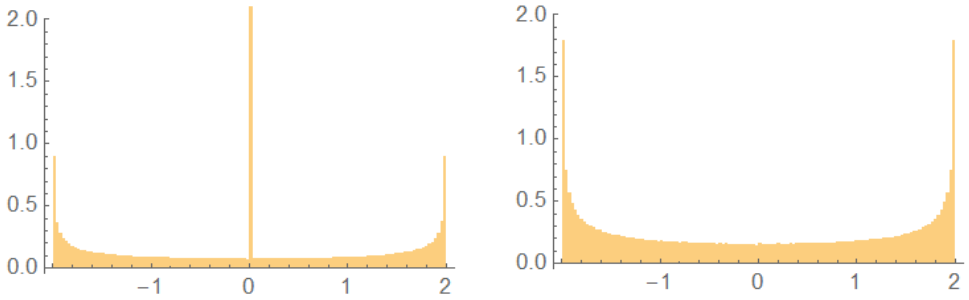
The probability density function of $-t_p/\sqrt{p}$ is

$$\frac{1}{2\pi}\sqrt{4 - t^2}\,.$$

The aspect ratio of axes in the above picture is not 1 and its shape reflects the $\sqrt{4 - t^2}$ part in the probability density function, which is a semicircle of radius 2.

Example 3.2. The elliptic curve $E : y^2 = x^3 + x$ has complex multiplication by $\mathbb{Q}(i)$. In this example, we regard E as defined both over $\mathbb{Q}$ and over its CM field $\mathbb{Q}(i)$.

The histograms of the probability density of the datas $-t_{\mathfrak{p}}/\left\|\mathfrak{p}\right\|^{1/2}$ for $\|\mathfrak{p}\| \leq 2^{20}$ (where $\mathfrak{p}$ is a prime in $\mathbb{Q}$ or $\mathbb{Q}(i)$, and $\|\mathfrak{p}\|$ is the usual norm) are shown below.



$\mathbb{Q}$ $\qquad$ $\mathbb{Q}(i)$: $\frac{1}{\pi}\frac{1}{\sqrt{4-t^2}}$

For $E/\mathbb{Q}$, it has trace zero for half of the primes. Thus we have a peak at zero in the picture. Besides this fact, the distributions of the normalized trace are the same in these two cases.

The following theorem summarizes the above facts.

Theorem 3.3 (Sato-Tate distributions for elliptic curves)**.** An elliptic curve $E/\mathbb{Q}$ without CM has the semi-circular trace distribution. An elliptic curve E/k with CM has one of the two trace distributions shown in the above examples, depending on whether k contains its CM field.

The three possible (normalized) trace distributions are in fact the distribution of traces in some closed subgroups of the unitary symplectic group $\mathrm{USp}(2) \cong \mathrm{SU}(2)$. The distributions are given by the Haar measure on these subgroups. These closed subgroups are called *Sato-Tate* groups (of the corresponding elliptic curve E). Only two of them arise for elliptic curves defined over $\mathbb{Q}$.

G	G/G^0	example curve E	k
$\mathrm{U}(1)$	C_1	$y^2 = x^3 + x$	$\mathbb{Q}(i)$
$N(\mathrm{U}(1))$	C_2	$y^2 = x^3 + x$	$\mathbb{Q}$
$\mathrm{SU}(2)$	C_1	$y^2 = x^3 + x + 1$	$\mathbb{Q}$

In Section 3.3.1, we explain more precisely the meaning of the above statement.

3.2 Probability space and random variables

In order to present the statements about the distributions of Frobenius actions, we have to recall basic notations and definitions from measure theory and probability theory.

Definition 3.4. Let X be a set and Σ be a collection of subsets of X. The collection Σ is called a *σ-algebra (over X)* if it satisfies the following three properties :

(1) $X \in \Sigma$.

(2) If $A \in \Sigma$, then its complement $X \backslash A$ is also in Σ.

(3) Σ is closed under countable unions : $A_n \in \Sigma$ for all $n \in \mathbb{N} \Rightarrow \bigcup_{n=1}^{\infty} A_n \in \Sigma$.

Remark 3.5. Condition (3) can be replaced by Σ is closed under countable intersections : $A_n \in \Sigma$ for all $n \in \mathbb{N} \Rightarrow \bigcap_{n=1}^{\infty} A_n \in \Sigma$.

Example 3.6. For any X, we have the largest σ-algebra $2^X = \{A \mid A \subset X\}$ (the power set of X) and the smallest σ-algebra $\{\varnothing, X\}$. For any σ-algebra Σ over X, we have $\{\varnothing, X\} \subset \Sigma \subset 2^X$.

Definition 3.7. A set X with a σ-algebra Σ is called a *measurable space*, and is usually denoted by (X, Σ). An element $A \in \Sigma$ is called a *measurable subset of* X or *measurable set in* X, which is with respect to the σ-algebra Σ.

Definition 3.8. Let (X, Σ) be a measurable space. A function $\mu : X \to [0, \infty]$ is called a *measure* if it satisfies $\mu(\varnothing) = 0$ and

$$\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu\left(A_n\right), \tag{3.2.1}$$

if $\{A_n\}_{n\in\mathbb{N}}$ is a collection of pairwise disjoint subsets of X in Σ. A *measure space* is a measurable space (X, Σ) together with a measure $\mu : X \to [0, \infty]$. It is denoted by (X, Σ, μ).

Remark 3.9. The condition (3.2.1) is called *countable additivity* or *σ-additivity*. Note that the measure μ can take the value $+\infty$.

Definition 3.10. A *probability measure* is a measure μ on a measurable space (X, Σ) such that $\mu(X) = 1$. A measure space (X, Σ, μ) is called a *probability space* if its measure μ is a probability measure.

Proposition 3.11. Let (X, Σ, μ) be a measure space. We have :

(1) For members A and B in Σ with $A \subset B$, the complement $B\backslash A$ of A in B is in Σ.

(2) For members A and B in Σ with $A \subset B$, we have $\mu(A) \leq \mu(B)$. More precisely, $\mu(B) = \mu(A) + \mu(B\backslash A)$, where $B\backslash A \in \Sigma$ is from (1). In particular, $\mu(X\backslash A) = 1 - \mu(A)$ if μ is a probability measure.

Remark 3.12. In probability theory, a probability space is usually a mathematical (or called *probabilistic*) model of a real-word situation or experiment in which the results occur randomly. Thinking a probability space (X, Σ, μ) as such a model, the set X is the *sample space*, i.e the set of *outcomes*. A set in the σ-algebra Σ is called an *event*. An event consists of a single outcome is also called an *elementary event* or *simple event*. The value $\mu(A)$ of the probability measure μ for an event $A \in \Sigma$ is the probability (frequency) that the event A occurs when the experiment being modeled repeats.

We have defined some abstract notions above, e.g σ-algebra and measure. In order to give an (important) example for the case $X = \mathbb{R}$, we still need some knowledge about σ-algebra.

Proposition 3.13. Let X be a set. The intersection of any number of σ-algebras over X is still a σ-algebra.

Definition 3.14. From Proposition 3.13, for any collection Σ of subsets of X, there is a smallest σ-algebra $\sigma(\Sigma)$ containing Σ :

$$\sigma(\Sigma) = \bigcap_{\substack{\mathcal{B}\supset\Sigma \\ \mathcal{B}:\,\sigma-\text{algebra}}} \mathcal{B}.$$

The intersection is taken in 2^X, since each $\mathcal{B}$ is a subset of 2^X. We call $\sigma(\Sigma)$ *the σ-algebra generated by Σ*.

Definition 3.15. For a topological space X, the *Borel σ-algebra* on X, denoted by $\mathfrak{B}(X)$, is the smallest σ-algebra containing all open subsets of X (or, equivalently, all closed subsets). Elements in $\mathfrak{B}(X)$ are called *Borel sets*, or more precisely, *Borel subsets of X*. Hence it is also common to call $\mathfrak{B}(X)$ *the σ-algebra of Borel sets*. The measurable space $(X, \mathfrak{B}(X))$ is called *the Borel space associated to X*.

Remark 3.16. In the above definition, $\mathfrak{B}(X)$ is also the smallest σ-algebra containing all closed subsets of X.

Example 3.17. Consider the collection of open intervals (a, b) with $a < b$ of $X = \mathbb{R}$. The *Borel σ-algebra on $\mathbb{R}$* is the σ-algebra generated by this collection, and it is denoted by $\mathfrak{B}(\mathbb{R})$.

Remark 3.18. If we start with other kinds of intervals, like $[a, b]$ or $(\infty, b]$, etc., or with the collection of all open subsets of $\mathbb{R}$ (with its usual topology), we get the same σ-algebra.

Definition 3.19. Let X be a locally compact Hausdorff space. A *Borel measure* is any measure μ on the Borel space $(X, \mathfrak{B}(X))$ associated to X.

Example 3.20. Consider the Borel space $(\mathbb{R}, \mathfrak{B}(\mathbb{R}))$. Let μ be the function $\mu([a, b]) = b - a$ for each bounded closed interval $[a, b]$ of $\mathbb{R}$. There is a unique extension of μ to $\mathfrak{B}(\mathbb{R})$ such that this extension is a Borel measure on $(\mathbb{R}, \mathfrak{B}(\mathbb{R}))$, see Example 1.4.4 in page 14 and Theorem 1.5.6 in page 18 of Bogachev's book [Bog07]. This is the "usual" Borel measure on the real line $\mathbb{R}$.

As mentioned in Remark 3.12, the probability theory models an experiment as a probability space (X, Σ, μ). This model gives the complete probabilistic information of the experiment and it helps people to understand the statistical aspect of the underlying experiment. Usually, we are interested in some quantities (numerical properties) of the outcomes, not other specific nature of them.

For example, if the experiment is tossing two dice, we may be interested only in the sum of their results, rather than the two results of each. Here is the definition of random variables :

Definition 3.21. Let (X, Σ_X) and (Y, Σ_Y) be measurable spaces. A function $\xi : X \to Y$ is called a *measurable function*, with respect to the σ-algebra Σ_X and Σ_Y, if $\xi^{-1}(B) \in \Sigma_X$ for every $B \in \Sigma_Y$. The map ξ is called an *isomorphism of measurable spaces* if it is a bijection and both ξ and ξ^{-1} are measurable functions.

Definition 3.22. Let (X, Σ_X, μ_X) and (Y, Σ_Y, μ_Y) be measure spaces. A function $\xi : X \to Y$ is called *measure preserving* if ξ is measurable and $\mu_X(\xi^{-1}(B)) = \mu_Y(B)$ for every $B \in \Sigma_Y$. The map ξ is called an *isomorphism of measure spaces* if it is an isomorphism of measurable spaces and measure preserving.

Definition 3.23. Let (X, Σ, μ) be a probability space. A *random variable* ξ on (X, Σ, μ) is a measurable function on the sample space X :

$$\xi : (X, \Sigma) \to (\mathbb{R}, \mathfrak{B}(\mathbb{R})). \tag{3.2.2}$$

If Σ and μ are understood, we simply call ξ a *random variable on* X. More generally, a *random element (with values in S)* is a measurable function $\xi : (X, \Sigma) \to (S, \mathcal{S})$ to a measurable space $(S, \mathcal{S})$.

Remark 3.24. A composition of measurable functions is still a measurable function. Given a measurable function $\eta : (X, \Sigma_X) \to (Y, \Sigma_Y)$ and a random element $\xi : (Y, \Sigma_Y) \to (Z, \Sigma_Z)$, the *pullback* $\eta^{-1}\xi = \xi \circ \eta$ of ξ is a random element on X.

Proposition 3.25. Let $\xi : (X, \Sigma, \mu) \to (\mathbb{R}, \mathfrak{B}(\mathbb{R}))$ be a random variable. It induces a measure μ_ξ on the Borel space $(\mathbb{R}, \mathfrak{B}(\mathbb{R}))$:

$$\mu_\xi(A) = \mu(\xi^{-1}(A)), \text{ for all } A \in \mathfrak{B}(\mathbb{R}). \tag{3.2.3}$$

This induced measure μ_ξ is called the *probability measure*, of the random variable ξ. Together with μ_ξ, the triple $(\mathbb{R}, \mathfrak{B}(\mathbb{R}), \mu_\xi)$ is a probability space.

Remark 3.26. Let $\eta : (X, \Sigma_X, \mu_X) \to (Y, \Sigma_Y, \mu_Y)$ be a measure preserving map and ξ is a random variable on Y. From Remark 3.24, we see $\eta^{-1}\xi$ is a random variable on X. It it easy to see the induced measures μ_ξ and $\mu_{\eta^{-1}\xi}$ are the same.

Let ξ be an random variable and $a \in \mathbb{R}$. The probability of the event

$$\{x \in X \mid \xi(x) = a\}$$

is just $\mu(\xi^{-1}(a)) = \mu_\xi(\{a\})$ by the notation in Proposition 3.25. It is common to denote this probability by $\mu(\xi = a)$. Similarly, we have notations $\mu(\xi \leq a)$ for the interval $(-\infty, a)$, or more generally, $\mu(\xi \in A)$ for a Borel set $A \in \mathfrak{B}(\mathbb{R})$.

Definition 3.27. Let ξ be a (real valued) random variable. The *cumulative distribution function* $F_\xi : \mathbb{R} \to \mathbb{R}$ *of* ξ is the function given by

$$F_\xi(x) = \mu(\xi \leq x).$$

The following proposition says that the probability measures of random variables ξ_1 and ξ_2 are the same if (and only if) they have the same distribution function.

Proposition 3.28. Let ξ_1 and ξ_2 be random variables. Then

$$\mu_{\xi_1} = \mu_{\xi_2} \Leftrightarrow F_{\xi_1} = F_{\xi_2}.$$

We will restrict ourselves to the following class of random variables.

Definition 3.29. A random variable ξ is called *absolutely continuous* if there exists a non-negative, Lebesgue integrable function f_ξ on $(-\infty, \infty)$ such that

$$F_\xi(x) = \int_{u=-\infty}^{u=x} f_\xi(u)du,\ x \in \mathbb{R}.$$

The function f_ξ is called the *probability density function* (PDF) of the random variable ξ.

Definition 3.30. For a random variable $\xi : (X, \Sigma, \mu) \to (\mathbb{R}, \mathfrak{B}(\mathbb{R}))$, its *expectation* is

$$E[\xi] = \int_{x \in X} \xi(x)\mu(dx) \tag{3.2.4}$$

when the integral exists, where the integral is the Lebesgue integral on the measure space (X, Σ, μ). If ξ is absolutely continuous with f_ξ as its probability density function, then its expectation can be computed by

$$\int_{u=-\infty}^{u=\infty} u\, f_\xi(u)du.$$

The n*-th moment* of ξ is $E[\xi^n]$.

3.2.1 Convergence of measures and equidistribution

In this section, we recall the notions and definitions related to equidistribution. We start with the definition of "uniformly distributed" of a sequence of real numbers.

Definition 3.31. A sequence (x_n) of real numbers is said to be *uniformly distributed* on an interval $[a, b]$ if for any subinterval $[c, d]$ of $[a, b]$ we have

$$\lim_{n\to\infty} \frac{\#\left\{x_i \in [c, d] \mid 1 \leq i \leq n\right\}}{n} = \frac{d-c}{b-a}\cdot \tag{3.2.5}$$

Example 3.32. Given an irrational number α. Consider the sequence $(\{n\alpha\})$, where $\{n\alpha\}$ is the fractional part of $n\alpha$. Weyl's Equidistribution theorem says that this sequence is uniformly distributed on $[0,1]$.

Now We define equidistribution with respect to a measure. The above definition is a special case with the usual Borel measure on the interval $[a,b]$.

Definition 3.33. Let μ be a probability measure on $[a,b]$ and (x_n) is a sequence with $x_n \in [a,b]$ for all n. The sequence (x_n) is said to be *equidistributed with respect to* μ if

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i) = \int_{x=a}^{x=b} f(x)\mu(dx) \tag{3.2.6}$$

for all bounded continuous functions f on $[a,b]$.

Remark 3.34. In practice, we can not test (3.2.6) for all bounded continuous functions f. A common choice is the function $x \to x^k$. Consider the probability measure space $([a,b], \mathfrak{B}([a,b]), \mu)$ and the random variable $\xi : x \in [a,b] \to x$. The quantity $\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} x_i^k$ is the k-th sample moment of the first n sample points $x_1, x_2, \ldots, x_n$. Thus we compute these numerical moments to see if they converge to the expected values.

It is easy to see that an equidistributed sequence (x_n) on an interval $[a,b]$ with respect to the Borel measure is uniformly distributed in the sense of Definition 3.31. The converse is also true. In fact, if (x_n) is uniformly distributed, 3.2.6 holds even for all Riemann integrable functions on $[a,b]$. In the following, we define convergences of measures. The definition of equidistribution is then just the convergence of the average of a sequence of point measures. This helps us to view the equidistribution of a sequence of numbers as the convergence of probabilities.

We discussed measure spaces and measurable functions. If the sample space X of a measure space (X, Σ, μ) is a topological space, we have the concept of continuous functions. If Σ is the Borel σ-algebra $\mathfrak{B}(X)$, every continuous function is measurable. The *Baire σ-algebra* is the smallest σ-algebra such that all continuous functions on X are measurable. If X is a metric space, the $\mathfrak{B}(X)$ is the Baire σ-algebra.

Definition 3.35. Let X be a metric space, μ and $\mu_1, \ldots, \mu_n, \ldots$ be a (sequence) of finite measures on $(X, \mathfrak{B}(X))$. We say that (μ_n) *converges weakly to* μ if

$$\int_X f d\mu_n \to \int_X f d\mu, \text{ for all bounded continuous real function on } X. \tag{3.2.7}$$

Theorem 3.36 (Portmanteau theorem)**.** The sequence (μ_n) of measures converges weakly to a measure μ if and only if $\lim_{n\to\infty} \mu_n(A) = \mu(A)$ for all $A \in \mathfrak{B}(X)$ with $\mu(\partial A) = 0$, where ∂A is the boundary of A.

Proof. See [Bil99, Thm 2.1, p.16] for the case of probability measure, [MS01, Prop 1.2.13, p. 11] for the case $X = \mathbb{R}^n$, or a lecture note of Molchanov and Zuyev [MZ, Theoremm 3.5, p.14]. □

In Definition 3.33, we require the convergence of $\mu_n(A)$ for a large class of sets. However, Definition 3.31 only requires to check on closed interval.

Definition 3.37. Let $\mathcal{A}$ be a subset of the Borel σ-algebra $\mathfrak{B}(X)$. We call $\mathcal{A}$ a *convergence determining class* if for every sequence (μ_n) of measures and μ, convergences $\mu_n(A) \to \mu(A)$ for all $A \in \mathcal{A}$ such that $\mu(\partial A) = 0$ implies that (μ_n) converges weakly to μ.

Theorem 3.38. For the space $(\mathbb{R}^n, \mathfrak{B}(\mathbb{R}^n))$, the set of closed bounded n-dimensional intervals form a convergence determining class.

Proof. See [Bil99, Theorem 2.4, p.18] and the Example 2.3 after it. □

By Theorem 3.38, the convergence of $\mu_n(I)$ for those closed bounded intervals with $\mu(\partial I) = 0$ implies that (μ_n) converges weakly to μ. Now assume (μ_n) converges weakly to μ. Let λ be the usual Borel measure on $(\mathbb{R}^n, \mathfrak{B}(\mathbb{R}^n))$. We have $\lambda(\partial I) = 0$. If our measure μ satisfies that $\lambda(A) = 0$ implies that $\mu(A) = 0$ for all Borel set A. Then we have $\mu(\partial I) = 0$ for all I. By 3.36, we obtain the convergence $\mu_n(I) \to \mu(I)$ for all closed bounded intervals.

Proposition 3.39. Consider a measure μ on the space $(\mathbb{R}^n, \mathfrak{B}(\mathbb{R}^n))$. Let λ be the usual Borel measure on $(\mathbb{R}^n, \mathfrak{B}(\mathbb{R}^n))$. Assume μ satisfies that $\lambda(A) = 0$ implies that $\mu(A) = 0$ for all Borel set A. The sequence (μ_n) converges weakly to μ if and only if $\lim_{n\to\infty} \mu_n(I) = \mu(I)$ for all closed bounded intervals.

Remark 3.40. The above condition on μ is called μ is *absolutely continuous with respect to the measure* λ. This is related to Definition 3.29. Hence Proposition 3.39 is valid if the measure μ has a probability density function.

We close this section by a discussion of another version of convergence of measures which is a natural analogue of pointwise convergence of function.

Definition 3.41. Let μ and $\mu_1, \ldots, \mu_n, \ldots$ be a (sequence) of finite measures on a measurable space (X, Σ). We say that (μ_n) *converges setwise to* μ if $\mu_n(A) \to \mu(A)$ for all $A \in \Sigma$. In this case, we write $\mu_n \xrightarrow{s} \mu$.

Proposition 3.42. The sequence (μ_n) converges setwise to μ if and only if

$$\int_X f d\mu_n \to \int_X f d\mu, \text{ for all bounded measurable real function on } X. \quad (3.2.8)$$

Proposition 3.43. Let X be a metric space, μ and $\mu_1, \ldots, \mu_n, \ldots$ be a (sequence) of finite measures on $(X, \mathfrak{B}(X))$. The following statements are equivalent :

(a) $\mu_n \xrightarrow{s} \mu$.

(b) $\lim_{n\to\infty} \mu_n(U) = \mu(U)$ for all open subset U of X.

(c) $\lim_{n\to\infty} \mu_n(C) = \mu(C)$ for all closed subset C of X.

Proof. See [FKZ14, Theorem 2.3, p.3]. □

Theorem 3.44. Let X be a metric space, μ and $\mu_1, \ldots, \mu_n, \ldots$ be a (sequence) of finite measures on $(X, \mathfrak{B}(X))$. If μ_n converge setwise to μ, then μ_n converges weakly to μ.

Proof. This is from Proposition 3.42. □

3.3 Moment sequences and Sato-Tate groups

In this section, we use the notions and definitions in the previous section for the special unitary group $\mathrm{SU}(2)$. Then we state the Sato-Tate conjecture and related results.

Definition 3.45. The *special unitary* group $\mathrm{SU}(2)$ is

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) : |\alpha|^2 + |\beta|^2 = 1 \right\}. \tag{3.3.1}$$

$\mathrm{SU}(2)$ is a subgroup of the general linear group $\mathrm{GL}_2(\mathbb{C})$, whose group operation is the matrix multiplication. In fact, it is a compact Lie group, which we will define later, see Definition 4.1. There is a Borel measure $\mu_{\mathrm{SU}(2)}$ on $\mathrm{SU}(2)$, which is translation invariant. This measure is called the Haar measure on $\mathrm{SU}(2)$. The Haar measure is a normalized measure so that it is a probability measure, thus we have a probability space $\big(\mathrm{SU}(2), \mathfrak{B}(\mathrm{SU}(2)), \mu_{\mathrm{SU}(2)}\big)$, which is the probability space in the Sato-Tate conjecture, as we will see in Conjecture 3.49. But we first study some probability-theory specific properties of this space. Consider the trace map $\mathrm{tr} : \mathrm{SU}(2) \to I = [-2, 2]$. It is easy to see tr is a measurable function from $(\mathrm{SU}(2), \mathfrak{B}(\mathrm{SU}(2)))$ to $(I, \mathfrak{B}(I))$, thus it is a random variable on $\big(\mathrm{SU}(2), \mathfrak{B}(\mathrm{SU}(2)), \mu_{\mathrm{SU}(2)}\big)$. Let t be the standard coordinate function on $I = [-2, 2]$.

Proposition 3.46. The random variable tr on $\mathrm{SU}(2)$ has the probability density function

$$f_{\mathrm{tr}} : [-2, 2] \to \mathbb{R},\ f_{\mathrm{tr}} = \frac{1}{2\pi}\sqrt{4 - t^2}\,. \tag{3.3.2}$$

Its n-th moment $M_n(\mathrm{tr})$ is then

$$\frac{1}{2\pi}\int_{-2}^{2} t^n \sqrt{4 - t^2}\, dt = \begin{cases} 0 & \text{if n is odd,} \\ \frac{2}{n+2}\binom{n}{n/2} & \text{if n is even.} \end{cases} \tag{3.3.3}$$

Definition 3.47. The *special orthogonal group* (in dimension 2) $\mathrm{SO}(2)$ is

$$\mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : \theta \in [0, 2\pi) \right\} . \tag{3.3.4}$$

It is clear that $\mathrm{SO}(2)$ is a subgroup of $\mathrm{SU}(2)$.

Definition 3.48. The *unitary group* (of degree 1) $\mathrm{U}(1)$ is the unit circle $\{z \in \mathbb{C} \mid |z| = 1\}$ in the complex plane. The group operation of $\mathrm{U}(1)$ is the multiplication of complex numbers. It is also called the *circle group* and often denoted by $\mathbb{T}$.

The group $\mathrm{U}(1)$ has a standard parametrization, which is the restriction to $[0, 2\pi)$ of the *exponential map* $\exp : \mathbb{R} \to \mathrm{U}(1)$, $\theta \mapsto z = e^{i\theta}$. We have a standard isomorphism $\phi : \mathrm{U}(1) \xrightarrow{\sim} \mathrm{SO}(2)$:

$$e^{i\theta} \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} . \tag{3.3.5}$$

We have an embedding $\iota : \mathrm{U}(1) \hookrightarrow \mathrm{SU}(2)$ given by

$$z = e^{i\theta} \mapsto \begin{pmatrix} z & 0 \\ 0 & \frac{1}{z} \end{pmatrix} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} .$$

Note that $\mathrm{SO}(2) \subset \mathrm{SU}(2)$ and $\iota(\mathrm{U}(1)) \subset \mathrm{SU}(2)$ are two different subgroups of $\mathrm{SU}(2)$, but they are conjugate by an element in $\mathrm{SU}(2)$:

$$\begin{pmatrix} i & -1 \\ 1 & -i \end{pmatrix}^{-1} \cdot \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} i & -1 \\ 1 & -i \end{pmatrix} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \in \iota(\mathrm{U}(1)) . \tag{3.3.6}$$

As for the group $\mathrm{SU}(2)$, each subgroup mentioned above is a probability space when it is equipped with its Haar measure. With the above explicit isomorphisms between $\mathrm{U}(1)$, $\iota(\mathrm{U}(1))$ and $\mathrm{SO}(2)$, it is easy to see that these are isomorphic probability spaces. Moreover, the random variables tr (one for each of these probability spaces) are the pullbacks of the other ones under these isomorphisms. Hence they induce the same probability measure on $I = [-2, 2]$ (Remark 3.26), and we will regard them as the same probability space and random variable.

One can (easily) compute the moments for the group $\mathrm{U}(1)$ and $N(\mathrm{U}(1))$. These are recorded in the following table. The normalizer $N(\mathrm{U}(1))$ of $\iota(\mathrm{U}(1))$ in $\mathrm{SU}(2)$ have two connected components : one is $\iota(\mathrm{U}(1))$, which consists of the diagonal matrices in $\iota(\mathrm{U}(1))$. The other component consists of the anti-diagonal matrices

$$\begin{pmatrix} 0 & -e^{-i\theta} \\ e^{i\theta} & 0 \end{pmatrix} \in \mathrm{SU}(2).$$

The random variable tr on this component is identical 0. This explains

$$M_{2n}\left(\mathrm{tr}|_{N(\mathrm{U}(1))}\right) = \frac{1}{2} M_{2n}\left(\mathrm{tr}|_{\mathrm{U}(1)}\right),$$

as we see in the table.

G	G/G^0	moments $M_{2n}(t)$
$\mathrm{U}(1)$	C_1	$1, 2, 6, 20, 70, 252, 924, 3432 \cdots$
$N(\mathrm{U}(1))$	C_2	$1, 1, 3, 10, 35, 126, 462, 1716 \cdots$
$\mathrm{SU}(2)$	C_1	$1, 1, 2, 5, 14, 42, 132, 429 \cdots$

Table 3.1 – Moments sequences

3.3.1 Sato-Tate conjecture for elliptic curves

After developing the necessary tools, we can give the precise statement of Sato-Tate conjecture.

