UNIVERSITY OF CALIFORNIA,
IRVINE

Generic Newton polygon for exponential sums in two variables with triangular base

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Mathematics

by

Rufei Ren

Dissertation Committee:
Professor Karl Rubin, Chair
Professor Liang Xiao
Professor Daqing Wan

2017

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

I would like to thank my advisors Professor Liang Xiao and Professor Karl Rubin for the extraordinary support to me and also thank Professor Daqing Wan for many helpful discussions.

I would like to thank my friends for accepting nothing less than excellence from me. Last but not the least, I would like to thank my parents for supporting me spiritually throughout writing this thesis and my life in general.

CURRICULUM VITAE

Rufei Ren

EDUCATION

Doctor of Philosophy in Mathematics **2017**
University of California, Irvine *Irvine, CA*

Bachelor of Science in mathematics **2012**
Fudan University *Shanghai, China*

TEACHING EXPERIENCE

Teaching Assistant **2015-2017**
University of California, Irvine *Irvine, CA*

REFEREED JOURNAL PUBLICATIONS

Slopes for higher rank Artin–Schreier–Witt towers **2016**
to appear in Trans. Amer. Math. Soc., arXiv:1605.02254.

TALKS AND POSTERS

The p-adic Langlands program and related topics, Indiana U., Bloomington **2016**
(poster)

Research Conference on elliptic curves, modular forms, and related topics **2016**
(talk)

Number Theory Seminar, Fudan University **2016**
(2-hour talk)

AMS Sectional Meetings, University of St. Thomas **2016**
(20-min talk)

Number Theory Seminar, UCSD **2016**
(1-hour talk)

ABSTRACT OF THE DISSERTATION

Generic Newton polygon for exponential sums in two variables with triangular base

By

Rufei Ren

Doctor of Philosophy in Mathematics

University of California, Irvine, 2017

Professor Karl Rubin, Chair

Let p be a prime number. Every two-variable polynomial $f(x_1, x_2)$ over a finite field of characteristic p defines an Artin–Schreier–Witt tower of surfaces whose Galois group is isomorphic to $\mathbb{Z}_p$. Our goal of this paper is to study the Newton polygon of the L-functions associated to a finite character of $\mathbb{Z}_p$ and a generic polynomial whose convex hull is a fixed triangle Δ. We denote this polygon by $\mathrm{GNP}(\Delta)$. We prove a lower bound of $\mathrm{GNP}(\Delta)$, which we call the improved Hodge polygon $\mathrm{IHP}(\Delta)$, and we conjecture that $\mathrm{GNP}(\Delta)$ and $\mathrm{IHP}(\Delta)$ are the same. We show that if $\mathrm{GNP}(\Delta)$ and $\mathrm{IHP}(\Delta)$ coincide at a certain point, then they coincide at infinitely many points.

When Δ is an isosceles right triangle with vertices $(0,0)$, $(0,d)$ and $(d,0)$ such that d is not divisible by p and that the residue of p modulo d is small relative to d, we prove that $\mathrm{GNP}(\Delta)$ and $\mathrm{IHP}(\Delta)$ coincide at infinitely many points. As a corollary, we deduce that the slopes of $\mathrm{GNP}(\Delta)$ roughly form an arithmetic progression with increasing multiplicities.

Chapter 1

Introduction

We shall state our main results and their motivation after recalling the notion of L-functions for Witt coverings. Let p be a prime number. Let

$$f(x_1, x_2) := \sum_{P \in \mathbb{Z}^2_{\geqslant 0}} a_P x_1^{P_x} x_2^{P_y}$$

be a two-variable polynomial in $\overline{\mathbb{F}}_p[x_1, x_2]$ and write

$$\hat{f}(x_1, x_2) := \sum_{P \in \mathbb{Z}^2_{\geqslant 0}} \hat{a}_P x_1^{P_x} x_2^{P_y}$$

for its Teichmüller lift, where $\hat{a}_P$ denotes the Teichmüller lift of a_P. We use $\mathbb{F}_p(f)$ to denote the extension of $\mathbb{F}_p$ generated by all coefficients of f and set $n(f) := [\mathbb{F}_p(f) : \mathbb{F}_p]$. The convex hull of the set of points $(0,0) \cup \left\{P \mid a_P \neq 0\right\}$ is called *the polytope* of f and denoted by Δ_f.

Let $(\mathbb{G}_m)^2$ be the two-dimensional torus over $\mathbb{F}_{p^{n(f)}}$. The main subject of our study is the

L-function associated to finite characters $\chi : \mathbb{Z}_p \to \mathbb{C}_p^\times$ of conductor p^{m_χ} given by

$$L_f^*(\chi, s) := \prod_{x \in |(\mathbb{G}_m)^2|} \frac{1}{1 - \chi\big(\mathrm{Tr}_{\mathbb{Q}_{p^{n(f)\deg(x)}}/\mathbb{Q}_p}(\hat{f}(\hat{x}))\big) s^{\deg(x)}},$$

where $|(\mathbb{G}_m)^2|$ is the set of closed points of $(\mathbb{G}_m)^2$ and $\hat{x}$ is the Teichmüller lift of a closed point x in $(\mathbb{G}_m)^2$. The characteristic power series $C_f^*(\chi, s)$ is a product of reciprocals of L-functions:

$$C_f^*(\chi, s) = \prod_{j=0}^{\infty} L_f^*(\chi, p^{jn(f)}s)^{-(j+1)}. \tag{1.1}$$

We can alternatively express $L_f^*(\chi, s)$ in terms of $C_f^*(\chi, s)$ as

$$L_f^*(\chi, s) = \Big(\frac{C_f^*(\chi, s) C_f^*(\chi, p^{2n(f)}s)}{C_f^*(\chi, p^{n(f)}s)^2}\Big)^{-1}.$$

Therefore, $C_f^*(\chi, s)$ and $L_f^*(\chi, s)$ determine each other.

Definition 1.1. *From (LWei), we know that*

$$L_f^*(\chi, s)^{-1} := \sum_{i=0}^{2p^{2(m_\chi - 1)}\mathrm{Area}(\Delta_f)} v_i s^i$$

is a polynomial of degree $2p^{2(m_\chi-1)}\mathrm{Area}(\Delta_f)$ *in* $\mathbb{Z}_p[\zeta_{p^{m_\chi}}][s]$*, where* $\zeta_{p^{m_\chi}}$ *is a primitive* p^{m_χ}*-th root of unity. We call the lower convex hull of the set of points* $\big(i, p^{m_\chi - 1}(p-1)v_{p^{n(f)}}(v_i)\big)$ *the* normalized Newton polygon of $L_f^*(\chi, s)^{-1}$*, which is denoted by* $\mathrm{NP}(f, \chi)_{L^{-1}}$*. Here,* $v_{p^{n(f)}}(-)$ *is the p-adic valuation normalized so that* $v_{p^{n(f)}}(p^{n(f)}) = 1$*. Similarly, we write* $\mathrm{NP}(f, \chi)_C$ *for the normalized Newton polygon of* $C_f^*(\chi, s)$*.*

In (DWX), Davis, Wan and Xiao studied the p-adic Newton slopes of $L_f^*(\chi, s)$ when $f(x)$ is a one-variable polynomial whose degree d is coprime to p. They concluded that, for each character $\chi : \mathbb{Z}_p \to \mathbb{C}_p^\times$ of relatively large conductor, $\mathrm{NP}(f, \chi)_{L^{-1}}$ depends only on its

conductor. We briefly introduce their proof as follows.

They proved a lower bound of $\mathrm{NP}(f,\chi)_C$ when χ is the so-called universal character and an upper bound by the Poincaré duality of roots of $L_f^*(\chi_1, s)$ for a *particular character* χ_1 of conductor p. The lower bound is called the *Hodge polygon* in their paper. Then they verified that the upper bound coincides with the lower bound at $x = kd$ for any non-negative integer k. Since the Newton polygon of $C_f^*(\chi, s)$ is confined between these two bounds, it also passes through their intersections. See more details in (DWX).

We also mention here that the aforementioned proof strongly inspired the proof of spectral halo conjecture by Liu, Wan, and Xiao in (LWX); we refer to (RWXY) for the discussion on the analogy of the two proofs. Motivated by the attempt of extending spectral halo type results beyond the case of modular forms, it is natural to ask whether one can generalize the main results of (DWX) to more general cases of exponential sums and Artin–Schreier–Witt towers. For example, in a joint work with Wan, Xiao, and Yu, we examined the case when the Galois group of the Artin–Schreier–Witt tower is canonically isomorphic to $\mathbb{Z}_{p^\ell}$.

In this paper, we mainly deal with the generic Newton polygon of L-functions for *two-variable* polynomials. We want to apply the methods in (DWX) to this case. Therefore, it is crucial for us to give a lower bound and an upper bound for $C_f^*(\chi, s)$. However, the Hodge polygon provided by Liu and Wan in (LWan) is no longer optimal, and is in general strictly lower than the upper bound we obtain by Poincare duality. Our main contribution in this paper is to find an improved lower bound for $\mathrm{NP}(f,\chi)_C$, which we call the *improved Hodge bound* $\mathrm{IHP}(\Delta)$. We conjecture that our improved Hodge polygon is optimal, and is equal to the generic Newton polygon, that is the lowest Newton polygon for all polynomials f with the same convex hull.

When Δ_f is an isosceles right triangle with vertices $(0,0)$, $(d,0)$ and $(0,d)$, we will give an equivalent condition to verify the coincidence of improved Hodge polygon with the Newton

polygon (at infinitely many points), and we will show that this condition is met for a generic polynomial with convex hull Δ_f.

We now turn to stating our main results more rigorously.

Notation 1.1. *For a two-dimensional convex polytope Δ which contains $(0,0)$, we denote its* cone *by*

$$\mathrm{Cone}(\Delta) := \Big\{ P \in \mathbb{R}^2 \;\Big|\; kP \in \Delta \text{ for some } k > 0 \Big\},$$

and put

$$\mathbb{M}(\Delta) := \mathrm{Cone}(\Delta) \cap \mathbb{Z}^2$$

to be the set of lattice points in $\mathrm{Cone}(\Delta)$.

Moreover, we write $\mathbb{T}_k(\Delta)$ (resp. $\mathbb{T}'_k(\Delta)$) for the set consisting of all points in $\mathbb{M}(\Delta)$ with weight w (See Definition 2.7) strictly less than k (resp. less than or equal to k), and denote its cardinality by $\mathbb{x}_k(\Delta)$ (resp. $\mathbb{x}'_k(\Delta)$).

Notation 1.2. *For integers a and b, we denote by $a\%b$ the residue of a modulo b.*

Definition 1.2. *The* generic Newton polygon *of Δ is defined by*

$$\mathrm{GNP}(\Delta) := \inf_{\substack{\chi:\mathbb{Z}_p/p^m\chi\mathbb{Z}_p \to \mathbb{C}_p^\times \\ \Delta_f = \Delta}} \Big(\mathrm{NP}(f,\chi)_{L^{-1}} \Big),$$

where $\chi : \mathbb{Z}_p \to \mathbb{C}_p^\times$ runs over all finite characters, and f runs over all polynomials in $\overline{\mathbb{F}}_p[x_1, x_2]$ such that $\Delta_f = \Delta$. The following are our main results.

Theorem 1.1. *Let Δ be a right isosceles triangle with vertices $(0,0),(0,d),(d,0)$, where d is a positive integer not divisible by p. Let p_0 be the residue of p modulo d. Suppose $d \geqslant 24(2p_0^2 + p_0)$. Then the generic Newton polygon* $\mathrm{GNP}(\Delta)$ *passes through points $(\mathbb{x}_k(\Delta)+i, h_k(\Delta)+ki)$*

for any $k \geqslant 0$ *and* $0 \leqslant i \leqslant kd+1$, *where*

$$\mathbb{x}_k(\Delta) = \frac{(kd+1)kd}{2} \quad \textit{and} \quad h_k(\Delta) = \frac{(p-1)(k-1)k(k+1)d^2}{3} + k \sum_{P \in \mathbb{T}_1(\Delta)} \lfloor pw(P) \rfloor.$$

The points $(\mathbb{x}_k, h_k(\Delta))$ are vertices for the improved Hodge polygon $\mathrm{IHP}(\Delta)$ (see Definition 2.11 and Proposition 3.2). So the essential content of the proof is to show that the generic Newton polygon $\mathrm{GNP}(\Delta)$ also passes through these points. The proof of Theorem 1.1 consists of two parts: first we show that, for a fixed polynomial f with convex hull Δ_f, if $\mathrm{IHP}(\Delta)$ coincides with the corresponding Newton polygon $\mathrm{NP}(f, \chi_1)_C$ at $\mathbb{x}_1$, then these two polygons agree at all points $x = \mathbb{x}_k(\Delta) + i$ for $k \geqslant 1$ and $0 \leqslant i \leqslant kd+1$. This is proved in Theorem 3.1, which in fact holds with less constraints on Δ. Next, we prove that, for a generic polynomial f, $\mathrm{NP}(f, \chi_1)_C$ agrees with $\mathrm{IHP}(\Delta)$ at $x = \mathbb{x}_1(\Delta)$. For this, we look at the leading term of $\widetilde{v}_{\mathbb{x}_1(\Delta)}$ for the universal polynomial f_{univ} with convex hull Δ and show that this term is non-zero when $d \geqslant 24(2p_0^2 + p_0)$. This is proved in Theorem 4.1, which in fact holds under a weaker condition on p_0.

From (LWei, Theorem 1.4), for a finite character χ of conductor p^{m_χ}, we know that $L_f^*(\chi, s)^{-1}$ has degree of $p^{2(m_\chi - 1)}d^2$.

Theorem 1.2. *Under the hypotheses of Theorem 1.1, if we put* $(\alpha_1, \ldots, \alpha_{p^{2(m_\chi-1)}d^2})$ *to be the sequence of* $p^{n(f)}$*-adic Newton slopes of* $L_f^*(\chi, s)^{-1}$ *(in non-decreasing order), then for first* $\frac{p^{2(m_\chi-1)}d^2 + p^{(m_\chi-1)}d}{2}$*-th slopes we have*

$$\begin{cases} \alpha_{\mathbb{x}_i'+1}, \ldots, \alpha_{\mathbb{x}_{i+1}} \in \left(\frac{i}{p^{m-1}}, \frac{i+1}{p^{m_\chi-1}}\right) & \textit{for } i = 0, 1, \ldots, p^{m_\chi-1} - 1, \\ \alpha_{\mathbb{x}_i+1}, \ldots, \alpha_{\mathbb{x}_i'} = \frac{i}{p^{m_\chi-1}} & \textit{for } i = 0, 1, 2, \ldots, p^{m_\chi-1} - 1, \\ \alpha_{\mathbb{x}_{p^{m_\chi-1}}+1}, \ldots, \alpha_{\mathbb{x}'_{p^{m_\chi-1}}-2} = 1. \end{cases}$$

In fact, points $(\mathbb{x}_k(\Delta), h(\mathbb{T}_k))$ are vertices of the improved Hodge polygon (see Definition 2.11

and Proposition 3.2).

We do not know if Theorem 1.1 still holds for polytopes which are not right isosceles triangle. However, for an arbitrary multi-variable polynomial f in $\overline{\mathbb{F}}_p[\underline{x}]$, we are still able to get an improved Hodge polygon for $\mathrm{NP}(f,\chi)$. Especially, when f is a two-variable polynomial, it is expected that the slopes of the improved Hodge polygon form certain generalized arithmetic progression. We plan to address this in a forthcoming paper."

The Newton polygon for exponential sums was explicitly computed in the "ordinary" case by Adolphson–Sperber (AS), Berndt–Evans (BE), and Wan (W) in many special cases, and in general (namely the T-adic setup) by Liu–Wan (LWan). For the Δ we considered in Theorem 1.1, the ordinary condition amounts to requiring $p \equiv 1 \pmod{d}$. Blache, Ferard, and Zhu in (BFZ) proved a lower bound for the Newton polygon of one-variable Laurent polynomial over $\mathbb{F}_q$ of degree (d_1, d_2), which is called a Hodge-Stickelberger polygon. They also showed that when p approaches to infinite, the Newton polygon coincides the Hodge-Stickelberger polygon.

Going beyond the ordinary case, there has been many researches on understanding the generic Newton polygon of $L_f(\chi, s)$ when f is a polynomial of a single variable. The first results are due to Zhu (Z1) and Scholten–Zhu (SZ), when p is large enough. In (BF), Blache and Ferard worked on the generic Newton polygon associated to characters of large conductors. In (OY), Ouyang and Yang studied the one-variable polynomial $f(x) = x^d + a_1 x$. A similar result can be found in (OZ), where Ouyang and Zhang studied the family of polynomials of the form $f(x) = x^d + a_{d-1}x^{d-1}$.

Our Theorem 1.1 maybe considered as the first step beyond the ordinary case when the base polynomial is multivariable. A similar result is obtained by Zhu in (Z2) independently which shows that $\mathrm{GNP}(\Delta_f)$ and $\mathrm{IHP}(\Delta_f)$ coincide for characters of $\mathbb{Z}_p$ of conductor p.

Chapter 2

Dwork trace formula

Let p be an odd prime and let $f(x_1, x_2) := \sum_{P \in \mathbb{Z}^2_{\geqslant 0}} a_P x_1^{P_x} x_2^{P_y}$ be a two-variable polynomial in $\overline{\mathbb{F}}_p[x_1, x_2]$. Denote $F_p(f)$ to be the finite field generated by the coefficients of f, which we call the *coefficient field* of f. The convex hull of the set of points $\{(0,0)\} \cup \left\{P \mid a_P \neq 0\right\}$ is called *the polytope* of f and denoted by Δ_f.

Our discussion will focus on a fixed f until Proposition 4.1. We put $\mathbb{F}_q = \mathbb{F}_p(f)$ and $n = [\mathbb{F}_q : \mathbb{F}_p]$. Let $\hat{a}_P \in \mathbb{Z}_q$ be the Teichmüller lift of a_P. We call $\hat{f}(x_1, x_2) := \sum_{P \in \mathbb{Z}^2_{\geqslant 0}} \hat{a}_P x_1^{P_x} x_2^{P_y}$ the *Teichmüller lift* of $f(x)$.

For convenience, we put $v_p(-)$ (resp. $v_q(-)$) be the p-adic valuation normalized so that $v_p(p) = 1$ (resp. $v_q(q) = 1$).

2.1 T-adic exponential sums.

Notation 2.1. *We recall that the* Artin–Hasse exponential series *is defined by*

$$E(\pi) = \exp\big(\sum_{i=0}^{\infty} \frac{\pi^{p^i}}{p^i}\big) = \prod_{p\nmid i,\ i\geqslant 1} \big(1-\pi^i\big)^{-\mu(i)/i} \in 1+\pi+\pi^2\mathbb{Z}_p[\![\pi]\!]. \tag{2.1}$$

Putting $E(\pi) = T+1$ gives an isomorphism $\mathbb{Z}_p[\![\pi]\!] \cong \mathbb{Z}_p[\![T]\!]$.

Definition 2.1. *For each power series in $\mathbb{Z}_q[\![T]\!]$, say $g(T)$, we define its* T-adic valuation *as the largest k such that $g \in T^k\mathbb{Z}_q[\![T]\!]$ and denote it by $v_T(g)$.*

Definition 2.2. *For each $k \geqslant 1$, the* T-adic exponential sum *of f over $\mathbb{F}_{q^k}^{\times}$ is*

$$S_f^*(k,T) := \sum_{(x_1,x_2)\in(\mathbb{F}_{q^k}^{\times})^2} (1+T)^{\mathrm{Tr}_{\mathbb{Q}_{q^k}/\mathbb{Q}_p}(\hat{f}(\hat{x}_1,\hat{x}_2))} \in \mathbb{Z}_p[\![T]\!].$$

Definition 2.3. *The* T-adic L-function *of f is defined by*

$$L_f^*(T,s) = \exp\Big(\sum_{k=1}^{\infty} S_f^*(k,T)\frac{s^k}{k}\Big)$$

and its corresponding T-adic characteristic power series *is defined by*

$$\begin{aligned} C_f^*(T,s) &:= \exp\Big(\sum_{k=1}^{\infty} -(q^k-1)^{-2} S_f^*(k,T)\frac{s^k}{k}\Big) \\ &= \sum_{k=0}^{\infty} u_k(T)s^k \in \mathbb{Z}_p[\![T.s]\!], \end{aligned} \tag{2.2}$$

We put $u_k(T) = u_{k,j}T^j \in \mathbb{Z}_p[\![T]\!]$.