Conjecture 3.49 (Sato-Tate)**.** Let $E/\mathbb{Q}$ be an elliptic curve as mentioned at the beginning of Section 3.1. Assume that E has no complex multiplication. Consider the sequence of normalized traces $t_p/\sqrt{p} \in [-2, 2]$ of the reduction of E modulo p, where p runs over the primes of good reduction of E. Then the sequence[2] $\left(t_p/\sqrt{p}\right)$ is equidistributed with respect to the induced measure on $[-2, 2]$ of the random variable tr on the group $\mathrm{SU}(2)$ with its Haar measure $\mu_{\mathrm{SU}(2)}$.

The induced measure of tr on $I = [-2, 2]$ is $\frac{1}{2\pi}\sqrt{4 - t^2}dt$, see Proposition 3.46. This measure is absolutely continuous with respect to the Borel measure on I, see Definition 3.29 and Remark 3.40. From Definition 3.33, Definition 3.35 and Proposition 3.39, Sato-Tate conjecture is equivalent to, for any interval $[a, b] \subset [-2, 2]$,

$$\lim_{X\to\infty} \frac{\#\left\{p \leq X \mid t_p/\sqrt{p} \in [a, b]\right\}}{\#\{p \leq X\}} = \int_a^b \frac{\sqrt{4 - t^2}}{2\pi} dt.$$

This may be the easiest form of Sato-Tate conjecture about the equidistribution of the normalized traces.

In literature, Sato-Tate conjecture is stated using the Frobenius angle $\theta_p \in [0, \pi]$, which is given by $\cos\theta_p = t_p/(2\sqrt{p}) \in [-1, 1]$. The induced measure on $[-1, 1]$ is given by $\frac{2}{\pi}\sin^2\theta\, d\theta$. The corresponding statement is then, for any interval $[\alpha, \beta] \subset [0, \pi]$,

$$\lim_{X\to\infty} \frac{\#\{p \leq X \mid \theta_p \in [\alpha, \beta]\}}{\#\{p \leq X\}} = \int_\alpha^\beta \frac{2}{\pi}\sin^2\theta\, d\theta.$$

2. Here, we give the set of primes the usual ordering.

The above distribution can be looked in a more intrinsic way, as we will see in Conjecture 3.50. Fix an prime number ℓ. Consider the map

$$\begin{aligned} \mathbf{Frob}: \quad \mathrm{Spec}_m\left(\mathbb{Z}\left[\tfrac{1}{\ell N_E}\right]\right) &\longrightarrow \mathrm{Gal}(\mathbb{Q}_{E,\ell}/\mathbb{Q}) \xrightarrow{\rho_{E,\ell}} \mathrm{Aut}(T_\ell(E)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \\ (p) &\longmapsto \boldsymbol{\sigma}_w \longmapsto \boldsymbol{F}_w \end{aligned} \tag{3.3.7}$$

where N_E is the conductor of E, $\mathrm{Spec}_m(A)$ denotes the set of maximal ideals of a commutative ring A, $\mathbb{Q}_{E,\ell} = \mathbb{Q}\left(E\left[\ell^\infty\right]\right)$, $\boldsymbol{\sigma}_w$ is the Frobenius element of a choice of place w over p, and $\rho_{E,\ell}$ is the ℓ-adic representation attached to the elliptic curve $E/\mathbb{Q}$. Consequently $\boldsymbol{F}_w$ is induced from the action of $\boldsymbol{\sigma}_w$ on $E(\mathbb{Q}_{E,\ell})$. Subject to the choices of places w over primes p, the map is well-defined because $p \nmid \ell N_E$ is unramified in $\mathbb{Q}_{E,\ell}$. Different choices of w determine conjugate Frobenius elements $\boldsymbol{\sigma}_w$, and hence conjugate actions $\boldsymbol{F}_w$.

As in (3.3.7), for a prime of good reduction $p \neq \ell$ of E, we also have

$$\begin{aligned} \mathrm{Gal}\left(\kappa(w)/\mathbb{F}_p\right) \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) &\xrightarrow{\rho_{E_p,\ell}} \mathrm{Aut}(T_\ell(E_p)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \\ \sigma_p &\longmapsto F_p \end{aligned} \tag{3.3.8}$$

where $\kappa(w)$ is the residue field of w, σ_p is just the usual p-th Frobenius map on $\overline{\mathbb{F}}_p$, E_p is the reduction of E modulo p. Hence F_p is the induced action from the Frobenius endomorphism on $E_p/\mathbb{F}_p$.

We have canonical isomorphisms such that the following diagram is commutative :

$$\begin{array}{ccc} T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell & \xrightarrow{\sim} & T_\ell(E_p) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \\ {\scriptstyle \mathbf{Frob}(p)}\uparrow & & \uparrow{\scriptstyle F_p} \\ T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell & \xrightarrow{\sim} & T_\ell(E_p) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \end{array} \tag{3.3.9}$$

This means that the Frobenius actions F_p, on different spaces $\mathrm{Aut}(T_\ell(E_p))$ for different p, can be put into a common space $\mathrm{Aut}(T_\ell(E))$ by identifying F_p and $\mathbf{Frob}(p)$. We have chosen a Frobenius element w for each p, and the $\mathbf{Frob}(p)$ is determined only up to conjugacy, we come up with a conjugacy class for the lifts $\boldsymbol{F}_w$ of the geometric Frobenius F_p. The module $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2, thus $\mathrm{Aut}(T_\ell(E)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is isomorphic to $\mathrm{GL}_2(\mathbb{Q}_\ell)$, after choosing a basis. In this way, we obtain $\mathbf{Frob} : \mathrm{Spec}_m\left(\mathbb{Z}\left[\tfrac{1}{\ell N_E}\right]\right) \to \mathrm{GL}_2(\mathbb{Q}_\ell)$.

We have a space $\mathrm{GL}_2(\mathbb{Q}_\ell)$ on which the Frobenius actions are realized. But we can work with a simpler space. Remember that we choose a basis to identify $T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ with $\mathrm{GL}_2(\mathbb{Q}_\ell)$. Hence it is the conjugacy class of F_p is defined intrin-

sic. We know that the characteristic polynomial of F_p has integer coefficients and is monic. Thus F_p is conjugate to an element in $\mathrm{GL}_2(\overline{\mathbb{Q}})$. The Hasse-Weil theorem implies that the normalized Frobenius $F_p/\sqrt{p}$ is in fact conjugate to an element in $\mathrm{SU}(2)$. Hence we get a map

$$\begin{aligned} \mathbf{NFrob} : \mathrm{Spec}_m\left(\mathbb{Z}\left[\frac{1}{\ell N_E}\right]\right) &\longrightarrow \mathrm{Cl}(\mathrm{SU}(2)) \\ (p) &\longmapsto F_p/\sqrt{p} \end{aligned} \tag{3.3.10}$$

where $\mathrm{Cl}(G)$ is the set of conjugacy classes of a group G. In this way, we can view the distribution of normalized Frobenius actions $\{\mathbf{NFrob}(p)\}$ in $\mathrm{Cl}(\mathrm{SU}(2))$, which turns out to be the probability space of Frobenius distribution [3], as we will explain now.

The quotient space $X = \mathrm{Cl}(\mathrm{SU}(2))$ inherits the quotient topology from the topology of $\mathrm{SU}(2)$. We then form a Borel σ-algebra $\mathfrak{B}(X)$ on X using the quotient topology. Now we push the Haar measure of $\mathrm{SU}(2)$ forward to X and obtain a probability space (X, μ_X). Now we have a sequence $(\mathbf{NFrob}(p))$ of normalized Frobenius in X, according to the usual well-ordering of $\mathbb{N}$. Now we can state the Sato-Tate conjecture in an intrinsic way.

Conjecture 3.50 (Sato-Tate, Revised, cf. 3.49)**.** Let $E/\mathbb{Q}$ be an elliptic curve without CM. The sequence $(\mathbf{NFrob}(p)) \subset X$ of Frobenius is equidistributed with respect to the induced measure μ_X of the Haar measure of $\mathrm{SU}(2)$.

It is easy to verify the trace map $\mathrm{tr} : \mathrm{SU}(2) \to I = [-2, 2]$ induces a map on X, and it is a random variable $\mathrm{tr} : (X, \mathfrak{B}(X), \mu_X) \to (I, \mathfrak{B}(I))$. This is totally the same as in the discussion after Definition 3.45. The induced measure of tr on I is $\frac{1}{2\pi}\sqrt{4-t^2}dt$ as mentioned. From this viewpoint, Conjecture 3.49 is about the distribution of the values of the random variable tr at the sample points $\mathbf{NFrob}(p)$, for $p \in S_\ell$, which are just the normalized traces $t_p/\sqrt{p}$.

In fact, each element of $\mathrm{SU}(2)$ has determinant 1, so its trace determines the characteristic polynomial, and thus its conjugacy class. Hence the random variable $\mathrm{tr} : X \xrightarrow{\sim} [-2, 2]$ is a isomorphism of measurable spaces. With the measures μ_X on X and $\frac{1}{2\pi}\sqrt{4-t^2}dt$ on $[-2, 2]$, it is an isomorphism of probability spaces. In this way, Conjecture 3.49 and Conjecture 3.50 are equivalent statements about the (complete information of) Frobenius distribution, but the latter one gives a quantity for the computation.

The study of Frobenius distribution for elliptic curves $\mathbb{Q}$ can be generalized to elliptic curves over a number field K. In this case, we consider the limiting distribution of Frobenius for the primes $\mathfrak{p}$ of the ring of integers O_K of K with $\|\mathfrak{p}\| \leq X$ when $X \to \infty$. In 2006, Richard Taylor, building on earlier work with

3. If $E/\mathbb{Q}$ has no complex multiplication.

Laurent Clozel, Michael Harris and Nicholas Shepherd-Barron, completed the proof of the Sato-Tate conjecture :

Theorem 3.51 ([Tay08])**.** Sato-Tate conjecture is true.[4] Moreover, let $K/\mathbb{Q}$ be a totally real field and E/K be an elliptic curve. If the j-invariant of E is not in the ring of integer O_K of K, then Sato-Tate conjecture is true for E.

For elliptic curves with complex multiplication, their Frobenius distributions are given by :

Theorem 3.52 (Sato-Tate distribution : CM case)**.** For an elliptic curve $E/\mathbb{Q}$ with CM, the distribution of non-zero[5] normalized traces is equidistributed on $I = [-2, 2]$ with respect to the induced measure from $\mathrm{SO}(2)$, which is $\frac{1}{\pi\sqrt{4-t^2}}dt$. In terms of Frobenius angle $\theta_p \in [0, \pi]$, it is $\frac{1}{\pi}d\theta$. This means that θ_p is uniformly distributed in the classical sense.[6] See [Deu41b].

Definition 3.53. For E/K, its *Sato-Tate group* is a closed subgroup C of $\mathrm{SU}(2)$ such that the Frobenius distribution of E is given by the (induced) Haar measure of C. This measure is called the *Sato-Tate measure of* E.

The following table summarizes the discussion in this section.

G	G/G^0	example curve E	K	moments $M_{2n}(t)$
$\mathrm{U}(1)$	C_1	$y^2 = x^3 + x$	$\mathbb{Q}(i)$	$1, 2, 6, 20, 70, 252, 924, 3432 \cdots$
$N(\mathrm{U}(1))$	C_2	$y^2 = x^3 + x$	$\mathbb{Q}$	$1, 1, 3, 10, 35, 126, 462, 1716 \cdots$
$\mathrm{SU}(2)$	C_1	$y^2 = x^3 + x + 1$	$\mathbb{Q}$	$1, 1, 2, 5, 14, 42, 132, 429 \cdots$

Table 3.2 – Sato-Tate groups for elliptic curves

The moment sequence determines each of these distributions. Here is a comparison of the expected moments and the moments computed with a data of 2^{10} sample points for the elliptic curve $E/\mathbb{Q} : y^2 = x^3 + x + 1$, whose Sato-Tate group is $\mathrm{SU}(2)$.

n	1	2	3	4	5	6	7
M_{2n}	1	2	5	14	42	132	429
Sample Moments	0.991	2.009	5.084	14.39	43.67	139.1	458.9

Table 3.3 – Sequence of sample moments for $E : y^2 = x^3 + x + 1$

4. The case for integral j-invariant is proved in 2011, see [Bar+11].
5. For a CM elliptic curve over $\mathbb{Q}$, half of the primes are supersingular. Its Frobenius distribution is given by $N(\mathrm{SO}(2))$. If we consider its extension E_K/K to a field containing the CM field of E, then the Frobenius distribution of E_K/K is given by $\mathrm{SO}(2)$.
6. See Definition 3.31.

One characteristic of moments is that they grow very quickly. Starting from $n = 4$, the sample moments computed from this data don't match the expected values. Their differences become large quickly also. These situations become more and more serious for higher dimensional abelian varieties. In Section 3.5, we will propose a new approach to avoid this problem.

3.4 Generalized Sato-Tate conjecture

For a curve $C/\mathbb{F}_q$ of genus g, its characteristic polynomial of Frobenius $P(x)$, called the Weil polynomial, is an integer polynomial of degree $2g$

$$P(x) = x^{2g} + a_1 x^{2g-1} + \cdots + a_{2g-1}x + q^g \,.$$

All of its roots have absolute value $\sqrt{q}$. Write $P(x) = \prod_{i=1}^{2g}(x - \alpha_i)(x - \bar{\alpha_i})$. The normalized Weil polynomial is

$$P(\sqrt{q}x)/q^g = \prod_{i_1}^{g}(x^2 - t_i x + 1), \text{ where } t_i = \frac{\alpha_i + \bar{\alpha}_i}{\sqrt{q}} \,.$$

We also consider the normalized real Weil polynomial

$$\prod_{i=1}^{g}(x - t_i) = x^g - s_1 x^{g-1} + \cdots + (-1)^g s_g \,.$$

For $g = 2$, we have $s_1 = -a_1/\sqrt{q}$ and $s_2 = a_2/q - 2$.

For a curve $C/\mathbb{Q}$ of genus g and a prime p, one can consider the Frobenius action F_p on the Tate-module $T_\ell(\mathrm{Jac}(C_p))$. Its normalized Weil polynomial is a characteristic polynomial of an element in the unitary symplectic group $\mathrm{USp}(2g)$ [7], hence the (matrix of the) normalized action $F_p/\sqrt{p}$ is conjugate to an element in $\mathrm{USp}(2g)$. We are interested in the distribution of $F_p/\sqrt{p}$, which is the same as the study of the distribution of normalized (real) Weil polynomials.

In [KS99], the random matrix model of Katz-Sarnak predicts that, in general, the distribution of normalized Frobenius should match the distribution of the characteristic polynomial of a random element in a compact subgroup G of $\mathrm{USp}(2g)$. This is true on average in certain families.

In general, Serre proposed a candidate for the subgroup G of $\mathrm{USp}(2g)$. This is called the *"Sato-Tate group"* of C.

Conjecture 3.54 (Generalized Sato-Tate Conjecture)**.** Let $G \subseteq \mathrm{USp}(2g)$ be the Sato-Tate group of C. The distribution of normalized Weil polynomials is determined by the Haar measure of G.

In 2012, Fité, Kedlaya, Rotger and Sutherland proved

7. See Example 4.3 for the definition.

Theorem 3.55 (FKRS, [Fit+12])**.** Up to conjugacy, there are exactly 52 subgroups of $\mathrm{USp}(4)$ that are Sato-Tate groups of genus 2 curves. Among them, 34 Sato-Tate groups can be obtained from curves defined over $\mathbb{Q}$.

They give explicitly these Sato-Tate groups. For each group G, they give a genus 2 curve that has G as its Sato-Tate group. For each example, they compared, using the moments of the coefficients of the characteristic polynomial, the distribution of Frobenius with the expected distribution predicted by the generalized Sato-Tate conjecture, and found that they agree very closely. We list only a few of them here.

G	G/G^0	example curve E	K
$\mathrm{SO}(2)^2$	C_1	$y^2 = x^6 + 3x^4 + x^2 - 1$	$\mathbb{Q}(i, \sqrt{2})$
$\mathrm{SU}(2)^2$	C_1	$y^2 = x^6 + x^2 + 1$	$\mathbb{Q}$
$N(\mathrm{SU}(2)^2)$	C_2	$y^2 = x^6 + x^5 + x - 1$	$\mathbb{Q}$
$\mathrm{USp}(4)$	C_1	$y^2 = x^5 - x + 1$	$\mathbb{Q}$

Table 3.4 – Some Sato-Tate Groups for $g = 2$

3.5 Characters and Sato-Tate groups

In Section 3.3, we have seen the usage of moments (moment sequences) to the study of Sato-Tate groups of elliptic curves. This is a classical tool in probability theory to understand different probability distributions. In the study of Sato-Tate groups, the distributions we are interested in are the distributions of (normalized) Frobenius for curves with different structure. This method is used in the work [Fit+12].

In this section, we look again the Sato-Tate groups of elliptic curves again, but from a different viewpoint. Instead of moments, we use irreducible characters of Lie groups to distinguish the 3 distributions of Frobenius for elliptic curves.

3.5.1 Irreducible characters of $\mathrm{SU}(2)$

The irreducible characters[8] (representations) of $\mathrm{SU}(2)$ are indexed by non-negative integers : $\chi_0 = 1$, $\chi_1 = t$, $\chi_2 = t^2 - 1$, $\chi_3 = t^3 - 2t$, which satisfy a recurrence formula

$$\chi_n = t \cdot \chi_{n-1} - \chi_{n-2}\,. \tag{3.5.1}$$

They are related to the Chebyshev polynomials of the second kind $U_n(x)$ by

$$\chi_n(t) = U_n(t/2)\,,\ n \geq 1\,.$$

8. See Definition 4.9 for the definition of (irreducible) characters.

The argument t here is the trace of elements in $\mathrm{SU}(2)$. Since characters on a Lie group are class functions, they are determined by the conjugacy classes. As we see in page 53, the conjugacy class of an element of $\mathrm{SU}(2)$ is determined by its trace, we can express the characters χ_n in t.[9]

The restriction of an irreducible character of a compact Lie group G to a closed subgroup H is not irreducible in general. A law of decomposition of irreducible characters, when they are restricted to a subgroup, is called a branching rule.

In Section 3.3, we regard the trace map $\mathrm{tr} : \mathrm{SU}(2) \to I = [-2, 2]$ as a random variable, and we study its moment sequence. Now instead tr, we look the irreducible characters χ_n of $\mathrm{SU}(2)$, and their restrictions on the subgroups $\mathrm{SO}(2)$ and $N(\mathrm{SO}(2))$. For any closed subgroup G of $\mathrm{SU}(2)$, each character $\chi_n|_G \colon G \to \mathbb{C}$ can be regarded as a random variable on G. We can compute their moment sequences and use them to distinguish the 3 distributions of Frobenius.

But the actual advantages of using irreducible characters to the study of Sato-Tate groups is to use the inner products of irreducible characters (which are either 0 or 1), and the inner products of the restrictions of them on Lie subgroups, which turn out to be small integers. For example, the inner product of χ_m and χ_n, with respect to the Haar measure μ_G on the compact Lie group $G = \mathrm{SU}(2)$, is given by

$$\langle \chi_m, \chi_n \rangle_G = \int_G \chi_m \chi_n \, d\mu_G = \int_{-2}^{2} \chi_m(t)\chi_n(t) \frac{\sqrt{4-t^2}}{2\pi} \, dt \,. \tag{3.5.2}$$

Reall the definition of expection of a random variable ξ in (3.2.4) :

$$E[\xi] = \int_{x \in X} \xi(x) d\mu \,.$$

Take the random variable ξ to be $\chi_m\chi_n$ on the space $X = G = \mathrm{SU}(2)$, it is clear from (3.5.2) that the inner product $\langle \chi_m, \chi_n \rangle_G$ is the expectation of $\xi = \chi_m\chi_n$, which is also the first moment (by definition) of $\chi_m\chi_n$. Thus the usage of irreducible characters is a natural generalization of moments (moment sequence). It is a well-known theorem that irreducible characters are orthonormal to each other, see Theorem 4.10. This provides us the expected values of the random variable $\chi_m\chi_n$:

$$E[\chi_m\chi_n] = \langle \chi_m, \chi_n \rangle_G = \delta_{m,n} = \begin{cases} 1 & \text{if } m = n, \\ 0 & \text{if } m \neq n. \end{cases}$$

For a Lie subgroup H, say $H = \mathrm{SO}(2)$, of $G = \mathrm{SU}(2)$, the restriction of the irreducible characters χ_m and χ_n of G to this subgroup H are no longer irreducible characters of H. This fact is the foundation of our new approach using characters to the study of Sato-Tate groups :

9. If we express χ_n in terms of functions on $\mathrm{SU}(2)$, we have $\chi_1 = \mathrm{tr}$, $\chi_2 = \mathrm{tr}^2 - 1$, $\chi_3 = \mathrm{tr}^3 - 2\,\mathrm{tr}$, etc.

1. Compute sample points of Frobenius.
2. Choose a set of irreducible characters $\{\chi_n\}$ of the generic group, e.g. $\mathrm{SU}(2)$ or $\mathrm{USp}(2g)$.
3. Compute the inner products of these irreducible characters χ_n using the sample points.
4. Compare the values with the expected values. This will indicate the Sato-Tate distribution of Frobenius.

The work behind this general strategy is to find the possible candidate Sato-Tate groups, and then compute the inner products of χ_n, irreducible characters of $\mathrm{USp}(2g)$, on these groups. The computation of such inner products is closely related to the branching rule, i.e. how an irreducible character is decomposed when it is restricted to a Lie subgroup.

The next subsection demonstrates these ideas with examples.

3.5.2 Examples

For $G = \mathrm{SU}(2)$ and $H = \mathrm{SO}(2)$, we have

$$\chi_n|_H = \sum_{k\in\mathbb{Z},\, n-2k\geq 0} \left(\lambda_{n-2k} + \lambda_{-(n-2k)}\right) ,$$

where the irreducible character λ_j on $\mathrm{SO}(2)$ is

$$\lambda_j : \mathrm{SO}(2) \to \mathbb{C}^\times,\ e^{i\theta} \to e^{ij\theta} .$$

Using this branching rule, we obtain the inner products on $\mathrm{SO}(2)$ and $N(\mathrm{SO}(2))$ of the (restriction of the) irreducible characters χ_n of $\mathrm{SU}(2)$. For example, for $H = \mathrm{SO}(2)$, $m = 2$ and $n = 4$, $\chi_2|_H = \lambda_2 + \lambda_0 + \lambda_{-2}$ and $\chi_4|_H = \lambda_4 + \lambda_2 + \lambda_0 + \lambda_{-2} + \lambda_{-4}$. Each of these λ_i is an irreducible character on H, hence they are orthonormal to each other (with respect to the Haar measure on H). It is then easy to compute the inner product $\langle \chi_2, \chi_4 \rangle_H$:

$$\begin{aligned}\langle \chi_2, \chi_4 \rangle_H &= \langle \lambda_2 + \lambda_0 + \lambda_{-2}, \lambda_4 + \lambda_2 + \lambda_0 + \lambda_{-2} + \lambda_{-4} \rangle \\ &= \langle \lambda_2, \lambda_2 \rangle + \langle \lambda_0, \lambda_0 \rangle + \langle \lambda_{-2}, \lambda_{-2} \rangle \\ &= 3.\end{aligned}$$

The left side of Table 3.7 gives the inner products of χ_n on the three Sato-Tate groups for elliptic curves. The value of (i, j) entry is the inner product $\langle \chi_{i-1}, \chi_{j-1} \rangle$ for $i, j \geq 1$.

Instead using the moments of the trace, one can use these invariants to identify the Sato-Tate group of an elliptic curve E. Here is a comparison of the inner products of irreducible characters of $\mathrm{SU}(2)$ on the three groups and the values

obtained from datas of 2^{10} sample points for each example in Section 3.1.

1	0	0	0	0
0	1	0	0	0
0	0	1	0	0
0	0	0	1	0
0	0	0	0	1

$\mathrm{SU}(2)$

1.00	0.03	0.00	0.02	0.03
0.03	0.99	0.05	0.02	0.03
0.00	0.05	1.02	0.07	0.01
0.02	0.02	0.07	1.01	0.14
0.03	0.03	0.01	0.14	1.04

$\mathrm{SU}(2)$

1	0	0	0	1
0	1	0	1	0
0	0	2	0	1
0	1	0	2	0
1	0	1	0	3

$N(\mathrm{SO}(2))$

1.00	0.01	0.02	0.01	0.96
0.01	0.97	0.03	0.94	0.05
0.02	0.03	1.94	0.07	0.90
0.01	0.94	0.07	1.90	0.11
0.96	0.05	0.90	0.11	2.84

$N(\mathrm{SO}(2))$

1	0	1	0	1
0	2	0	2	0
1	0	3	0	3
0	2	0	4	0
1	0	3	0	5

$\mathrm{SO}(2)$

1.00	0.01	0.99	0.00	0.98
0.01	1.99	0.00	1.97	0.00
0.99	0.00	2.97	0.00	2.93
0.00	1.97	0.00	3.93	0.02
0.98	0.00	2.93	0.02	4.86

$\mathrm{SO}(2)$

Table 3.7 – Inner products of χ_n on Sato-Tate groups for elliptic curves

This example shows that, even we use very few sample points (2^{10}), the numerical values of these inner products match the expected values very well, unlike the poor convergence of moments in Table 3.3. This justify the advantage this new approach using characters to the study of Sato-Tate groups.

Our goal is to generalize the above ideas to higher genus : A recurrence formula for irreducible characters similar to the usual Chebyshev polynomials, and the usage of these characters to the study of Sato-Tate groups.

Chapitre 4

Brauer-Klimyk Formula and Computation of Characters

In Chapter 3, we introduce the idea of using irreducible characters to study Sato-Tate groups, which is a natural generalization of moments (moment sequences) and has advantages over using moments (Section 3.5.1).

A natural question is how one can compute the irreducible characters. For our purposes of studying Sato-Tate groups, we work mostly with the unitary symplectic group $\mathrm{USp}(2g)$ and some closed subgroups of it. In this chapter, we present some ways to the computation of irreducible characters. Section 4.1 and Section 4.3 provide a basic introduction to the theory of compact Lie groups and their characters. In Section 4.2, we present a direct way to compute the irreducible characters. Using the Brauer-Klimyk formula (Theorem 4.35) in Section 4.3, we give a recursive algorithm to compute the irreducible characters in Section 4.6. In Section 4.7, we use these irreducible characters to study the Sato-Tate groups, and show the advantage of this new method over using moment sequences.

4.1 Compact Lie groups

Definition 4.1. A *Lie group* is a differentiable manifold G with a smooth map $G \times G \to G$ which makes G into a group such that the inverse map $\mathrm{inv} : G \to G,\ g \to g^{-1}$ is also a smooth map.

Example 4.2. The *general linear group* $\mathrm{GL}_n(F)$ of degree n over a field F is the set of $n \times n$ invertible matrices whose entries is in F. The matrix multiplication as group operation makes $\mathrm{GL}_n(F)$ a group. When F is the field $\mathbb{R}$ or $\mathbb{C}$, it is easy to verify $\mathrm{GL}_n(F)$ is a Lie group.

The Lie groups $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$ are not compact. There are many (and classical) compact Lie groups. For our purpose, we give the following example.

Example 4.3. The *unitary group* is $\mathrm{U}(n) = \{g \in \mathrm{GL}_n(\mathbb{C}) \,|\, g \cdot \overline{g^t} = I_n\}$. The *symplectic group* $\mathrm{Sp}(2n, F)$, $F = \mathbb{R}$ or $\mathbb{C}$, is

$$\mathrm{Sp}(2n, F) = \{g \in \mathrm{GL}_n(2n, F) \,|\, g \cdot J \cdot g^t = J\}, J = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}. \tag{4.1.1}$$

The *unitary symplectic group* is $\mathrm{USp}(2n) = \mathrm{Sp}(2n, \mathbb{C}) \cap \mathrm{U}(2n)$, which is also denoted by $\mathrm{Sp}(n)$. It is compact and simply connected.

Remark 4.4. From now on, the letter g is mainly used to indicate the genus of an algebraic curve, e.g. a genus g curve or the "rank" of a Lie group, e.g. $\mathrm{USp}(2g) = \mathrm{Sp}(g)$. In some case, we will use the letter g to mean an element in a group, e.g. $g \in G$, which may cause confusion, but the meaning is still clear from the context.

Definition 4.5. A *compact torus* is a compact connected Lie group that is Abelian. The simplest case is the circle group $\mathbb{T} = \{z \in \mathbb{C} \,|\, |z| = 1\}$.

Every compact connected Lie group G contains a torus. By considering the dimension, there is a maximal torus, but not unique.

Example 4.6. For the unitary symplectic group $\mathrm{USp}(2g)$, a maximal T torus is given by matrices of the form

$$\begin{pmatrix} e^{i\theta_1} & & & & & & \\ & \ddots & & & & & \\ & & e^{i\theta_g} & & & & \\ & & & e^{-i\theta_1} & & & \\ & & & & \ddots & & \\ & & & & & e^{-i\theta_g} & \end{pmatrix}.$$

For a compact Lie group G, there is a unique (regular Borel) measure μ on G which is invariant under left and right translation, i.e. $\mu(g \cdot X) = \mu(X \cdot g) = \mu(X)$ for all measurable sets X, such that $\mu(G) = 1$. This is called the *Haar measure* of G.

The existence of Haar measure on a compact Lie group is one thing, but to "see" what it is (or compute it) is another. Before discussing it further, we turn to another important part of the theory of Lie groups, which will demonstrate the motivation for an explicit knowledge of the Haar measure.

Definition 4.7. Let G be a compact Lie group. The Hilbert space $L^2(G)$ is the space of functions on G that are square-integrable with respect to the Haar measure μ_G of G, whose inner product is given by

$$\langle f_1, f_2 \rangle_G = \int_G f_1(g) \overline{f_2(g)} \, d\mu_G(g).$$

The inner product defined in (3.5.2) is a special case of the general definition Definition 4.7 with $G = \mathrm{USp}(2) = \mathrm{SU}(2)$. We use a fact that the Haar measure, when one changes from the space G to the space $I = [-2, 2]$ via the trace map $\mathrm{tr} : G \to I$, is given by $\frac{1}{2\pi}\sqrt{4 - t^2}\, dt$. For our new approach to the study of Sato-Tate groups, we need to compute inner products of characters, as demonstrated in Section 3.5.2. In general, we have to know how to integrate a *class function* [1] on a compact Lie group with respect to its Haar measure. The following proposition is a consequence of the *Weyl integration formula*.

Proposition 4.8. Let $G = \mathrm{USp}(2g)$ and μ_G be its Haar measure. Let T be its maximal torus given in Example 4.6 and $t_k = e^{i\theta_k} + e^{-i\theta_k} \in I = [-2, 2]$, for $k = 1, \ldots, g$. Let $t = (t_1, \ldots, t_g) \in I^g$ and $dt = dt_1 dt_2 \ldots dt_g$ be the usual measure on it. For a class function f, we have

$$\int_{x \in G} f(x)\, d\mu_G(x) = \int_{I^g} f(t) \frac{1}{g!} \prod_{i=1}^{g} \frac{\sqrt{4 - t_i^2}}{2\pi} \left(\prod_{j<k} (t_j - t_k) \right)^2 dt_1 dt_2 \ldots dt_g\,. \quad (4.1.2)$$

Proposition (4.1.2) gives us a way to compute integrals of class functions on $\mathrm{USp}(2g)$. Examples are the trace function $\mathrm{tr} : \mathrm{USp}(2g) \to \mathbb{C}, x \to \mathrm{tr}(x)$, and the power tr^n of the trace map. This is used in the approach using moment sequence to study Sato-Tate groups. But there are far more class functions than tr and its powers : we have characters of representations of a Lie group.

Definition 4.9. A *representation* of a Lie group G is a continuous homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is a finite dimensional (complex) vector space. The *character* χ_ρ of a representation ρ is the function $\chi_\rho : G \to \mathbb{C},\ g \to \mathrm{tr}(\rho(g))$. A representation (ρ, V) is called *irreducible* if V has no proper nonzero invariant subspaces. A character χ is called *irreducible* if $\chi = \chi_\rho$ for an irreducible representation ρ.

We have the following important theorem :

Theorem 4.10 (Schur orthogonality)**.** Let G be a compact Lie group and χ_1, χ_2 be 2 irreducible characters of G. Then

$$\langle \chi_1, \chi_2 \rangle_G := \int_G \chi_1(g)\overline{\chi_2(g)}\, d\mu_G(g) = \begin{cases} 1 & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise.} \end{cases} \quad (4.1.3)$$

4.2 A first approach to computation of characters

In this section, we present a way to obtain a sequence of characters of irreducible representations of the compact Lie group $\mathrm{USp}(2g)$.

1. A function on a group G which is invariant under the conjugation map on G is called a *class function*.

Recall that our focus is on the coefficients s_i of the normalized real Weil polynomial defined in Section 3.4, and they can be regarded as a class function on the Lie group $\mathrm{USp}(2g)$. The computations with class functions can be done in the quotient of $\mathrm{USp}(2g)$ by conjugacy. Now each element A in $\mathrm{USp}(2g)$ is conjugate to a $2g \times 2g$ diagonal matrix of the following form

$$\begin{pmatrix} e^{i\theta_1} & & & & & \\ & e^{-i\theta_1} & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & e^{i\theta_g} & \\ & & & & & e^{-i\theta_g} \end{pmatrix}.$$

Taking $t_k = e^{i\theta_k} + e^{-i\theta_k} = 2\cos\theta_k \in [-2, 2]$, our work will be presented on the space $t = (t_1, \cdots, t_g) \in [-2, 2]^g$. Our computation is based on the Weyl integration formula, which is a restatement of Proposition 4.8 :

Corollary 4.11. The induced measure on $[-2, 2]^g$ of the Haar measure on $\mathrm{USp}(2g)$ is given by

$$\mu_g(t_1, \cdots, t_g) = \frac{1}{(2\pi)^g g!} \prod_{i=1}^{g} \sqrt{4 - t_i^2} \left(\prod_{j<k} (t_j - t_k) \right)^2 dt_1\, dt_2 \cdots dt_g\,.$$

Using Corollary 4.11, one can compute the inner product of two class functions on $\mathrm{USp}(2g)$: Let f_1 and f_2 be 2 class functions on $\mathrm{USp}(2g)$, then their inner product is given by

$$\int_{-2}^{2} \cdots \int_{-2}^{2} f_1 f_2 \prod_{i=1}^{g} \left(\frac{1}{2\pi} \sqrt{4 - t_i^2} \right) \left(\prod_{j<k} (t_j - t_k) \right)^2 dt_1\, dt_2 \cdots dt_g\,, \tag{4.2.1}$$

with f_1 and f_2 as functions on the space $(t_1, \cdots, t_g) \in [-2, 2]^g$.

The $\left(\prod_{j<k}(t_j - t_k)\right)^2$ part in the above integration is not separable, but it is a combination of monomials $\prod_i t_i^{m_i}$. The functions that we will compute the integral with respect to μ_g are also polynmoials in these t_i's (in fact, in s_i's). If we know about the value of

$$\int_{-2}^{2} \cdots \int_{-2}^{2} \prod_{i=1}^{g} \left(\frac{1}{2\pi} t_i^{n_i} \sqrt{4 - t_i^2} \right) dt_1\, dt_2 \cdots dt_g\,,$$

we are able to compute the integrals of class functions. Now the above integral is separable : using Proposition 4.12 below (which is just the case of $g = 1$) for each variable t_i will give the result. We state it as a proposition.

Proposition 4.12. For non-negative integer n, let a_n be $\frac{1}{2\pi}\int_{-2}^{2} t^n\sqrt{4-t^2}\,dt$. Then $a_n = 0$ if n is odd, and $a_{2n} = \binom{2n}{n}/(n+1)$.

Proposition 4.13. Let a_n be defined as above. We have

$$\int_{-2}^{2}\cdots\int_{-2}^{2}\prod_{i=1}^{g}\left(\frac{1}{2\pi}t_i^{n_i}\sqrt{4-t_i^2}\right)dt_1\,dt_2\cdots dt_g = a_{n_1}a_{n_2}\cdots a_{n_g}\,.$$

Example 4.14 ($g=1$)**.** Using (4.2.1) and Proposition 4.13, one can compute a sequence of orthogonal polynomials

$$\begin{aligned}
\chi_0 &= 1\\
\chi_1 &= t\\
\chi_2 &= t^2-1\\
\chi_3 &= t^3-2t\\
\chi_4 &= t^4-3t^2+1\\
\chi_5 &= t^5-4t^3+3t\\
\chi_6 &= t^6-5t^4+6t^2-1\\
&\vdots
\end{aligned}$$

We have recurrence relation : $\chi_n = t\cdot\chi_{n-1}-\chi_{n-2}$. All of these χ_n have length 1 (with respect to the inner product in (4.2.1)).

One way to obtain the sequence of polynomials in Example 4.14 is to start with t^n for χ_n, then apply the Gram-Schmidt process. But there is another way to obtain it, and which turns out to be more efficient : We start with $t\cdot\chi_{n-1}$ then apply the Gram-Schmidt process. In $g=1$ case, this may seem to have no difference, but it is crucial when one works on $g\geq 2$ cases.

The function $\chi_1 = t$ in the above example is in fact the character (the trace) of the natural representation of the Lie group $\mathrm{USp}(1)=\mathrm{SU}(2)$:

$$\begin{aligned}
t : \mathrm{SU}(2) &\longrightarrow \mathbb{C}\\
A=\begin{pmatrix}\alpha & \overline{\beta}\\ \beta & \overline{\alpha}\end{pmatrix} &\longrightarrow \mathrm{trace}(A)\,.
\end{aligned}$$

From the description, in the above paragraph, of the way in which this sequence is obtained, these functions are the characters of the irreducible representations of $\mathrm{SU}(2)$. The recurrence relation $\chi_n = t\cdot\chi_{n-1}-\chi_{n-2}$ means that the corresponding irreducible representations ρ_n have relations : $\rho_1\otimes\rho_{n-1} = \rho_{n-2}\bigoplus\rho_n$.

Now I am going to present a systematic way to construct the irreducible characters of the (representations of) Lie groups $\mathrm{USp}(2g)$.

Algorithm 4.15. The input are positive integers g and d. The output is a sequence of polynomials $\chi_{\mathbf{m}}$ in the variables $s_1, \cdots, s_g$, where the index $\mathbf{m} = (m_1, \cdots, m_g) \in \mathbb{N}_{\geq 0}^g$, such that $\chi_{\mathbf{m}}$ are the characters of the irreducible representations of highest weight [2] [3] $\mathbf{m}$ of the Lie group $\mathrm{USp}(2g)$, with $\sum_{i=1}^g m_i \leq d$.

Step 1. Set $\chi_{\mathbf{0}} = 1$, here $\mathbf{0} = (0, \cdots, 0)$. Set $I = \{\mathbf{0}\}$. Set $i = 1$ and $\tilde{d} = 1$.

Step 2. If $i \leq g$, set $\chi_{e_i} = s_i$, here e_i is the element $(\cdots, 0, 1, 0, \cdots)$ with the only non-zero element 1 appearing at the i-th position. Then apply the Gram-Schmidt process to obtain a polynomial which is orthogonal to $\chi_{\mathbf{0}}$ and to all of the χ_{e_j} with $j < i$, and having length 1. Set this new polynomial to χ_{e_i}. Append e_i to I. Set i to $i + 1$ and run this step again.

Step 3. Set $S_{\tilde{d}}$ to be the set of solutions $(m_1, \cdots, m_g) \in \mathbb{N}_{\geq 0}^g$ of $\sum_{i=1}^g m_i = \tilde{d}$. Sort the set $S_{\tilde{d}}$ using the reverse order of the usual lexicographical order.

Step 4. Set $\mathbf{m} = (m_1, \cdots, m_g)$ to be the first element in $S_{\tilde{d}}$, and set $i = 1$.

Step 5. If $i \leq g$ and $\mathbf{m} + e_i \notin I$, set $\chi = \chi_{e_i} \cdot \chi_{\mathbf{m}}$. Apply the Gram-Schmidt process to obtain a polynomial which is orthogonal to all of the polynomials $\chi_{\mathbf{n}}$ with $\mathbf{n} \in I$ and having length 1. Set this new polynomial to $\chi_{\mathbf{m}+e_i}$. Append $\mathbf{m}+e_i$ to I. Set i to $i + 1$ and run this step again.

Step 6. If $\mathbf{m}$ is not the last element in $S_{\tilde{d}}$, set $\mathbf{m}$ be the next element in $S_{\tilde{d}}$ after (the current value of) $\mathbf{m}$, set $i = 1$ and run Step 5 again.

Step 7. Set $\tilde{d} = \tilde{d}+1$. If $\tilde{d} \leq d$, go to Step 3. Otherwsie terminate the algorithm.

Remark 4.16. We don't give a complexity analysis here. However, in Step 5 of Algorithm 4.15, we start with $\chi = \chi_{e_i} \cdot \chi_{\mathbf{m}}$, then each step in the Gram-Schmidt process computes the inner products of χ with one of the previously computed irreducible characters $\chi_{\mathbf{n}}$, $\mathbf{n} \in I$, and updates the value of χ. This process is done for each $\mathbf{n} \in I$. If $\mathbf{n}$ is orthogonal to χ, then it won't change the value χ. Hence the computations of $\langle \chi, \chi_{\mathbf{n}} \rangle$ in such steps waste the time.

On the other hand, Algorithm 1, which we will present later, is based on the Brauer-Klimyk formula (Theorem 4.35). Essentially, it determines which irreducible characters $\chi_{\mathbf{n}}$ is in the decomposition of $\chi_{e_i} \cdot \chi_{\mathbf{m}}$: They are related to the weights of χ_{e_i}. Thus Algorithm 1 is faster than Algorithm 4.15.

Using Algorithm 4.15, one can compute all the irreducible characters of $\mathrm{USp}(2g)$ up to any degree. Here are the first few irreducible characters for $g = 2$ and $g = 3$.

2. See Definition 4.20 for the definition of weight, and Proposition 4.33, Theorem 4.34 together with the partial order defined before them for the meaning of highest weight.

3. The correctness of Algorithm 4.15, in particular about the claim of highest weight, will be apparent after a further study of the character theory of $\mathrm{USp}(2g)$ in the following sections.

Example 4.17 ($g = 2$, $\mathrm{USp}(4)$)**.** We have

$$\begin{aligned}
\chi_{(0,0)} &= 1 \\
\chi_{(1,0)} &= s_1 \\
\chi_{(0,1)} &= s_2 + 1 \\
\chi_{(2,0)} &= s_1^2 - s_2 - 2 \\
\chi_{(1,1)} &= s_1 s_2 \\
\chi_{(0,2)} &= s_2^2 - s_1^2 + 3s_2 + 2 \\
\chi_{(3,0)} &= s_1^3 - 2s_1 s_2 - 3s_1 \\
\chi_{(2,1)} &= s_1^2 s_2 - s_2^2 - 3s_2 - 1 \\
\chi_{(1,2)} &= s_1 s_2^2 - s_1^3 + 2s_1 s_2 + 2s_1 \\
\chi_{(0,3)} &= s_2^3 - 2s_1^2 s_2 + 5s_2^2 - s_1^2 + 7s_2 + 2
\end{aligned}$$

Example 4.18 ($g = 3$, $\mathrm{USp}(6)$)**.** We have

$$\begin{aligned}
\chi_{(0,0,0)} &= 1 \\
\chi_{(1,0,0)} &= s_1 \\
\chi_{(0,1,0)} &= s_2 + 2 \\
\chi_{(0,0,1)} &= s_3 + s_1 \\
\chi_{(2,0,0)} &= s_1^2 - s_2 - 3 \\
\chi_{(1,1,0)} &= s_1 s_2 - s_3 \\
\chi_{(1,0,1)} &= s_1 s_3 + s_1^2 - s_2 - 2 \\
\chi_{(0,2,0)} &= s_2^2 - s_1 s_3 - 2s_1^2 + 5s_2 + 6 \\
\chi_{(0,1,1)} &= s_2 s_3 + s_1 + 3s_3 \\
\chi_{(0,0,2)} &= s_3^2 + 3s_1 s_3 - s_2^2 + 2s_1^2 - 4s_2 - 4
\end{aligned}$$

4.3 Character theory and Brauer-Klimyk formula

In Section 4.2, we present a direct and simple way to compute irreducible characters of the compact Lie group $\mathrm{USp}(2g)$. The idea is to apply the Gram-Schmidt process on a sequence of characters of $\mathrm{USp}(2g)$. We explain how to compute the inner products after Corollary 4.11. Although it is simple and works well for the first few irreducible characters and for small g (e.g. $g \leq 6$), it is not practical if one wants to go further.

It is always a non-trivial result in mathematics, a simple idea or a difficult theorem, to make the magic. It turns out that there is a much faster way to compute the irreducible characters of $\mathrm{USp}(2g)$, and other compact Lie groups as well. The tool is Brauer-Klimyk formula, which might be seem as a recurrence

relation that generalizes (3.5.1).

In this section, we present Brauer-Klimyk formula and the basic background to state it. The main reference for this section is [Bum13].

Definition 4.19. Let G be a compact connected Lie group. The *(virtual) character ring* $R(G)$ of G is the free abelian group generated by irreducible characters of complex representations of G. The ring structure comes from the direct sum and tensor product of representations of G. It contains all characters of G.

Every element of $R(G)$ is of the form

$$\sum_{\chi} n_\chi \chi,\ n_\chi \in \mathbb{Z}, \tag{4.3.1}$$

where χ are irreducible characters of G and $n_\chi = 0$ for all but finitely many χ.

Let G be a compact, connected Lie group and T be a maximal torus. A linear character λ of T is a continuous homomorphism $\lambda : T \to \mathbb{C}^\times$, which are just the characters of irreducible representations of T (since T is compact Abelian, all irreducible representations are of degree 1). In fact, such characters takes values in the Lie group $\mathbb{T}$ of complex numbers of absolute value 1. The group of linear characters of T is denoted by $X^*(T)$. It is a commutative group and we write its group operation additively. It forms a lattice and we also denote it by Λ.

Definition 4.20. The elements of Λ are called *weights*, and Λ is called the *weight lattice*.

We discuss virtual character ring $R(G)$ and give the form of its generic element in (4.3.1). In the case of $G = T$, we prefer to use the notation of weights to describe the ring $R(T)$. Hence an element in $R(T)$ is of the form

$$\sum_{\lambda} n_\lambda e^\lambda,\ n_\lambda \in \mathbb{Z}, \tag{4.3.2}$$

where $\lambda \in \Lambda$ are weights $n_\lambda = 0$ for all but finitely many λ. We have an embedding of Λ into $R(T)$ given by $\lambda \mapsto e^\lambda$. The symbol e^λ is just a notation of the image of λ under this embedding, and should not be confused with the exponential map. The multiplication in $R(T)$ is then written as

$$\left(\sum_{\lambda} m_\lambda e^\lambda\right)\left(\sum_{\mu} n_\mu e^\mu\right) = \sum_{\nu}\left(\sum_{\lambda+\mu=\nu} m_\lambda n_\mu\right) e^\nu. \tag{4.3.3}$$

Definition 4.21. Let $\pi : G \to \mathrm{GL}(V)$ be a complex representation. We can restrict π to T, which is a representation $\pi|_T = \pi \circ i : T \to V$ of T. It decomposes into one-dimensional (hence irreducible) characters, i.e. elements in Λ. These will be called *weights of the representation* π. In other words, a weight of π is just an eigenfunction of a simultaneous eigenvector of the linear maps $\{\pi(v)\}_{v\in T}$.

The *multiplicity* $m_\lambda = m(\lambda)$ *of a weight* $\lambda \in \Lambda$ *in* π is the multiplicity of this eigenfunction, if λ is the weight of π. Otherwise, we define $m(\lambda) = 0$. Notice that the restriction $\chi|_T$ (to T) of the character $\chi : G \to \mathbb{C}$ of the representation π is the "sum of the weights of π (with multiplicities)". When $\chi|_T$ is regarded as an element in $R(T)$, we have $\chi|_T = \sum_{\lambda\,:\,\text{weight of }\pi} m_\lambda e^\lambda$, using the notation in (4.3.2). This gives a ring homomorphism $R(G) \to R(T)$. We also call m_λ the *multiplicity of the weight* $\lambda \in \Lambda$ *in* χ.

Given a Lie group G, its *Lie algebra* $\mathfrak{g}$ is its tangent space $T_e(G)$ at the point $e \coloneqq \mathrm{id}_G$. The distinction between the notion of the Lie algebra $\mathfrak{g}$ and the tangent space $T_e(G)$ is that $\mathfrak{g}$ admits a special bilinear map called *Lie bracket* which have to be considered as part of the Lie algebra $\mathfrak{g}$. We don't need the abstract definition of Lie bracket of the Lie algebra of G for our exhibition here. For $F = \mathbb{R}$ or $\mathbb{C}$ and $G = \mathrm{GL}(n, F)$, its Lie algebra $\mathfrak{gl}(n, F)$ is the ring $M_n(F)$ of $n \times n$ matrices, with the Lie bracket defined by $[X, Y] = XY - YX$ for $X, Y \in M_n(F)$. When G is a matrix Lie group, its Lie algebra $\mathfrak{g}$ is a subspace of $\mathfrak{gl}(n, F)$ with Lie bracket inherited from $\mathfrak{gl}(n, F)$.

Given $g \in G$, we have an *inner automorphism of* G which is $\mathrm{Inn}_g : G \to G, h \mapsto ghg^{-1}$. It is a smooth map of smooth manifolds, hence it induces an (invertible) linear map on the tangent spaces $\mathrm{Ad}_g : \mathfrak{g} \to \mathfrak{g}$. In fact, it is a Lie algebra homomorphism (i.e. preserving the Lie bracket). The map $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g})$, $g \mapsto \mathrm{Ad}_g$ is a representation of G on its Lie algebra $\mathfrak{g}$. This representation Ad is called the *adjoint representation of* G. It can be extended to a representation of G on the complexification $\mathfrak{g}_\mathbb{C}$ of $\mathfrak{g}$, which is also denoted by Ad.

Definition 4.22. A *root* of G, with respect to T, is a weight of the adjoint representation $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g}_\mathbb{C})$ of G. The set of roots of G with respect to T is denoted by Φ.

It is clear that Φ is a finite subset of $\Lambda = X^*(T)$. It has many properties that we won't exhibit here, that make it the so-called *root system*.

In Definition 4.20, we defined the weight lattice $\Lambda = X^*(T)$. We can regard it as in the real vector space $\mathcal{V} \coloneqq \Lambda \otimes_\mathbb{Z} \mathbb{R}$. We will assume that the set Φ spans $\mathcal{V}$. In order to talk further about the weights and roots, it is necessary to discuss extra structures on the space $\mathcal{V}$.

Consider the normalizer of $N(T) = N_G(T) \coloneqq \{g \in G \mid gTg^{-1} = T\}$ of T in G.

Proposition 4.23. $N(T)$ is a closed subgroup of G. The connected component of the identity in $N(T)$ is T. The quotient $N(T)/T$ is a finite group.

Proof. See [Bum13, Proposition 15.8, p.106]. □

Definition 4.24. The quotient $W \coloneqq N(T)/T$ is called the *Weyl group* of G with respect to T.

Given $w \in N(T)$, the maximal torus T is invariant under the inner automorphism Inn_w (this is just the definition of normalizer). This means we have a Lie group homomorphism $\mathrm{Inn}_w|_T$ induced by Inn_w, and hence it induce a map on the weight lattice $X^*(T)$, which sends a weight $\lambda : T \to \mathbb{C}^*$ to $\lambda \circ \mathrm{Inn}_w|_T$. If $w \in T$, it is clear that $\mathrm{Inn}_w|_T = \mathrm{Id}_T$. Hence the Weyl group $W = N(T)/T$ acts on $\lambda = X^*(T)$, and so on the real vector space $\mathcal{V} = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. Since W is a finite group, one can give $\mathcal{V}$ an inner product $\langle \cdot, \cdot \rangle$ which is invariant under the action of W.

In the statement of Baruer-Klimyk formula, the action of W on certain weights appear. This means that we need to know how to compute this action if we want apply Baruer-Klimyk to compute irreducible characters of G. For a given root α, there is an associated element $w_\alpha \in W$ whose action on $\mathcal{V} = X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$ is the reflection :

$$s_\alpha : \mathcal{V} \to \mathcal{V},\ x \mapsto x - \frac{2\langle x, \alpha \rangle}{\langle \alpha, \alpha \rangle}\alpha. \tag{4.3.4}$$

Hence the quantity $\frac{2\langle x,\alpha\rangle}{\langle \alpha,\alpha\rangle}$ is important for the understanding of the action w_α. Let $\alpha^\vee$ be the linear functional on $\mathcal{V}$

$$\alpha^\vee(x) = \frac{2\langle x, \alpha \rangle}{\langle \alpha, \alpha \rangle}\cdot \tag{4.3.5}$$

The W-invariant inner product is given implicitly, so (4.3.5) doesn't give any actual information about $\alpha^\vee$ and hence the action w_α. We need to discuss roots from the viewpoint of Lie algebra.

Recall that a weight $\lambda \in \Lambda = X^*(T)$ is a linear character $\lambda : T \to \mathbb{C}^\times$ of T, which can be seen as a Lie group homomorphism. It is not difficult to see that its differential map $d\lambda : \mathfrak{t} \to \mathbb{C}$ takes values in $i\mathbb{R}$ (the Lie algebra of the Lie group $\mathbb{T}$ of complex numbers of absolute value 1, if we identify the Lie algebra of $\mathbb{C}^\times$ as $\mathbb{C}$ as usual). One can extend $d\lambda$ to the complexification of $\mathfrak{h} := \mathfrak{t}_{\mathbb{C}}$, and then it is a linear functional on $\mathfrak{h}$. The linear functionals on $\mathfrak{h}$ are called *weights* (from the viewpoint of Lie algebra). Similarly, we can talk about a weight of a Lie algebra representation of $\mathfrak{g}_{\mathbb{C}}$ and roots of the Lie algebra $\mathfrak{g}_{\mathbb{C}}$.

If $\alpha : T \to \mathbb{C}^\times$ is a root of the Lie group G, its differential $d\alpha$ (or more correctly, its extension to $\mathfrak{g}_{\mathbb{C}}$), which is a weight as mentioned in the above paragraph, will be a root of its (complexified) Lie algebra $\mathfrak{g}_{\mathbb{C}}$. We have explained (see here in page 67) a root is a eigenfunction of a simultaneous eigenvector for the adjoint representation (Ad or ad). If $X \in \mathfrak{g}_{\mathbb{C}}$ is such a simultaneous eigenvector for (the restriction to T of) the adjoint representation Ad of G and α is the associated root (i.e. $\mathrm{Ad}_t(X) = \alpha(t)X, \forall t \in T$), then it is easy to show that X is also a simultaneous eigenvector for (the restriction to $\mathfrak{h}$ of) the adjoint representation $\mathrm{ad} : \mathfrak{g}_{\mathbb{C}} \to \mathrm{gl}(\mathfrak{g}_{\mathbb{C}})$ and $d\alpha$ is the associated root (i.e. $\mathrm{ad}_H(X) = d\alpha(H)X, \forall H \in \mathfrak{h}$).