Moreover, they determine each other by relations:

$$C_f^*(T,s) = \Big(\prod_{j=0}^{\infty} L_f^*(T, q^j s)^{j+1}\Big)^{-1} \tag{2.3}$$

and

$$L_f^*(T,s) = \Big(\frac{C_f^*(T,s)C_f^*(T,q^2 s)}{C_f^*(T,qs)^2}\Big)^{-1}. \tag{2.4}$$

It is clear that for a finite character $\chi : \mathbb{Z}_p \to \mathbb{C}_p^\times$, we have

$$L_f^*(\chi,s) = L_f^*(T,s)\big|_{T=\chi(1)-1} \quad \textit{and} \quad C_f^*(\chi,s) = C_f^*(T,s)\big|_{T=\chi(1)-1},$$

where $L_f^*(\chi,s)$ and $C_f^*(\chi,s)$ are defined in the introduction.

Notation 2.2. *Recall that we put $E(\pi) = T+1$. We put*

$$\begin{aligned} E_f(x_1,x_2) &:= \prod_{P\in\mathbb{Z}^2_{\geqslant 0}} E(\hat{a}_P \pi x_1^{P_x} x_2^{P_y}) \\ &= \sum_{P\in\mathbb{Z}^2_{\geqslant 0}} e_P(T) x_1^{P_x} x_2^{P_y} \in \mathbb{Z}_q[\![T]\!][\![x_1,x_2]\!]. \end{aligned} \tag{2.5}$$

2.2 Dwork's trace formula

Recall that Δ_f is the convex hull of $f(x_1,x_2)$ and $\mathbb{M}(\Delta_f)$ is defined in Notation 1.1 as a set consisting of all the lattice points in the Cone(Δ_f). Let D be the smallest positive integer such that $w(\mathbb{M}(\Delta_f)) \subset \frac{1}{D}\mathbb{Z}$.

Definition 2.4. *We fix a D-th root $T^{1/D}$ of T. Define*

$$\boldsymbol{B} = \Big\{ \sum_{P\in\mathbb{M}(\Delta_f)} b_P (T^{1/D}x_1)^{P_x} (T^{1/D}x_2)^{P_y} \;\Big|\; b_P \in \mathbb{Z}_q[\![T^{1/D}]\!], v_T(b_P) \to +\infty, \textit{when } w(P)\to\infty \Big\}.$$

Let ψ_p denote the operator on $\mathbf{B}$ such that

$$\psi_p\Big(\sum_{P\in\mathbb{M}(\Delta_f)} b_P x_1^{P_x} x_2^{P_y}\Big) := \sum_{P\in\mathbb{M}(\Delta_f)} b_{(pP)} x_1^{P_x} x_2^{P_y}.$$

Recall that $n = [\mathbb{F}_q : \mathbb{F}_p]$.

Definition 2.5. *Define*

$$\psi := \sigma_{\mathrm{Frob}}^{-1} \circ \psi_p \circ E_f(x_1, x_2) : \mathbf{B} \longrightarrow \mathbf{B}, \tag{2.6}$$

and its n-th iterate

$$\psi^n = \psi_p^n \circ \prod_{i=0}^{n-1} E_f^{\sigma_{\mathrm{Frob}}^i}(x_1^{p^i}, x_2^{p^i}),$$

where σ_{Frob} represents the arithmetic Frobenius acting on the coefficients, and for any $g \in \mathbf{B}$ we have $E_f(x_1, x_2)(g) := E_f(x_1, x_2) \cdot g$.

One can easily check that

$$\psi_p \circ E_f(x_1, x_2)\big(x_1^{P_x} x_2^{P_y}\big) = \sum_{Q\in\mathbb{M}(\Delta_f)} e_{pQ-P}(T) x_1^{Q_x} x_2^{Q_y},$$

where $e_{pQ-P}(T)$ is defined in (2.5).

Theorem 2.1 (Dwork Trace Formula)**.** *For every integer $k > 0$, we have*

$$(q^k - 1)^{-2} S_f^*(k, \underline{\pi}) = \mathrm{Tr}_{\mathbf{B}/\mathbb{Z}_q[\![\pi]\!]}\big(\psi^{nk}\big).$$

Proof. This was proved by (LWei, Lemma 4.7). □

One can see (W) for a a thorough treatment of the universal Dwork trace formula.

Proposition 2.1 (Analytic trace formula)**.** *The theorem above has an equivalent multiplicative form:*

$$C_f^*(T,s) = \det\left(I - s\psi^n \mid \mathbf{B}/\mathbb{Z}_q[\![\pi]\!]\right). \tag{2.7}$$

Proof. Also see (LWei, Theorem 4.8). □

Definition 2.6. *The normalized Newton polygon of $C_f^*(T,s)$, denoted by $\mathrm{NP}(f,T)_C$, is the lower convex hull of the set of points $\left\{\left(i, \frac{v_T(u_i)}{n}\right)\right\}$.*

Notation 2.3. *In this paper, we fix Δ to be a triangle with vertices at $(0,0)$, $\mathbf{P_1} := (a_1, b_1)$ and $\mathbf{P_2} := (a_2, b_2)$.*

Definition 2.7. *For each lattice point P in $\mathbb{Z}^2$, assume that Q is the intersection of the lines $\overline{OP}$ and $\overline{\mathbf{P_1P_2}}$. Then we call*

$$w(P) := \frac{\overrightarrow{OP}}{\overrightarrow{OQ}}$$

the weight *of P.*

The weight function w is linear, i.e. Any two points P and Q in $\mathbb{Z}^2_{\geqslant 0}$ satisfy

$$w(P+Q) = w(P) + w(Q). \tag{2.8}$$

Equality (2.8) *does not always hold for a general polytope.*

We shall frequently work with multisets, i.e. sets of possibly repeating elements. They are often marked by a superscript star to be distinguished from regular sets, e.g. $S^\star$. The disjoint union of two multiset $S^\star$ and $S'^\star$ is denoted by $S^\star \uplus S'^\star$ as a multiset.

Definition 2.8. *Let $\mathbb{S}$ be a subset of $\mathbb{M}(\Delta)$. Then we write $\mathbb{S}^{\star m}$ (resp. $\mathbb{S}^{\star\infty}$) for the union of m (resp. countably infinite) copies of $\mathbb{S}$ as a multiset.*

Notation 2.4. *For any sets* $\mathbb{S}_1^\star$ *and* $\mathbb{S}_2^\star$ *in* $\mathbb{M}(\Delta)^{\star^\infty}$ *of the same cardinality, we denote by* $\mathrm{Iso}(\mathbb{S}_1^\star, \mathbb{S}_2^\star)$ *the set of all bijections (as multisets) from* $\mathbb{S}_1^\star$ *to* $\mathbb{S}_2^\star$*. When* $\mathbb{S}_1^\star = \mathbb{S}_2^\star = \mathbb{S}^\star$*, we denote* $\mathrm{Iso}(\mathbb{S}^\star) := \mathrm{Iso}(\mathbb{S}^\star, \mathbb{S}^\star)$*.*

Definition 2.9. *For a bijection* τ *in* $\mathrm{Iso}(\mathbb{S}_1^\star, \mathbb{S}_2^\star)$*, we define*

$$h(\mathbb{S}_1^\star, \mathbb{S}_2^\star, \tau) := \sum_{P \in \mathbb{S}_1^\star} \big[w(p\tau(P) - P) \big]. \tag{2.9}$$

For any submultiset $\mathbb{S}_1'^\star$ *of* $\mathbb{S}_1^\star$*, we write* $\tau|_{\mathbb{S}_1'^\star}$ *for the restriction of* τ *to* $\mathbb{S}_1'^\star$*. Moreover, the minimum of* $h(\mathbb{S}_1^\star, \mathbb{S}_2^\star, \tau)$ *is denoted by*

$$h(\mathbb{S}_1^\star, \mathbb{S}_2^\star) := \min_{\tau \in \mathrm{Iso}(\mathbb{S}_1^\star, \mathbb{S}_2^\star)} (h(\mathbb{S}_1^\star, \mathbb{S}_2^\star, \tau)), \tag{2.10}$$

where τ *varies among all bijections from* $\mathbb{S}_1^\star$ *to* $\mathbb{S}_2^\star$*.*

Definition 2.10. *We call a bijection from* $\mathbb{S}_1^\star$ *to* $\mathbb{S}_2^\star$ minimal*, if it reaches the minimum in* (2.10)*. When* $\mathbb{S}_1^\star = \mathbb{S}_2^\star$*, we call it a* minimal permutation *of* $\mathbb{S}^\star$ *and abbreviate* $h(\mathbb{S}^\star, \mathbb{S}^\star, \bullet)$ *(resp.* $h(\mathbb{S}^\star, \mathbb{S}^\star)$*) to* $h(\mathbb{S}^\star, \bullet)$ *(resp.* $h(\mathbb{S}^\star)$*).*

Remark 2.1. *If* $S_i^\star$ *for* $i = 1, 2$ *belongs* $\mathbb{M}(\Delta)$*, we suppress the star from the notation.*

Definition 2.11. *The* improved Hodge polygon *of* Δ*, denoted by* $\mathrm{IHP}(\Delta)$*, is the lower convex hull of the set of points* $\left\{ \left(\ell, \min_{\mathbb{S}^\star \in \mathscr{M}_\ell(n)} \frac{h(\mathbb{S}^\star)}{n} \right) \right\}$*, where* $\mathscr{M}_\ell(n)$ *represents for the set consisting of all multi-subsets of* $\mathbb{M}(\Delta)^{\star^n}$ *of cardinality* $n\ell$*, note* $\mathscr{M}_\ell(1) = \mathscr{M}_\ell$*.*

we shall prove in Proposition 3.2 later that

$$\min_{\mathbb{S}^\star \in \mathscr{M}_\ell(n)} h(\mathbb{S}^\star) = n \cdot \min_{\mathbb{S} \in \mathscr{M}_\ell} h(\mathbb{S}),$$

and hence the $\mathrm{IHP}(\Delta)$ is independent of n. In particular, $\mathrm{IHP}(\Delta)$ is the convex hull of the

set of points

$$\left(\ell, \min_{\mathbb{S}\in\mathscr{M}_\ell} h(\mathbb{S})\right).$$

Notation 2.5. *We denote by*

$$\begin{bmatrix} m_0 & m_1 & \cdots & m_{\ell-1} \\ n_0 & n_1 & \cdots & n_{\ell-1} \end{bmatrix}_M$$

the $\ell\times\ell$-submatrix formed by elements of a matrix M whose row indices belong to $\{m_0, m_1, \ldots, m_{\ell-1}\}$ and whose column indices belong to $\{n_0, n_1, \ldots, n_{\ell-1}\}$.

Put $\Delta_f = \Delta$. Recall that we define $\mathbb{T}_1'$ in Notation 1.1.

Lemma 2.1. *We have $e_O(T) = 1$ and $v_T(e_Q(T)) \geqslant \lceil w(Q) \rceil$ for all $Q \in \mathbb{M}(\Delta)$.*

Proof. (1) It follows from the definition of $e_O(T)$ in (2.5).

(2) Let

$$\mathbb{S}(f) := \{P \in \mathbb{T}_1' \mid a_P \neq 0\} = \{Q_1, Q_2, \ldots, Q_t\},$$

where $\{a_P\}$ is the set of coefficients of $f(x_1, x_2)$ and t is the cardinality of $\mathbb{S}(f)$.

Expanding each $E(\hat{a}_{Q_i}\pi x_1^{(Q_i)_x} x_2^{(Q_i)_y})$ to be a power series in variables x_1 and x_2, we get

$$E_f(x_1, x_2) = \prod_{i=1}^{t} E(\hat{a}_{Q_i}\pi x_1^{(Q_i)_x} x_2^{(Q_i)_y}) = \sum_{\vec{j}\in\mathbb{Z}_{\geqslant 0}^t} c_{\vec{j}} \prod_{i=1}^{t} (\hat{a}_{Q_i}\pi x_1^{(Q_i)_x} x_2^{(Q_i)_y})^{j_i},$$

where $\{\hat{a}_P\}$ is the set of coefficients of $\hat{f}(x_1, x_2)$ and $c_{\vec{j}}$ belongs to $\mathbb{Z}_q$.

It is not hard to get that

$$\begin{aligned} e_Q(T) &= \sum_{\left\{\vec{j}\,\middle|\, \sum_{i=1}^{t} j_i Q_i = Q\right\}} c_{\vec{j}} \prod_{i=1}^{t} (\hat{a}_{Q_i}\pi)^{j_i} \\ &= \sum_{\left\{\vec{j}\,\middle|\, \sum_{i=1}^{t} j_i Q_i = Q\right\}} \Big(c_{\vec{j}} \prod_{i=1}^{t} (\hat{a}_{Q_i})^{j_i} \pi^{\sum_{i=1}^{t} j_i} \Big). \end{aligned}$$

Since $w(Q_i) \leqslant 1$ for each $Q_i \in \mathbb{S}(f)$, then for each $\vec{j}$ such that $\sum_{i=1}^{t} j_i Q_i = Q$, we have

$$v_T\Big(c_{\vec{j}} \prod_{i=1}^{t} (\hat{a}_{Q_i})^{j_i} \pi^{\sum_{i=1}^{t} j_i} \Big) = \sum_{i=1}^{t} j_i \geqslant \sum_{i=1}^{t} j_i w(Q_i) = w(Q),$$

where $T = E(\pi) - 1$. Therefore, we immediately get that $v_T(e_Q(T)) \geqslant w(Q)$. Since $v_T(e_Q(T))$ is an integer, we have

$$v_T(e_Q(T)) \geqslant \lceil w(Q) \rceil. \qquad \square$$

Notation 2.6. *We label points in* $\mathbb{M}(\Delta)$ *such that* $\mathbb{M}(\Delta) = \{P_1, P_2, \dots\}$.

Proposition 2.2. *The normalized Newton polygon* $\mathrm{NP}(f,T)_C$ *lies above* $\mathrm{IHP}(\Delta_f)$.

Proof. We write N for the standard matrix of $\psi_p \circ E_f$ corresponding to the basis

$$\{x_1^{(P_1)_x} x_2^{(P_1)_y}, x_1^{(P_2)_x} x_2^{(P_2)_y}, \cdots\}$$

of the Banach space $\mathbf{B}$. By (RWXY, Corollary 3.9), we know that the standard matrix of ψ^n corresponding to the same basis is equal to $\sigma_{\mathrm{Frob}}^{n-1}(N) \circ \sigma_{\mathrm{Frob}}^{n-2}(N) \circ \cdots \circ N$. Then by (RWXY,

Proposition 4.6), for every $\ell \in \mathbb{N}$ we have

$$u_\ell(T) = \sum_{\substack{\{P_{m_{0,0}}, P_{m_{0,1}}, \ldots, P_{m_{0,\ell-1}}\} \in \mathscr{M}_\ell \\ \{P_{m_{1,0}}, P_{m_{1,1}}, \ldots, P_{m_{1,\ell-1}}\} \in \mathscr{M}_\ell \\ \vdots \\ \{P_{m_{n-1,0}}, P_{m_{n-1,1}}, \ldots, P_{m_{n-1,\ell-1}}\} \in \mathscr{M}_\ell}} \det\left(\prod_{j=0}^{n-1} \begin{bmatrix} m_{j+1,0} & m_{j+1,1} & \cdots & m_{j+1,\ell-1} \\ m_{j,0} & m_{j,1} & \cdots & m_{j,\ell-1} \end{bmatrix}_{\sigma^j_{\mathrm{Frob}}(N)} \right), \tag{2.11}$$

where $m_{n,i} := m_{0,i}$ for each $0 \leqslant i \leqslant \ell - 1$.

Then for $\mathbb{S}_j = \{P_{m_{j,0}}, P_{m_{j,1}}, \ldots, P_{m_{j,\ell-1}}\}$, we have

$$\begin{aligned} & v_T\Big(\det\Big(\prod_{j=0}^{n-1} \begin{bmatrix} m_{j+1,0} & m_{j+1,1} & \cdots & m_{j+1,\ell-1} \\ m_{j,0} & m_{j,1} & \cdots & m_{j,\ell-1} \end{bmatrix}_{\sigma^j_{\mathrm{Frob}}(N)} \Big) \Big) \\ =& v_T\Big(\prod_{j=0}^{n-1} \sum_{\tau_j = \mathrm{Iso}(\mathbb{S}_{j+1}, \mathbb{S}_j)} \mathrm{sgn}(\tau_j) \prod_{P \in \mathbb{S}_{j+1}} \sigma^j_{\mathrm{Frob}}(e_{P\tau_j(P) - P}) \Big) \\ \geqslant & \sum_{j=0}^{n-1} h(\mathbb{S}_{j+1}, \mathbb{S}_j) \\ \geqslant & h\Big(\biguplus_{j=0}^{n-1} \mathbb{S}^\star_j \Big), \end{aligned} \tag{2.12}$$

where $\mathbb{S}_n = \mathbb{S}_0$. Therefore, it is easily seen that

$$v_T(u_\ell(T)) \geqslant \min_{\mathbb{S}^\star \in \mathscr{M}_\ell(n)} h(\mathbb{S}^\star). \tag{2.13}$$

Chapter 3

Improved Hodge polygon for a triangle Δ

Recall that Δ is a triangle with vertices $(0,0)$, $\mathbf{P_1} := (a_1, b_1)$ and $\mathbf{P_2} := (a_2, b_2)$ and as we defined in Notation 1.1, $\mathbb{x}_k = \mathbb{x}_k(\Delta)$ (resp. $\mathbb{x}'_k = \mathbb{x}'_k(\Delta)$) is the number of lattice points in $\mathbb{M}(\Delta)$ whose weight is strictly less than (resp. less than or equal to) k. For the rest of this paper, we restrict p to be a prime satisfying

$$p \nmid a_2b_1 - a_1b_2 \quad \text{and} \quad p > \frac{2(b_1a_2 - b_2a_1)}{\gcd(a_1 - a_2, b_1 - b_2)} + 1.$$

The goal of this chapter is to show that if $\mathrm{NP}(f, \chi)_C$ (See Definition 1.1) and $\mathrm{IHP}(\Delta)$ coincide at a certain point, then they will coincide at infinitely many points. More precisely, we have the following.

Theorem 3.1. *Let $f(x_1, x_2)$ be a two-variable polynomial with convex hull Δ. Suppose that there exists a nontrivial finite character $\chi_1 : \mathbb{Z}_p \to \mathbb{C}_p^\times$ and an integer $k_1 > 0$ such that $\mathrm{NP}(f, \chi_1)_C$ coincides with $\mathrm{IHP}(\Delta)$ at $x = \mathbb{x}_{k_1}$. Then for any finite character χ and positive integer k, $\mathrm{IHP}(\Delta)$ and $\mathrm{NP}(f, \chi)_C$ coincide at $\mathbb{x}_k + i_k$ for all $0 \leqslant i_k \leqslant \mathbb{x}'_k - \mathbb{x}_k$.*

Moreover, the leading coefficients $u_{\mathbb{x}_k, nh(\mathbb{T}_k)}$ (resp. $u_{\mathbb{x}'_k, nh(\mathbb{T}'_k)}$) *of the* $\mathbb{x}_k$*-th* (resp. $\mathbb{x}'_k$*-th*) *terms of the characteristic power series (see (2.2) for precise definition) are* $\mathbb{Z}_p$*-units.*

The proof of this theorem will occupy the rest of this chapter.