From now on, when we say weights or roots, we don't specify the viewpoints with which we look at them. It depends on the context.

As in Definition 4.20, Definition 4.21 and Definition 4.22, a root of $\mathfrak{g}_{\mathbb{C}}$ is just one of the eigenvalue functions of the *adjoint representation* $\mathrm{ad} \coloneqq d(\mathrm{Ad})$ of $\mathfrak{g}_{\mathbb{C}}$ with respect to $\mathfrak{h}$.

Definition 4.25. For a root α, the *root space* $\mathfrak{g}_{\mathbb{C},\alpha}$, or simply denoted by $\mathfrak{g}_\alpha$ (with the caution that it is not a subspace of $\mathfrak{g}$ but of $\mathfrak{g}_{\mathbb{C}}$), is the space of all X in $\mathfrak{g}_{\mathbb{C}}$ for which $\mathrm{ad}_H(X) = \alpha(H)X$ for all H in $\mathfrak{h}$, where $\mathrm{ad}_H(X)$ is $[H, X]$.

Theorem 4.26. For a root α, $-\alpha$ is also a root. We can find nonzero elements X_α in $\mathfrak{g}_\alpha$, Y_α in $\mathfrak{g}_{-\alpha}$ and H_α in $\mathfrak{h}$ such that

$$[H_\alpha, X_\alpha] = 2X_\alpha, \tag{4.3.6}$$
$$[H_\alpha, Y_\alpha] = -2Y_\alpha, \tag{4.3.7}$$
$$[X_\alpha, Y_\alpha] = H_\alpha. \tag{4.3.8}$$

The element H_α is independent of the choice of X_α and Y_α.

Proof. See [Bum13, Proposition 18.8, p.138]. □

Definition 4.27. For a root α, the elements $H_\alpha \in \mathfrak{h}$ are called the *coroots*.

Proposition 4.28. Let $\lambda \in \mathcal{V}$ and $\alpha \in \Phi$ be a root as defined in Definition 4.22. Then

$$d\lambda(H_\alpha) = \alpha^\vee(\lambda). \tag{4.3.9}$$

Proof. See [Bum13, Proposition 18.13, p.141]. □

In (4.3.4) and (4.3.5), we explain the relation of the linear functional $\alpha^\vee$ and the action of an element w_α in the Weyl group W, but they didn't provide computation information (without knowing explicitly the W-invariant inner product). (4.3.9) is a tool to compute $\alpha^\vee$ and hence w_α. The only task is to find the element H_α in Theorem 4.26.

The set Φ of roots is a finite set in the inner product space $\mathcal{V}$. So it can be partioned into two parts Φ^+ and Φ^- which are the two sides of a hyperplane through the origin with no point of Φ on it.

Definition 4.29. Fix a choice of Φ^+ and Φ^-. Let Σ be the set of elements in Φ^+ that cannot be expressed as a sum of other elements in Φ^+. Elements of Φ^+ are called *positive roots*. Elements of Φ^- are called *negative roots*. Elements of Σ are called *simple positive roots*. They are linear independent and form a basis of $\mathcal{V}$ if Φ spans $\mathcal{V}$. The *positive Weyl chamber* is

$$\mathcal{C}_+ = \{x \in \mathcal{V} \mid \langle x, \alpha\rangle \geq 0 \text{ for all } \alpha \in \Sigma\}.$$

A weight $\lambda \in \Lambda = X^*(T)$ is called *dominant* if $\lambda \in \mathcal{C}_+$.

Definition 4.30. Assuming the set Φ of roots spans $\mathcal{V}$. As mentioned in Definition 4.29, the set Σ of simple positive roots form a basis of $\mathcal{V}$. For each $\alpha_i \in \Sigma$, the linear functional $\alpha_i^\vee$ is in $\mathcal{V}^*$. The *fundamental dominant weights* are the dual basis $\varpi_j \in \mathcal{V}$ of $\alpha_i^\vee$, i.e. $\alpha_i^\vee(\varpi_j) = \delta_{ij}$. These ϖ_j are not necessary in the weight lattice Λ, but the terminology "fundamental dominant weight" is standard. If G is simply connected, then these ϖ_j form a basis of the lattice Λ (hence also of $\mathcal{V}$).

Definition 4.31. The *Weyl vector* is

$$\rho = \frac{1}{2} \sum_{\alpha \in \Phi^+} \alpha \in \mathcal{V}. \tag{4.3.10}$$

Under the assumption that Φ spans $\mathcal{V}$, it can be shown that $\rho = \varpi_1 + \cdots + \varpi_g$, which is in the interior $\mathcal{C}_+^\circ$ of the positive Weyl chamber $\mathcal{C}_+$. In particular, ρ is a dominant weight.

As discussed in Definition 4.21, we have a map $R(G) \to R(T)$ by restriction of characters of G to T. Use the notation in Definition 4.21, we write $\chi|_T = \sum_{\lambda\,:\,\text{weight of }\pi} m_\lambda e^\lambda$ for a character χ of a representation π of G. From now on, we will identify a character $\chi \in R(G)$ as its restriction $\chi|_T$ and just write $\chi = \sum_\lambda m_\lambda e^\lambda$.

Definition 4.32. Let Δ defined by

$$\Delta = \sum_{w \in W} (-1)^{l(w)} e^{w(\rho)} \in R(T), \tag{4.3.11}$$

where $\rho \in \Lambda$ is the Weyl vector defined in (4.3.10), $w(\rho)$ is the action of $w \in W$ on $\rho \in \Lambda$ which is described after Definition 4.24 and $l(w)$ is the number of $\alpha \in \Phi^+$ such that $w(\alpha) \in \Phi^-$. Similarly, for $\lambda \in \Lambda \cap \mathcal{C}_+$, i.e. a dominant weight, consider

$$\xi = \sum_{w \in W} (-1)^{l(w)} e^{w(\lambda+\rho)} \in R(T). \tag{4.3.12}$$

It turns out that ξ is divisible by Δ in the ring $R(T)$. Define

$$\chi(\lambda) = \frac{\xi}{\Delta} \in R(T). \tag{4.3.13}$$

We define a partial order on $\mathcal{V}$ by $\lambda \succcurlyeq \mu$ if $\lambda - \mu = \sum c_\alpha \alpha$ with all the $c_\alpha \geq 0$ for all simple positive roots $\alpha \in \Sigma$.

Proposition 4.33. Let λ be a dominant weight, i.e. $\lambda \in \Lambda \cap \mathcal{C}_+$. Let n_λ be the multiplicity of λ in $\chi(\lambda) \in R(T)$. Then $n_\lambda = 1$. For any μ whose multiplicity in $\chi(\lambda)$ is non-zero, we have $\lambda - \mu$ is in the lattice $\Lambda_{\text{roots}} \subset \Lambda$ generated by roots and $\lambda \succcurlyeq \mu$.

Proof. See [Bum13, Proposition 22.4, p.179]. □

The following theorem is the highlight of the above theory. It says that the irreducible characters of G are parametrized by dominant weights of G, which are the highest weight of the corresponding irreducible representations by Proposition 4.33.

Theorem 4.34. Let G be a compact connected Lie group. Assume the set Φ of roots spans $\mathcal{V}$. For a dominant weight $\lambda \in \Lambda \cap \mathcal{C}_+$, the element $\chi(\lambda) \in R(T)$ defined in (4.3.13) is the restriction of an irreducible character of G. Moreover, each irreducible character of G is obtained this way. Since the dominant weights parametrize the irreducible characters of G, we will use the notation χ_λ for the irreducible character whose restriction to T is $\chi(\lambda)$. But as mentioned after Definition 4.31, we don't distinct $\chi_\lambda \in R(G)$ and $\chi(\lambda) \in R(T)$.

Proof. See [Bum13, Theorem 22.3, p.182]. □

Finally, we are able to state the main theorem, Brauer-Klimyk formula, which provides a recursive way to compute the irreducible characters of G.

Theorem 4.35 (Brauer, Klimyk)**.** Let λ be a dominant weight and ν be any weight. There is an element w of the Weyl group W such that $w(\nu+\lambda+\rho) \in \mathcal{C}_+$. The point $w(\nu+\lambda+\rho) \in \mathcal{C}_+$ is uniquely determined. If it is on the boundary of $\mathcal{C}_+$, we define $\xi(\nu,\lambda) = 0$. Otherwise w is also uniquely determined, $w(\nu+\lambda+\rho)-\rho \in \mathcal{C}_+$, so it is a dominant weight, and we define $\xi(\nu,\lambda) = (-1)^{l(w)}\chi_{w(\nu+\lambda+\rho)-\rho}$, where $l(w)$ is the same as in (4.3.11). For a dominant weight μ with $\chi_\mu = \sum m(\nu)e^\nu \in R(T)$, we have

$$\chi_\mu \chi_\lambda = \sum_\nu m(\nu)\xi(\nu,\lambda). \tag{4.3.14}$$

Proof. See [Bum13, Proposition 22.9, p.185]. □

4.4 Examples : $\mathrm{USp}(2g)$

In Section 4.3, we introduce many notions quickly in order to state the Braure-Klimyk formula Theorem 4.35. Before presenting an algorithm to compute the irreducible characters of the unitary symplectic group $\mathrm{USp}(2g)$, it is good to see an example that demonstrates the notions in Section 4.3 and a picture of the algorithm in Section 4.6. We use $\mathrm{USp}(6)$ as our example, which corresponds to $g = 3$.

From the paragraph where (4.3.4) is to the paragraph after Proposition 4.28, we explain the action of the Weyl group W on the weight lattice $\Lambda = X^*(T)$ (and on its underlying space $\mathcal{V} = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$), the reflection s_α on $\mathcal{V}$ with respect to a W-invariant inner product on it, the quantity $\alpha^\vee$ that appear in s_α, an element

$H_\alpha \in \mathfrak{h} = \mathfrak{t}_{\mathbb{C}}$ that gives a way to compute $\alpha^\vee$, see Proposition 4.28, and a characterization of this element H_α (Theorem 4.26). Hence we begin with the task to find the elements X_α, Y_α and H_α in Theorem 4.26.

For $1 \leq i \neq j \leq g$, let $E_{ij}^{(g)}$ be the matrix of dimension g whose (k,l) entry is 1 if $k = i$ and $l = j$, otherwise it is 0. Let X_{ij} be the matrix of dimension $2g$ which is given by the following block from :

$$X_{ij} = \begin{pmatrix} E_{ij} & \mathbf{0} \\ \mathbf{0} & -E_{ji} \end{pmatrix}. \tag{4.4.1}$$

Similarly, let Y_{ij} be the matrix of dimension $2g$

$$Y_{ij} = \begin{pmatrix} E_{ji} & \mathbf{0} \\ \mathbf{0} & -E_{ij} \end{pmatrix}. \tag{4.4.2}$$

Let

$$u = \begin{pmatrix} U & 0 \\ 0 & \frac{1}{U} \end{pmatrix}, \text{ where } U = \begin{pmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & u_g \end{pmatrix}, u_i \in \mathbb{C}, |u_i| = 1, \tag{4.4.3}$$

be a generic element in the maximal torus (of our choice) T in $\mathrm{USp}(2g)$. Then by direct computing, we get

$$\mathrm{Inn}_u(e^{X_{ij}}) = u \cdot e^{X_{ij}} \cdot u^{-1} = e^{\frac{u_i}{u_j} X_{ij}}, \tag{4.4.4}$$

$$\mathrm{Inn}_u(e^{Y_{ij}}) = u \cdot e^{Y_{ij}} \cdot u^{-1} = e^{\frac{u_j}{u_i} Y_{ij}}. \tag{4.4.5}$$

This is translated to $\mathrm{Ad}_u(X_{ij}) = \frac{u_i}{u_j} X_{ij}$, and it means that X_{ij} is a simultaneous eigenvector of the restriction $\mathrm{Ad}|_T$ of the adjoint representation Ad, and the eigenfunction $\alpha_{ij} : T \to \mathbb{C}^\times, u \mapsto \frac{u_i}{u_j}$ is thus a root by Definition 4.20 and Definition 4.22. As explained in this paragraph in page 69, X_{ij} is also a simultaneous eigenvector for $\mathrm{ad}|_{\mathfrak{h}}$ and $d\alpha_{ij}$ is the associated root. This means that $X_{ij} \in \mathfrak{g}_{\alpha_{ij}}$, the root space of the root α_{ij}, see Definition 4.25. Similarly, $Y_{ij} \in \mathfrak{g}_{-\alpha_{ij}}$ after one sees that the map $u \in T \mapsto \frac{u_j}{u_i}$ is indeed the inverse of α_{ij} in the group $\Lambda = X^*(T)$. If we define $H_{ij} = [X_{ij}, Y_{ij}]$, one can easily verify that the the triple (X_{ij}, Y_{ij}, H_{ij}) satisfy the relations in Theorem 4.26, with $\alpha = \alpha_{ij}$. Theorem 4.26 says that such H is uniquely determined for each α_{ij}. And Proposition 4.28 can be used to compute the $\alpha_{ij}^\vee$ from H_{ij}. As explained in (4.3.4) and (4.3.5), α_{ij} is related to $s_{\alpha_{ij}}$ and hence to the action of a certain element $w_{ij} := w_{\alpha_{ij}}$ of the Weyl group W. We are mostly interested this action on the roots of G. We have not determined the roots completely, neither a complete set of simple positive

roots. But we can compute

$$
\begin{aligned}
w_{ij}(\alpha_{kl}) &= w_{\alpha_{ij}}(\alpha_{kl}) && (4.4.6)\\
&= s_{\alpha_{ij}}(\alpha_{kl}) && (4.4.7)\\
&= \alpha_{kl} - \frac{2\langle \alpha_{kl}, \alpha_{ij}\rangle}{\langle \alpha_{ij}, \alpha_{ij}\rangle}\,\alpha_{ij} && (4.4.8)\\
&= \alpha_{kl} - \alpha_{ij}^{\vee}(\alpha_{kl})\,\alpha_{ij} && (4.4.9)\\
&= \alpha_{kl} - ((d\alpha_{kl})(H_{ij}))\ \alpha_{ij}. && (4.4.10)
\end{aligned}
$$

So in order to know the action of w_{ij}, at least at the roots α_{kl}, we have to know the value of $d\alpha_{kl}$ at H_{ij}. We have known that $H_{ij} = [X_{ij}, Y_{ij}]$, but we have not compute this Lie bracket yet (hence we don't konw H_{ij} explicitly yet). The following lemma gives the result.

Lemma 4.36.

$$
H_{ij} = [X_{ij}, Y_{ij}] = \begin{pmatrix} E_{ii} - E_{jj} & \mathbf{0} \\ \mathbf{0} & -(E_{ii} - E_{jj}) \end{pmatrix}, \tag{4.4.11}
$$

where $E_{*,*}$ is the same as in (4.4.1). If we use the notation in (4.4.12), H_{ij} corresponds to the case $h_i = 1, h_j = -1$ and otherwise 0.

It just left to know $d\alpha_{kl}$ which is fairly easy, as demonstrated in the following lemma.

Lemma 4.37. Let

$$
H = \begin{pmatrix} \mathcal{H} & 0 \\ 0 & -\mathcal{H} \end{pmatrix}, \text{ where } \mathcal{H} = \begin{pmatrix} h_1 & 0 & 0 & 0 \\ 0 & h_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & h_g \end{pmatrix}, h_i \in \mathbb{C}, \tag{4.4.12}
$$

be a generic element in $\mathfrak{h}$. Let $\alpha_{kl} : T \to \mathbb{C}^{\times}, u \mapsto \frac{u_k}{u_l}$ be the root as described after (4.4.5) , where u is the same as in (4.4.3). Then

$$
d\alpha_{kl}(H) = h_k - h_l. \tag{4.4.13}
$$

Proof. Assume that $H \in \mathfrak{t} \subset \mathfrak{h}$. This means that $h_j \in i\mathbb{R}$ for all $j = 1, 2, \ldots, g$. Let $\exp : \mathfrak{t} \to T$ be the exponential map from the Lie algebra of the Lie group T to the Lie group T itself. In our case, $\exp(H) = e^H$ is just the matrix exponential. We have

$$
e^H = \begin{pmatrix} e^{\mathcal{H}} & 0 \\ 0 & e^{-\mathcal{H}} \end{pmatrix}, \text{ where } e^{\mathcal{H}} = \begin{pmatrix} e^{h_1} & 0 & 0 & 0 \\ 0 & e^{h_2} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & e^{h_g} \end{pmatrix}, \tag{4.4.14}
$$

where e^{h_i} is just the usual exponential of a complex number, which is the exponential map from the Lie algebra $\mathbb{C}$ of the Lie group $\mathbb{C}^\times$ to itself (if we choose the "natural" paramatrization). Hence $\alpha_{kl}\left(e^H\right) = \frac{e^{h_k}}{e^{h_l}} = e^{h_k - h_l}$. It is from a general fact that $\alpha_{kl}(e^H) = e^{d\alpha_{kl}(H)}$. Hence we have $e^{d\alpha_{kl}(H)} = e^{h_k - h_l}$, and from this we have $d\alpha_{kl}(H) = h_k - h_l$, if we take into account the facts that $d\alpha_{kl}(\mathbf{0}) = 0$ and $\mathfrak{t}$ is connected. Since $\mathfrak{h}$ is the complexification of $\mathfrak{t}$ and $d\alpha_{kl}$ is obtained by the natural (linear) extension from $\mathfrak{t}$ to $\mathfrak{h} = \mathfrak{t}_{\mathbb{C}}$, the above result implies (4.4.13) is true for all $H \in \mathfrak{h}$. □

After knowing explicitly H_{ij} and $d\alpha_{kl}$, it is a direct and easy to compute $d\alpha_{kl}(H_{ij})$:

Proposition 4.38. We have

$$d\alpha_{kl}(H_{ij}) = (\delta_{ik} - \delta_{jk}) - (\delta_{il} - \delta_{jl}). \tag{4.4.15}$$

Proof. As mentioned in (4.4.11),

$$H_{ij} = \begin{pmatrix} \mathcal{H}_{ij} & 0 \\ 0 & -\mathcal{H}_{ij} \end{pmatrix}, \text{ where } \mathcal{H}_{ij} = \begin{pmatrix} h_1 & 0 & 0 & 0 \\ 0 & h_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & h_g \end{pmatrix}, h_n \in \mathbb{C}, \tag{4.4.16}$$

where

$$h_n = \left\{ \begin{array}{ll} 1, & \text{if } n = i \\ -1, & \text{if } n = j \\ 0, & \text{if } n \neq i, j \end{array} \right\} = \delta_{in} - \delta_{jn}. \tag{4.4.17}$$

Here we use the fact that $i \neq j$, see the definition of $E_{ij}^{(g)}$ before (4.4.1). Use (4.4.13), we have

$$d\alpha_{kl}\left(H_{ij}\right) = h_k - h_l = (\delta_{ik} - \delta_{jk}) - (\delta_{il} - \delta_{jl}). \tag{4.4.18}$$

In particular, if we restrict to the roots of the form $\alpha_k := \alpha_{k,k+1}$ for $k = 1, 2, \ldots, g-1$, and hence to the corresponding coroots $H_i := H_{i,i+1}$ for $i = 1, 2, \ldots, g-1$, we have

$$\begin{aligned} d\alpha_k\left(H_i\right) &= d\alpha_{k,k+1}\left(H_{i,i+1}\right) && (4.4.19)\\ &= (\delta_{i,k} - \delta_{i+1,k}) - (\delta_{i,k+1} - \delta_{i+1,k+1}) && (4.4.20)\\ &= \left\{ \begin{array}{ll} 2, & \text{if } k = i \\ -1, & \text{if } |k-i| = 1 \\ 0, & \text{if } |k-i| \geq 2 \end{array} \right. && (4.4.21) \end{aligned}$$

□

We have consider the case where $i \neq j$, see (4.4.1). Next we consider the case where $i = j$ but skip the details, since we have demonstrated how to work out

the computation. For $i = 1, 2, \ldots, g$, let

$$X_{ii} = \begin{pmatrix} \mathbf{0} & E_{ii} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}, \; Y_{ii} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ E_{ii} & \mathbf{0} \end{pmatrix}. \tag{4.4.22}$$

The corresponding formula to (4.4.4) is

$$\mathrm{Inn}_u(e^{X_{ii}}) = u \cdot e^{X_{ii}} \cdot u^{-1} = e^{u_i^2 X_{ii}}, \tag{4.4.23}$$

$$\mathrm{Inn}_u(e^{Y_{ii}}) = u \cdot e^{Y_{ii}} \cdot u^{-1} = e^{u_i^{-2} Y_{ii}}. \tag{4.4.24}$$

This means that $\mathrm{Ad}_u(X_{ii}) = u_i^2 X_{ii}$. The corresponding root is $\alpha_{ii} : T \to \mathbb{C}^\times, u \mapsto u_i^2$. The coroots H_{ii} are given by

$$H_{ii} = [X_{ii}, Y_{ii}] = \begin{pmatrix} E_{ii} & \mathbf{0} \\ \mathbf{0} & -E_{ii} \end{pmatrix}, \tag{4.4.25}$$

where $E_{*,*}$ is the same as in (4.4.1). If we use the notation in (4.4.26), H_{ii} corresponds to the case $h_i = 1$ and otherwise 0. The following lemma is similar to Lemma 4.37.

Lemma 4.39. Let

$$H = \begin{pmatrix} \mathcal{H} & 0 \\ 0 & -\mathcal{H} \end{pmatrix}, \text{ where } \mathcal{H} = \begin{pmatrix} h_1 & 0 & 0 & 0 \\ 0 & h_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & h_g \end{pmatrix}, \; h_i \in \mathbb{C}, \tag{4.4.26}$$

be a generic element in $\mathfrak{h}$. Let $\alpha_{kk} : T \to \mathbb{C}^\times, u \mapsto u_k^2$ be the root as described after (4.4.24) , where u is the same as in (4.4.3). Then

$$d\alpha_{kk}(H) = 2h_k. \tag{4.4.27}$$

The results from Lemma 4.36 to Lemma 4.39 can be summarized in the following proposition :

Proposition 4.40. We have

$$d\alpha_{kl}(H_{ij}) = (\delta_{ik} - \delta_{jk}) - (\delta_{il} - \delta_{jl}) \tag{4.4.28}$$

$$d\alpha_{kk}(H_{ij}) = 2(\delta_{ik} - \delta_{jk}) \tag{4.4.29}$$

$$d\alpha_{kl}(H_{ii}) = \delta_{ik} - \delta_{il} \tag{4.4.30}$$

$$d\alpha_{kk}(H_{ii}) = 2\delta_{ik} \tag{4.4.31}$$

We have defined the roots $\alpha_k = \alpha_{k,k+1}$ for $k = 1, 2, \ldots, g-1$, see this paragraph on page 75. Define furthermore that $\alpha_g := \alpha_{gg}$ and $H_g := H_{gg}$. It can be shown

that $\Sigma := \{\alpha_k\}_{1\leq k\leq g}$ is the set of simple positive roots (under a choice for the set Φ^+ of positive roots which we won't specify here).

Proposition 4.41. We have

$$d\alpha_k(H_i) = \begin{cases} 2, & \text{if } k = i \\ -1, & \text{if } |k-i| = 1 \text{ but } k \neq g \\ -2, & \text{if } k = g \text{ and } i = g-1 \\ 0, & \text{if } |k-i| \geq 2 \end{cases} \tag{4.4.32}$$

We have certain elements $w_{ij} \in W$ in the Weyl group, for $1 \leq i \neq j \leq g$. These w_{ij} are not defined explicitly, but are given by the relations in (4.4.6). In particular, we can look at $w_i := w_{ii}$ for $1 \leq i \leq g-1$, which correspond to the roots α_i. Similarly we have a $w_g \in W$ corresponding to the root α_g. Just as in (4.4.6), we write again these relations for all the simple positive roots :

$$w_i(\alpha_k) = \alpha_k - \left((d\alpha_k)\left(H_i\right)\right)\ \alpha_i. \tag{4.4.33}$$

We want to express the action of $w_i \in W$, $i = 1, 2, \ldots, g$, with respect to the basis $\Sigma = \{\alpha_1, \alpha_2, \ldots, \alpha_g\}$ which is represented by a matrix (of size $g \times g$) denoted by $[w_i]_\Sigma$. Its (l,k)-entry, i.e. the entry in the l-th row and k-th column and denoted by $[w_i]_{\Sigma,l,k}$ is just the coefficient of α_l in the vector of $w_i(\alpha_k)$. By (4.4.33), we have

$$[w_i]_{\Sigma,l,k} = \delta_{kl} - \left((d\alpha_k)\left(H_i\right)\right)\ \delta_{il}. \tag{4.4.34}$$

Using Proposition 4.41, it is easy to compute $[w_i]_{\Sigma,l,k}$. Now we restrict ourselves to the case $g = 3$ for visualizing the examples more easily.

Example 4.42 (The action of w_i on Σ for $g = 3$)**.** The actions are represented by the matrices

$$[w_1]_\Sigma = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{4.4.35}$$

$$[w_2]_\Sigma = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \tag{4.4.36}$$

$$[w_3]_\Sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \tag{4.4.37}$$

We have worked with the simple positive roots $\alpha_i \in \Sigma$ defined after Proposition 4.40. More precisely, we try to understand the action of the Weyl group by its action on Σ. But Our goal is to compute irreducible characters of $\mathrm{USp}(2g)$ in the next section using Brauer-Klimyk formula in Theorem 4.35. These irreducible

characters are parametrized by dominant weights as shown in Theorem 4.34. Moreover, in the Brauer-Klimyk formula, we need to compute the actions of certain elements $w \in W$ of the Weyl group at certain weights, i.e. $w(\nu + \lambda + \rho)$ in Theorem 4.35. So it is reasonable to work with the weighs and hence with the fundamental weights ϖ_i introduced in Definition 4.30.

Definition 4.43. Let V_1 and V_2 be finite dimensional vector spaces over a same field, and B_i be a basis of V_i for $i = 1, 2$. Let $f : V \to W$ be a linear transformation. Then $[f]_{B_1}^{B_2}$ is defined to be the matrix representation of the f with respect to the basis B_1 and B_2. If $V_1 = V_2 = V$ is the same space and $f = \mathrm{Id} = \mathrm{Id}_V$ is the identity map, $[\mathrm{Id}]_{B_1}^{B_2}$ is just the matrix of basis change from B_1 to B_2.

Let $\varpi := \{\varpi_1, \varpi_2, \ldots, \varpi_g\}$ be the set of fundamental weights (for our choice of simple positive roots α_i), which forms a basis of $\mathcal{V}$. As mentioned at the end of the paragraph before Definition 4.43, our goal is to find the matrix representation $[w_i]_\varpi$ for the elements $w_i \in W$. The fundamental weights $\varpi_j \in \Lambda \subset \mathcal{V}$ are defined to be the dual basis of $\alpha_i^\vee \in \mathcal{V}^*$. This means that $\alpha_i^\vee(\varpi_j) = \delta_{ij}$. By Proposition 4.28, this means $d\varpi_j(H_{\alpha_i}) = d\varpi_j(H_i) = \delta_{ij}$. One can use Proposition 4.41 to determine ϖ_j in terms of the fundamental roots α_k and thus the basis change matrix $[\mathrm{Id}]_\varpi^\Sigma$, which is (for any given fixed g) just an easy exercise of solving a system of linear equations. But instead of doing this directly, we will use a third basis ϖ of λ, obtain $[\mathrm{Id}]_\Sigma^\varpi$ through ϖ. This will give $[w_i]_\varpi$. But we will also compute $[w_i]_\varpi$, which is helpful to demonstrate how to find a certain element $w \in W$ which satisfies the condition $w(\nu + \lambda + \rho) \in \mathcal{C}_+$ as required in Theorem 4.35.

Define ϖ_j to be $\varpi_j : T \to \mathbb{C}^\times, u \mapsto u_j$, where u is the same as in (4.4.3). Let $\varpi := \{\varpi_1, \varpi_2, \ldots, \varpi_g\}$. Recall that $\alpha_i = \alpha_{i,i+1} : T \to \mathbb{C}^\times, u \mapsto \frac{u_i}{u_{i+1}}$, for $1 \leq i \leq g-1$ and $\alpha_g = \alpha_{g,g} : u \mapsto u_g^2$. This means that we have :

Proposition 4.44. We have

$$\alpha_i = \begin{cases} \varpi_i - \varpi_{i+1} & \text{if } 1 \leq i \leq g-1 \\ 2\varpi_g & \text{if } i = g \end{cases} \tag{4.4.38}$$

This gives the basis change matrix

$$[\mathrm{Id}]_\Sigma^\varpi = \begin{pmatrix} 1 & 0 & 0 & & 0 & 0 & 0 \\ -1 & 1 & 0 & & 0 & 0 & 0 \\ 0 & -1 & 1 & & 0 & 0 & 0 \\ 0 & 0 & -1 & & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots\cdots\cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & 0 & & -1 & 1 & 0 \\ 0 & 0 & 0 & & 0 & -1 & 2 \end{pmatrix}. \tag{4.4.39}$$

Proposition 4.45. For $1 \leq i \leq g-1$, the action of w_i permutates ϖ_i and ϖ_{i+1} and fixes other ϖ_j for $j \neq i, i+1$. For the action of w_g, we have $w_g(\varpi_g) = -\varpi_g$ and $w_g(\varpi_j) = \varpi_j$ for $j \neq g$. The basis change matrix $[w_i]_{\varpi}$ is then very easy to obtain.

Proof. From the paragraphs where (4.3.4) and (4.3.5) locate, and also Proposition 4.28, we have

$$\begin{aligned} w_i(\lambda) &= \lambda - \alpha_i^\vee(\lambda)\,\alpha_i \\ &= \lambda - (d\lambda(H_i))\,\alpha_i, \end{aligned}$$

for all weight λ. This is used in (4.4.6) but with more details there. For $\lambda = \varpi_j$ and a generic element $H \in \mathfrak{h}$, as in Lemma 4.37 and in Lemma 4.39, it is easy to show

$$d\varpi_j\,(H) = h_j. \tag{4.4.40}$$

In particular,

$$d\varpi_j\,(H_i) = \begin{cases} \delta_{ij} - \delta_{i+1,j} & \text{for } 1 \leq i \leq g-1 \\ \delta_{gj} & \text{if } i = g \end{cases} \tag{4.4.41}$$

Hence we have

$$w_i(\varpi_j) = \begin{cases} \varpi_j - (\delta_{ij} - \delta_{i+1,j})\,\alpha_i & \text{for } 1 \leq i \leq g-1 \\ \varpi_j - \delta_{gj}\,\alpha_i & \text{if } i = g \end{cases} \tag{4.4.42}$$

Using (4.4.38), the proof is a direct and easy computation. □

Example 4.46 (The action of w_i on ϖ for $g = 3$)**.** We have

$$[w_1]_{\varpi} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ [w_2]_{\varpi} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ [w_3]_{\varpi} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Proposition 4.47. For all $1 \leq j \leq g$, we have

$$\varpi_j = \sum_{k=1}^{j} \varpi_k. \tag{4.4.43}$$

This means that the matrix of basis change $[\mathrm{Id}]_{\varpi}^{\varpi}$ from the set ϖ of fundamental

weights to the set ϖ is given by

$$[\mathrm{Id}]_{\varpi}^{\varpi} = \begin{pmatrix} 1 & 1 & 1 & & 1 & 1 & 1 \\ 0 & 1 & 1 & & 1 & 1 & 1 \\ 0 & 0 & 1 & & 1 & 1 & 1 \\ 0 & 0 & 0 & & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \cdots\cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & & 1 & 1 & 1 \\ 0 & 0 & 0 & & 0 & 1 & 1 \\ 0 & 0 & 0 & & 0 & 0 & 1 \end{pmatrix}. \tag{4.4.44}$$

Its inverse, which is the basis change from ϖ to ϖ, is

$$[\mathrm{Id}]_{\varpi}^{\varpi} = \begin{pmatrix} 1 & -1 & 0 & 0 & & 0 & 0 \\ 0 & 1 & -1 & 0 & & 0 & 0 \\ 0 & 0 & 1 & -1 & & 0 & 0 \\ 0 & 0 & 0 & 1 & & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots\cdots\cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & & -1 & 0 \\ 0 & 0 & 0 & 0 & & 1 & -1 \\ 0 & 0 & 0 & 0 & & 0 & 1 \end{pmatrix}. \tag{4.4.45}$$

From the definition of ϖ_k, we see that

$$\varpi_j : T \to \mathbb{C}^\times,\ u \mapsto \prod_{k=1}^{j} u_k. \tag{4.4.46}$$

Proof. In the paragraph on page 78, we see that the fundamental irreducible characters ϖ_j are determined by the relations

$$d\varpi_j(H_i) = \delta_{ij}. \tag{4.4.47}$$

Combine this with (4.4.41), we obtain, for $2 \leq j \leq g$

$$d\varpi_j\,(H_i) = \begin{cases} \delta_{ij} - \delta_{i,j-1} = (d\varpi_j - d\varpi_{j-1})(H_i) & \text{if } 1 \leq i \leq g-1 \\ \delta_{gj} - \delta_{g,j-1} = (d\varpi_j - d\varpi_{j-1})(H_g) & \text{if } i = g \end{cases} \tag{4.4.48}$$

$$= (d\varpi_j - d\varpi_{j-1})(H_i). \tag{4.4.49}$$

Note that we have $\delta_{g,j-1} = 0$ since $j - 1 < g$. The above equation is also true for $j = 1$ with an easy extra argument and set $\varpi_0 = 1$. The equation holds for all $1 \leq i \leq g$, and this implies that

$$d\varpi_j = d\varpi_j - d\varpi_{j-1},\ \text{for } 1 \leq j \leq g. \tag{4.4.50}$$

Hence we have the relations $\varpi_j = \sum_{k=1}^{j} \varpi_k$. The rest statements follow easily. $\square$

Finally, we can compute the matrix representation of w_i with respect to the basis ϖ. The reason to do so is mentioned in this paragraph on page 77.

Corollary 4.48. For $w \in W$, we have

$$[w]_{\varpi} = [\mathrm{Id}]_{\varpi}^{\varpi} \cdot [w]_{\varpi} \cdot [\mathrm{Id}]_{\varpi}^{\varpi}. \tag{4.4.51}$$

The matrices $[\mathrm{Id}]_{\varpi}^{\varpi}$ and $[\mathrm{Id}]_{\varpi}^{\varpi}$ are given in Proposition 4.47. For $w = w_i$, $[w_i]_{\varpi}$ is given in Proposition 4.45.

Example 4.49 (The action of w_i on ϖ for $g = 3$)**.** We have

$$[w_1]_{\varpi} = \begin{pmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ [w_2]_{\varpi} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \ [w_3]_{\varpi} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & -1 \end{pmatrix}.$$

We give a general description of $[w_i]_{\varpi}$ for $\mathrm{USp}(2g)$ without proof.

Proposition 4.50. For $1 \leq j \leq g-1$, let v_j be the column vector of length g whose entry at i-th row, denoted by v_{ij}, is given by

$$v_{ij} = \begin{cases} 1, & \text{if } i = j-1 \\ -1, & \text{if } i = j \\ 1, & \text{if } i = j+1 \\ 0, & \text{othewise} \end{cases} \tag{4.4.52}$$

Let v_g be the (column) vector $(0, 0, \ldots, 0, 2, -1)^t$ of length g. Then $[w_i]_{\varpi}$ is the same as the $g \times g$ identity matrix except that the i-th column of $[w_i]_{\varpi}$ is replaced by v_i. It is best to see examples for $g = 6$ to have a picture of these matrices :

$$[w_1]_{\varpi} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \ [w_2]_{\varpi} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \ [w_3]_{\varpi} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$[w_4]_{\varpi} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \ [w_5]_{\varpi} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \ [w_6]_{\varpi} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

We have given enough information to state the algorithm for computing irreducible characters for $\mathrm{USp}(2g)$ in the next section. The Weyl vector ρ appears in Brauer-Klimyk formula in Theorem 4.35, so it is used in the algorithm. It is

defined in (4.3.10) and we have $\rho = \sum_{i=1}^{g} \varpi_i$, so with respect to the basis ϖ, it is the (column) vector $[\rho]_{\varpi} = (1, 1, \ldots, 1)^t$, where t means the transpose.

4.5 Fundamental irreducible characters of $\mathrm{USp}(2g)$

In this section, we use the notation $\mathrm{Sp}(g)$ for the group $\mathrm{USp}(2g)$. In previous section, we have studied the fundamental dominant weights of ϖ_i. As mentioned in Theorem 4.34, each dominant weight λ corresponds to an irreducible character which is denoted by χ_λ. The corresponding irreducible characters χ_{ϖ_i} of the fundamental dominant weights ϖ_i are called the fundamental irreducible characters and are also denoted by χ_i. Every dominant weight is a linear combinations of these ϖ_i with positive integers as coefficients. If $\lambda = \sum_{i=1}^{g} n_i \varpi_i$, then we denote its corresponding irreducible character by χ_v, where $v = (n_1, n_2, \ldots, n_g)$. In particular, we have $\chi_{\varpi_i} = \chi_i = \chi_{e_i}$, where e_i are just the standard basis of $\mathbb{Z}^g$.

In Brauer-Klimyk formula (4.3.14), the multiplication $\chi_\mu \chi_\lambda$ of irreducible characters χ_μ and χ_λ, where μ and λ are dominant weights, are computed using the information of how χ_μ is decomposed into irreducible characters of T. For our algorithm, we only need to consider the case where $\mu = \varpi_i$ is one of the fundamental irreducible weight of $\mathrm{Sp}(g)$. This means that we need to know how the fundamental irreducible characters $\chi_{e_i} = \chi_i = \chi_{\varpi_i}$ of $\mathrm{Sp}(g)$ decompose on the virtual character ring $R(T)$ of T. Its virtual character ring G

Consider products of Lie groups $G = G_1 \times G_2 \cdots \times G_n$. Its virtual character ring $R(G)$. We have a multi-linear map

$$\varphi : R(G_1) \times R(G_2) \times \cdots \times R(G_n) \longrightarrow R(G)$$

$$(\boldsymbol{\chi}_1, \boldsymbol{\chi}_2, \ldots, \boldsymbol{\chi}_n) \longmapsto \boldsymbol{\chi} : G \to \mathbb{C},\ \boldsymbol{\chi}(g) = \textstyle\prod_{i=1}^{g} \boldsymbol{\chi}_i(g_i) \tag{4.5.1}$$

where $\boldsymbol{\chi}_i$ are characters of G_i (not the fundamental irreducible characters χ_i define in the previous paragraphs. Note that the symbol $\boldsymbol{\chi}$ is in bold font, which indicates the difference), and $g = (g_1, g_2, \ldots, g_n) \in G$. We define φ for characters only, but it extends to the whole domain. This gives an isomorphism (we omit the proof), also denoted by φ,

$$\varphi : R(G_1) \otimes R(G_2) \otimes \cdots \otimes R(G_n) \longrightarrow R(G) \tag{4.5.2}$$

$$\boldsymbol{\chi}_1 \otimes \boldsymbol{\chi}_2 \otimes \cdots \otimes \boldsymbol{\chi}_n \longmapsto \boldsymbol{\chi}$$

For the group $\mathrm{Sp}(1) = \mathrm{SU}(2)$, its fundamental irreducible character is the trace map $t = \mathrm{tr}$ on $\mathrm{SU}(2)$. Its virtual character ring is isomorphic to the polynomial

ring $\mathbb{Z}[t]$. Now consider $n = g$ and $G_i = \mathrm{Sp}(1)$ for all $1 \leq i \leq g$ and their fundamental irreducible characters t_i. We then have $R(\mathrm{Sp}(1)^g) \cong \otimes_{i=1}^g \mathbb{Z}[t_i] \cong \mathbb{Z}[t_1, t_2, \ldots, t_g]$. Let s_i be the i-th symmetric polynomial in $t_1, t_2, \ldots, t_g$. Their images in $R(\mathrm{Sp}(1)^g)$ are in fact in the subring $R(\mathrm{Sp}(g))$ of $R(\mathrm{Sp}(1)^g)$ under a natural embedding $\mathrm{Sp}(1)^g \hookrightarrow \mathrm{Sp}(g)$. Furthermore, under this embedding of virtual character rings $R(\mathrm{Sp}(g)) \hookrightarrow R(\mathrm{Sp}(1)^g) \cong \mathbb{Z}[t_1, t_2, \ldots, t_g]$, we have $\mathbb{Z}[s_1, s_2, \ldots, s_g]$.

We have mentioned we need to decompose the fundamental irreducible characters χ_i of $\mathrm{Sp}(g)$ into weights (i.e. irreducible characters of T) in this paragraph on page 82. This decomposition can be done through $\mathrm{Sp}(1)^g$ by $T \hookrightarrow \mathrm{Sp}(1)^g \hookrightarrow \mathrm{Sp}(g)$. Hence we first state a result of the decomposition of χ_i in the ring $R(\mathrm{Sp}(1)^g)$. In some sense, this is equivalent to find the polynomial expressions of χ_i in $t_1, t_2, \ldots, t_g$, and these can be obtained easily after the polynomial expressions of χ_i in $s_1, s_2, \ldots, s_g$ is known. The following proposition gives this relations.

Proposition 4.51. Identify $R(\mathrm{Sp}(g))$ with $\mathbb{Z}[s_1, s_2, \ldots, s_g]$ as explained above. Let χ_0 be the trivial character of $\mathrm{Sp}(g)$. Let $s_0 = 1$, as an element in $\mathbb{Z}[s_1, s_2, \ldots, s_g]$. It is easy to see χ_0 corresponds to s_0 under the identification. For all $0 \leq i \leq g$, the fundamental irreducible character χ_i of $\mathrm{Sp}(g)$ is linear in $s_0, s_1, s_2, \ldots, s_g$. Let A_{g+1} be the matrix of size $(g+1) \times (g+1)$ whose i-th row v_{i-1} is obtained recursively from v_{i-1} by the following rules :

$$
\begin{aligned}
v_0 &= (1, 0, 0, 0, 0, 0, \ldots, 0, 0) \\
v_1 &= (0, 1, 0, 0, 0, 0, \ldots, 0, 0) \\
v_2 &= (1, 0, 1, 0, 0, 0, \ldots, 0, 0) \\
v_3 &= (0, 2, 0, 1, 0, 0, \ldots, 0, 0) \\
v_4 &= (2, 0, 3, 0, 1, 0, \ldots, 0, 0) \\
v_5 &= (0, 5, 0, 4, 0, 1, \ldots, 0, 0) \\
&\vdots \\
v_i &= (v_{i0}, v_{i1}, v_{i2}, \ldots, , v_{i,g-1}, v_{ig}) \,,\ v_{ij} = v_{i-1,j-1} + v_{i-1,j+1} \\
&\vdots
\end{aligned}
$$

Let $[\mathrm{Id}_{g+1}]_\chi^s$ be the matrix of size $(g+1) \times (g+1)$ that represents these linear relations. Then for $1 \leq i, j \leq g+1$, the (i,j)-entry of $[\mathrm{Id}_{g+1}]_\chi^s$ is given by the $(g+1-i, g+1-j)$-entry of A_{g+1}. For example, for $g = 5$, we have

$$
A_6 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 \\
0 & 2 & 0 & 1 & 0 & 0 \\
2 & 0 & 3 & 0 & 1 & 0 \\
0 & 5 & 0 & 4 & 0 & 1
\end{pmatrix}, \quad
[\mathrm{Id}_6]_\chi^s = \begin{pmatrix}
1 & 0 & 4 & 0 & 5 & 0 \\
0 & 1 & 0 & 3 & 0 & 2 \\
0 & 0 & 1 & 0 & 2 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}. \tag{4.5.3}
$$

Proof. Consider the natural embedding $\mathrm{Sp}(g-1)\times\mathrm{Sp}(1)\hookrightarrow\mathrm{Sp}(g)$, where the factor $\mathrm{Sp}(1)$, embedded into $\mathrm{Sp}(g)$ has (t_g, t_g^{-1}) as coordinates. We write the trivial and fundamental irreducible characters of $\mathrm{Sp}(g-1)$ and $\mathrm{Sp}(1)$ by $\chi_j^{(g-1)}$ and $\chi_k^{(1;g)}$ respectively, to indicate this choice of embedding, where $0\leq j\leq g-1$ and $k=0,1$. For other indices, they are defined to be zero. From a general branching rule [4] from $\mathrm{Sp}(g)$ to $\mathrm{Sp}(g-1)\times\mathrm{Sp}(1)$, one can deduce that, for $0\leq i\leq g$,

$$\chi_i^{(g)}=\chi_i^{(g-1)}\cdot\chi_0^{(1;g)}+\chi_{i-1}^{(g-1)}\cdot\chi_1^{(1;g)}+\chi_{i-2}^{(g-1)}\cdot\chi_0^{(1;g)}, \tag{4.5.4}$$

where $\chi_0^{(1;g)}=1$ and $\chi_1^{(1;g)}=t_g$. Similarly, we have

$$s_i^{(g)}=s_i^{(g-1)}+s_{i-1}^{(g-1)}\cdot s_1^{(1;g)}, \tag{4.5.5}$$

where $s_1^{(1;g)}=t_g$ and $s_i^{(g-1)}$ and $s_i^{(g)}$ are the i-th symmetric polynomials in $t_1,\ldots,t_{g-1}$ and $t_1,\ldots,t_g$ respectively. Using (4.5.4) and (4.5.5), the relations of $\left\{\chi_i^{(g)}\right\}_{i=0}^{g}$ and $\left\{s_i^{(g)}\right\}_{i=0}^{g}$ can be determined by induction on g. This leads to a proof of the proposition. □

Now we know the (linear) expression of χ_i in $s_1,s_2,\ldots,s_g$, and hence the polynomial expression in $t_1,t_2,\ldots,t_g$. The monomials that appear in the expression of χ_i have the form $\prod_{j=1}^g t_j^{n_j}$ with each $n_j\in\{0,1\}$. In order to know the decomposition of χ_i in $R(T)$, we only need to know how these monomials are expressed in $R(T)$.

Recall $\mathbb{T}=\{z\in\mathbb{C}\,|\,|z|=1\}$. Consider the irreducible character $\mathbb{T}\to\mathbb{C}^\times, z\mapsto z$ of $\mathbb{T}$, and we denote it by z, which can be thought as the coordinate function of $\mathbb{T}$. Similar we have the irreducible character $\mathbb{T}\to\mathbb{C}^\times, z\mapsto\frac{1}{z}$, which is denote by $\frac{1}{z}$. Consider the embedding

$$\begin{array}{ccc}\mathbb{T} & \longrightarrow & \mathrm{Sp}(1)\\ z & \longmapsto & \begin{pmatrix} z & 0\\ 0 & \frac{1}{z}\end{pmatrix}.\end{array}$$

The fundamental irreducible character t of $\mathrm{Sp}(1)$ is the trace map, hence the restriction of t on $\mathbb{T}$ is given by $z\mapsto z+\frac{1}{z}$. Use the above notation, we can write $t=z+\frac{1}{z}$, where z and $\frac{1}{z}$ are irreducible characters of $\mathbb{T}$ defined above. They are elements in the virtual character ring $R(\mathbb{T})$ of $\mathbb{T}$, and t is an element in $R(\mathrm{Sp}(1))$ and also in $R(\mathbb{T})$ since we have an induced embedding $R(\mathrm{Sp}(1))\hookrightarrow R(\mathbb{T})$.

The maximal torus T of $\mathrm{Sp}(g)$ is chosen explicitly, see (4.4.3) for the generic element in T. We have the embedding $\mathbb{T}^g\hookrightarrow\mathrm{Sp}(1)^g$ which is the product of the embedding $\mathbb{T}\hookrightarrow\mathrm{Sp}(1)$ defined in the previous paragraph. It is easy to give an isomorphism $\mathbb{T}^g\xrightarrow{\sim}T$ and embeddings $T\hookrightarrow\mathrm{Sp}(1)^g$ and $\mathrm{Sp}(1)^g\hookrightarrow\mathrm{Sp}(g)$ such

4. See [Lep71, Theorem 2].

that the following diagram is commutative :

$$\begin{array}{ccc} \mathbb{T}^g & \longrightarrow & T \\ \downarrow & \swarrow & \downarrow \\ \mathrm{Sp}(1)^g & \longrightarrow & \mathrm{Sp}(g) \end{array} \tag{4.5.6}$$

Apply (4.5.2) for $G_i = \mathbb{T}$ and $G = \mathbb{T}^g$, we get isomorphisms $\otimes_{i=1}^g R(\mathbb{T}) \xrightarrow{\sim} R(\mathbb{T}^g)$. The embeddings of $R(\mathrm{Sp}(1)) \hookrightarrow R(\mathbb{T})$ induces $\otimes_{i=1}^g R(\mathrm{Sp}(1)) \hookrightarrow \otimes_{i=1}^g R(\mathbb{T})$. Combined these with the induced diagram of (4.5.6) on virtual character rings, we have the following commutative diagram :

$$\begin{array}{ccccccccc} \mathbb{Z}[z_1, \frac{1}{z_1}, \ldots, z_g, \frac{1}{z_g}] & \xrightarrow{\sim} & \bigotimes_{i=1}^g \mathbb{Z}[z_i, \frac{1}{z_i}] & \xrightarrow{\sim} & \bigotimes_{i=1}^g R(\mathbb{T}) & \xrightarrow{\sim} & R(\mathbb{T}^g) & \xleftarrow{\sim} & R(T) \\ \uparrow & & \uparrow & & \uparrow & & \uparrow & \nearrow & \uparrow \\ \mathbb{Z}[t_1, \ldots, t_g] & \xrightarrow{\sim} & \bigotimes_{i=1}^g \mathbb{Z}[t_i] & \xrightarrow{\sim} & \bigotimes_{i=1}^g R(\mathrm{Sp}(1)) & \xrightarrow{\sim} & R(\mathrm{Sp}(1)^g) & \longleftarrow & R(\mathrm{Sp}(g)) \end{array} \tag{4.5.7}$$

All the ring homomorphisms above are in fact $\mathbb{Z}$-algebra homomorphisms, and the most left map in the above diagram is determined by $t_i \to z_i + \frac{1}{z_i}$.

Now given an element of $R(\mathrm{Sp}(1)^g$, identified with $\prod_{j=1}^g t_j^{n_j}$, $n_j \in \mathbb{Z}$. Its image in $\mathbb{Z}[z_1, \frac{1}{z_1}, \ldots, z_g, \frac{1}{z_g}]$ is $\prod_{j=1}^g (z_j + \frac{1}{z_j})^{n_j}$. As mentioned here in page 84, for the fundamental irreducible characters of $\mathrm{Sp}(g)$, we just need to consider $n_j \in \{0, 1\}$. In this case, $\prod_{j=1}^g (z_j + \frac{1}{z_j})^{n_j}$ is very easy to expand as monomials (whose powers may be negative integers) in z_j. We have defined weights $\varpi_j : T \to \mathbb{C}^\times$ in page 78. It is easy to see the restriction of ϖ_j to $\mathbb{T}$ under $\mathbb{T} \hookrightarrow \mathbb{T}^g \hookrightarrow T$ is just the irreducible character $z_j : \mathbb{T} \to \mathbb{C}^\times$ define here in 84. Here the embedding of $\mathbb{T} \hookrightarrow \mathbb{T}^g$ is the j-th component. This means that the monomial $\prod_j z_j^{n_j}$ corresponds to the weight $\sum_j n_j \varpi_j$. Thus the weighs (and their multiplicities) of the fundamental irreducible characters χ_i of $\mathrm{Sp}(g)$ are completely determined. Finally, we have to change to the basis of fundamental dominant weights $\varpi_1, \ldots, \varpi_g$ using (4.4.45).

Example 4.52. Consider $g = 3$ and χ_3 in Proposition 4.51. We have $\chi_3 = s_1 + s_3$. From the definition, we have $s_1 = t_1 + t_2 + t_3$ and $s_3 = t_1 t_2 t_3$. Hence

$$s_1 = (z_1 + z_1^{-1}) + (z_2 + z_2^{-1}) + (z_3 + z_3^{-1}).$$

The corresponding weights are

$$\varpi_1, -\varpi_1, \varpi_2, -\varpi_2, \varpi_3, -\varpi_3.$$

Similarly, we have

$$\begin{aligned} s_3 &= (z_1 + z_1^{-1})(z_2 + z_2^{-1})(z_3 + z_3^{-1}) \\ &= z_1 z_2 z_3 + z_1 z_2 z_3^{-1} + z_1 z_2^{-1} z_3 + z_1 z_2^{-1} z_3^{-1} + \\ &\quad z_1^{-1} z_2 z_3 + z_1^{-1} z_2 z_3^{-1} + z_1^{-1} z_2^{-1} z_3 + z_1^{-1} z_2^{-1} z_3^{-1}. \end{aligned}$$

The corresponding weights are

$$\begin{aligned} \varpi_1 + \varpi_2 + \varpi_3 \\ \varpi_1 + \varpi_2 - \varpi_3 \\ \varpi_1 - \varpi_2 + \varpi_3 \\ \varpi_1 - \varpi_2 - \varpi_3 \\ -\varpi_1 + \varpi_2 + \varpi_3 \\ -\varpi_1 + \varpi_2 - \varpi_3 \\ -\varpi_1 - \varpi_2 + \varpi_3 \\ -\varpi_1 - \varpi_2 - \varpi_3 \end{aligned}$$

The 14 weights above are thus the weights of the fundamental irreducible character χ_3 and each of them has multiplicity 1.

We summarize the results in this section in the following proposition (which follows from Proposition 4.51) :

Proposition 4.53. Let χ_i be the fundamental irreducible character of $\mathrm{Sp}(g)$ corresponding to the fundamental dominant weight ϖ_i, as mentioned in page 82. Then χ_i is linear in $s_1, \ldots, s_g$, see Proposition 4.51. Write $\chi_i = \sum_{j=1}^{g} m_{ji} s_j$, where m_{ji} is the (j,i)-entry of $[\mathrm{Id}_{g+1}]_\chi^s$ in Proposition 4.51. We have $m_{ii} = 1$. Let $\nu \in \Lambda$ be a weight whose vector representation, with respect to the basis ϖ introduced in page 78, is $[\nu]_\varpi = v = (v_1, v_2, \ldots, v_g)$ with exactly j non-zero coordinates. Then ν is a weight of χ_i if and only if $v_k \in \{-1, 0, 1\}$ for all k and $m_{ji} \neq 0$. More precisely, the multiplicity of ν in χ_i is m_{ji}. Using (4.4.45), we see that the vector representation $[\nu]_\varpi$ of a weight ν of χ_i with respect to the basis ϖ has the form $(v_1 - v_2, v_2 - v_3, \ldots, v_{g-1} - v_g, v_g)$ with all $v_k \in \{-1, 0, 1\}$.

4.6 Computation of irreducible characters

In this section, we present an algorithm to compute the irreducible characters of $\mathrm{USp}(2g)$. More precisely, our task is to express an irreducible character χ of $\mathrm{USp}(2g)$ as a polynomial expression in $s_1, \ldots, s_g$, under the isomorphism in (4.5.7). For the fundamental irreducible characters χ_i, the answer is given in Proposition 4.51 in the previous section. Furthermore, we also discussed the

weights of χ_i. These extra information are used in the algorithm, as explained in page 82.