Notation 3.1. *Without loss of generality, we can assume that* $a_2b_1 - a_1b_2 > 0$*. We call the parallelogram with vertices* $O, \mathbf{P}_1, \mathbf{P}_2$ *and* $\mathbf{P}_1 + \mathbf{P}_2$ *(excluding the upper and right sides) the* fundamental parallelogram *of* Δ*, and denote it by* $\square_\Delta$*, i.e. the shadow region in Figure 3.1.*

We put $\square_\Delta^{\mathrm{Int}}$ *to be the set of lattice points in* $\square_\Delta$*, which contains* $a_2b_1 - a_1b_2$ *points. Let* Λ *be the lattice generated by* $\mathbf{P_1}$ *and* $\mathbf{P_2}$*. For each point* P *in* $\mathrm{Cone}(\Delta)$*, we write* $P\%$ *for its residue in* $\square_\Delta$ *modulo* Λ*.*

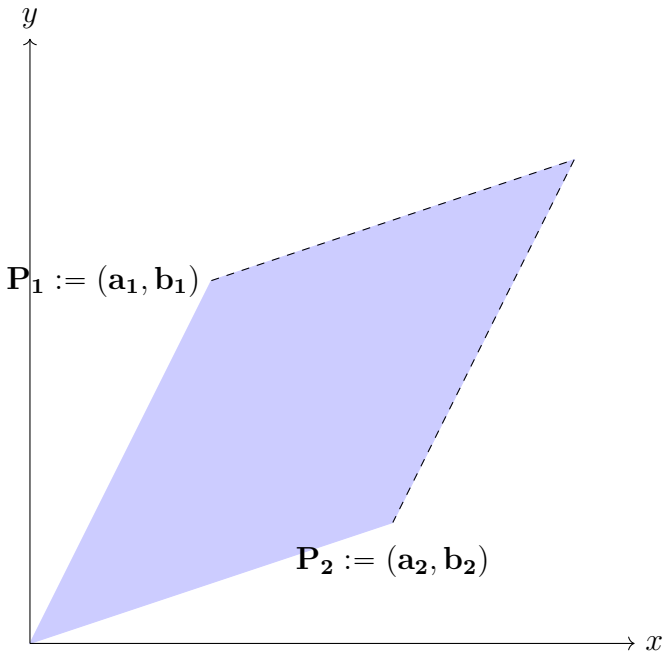

Figure 3.1: The fundamental parallelogram.

Lemma 3.1. *The map*

$$\begin{aligned} \eta: \quad & \square_\Delta^{\mathrm{Int}} \to \square_\Delta^{\mathrm{Int}} \\ & P \mapsto (pP)\% \end{aligned}$$

is a permutation.

Proof. since p and $a_2b_1 - a_1b_2$ are coprime, there exist integers p' and n_1 such that $pp' - 1 = (a_2b_1 - a_1b_2)n_1$. For a point $P = (P_x, P_y)$, we have

$$(pp' - 1)P = n_1(b_2P_x - a_2P_y)\mathbf{P_1} + n_1(-b_1P_x + a_1P_y)\mathbf{P_2} \in \Lambda.$$

It implies that composite

$$\square_\Delta^{\mathrm{Int}} \xrightarrow{P \mapsto pP\%} \square_\Delta^{\mathrm{Int}} \xrightarrow{P \mapsto p'P\%} \square_\Delta^{\mathrm{Int}}$$

is the identity map. □

The key to proving Theorem 3.1 is to gain precise control of the improved Hodge polygon in Proposition 2.2. In (W), Wan made use of the following coarser estimate of this Hodge polygon, for each multiset $\mathbb{S}^\star$ of $\mathbb{M}(\Delta)^{\star^\infty}$ we have

$$h_1(\mathbb{S}^\star) \geqslant h_1(\mathbb{S}^\star) := (p-1)\sum_{P \in \mathbb{S}^\star} w(P).$$

It is however important for our method to understand the difference between $h_1(\mathbb{S}^\star)$ and $h(\mathbb{S}^\star)$ (or more generally $h(\mathbb{S}^\star, \tau)$.

For each $r \in \mathbb{R}$, we put $R(r) := \lceil r \rceil - r$; and for a permutation τ of $\mathbb{S}^\star$, we set

$$U^\star(\mathbb{S}^\star, \tau) := \Big\{ R\left(w\left(p\tau(P) - P\right)\right) \mid P \in \mathbb{S}^\star \Big\}^\star, \tag{3.1}$$

$$U^\star(\mathbb{S}^\star, \tau)^{\leqslant a} := \Big\{ r \in U^\star(\mathbb{S}^\star, \tau) \mid r \leqslant a \Big\}^\star \quad \text{and} \quad U^\star(\mathbb{S}^\star, \tau)^{<a} := \Big\{ r \in U^\star(\mathbb{S}^\star, \tau) \mid r < a \Big\}^\star \tag{3.2}$$

to measure the distance of these weights to the next integer values.

Write

$$h_2(\mathbb{S}^\star,\tau) := \sum_{r\in U^\star(\mathbb{S}^\star,\tau)} r \quad \text{and} \quad h_2(\mathbb{S}^\star) = \min_{\tau\in \mathrm{Iso}(\mathbb{S}^\star)} \Big\{ h_2(\mathbb{S}^\star,\tau)\Big\} \tag{3.3}$$

where $\mathrm{Iso}(\mathbb{S}^\star)$ is set consisting all permutations of $\mathbb{S}^\star$ (see Notation 2.4).

Lemma 3.2. *We have*

$$h(\mathbb{S}^\star,\tau) = h_1(\mathbb{S}^\star) + h_2(\mathbb{S}^\star,\tau) \quad \textit{and} \quad h(\mathbb{S}^\star) = h_1(\mathbb{S}^\star) + h_2(\mathbb{S}^\star). \tag{3.4}$$

Proof. By the definition of $h(\mathbb{S}^\star,\tau)$ in (2.9), we have

$$\begin{aligned} h(\mathbb{S}^\star,\tau) &= \sum_{P\in\mathbb{S}^\star} \big\lceil w\big(p\tau(P)-P\big)\big\rceil \\ &= \sum_{P\in\mathbb{S}^\star} w\big(p\tau(P)-P\big) + \sum_{P\in\mathbb{S}^\star} \Big\{ \big\lceil w\big(p\tau(P)-P\big)\big\rceil - w\big(p\tau(P)-P\big)\Big\} \\ &= \sum_{P\in\mathbb{S}^\star} pw\big(\tau(P)\big) - \sum_{P\in\mathbb{S}^\star} w(P) + \sum_{P\in\mathbb{S}^\star} R\big(w\big(p\tau(P)-P\big)\big) \\ &= (p-1)\sum_{P\in\mathbb{S}^\star} w(P) + h_2(\mathbb{S}^\star,\tau) \\ &= h_1(\mathbb{S}^\star) + h_2(\mathbb{S}^\star,\tau). \end{aligned}$$

Taking the minimal over all $\tau\in\mathrm{Iso}(\mathbb{S}^\star)$ implies

$$h(\mathbb{S}^\star) = h_1(\mathbb{S}^\star) + h_2(\mathbb{S}^\star). \qquad \square$$

Lemma 3.3. *For any two permutations τ_1,τ_2 of $\mathbb{S}^\star$, if $U^\star(\mathbb{S}^\star,\tau_1) = U^\star(\mathbb{S}^\star,\tau_2)$, then*

$$h_2(\mathbb{S}^\star,\tau_1) = h_2(\mathbb{S}^\star,\tau_2) \quad \textit{and} \quad h(\mathbb{S}^\star,\tau_1) = h(\mathbb{S}^\star,\tau_2).$$

Proof. This lemma follows from the definition of h_2 and Lemma 3.2. □

Lemma 3.4. *Suppose* $\mathbb{S}_1^\star, \mathbb{S}_2^\star \subset \mathbb{M}(\Delta)^{\star^\infty}$ *satisfy*

$$\left\{w(P) \mid P \in \mathbb{S}_1^\star\right\}^\star = \left\{w(P) \mid P \in \mathbb{S}_2^\star\right\}^\star \tag{3.5}$$

as multisets. Then we have

$$h_2(\mathbb{S}_1^\star) = h_2(\mathbb{S}_2^\star) \quad \textit{and} \quad h(\mathbb{S}_1^\star) = h(\mathbb{S}_2^\star). \tag{3.6}$$

Proof. Let $\xi : \mathbb{S}_1^\star \to \mathbb{S}_2^\star$ be a bijection such that the induced map of weights from $\left\{w(P) \mid P \in \mathbb{S}_1^\star\right\}^\star$ to $\left\{w(P) \mid P \in \mathbb{S}_2^\star\right\}^\star$ realizes the equality (3.5). Then ξ induces a bijection from $\mathrm{Iso}(\mathbb{S}_1^\star)$ to $\mathrm{Iso}(\mathbb{S}_2^\star)$. Moreover, we have

$$h_2(\mathbb{S}_1^\star, \tau) = h_2(\mathbb{S}_2^\star, \xi^{-1}\tau\xi).$$

We immediately get the first equality in (3.6). Combining it with Lemma 3.2, we can easily check the second equality. □

We prove Theorem 3.1 in two steps.

Step I. Recall that a permutation τ of $\mathbb{S}^\star$ that achieves the minimum of $h(\mathbb{S}^\star)$ or equivalently the minimum of $h_2(\mathbb{S}^\star)$ is called minimal. The first core result in this chapter is Proposition 3.1. It shows for a given $\mathbb{S}^\star \subset \mathbb{M}(\Delta)^{\star^\infty}$ how to construct an explicit minimal permutation $\overline{\tau}$ of $\mathbb{S}^\star$.

First, we construct a minimal permutation inductively for a general subset $\mathbb{S}^\star$ of $\mathbb{M}(\Delta)^{\star^\infty}$ as follows.

Construction 3.1. *We choose a pair of points (P_0, Q_0) in $\mathbb{S}^\star \times \mathbb{S}^\star$ such that $R(w(pQ_0 - P_0))$ reaches the minimum among all pairs (P, Q) in $\mathbb{S}^\star \times \mathbb{S}^\star$. Define $\overline{\tau}(P_0) := Q_0$.*

Then we take out P_0 from the first $\mathbb{S}^\star$ and Q_0 from the second $\mathbb{S}^\star$. We pick another pair of points (P_1, Q_1) from $\mathbb{S}^\star \backslash \{P_0\} \times \mathbb{S}^\star \backslash \{Q_0\}$ such that $R(w(pQ_1 - P_1))$ reaches the minimum among all pairs (P, Q) in $\mathbb{S}^\star \backslash \{P_0\} \times \mathbb{S}^\star \backslash \{Q_0\}$, and define $\overline{\tau}(P_1) := Q_1$. Similarly, we pick a "minimal" pair of points (P_2, Q_2) from $\mathbb{S}^\star \backslash \{P_0, P_1\} \times \mathbb{S}^\star \backslash \{Q_0, Q_1\}$. Define $\overline{\tau}(P_2) := Q_2$. Iterating this process defines $\overline{\tau}$.

Lemma 3.5. *Let $\overline{\tau}$ be a minimal permutation constructed in Construction 3.1, and let τ be an arbitrary permutation of $\mathbb{S}^\star$. Suppose*

$$U^\star(\mathbb{S}^\star, \overline{\tau})^{<r_0} = U^\star(\mathbb{S}^\star, \tau)^{<r_0} \quad \text{for some rational number } r_0. \tag{3.7}$$

Then by taking finite times of the following operations:

1. *swapping the images of two points of the same weight; and*
2. *swapping the preimages of two points of the same weight,*

we obtain a permultation τ' from τ such that $\tau'(P) = \overline{\tau}(P)$ for all $P \in \mathbb{S}^\star$ satisfying $R\big(w(p\tau'(P) - P)\big) \leqslant r_0$ and $U^\star(\mathbb{S}^\star, \tau') = U^\star(\mathbb{S}^\star, \tau)$.

In particular, $U^\star(\mathbb{S}^\star, \overline{\tau})$ defined in (3.1) *is independent of the choice made in Construction 3.1.*

Proof. Assuming (3.7) holds for every $r \leqslant r_0$. Then we induce a permutation $\widetilde{\tau}$ from τ by taking finite times of operations (1) and (2) such that $\widetilde{\tau}(P) = \overline{\tau}(P)$ for all $P \in \mathbb{S}^\star$ satisfying $R\big(w(p\widetilde{\tau}(P) - P)\big) < r_0$ and $U^\star(\mathbb{S}^\star, \widetilde{\tau}) = U^\star(\mathbb{S}^\star, \tau)$. It is not hard to check that it is enough

for us to show this lemma works for $\widetilde{\tau}$. In other words, we can assume that

$$\tau(P) = \overline{\tau}(P) \text{ for each } P \in \mathbb{S}^\star \text{ satisfying } R\big(w(p\overline{\tau}(P) - P)\big) < r_0. \tag{3.8}$$

Suppose that $\tau(P) = \overline{\tau}(P)$ for all $P \in \mathbb{S}^\star$ satisfying $R\big(w(p\tau(P) - P)\big) \leqslant r_0$. Then we are done. Otherwise there exists a point P in $\mathbb{S}^\star$ such that $R\big(w(p\tau(P) - P) = r_0$, but $\tau(P) \neq \overline{\tau}(P)$. By Construction 3.1, it is not hard to see that at least one of the following cases will happen:

(a) $R\big(w(p\overline{\tau}(P) - P\big) = r_0$.

(b) There exists a point P_1 in $\mathbb{S}^\star$ such that $w(P) = w(P_1)$ and $\overline{\tau}(P_1) = \tau(P)$.

When case (a) happens, we put $Q_1 = \overline{\tau}(P)$ and define $\tau_1 : \mathbb{S}^\star \to \mathbb{S}^\star$ to be the same permutation as τ except we swap the preimages of Q_1 and $\tau(P)$.

Otherwise, we define τ_1 to be the same permutation as τ except we swap the images of P and P_1, where P_1 is defined in (b).

By (3.8), we know that either

$$R\big(w(pQ_1 - \tau^{-1}(Q_1))\big) \geqslant r_0 \quad \text{or} \quad R\big(w(p\tau(P_1) - P_1)\big) \geqslant r_0,$$

which implies that τ_1 also satisfies (3.8) and

$$\#\Big\{P \in U^\star(\mathbb{S}^\star, \tau_1)^{=r_0} \;\Big|\; \tau_1(P) = \overline{\tau}(P)\Big\} \geqslant \#\Big\{P \in U^\star(\mathbb{S}^\star, \tau)^{=r_0} \;\Big|\; \tau_1(P) = \overline{\tau}(P)\Big\} + 1.$$

If τ_1 does not satisfy the wanted property, then we run the same argument with τ_1 in place of τ to obtain another permutation τ_2. Iterating this process eventually gives us a permutation τ' of $\mathbb{S}^\star$. It is easy to check that $\tau'(P) = \overline{\tau}(P)$ for all $P \in \mathbb{S}^\star$ satisfying $R\big(w(p\tau'(P) - P)\big) \leqslant r_0$.

Since both operations (1), (2) do not change the set $U^\star(\mathbb{S}^\star, \tau)$, we have $U^\star(\mathbb{S}^\star, \tau') = U^\star(\mathbb{S}^\star, \tau)$.

We now prove the last statement of the lemma. Let $\overline{\tau}_1$ and $\overline{\tau}_2$ be two permutations constructed in Construction 3.1 by different choices of pairs of points. Suppose that $U^\star(\mathbb{S}^\star, \overline{\tau}) \neq U^\star(\mathbb{S}^\star, \overline{\tau})$. Then there is a rational number r_0, such that

$$U^\star(\mathbb{S}^\star, \overline{\tau}_1)^{<r_0} = U^\star(\mathbb{S}^\star, \overline{\tau}_2)^{<r_0} \quad \text{and} \quad U^\star(\mathbb{S}^\star, \overline{\tau}_1)^{\leqslant r_0} \neq U^\star(\mathbb{S}^\star, \overline{\tau}_2)^{\leqslant r_0}.$$

Without loss of generality, we assume that

$$U^\star(\mathbb{S}^\star, \overline{\tau}_1)^{\leqslant r_0} \subsetneq U^\star(\mathbb{S}^\star, \overline{\tau}_2)^{\leqslant r_0}.$$

From the argument in this lemma above, we know that there exists a permutation τ' of $\mathbb{S}^\star$ such that $\tau'(P) = \overline{\tau}_1(P)$ for all $P \in \mathbb{S}^\star$ satisfying $R\big(w(p\tau'(P) - P)\big) \leqslant r_0$ and

$$U^\star(\mathbb{S}^\star, \overline{\tau}_2) = U^\star(\mathbb{S}^\star, \tau').$$

Therefore, we have

$$U^\star(\mathbb{S}^\star, \overline{\tau}_1)^{\leqslant r_0} = U^\star(\mathbb{S}^\star, \tau')^{\leqslant r_0} = U^\star(\mathbb{S}^\star, \overline{\tau}_2)^{\leqslant r_0},$$

a contradiction. □

Corollary 3.1. *For τ and τ' as in the last lemma, we have $h_2(\mathbb{S}^\star, \tau') = h_2(\mathbb{S}^\star, \tau)$.*

Proof. Since $U^\star(\mathbb{S}^\star, \tau') = U^\star(\mathbb{S}^\star, \tau)$, then it follows directly from the definition of h_2 in (3.3). □

Proposition 3.1. *The permutation $\overline{\tau}$ in Construction 3.1 is a minimal permutation of $\mathbb{S}^\star$, i.e.*

$$h(\mathbb{S}^\star, \overline{\tau}) = h(\mathbb{S}^\star).$$

Proof. By Lemma 3.2, it is enough to prove that $\overline{\tau}$ minimizes $h_2(\mathbb{S}^\star, \bullet)$ among all permutations of $\mathbb{S}^\star$.

Assume that τ is a minimal permutation of $\mathbb{S}^\star$. If $U^\star(\mathbb{S}^\star, \overline{\tau}) = U^\star(\mathbb{S}^\star, \tau)$, we are done by Lemma 3.3. Otherwise we shall construct below a finite sequence of permutations $(\tau_0 = \tau, \tau_1, \ldots, \tau_m)$ satisfying

(1) for each $0 \leqslant i \leqslant m$, we have $h_2(\mathbb{S}^\star, \tau_i) = h_2(\mathbb{S}^\star)$.

(2) $U^\star(\mathbb{S}^\star, \tau_m) = U^\star(\mathbb{S}^\star, \overline{\tau})$.

Combining Property (2) with Lemma 3.3, we would deduce

$$h(\mathbb{S}^\star, \tau_m) = h(\mathbb{S}^\star, \overline{\tau}),$$

which completes the proof.

Now we come to the inductive construction of the sequence $(\tau_0 = \tau, \tau_1, \ldots, \tau_m)$. We take induction on i. First, we put $\tau_0 = \tau$, where τ is a minimal permutation of $\mathbb{S}$. Hence, it satisfies $h_2(\mathbb{S}^\star, \tau_0) = h_2(\mathbb{S}^\star)$.

Suppose that we have defined τ_i. If $U^\star(\mathbb{S}^\star, \tau_i) = U^\star(\mathbb{S}^\star, \overline{\tau})$, we terminate this induction. Otherwise let t_i be the smallest number in the multiset $U^\star(\mathbb{S}^\star, \overline{\tau}) \backslash U^\star(\mathbb{S}^\star, \tau_i)$. Let $\tau_i' : \mathbb{S}^\star \to \mathbb{S}^\star$ be the permutation constructed from τ_i in Lemma 3.5. It is not hard to check that

- $h_2(\mathbb{S}^\star, \tau_i) = h_2(\mathbb{S}^\star, \tau_i')$.
- $\tau_i'(P) = \overline{\tau}(P)$ holds for each $P \in \mathbb{S}^\star$ satisfying $w(P - \tau_i'(P)) \leqslant t_i$.
- $U^\star(\mathbb{S}^\star, \overline{\tau})^{\leqslant t_i} \supsetneq U^\star(\mathbb{S}^\star, \tau_i')^{\leqslant t_i}$.

Therefore, there exists a point P_i in $\mathbb{S}^\star$ with

$$Q_i = \overline{\tau}(P_i), \quad \tau_i'(P_i') = Q_i \quad \text{and} \quad \overline{\tau}(P_i') = Q_i'$$

such that

- $R(w(pQ_i - P_i)) = t_i$,
- $R(w(pQ_i' - P_i')) \geqslant t_i$,
- $R(w(pQ_i - P_i')) > t_i$, and
- $R(w(pQ_i' - P_i)) > t_i$.

We define τ_{i+1} to be the same permutation as τ_i' except we swap the images of P_i and P_i'. This process gives us a sequence with elements from $\mathrm{Iso}(\mathbb{S}^\star)$, whose length, say m, is less than or equal to $\#(\mathbb{S}^\star)$.

Then we check $h_2(\mathbb{S}^\star, \tau_{i+1}) = h_2(\mathbb{S}^\star, \tau_i)$. From the induction we know that $h_2(\mathbb{S}^\star, \tau_i) = h_2(\mathbb{S}^\star)$. Hence, we ha

$$h_2(\mathbb{S}^\star, \tau_{i+1}) \geqslant h_2(\mathbb{S}^\star, \tau_i).$$

On the other hand, from the definition of h_2, we have

$$\begin{aligned}
h_2(\mathbb{S}^\star, \tau_{i+1}) - h_2(\mathbb{S}^\star, \tau_i) =& h_2(\mathbb{S}^\star, \tau_{i+1}) - h_2(\mathbb{S}^\star, \tau_i') \\
=& R\big(w(p\tau_{i+1}(P_i) - P_i)\big) + R\big(w\big(p\tau_{i+1}(P_i') - P_i'\big)\big) \\
& - R\big(w(p\tau_i'(P_i') - P_i')\big) - R\big(w(p\tau_i'(P_i) - P_i)\big) \\
<& t_i + R\big(w(p\tau_{i+1}(P_i') - P_i')\big) - t_i - R\big(w(p\tau_i(P_i) - P_i)\big) \\
\leqslant& 1 - R\big(w(p\tau_i(P_i) + P_i)\big) \\
\leqslant& 1.
\end{aligned} \tag{3.9}$$

From the linearity of w, we have

$$w\big(p\tau_{i+1}(P_i) - P_i\big) + w\big(p\tau_{i+1}(P_i') - P_i'\big) = w\big(p\tau_i'(P_i') - P_i'\big) + w\big(p\tau_i'(P_i) - P_i\big).$$

It implies that $h_2(\mathbb{S}^\star, \tau_{i+1}) - h_2(\mathbb{S}^\star, \tau_i)$ is an integer. Combining it with (3.9), we have

$$h_2(\mathbb{S}^\star, \tau_{i+1}) \leqslant h_2(\mathbb{S}^\star, \tau_i).$$

Combining these inequalities, we obtain

$$h_2(\mathbb{S}^\star, \tau_{i+1}) = h_2(\mathbb{S}^\star, \tau_i) = h_2(\mathbb{S}^\star). \tag{3.10}$$

Finally, from the termination condition of this induction, we know that

$$U^\star(\mathbb{S}^\star, \tau_m) = U^\star(\mathbb{S}^\star, \overline{\tau}). \qquad \square$$

Remark 3.1. *Notice that this result crucially depends on the linearity of w as in* (2.8)*. For general polytopes, we have a similar definition for the weight of a point, however, it is no longer linear. We will address this case in a future work.*

For any subset $\mathbb{S}$ of $\mathbb{M}(\Delta)$, we write $\mathbb{S} + P$ for the shift of $\mathbb{S}$ by P.

Corollary 3.2. *Let $\mathbb{S}_2$ be a subset of $\mathbb{M}(\Delta)$, and let $Q_1, Q_2, \ldots, Q_k$ be points of $\mathbb{M}(\Delta)$ with integer weights. Put*

$$\mathbb{S}_1^\star = \mathbb{S}_2^\star \uplus \biguplus_{i=1}^{k} (\square_\Delta^{\mathrm{Int}} + Q_i)^\star,$$

then $h_2(\mathbb{S}_1^\star) = h_2(\mathbb{S}_2^\star)$.

Proof. Recall that for each point $P \in \mathbb{M}(\Delta)$, we denote by $P\%$ its residue in $\square_\Delta$. Lemma 3.1

defines a permutation of $\square_\Delta^{\mathrm{Int}}$ such that $\eta(P) = (pP)\%$. We write

$$\begin{aligned}\eta_i : \square_\Delta^{\mathrm{Int}} + Q_i &\to \square_\Delta^{\mathrm{Int}} + Q_i \\ P &\mapsto \eta^{-1}(P - Q_i) + Q_i.\end{aligned}$$

It is easy to check that $R(p\eta_i(P) - P) = 0$ for all point P in $\square_\Delta^{\mathrm{Int}} + Q_i$.

Then we apply Construction 3.1 to $\mathbb{S}_2$ and get a minimal permutation $\tau_{\mathbb{S}_2}$ of $\mathbb{S}_2$. It is not hard to see that $\tau_{\mathbb{S}_2}, \eta_1, \ldots, \eta_k$ together construct a permutation τ of $\mathbb{S}_1^\star$ which agrees with Construction 3.1. Therefore, we have

$$\begin{aligned}h_2(\mathbb{S}_1^\star) =& h_2(\mathbb{S}_2, \tau_{\mathbb{S}_2}) + \sum_{i=1}^{k} h_2(\square_\Delta^{\mathrm{Int}} + Q_i, \eta_i) \\ =& h_2(\mathbb{S}_2, \tau_{\mathbb{S}_2}) \\ =& h_2(\mathbb{S}_2).\end{aligned}$$

□

Corollary 3.3. *Let $\mathbb{S}_2$ be a subset of $\mathbb{M}(\Delta)$, and let $Q_1, Q_2, \ldots, Q_k$ be points of $\mathbb{M}(\Delta)$ of integer weights. Put $\mathbb{S}_1^\star = \biguplus_{i=1}^{k} (\mathbb{S}_2 + Q_i)$. Then we have $h_2(\mathbb{S}_1^\star) = kh_2(\mathbb{S}_2)$.*

Proof. Let τ_0 be the minimal permutation of $\mathbb{S}_2$ constructed in Construction 3.1. For each $1 \leqslant i \leqslant k$, put

$$\begin{aligned}\tau_i : \mathbb{S}_2 + Q_i &\to \mathbb{S}_2 + Q_i \\ P &\mapsto \tau_0(P - Q_i) + Q_i.\end{aligned}$$

It is not hard to see that $\tau_1, \tau_2, \ldots, \tau_k$ together induce a permutation τ of $\mathbb{S}_1^\star$ which agrees

with Construction 3.1 and for each $1 \leqslant i \leqslant k$ we have

$$h_2(\mathbb{S}_2 + Q_i, \tau_i) = h_2(\mathbb{S}_2, \tau_0) = h_2(\mathbb{S}_2).$$

Therefore,

$$\begin{aligned} h_2(\mathbb{S}_1^\star) =& h_2(\mathbb{S}_1^\star, \tau) \\ =& \sum_{i=1}^{k} h_2(\mathbb{S}_2 + Q_i, \tau_i) \\ =& k h_2(\mathbb{S}_2). \end{aligned}$$

□

Lemma 3.6. *we have*

$$h_2(\mathbb{T}_k) = k h_2(\mathbb{T}_1).$$

Proof. We can decompose $\mathbb{T}_k$ into a disjoint union of sets as follows:

$$\mathbb{T}_k = \bigsqcup_{i=0}^{k-1} (\mathbb{T}_1 + (k-1-i)\mathbf{P_2} + i\mathbf{P_1}) \sqcup \bigsqcup_{i=0}^{k-2} \bigsqcup_{j=0}^{i} (\square_\Delta^{\mathrm{Int}} + i\mathbf{P_1} + j\mathbf{P_2}). \tag{3.11}$$

Applying Corollary 3.2 and 3.3 to (3.11), we complete the proof of this lemma. □

Lemma 3.7. *Let l_1+2 (resp. l_2+2) represent the number of lattice points on closed segment $O\mathbf{P_1}$ (resp. $O\mathbf{P_2}$). For each $k > 0$, we have*

(1) $\mathbb{x}_k = k\mathbb{x}_1 + \frac{k(k-1)}{2}(a_2b_1 - a_1b_2)$.

(2) $h(\mathbb{T}_k) = (p-1)\sum_{i=0}^{k-2} \big[(a_2b_1 - a_1b_2)(i+1) - \frac{1}{2}(l_1+l_2)\big](i+1) + k\big[h(\mathbb{T}_1) + (p-1)(k-1)\mathbb{x}_1\big]$.

Proof. (1) Since there are totally $a_2b_1 - a_1b_2$ points in $\square_\Delta^{\mathrm{Int}}$, (1) follows directly from (3.11) above.

(2) A tautological computation shows that

$$\begin{aligned} h_1(\mathbb{T}_k) = & k\big[h_1(\mathbb{T}_1) + (p-1)(k-1)\mathbb{x}_1\big] \\ & + (p-1)\sum_{i=0}^{k-2}\big[a_2b_1 - a_1b_2 - \tfrac{1}{2}(l_1+l_2) - 1 + i(a_2b_1 - a_1b_2)\big](i+1). \end{aligned}$$

For each $k \geqslant 1$, we know from Lemma 3.6 that

$$\begin{aligned} h(\mathbb{T}_k) =& h_1(\mathbb{T}_k) + h_2(\mathbb{T}_k) \\ =& k\big[h_1(\mathbb{T}_1) + (p-1)(k-1)\mathbb{x}_1\big] + kh_2(\mathbb{T}_1) \\ &+ (p-1)\sum_{i=0}^{k-2}\big[(a_2b_1 - a_1b_2)(i+1) - \tfrac{1}{2}(l_1+l_2) - 1\big](i+1). \end{aligned}$$

Combining it with $h(\mathbb{T}_1) = h_1(\mathbb{T}_1) + h_2(\mathbb{T}_1)$, we complete the proof. □

Step II. The following proposition is the second core result of studying the improved Hodge polygon $\mathrm{IHP}(\Delta)$ at $x = \mathbb{x}_k$.

Proposition 3.2. *We have*

$$\min_{\mathbb{S}^\star \in \mathscr{M}_\ell(n)} h(\mathbb{S}^\star) = n \cdot \min_{\mathbb{S} \in \mathscr{M}_\ell} h(\mathbb{S}). \tag{3.12}$$

Therefore, we give a simpler expression of $\mathrm{IHP}(\Delta)$ *as the lower convex hull of the set of points*

$$\left(\ell, \min_{\mathbb{S} \in \mathscr{M}_\ell} h(\mathbb{S})\right),$$

which is independent of n.

We will prove this proposition after two lemmas.

Lemma 3.8. *For any two distinct points $P, Q \in \mathbb{M}(\Delta)$ if $w(P) \neq w(Q)$, then*

$$|w(P-Q)| \geqslant \frac{\gcd(a_1-a_2, b_1-b_2)}{b_1a_2 - b_2a_1}.$$

Proof. It is easily known that

$$w((1,0)) = \frac{a_2-a_1}{b_1a_2-b_2a_1} \quad \text{and} \quad w((0,1)) = \frac{b_1-b_2}{b_1a_2-b_2a_1}.$$

Since each point in $\mathbb{Z}^2$ is a linear combination of $(1,0)$ and $(0,1)$, this lemma follows from the linearity of w □

Lemma 3.9. *Let $\mathbb{M}'$ be a subset of $\mathbb{M}(\Delta)^{\star^\infty}$ and let $\mathscr{S}_\ell$ be the set consisting of all subsets of $\mathbb{M}'$ of cardinality ℓ. Choose a multiset $\mathbb{S}^\star_{min} \in \mathscr{S}_\ell$ such that*

$$\sum_{P \in \mathbb{S}^\star_{min}} w(P) = \min_{\mathbb{S}^\star \in \mathscr{S}_\ell} \Big(\sum_{P \in \mathbb{S}^\star} w(P) \Big).$$

Suppose that $p > \frac{2(b_1a_2-b_2a_1)}{\gcd(a_1-a_2,b_1-b_2)} + 1$. Then if $\widetilde{\mathbb{S}}^\star \in \mathscr{S}_\ell$ satisfy

$$\sum_{P \in \widetilde{\mathbb{S}}^\star} w(P) = \sum_{P \in \mathbb{S}^\star_{min}} w(P) \quad (\textit{resp.} \sum_{P \in \mathbb{S}^\star_{min}} w(P) > \min_{\mathbb{S}^\star \in \mathscr{S}_\ell} \Big(\sum_{P \in \mathbb{S}^\star} w(P) \Big)), \tag{3.13}$$

we have

$$h(\widetilde{\mathbb{S}}^\star) = h(\mathbb{S}^\star_{min}) \quad (\textit{resp. } h(\widetilde{\mathbb{S}}^\star) > h(\mathbb{S}^\star_{min})). \tag{3.14}$$

In other words, the minimal $h(\mathbb{S}^\star)$ is achieved by exactly those $\mathbb{S}^\star$ for which the sum of weights of $\mathbb{S}^\star$ is minimal.

Proof. For a subset $\widetilde{\mathbb{S}}^\star \in \mathscr{S}_\ell$, if $\Big\{ w(P) \mid P \in \widetilde{\mathbb{S}}^\star \Big\}^\star = \Big\{ w(P) \mid P \in \mathbb{S}^\star_{\min} \Big\}^\star$, then by Lemma 3.4,

we know

$$h(\widetilde{\mathbb{S}}^\star) = h(\mathbb{S}^\star_{\min}).$$

Otherwise we construct a sequence $(\mathbb{S}^\star_0 = \widetilde{\mathbb{S}}^\star, \mathbb{S}^\star_1, \ldots, \mathbb{S}^\star_m)$ in $\mathscr{S}_\ell$ of length less than or equal to ℓ such that

- for any $0 \leqslant i \leqslant m-1$, $h(\mathbb{S}_i) > h(\mathbb{S}_{i+1})$, and
- $\Big\{w(P) \mid P \in \mathbb{S}^\star_m\Big\}^\star = \Big\{w(P) \mid P \in \mathbb{S}^\star_{\min}\Big\}^\star$.

The following is the construction:

Assume that we have constructed $\mathbb{S}^\star_i$. If $\Big\{w(P) \mid P \in \mathbb{S}^\star_i\Big\}^\star = \Big\{w(P) \mid P \in \mathbb{S}^\star_{\min}\Big\}^\star$, then we stop. Otherwise there exists a rational number t_i such that

$$\Big\{w(P) < t_i \mid P \in \mathbb{S}^\star_i\Big\}^\star = \Big\{w(P) < t_i \mid P \in \mathbb{S}^\star_{\min}\Big\}^\star$$

and

$$\Big\{w(P) \leqslant t_i \mid P \in \mathbb{S}^\star_i\Big\}^\star \subsetneq \Big\{w(P) \leqslant t_i \mid P \in \mathbb{S}^\star_{\min}\Big\}^\star.$$

Then there exist points $P_i \in \mathbb{S}^\star_{\min} - \mathbb{S}^\star_i$ and $Q_i \in \mathbb{S}^\star_i - \mathbb{S}^\star_{\min}$ such that

$$w(P_i) = t_i < w(Q_i).$$

Put $\mathbb{S}^\star_{i+1}$ to be the set induced from $\mathbb{S}^\star_i$ by simply substituting Q_i with P_i. Then we get a sequence $(\mathbb{S}^\star_0 = \mathbb{S}^\star, \mathbb{S}^\star_1, \ldots, \mathbb{S}^\star_m)$ in $\mathscr{S}_\ell$ of length, say m, less than or equal to ℓ, which satisfies the following conditions.

(1) $\mathbb{S}^\star_0 = \widetilde{\mathbb{S}}^\star$.

(2) $\Big\{w(P) \mid P \in \mathbb{S}^\star_m\Big\}^\star = \Big\{w(P) \mid P \in \mathbb{S}^\star_{\min}\Big\}^\star$.

(3) For each $0 \leqslant i \leqslant m-1$, we have $\mathbb{S}^\star_{i+1} - \mathbb{S}^\star_i = \{P_i\}$ and $\mathbb{S}^\star_i - \mathbb{S}^\star_{i+1} = \{Q_i\}$.

(4) The points above satisfy $w(P_i) < w(Q_i)$.

From Lemma 3.4, we know that (2) implies that

$$h(\mathbb{S}^\star_m) = h(\mathbb{S}^\star_{\min}).$$

Therefore, it is enough to show that $h(\mathbb{S}^\star_i) > h(\mathbb{S}^\star_{i+1})$ holds for each $0 \leqslant i \leqslant m-1$.

For $0 \leqslant i \leqslant m-1$, let $\tau_i \in \mathrm{Iso}(\mathbb{S}^\star_i)$ be a minimal permutation of $\mathbb{S}^\star_i$, i.e. $h(\mathbb{S}^\star_i, \tau_i) = h(\mathbb{S}^\star_i)$. We denote by τ_{i+1} a permutation of $\mathbb{S}^\star_{i+1}$ induced from τ_i by simply substituting Q_i with P_i, i.e.

$$\tau_{i+1}(P) = \begin{cases} \tau_i(Q_i) & \text{if } P = P_i \\ P_i & \text{if } \tau_i(P) = Q_i \\ \tau_i(P) & \text{otherwise.} \end{cases}$$

Now we claim that $h(\mathbb{S}^\star_i, \tau_i) - h(\mathbb{S}^\star_{i+1}, \tau_{i+1}) > 0$. We need to consider the following two cases.

Case 1: When $\tau_i(Q_i) = Q_i$, we have

$$\begin{aligned}
& h(\mathbb{S}^\star_i, \tau_i) - h(\mathbb{S}^\star_{i+1}, \tau_{i+1}) \\
=& \big\lceil pw(Q_i) - w(Q_i) \big\rceil - \big\lceil pw(P_i) - w(P_i) \big\rceil \\
=& \big\lceil (p-1)w(Q_i) \big\rceil - \big\lceil (p-1)w(P_i) \big\rceil \\
\geqslant& \big\lceil (p-1)(w(Q_i) - w(P_i)) \big\rceil - 1 \\
\geqslant& \Big\lceil \frac{(p-1)\gcd(a_1 - a_2, b_1 - b_2)}{b_1 a_2 - b_2 a_1} \Big\rceil - 1 \qquad \text{Lemma 3.8} \\
>& 0.
\end{aligned}$$

Case 2: When $\tau_i(Q_i) \neq Q_i$, let $Q_i' = \tau_i^{-1}(Q_i)$. Then we have

$$\begin{aligned}
&h(\mathbb{S}_i^\star, \tau_i) - h(\mathbb{S}_{i+1}^\star, \tau_{i+1}) \\
=&\big\lceil pw\big(\tau_i(Q_i)\big) - w(Q_i)\big\rceil - \big\lceil pw\big(\tau_i(Q_i)\big) - w(P_i)\big\rceil + \big\lceil pw(Q_i) - w(Q_i')\big\rceil - \big\lceil pw(P_i) - w(Q_i')\big\rceil \\
\geqslant& -\big\lceil w(Q_i) - w(P_i)\big\rceil + \big\lceil pw(Q_i) - pw(P_i)\big\rceil - 1 \\
\geqslant&\big\lceil (p-1)\big(w(Q_i) - w(P_i)\big)\big\rceil - 2 \\
\geqslant&\Big\lceil \frac{(p-1)\gcd(a_1 - a_2, b_1 - b_2)}{b_1 a_2 - b_2 a_1}\Big\rceil - 2 \qquad \text{Lemma 3.8} \\
>&0.
\end{aligned}$$

Then this lemma follows from the following **strict** inequality

$$h(\mathbb{S}_i^\star) = h(\mathbb{S}_i^\star, \tau_i) > h(\mathbb{S}_{i+1}^\star, \tau_{i+1}) \geqslant h(\mathbb{S}_{i+1}^\star). \qquad \square$$

Proof of Proposition 3.2. First, we fix a subset $\mathbb{S}' \in \mathscr{M}_\ell$ such that

$$h(\mathbb{S}') = \min_{\mathbb{S} \in \mathscr{M}_\ell} \big(h(\mathbb{S})\big).$$

Let $\widetilde{\mathbb{S}}^\star$ be an arbitrary submultiset in $\mathscr{M}_\ell(n)$ such that

$$h(\widetilde{\mathbb{S}}^\star) = \min_{\mathbb{S}^\star \in \mathscr{M}_\ell(n)} \big(h(\mathbb{S}^\star)\big).$$

By Lemma 3.9, we know that

$$\sum_{P \in \mathbb{S}'} w(P) = \min_{\mathbb{S} \in \mathscr{M}_\ell} \Big(\sum_{P \in \mathbb{S}} w(P)\Big) \quad \text{and} \quad \sum_{P \in \widetilde{\mathbb{S}}^\star} w(P) = \min_{\mathbb{S}^\star \in \mathscr{M}_\ell(n)} \Big(\sum_{P \in \mathbb{S}^\star} w(P)\Big).$$

It is not hard to see that

$$\sum_{P \in (\mathbb{S}'^\star)^n} w(P) = \sum_{P \in \widetilde{\mathbb{S}}^\star} w(P).$$

Therefore, by Lemma 3.9 again, we have $h(\widetilde{\mathbb{S}}^\star) = h((\mathbb{S}'^\star)^n)$. By Corollary 3.3, we know that

$$h((\mathbb{S}'^\star)^n) = nh(\mathbb{S}').$$

Combining these equalities above gives us (3.12). □

Definition 3.1. *For any subset $\mathbb{S}$ of $\mathbb{M}(\Delta)$, we write*

$$\det(\mathbb{S})_f = \sum_{\tau \in \mathrm{Iso}(\mathbb{S})} \mathrm{sgn}(\tau) \prod_{P \in \mathbb{S}} e_{p\tau(P)-P}.$$

Then as a corollary of Proposition 3.2, we get the following.