Every irreducible character corresponds an dominant weight λ. We will use the set of fundamental dominant weights ϖ as the basis for weights. Our task is to compute the irreducible character corresponding to a dominant weight in a recursive way. More precisely : Fix an integer $1 \leq l \leq g$. The Brauer-Klimyk formula (4.3.14) involves $\chi_\mu \chi_\lambda$ for another dominant weight μ, which will be the fundamental dominant weight ϖ_l in our algorithm. We will compute $\chi_{\lambda+\mu}$ from $\chi_\mu \chi_\lambda$ and other terms. The weight λ and the other terms are "smaller" than $\lambda + \mu$, which will be defined later (but it is not the partial order we defined in page 71). This is what we mean by "in a recursive way" above. In fact, we don't define an order on the set of dominant weights, but on its coordinate space with respect to the basis ϖ, see Definition 4.60.

In Proposition 4.53, we give a description of the weights ν of $\chi_\mu = \chi_{\varpi_l} = \chi_l$. In order to apply the Brauer-Klimyk formula, we need to find a certain element $w \in W$ in the Weyl group such that $w(\nu+\lambda+\rho)$ lies in the positive Weyl chamber $\mathcal{C}_+$ defined in Definition 4.29, where $\rho = \sum_{i=1}^g \varpi_i$ is the Weyl vector in Definition 4.31. The Weyl group W of $\mathrm{USp}(2g)$ has order $(2g)!! = 2^g g!$ (double factorial of $2g$), which grows extremely fast : For $1 \leq g \leq 10$, we have

g	1	2	3	4	5	6	7	8	9	10
$\lvert W\rvert$	2	8	48	384	3840	46080	645120	10321920	185794560	3715891200

Thus a naive approach to find a required element $w \in W$ is not feasible for $g \geq 8$ and it is already very slow for $g = 6$. Hence before we present our algorithm, it is necessary to address this question about efficiency.

It follows the definitions of positive Weyl chamber $\mathcal{C}_+$ (Definition 4.29) and of fundamental dominant weights (Definition 4.30) that every element $x \in \mathcal{C}_+$ have positive coordinates with respect to the basis ϖ : For $x \in \mathcal{C}_+$, we have $[x]_\varpi = (x_1, x_2, \ldots, x_g)$ with $x_i \geq 0$ for all i. If x is a dominant weight, i.e. $x \in \Lambda \cap \mathcal{C}_+$, then $[x]_\varpi = (x_1, x_2, \ldots, x_g) \in \mathbb{Z}^g_{\geq 0}$. Since $\mathrm{USp}(2g)$ is simply connected, ϖ form a basis of Λ (Definition 4.30) and the set $\Lambda \cap \mathcal{C}_+$ of dominant weights is identified as $\mathbb{Z}^g_{\geq 0}$ via $x \mapsto [x]_\varpi$.

Back to the question of finding $w \in W$ such that $w(\nu + \lambda + \rho) \in \mathcal{C}_+$. We work with the basis ϖ. Let $[\lambda]_\varpi = (x_1, x_2, \ldots, x_g) \in \mathbb{Z}^g_{\geq 0}$. We have $[\rho]_\varpi = (1, 1, \ldots, 1)$, as explained in page 81. For a weight ν of an fundamental irreducible character χ_l, we have $[\nu]_\varpi = (v_1 - v_2, v_2 - v_3, \ldots, v_{g-1} - v_g, v_g)$ with all $v_k \in \{-1, 0, 1\}$, see

Proposition 4.53. So the question is translated to find $w \in W$ such that

$$[w]_{\varpi} \cdot [\nu + \lambda + \rho]_{\varpi} = [w]_{\varpi} \cdot \begin{pmatrix} x_1 + 1 + (v_1 - v_2) \\ x_2 + 1 + (v_2 - v_3) \\ \vdots \\ x_{g-1} + 1 + (v_{g-1} - v_g) \\ x_g + 1 + (v_g) \end{pmatrix} \in \mathbb{Z}^g_{\geq 0}\,, \tag{4.6.1}$$

where $x_i \in \mathbb{Z}^g_{\geq 0}$ and $v_i \in \{-1, 0, 1\}$ for all i. We will answer this question, but before that, we discuss a more general question.

Let $\lambda \in \Lambda$ be any weight (not necessary dominant) with $[\lambda]_{\varpi} = (x_1, x_2, \ldots, x_g) \in \mathbb{Z}^g$. How one can find $w \in W$ such that $w(\lambda) \in \mathcal{C}_+$, i.e. $[w]_{\varpi} \cdot (x_1, x_2, \ldots, x_g) \in \mathbb{Z}^g_{\geq 0}$? We have seen that $\Lambda \cap \mathcal{C}_+ \xrightarrow{\sim} \mathbb{Z}^g_{\geq 0}\,,\ x \mapsto [x]_{\varpi}$. Using the basis change of ϖ and ϖ given in Proposition 4.47, we see that $\Lambda \cap \mathcal{C}_+ \xrightarrow{\sim} \mathbb{Z}^g_{\measuredangle}\,,\ x \mapsto [x]_{\varpi}$, where $\mathbb{Z}^g_{\measuredangle}$ is

$$\mathbb{Z}^g_{\measuredangle} = \{(y_1, y_2, \ldots, y_g) \in \mathbb{Z}^g \mid y_1 \geq y_2 \geq \cdots \geq y_g \geq 0\}\,. \tag{4.6.2}$$

Hence the question is equivalent to find $w \in W$ such that $[w]_{\varpi} \cdot (y_1, y_2, \ldots, y_g) \in \mathbb{Z}^g_{\measuredangle}$, for any given $[\lambda]_{\varpi} = (y_1, y_2, \ldots, y_g) \in \mathbb{Z}^g$. This equivalence is both theoretically and computationally : If one question is solved, the another is also solved by changing the basis, which is very easy since we know explicitly the basis change matrix. Finally, we don't actually need to know $w \in W$ such that $w(\lambda) \in \mathcal{C}_+$: We just need to find a vector $v \in \mathcal{C}_+$ such that $v = w(\lambda)$ for some $w \in W$.

Proposition 4.54. Given $[\lambda]_{\varpi} = (y_1, y_2, \ldots, y_g) \in \mathbb{Z}^g$, there is $(\tilde{y_1}, \tilde{y_2}, \ldots, \tilde{y_g}) \in \mathbb{Z}^g_{\measuredangle}$ such that there is $w \in W$ for which we have $[w]_{\varpi} \cdot [\lambda]_{\varpi} \in \mathbb{Z}^g_{\measuredangle}$. To find one such $(\tilde{y_1}, \tilde{y_2}, \ldots, \tilde{y_g}) \in \mathbb{Z}^g_{\measuredangle}$, it takes at most g steps to take absolute values of each y_i and then at most $\frac{g(g-1)}{2}$ steps to sort the g non-negative integers in the sequence $(|y_1|, |y_2|, \ldots, |y_g|)$ to obtain an element in $\mathbb{Z}^g_{\measuredangle}$.

Proof. In Proposition 4.45, we computed w_i. We see that w_i permutates ϖ_i and ϖ_{i+1} but fixes other ϖ_j, for $1 \leq i \leq g-1$. Moreover, w_g just changes ϖ_g to $-\varpi_g$. Using the coordinates with respect to the basis ϖ, this means that $[w_i]_{\varpi} \cdot (y_1, \ldots, y_g)$ exchanges y_i and y_{i+1} for $1 \leq i \leq g-1$, and $[w_g]_{\varpi} \cdot (y_1, \ldots, y_g) = (y_1, y_2, \ldots, -y_g)$. Combine these two facts, we know that we can find an element in W, for each pair (i, j), to exchange y_i and y_j. Also, for any i, there is an element in W to change y_i to $-y_i$: Just exchange y_i and y_g, change y_i (which is at the g-position now) to $-y_i$ using $[w_g]_{\varpi}$, and finally exchange $-y_i$ and y_g again. We mentioned that we don't have to compute $w \in W$, so we don't have to know the elements in W mentioned above. Now it is clear that the operations mentioned in the proposition correspond to actions of elements in the Weyl group W. The claim about the number of steps is clear. □

Remark 4.55. The (at most) g steps to take absolute values y_i is optimal and fast. For the sorting, it can be done much faster using well-known sorting algorithms.

Although we want to make our algorithm of computing irreducible characters fast so we can deal with the cases beyond, say, $g \geq 10$. But we still consider only small g, say $g \leq 20$. So the faster sorting algorithms are not necessary at all in these cases. Also, the question of finding some particular element in $\mathcal{C}_+$ for our algorithm is a special version of the question solved in Proposition 4.54, see (4.6.1). In this case, we will see that we can solve the question in time $O(g)$.

After solving the above general question, we go back to the special question mentioned in (4.6.1). Contrary to the solution for the general question for which we work with the basis ϖ, we work with the basis ϖ for the special question. As we mentioned in the discussion of the general question, we don't need to know $w \in W$, but just a vector $(\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_g) \in \mathbb{Z}^g_{\geq 0}$ such that

$$(\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_g) = [w]_\varpi \cdot [\nu + \lambda + \rho]_\varpi = [w]_\varpi \cdot \begin{pmatrix} x_1 + 1 + (v_1 - v_2) \\ x_2 + 1 + (v_2 - v_3) \\ \vdots \\ x_{g-1} + 1 + (v_{g-1} - v_g) \\ x_g + 1 + (v_g) \end{pmatrix}, \tag{4.6.3}$$

for some $w \in W$. Recall that we have $x_i \in \mathbb{Z}^g_{\geq 0}$ and $v_i \in \{-1, 0, 1\}$, see (4.6.1). Let $y_i = x_i + 1 + (v_i - v_{i+1})$, where $v_{g+1} = 0$.

Lemma 4.56. We have $y_g \geq 0$ and $y_i \geq -1$ for $1 \leq i \leq g-1$. If $y_i = -1$ (hence $i \leq g-1$), we have $y_{i-1} \geq 1$ (if $i > 1$) and $y_{i+1} \geq 1$.

Proof. It clear that $y_i = x_i + 1 + (v_i - v_{i+1}) \geq 0 + 1 + ((-1) - (1)) = -1$, for $1 \leq i \leq g-1$, and $y_i = -1$ if and only if $x_i = 0, v_i = -1$ and $v_{i+1} = 1$. Hence if $y_i = -1$, we have

$$y_{i-1} = x_{i-1} + 1 + (v_{i-1} - v_i) = x_{i-1} + 1 + (v_{i-1} - (-1)) \geq 0 + 1 + (-1 - (-1)) = 1,$$
$$y_{i+1} = x_{i+1} + 1 + (v_{i+1} - v_{i+2}) = x_{i+1} + 1 + (1 - (v_{i+2})) \geq 0 + 1 + (1 - (1)) = 1,$$

where the first inequality is valid for $i > 1$. Similarly, we have $y_g = x_g + 1 + (v_g) \geq 0 + 1 + (-1) \geq 0$. □

Recall that we want to transform the vector $[\nu + \lambda + \rho]_\varpi = (y_1, y_2, \ldots, y_g)$ to $\mathbb{Z}^g_{\geq 0}$ using the matrices $[w]$ with $w \in W$.

Corollary 4.57. Let y_i as above. Assume $y_i < 0$ (hence $i < g$, as shown above). Let

$$(\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_g) = [w_i]_\varpi \cdot (y_1, y_2, \ldots, y_g). \tag{4.6.4}$$

Then $\tilde{y}_i = 1$, $\tilde{y}_{i-1} \geq 0$ (if $i > 1$), $\tilde{y}_{i+1} \geq 0$ and $\tilde{y}_j = y_j$ for all other j.

Proof. From Proposition 4.50, we see that $(\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_g) = [w_i]_\varpi \cdot (y_1, y_2, \ldots, y_g)$ is given by $\tilde{y}_i = -y_i$, $\tilde{y}_{i-1} = y_{i-1} + y_i$, $\tilde{y}_{i+1} = y_i + y_{i+1}$ and $\tilde{y}_j = y_j$ for all other

j. Since we assume $y_i < 0$, Lemma 4.56 implies $y_i = -1$, $y_{i-1} \geq 1$ and $y_{i+1} \geq 1$. The corollary follows easily. □

The above corollary says that we can transform

$$(\dots, y_{i-2}, y_{i-1}, y_i = -1, y_{i+1}, y_{i+2} \dots)$$

to $(\dots, y_{i-2}, y_{i-1} - 1, 1, y_{i+1} - 1, y_{i+2} \dots)$ where $y_{i-1} - 1 \geq 0$ and $y_{i+1} - 1 \geq 0$. If $y_{i-2} < 0$ or $y_{i+2} < 0$ (hence it must be -1), we get $y_{i-1} - 2$ or $y_{i+1} - 2$ after applying Corollary 4.57 again, and this time we don't know anymore if $y_{i-1} - 2 \geq 0$ or $y_{i+1} - 2 \geq 0$. These cases occur when we have $(\dots, -1, y_{i-1}, -1, \dots)$ or $(\dots, -1, y_{i+1}, -1, \dots)$. The following lemma shows that in this situation, we have $y_{i-1} \geq 3$ or $y_{i+1} \geq 3$ respectively. Hence we never fall into an infinite loop of changing sign.

Lemma 4.58. Let y_i as in Lemma 4.56. If $y_{i-1} = -1$ and $y_{i+1} = -1$, we have $y_i \geq 3$.

Proof. As proved in Lemma 4.56, $y_{i-1} = -1$ if and only if $x_{i-1} = 0$, $v_{(i-1)} = -1$ and $v_{(i-1)+1} = 1$. Similarly, $y_{i+1} = -1$ if and only if $x_{i+1} = 0$, $v_{(i+1)} = -1$ and $v_{(i+1)+1} = 1$. Hence $y_i = x_i + 1 + (v_i - v_{i+1}) = x_i + 1 + ((1) - (-1)) \geq 3$. □

Proposition 4.59. Let y_i as in Lemma 4.56. Let $\tilde{y}_i$ defined by

$$\overline{y}_i = \delta_{y_i,-1}\, y_i$$
$$\tilde{y}_i = \overline{y}_{i-1} + |y_i| + \overline{y}_{i+1}$$

Then $(\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_g) \in \mathbb{Z}^g_{\geq 0}$, and it is the image of $(y_1, y_2, \dots, y_g)$ under $[w]_\varpi$ for some $w \in W$.

Proof. In Lemma 4.56, we proved that $y_i < 0$ if and only if $y_i = -1$. Hence $\overline{y_i} = 0$ if $y_i \geq 0$ and $\overline{y_i} = y_i$ if $y_i < 0$. If $y_{i-1} < 0$, Corollary 4.57 says $y_i > 0$, hence $|y_i| = y_i$. In this case, the value $\overline{y}_{i-1} = y_{i-1}$ is added to $|y_i| = y_i$ (and y_{i-2}), as shown in Corollary 4.57, which corresponds to the action of $[w_{i-1}]_\varpi$ (which changes the sign of y_{i-1} also). The same arguments apply to y_{i+1}. This shows that the value $\tilde{y}_i$ is the result of applying $[w_{i-1}]_\varpi$ and/or $[w_{i+1}]_\varpi$ when $y_{i-1} < 0$ and/or $y_{i+1} < 0$. Now assume that $y_{i-1} \geq 0$ and $y_{i+1} \geq 0$. We have $\overline{y_{i-1}} = \overline{y_{i+1}} = 0$. If $y_i \geq 0$, we don't change the value of y_i, hence $\tilde{y}_i = y_i = |y_i| = 0 + |y_i| + 0 = \overline{y_{i-1}} + |y_i| + \overline{y_{i-1}}$. Finally, if $y_i < 0$, we use $[w_i]_\varpi$ to change the sign of y_i, and we still get $\tilde{y}_i = \overline{y_{i-1}} + |y_i| + \overline{y_{i-1}}$. Hence the $(\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_g)$ is obtained from $(y_1, y_2, \dots, y_g)$ under $[w]_\varpi$ for some $w \in W$. $(\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_g) \in \mathbb{Z}^g_{\geq 0}$ is the result of Lemma 4.56, Corollary 4.57 and Lemma 4.58. □

Definition 4.60. For $x = (x_1, x_2, \dots, x_g)$, we define $\sigma(x) = \sum_{i=1}^g x_i$. We define an well-ordering on $\mathbb{Z}^g_{\geq 0}$ as follows : For $x = (x_1, x_2, \dots, x_g)$ and $y = (y_1, y_2, \dots, y_g)$ in $\mathbb{Z}^g_{\geq 0}$, $x < y$ if and only if one of the following two conditions are satisfied :

(1) $\sigma(x) < \sigma(y)$, or

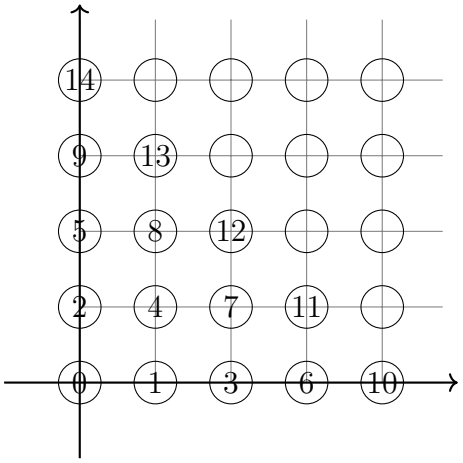
(2) $\sigma(x) = \sigma(y)$ and there exists $1 \leq i \leq g$ such that $x_j = y_j$ for all $j < i$ and $x_i > y_i$.

Be careful that, for the definition $x < y$, the condition in (2) is $x_i > y_i$.

Example 4.61. For $g = 3$, we have

$$\begin{bmatrix}0\\0\\0\end{bmatrix} < \begin{bmatrix}1\\0\\0\end{bmatrix} < \begin{bmatrix}0\\1\\0\end{bmatrix} < \begin{bmatrix}0\\0\\1\end{bmatrix} < \begin{bmatrix}2\\0\\0\end{bmatrix} < \begin{bmatrix}1\\1\\0\end{bmatrix} < \begin{bmatrix}1\\0\\1\end{bmatrix} < \begin{bmatrix}0\\2\\0\end{bmatrix} < \begin{bmatrix}0\\1\\1\end{bmatrix} < \begin{bmatrix}0\\0\\2\end{bmatrix} <$$
$$\begin{bmatrix}3\\0\\0\end{bmatrix} < \begin{bmatrix}2\\1\\0\end{bmatrix} < \begin{bmatrix}2\\0\\1\end{bmatrix} < \begin{bmatrix}1\\2\\0\end{bmatrix} < \begin{bmatrix}1\\1\\1\end{bmatrix} < \begin{bmatrix}1\\0\\2\end{bmatrix} < \begin{bmatrix}0\\3\\0\end{bmatrix} < \begin{bmatrix}0\\2\\1\end{bmatrix} < \begin{bmatrix}0\\1\\2\end{bmatrix} < \begin{bmatrix}0\\0\\3\end{bmatrix} \cdots$$

Example 4.62. For $g = 2$, the order can be visualized as :



For 2 grid points x with label i and y with label j, we have : $x < y$ if and only if $i < j$.

Let λ be a dominant weight and ν be a weight of the fundamental irreducible character χ_l, which corresponds to the (fundamental) dominant weight $\mu = \varpi_l$ whose coordinate is $[\mu]_\varpi = e_l$. As in 87, let $[\lambda]_\varpi = (x_1, x_2, \ldots, x_g) \in \mathbb{Z}^g_{\geq 0}$ and $[\nu]_\varpi = (v_1 - v_2, v_2 - v_3, \ldots, v_{g-1} - v_g, v_g)$ with all $v_k \in \{-1, 0, 1\}$. The weight $\lambda+\rho+\nu$ has coordinate $[\lambda + \rho + \nu]_\varpi = (y_1, y_2, \ldots, y_g)$, where $y_i = x_i+1+(v_i-v_{i+1})$ with the convention $v_{g+1} = 0$. Brauer-Klimyk formula Theorem 4.35, says that we can find $w \in W$ such that $w(\lambda + \rho + \nu)$ is a dominant weight, which is uniquely determined although such w is not unique. Proposition 4.59 tells us the coordinate $[w(\lambda + \rho + \nu)]_\varpi = (\tilde{y}_1, \tilde{y}_1, \ldots, \tilde{y}_g) \in \mathbb{Z}^g_{\geq 0}$. If there is $\tilde{y}_i = 0$, which means that $w(\lambda + \rho + \nu)$ is on the boundary of $\mathcal{C}_+$, then Brauer-Klimyk formula says that such ν has no contribution to the decomposition of $\chi_\mu\chi_\lambda$ in (4.3.14). Hence we will look only those ν such that $[w(\lambda + \rho + \nu)]_\varpi = (\tilde{y}_1, \tilde{y}_1, \ldots, \tilde{y}_g)$ has

the property : $\tilde{y}_i \geq 1$ for all $1 \leq i \leq g$. In this case, the weight $w(\lambda+\rho+\nu)-\rho$ is dominant and its corresponding irreducible character $\chi_{w(\nu+\lambda+\rho)-\rho}$ appears in the decomposition of $\chi_\mu\chi_\lambda$ with multiplicity $(-1)^{l(w)}m(\nu)$, where $m(\nu)$ is the multiplicity of ν in $\chi_\mu = \chi_l$. The dominant weight $\chi_{w(\nu+\lambda+\rho)-\rho}$ has coordinate $\left[\chi_{w(\nu+\lambda+\rho)-\rho}\right]_\varpi = (\tilde{y}_1-1, \tilde{y}_2-1, \ldots, \tilde{y}_g-1)$. We will study these vectors in $\mathbb{Z}^g_{\geq 0}$, which eventually shows that we have a recurrence formula for irreducible characters of $\mathrm{USp}(2g)$. To simplify the presentation, we fix the following notations and conditions (discussed above) :

$$\begin{aligned}
x &= (x_1, x_2, \ldots, x_g) = [\lambda]_\varpi\,,\\
y &= (y_1, y_2, \ldots, y_g) = [\lambda+\rho+\nu]_\varpi\,,\\
\tilde{y} &= (\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_g) = [w(\lambda+\rho+\nu)]_\varpi\,,\\
\hat{y} &= (\hat{y}_1, \hat{y}_2, \ldots, \hat{y}_g) = [w(\lambda+\rho+\nu)-\rho]_\varpi\,,
\end{aligned}$$

where $x_i \geq 0$, $y_i = x_i + 1 + (v_i - v_{i+1})$, $\tilde{y}_i \geq 1$, $\hat{y}_i = \tilde{y}_i - 1 \geq 0$, and $v_i \in \{-1, 0, 1\}$ with $v_{g+1} = 0$. All of these are integers. Finally, since ν is a weight of χ_l, Proposition 4.53 also implies that there are at most l non-zero elements in these v_i.

Lemma 4.63. We have $\sigma(\tilde{y}) = \sigma(y)$ and $\sigma(\hat{y}) = \sigma(x) + v_1$.

Proof. In the proof of Corollary 4.57, we change $(\ldots, y_{i-1}, y_i, y_{i+1}\ldots)$ to $(\ldots, y_{i-1}+y_i, -y_i, y_{i+1}+y_i\ldots)$, if $y_i < 0$, and the other coordinates are not changed. Since $(y_{i-1}+y_i)+(-y_i)+(y_{i+1}+y_i) = y_{i-1}+y_i+y_{i+1}$, the first claim follows. We have $\sigma(\hat{y}) = \sigma(\tilde{y}) - g = \sigma(y) - g = \sigma(x) + g + \sum_{i=1}^g (v_i - v_{i+1}) - g = \sigma(x) + v_1$. □

Lemma 4.64. We have $\sigma([w(\lambda+\rho+\nu)-\rho]_\varpi) \leq \sigma([\lambda+\mu]_\varpi)$, and the equality holds if and only if $v_1 = 1$. In particular, $[w(\lambda+\rho+\nu)-\rho]_\varpi < [\lambda+\mu]_\varpi$ if $v_1 < 1$.

Proof. Recall that $\mu = \varpi_l$, we have $\sigma([\lambda+\mu]_\varpi) = \sigma(x) + 1$. This implies that $\sigma([w(\lambda+\rho+\nu)-\rho]_\varpi) = \sigma(\hat{y}) = \sigma(x) + v_1 \leq \sigma(x) + 1 = \sigma([\lambda+\mu]_\varpi)$. The claim about the equality and the last statement are easy. □

The above discussion focus on a generic weight of the irreducible character χ_l. In this paragraph, we focus on a particular one. From Proposition 4.33 and Theorem 4.34, we know that $\mu = \varpi_l$ is the highest weight of $\chi_l = \chi_{\varpi_l}$ whose multiplicity is 1. The sequence $(v_1, v_2, \ldots, v_g)$ for ϖ_l is just $[\varpi_l]_\varpi$, which is $v_i = 1$ for $i \leq l$ and otherwise 0. This can be seen easily from $[\varpi_l]_\varpi = e_l$ and the basis change matrix in (4.4.44). It is clear that $\lambda+\rho+\varpi_l$ is a dominant weight and not on the boundary of $\mathcal{C}_+$, so we can take w to be the identity element of the Weyl group W, and thus $w(\lambda+\rho+\varpi_l)-\rho = \lambda+\varpi_l = \lambda+\mu$ appears in the right side of the Brauer-Klimyk formula with multiplicity 1. We restrict ourselves here to the group $\mathrm{USp}(2g)$, but this is true in general, by the same reason.

Lemma 4.64 says that the weight $w(\lambda+\rho+\nu)-\rho$, which contributes to the right side of the Brauer-Klimyk formula (4.3.14), is "strictly smaller" than the

wight $\lambda+\mu = \lambda+\varpi_l$ for those ν with $v_1 < 1$. Our next task is to study the situation for those ν with $v_1 = 1$.

Lemma 4.65. Assume that $v_1 = 1$. Let $j = \max\{1 \le i \le g \mid v_i = 1\}$. Then $j \le l$. There is only one ν for which we have $j = l$, which is $\nu = \varpi_l$. For any other ν, we have $[w(\lambda+\rho+\nu)-\rho]_\varpi < [\lambda+\mu]_\varpi$.

Proof. Since $v_1 = 1$, we have $\sigma([w(\lambda+\rho+\nu)-\rho]_\varpi) = \sigma([\lambda+\mu]_\varpi)$ by Lemma 4.64. For $1 \le i \le j-1$, we have $v_i = v_{i+1} = 1$, hence $y_i = x_i+1+(v_i-v_{i+1}) = x_i+1 \ge 1$. For $i = j$, we have $y_j = x_j + 1 + (v_j - v_{j+1}) \ge x_j + 2$, since $v_j = 1$ but $v_{j+1} < 1$. If $y_{j+1} \ge 0$, then $\tilde{y}_j = y_j$. Otherwise $y_{j+1} = -1$, $v_{j+1} = -1$ and we have $\tilde{y}_j = y_j - 1 = x_j + 1 + ((1)-(-1)) - 1 = x_j + 2$. These show that $\hat{y}_i = x_i$ for $1 \le i \le j-1$ and $\hat{y}_j = x_j + 1$. If $j < l$, we have $\hat{y} < x + e_l$ from the definition Definition 4.60, which proves the last claim. The claim about $j \le l$ and the uniqueness of ν such that $j = l$ is mentioned in page 92, which is a consequence of Proposition 4.53. □

The Brauer-Klimyk formula (4.3.14) can be written as

$$\chi_{\mu+\lambda} = \chi_\mu \chi_\lambda - \sum_{\nu \ne \lambda+\mu} (-1)^{l(w)} m(\nu) \chi_{w(\lambda+\rho+\nu)-\rho}. \tag{4.6.5}$$

The multiplicity of $\lambda+\mu$ is 1 is discussed in the paragraph after Lemma 4.64. For the group $\mathrm{USp}(2g)$ and $\mu = \varpi_l$, we have shown that $w(\lambda+\rho+\nu)-\rho$ is "strictly smaller" than $\lambda+\mu$ in the sense $[w(\lambda+\rho+\nu)-\rho]_\varpi < [\lambda+\mu]_\varpi$. We can present our main algorithm in this chapter now :

Algorithm 1 Compute Irreducible Characters of $\mathrm{USp}(2g)$ in $\mathbb{Z}[\chi_1, \dots, \chi_g]$

```
def CHI(x)                                          # χ_λ for [λ]_ϖ = x
  if x ∉ Z^g_{≥0} :                                 # λ must be a dominant weight.
    return 0
  if σ(x) = 0 :                                     # x = (0, ..., 0)
    return 1
  Find smallest 1 ≤ l ≤ g such that x_l ≥ 1
  if σ(x) = 1 :                                     # x = e_l
    return the symbol χ_l                           # Recursive computing
  Set χ̃ = Σ_{ν ≠ ϖ_l} (-1)^{det(w)} m(ν) CHI([w(λ+ρ+ν)-ρ]_ϖ)
  return CHI(e_l) CHI(x - e_l) - χ̃
```

Here ν runs over the weights of χ_l except ϖ_l. These weights and their multiplicity $m(\nu)$ in χ_l are determined by Proposition 4.51 and Proposition 4.53, which are easy to compute. The dominant weight $[w(\lambda+\rho+\nu)-\rho]_\varpi$ is computed using Proposition 4.59. We don't have to find $w \in W$ explicitly, but it is easy to compute using Corollary 4.57. The power $l(w)$ is the number of -1 in the

entries of $[\lambda+\rho+\nu]_{\varpi}$. The algorithm terminates is proved by Lemma 4.64 and Lemma 4.65.