Proposition 3.3. *We have*

$$v_T\Big(\prod_{j=0}^{n-1} \sigma_{\mathrm{Frob}}^j(\det(\mathbb{T}_k)_f) - u_{\mathbb{x}_k, nh(\mathbb{T}_k)} T^{nh(\mathbb{T}_k)}\Big) \geqslant nh(\mathbb{T}_k) + 1,$$

where $u_{\mathbb{x}_k, nh(\mathbb{T}_k)}$ is defined in (2.2).

Proof. By Lemma 3.9, we know that $\mathbb{T}_k^{\star n}$ is the only element in $\mathscr{M}_{\mathbb{x}_k}(n)$ which makes (2.13) an equality. Therefore, we have

$$v_T\Big(u_{\mathbb{x}_k, nh(\mathbb{T}_k)} T^{nh(\mathbb{T}_k)} - \prod_{j=0}^{n-1} \big(\sum_{\tau_j = \mathrm{Iso}(\mathbb{T}_k)} \mathrm{sgn}(\tau_j) \prod_{P \in \mathbb{T}_k} \sigma_{\mathrm{Frob}}^j(e_{p\tau_j(P)-P})\big)\Big) \geqslant nh(\mathbb{T}_k) + 1.$$

Then this proposition follows directly from checking the definition of $\det(\mathbb{T}_k)_f$. □

Notation 3.2. *For each character $\chi : \mathbb{Z}_p \to \mathbb{C}_p^\times$ of conductor p, from (LWei, Theorem 1.4), $L_f^*(\chi, s)^{-1}$ is a polynomial of degree $a_2b_1 - a_1b_2$. We denote its q-adic Newton slopes by*

$$\Big(\alpha_1, \alpha_2, \ldots, \alpha_{a_2b_1 - a_1b_2}\Big)$$

in a non-descending order and put $\Sigma(\chi) := \sum_{j=1}^{\mathbb{x}_1} \alpha_j$.

Lemma 3.10. *For each character* $\chi : \mathbb{Z}_p \to \mathbb{C}_p^\times$ *of conductor* p*, the normalized Newton polygon of* $C_f^*(\chi, s))$*, i.e.* $\mathrm{NP}(\chi, s)_C$ *is not above points*

$$\Big(\mathbb{x}_k, \big[(a_2b_1 - a_1b_2)\sum_{i=1}^{k-1} i^2 - \frac{1}{2}(l_1 + l_2)\sum_{i=1}^{k-1} i + \mathbb{x}_1(k-1)k + k\Sigma(\chi)\big](p-1)\Big)$$

for all integers $k \geqslant 0$.

Proof. First recall that $n = [\mathbb{F}_q : \mathbb{F}_p]$ is the degree of the coefficient field of f (see chapter 2). It is well known that the roots of $L_f^*(\chi, s)^{-1}$ are Weil numbers of weight 0, n, or $2n$. We put them into three classes according to the Weil weights:

Weil weight	the number of roots of $L_f^*(\chi, s)^{-1}$
0	1
n	$l_1 + l_2$
$2n$	$a_2b_1 - a_1b_2 - l_1 - l_2 - 1$

Since α_i's are the q-adic Newton slopes of $L_f^*(\chi, s)^{-1}$, we know easily that they belong to $[0, 2)$. Moreover, an algebraic number, say z, and its complex dual $\overline{z}$ are both roots of $L_f^*(\chi, s)^{-1}$ or both not. Suppose that they are roots of $L_f^*(\chi, s)^{-1}$ and z as Weil weight t. Then we have $v_p(z) + v_p(\overline{z}) = t$. Therefore, the sum of all q-adic Newton slopes of $L_f^*(\chi, s)^{-1}$ can be computed as follows:

$$\begin{aligned} &(a_2b_1 - a_1b_2 - l_1 - l_2 - 1) \times 1 + (l_1 + l_2) \times \frac{1}{2} + 1 \times 0. \\ =&a_2b_1 - a_1b_2 - \tfrac{1}{2}(l_1 + l_2) - 1. \end{aligned} \tag{3.15}$$

On the other hand, from (1.1), i.e.

$$C_f^*(\chi,s)=\prod_{j=0}^{\infty}L_f^*(\chi,q^js)^{-(j+1)}, \tag{3.16}$$

we know that

$$\Big(\biguplus_{i=0}^{k-1}\{\alpha_1+i,\alpha_2+i,\ldots,\alpha_{a_2b_1-a_1b_2}+i\}^\star\Big)^{i+1}\uplus\Big(\{\alpha_1+k-1,\alpha_2+k-1,\ldots,\alpha_{\mathbb{x}_1}+k-1\}^\star\Big)^k \tag{3.17}$$

is included in the set of q-adic Newton slopes of $C_f^*(\chi,s)$ as multisets and its cardinality is equal to $\mathbb{x}_k$. Since elements in this set are not necessary to be the smallest $\mathbb{x}_k$ Newton slopes of $C_f^*(\chi,s)$, then the height of $\mathrm{NP}(\chi,s)_C$ at $x=\mathbb{x}_k$ is not above the sum

$$\begin{aligned}&(p-1)\Big[\sum_{i=1}^{k-1}i\sum_{j=1}^{a_2b_1-a_1b_2}(i-1+\alpha_j)+k\sum_{j=1}^{\mathbb{x}_1}(k-1+\alpha_j)\Big]\\ =&(p-1)\Big[(a_2b_1-a_1b_2)\sum_{i=1}^{k-1}i^2-(\frac{1}{2}(l_1+l_2)+1)\sum_{i=1}^{k-1}i+\mathbb{x}_1(k-1)k+k\Sigma(\chi)\Big],\end{aligned} \tag{3.18}$$

where $p-1$ is from normalization in the definition of $\mathrm{NP}(\chi,s)_C$. □

Lemma 3.11. *For each $k\geqslant 1$,*

(1) *both $(\mathbb{x}_k,h(\mathbb{T}_k))$ and $(\mathbb{x}'_k,h(\mathbb{T}'_k))$ are vertices of* $\mathrm{IHP}(\Delta)$*, and*

(2) *the segment with endpoints $(\mathbb{x}_k,h(\mathbb{T}_k))$ and $(\mathbb{x}'_k,h(\mathbb{T}'_k))$ is contained in* $\mathrm{IHP}(\Delta)$.

Proof. (1) Suppose the lemma were false. Then there exists an integer k and a segment in $\mathrm{IHP}(\Delta)$, say $\overline{P_1P_2}$, such that $P_0:=(\mathbb{x}_k,h(\mathbb{T}_k))$ is either a point strictly above $\overline{P_1P_2}$ or an interior point on $\overline{P_1P_2}$. From Proposition 3.2, we know that

$$P_1=\Big(\mathbb{x}_k-i_1,\min_{\mathbb{S}\in\mathscr{M}_{\mathbb{x}_k-i_1}}(h(\mathbb{S}))\Big)\quad\text{and}\quad P_2=\Big(\mathbb{x}_k+i_2,\min_{\mathbb{S}\in\mathscr{M}_{\mathbb{x}_k+i_2}}(h(\mathbb{S}))\Big)$$

for some positive integers i_1 and i_2.

Put $\mathbb{S}_1$ to be an element of $\mathscr{M}_{\mathbb{x}_k - i_1}$ such that

$$\sum_{P \in \mathbb{S}_1} w(P) = \min_{\mathbb{S} \in \mathscr{M}_{\mathbb{x}_k - i_1}} \Big(\sum_{P \in \mathbb{S}} w(P) \Big). \tag{3.19}$$

By Lemma 3.9, we get

$$h(\mathbb{S}_1) = \min_{\mathbb{S} \in \mathscr{M}_{\mathbb{x}_k - i_1}} \big(h(\mathbb{S}) \big). \tag{3.20}$$

It is easy to know that $\mathbb{S}_1$ is a subset of $\mathbb{T}_k$. We denote its complement in $\mathbb{T}_k$ by $\mathbb{S}_1'$, which is of cardinality i_1. By Lemma 3.8, we know that each point P in $\mathbb{T}_k$ satisfies

$$w(P) \leqslant k - \frac{\gcd(a_1 - a_2, b_1 - b_2)}{a_2 b_1 - a_1 b_2}.$$

Combining it with

$$h_2(\mathbb{S}_1') \leqslant \#\mathbb{S}_1' = i_1,$$

we have

$$\begin{aligned} h(\mathbb{T}_k) &\leqslant h(\mathbb{S}_1) + h(\mathbb{S}_1') = h(\mathbb{S}_1) + h_1(\mathbb{S}_1') + h_2(\mathbb{S}_1') \\ &\leqslant h(\mathbb{S}_1) + i_1(p-1) \left[k - \frac{\gcd(a_1 - a_2, b_1 - b_2)}{a_2 b_1 - a_1 b_2} \right] + i_1. \end{aligned}$$

It simply implies that the slope of $\overline{P_1 P_0}$ is less than or equal to

$$(p-1) \left[k - \frac{\gcd(a_1 - a_2, b_1 - b_2)}{a_2 b_1 - a_1 b_2} \right] + 1.$$

On the other hand, by a similar argument, we choose an element $\mathbb{S}_2$ from $\mathscr{M}_{\mathbb{x}_k + i_2}$ such that

$$\sum_{P \in \mathbb{S}_2} w(P) = \min_{\mathbb{S} \in \mathscr{M}_{\mathbb{x}_k + i_2}} \big(\sum_{P \in \mathbb{S}} w(P) \big).$$

By Lemma 3.9 again, we have

$$h(\mathbb{S}_2) = \min_{\mathbb{S}\in\mathscr{M}_{\pi_k+i_2}} \big(h(\mathbb{S})\big). \tag{3.21}$$

We also easily know that $\mathbb{T}_k$ is included in $\mathbb{S}_2$. Let τ be a minimal permutation of $\mathbb{S}_2$. We shall construct below a finite sequence of permutations of $\mathbb{S}_2$, denoted by $(\tau_0 = \tau, \tau_1, \ldots, \tau_m)$, satisfying

(a) the length m of this sequence is less than or equal to i_2,

(b) $h(\tau_{i+1}) \leqslant h(\tau_i) + 1$, and

(c) τ_m fixes every point in $\mathbb{S}_2\backslash\mathbb{T}_k$.

Put $\tau_0 = \tau$. Assume that we have τ_i already. If it fixes each point in $\mathbb{S}_2\backslash\mathbb{T}_k$, then we are done. Otherwise put P_i to be a point in $\mathbb{S}_2\backslash\mathbb{T}_k$ such that $\tau_i(P_i) \neq P_i$. Then we define τ_{i+1} the same permutation as τ_i except we swap images of P_i and $\tau_i^{-1}(P_i)$. Iterating this process gives us a sequence of permutations of $\mathbb{S}_2$. If τ_m is the last element in this sequence, we know that it fixes each point in $\mathbb{S}_2\backslash\mathbb{T}_k$, namely,

$$\tau_m(P) = P \quad \text{for each } P \in \mathbb{S}_2\backslash\mathbb{T}_k.$$

Since there are at most i_2 points in $\mathbb{S}_2$ whose images are changed by these modifications, we know that $m \leqslant i_2$. Put $Q_i = \tau_i(P_i)$ and $P_i' = \tau_i^{-1}(P_i)$. We compute

$$\begin{aligned}
&h(\tau_i) - h(\tau_{i+1}) \\
=&\lceil w(pQ_i - P_i)\rceil + \lceil w(pP_i - P_i')\rceil - \lceil w(pQ_i - P_i)\rceil - \lceil w(pP_i - P_i')\rceil \\
\geqslant&1
\end{aligned}$$

Then we simply prove that the constructed sequence of permutations of $\mathbb{S}_2$ satisfies conditions

(a)-(c) above. Moreover, we have

$$h_2(\mathbb{S}_2, \tau) \geqslant h_2(\mathbb{S}_2, \tau_m) - i_2.$$

As τ is minimal, we get

$$\begin{aligned} h(\mathbb{S}_2) =& h_1(\mathbb{S}_2) + h_2(\mathbb{S}_2, \tau) \\ \geqslant& h_1(\mathbb{S}_2) + h_2(\mathbb{S}_2, \tau_m) - i_2 \\ =& h(\mathbb{S}_2, \tau_m) - i_2. \end{aligned} \tag{3.22}$$

Since the restriction of τ_m on $\mathbb{T}_k$ is a permutation of $\mathbb{T}_k$ and $w(P) \geqslant k$ for any point P in $\mathbb{S}_2 \backslash \mathbb{T}_k$, we have

$$\begin{aligned} h(\mathbb{S}_2, \tau_m) &= h\left(\mathbb{T}_k, \tau_m\big|_{\mathbb{T}_k}\right) + h\left(\mathbb{S}_2 \backslash \mathbb{T}_k, \tau_m\big|_{\mathbb{S}_2 \backslash \mathbb{T}_k}\right) \\ &\geqslant h\left(\mathbb{T}_k\right) + h_1(\mathbb{S}_2 \backslash \mathbb{T}_k) \\ &\geqslant h\left(\mathbb{T}_k\right) + i_2(p-1)k. \end{aligned} \tag{3.23}$$

By (3.22) and (3.23), the slope of $\overline{P_0P_2}$ is greater than or equal to

$$k(p-1) - 1.$$

Under the assumption $p > \frac{2(a_2b_1 - a_1b_2)}{\gcd(a_1 - a_2, b_1 - b_2)} + 1$ in Theorem 3.1, it is easy to check that the slope of $\overline{P_0P_2}$ is strictly greater than the slope of $\overline{P_1P_0}$, which is a contradiction.

By a similar argument, we know that $(\mathbb{x}'_k, h(\mathbb{T}'_k))$ is also a vertex of $\mathrm{IHP}(\Delta)$.

(2) Let $0 \leqslant i \leqslant \mathbb{x}'_k - \mathbb{x}_k$. By Lemma 3.9, there exists $\mathbb{T}_k \subset \mathbb{S}'_i \subset \mathbb{T}'_k$ such that

$$h(\mathbb{S}'_i) = \min_{\mathbb{S} \in \mathscr{M}_{\mathbb{x}_k + i}} (h(\mathbb{S})).$$

Since all points in $\mathbb{T}'_k \backslash \mathbb{T}_k$ have integer weight k, the we have

$$h(\mathbb{S}'_i) = h(\mathbb{T}_k) + ik(p-1),$$

which implies (2) immediately. □

Lemma 3.12. *Let χ_1 be a nontrivial finite character. Suppose that $\mathrm{NP}(f,\chi_1)_C$ coincides with $\mathrm{IHP}(\Delta)$ at point $\big(\mathbb{x}_{k_1}, h(\mathbb{T}_{k_1})\big)$ for a positive integer k_1. Then*

(1) *$\big(\mathbb{x}_{k_1}, h(\mathbb{T}_{k_1})\big)$ is also a vertex of $\mathrm{NP}(f,\chi_1)_C$, and*

(2) *$u_{\mathbb{x}_{k_1}, nh(\mathbb{T}_{k_1})}$ is a $\mathbb{Z}_p$-unit.*

Proof. (1) This follows from the fact that the normalized Newton polygon $\mathrm{NP}(f,\chi_1)_C$ always lies above the improved Hodge polygon $\mathrm{IHP}(\Delta)$ by Proposition 2.2 and that $\big(\mathbb{x}_{k_1}, h(\mathbb{T}_{k_1})\big)$ is a vertex of $\mathrm{IHP}(\Delta)$ by Lemma 3.11.

(2) Suppose that $u_{\mathbb{x}_{k_1}, nh(\mathbb{T}_{k_1})}$ is not a $\mathbb{Z}_p$-unit. Since we know that $(\mathbb{x}_{k_1}, h(\mathbb{T}_{k_1}))$ is a vertex of $\mathrm{NP}(f,\chi_1)_C$, then specializing $\mathrm{NP}(f,T)_C$ to $T = \chi_1(1) - 1$ makes $\mathrm{NP}(f,\chi_1)_C$ strictly higher than $\mathrm{NP}(f,T)_C$ at $x = \mathbb{x}_{k_1}$. By Lemma 2.2, it is also strictly higher than $\mathrm{IHP}(\Delta)$ at this point, which leads to a contradiction. □

Proof of Theorem 3.1. Let $\chi_0 : \mathbb{Z}_p \to \mathbb{C}_p^\times$ be a nontrivial character of conductor p. Since $\mathrm{NP}(f,\chi_0)_C$ is not below $\mathrm{IHP}(\Delta)$ and the expression in (3.18) is an upper bound for $\mathrm{IHP}(\Delta)$ at $x = \mathbb{x}_k$ for each $k \geqslant 1$, then we have

$$\begin{aligned} &k\Big[\frac{h(\mathbb{T}_1)}{p-1} + \mathbb{x}_1(k-1)\Big] + \sum_{i=0}^{k-2}\big[(a_2b_1 - a_1b_2)(i+1) - \frac{1}{2}(l_1+l_2)\big](i+1) \\ \leqslant &\mathbb{x}_1(k-1)k + k\Sigma(\chi_1) + (a_2b_1 - a_1b_2)\sum_{i=1}^{k-1} i^2 - \Big[\frac{1}{2}(l_1+l_2)+1\Big]\sum_{i=1}^{k-1} i. \end{aligned} \tag{3.24}$$

A simplification of these inequalities above shows that they all equivalent to

$$h(\mathbb{T}_1) \leqslant (p-1)\Sigma(\chi_0), \tag{3.25}$$

an equality independent of k.

Since $\mathrm{NP}(f,\chi_1)_C$ coincides with $\mathrm{IHP}(\Delta)$ at $\big(\mathbb{x}_{k_1}, h(\mathbb{T}_{k_1})\big)$ for a finite character χ_1 and an integer k_1, by Lemma 3.12, we know that $u_{\mathbb{x}_{k_1},nh(\mathbb{T}_{k_1})}$ is a $\mathbb{Z}_p$-unit. It implies that $\mathrm{NP}(f,\chi_0)_C$ also coincides with $\mathrm{IHP}(\Delta)$ at $(\mathbb{x}_{k_1}, h(\mathbb{T}_{k_1}))$. Therefore, by Lemma 3.11 (2), the slopes of segments in $\mathrm{NP}(f,\chi_0)_C$ after points $x = \mathbb{x}_{k_1}$ are all greater than or equal to $(p-1)k_1$.