Algorithm 1 computes the irreducible characters of $\mathrm{USp}(2g)$ as polynomials in $\chi_1,\ldots,\chi_g$. Using Proposition 4.51, we obtain their polynomial expressions in $s_1,\ldots,s_g$.

After developing a general recursive algorithm for computing the irreducible characters of $\mathrm{USp}(2g)$, we can present explicit formulas for the cases $g=2$ and $g=3$. The proofs are the results of computations in the previous sections. In following, we define $\chi_{\mathbf{m}}=0$ if any of the m_j in $\mathbf{m}=(m_1,\cdots,m_g)$ is negative. We also define $\epsilon:\mathbb{Z}\to\{0,1\}$ by

$$\epsilon(x)=\begin{cases}0 & \text{if } x=0,\\ 1 & \text{if } x\neq 0.\end{cases}$$

Proposition 4.66. Let $\chi_{(i,j)}$ be the characters computed using Algorithm 1 for $g=2$. We have

$$\begin{aligned}\chi_{(i+1,j)}&=\chi_{(1,0)}\cdot\chi_{(i,j)}-\sum_{v\in S_1}\chi_{(i,j)+v}\,,\\ \chi_{(i,j+1)}&=\chi_{(0,1)}\cdot\chi_{(i,j)}-\sum_{v\in S_2}\chi_{(i,j)+v}-\epsilon(i)\,\chi_{(i,j)}\,,\end{aligned}$$

where (we use both the row and column notation for the indices of χ)

$$\begin{aligned}S_1&=\left\{-\begin{pmatrix}1\\0\end{pmatrix},\pm\begin{pmatrix}1\\-1\end{pmatrix}\right\},\\ S_2&=\left\{-\begin{pmatrix}0\\1\end{pmatrix},\pm\begin{pmatrix}2\\-1\end{pmatrix}\right\}.\end{aligned}$$

Proposition 4.67. Let $\chi_{(i,j,k)}$ be the characters computed using Algorithm 1 for $g=3$. We have

$$\begin{aligned}\chi_{(i+1,j,k)}&=\chi_{(1,0,0)}\cdot\chi_{(i,j,k)}-\sum_{v\in S_1}\chi_{(i,j,k)+v}\,,\\ \chi_{(i,j+1,k)}&=\chi_{(0,1,0)}\cdot\chi_{(i,j,k)}-\sum_{v\in S_2}\chi_{(i,j,k)+v}-\left(\epsilon(i)+\epsilon(j)\right)\,\chi_{(i,j,k)}\,,\\ \chi_{(i,j,k+1)}&=\chi_{(0,0,1)}\cdot\chi_{(i,j,k)}-\sum_{v\in S_3}\chi_{(i,j,k)+v}\\ &\qquad-\epsilon(i)\,\chi_{(i,j,k)\pm(0,1,-1)}-\epsilon(j)\,\chi_{(i,j,k)\pm(1,0,0)}\,,\end{aligned}$$

where (again, we use both the row and column notation for the indices of χ)

$$S_1 = \left\{ -\begin{pmatrix}1\\0\\0\end{pmatrix}, \pm\begin{pmatrix}1\\-1\\0\end{pmatrix}, \pm\begin{pmatrix}0\\1\\-1\end{pmatrix} \right\},$$
$$S_2 = \left\{ -\begin{pmatrix}0\\1\\0\end{pmatrix}, \pm\begin{pmatrix}1\\-2\\1\end{pmatrix}, \pm\begin{pmatrix}1\\-1\\1\end{pmatrix}, \pm\begin{pmatrix}1\\0\\-1\end{pmatrix}, \pm\begin{pmatrix}1\\1\\-1\end{pmatrix}, \pm\begin{pmatrix}2\\-1\\0\end{pmatrix} \right\},$$
$$S_3 = \left\{ -\begin{pmatrix}0\\0\\1\end{pmatrix}, \pm\begin{pmatrix}1\\-1\\0\end{pmatrix}, \pm\begin{pmatrix}2\\-2\\1\end{pmatrix}, \pm\begin{pmatrix}0\\2\\-1\end{pmatrix}, \pm\begin{pmatrix}2\\0\\-1\end{pmatrix} \right\}.$$

Define $T(g,d)$ to be the total number of summands in Step 9 of Algorithm 1 for the computation of all the irreducible characters of $\mathrm{USp}(2g)$ with $\sigma(x) \leq d$. It is a straightforward computation that

$$T(g,d) = \sum_{\tilde{d}=0}^{d} \left(\sum_{\ell=1}^{g} C_{\tilde{d}-1}^{g-\ell+\tilde{d}-1} \cdot \left(1 + \sum_{k=0}^{\ell} \left(\frac{1+(-1)^{k-\ell}}{2} \right) 2^k \, C_k^g \right) \right),$$

where $C_n^m = \binom{m}{n}$ is the binomial coefficient. Here the summation over $\tilde{d}$ starting with $\tilde{d} = 0$ is just for the simpleness of formula. One can prove the inequality, for $d \geq g^2$,

$$T(g,d) \leq e\, 2^{g+1}\, e^{\frac{d}{2}+g} \frac{\Gamma\left(g+2, \frac{d}{2}+g\right)}{\Gamma(g+2)},$$

where $\Gamma(s,z)$ is the incomplete gamma function, which satisfies

$$\lim_{x\to\infty} \frac{\Gamma(s,x)}{x^{s-1}\, e^{-x}} = 1.$$

The number of $x = (x_1, x_2, ..., x_g)$ for which $\sigma(x) \leq d$ is C_d^{g+d}. We define the average complexity per character for Algorithm 1 to compute all the irreducible characters of $\mathrm{USp}(2g)$ up to a unweighted degree $d \geq g^2$ by

$$t(g,d) = \frac{T(g,d)}{C_d^{g+d}}.$$

Using the above results, we obtain

$$\lim_{d\to\infty} \frac{t(g,d)}{d} \leq \frac{\sqrt{2\pi} e^{1-g} g^g \sqrt{g}}{(g+1)!}.$$

We have proved

Proposition 4.68. For any fixed genus g, the average time $t(g,d)$ per character of Algorithm 1 is $O(d)$. Furthermore, the "constant" factor behind this Big-O, which depends on g, is at most $\frac{\sqrt{2\pi}e^{1-g}g^g\sqrt{g}}{(g+1)!} \approx \frac{e}{g}$.

4.7 Explicit computation of Frobenius distributions

In Section 4.5, we apply the Brauer-Klimyk formula (Theorem 4.35) to develop an algorithm to compute the irreducible characters of $\mathrm{USp}(2g)$, in terms of the symmetric polynomials $s_1, s_2, \ldots, s_g$ in $t_1, t_2, \ldots, t_g$. See Section 4.5 for these notations, in particular the paragraph above Proposition 4.51. The motivation comes from using irreducible characters to study Sato-Tate groups, see Section 3.5.2. In this section, we work with some examples of families of genus 2 and genus 3 curves.

4.7.1 Generic curves : heuristic behavior in the genus

In this section, we consider a generic hyperelliptic curve of genus g whose Sato-Tate group is $\mathrm{USp}(2g)$. We consider the trivial character and the fundamental irreducible characters of $\mathrm{USp}(2g)$. These are the irreducible characters corresponding to the dominant weights whose vector representation $\mathbf{m} = (m_1, \cdots, m_g)$ with respect to the fundamental dominant weights satisfying $m_1+m_2+\ldots+m_g \leq 1$. For $g = 2$ and $g = 3$, their expressions in s_i can be found in Example 4.17 and Example 4.18.

Assume we have a Frobenius action F_q for a genus g curve over $\mathbb{F}_q$ whose characteristic polynomial is given by

$$P(x) = x^{2g} + a_1 x^{2g-1} + \cdots + a_{2g-1}x + q^g\,. \tag{4.7.1}$$

For $g = 2$, we then have $s_1 = -a_1/\sqrt{q}$ and $s_2 = (a_2 - 2q)/q$. For $g = 3$, we have $s_1 = -a_1/\sqrt{q}$, $s_2 = (a_2 - 3q)/q$ and $s_3 = (-a_3 + 2a_1q)/q^{3/2}$. For an irreducible character χ, which is expressed in s_i, we then define $\chi(F_q)$ to be the value of χ when s_i are assigned the above values.

Let $\{F_x\}_{x\in X}$ be the sample space of Frobenius that we are interested. For two irreducible characters χ_1 and χ_2 of $\mathrm{USp}(2g)$ and a finite subset A of X, we define $\epsilon(\chi_1, \chi_2, A) = \frac{1}{\#A}\sum_{x\in A}\chi_1(F_x)\chi_2(F_x)$. This is the sample mean of the inner product of χ_1 and χ_2 over the subset $\{F_x\}_{x\in A}$ of samples. For an closed subgroup H of $\mathrm{USp}(2g)$, we define $\mathrm{err}_H(\chi_1, \chi_2, A) = \epsilon(\chi_1, \chi_2, A) - \langle\chi_1, \chi_2\rangle_H$, where $\langle\chi_1, \chi_2\rangle_H$ is the inner product of the restriction $\chi_1|_H$ and $\chi_2|_H$ with respect to the Haar measure of H. If H is the Sato-Tate group for the Frobenius distribution $\{F_x\}_{x\in X}$, then we expect that $\lim_{A\to X}\mathrm{err}_H(\chi_1, \chi_2, A) = 0$ for any χ_1 and χ_2, where the limit is taken over the subset of X under the partial order of inclusion. Given

a set of irreducible characters $\{\chi_i\}_{i\in I}$, we define $\mathrm{Err}_H(I,A)$ to be the maximum $\max_{i,j\in I}|\mathrm{err}_H(\chi_i,\chi_j,A)|$.

Assume that we consider curves over the rational field. Let $(p_1,p_2,\ldots,p_n,\ldots)$ be the sequence of primes of good reduction for a curve, determined by the usual order on $\mathbb{N}$. For a positive integer n and two irreducible characters χ_1 and χ_2, we define $\epsilon(\chi_1,\chi_2,n)=\frac{1}{n}\sum_{k=1}^{n}\chi_1(F_{p_k})\chi_2(F_{p_k})$. Similarly, we define $\mathrm{err}_H(\chi_1,\chi_2,n)=\epsilon(\chi_1,\chi_2,n)-\langle\chi_1,\chi_2\rangle_H$. We also have $\mathrm{Err}_H(I,n)$ for a set of irreducible characters $\{\chi_i\}_{i\in I}$, and we simply write $\mathrm{Err}(n)$ when the subgroup H and the set I is understood.

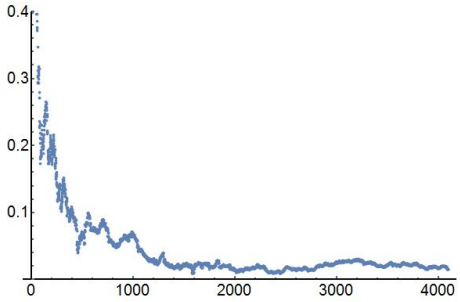
In this section, we are interested in the Frobenius distributions which are determined the by Haar measure of $G=\mathrm{USp}(2g)$, hence the inner product $\langle\chi_1,\chi_2\rangle_G=1$ if $\chi_1=\chi_2$, otherwise $\langle\chi_1,\chi_2\rangle_G=0$. We also restrict ourselves to the trivial and fundamental irreducible characters.

We will investigate how $\mathrm{Err}(n)$ converges to 0 when $n\to 0$. We also consider the (sample) standard deviation of errors

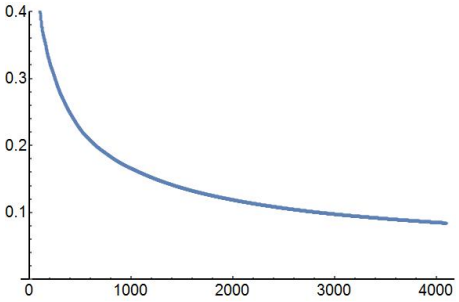
$$\mathrm{SErr}(n)=\sqrt{\frac{\sum_{k=1}^{n}\mathrm{Err}(k)^2}{n}},$$

which is just the (sample) standard deviation of the points in the sequence $(\mathrm{Err}(k))_{k=1}^{n}$. This quantity measures the stability of the convergence.

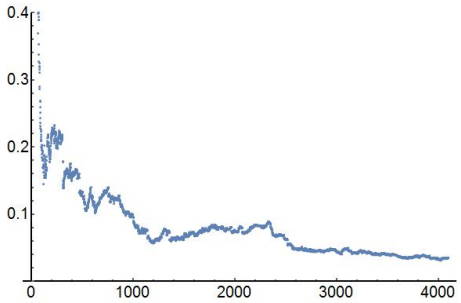
For $g=2,3,4,5$ and 6, we choose the hyperelliptic curve $y^2=x^{2g+1}+x+1$. We plot $\mathrm{Err}(n)$ and $\mathrm{SErr}(n)$ for $n=1,2,\ldots,4096$. These data demonstrate empirically that the errors don't increase when g grows.



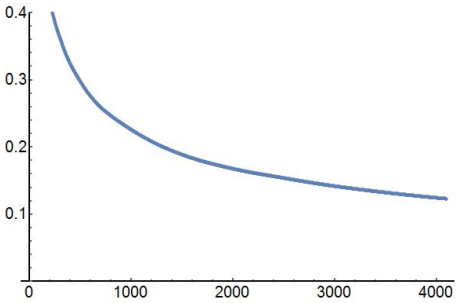
$g=2$, $\mathrm{Err}(n)$



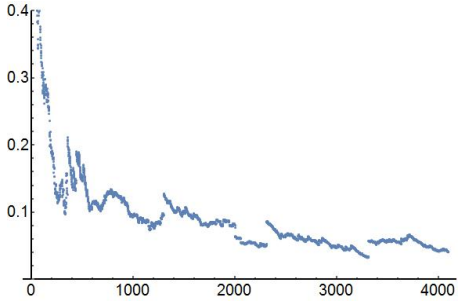
$g=2$, $\mathrm{SErr}(n)$



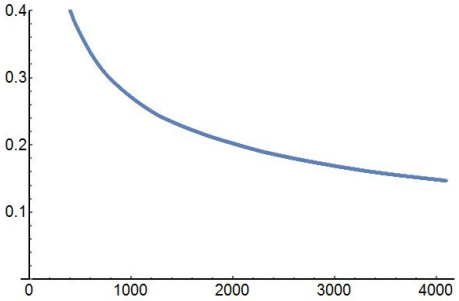
$g = 3$, $\mathrm{Err}(n)$



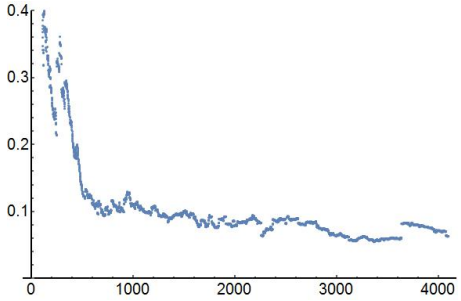
$g = 3$, $\mathrm{SErr}(n)$



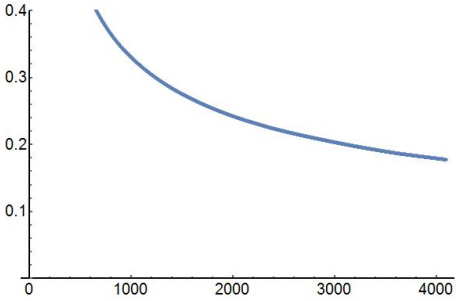
$g = 4$, $\mathrm{Err}(n)$



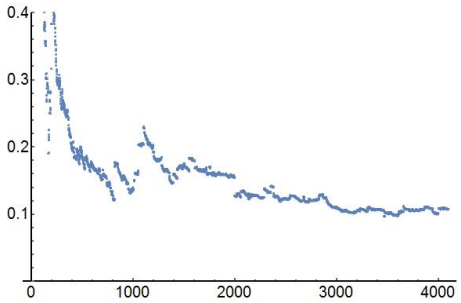
$g = 4$, $\mathrm{SErr}(n)$



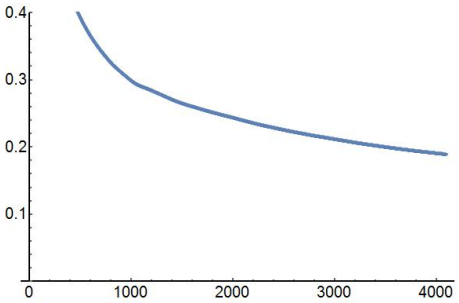
$g = 5$, $\mathrm{Err}(n)$



$g = 5$, $\mathrm{SErr}(n)$



$g = 6$, $\mathrm{Err}(n)$



$g = 6$, $\mathrm{SErr}(n)$

4.7.2 Moment sequences vs. orthogonality relations

In this section, we compare the approach using inner products of irreducible characters to moment sequences.

Let $P(X)$ be a Weil polynomial as in (4.7.1), we write its normalized Weil polynomial $P(\sqrt{q}x)/q^g$ as $\bar{P}(x) = x^{2g} + \bar{a}_1 x^{2g-1} + \bar{a}_2 x^{2g-2} + \cdots + \bar{a}_{2g-1}x + 1$. We have $\bar{a}_i = \bar{a}_{2g-i}$ for all $1 \leq i \leq 2g-1$. When the Frobenius distribution is determined by a subgroup H of $\mathrm{USp}(2g)$, we can study the moment sequences of $\bar{a}_1, \bar{a}_2, \ldots$ and $\bar{a}_g$ with respect to the Haar measure on H. For $g = 2$, a complete list of these moment sequences can be found in Sutherland's webpage [Sut]. For the group $\mathrm{USp}(4)$, the moments is given in the left side of Table 4.6.

We work with the hyperelliptic curve $y^2 = x^5 + x + 1$. For a positive integer N, we compute the sample moments of $\bar{a}_1$ and $\bar{a}_2$ using N sample points of Frobenius. Table 4.6 gives the comparison of the expected values and the numerical values for $N = 2^{12}$ and $N = 2^{16}$. It shows that beyond $n = 5$, even for 2^{16} sample points, we don't have useful approximations of $M_n[\bar{a}_1]$ and $M_n[\bar{a}_2]$.

n	$N = 2^{12}$	$N = 2^{16}$	$N = \infty$
1	0.002	0.006	0
2	0.984	0.996	1
3	0.046	−0.001	0
4	2.833	2.970	3
5	0.196	−0.128	0
6	12.306	13.743	14
7	0.397	−1.487	0
8	66.441	81.446	84
9	−3.853	−14.304	0
10	409.298	565.972	594

$M_n[\bar{a}_1]$

n	$N = 2^{12}$	$N = 2^{16}$	$N = \infty$
1	0.989	0.999	1
2	1.964	1.992	2
3	3.815	3.966	4
4	9..250	9.853	10
5	23.747	26.423	27
6	67.907	79.611	82
7	205.367	257.730	268
8	658.293	893.546	940
9	2192.789	3257.407	3476
10	7550.758	12387.749	13448

$M_n[\bar{a}_2]$

Table 4.6 – Moments for $g = 2$, $\mathrm{USp}(4)$, $y^2 = x^5 + x + 1$

Now we consider the inner products of the irreducible characters of $\mathrm{USp}(4)$ whose weight vector representation $\mathbf{m} = (m_1, m_2)$ satisfy $m_1 + m_2 \leq 2$. There are 6 such characters and they are given in Example 4.17. Using the order given in Example 4.62, we use χ_i for $0 \leq i \leq 5$ to denote them, rather than using the vector $\mathbf{m}$. The expected value of $\langle \chi_i, \chi_j \rangle$ is δ_{ij}. We use N sample points of Frobenius of the same curve to compute the sample mean of $\langle \chi_i, \chi_j \rangle$, and compare them with the expected values. For $N = 2^{10}$ and $N = 2^{12}$, the results is given in Table 4.7. Compared with Table 4.6, we see the numerical inner products approximate very well to the expected values, even using only 2^{10} sample points.

0	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5
χ_0	1.000	−0.037	0.003	0.004	−0.021	−0.050
χ_1	−0.037	1.007	−0.058	−0.095	−0.057	−0.017
χ_2	0.003	−0.058	0.954	−0.006	−0.091	−0.038
χ_3	0.004	−0.095	−0.006	0.928	−0.054	−0.071
χ_4	−0.021	−0.057	−0.091	−0.054	0.879	−0.075
χ_5	−0.050	−0.017	−0.038	−0.071	−0.075	0.947

$N = 2^{10}$

0	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5
χ_0	1.000	−0.002	−0.010	−0.004	−0.012	−0.009
χ_1	−0.002	0.984	−0.015	−0.028	−0.049	−0.014
χ_2	−0.010	−0.015	0.986	−0.040	−0.030	−0.059
χ_3	−0.004	−0.028	−0.040	0.959	0.008	−0.046
χ_4	−0.012	−0.049	−0.030	0.008	0.898	−0.019
χ_5	−0.009	−0.014	−0.059	−0.046	−0.019	0.980

$N = 2^{12}$

Table 4.7 – Inner products for $g = 2$, $\mathrm{USp}(4)$, $y^2 = x^5 + x + 1$

4.7.3 Generic curves : heuristic behavior in the degree

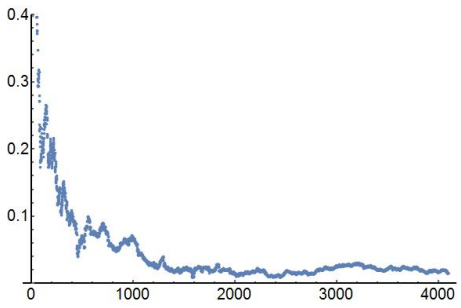
In this section, we continue to consider the representative hyperelliptic curve $y^2 = x^5 + x + 1$ over $\mathbb{Q}$. Let $d \geq 1$ be an integer. We consider the trivial character and the irreducible characters of $\mathrm{USp}(4)$ whose corresponding dominant weights have vector representation $\mathbf{m} = (m_1, m_2)$ satisfy $m_1 + m_2 \leq d$. We study how the errors behave when the (total) degree d grows.

We use the same notation $\mathrm{Err}(n)$ as in Section 4.7.1, however here we use more and more irreducible characters, when Section 4.7.1 focus only on $d = 1$. The following table demonstrates that the errors do increase when d increases, but in a rather slow speed. Let $\#(d)$ be the number of irreducible characters for which $m_1 + m_2 \leq d$, we have $\#(d) = \frac{(d+2)(d+1)}{2}$. We obtain :

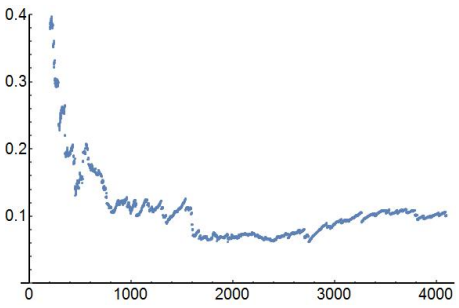
d	1	2	3	4	5	6
$\#(d)$	3	6	10	15	21	28
$\mathrm{Err}(2^{12})$	0.0155	0.1010	0.1893	0.2105	0.2105	0.2105
$\mathrm{Err}(2^{14})$	0.0060	0.0256	0.0378	0.0711	0.0988	0.1425

Table 4.8 – Error's behavior in d for $g = 2$

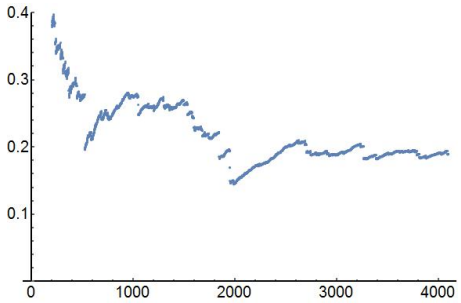
The following table demonstrates the relation between the error function $\mathrm{Err}(n)$ and the degree d in a global view.



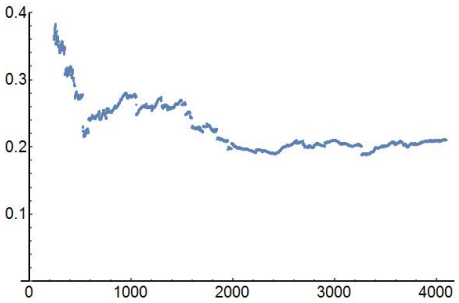
$d = 1$, $\mathrm{Err}(n)$



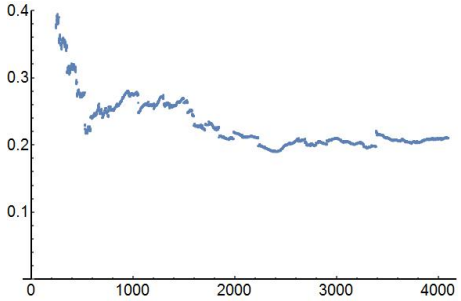
$d = 2$, $\mathrm{Err}(n)$



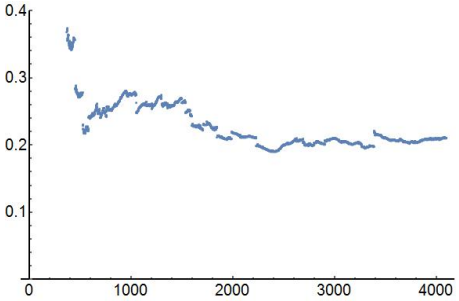
$d = 3$, $\mathrm{Err}(n)$



$d = 4$, $\mathrm{Err}(n)$



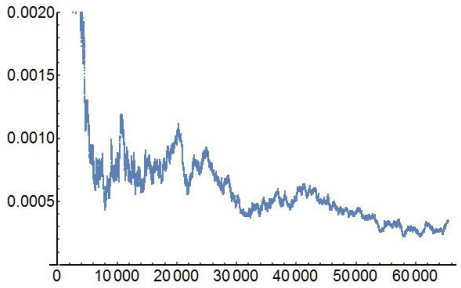
$d = 5$, $\mathrm{Err}(n)$



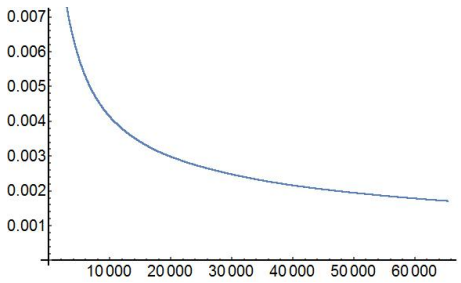
$d = 6$, $\mathrm{Err}(n)$

4.7.4 Generic curves : heuristic behavior in the sample size

The behavior of errors in the sample size n is nontrivial to determine experimentally. In particular, we need to compute many samples in order to obtain a more confident guess of the answer. Hence we choose the elliptic $E : y^2 = x^3 + x + 1$ as our example. We compute 2^{26} Frobenius and plot the function $\mathrm{Err}(n)$ for $n = 2^{10}\,k$, $k = 1, 2, \ldots, 2^{16}$. The following table shows the pictures of $\mathrm{Err}(2^{10}\,k)$ and $\mathrm{SErr}(2^{10}\,k)$:

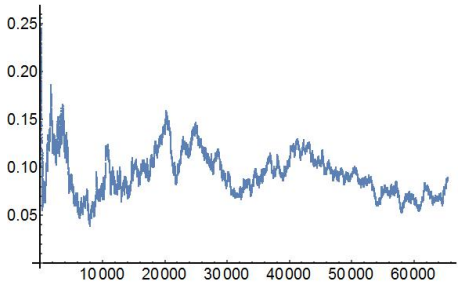


$g = 1,\ \mathrm{Err}(2^{10}\,k)$

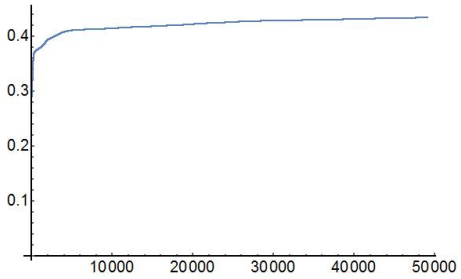


$g = 1,\ \mathrm{SErr}(2^{10}\,k)$

It is difficult to have a clear idea how $\mathrm{Err}(n)$ behaves in n, but the "average" error $\mathrm{SErr}(n)$ provides an insight. The table below is for the functions of $\mathrm{Err}(2^{10}\,k)$ and $\mathrm{SErr}(2^{10}\,k)$, multiplied by $\sqrt{k}$.