One the other hand, recall that in Notation 3.2 we put $\{\alpha_1, \alpha_2, \ldots, \alpha_{a_2b_1-a_1b_2}\}$ (in a non-decreasing order) to be the set of q-adic Newton slopes for $L_f^*(\chi_0, s)$, which is contained in $[0,2)$. Therefore, each q-adic Newton slope of $L_f^*(\chi_0, q^i s)$ belongs to $[i, i+2)$. Then from the decomposition of $C_f^*(\chi_0, s)$ in (3.16), we know that $\alpha_j + k_1 - 1 \geqslant k_1$ for all $j \geqslant \mathbb{x}_1 + 1$. For otherwise there are more than $\mathbb{x}_{k_1}$ roots of $C_f^*(\chi_0, s)$ whose q-adic valuations are less than or equal to k_1, which is a contradiction to the statement in the previous paragraph.

From the argument above, we see that (3.24) must be an equality, and when $k = k_1$, the height of $\mathrm{NP}(\chi_0, s)_C$ coincides with its upper bound given in (3.18). Hence, we have

$$h(\mathbb{T}_1) = (p-1)\Sigma(\chi_0).$$

Notice that (3.25) is independent of k. Then the inequalities in (3.24) are equalities for all $k \geqslant 0$. Combining it with Proposition 3.12, we have that $u_{\mathbb{x}_k,nh(\mathbb{T}_k)}$ is a $\mathbb{Z}_p$-unit for each $k \geqslant 0$. Therefore, it is not hard to show that $\mathrm{NP}(f,\chi)_C$ coincides with $\mathrm{IHP}(\Delta)$ at $(\mathbb{x}_k, h(\mathbb{T}_k))$ for any integer k and nontrivial finite character χ. Then by Lemma 3.11 again, we know that $\alpha_i \geqslant 1$ for $\mathbb{x}_1 \leqslant i \leqslant \mathbb{x}_1'$. Combining it with Poincaré duality, we have $\alpha_i = 1$ for $\mathbb{x}_1 + 1 \leqslant i \leqslant \mathbb{x}_1'$. It implies that $\mathrm{IHP}(\Delta)$ and $\mathrm{NP}(f,\chi)_C$ coincide at $x = \mathbb{x}_k + i_k$ for any

$0 \leqslant i_k \leqslant \mathbb{x}'_k - \mathbb{x}_k$.

By a similar argument to Lemma 3.12 (2), we know that $u_{\mathbb{x}'_k, nh(\mathbb{T}'_k)}$ is also a $\mathbb{Z}_p$-unit. $\square$

Chapter 4

The case when Δ is an isosceles right triangle I.

In order to apply Theorem 3.1 we need that $\mathrm{NP}(f,\chi_1)_C$ coincides with $\mathrm{IHP}(\Delta)$ at $x=\mathbb{x}_{k_1}$ for some character χ_1 and some integer k_1. This however seems to be a very difficult question. We have the following folklore conjecture.

Conjecture 4.1. *Let Δ be a triangle with vertices at $(0,0)$, $\mathbf{P}_1=(a_1,b_1)$, $\mathbf{P}_2=(a_2,b_2)$. We assume the hypotheses (as in Theorem 3.1) on the prime p. In the moduli space of all polynomials $f(x_1,x_2)$ of convex hull Δ, there exists an open dense subspace over which the corresponding Newton polygon $\mathrm{NP}(f,\chi)_C$ agrees with $\mathrm{IHP}(\Delta)$ at $x=\mathbb{x}_k+i_k$ for all finite characters χ, integers $k\geqslant 1$ and $0\leqslant i_k\leqslant \mathbb{x}'_k-\mathbb{x}_k$.*

Generically, the Newton polygon of $C_f^*(\chi,s)$ should be as low as possible, namely, coinciding with the improved Hodge bound $\mathrm{IHP}(\Delta)$.

In this chapter, we will study a special case when Δ is an isosceles right triangle with vertices at $(0,0)$, $(d,0)$ and $(0,d)$, where $p\nmid d$. We claim that Conjecture 4.1 holds true when the

residue of p modulo d is small enough. More precisely, we will prove the following.

Theorem 4.1. *Let p_0 be the residue of p modulo d, and let d_0 be the residue of d modulo p_0. Conjecture 4.1 holds when*

$$d \geqslant \begin{cases} 4p_0^{\frac{3}{2}}\Big[\ln 3 + \frac{27}{4} + (2+\frac{3}{\ln 2})\ln p_0\Big] + 13p_0 & \text{if } h \geqslant \frac{1}{4}, \\ 4p_0^{\frac{5-2h}{3}}\Big[\ln 3 + \frac{27}{4} + (2+\frac{3}{\ln 2})\ln p_0\Big] + 13p_0 & \text{if } h < \frac{1}{4}, \end{cases} \tag{4.1}$$

where $h := \log_{p_0}(p_0 - d_0)$.

In particular, the condition $d \geqslant 24(2p_0^2 + p_0)$ implies (4.1); so Theorem 1.1 follows from this. We will complete the proof at the end of this chapter.

4.1 An interpretation of Theorem 4.1.

First, we consider the "*universal polynomial*"

$$f_{\mathrm{univ}}(x_1, x_2) = \sum_{P \in \Delta \cap \mathbb{M}(\Delta)} \widetilde{a}_P x_1^{P_x} x_2^{P_y}$$

whose coefficients are treated as variables.

Notation 4.1. *Recall the infinite matrix N defined in Proposition 2.2. Let $\widetilde{N}$ be the matrix given by substituting $\hat{a}_P$ in N by $\widetilde{a}_P$. More rigorously, we put*

$$E_{f_{univ}}(x_1, x_2) := \sum_{P \in \mathbb{Z}^2_{\geqslant 0}} \widetilde{e}_P(\underline{\widetilde{a}}, T) x_1^{P_x} x_2^{P_y} \in \mathbb{Z}_p[\underline{\widetilde{a}}][\![T, x_1, x_2]\!],$$

and write

$$\widetilde{e}_P := \widetilde{e}_P(\underline{\widetilde{a}}, T).$$

Similar to Lemma 2.1, we have

$$\widetilde{e}_P \in T^{\lceil w(P) \rceil}\mathbb{Z}_p[\underline{\widetilde{a}}][\![T]\!] \quad \textit{and} \quad \widetilde{e}_O = 1. \tag{4.2}$$

Then, using the list $(P_1, P_2, \dots)$ *of points in* $\mathbb{M}(\Delta)$ *given in Notation 2.6, we define* $\widetilde{N}$ *to be the infinite matrix whose* (i,j) *entry is* $\widetilde{e}_{pP_i - P_j} \in \mathbb{Z}_p[\underline{\widetilde{a}}][\![T]\!]$.

Similar to Definition 3.1, we put

$$\begin{aligned} \det(\mathbb{T}_1)_{univ} &= \sum_{\tau \in \mathrm{Iso}(\mathbb{T}_1)} \mathrm{sgn}(\tau) \prod_{P \in \mathbb{T}_1} \widetilde{e}_{p\tau(P)-P} \\ &= \sum_{i=h(\mathbb{T}_1)}^{\infty} \widetilde{v}_i T^i \in \mathbb{Z}_p[\underline{\widetilde{a}}][\![T]\!], \end{aligned}$$

where $\mathrm{sgn}(\tau)$ *is the sign of* τ *as a permutation.*

Since all results in Section 3 for the "fixed" f actually hold for on general polynomials $f(x_1, x_2) \in \overline{\mathbb{F}}_p[x_1, x_2]$, we have the following.

Proposition 4.1. *The polygons* $\mathrm{GNP}(\Delta)$ *and* $\mathrm{IHP}(\Delta)$ *coincide at* $\big(\mathbb{x}_1, h(\mathbb{T}_1)\big)$ *if and only if* $\widetilde{v}_{h(\mathbb{T}_1)}$ *is not divisible by* p.

Moreover, when either condition holds, Conjecture 4.1 holds for that Δ.

Proof. We first prove the "only if" part. Suppose that $\widetilde{v}_{h(\mathbb{T}_1)}$ is divisible by p. For any pair of a two-variable polynomial $\mathring{f}(x_1, x_2) \in \overline{\mathbb{F}}_p[x_1, x_2]$ with convex hull Δ and a finite character $\mathring{\chi}$ of conductor $p^{m_{\mathring{\chi}}}$, we write $\mathring{v}_{h(\mathbb{T}_1)} \in \mathbb{Z}_{p^{n(\mathring{f})}}[\zeta_{p^{m_{\mathring{\chi}}}}]$ as the specialization of $\widetilde{v}_{h(\mathbb{T}_1)}$ at $T = \mathring{\chi}(1) - 1$ and at $\widetilde{a}_P$ equals to the Teichmuller lifts of the coefficients of f, where $\zeta_{p^{m_{\mathring{\chi}}}}$ is a primitive $p^{m_{\mathring{\chi}}}$-th root of unity. Then we have

$$v_p(\mathring{v}_{h(\mathbb{T}_1)}) \geqslant \frac{h(\mathbb{T}_1)}{p^{m_{\mathring{\chi}}-1}(p-1)} + 1.$$

As in (1.1), we denote

$$C^*_{\mathring{f}}(\mathring{\chi}, s) = \prod_{j=0}^{\infty} L^*_{\mathring{f}}(\mathring{\chi}, p^{jn(\mathring{f})}s)^{-(j+1)} = \sum_{k=0}^{\infty} \mathring{u}_k s^k \in \mathbb{Z}_p[\zeta_{p^{m_{\mathring{\chi}}}}][\![s]\!].$$

By Proposition 3.3, we know that

$$v_p\Big(\prod_{i=0}^{n(f)-1} \sigma^i_{\mathrm{Frob}}(\mathring{v}_{h(\mathbb{T}_1)}) - \mathring{u}_{\mathbb{x}_1} \Big) \geqslant \frac{n(\mathring{f})h(\mathbb{T}_1)+1}{p^{m_{\mathring{\chi}}-1}(p-1)},$$

where σ_{Frob} represents the arithmetic Frobenius acting on the coefficients.

Combining the equalities above, we get that

$$v_p(\mathring{u}_k) \geqslant \frac{n(\mathring{f})h(\mathbb{T}_1)+1}{p^{m_{\mathring{\chi}}-1}(p-1)}.$$

Since we choose $\mathring{f}$ and $\mathring{\chi}$ arbitrarily, we know that GNP(Δ) is strictly above IHP(Δ) at $x = \mathbb{x}_1$, a contradiction.

We prove the "if" part. Let $\overline{\widetilde{v}}_{h(\mathbb{T}_1)}$ be the image of $\widetilde{v}_{h(\mathbb{T}_1)}$ in the quotient ring

$$\mathbb{Z}_p[\underline{\widetilde{a}}]/p\mathbb{Z}_p[\underline{\widetilde{a}}] \cong \mathbb{F}_p[\underline{\widetilde{a}}].$$

Since $\widetilde{v}_{h(\mathbb{T}_1)}$ is not divisible by p, we know that $\overline{\widetilde{v}}_{h(\mathbb{T}_1)} \neq 0$.

Recall that we defined $\mathbb{T}'_1 = \{P \in \mathbb{M}(\Delta) \mid w(P) \leqslant 1\}$ and $\mathbb{x}'_1$ to be its cardinality in Notation 1.1. Let $f_1(x_1, x_2) = \sum_{P \in \mathbb{T}'_1} b_P x_1^{P_x} x_2^{P_y} \in \overline{\mathbb{F}}_p[x_1, x_2]$ be a polynomial satisfies that

- f_1 has convex hull Δ.
- $\overline{\widetilde{v}}_{h(\mathbb{T}_1)}|_{\widetilde{a}_P = b_P} \neq 0$.

It is easy to check that for any finite character χ of conductor p, NP$(f_1, \chi)_L$ coincides with

IHP(Δ) at $x = \mathbb{x}_1$. Since GNP(Δ) is not below IHP(Δ) and the set of polynomials which satisfy these conditions forms a Zariski open subset in the affine space $\mathbb{A}^{\mathbb{x}'_1}_{\mathbb{F}_p}$, we complete the proof. □

Now we are left to show that $\widetilde{v}_{h(\mathbb{T}_1)}$ is not divisible by p.

Definition 4.1. *We label the elements in* $\mathbb{T}'_1$ *as*

$$\mathbb{T}'_1 := \left\{Q_1, Q_2, \ldots, Q_{\mathbb{x}'_1}\right\}$$

such that $Q_1 := (d, 0)$ *and* $Q_2 := (0, d)$. *Each point* $P \in \mathbb{M}(\Delta)$ *can be written as a linear combination of points in* $\mathbb{T}'_1$ *with non-negative integer coefficients, namely*

$$P = \sum_{i=1}^{\mathbb{x}'_1} b_{P,i} Q_i.$$

We call the vector $\vec{b}_P \in \mathbb{Z}^{\mathbb{x}'_1}_{\geqslant 0}$ *(or the linear combination)* P-minimal *if it satisfies*

$$\sum_{i=1}^{\mathbb{x}'_1} b_{P,i} = \left\lceil w(P) \right\rceil.$$

Definition 4.2. *A* combo*, denoted by* $(\tau, \vec{b}_{\bullet,\tau})$*, is a pair consisting of an arbitrary permutation* τ *of* $\mathbb{T}_1$ *together with, for each* $P \in \mathbb{T}_1$*, a vector* $\vec{b}_{P,\tau} \in \mathbb{Z}^{\mathbb{x}'_1}_{\geqslant 0}$ *such that*

$$\sum_{i=1}^{\mathbb{x}'_1} b_{P,\tau,i} Q_i = p\tau(P) - P. \tag{4.3}$$

A combo $(\tau, \vec{b}_{\bullet,\tau})$ *is called* optimal *if* τ *is minimal and for each* $P \in \mathbb{T}_1$ *vector* $\vec{b}_{P,\tau}$ *is* $\big(p\tau(P) - P\big)$*-minimal.*

A combo $(\tau, \vec{b}_{\bullet,\tau})$ *is optimal if and only if*

$$\sum_{P\in\mathbb{T}_1}\sum_{i=1}^{\mathbb{x}_1'} b_{P,\tau,i} = h(\mathbb{T}_1).$$

We have the following explicit expression of the leading coefficient $\widetilde{v}_{h(\mathbb{T}_1)}$.

Lemma 4.1. *We have*

$$\widetilde{v}_{h(\mathbb{T}_1)} = \sum_{(\tau,\vec{b}_{\bullet,\tau})\ optimal} \operatorname{sgn}(\tau) \prod_{P\in\mathbb{T}_1}\prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{P,\tau,i}}}{b_{P,\tau,i}!}, \tag{4.4}$$

where the sum runs over all optimal combos, and $\operatorname{sgn}(\tau)$ *is the sign of* τ*.*

Proof. We let

$$\prod_{Q\in\mathbb{T}_1'} e^{\widetilde{a}_Q \pi x_1^{Q_x} x_2^{Q_y}} = \sum_{p\in\mathbb{Z}^2_{\geqslant 0}} \widetilde{e}'_P x_1^{P_x} x_2^{P_y}.$$

For any optimal combo $(\tau, \vec{b}_{\bullet,\tau})$, we have

$$b_{P,\tau,i} \leqslant p-1 \quad \text{for each } P \in \mathbb{T}_1 \text{ and } 1 \leqslant i \leqslant \mathbb{x}_1',$$

which implies that

$$\begin{aligned} \det(\mathbb{T}_1)_{\mathrm{univ}} &= \sum_{\tau\in\mathrm{Iso}(\mathbb{T}_1)} \operatorname{sgn}(\tau) \prod_{P\in\mathbb{T}_1} \widetilde{e}'_{p\tau(P)-P} + O(T^{h(\mathbb{T}_1)+1}) \\ &= \sum_{(\tau,\vec{b}_{\bullet,\tau})} \Big(\operatorname{sgn}(\tau) \prod_{P\in\mathbb{T}_1}\prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{P,\tau,i}}}{b_{P,\tau,i}!}\Big) T^{\sum_{P\in\mathbb{T}_1}\sum_{i=1}^{\mathbb{x}_1'} b_{P,\tau,i}} + O(T^{h(\mathbb{T}_1)+1}), \end{aligned} \tag{4.5}$$

where $(\tau, \vec{b}_{\bullet,\tau})$ runs over all combos for $\mathbb{T}_1$ and $O(T^{h(\mathbb{T}_1)+1})$ represents for a power series in $\mathbb{Z}_p[\underline{\widetilde{a}}][\![T]\!]$ of T-adic valuation greater than or equal to $h(\mathbb{T}_1)+1$. Then this lemma follows from the last statement in Definition 4.2. □

Definition 4.3. *Lemma 4.1 gives an explicit expression of* $\widetilde{v}_{h(\mathbb{T}_1)}$ *as the sum of terms labeled by optimal combos. For a combo* $(\tau, \vec{b}_{\bullet,\tau})$*, we call*

$$\operatorname{sgn}(\tau) \prod_{P\in\mathbb{T}_1} \prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{P,\tau,i}}}{b_{P,\tau,i}!}$$

its corresponding monomial*.*

Two combos $(\tau, \vec{b}_{\bullet,\tau})$ *and* $(\tau', \vec{b}'_{\bullet,\tau'})$ *have a same corresponding monomial (with possibly different coefficients) if and only if*

$$\sum_{P\in\mathbb{T}_1} b_{P,\tau,i} = \sum_{P\in\mathbb{T}_1} b'_{P,\tau,i}$$

for all $1 \leqslant i \leqslant \mathbb{x}_1'$*.*

Recall that our task is to prove that $\widetilde{v}_{h(\mathbb{T}_1)}$ is not divisible by p. For this it is enough to show that $\widetilde{v}_{h(\mathbb{T}_1)}$ has a monomial whose coefficient is not divisible by p. To this end, we restrict our study to those monmials corresponding to some "extreme" optimal combos.

Lemma 4.2. *For each combo* $(\tau, \vec{b}_{\bullet,\tau})$ *for* $\mathbb{T}_1$*, we have*

$$\sum_{P\in\mathbb{T}_1} b_{P,\tau,1} \leqslant \sum_{P\in\mathbb{T}_1} \left\lfloor \frac{pP_x}{d} \right\rfloor \quad \textit{and} \quad \sum_{P\in\mathbb{T}_1} b_{P,\tau,2} \leqslant \sum_{P\in\mathbb{T}_1} \left\lfloor \frac{pP_y}{d} \right\rfloor, \tag{4.6}$$

where P_x *and* P_y *are the* x, y*-coordinates of* P*.*

Proof. We will prove the first inequality, and the proof of the second is similar

Recall that $Q_1 = (d, 0)$. By equality (4.3), we get

$$b_{\tau^{-1}(P),\tau,1} \leqslant \left\lfloor \frac{pP_x}{d} \right\rfloor. \tag{4.7}$$

Hence, we have that

$$\sum_{P\in\mathbb{T}_1} b_{P,\tau,1} = \sum_{P\in\mathbb{T}_1} b_{\tau^{-1}(P),\tau,1} \leqslant \sum_{P\in\mathbb{T}_1} \Big\lfloor \frac{pP_x}{d} \Big\rfloor. \qquad \square$$

Definition 4.4. *We call a combo* special *if it is optimal and both inequalities in* (4.6) *are equalities.*

Notice that these two sums are the exponents of $\widetilde{a}_{Q_1}$ and $\widetilde{a}_{Q_2}$ in the corresponding monomial; so special combos contribute to terms in $\widetilde{v}_{h(\mathbb{T}_1)}$ with maximal degrees in the coefficients $\widetilde{a}_{Q_1}$ and $\widetilde{a}_{Q_2}$ at the two vertices of Δ.

Recall that for each point P in $\mathbb{M}(\Delta)$, we denoted by $P\%$ its residue in $\square_\Delta$.

Notation 4.2. *We put* $\mathbb{T}_1 = \mathbb{T}_{1,1} \sqcup \mathbb{T}_{1,2}$, *where* $\mathbb{T}_{1,1} = \{P \in \mathbb{T}_1 \mid (pP)\% \in \mathbb{T}_1\}$ *and* $\mathbb{T}_{1,2}$ *is the complement of* $\mathbb{T}_{1,1}$ *in* $\mathbb{T}_1$. *In other words, we have* $\mathbb{T}_{1,2} = \{P \in \mathbb{T}_1 \mid (pP)\% \notin \mathbb{T}_1\}$.