$g = 1,\ \sqrt{k}\,\mathrm{Err}(2^{10}\,k)$



$g = 1,\ \sqrt{k}\,\mathrm{SErr}(2^{10}\,k)$

The picture on the left side still has oscillation, but the picture of $\sqrt{k}\,\mathrm{SErr}(2^{10}\,k)$ suggests that it converges to a constant. After a change to the variable n, one may guess $\mathrm{SErr}(n) \approx \frac{32c}{\sqrt{n}}$. If this is correct and can be proved, since $\mathrm{SErr}(n)$ is the standard deviation of $\mathrm{Err}(n)$, we should have the same order of magnitude for $\mathrm{Err}(n)$.

4.7.5 Strategy for non-generic curves

Given a curve of genus g, we can always compute a set of Frobenius and use the irreducible characters χ of $\mathrm{USp}(2g)$ to make a table as we did above. If C has a proper subgroup H of $\mathrm{USp}(2g)$ as its Sato-Tate group, the table gives approximated values of the inner products $\langle \chi_1|_H, \chi_2|_H \rangle_H$, where the inner product is given by the Haar measure on H. The inner product is determined by the decomposition of $\chi|_H$ into irreducible characters of H, i.e the branching rule from

$\mathrm{USp}(2g)$ to H. For different groups, they must have different tables of expected values.

On the other hand, instead of using the irreducible characters of $\mathrm{USp}(2g)$, we can work with the irreducible characters of the subgroup H directly. This gives a matrix whose entries are small integers, and usually it is a diagonal matrix or even the identity matrix. Instead of using the irreducible characters for $\mathrm{USp}(2g)$, we propose to precompute the irreducible characters for each potential group H and verify empirically that their inner products converge to the expect matrix of orthogonality relations for H.

A natural question is raised : Which strategy is better ? We will answer this question by an example in this section. Consider the family of genus 3 curves that we consider in Chapter 2. The automorphism groups of such curves contain an involution, and they admit a representation $y^4+g(x)y^2+h(x)$ with $\deg(g) \leq 2$ and $\deg(h) \leq 4$. Let C be a curve in this family. It admits a degree 2 map to the elliptic curve E defined by $y^2 + g(x)y + h(x)$. The map is given by $\pi : C \to E$, $(x, y) \mapsto (x, y^2)$. See Section 2.5 for more information. This gives a decomposition $0 \to A \to \mathrm{Jac}(C) \xrightarrow{\pi_*} E \to 0$ of abelian varieties, where A is the kernel of π_*. For any Frobenius action $F_{p,C}$ on C, we obtain a pair $(F_{p,E}, F_{p,A})$ of Frobenius on E and C and their characteristic polynomials satisfy $P_{p,C} = P_{p,E}P_{p,A}$.

The Frobenius distribution of C gives Frobenius distributions on the elliptic curve E and the abelian surface A. In this section, we consider the distribution of Frobenius for the family of curves, not just a single particular curve, and we use only primes of good reduction less than or equal to 47.

For the elliptic curve factor, we use the irreducible characters of $\mathrm{SU}(2)$ to produce the table, and we obtain

1.00	0.07	−0.01	0.00	0.00	0.00
0.07	0.99	0.07	−0.01	0.00	0.00
−0.01	0.07	0.99	0.07	−0.01	0.00
0.00	−0.01	0.07	0.99	0.07	−0.01
0.00	0.00	−0.01	0.07	0.99	0.06
0.00	0.00	0.00	−0.01	0.06	0.92

Table 4.14 – Using $\mathrm{SU}(2)$

For the abelian surface factor, we use the irreducible characters of $\mathrm{USp}(4)$ to produce the table, and we obtain

1.00	0.00	−0.06	0.07	0.00	0.02
0.00	1.01	0.00	0.00	0.01	0.00
−0.06	0.00	1.09	−0.01	0.00	−0.09
0.07	0.00	−0.01	1.02	0.00	0.07
0.00	0.01	0.00	0.00	1.06	0.00
0.02	0.00	−0.09	0.07	0.00	1.08

Table 4.15 – Using $\mathrm{USp}(4)$

The above 2 tables suggest that the 2 distributions on elliptic curve factor and abelian surface factor are determined by $\mathrm{SU}(2)$ and $\mathrm{USp}(4)$, i.e. both of them are the generic cases.

If we consider the distribution of $F_{p,C}$ and use the irreducible characters of $\mathrm{USp}(6)$, we obtain

1.00	0.07	0.94	−0.27	0.07	−0.16
0.07	2.01	−0.35	0.95	−0.06	2.04
0.94	−0.35	3.00	−0.31	1.06	−1.16
−0.27	0.95	−0.31	2.13	−0.70	2.05
0.07	−0.06	1.06	−0.70	3.07	−1.16
−0.16	2.04	−1.16	2.05	−1.16	6.24

Table 4.16 – Using $\mathrm{USp}(6)$

1	0	1	0	0	0
0	2	0	1	0	2
1	0	3	0	1	−1
0	1	0	2	−1	2
0	0	1	−1	3	−1
0	2	−1	2	−1	6

(4.17.a) Rounded values

1	0	1	0	0	0
0	2	0	1	0	2
1	0	3	0	1	0
0	1	0	2	0	2
0	0	1	0	3	0
0	2	0	2	0	6

(4.17.b) Expected values

We obtain negative numbers on the left side of the above table, which should not appear, and they are caused by the very few primes used to produce the samples. However, the distribution of $F_{p,C}$ should be determined by $\mathrm{SU}(2) \times \mathrm{USp}(4)$, as we have seen that this is true on both factors. However, the above verifications is not sufficient to support our guess. We need to verify that the distributions on elliptic curve factor and abelian surface factor are independent. Hence we use the products of the first 4 irreducible characters of $\mathrm{SU}(2)$ and $\mathrm{USp}(4)$ as our test functions. These are the irreducible characters of the Lie group $\mathrm{SU}(2) \times \mathrm{USp}(4)$. We then obtain a table :

1	0.1	0	0	0	0	0	0	−0.1	−0.3	0	0	0.1	0	0	0
0.1	1	0.1	0	0	0	0	0	−0.3	−0.1	−0.3	0	0	0.1	0	0
0	0.1	1	0.1	0	0	0	0	0	−0.3	−0.1	−0.3	0	0	0.1	0
0	0	0.1	1	0	0	0	0	0	0	−0.3	−0.1	0	0	0	0.1
0	0	0	0	1	−0.2	0	0	0	0	0	0	0	0	0	0
0	0	0	0	−0.2	1	−0.2	0	0	0	0	0	0	0	0	0
0	0	0	0	0	−0.2	1	−0.2	0	0	0	0	0	0	0	0
0	0	0	0	0	0	−0.2	1	0	0	0	0	0	0	0	0
−0.1	−0.3	0	0	0	0	0	0	1	0.1	0	0	0	−0.3	0	0
−0.3	−0.1	−0.3	0	0	0	0	0	0.1	1	0.1	0	−0.3	0	−0.2	0
0	−0.3	−0.1	−0.3	0	0	0	0	0	0.1	1	0.1	0	−0.2	0	−0.2
0	0	−0.3	−0.1	0	0	0	0	0	0	0.1	1	0	0	−0.2	0
0.1	0	0	0	0	0	0	0	0	−0.3	0	0	1	−0.2	0	0
0	0.1	0	0	0	0	0	0	−0.3	0	−0.2	0	−0.2	1	−0.1	0
0	0	0.1	0	0	0	0	0	0	−0.2	0	−0.2	0	−0.1	1	−0.1
0	0	0	0.1	0	0	0	0	0	0	−0.2	0	0	0	−0.1	1

Table 4.18 – Using $\mathrm{SU}(2) \times \mathrm{USp}(4)$

This supports that the Sato-Tate group for the family of curves in Chapter 2 is $\mathrm{SU}(2)\times\mathrm{USp}(4)$. Moreover, this example demonstrates that the irreducible characters of a subgroup H gives a much good convergence than using the restriction of irreducible characters of $\mathrm{USp}(2g)$ to H.

Our family admits a decomposition of the Jacobian of curves. But in general, we may not have such decomposition. However, the Frobenius distributions for curves with real multiplications behave like a totally split Jacobian, but there is no splitting in general. In this case, we should use the character theory of $\mathrm{SU}(2)^g$.

Conclusion : We should use the character theory for the smallest group we know containing the Sato-Tate group.

4.8 Conclusion

We have developed a systematic way for the computation of irreducible characters of $\mathrm{USp}(2g)$ in terms of the coefficients s_i of the real Weil polynomial as defined in Section 3.4. The main tool is the Brauer-Klimyk formula (see Theorem 4.35), which we express as the recurrence relation (4.6.5). Hence we obtain the recursive Algorithm 1 for the computation of irreducible characters, which is much faster than the naive Algorithm 4.15 in Section 4.2. Although we work with $\mathrm{USp}(2g)$, the algorithm can be modified to compute the irreducible characters of other compact Lie groups. In fact, the Brauer-Klimyk formula is already used in Sage to decompose tensor products of two irreducible representations into direct sum of irreducible representations, and it works with a wide collection of classical and exceptional Lie groups (see the Sage documentation [BSS]). However, using the Brauer-Klimyk formula in the form of Algorithm 1 is new.

The use of orthogonality relations of irreducible characters provides a new perspective to the study of Sato-Tate groups. Even for elliptic curves, Table 3.3 and Table 3.7 already show that the approach using moment sequences needs more sample points to obtain good approximations of moments. The approach using orthogonality relations of irreducible characters has very good approximations to the expected values even with only 1024 sample points, as we see in Table 3.7. However, there are only three Sato-Tate groups for elliptic curves, so moment sequences can be used to identify the Sato-Tate groups quickly. Moreover, the point counting for elliptic curves is very fast, in particular in time $\tilde{O}(\log(q)^5)$ where q is the cardinality of the base field. So the advantages of using irreducible characters is not significant for $g = 1$.

However, since the moments become large when g increases and the number of Sato-Tate groups also become numerous, we need much more sample points to identify the Sato-Tate groups of curves with genus $g \geq 2$. Furthermore, for $g \geq 2$, the point counting using Monsky-Washnitzer cohomology is in exponential time in $\log(p)$ where p is the characteristic of the base field. Thus the time required to understand the Sato-Tate groups become much greater for higher genus.

Our new approach using inner products of irreducible characters of $\mathrm{USp}(2g)$ shows significant advantages for $g{\geq}2$. In Section 4.7.1, the analysis of empirical data shows that the errors of the expected values and experimental values do not increase when the genus g increase. In Section 4.7.2, we show that our new approach requires many fewer sample points (4096 is enough) to identify the Sato-Tate group $\mathrm{USp}(4)$ in contrast to the approach using moment sequences. The examples in Section 4.7.3 show that the errors increase very slow when the number of irreducible characters increases. Moreover, we obtain an empirical upper bound of the errors between the numerical values and expected values in Section 4.7.4, which is $O(\frac{1}{\sqrt{n}})$, where n is the number of samples. The empirical results that a surprisingly small sample size suffices to characterize the Sato-Tate group, as shown in the previous subsections, is consistent with this complexity estimate.

In Section 4.7.5, we demonstrate that it is better to use the character theory of the smallest group we know containing the Sato-Tate group. When we study families of curves with particular structures, like RM curves, this is very useful. This way, the tables of inner products we obtain always have small integer entries. Combine the results in Section 4.7.4, we believe that a small size of sample points is enough not only for the generic case, but also for all of the possible connected (components of) Sato-Tate groups. Furthermore, in the cases where we don't know the structure of a target curve or family, we can start with the irreducible characters of $\mathrm{USp}(2g)$. It is very likely that we get useful information from them, but without a very good convergence to distinguish the Sato-Tate group from just a few possible candidates. Then we use the character theory for these possible groups to find out the actual one.

We have established the necessary tools in this thesis and we have seen the

heuristic advantages of this new method. I expect to complete a further study of Sato-Tate groups using this method, in particular for $g = 2$ and $g = 3$, along with more interesting applications.

Bibliographie

[Art21] E. Artin. *Quadratische Körper im Gebiete der höheren Kongruenzen.* German. Jahrb. phil. Fak. Leipzig 1921, II. Halbjahr 157-165. (Dissertationsauszug.) (1921). 1921 (cit. on p. 10).

[Art24] E. Artin. « Quadratische Körper im Gebiete der höheren Kongruenzen I. (Arithmetischer Teil.) II. (Analytischer Teil.). » German. In: *Math. Z.* 19 (1924), pp. 153–206, 207–246. ISSN: 0025-5874 ; 1432-1823/e. DOI: 10.1007/BF01181074 (cit. on p. 10).

[Atk92] Arthur Oliver L Atkin. *The number of points on an elliptic curve modulo a prime (II)*. Draft. 1992 (cit. on p. 15).

[Bar+11] Tom Barnet-Lamb, David Geraghty, Michael Harris, et al. « A family of Calabi-Yau varieties and potential automorphy. II. » English. In: *Publ. Res. Inst. Math. Sci.* 47.1 (2011), pp. 29–98. ISSN: 0034-5318 ; 1663-4926/e. DOI: 10.2977/PRIMS/31 (cit. on p. 54).

[Bil99] Patrick Billingsley. *Convergence of probability measures. 2nd ed.* English. 2nd ed. Chichester : Wiley, 1999, pp. x + 277. ISBN: 0-471-19745-9 (cit. on p. 48).

[Bog07] V. I. Bogachev. *Measure theory. Vol. I and II.* English. Berlin : Springer, 2007, pp. xvii + 500. ISBN: 978-3-540-34513-8/hbk (cit. on p. 44).

[Bom74] Enrico Bombieri. *Counting points on curves over inite fields (d'apres S. A. Stepanov)*. English. Sem. Bourbaki 1972/73, Expose No.430, Lect. Notes Math. 383, 234-241 (1974). 1974 (cit. on p. 10).

[Bum13] Daniel Bump. *Lie groups. 2nd ed.* English. 2nd ed. New York, NY : Springer, 2013, pp. xiii + 551. ISBN: 978-1-4614-8023-5/hbk ; 978-1-4614-8024-2/ebook. DOI: 10.1007/978-1-4614-8024-2 (cit. on pp. 67, 68, 70, 72).

[BSS] Daniel Bump, Ben Salisbury, and Anne Schilling. *Lie Methods and Related Combinatorics in Sage*. URL: http://doc.sagemath.org/html/en/thematic_tutorials/lie/weyl_character_ring.html (cit. on p. 106).

[Cas06] Wouter Castryck. « Point counting on nondegenerate curves. » PhD thesis. Katholieke Universiteit Leuven, 2006 (cit. on p. 18).

[Coh+06] Henri Cohen, Gerhard Frey, Robero M. Avanzi, et al. *Handbook of elliptic and hyperelliptic curve cryptography*. English. Boca Raton, FL : Chapman & Hall/CRC, 2006, pp. xxxiv + 808. ISBN: 1-58488-518-1/hbk ; 978-1-4200-3498-1/ebook. DOI: 10.1201/9781420034981 (cit. on p. 14).

[Del73] Pierre Deligne. « La conjecture de Weil. I. » French. In: *Publ. Math., Inst. Hautes Étud. Sci.* 43 (1973), pp. 273–307. ISSN: 0073-8301 ; 1618-1913/e. DOI: 10.1007/BF02684373 (cit. on p. 11).

[Del75] Pierre Deligne. « La conjecture de Weil. I. » Russian. In: *Usp. Mat. Nauk* 30.5(185) (1975), pp. 159–190. ISSN: 0042-1316 ; 2305-2872/e (cit. on p. 11).

[Del80] Pierre Deligne. « La conjecture de Weil. II. » French. In: *Publ. Math., Inst. Hautes Étud. Sci.* 52 (1980), pp. 137–252. ISSN: 0073-8301 ; 1618-1913/e. DOI: 10.1007/BF02684780 (cit. on p. 11).

[DV06] Jan Denef and Frederik Vercauteren. « Counting points on C_{ab} curves using Monsky-Washnitzer cohomology. » In: *Finite Fields Appl.* 12.1 (2006), pp. 78–102. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2005.01.003. URL: http://dx.doi.org/10.1016/j.ffa.2005.01.003 (cit. on pp. 18, 31).

[Deu41a] Max Deuring. « Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. » German. In: *Abh. Math. Semin. Univ. Hamb.* 14 (1941), pp. 197–272. ISSN: 0025-5858 ; 1865-8784/e. DOI: 10.1007/BF02940746 (cit. on p. 16).

[Deu41b] Max Deuring. « Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. » German. In: *Abh. Math. Semin. Univ. Hamb.* 14 (1941), pp. 197–272. ISSN: 0025-5858 ; 1865-8784/e. DOI: 10.1007/BF02940746 (cit. on p. 54).

[Dwo60] Bernard Dwork. « On the rationality of the zeta function of an algebraic variety. » English. In: *Am. J. Math.* 82 (1960), pp. 631–648. ISSN: 0002-9327 ; 1080-6377/e. DOI: 10.2307/2372974 (cit. on pp. 11, 16).

[Elk73] Renée Elkik. « Solutions d'équations à coefficients dans un anneau hensélien. » French. In: *Ann. Sci. Éc. Norm. Supér. (4)* 6 (1973), pp. 553–603. ISSN: 0012-9593 (cit. on p. 19).

[FKZ14] Eugene A. Feinberg, Pavlo O. Kasyanov, and Michael Z. Zgurovsky. « Convergence of probability measures and Markov decision models with incomplete information. » English. In: *Proc. Steklov Inst. Math.* 287 (2014), pp. 96–117. ISSN: 0081-5438 ; 1531-8605/e. DOI: 10.1134/S0081543814080069 (cit. on p. 49).

[Fit+12] Francesc Fité, Kiran S. Kedlaya, Victor Rotger, et al. « Sato-Tate distributions and Galois endomorphism modules in genus 2. » English. In: *Compos. Math.* 148.5 (2012), pp. 1390–1442. ISSN: 0010-437X ; 1570-5846/e. DOI: 10.1112/S0010437X12000279 (cit. on p. 56).

[GG01] Pierrick Gaudry and Nicolas Gürel. « An extension of Kedlaya's point-counting algorithm to superelliptic curves. » In: *Advances in cryptology - ASIACRYPT 2001. 7th international conference on the theory and application of cryptology and information security, Gold Coast, Australia, December 9–13, 2001. Proceedings*. Berlin : Springer, 2001, pp. 480–494. ISBN: 3-540-42987-5. DOI: 10.1007/3-540-45682-1_28. URL: http://dx.doi.org/10.1007/3-540-45682-1_28 (cit. on p. 18).

[Gro95] Alexander Grothendieck. « Formule de Lefschetz et rationalité des fonctions ». In: *Séminaire Bourbaki, Vol. 9*. 1995 (cit. on p. 11).

[Har07] David Harvey. « Kedlaya's algorithm in larger characteristic. » English. In: *Int. Math. Res. Not.* 2007.22 (2007), p. 29. ISSN: 1073-7928 ; 1687-0247/e. DOI: 10.1093/imrn/rnm095 (cit. on p. 17).

[Har14] David Harvey. « Counting points on hyperelliptic curves in average polynomial time. » English. In: *Ann. Math. (2)* 179.2 (2014), pp. 783–803. ISSN: 0003-486X ; 1939-8980/e. DOI: 10.4007/annals.2014.179.2.7 (cit. on p. 17).

[HS16] David Harvey and Andrew V. Sutherland. « Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II. » In: *Contemporary Mathematics* 663 (2016). To appear in "Frobenius Distributions : Lang-Trotter and Sato-Tate conjectures", D. Kohel and I. Shparlinski, eds. (cit. on p. 17).

[Has33] Helmut Hasse. « Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorl. Mitt. » German. In: *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl.* 1933 (1933), pp. 253–262 (cit. on p. 10).

[Hen76] Peter Gregor Henn. « Die Automorphismengruppen der algebraischen Funktionenkörper vom Geschlecht 3 ». PhD thesis. 1976 (cit. on p. 18).

[Ito] Tetsushi Ito. *Tetsushi Ito's slide : On the history of the Sato-Tate conjecture*. URL: https://www.math.kyoto-u.ac.jp/~tetsushi/workshop200911/notes/ito.pdf (cit. on p. 40).

[KL82] Goro C. Kato and Saul Lubkin. « Zeta matrices of elliptic curves. » English. In: *J. Number Theory* 15 (1982), pp. 318–330. ISSN: 0022-314X ; 1096-1658/e. DOI: 10.1016/0022-314X(82)90036-1 (cit. on p. 16).

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*. English. Providence, RI : American Mathematical Society, 1999, pp. xi + 419. ISBN: 0-8218-1017-0/hbk (cit. on p. 55).

[Ked01] Kiran S. Kedlaya. « Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. » In: *J. Ramanujan Math. Soc.* 16.4 (2001), pp. 323–338. ISSN: 0970-1249 (cit. on p. 18).

[Ked04] Kiran S. Kedlaya. « Computing zeta functions via p-adic cohomology. » In: *Algorithmic number theory*. Vol. 3076. Lecture Notes in Comput. Sci. Springer, Berlin, 2004, pp. 1–17. DOI: 10.1007/978-3-540-24847-7_1. URL: http://dx.doi.org/10.1007/978-3-540-24847-7_1 (cit. on p. 21).

[Lep71] J. Lepowsky. « Multiplicity formulas for certain semisimple Lie groups. » English. In: *Bull. Am. Math. Soc.* 77 (1971), pp. 601–605. ISSN: 0002-9904 ; 1936-881X/e. DOI: 10.1090/S0002-9904-1971-12767-2 (cit. on p. 84).

[LST64] J Lubin, JP Serre, and J Tate. *Elliptic curves and formal groups, Lecture notes from the Summer Institute on Algebraic Geometry (Woods Hole, MA, 1964)*. 1964 (cit. on p. 16).

[MS01] Mark M. Meerschaert and Hans-Peter Scheffler. *Limit distributions for sums of independent random vectors. Heavy tails in theory and practice*. English. Chichester : Wiley, 2001, pp. xiii + 484. ISBN: 0-471-35629-8/hbk (cit. on p. 48).

[MZ] Ilya Molchanov and Sergei Zuyev. *Advanced Course in Probability : Weak Convergence and Asymptotics*. URL: http://www.math-stat.unibe.ch/unibe/philnat/math-stat/content/e8055/e8065/e9748/e15787/e15796/e16953/files17412/advprob_ger.pdf (cit. on p. 48).

[Mon68] P. Monsky. « Formal cohomology. II : The cohomology sequence of a pair. » In: *Ann. Math. (2)* 88 (1968), pp. 218–238. ISSN: 0003-486X ; 1939-8980/e. DOI: 10.2307/1970572 (cit. on p. 19).

[Mon71] P. Monsky. « Formal cohomology. III : Fixed point theorems. » In: *Ann. Math. (2)* 93 (1971), pp. 315–343. ISSN: 0003-486X ; 1939-8980/e. DOI: 10.2307/1970777 (cit. on p. 19).

[MW68] P. Monsky and G. Washnitzer. « Formal cohomology. I. » In: *Ann. Math. (2)* 88 (1968), pp. 181–217. ISSN: 0003-486X ; 1939-8980/e. DOI: 10.2307/1970571 (cit. on p. 19).

[Mor91] Carlos J. Moreno. *Algebraic curves over finite fields.* English. Cambridge etc. : Cambridge University Press, 1991, pp. ix + 246. ISBN: 0-521-34252-X/hbk (cit. on pp. 10, 11, 14).

[Put86] Marius van der Put. « The cohomology of Monsky and Washnitzer. » In: *Mém. Soc. Math. France (N.S.)* 23 (1986). Introductions aux cohomologies p-adiques (Luminy, 1984), pp. 4, 33–59. ISSN: 0037-9484 (cit. on p. 20).

[Sat00] Takakazu Satoh. « The canonical lift of an ordinary elliptic curve over a finite field and its point counting. » English. In: *J. Ramanujan Math. Soc.* 15.4 (2000), pp. 247–270. ISSN: 0970-1249 ; 2320-3110/e (cit. on p. 16).

[Sch] Ralf Schmidt. *Ralf Schmidt's web page about The Sato-Tate Conjecture - History.* URL: http://www2.math.ou.edu/~rschmidt/satotate/page5.html (cit. on p. 40).

[Sch85] René Schoof. « Elliptic curves over finite fields and the computation of square roots mod p. » English. In: *Math. Comput.* 44 (1985), pp. 483–494. ISSN: 0025-5718 ; 1088-6842/e. DOI: 10.2307/2007968 (cit. on p. 15).

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes. 2nd ed.* English. 2nd ed. Berlin : Springer, 2009, pp. xiii + 355. ISBN: 978-3-540-76877-7/hbk. DOI: 10.1007/978-3-540-76878-4 (cit. on pp. 11, 13, 14).

[Sut] Andrew V. Sutherland. *Sato-Tate Distributions in Genus 2*. URL: https://math.mit.edu/~drew/g2SatoTateDistributions.html (cit. on p. 99).

[Tat65] John T. Tate. *Algebraic cycles and poles of zeta functions.* English. Arithmetical algebraic Geom., Proc. Conf. Purdue Univ. 1963, 93-110 (1965). 1965 (cit. on p. 40).

[Tay08] Richard Taylor. « Automorphy for some l-adic lifts of automorphic mod l Galois representations. II. » English. In: *Publ. Math., Inst. Hautes Étud. Sci.* 108 (2008), pp. 183–239. ISSN: 0073-8301 ; 1618-1913/e. DOI: 10.1007/s10240-008-0015-2 (cit. on p. 54).

[Ver83] Alexius Maria Vermeulen. *Weierstrass points of weight two on curves of genus three.* Dissertation, University of Amsterdam, Amsterdam, 1983, With a Dutch summary. Universiteit van Amsterdam, Amsterdam, 1983, pp. iii+183 (cit. on p. 18).

[Wei48] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. French. Actualités Sci. Ind., No. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945). Paris : Hermann & Cie. iv, 85 pp. (1948). 1948 (cit. on p. 10).

[Wei49] André Weil. « Numbers of solutions of equations in finite fields. » English. In: *Bull. Am. Math. Soc.* 55 (1949), pp. 497–508. ISSN: 0002-9904 ; 1936-881X/e. DOI: 10.1090/S0002-9904-1949-09219-4 (cit. on p. 11).

Index