Example 4.1. *When* $d = 7$ *and* $p = 17$, *the following graph shows the distribution of* $\mathbb{T}_{1,1}$ *and* $\mathbb{T}_{1,2}$ *in* $\mathbb{T}_1$, *where "*$\times$*" and "*$\bullet$*" represent points in* $\mathbb{T}_{1,1}$ *and* $\mathbb{T}_{1,2}$ *respectively.*

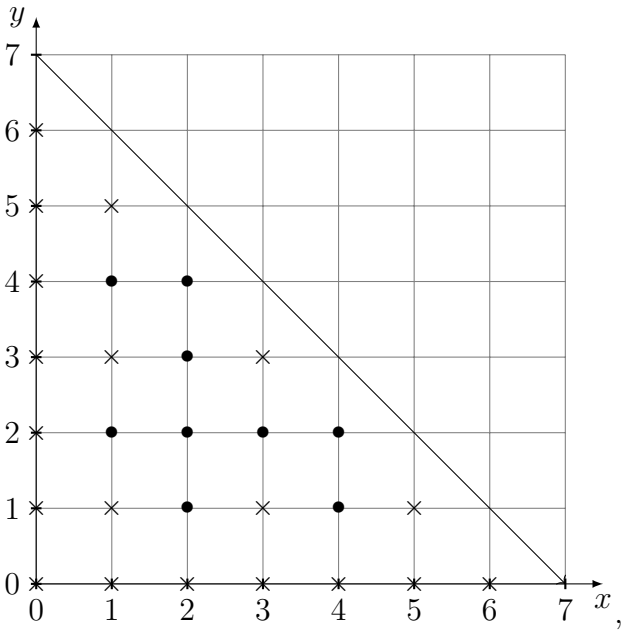

Figure 4.1: The distributions of $\mathbb{T}_{1,1}$ and $\mathbb{T}_{1,2}$ when $d = 7$ and $p = 17$.

Lemma 4.3. *A combo $(\tau, \vec{b}_{\bullet,\tau})$ is special if and only if it satisfies the following two conditions.*

(1) *For each $P \in \mathbb{T}_{1,1}$, we have*

$$\tau^{-1}(P) = (pP)\%$$

and all other $b_{\tau^{-1}(P),\tau,*}$'s are zero except $b_{\tau^{-1}(P),\tau,1}$ and $b_{\tau^{-1}(P),\tau,2}$ which are equal to $i_{P,1}$ and $i_{P,2}$.

(2) *For each $P \in \mathbb{T}_{1,2}$, assume that $Q_{j_P} = (pP)\% - \tau^{-1}(P)$, then we have*

$$(pP)\% - \tau^{-1}(P) \in \mathbb{T}_1'$$

and all other $b_{\tau^{-1}(P),\tau,*}$'s are zero except $b_{\tau^{-1}(P),\tau,1}, b_{\tau^{-1}(P),\tau,2}$ and $b_{\tau^{-1}(P),\tau,j_P}$ which are equal to $i_{P,1}$, $i_{P,2}$ and 1.

In particular, if $(\tau, \vec{b}_{\bullet,\tau})$ is a special combo, then τ uniquely determines $\vec{b}_{\bullet,\tau}$.

Proof. "$\Longleftarrow$". Let $(\tau, \vec{b}_{\bullet,\tau})$ be any combo for $\mathbb{T}_1$ which satisfies these two conditions.

We easily see that for $(\tau, \vec{b}_{\bullet,\tau})$ to be special, it is enough to show that τ is minimal, which follows directly from

$$h(\mathbb{T}_1) \geqslant \sum_{P \in \mathbb{T}_1} \lfloor w(P) \rfloor \quad \text{and} \quad \lceil w(p\tau(P) - P) \rceil = \lfloor w(P) \rfloor.$$

"$\Longrightarrow$". Assume that $(\tau, \vec{b}_{\bullet,\tau})$ fails one of these conditions. Then it is easy to check that the monomial corresponding to this combo either has degree greater than equal to $h(\mathbb{T}_1)$ or the exponent of $\widetilde{a}_{Q_1}$ or $\widetilde{a}_{Q_2}$ is not maximal, a contraction to $(\tau, \vec{b}_{\bullet,\tau})$ being special. □

Example 4.2. *The following gives an example of a minimal permutation of $\mathbb{T}_1$ in the case*

of Example 4.1. Let

$$\begin{aligned}
&\tau^{-1}(0,0)=(0,0), \quad \tau^{-1}(0,1)=(0,3), \quad \tau^{-1}(0,2)=(0,6),\\
&\tau^{-1}(0,3)=(0,2), \quad \tau^{-1}(0,4)=(0,5), \quad \tau^{-1}(0,5)=(0,1),\\
&\tau^{-1}(0,6)=(0,1), \quad \tau^{-1}(1,0)=(3,0), \quad \tau^{-1}(1,1)=(3,3),\\
&\tau^{-1}(1,5)=(3,1), \quad \tau^{-1}(2,0)=(6,0), \quad \tau^{-1}(3,0)=(2,0),\\
&\tau^{-1}(3,1)=(2,3), \quad \tau^{-1}(3,3)=(2,2), \quad \tau^{-1}(4,0)=(5,0),\\
&\tau^{-1}(5,0)=(1,0), \quad \tau^{-1}(5,1)=(1,3), \quad \tau^{-1}(6,0)=(4,0),\\
&\tau^{-1}(1,2)=(2,1), \quad \tau^{-1}(1,4)=(1,1), \quad \tau^{-1}(2,1)=(4,1).\\
&\tau^{-1}(2,2)=(2,4), \quad \tau^{-1}(2,3)=(5,1), \quad \tau^{-1}(2,4)=(1,4),\\
&\tau^{-1}(3,2)=(1,2), \quad \tau^{-1}(4,1)=(4,2), \quad \tau^{-1}(4,2)=(1,5).
\end{aligned}$$

From the last statement in Lemma 4.3, it determines a unique special combo. We leave it to the reader to complete its corresponding special combo.

Lemma 4.4. *There is at least one special (optimal) combo among all combos for* $\mathbb{T}_1$.

Proof. In Definition 4.7, we will give a correspondence between the set of special combos and the set of special bijections (See Definition 4.7); and in (5.19), we construct an explicit special bijection $\widetilde{\beta}$. This lemma follows from an easy check that the combo corresponding to $\widetilde{\beta}$ is special.

Since the construction of $\widetilde{\beta}$ requires nothing but $p > 2d+1$ and d to be relatively large with respect to p_0 (the residue of p modulo d), this is not a circular argument. □

Definition 4.5. *We write* $\widetilde{v}^{\mathrm{sp}}_{h(\mathbb{T}_1)}$ *for*

$$\sum_{(\tau,\vec{b}_{\bullet,\tau})\ special} \mathrm{sgn}(\tau) \prod_{P\in\mathbb{T}_1} \prod_{i=1}^{\mathbb{x}'_1} \frac{(\widetilde{a}_{Q_i})^{b_{P,\tau,i}}}{b_{P,\tau,i}!},$$

where the sum runs over all special combos.

By Lemma 4.4, for Theorem 4.1 to hold, it is enough to prove the following.

Proposition 4.2. *There is a monomial in* $\widetilde{v}^{\mathrm{sp}}_{h(\mathbb{T}_1)}$ *with coefficient not divisible by* p*.*

Its proof will be given later.

By the last statement of Lemma 4.3, we are reduced to studying minimal permutations in special combos, which will be further reduced by the correspondence given in Definition 4.7 soon.

Definition 4.6. *For each point* $P \in \square_\Delta$*, we call point* $(d,d) - P$ *its* mirror reflection *and denote it by* $m(P)$*.*

Notation 4.3. *Let* $\mathbb{Y}$ *be the set consisting of all lattice points strictly inside the upper right triangle of* $\square_\Delta$*. We put*

$$\mathbb{Y}_0 := \Big\{ (pQ)\% \;\Big|\; Q \in \mathbb{T}_{1,2} \Big\}$$

to be a subset of $\mathbb{Y}$*.*

Lemma 4.5. *We have*

$$\Big\{ (pP)\% \;\Big|\; P \in \mathbb{T}_1 \Big\} = \mathbb{Y}_0 \sqcup (\mathbb{T}_1 \backslash m(\mathbb{Y}_0)).$$

Proof. Suppose that there exists a point $P_0 \in \mathbb{T}_1$ such that $P_0 = (pQ_0)\%$ and $m(P_0) = pQ_1\%$ for two points $Q_0, Q_1 \in \mathbb{T}_1$. Let p' be an integer such that $p'p \equiv 1 \pmod{d}$. We know that $(p'P_0)\% = Q_0$ and $[p'm(P_0)]\% = Q_1$ are mirror reflections, a contradiction. $\square$

Figure 4.2 shows the distribution of $\{(pP)\% \mid P \in \mathbb{T}_1\}$ in the case of Example 4.1, where "$\bullet$" and "$\times$" represent points in $\mathbb{Y}_0$ and $\{(pP)\% \mid P \in \mathbb{T}_1\} \backslash \mathbb{Y}_0$ respectively.

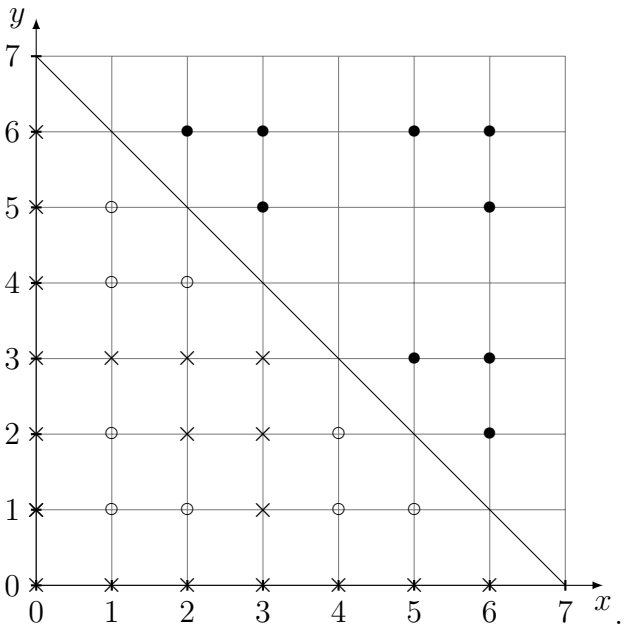

Figure 4.2: The distributions of $\{(pP)\% \mid P \in \mathbb{T}_1\}$ when $d = 7$ and $p = 17$.

Definition 4.7. *A bijection $\beta : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$ is called* special *if $P - \beta(P) \in \mathbb{T}_1'$ for each point $P \in \mathbb{Y}_0$.*

We define a one-to-one correspondence between special combos and special bijections $\beta : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$ is defined as follows:

For a special combo $\left(\tau, \vec{b}_{\bullet,\tau}\right)$, we assign it a special bijection β from $\mathbb{Y}_0$ to $m(\mathbb{Y}_0)$ given by

$$\beta(P) = \tau^{-1}((p'P)\%)$$

for each $P \in \mathbb{Y}_0$.

In the opposite direction, for a special bijection $\beta : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$, we assign to it a special

combo τ given by

$$\tau^{-1}(P) = \begin{cases} (pP)\% & \text{if } P \in \mathbb{T}_{1,1}, \\ \beta((pP)\%) & \text{if } P \in \mathbb{T}_{1,2}. \end{cases}$$

Since the composite of these map is the identity map, it is truly a one-to-one correspondence.

Example 4.3. *The special bijection $\beta : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$ corresponding to the special combo in Example 4.2 is given by*

$$\begin{aligned} &\beta(2,6) = (1,2), \quad \beta(3,5) = (1,1), \quad \beta(3,6) = (2,1), \\ &\beta(5,3) = (4,2), \quad \beta(5,6) = (1,5), \quad \beta(6,2) = (5,1), \\ &\beta(6,3) = (4,1), \quad \beta(6,5) = (1,4), \quad \beta(6,6) = (2,4). \end{aligned}$$

Notation 4.4. *1. For a special bijection β, we let $\tau(\beta) \in \mathrm{Iso}(\mathbb{T}_1)$ denote the minimal permutation of the corresponding special combo. In view of Lemma 4.3, $\tau(\beta)$ uniquely determines β.*

2. The composite $m \circ \beta$ can be viewed as a permutation of $\mathbb{Y}_0$. Then we denote by $\mathrm{sgn}(\beta)$ *the sign of this permutation and also call it the* sign of β.

Lemma 4.6. *We have*

$$\widetilde{v}^{\mathrm{sp}}_{h(\mathbb{T}_1)} = \sum_{\beta \ special} \mathrm{sgn}(\beta) \prod_{P \in \mathbb{T}_1} \prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{P,\tau(\beta),i}}}{b_{P,\tau(\beta),i}!}. \tag{4.8}$$

Proof. First, by the one-to-one correspondence in Definition 4.7, we know that the sum of $\widetilde{v}^{\mathrm{sp}}_{h(\mathbb{T}_1)}$ over all special combos is the same as the sum over all special β's. Let β be special and let $\tau(\beta)$ be the corresponding minimal permutation of $\mathbb{T}_1$. Since the restriction of $\tau(\beta)$

to $\tau(\beta)^{-1}(\mathbb{T}_{1,1}) = \mathbb{T}_1 \backslash m(\mathbb{Y}_0)$ is symmetric about $y = x$, we know that $\mathrm{sgn}(\tau(\beta))$ depends only on $\mathrm{sgn}(\beta)$. More precisely, we have

$$\mathrm{sgn}(\beta) = \mathrm{sgn}\big(\tau(\beta)\big), \qquad \square$$

which completes the proof of this lemma.

Lemma 4.7. (1) *The contribution to* $\widetilde{v}^{\mathrm{sp}}_{h(\mathbb{T}_1)}$ *in* (4.8) *of terms coming from* $P \in \mathbb{T}_{1,1}$ *is same for all special bijections, namely, for two special bijections* $\beta_1, \beta_2 : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$*, we have*

$$\prod_{P \in \mathbb{T}_{1,1}} \prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta_1)^{-1}(P),\tau(\beta_1),i}}}{b_{\tau(\beta_1)^{-1}(P),\tau(\beta_1),i}!} = \prod_{P \in \mathbb{T}_{1,1}} \prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta_2)^{-1}(P),\tau(\beta_2),i}}}{b_{\tau(\beta_2)^{-1}(P),\tau(\beta_2),i}!}.$$

(2) *For the contributions of terms coming from* $P \in \mathbb{T}_{1,2}$*, we have that the equality*

$$\prod_{P \in \mathbb{T}_{1,2}} \prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta_1)^{-1}(P),\tau(\beta_1),i}}}{b_{\tau(\beta_1)^{-1}(P),\tau(\beta_1),i}!} = \prod_{P \in \mathbb{T}_{1,2}} \prod_{i=1}^{\mathbb{x}_1'} \frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta_2)^{-1}(P),\tau(\beta_2),i}}}{b_{\tau(\beta_2)^{-1}(P),\tau(\beta_2),i}!}$$

holds if and only if we have the following equality

$$\Big\{P - \beta_1(P) \;\Big|\; P \in \mathbb{Y}_0\Big\}^{\star} = \Big\{P - \beta_2(P) \;\Big|\; P \in \mathbb{Y}_0\Big\}^{\star} \tag{4.9}$$

as multisets.

Proof. The first statement directly follows from condition (1) for a special permutation in Lemma 4.3.

For any special bijection β, we have

$$\begin{aligned}
&\prod_{P\in\mathbb{T}_{1,2}}\prod_{i=1}^{\mathbb{x}_1'}\frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}}}{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}!}\\
=&\prod_{P\in\mathbb{T}_{1,2}}\prod_{i=1}^{2}\frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}}}{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}!}\times\prod_{P\in\mathbb{T}_{1,2}}\widetilde{a}_{(pP)\%-\tau(\beta)^{-1}(P)}\\
=&\prod_{P\in\mathbb{T}_{1,2}}\prod_{i=1}^{2}\frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}}}{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}!}\times\prod_{P\in\mathbb{Y}_0}\widetilde{a}_{P-\beta(P)}.
\end{aligned}$$

Since

$$\prod_{P\in\mathbb{T}_{1,2}}\prod_{i=1}^{2}\frac{(\widetilde{a}_{Q_i})^{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}}}{b_{\tau(\beta)^{-1}(P),\tau(\beta),i}!}$$

is same to all special permutations, we complete the proof of the second statement. □

Definition 4.8. *We call* $\beta,\beta':\mathbb{Y}_0\to m(\mathbb{Y}_0)$ related *if they satisfy equality* (4.9).

Corollary 4.1. *If* $\beta_1,\beta_2:\mathbb{Y}_0\to m(\mathbb{Y}_0)$ *are two related special bijections and* $\mathrm{sgn}(\beta_1)=\mathrm{sgn}(\beta_2)$*, then they contribute to a same monomial in* $\widetilde{v}_{h(\mathbb{T}_1)}$.

Proposition 4.3. (1) *There exists a special* $\widetilde{\beta}:\mathbb{Y}_0\to m(\mathbb{Y}_0)$ *such that every* β' *related to* $\widetilde{\beta}$ *is even, i.e.* $\mathrm{sgn}(\beta')=1$*, and the number of such* β' *is equal to* 2^i *for some integer* i.

(2) *Therefore, there exists a monomial in* $\widetilde{v}_{\mathbb{x}_1,h(\mathbb{T}_1)}$ *such that its coefficient is in the form of* $\frac{2^i}{\mathscr{N}_1}$*, where* N_1 *is an integer which is not divisible by* p.

Its proof will be completed in chapter 5.

Theorems 4.1, 1.1 and 1.2 would follow from this proposition.

proof of Theorem 4.1 assuming Proposition 4.3. This theorem follows directly from Proposition 4.3, Proposition 4.1 and Theorem 3.1. □

Proof of Theorem 1.1. It is easy to check that $d\geqslant 24(2p_0^2+p_0)$ satisfies (4.1). Therefore,

the only task left is to compute $\mathbb{x}_k$, $\mathbb{x}'_k$ and $h(\mathbb{x}_k)$ explicitly. It follows directly from applying Lemma 3.7 to this specific Δ. □

Proof of Theorem 1.2. Its proof follows from Theorem 1.1 and a consideration of Poincaré duality. □

Chapter 5

The case when $\triangle$ is an isosceles right triangle II.

5.1 Overview

The goal of this chapter is to prove Proposition 4.3 by constructing explicitly the special bijection $\widetilde{\beta} : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$. This is done in several steps. First, for a large subset $\mathbb{L}_1$ of $\mathbb{Y}_0$, we shall define a bijection $\widetilde{\beta}_1$ (i.e. $\widetilde{\beta}|_{\mathbb{L}_1}$) : $\mathbb{L}_1 \to m(\mathbb{L}_1)$ which is "diagonal", namely the line segment $\overline{\widetilde{\beta}_1(P)P}$ is parallel to the line $y = x$. For the remaining points in $\mathbb{Y}_0$, we divide them into two subsets $\mathbb{L}_2$ and $\mathbb{L}_3$ as in (5.1), where $\mathbb{L}_2$ is contained in $\mathbb{K}_1$ (see the blue region in Figure 5.1) as will be proved in Proposition 5.1, and $\mathbb{L}_3$ is contained in the green region in Figure 5.1 by definition.

The map $\widetilde{\beta}_2$ (i.e. $\widetilde{\beta}|_{\mathbb{L}_2}$) will map $\mathbb{L}_2$ into the union of appropriate shifts of the subset $\mathbb{K}_2$ (see the yellow region in Figure 5.1). More precisely, we write $\mathbb{L}_2$ as the disjoint union $\mathbb{L}_{2,i_1} \sqcup \cdots \sqcup \mathbb{L}_{2,i_r}$ (for some non-negative integers $i_1, \ldots, i_r$) and $\widetilde{\beta}_2$ is the union of maps $L_{2,i_k} \to (\mathbb{K}_2 + (i_k p_0, -i_k p_0)) \cap m(\mathbb{Y}_0)$ such that the line segments $\overline{\widetilde{\beta}_2(P)P}$ are parallel for

all points P in a fixed L_{2,i_k}. We extend $\widetilde{\beta}_2$ to a map $\mathbb{s}(\widetilde{\beta}_2)$ on $\mathbb{L}_2 \sqcup m(\mathrm{Im}(\mathbb{L}_2))$ by requiring $\mathbb{s}(\widetilde{\beta}_2)(P) = m \circ \beta^{-1} \circ m(P)$ for any point $P \in m(\mathrm{Im}(\beta))$ and hence determine the preimages of points in $m(\mathbb{L}_2)$ under the map $\widetilde{\beta}$ (see the pink region in Figure 5.1). At last, we write $\widetilde{\beta}_3$ (i.e. $\widetilde{\beta}|_{\mathbb{Y}_0\setminus(\mathbb{L}_1\cup\mathrm{Dom}(\mathbb{s}(\widetilde{\beta}_2))}$) for the unique diagonal symmetric bijection from $\mathbb{Y}_0\setminus\Big(\mathbb{L}_1 \cup \mathrm{Dom}(\mathbb{s}(\widetilde{\beta}_2))\Big)$ to $m(\mathbb{Y}_0)\setminus\Big(m(\mathbb{L}_1) \cup \mathrm{Im}(\mathbb{s}(\widetilde{\beta}_2))\Big)$. Finally we will show that $\widetilde{\beta}_1, \mathbb{s}(\widetilde{\beta}_2)$ and $\widetilde{\beta}_3$ altogether define the needed special bijection $\widetilde{\beta} : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$.

5.2 Construction of $\widetilde{\beta}_1$.

Hypothesis 5.1. *Recall that we put $p_0 = p\%d$. From now on we assume that $p > 2d + 1$ and $p_0 < \frac{d}{6}$.*

Notation 5.1. *Here is a list of symbols:*

- *$\mathscr{D}_k$: the set consisting of all lattice points on the diagonal line $y = x + k$.*
- *$\mathscr{W}_k$: the set consisting of all lattice points on the anti-diagonal line $x + y = k$.*
- *For an interval $I \subseteq \mathbb{R}$, we write $\mathscr{D}_I := \coprod_{i\in I\cap\mathbb{Z}} \mathscr{D}_i$ and $\mathscr{W}_I := \coprod_{i\in I\cap\mathbb{Z}} \mathscr{W}_i$.*
- *$\mathbb{K}_1 := \mathscr{W}_{[2d-3p_0,2d]} \cap \mathscr{D}_{[-p_0,p_0)} \cap \mathbb{Y}$ (see an example in Figure 5.1).*

Definition 5.1. *Let β be an injection from a subset of $\mathbb{Y}_0$ to $m(\mathbb{Y}_0)$.*

1. *We call β* weakly symmetric *if its domain and image are symmetric about the line $y = d - x$; i.e. $\mathrm{Dom}(\beta) = m(\mathrm{Dom}(\beta))$ and $\mathrm{Im}(\beta) = m(\mathrm{Im}(\beta))$.*
2. *We call β* symmetric *if each point $P \in \mathrm{Dom}(\beta)$ satisfies*

$$\beta\big(m(\beta(P))\big) = m(P).$$

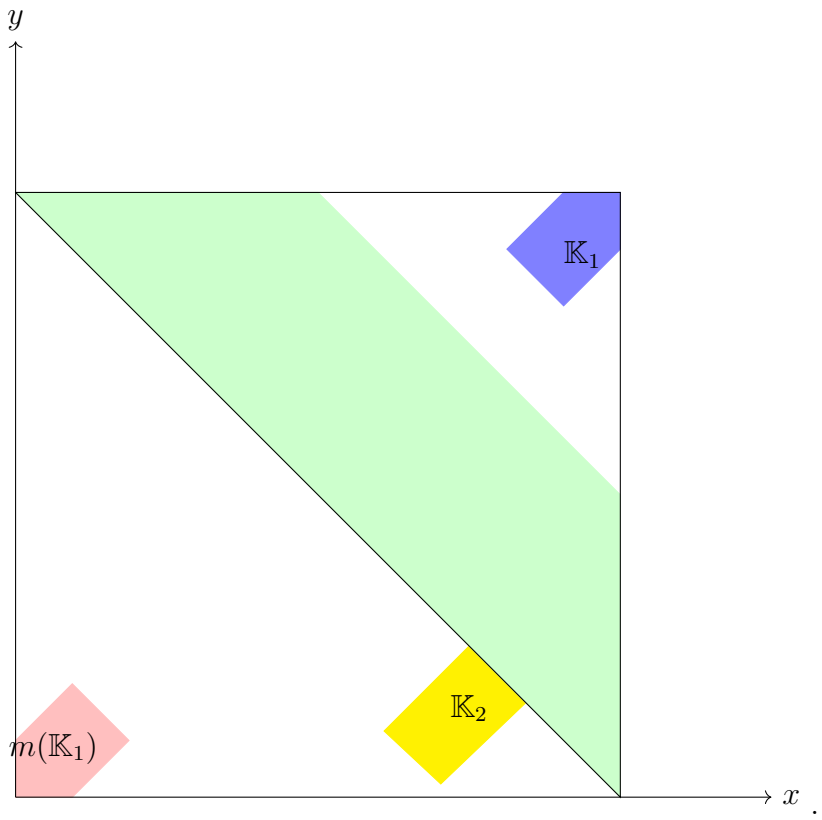

Figure 5.1: Regions $\mathbb{K}_1$ and $\mathbb{K}_2$ when $d = 16$, $p = 19$.

3. If there exists some symmetric map β' with domain included in $\mathbb{Y}_0$ such that

$$\mathrm{Dom}(\beta') = \mathrm{Dom}(\beta) \cup m\big(\mathrm{Im}(\beta)\big) \quad \textit{and} \quad \beta'\big|_{\mathrm{Dom}(\beta)} = \beta,$$

then we call β' the symmetric closure *of β and denoted it by $\mathbb{s}(\beta)$.*

Lemma 5.1. *Let β be an injection from a subset of $\mathbb{Y}_0$ to $m(\mathbb{Y}_0)$. If $\mathrm{Dom}(\beta) \cap m(\mathrm{Im}(\beta)) = \varnothing$, then $\mathbb{s}(\beta)$ exists.*

Proof. Let

- $\mathbb{s}(\beta)\big|_{\mathrm{Dom}(\beta)} = \beta$, and
- for any point $P \in m(\mathrm{Im}(\beta))$ let $\mathbb{s}(\beta)(P) = m \circ \beta^{-1} \circ m(P)$.

It is a trivial check that $\mathbb{s}(\beta)$ is the symmetric closure of β. $\square$

Definition 5.2. *A vector is called* diagonal *if it is parallel to the line $y = x$. Let $V^\star$ be a multiset of vectors. We call it* diagonal *if each $\vec{v} \in V^\star$ is diagonal. We write*

$$\mathscr{V} := \Big\{ V^\star \;\Big|\; V^\star \text{ is a diagonal multiset} \Big\}.$$

We define the weight on vectors on $\mathbb{R}^2$ so that $w(\overrightarrow{OP}) = w(P)$.

For each $V^\star \in \mathscr{V}$ and each $r \in \mathbb{R}$, we write

$$(V^\star)^{\geqslant r} := \Big\{ \vec{v} \in V^\star \;\Big|\; w(\vec{v}) \geqslant r \Big\}.$$

We define a total order "$\prec_1$" on $\mathscr{V}$ as follows:

Definition 5.3. *For any two sets $V_1^\star, V_2^\star \in \mathscr{V}$, we denote $V_1^\star \prec_1 V_2^\star$ if one of the following cases happens:*

Case 1: $\#V_1^\star < \#V_2^\star$;

Case 2: $\#V_1^\star = \#V_2^\star$ *and there exists a real number r_0 such that $\#(V_1^\star)^{\geqslant r} = \#(V_2^\star)^{\geqslant r}$ for all $r > r_0$ but $\#(V_1^\star)^{\geqslant r_0} < \#(V_2^\star)^{\geqslant r_0}$.*

To construct $\widetilde{\beta}$ needed for Proposition 4.3, we shall construct it so that for a largest possible subset $\mathbb{L}_1 \subseteq \mathbb{Y}_0$, $\overrightarrow{\widetilde{\beta}(P)P}$ is diagonal for all $P \in \mathbb{L}_1$, or equivalently, the set $\{P - \beta(P) \mid P \in \mathbb{Y}_0\}$ contains as many diagonal vectors (and as highest weight) as possible.

Definition 5.4. *Let $\mathbb{S}$ be an arbitrary subset of $\mathbb{Y}_0$, and let $\beta : \mathbb{S} \to m(\mathbb{Y}_0)$ be an injection. We set*

$$V^\star(\beta) := \Big\{ P - \beta(P) \;\Big|\; P \in \mathbb{S} \Big\}^\star.$$

If $V^\star(\beta)$ is diagonal, then we also call β diagonal.

Definition 5.5. *We call a pair* (P, Q) *in* $\mathbb{Y}_0 \times m(\mathbb{Y}_0)$ eligible *if it satisfies the following two conditions:*

(a) $\overrightarrow{QP}$ *is diagonal with weight less than or equal to* 1*, and*

(b) either $w(P) > \frac{3}{2}$ *or* $w(Q) < \frac{1}{2}$.

We write

$$\mathscr{E}_1 := \bigcup_{\mathbb{S} \subset \mathbb{Y}_0} \Big\{ \beta : \mathbb{S} \to m(\mathbb{Y}_0) \mid (P, \beta(P)) \text{ is eligible for each } P \in \mathbb{S} \Big\},$$

where $\mathbb{S}$ runs over all subsets of $\mathbb{Y}_0$. For simplicity of notation, we put

$$V(\mathscr{E}_1) := \{ V^\star(\beta) \;\big|\; \beta \in \mathscr{E}_1 \}.$$

Definition 5.6. *Define* $\widetilde{\beta}_1$ *to be an element in* $\mathscr{E}_1$ *such that* $V^\star(\widetilde{\beta}_1)$ *is a maximal element in* $\big(V(\mathscr{E}_1), \prec_1\big)$.

In fact, $\widetilde{\beta}_1$ can be constructed in the following way:

Assume that $\widetilde{\beta}_1$ has been defined on some subset of $\mathbb{Y}_0$, say $\mathbb{Y}_0'$. If there is no eligible pair in $\mathbb{Y}_0 \backslash (\mathbb{Y}_0)' \times m(\mathbb{Y}_0) \backslash \widetilde{\beta}_1(\mathbb{Y}_0')$, then we call the definition of $\widetilde{\beta}_1$ is completed. Otherwise, we choose an eligible pair (P_0, Q_0) in $\mathbb{Y}_0 \backslash \mathbb{Y}_0' \times m(\mathbb{Y}_0) \backslash \widetilde{\beta}_1(\mathbb{Y}_0')$ which maximizes the weight $w(P_0 - Q_0)$, and define $\widetilde{\beta}_1(P_0) = Q_0$.

Lemma 5.2. *The map* $\widetilde{\beta}_1$ *is the unique maximal element in the totally ordered set* $(V(\mathscr{E}_1), \prec_1)$.

Proof. Assume that we have defined β_1 on the subset $\mathbb{Y}_0'$ by the construction above and

(P_0, Q_0) and (P_0', Q_0') are two eligeble pairs in $\mathbb{Y}_0 \backslash (\mathbb{Y}_0)' \times m(\mathbb{Y}_0) \backslash \widetilde{\beta}_1(\mathbb{Y}_0')$ which maximize

$$w(P_0 - Q_0) = w(P_0' - Q_0').$$

Since $\overrightarrow{Q_0 P_0}$ and $\overrightarrow{Q_0' P_0'}$ are required to be diagonal, we know that $P_0 \neq P_0'$ and $Q_0 \neq Q_0'$. Therefore, the definition of $\widetilde{\beta}_1$ is independent of the choices of pairs. □

Write $\mathbb{L}_1$ for the domain of $\widetilde{\beta}_1$. Since we require $\widetilde{\beta}_1$ to be the maximal element in $V(\mathscr{E}_1)$, tt is easily known that $\widetilde{\beta}_1$ is symmetric. Put

$$\mathbb{L}_2 := \left\{ P \in \mathbb{Y}_0 \backslash \mathbb{L}_1 \;\middle|\; w(P) > \frac{3}{2} \right\} \quad \text{and} \quad \mathbb{L}_3 := \left\{ P \in \mathbb{Y}_0 \backslash \mathbb{L}_1 \;\middle|\; w(P) \leqslant \frac{3}{2} \right\}. \tag{5.1}$$

Then we obtain a disjoint decomposition of $\mathbb{Y}_0$ as

$$\mathbb{Y}_0 = \mathbb{L}_1 \sqcup \mathbb{L}_2 \sqcup \mathbb{L}_3.$$

We next will

1. define a map $\widetilde{\beta}_2$ on $\mathbb{L}_2$,
2. find its symmetric closure $\mathbb{s}(\widetilde{\beta}_2)$,
3. define a map $\widetilde{\beta}_3$ on the complement of $\mathbb{L}_1 \cup \mathrm{Dom}(\mathbb{s}(\widetilde{\beta}_2))$ in $\mathbb{Y}_0$, and
4. put together the maps $\widetilde{\beta}_1, \mathbb{s}(\widetilde{\beta}_2)$, and $\widetilde{\beta}_3$ to get a bijection $\widetilde{\beta} : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$ which satisfies the conditions in Proposition 4.3.

5.3 Study of $\mathbb{L}_2$.

Recall that $\mathbb{L}_2$ defined in (5.1) is the subset where we cannot define $\widetilde{\beta}$ diagonally and where the weight of the points is strictly bigger than $\frac{3}{2}$."

In this section, we will complete the definition of $\widetilde{\beta}_2 : \mathbb{L}_2 \to m(\mathbb{Y}_0)$. We start with a proposition about the distribution of its domain $\mathbb{L}_2$ in $\mathbb{Y}_0$, which plays an important role in its construction.

Proposition 5.1. *The subset $\mathbb{L}_2$ is included in $\mathbb{K}_1$ (See Notation 5.1).*

Proof. The proof will occupy the entire Section 5.2 and it will follow from Propositions 5.3 and 5.4 below. □

Lemma 5.3. *Recall that $p_0 = p\%d$. Let P be any point in $\mathbb{Y}_0$. If $P + p_0(i,j)$ is contained in $\mathbb{Y}$ for a pair of integers (i,j), then it is also contained in $\mathbb{Y}_0$.*

Proof. Before proving the lemma, we refer to Figure4.2, where the bullet points in the upper-right triangle are periodic with period 3. Since the upper-right triangle in $\square_\Delta$ is convex, it is enough to show that the lemma holds for $(i,j) = (1,0), (-1,0), (0,1), (0,-1), (1,-1)$, and $(-1,1)$. We will just prove the case when $i = 1$ and $j = -1$, and the rest can be handled similarly.

Let Q be the point in $\mathbb{T}_1$ such that $(pQ)\% = P$. It is easy to check that

$$\begin{aligned} P + p_0(1,-1) &\equiv pQ + p_0(1,-1) \\ &\equiv pQ + p(1,-1) \\ &= p(Q + (1,-1)) \pmod{d}. \end{aligned}$$

In fact, the point $Q + (1,-1)$ is strictly contained in Δ_f, for otherwise $P + p_0(1,-1)$ is on

the boundary of $\square_{\Delta_f}$, which is a contradiction to $P + p_0(1,-1) \in \mathbb{Y}$. Then by the definition of $\mathbb{Y}_0$, we know that $P + p_0(1,-1)$ belongs to $\mathbb{Y}_0$. □

Notation 5.2. *We call the square with vertices* $(d-p_0, d-p_0)$, $(d-p_0, d-1)$, $(d-1, d-p_0)$ *and* $(d-1, d-1)$ the fundamental cell, *denoted by* $\mathscr{C}$, *and write*

$$\mathscr{C}_0 := \mathscr{C} \cap \mathbb{Y}_0.$$

Back to the example in Figure 4.2, the corresponding subset

$$\mathscr{C}_0 = \{(5,6), (6,5), (6,6)\}.$$

Corollary 5.1. *We know that* $\mathbb{Y}_0$ *distributes periodically in* $\mathbb{Y}$ *of period* p_0. *More precisely, each point in* $\mathbb{Y}_0$ *is a shift of some point in* $\mathscr{C}_0$ *by* (ip_0, jp_0), *where* (i,j) *is a pair of integers.*

Proof. It follows directly from Lemma 5.3. □

Corollary 5.2. *Let* k_1, k_2, j_1 *and* j_2 *be integers satisfying* $k_1, k_2 \geqslant d$ *and* $p_0|(k_2 - k_1)$. *If both* $\mathscr{W}_{k_1} \cap \mathscr{D}_{[j_1, j_1+2p_0)}$ *and* $\mathscr{W}_{k_2} \cap \mathscr{D}_{[j_2, j_2+2p_0)}$ *are contained in* $\square_\Delta$, *then*

1. $\#\Big(\mathbb{Y}_0 \cap \mathscr{W}_{k_1} \cap \mathscr{D}_{[j_1, j_1+2p_0)}\Big) = \#\Big(\mathbb{Y}_0 \cap \mathscr{W}_{k_2} \cap \mathscr{D}_{[j_2, j_2+2p_0)}\Big)$.
2. *If moreover we have* $p_0|(j_2 - j_1)$, *we have the following equality of sets*

$$\mathbb{Y}_0 \cap \mathscr{W}_{k_1} \cap \mathscr{D}_{[j_1, j_1+2p_0)} = \mathbb{Y}_0 \cap \mathscr{W}_{k_2} \cap \mathscr{D}_{[j_2, j_2+2p_0)} + (k_1 - k_2)(1,1) + (j_1 - j_2)(-1,1).$$

Proof. In fact, this corollary follows directly from previous corollary. □

Since $\mathbb{Y}_0$ is distributed periodically of period p_0, by Corollary 5.1, it is enough for us to understand $\mathscr{C}_0$. The following two lemmas show the details.

Lemma 5.4. *The distribution of $\mathscr{C}_0$ in $\mathscr{C}$ has the following properties:*

(1) There is no point of $\mathbb{Y}_0$ (or $\mathscr{C}_0$) on the top row or the first column of $\mathscr{C}$.

(2) If the point (i, j) is in $\mathscr{C}$ and $i + j = 2d - p_0$, then it is also in $\mathscr{C}_0$.

(3) For each point P in $\mathscr{C}$, either P or $(2d - p_0, 2d - p_0) - P$ is contained in $\mathscr{C}_0$.

Proof. The first two statements are straightforward. Therefore, we only prove Property (3).

Let (i_1, j_1) and (i_2, j_2) be two points in $\mathscr{C}$ symmetric about $y = 2d - p_0 - x$. Without loss of generality, we assume that the weight of (i_1, j_1) is less than the weight of (i_2, j_2). Then it is easy to check that they satisfy

- $2(d - p_0) \leqslant i_1 + j_1 < 2d - p_0$,
- $i_1 + j_2 = 2d - p_0$, and
- $i_2 + j_1 = 2d - p_0$.

Suppose that both (i_1, j_1) and (i_2, j_2) are in $\mathscr{C}_0$. Then there are two points (i'_1, j'_1) and (i'_2, j'_2) in $\mathbb{T}_1$ such that

$$(p(i'_1, j'_1))\% = (i_1, i_1) \quad \text{and} \quad (p(i'_2, j'_2))\% = (i_2, i_2).$$

It is easy to show that

$$p(i'_1 + j'_2) \equiv 2d - p_0 \pmod{d} \quad \text{and} \quad p(i'_2 + j'_1) \equiv 2d - p_0 \pmod{d}.$$

Since $(d, p) = 1$ and $p \equiv p_0 \pmod{d}$, we have

$$i'_1 + j'_2 \equiv -1 \pmod{d} \quad \text{and} \quad i'_2 + j'_1 \equiv -1 \pmod{d}.$$

Combining these two congruence equations with

$$d \cdot w(i_1', j_1') = i_1' + j_1' \leqslant d-1 \quad \text{and} \quad d \cdot w(i_2', j_2') = i_2' + j_2' \leqslant d-1,$$

we get that

$$d \cdot w(i_1', j_1') = d-1 \quad \text{and} \quad d \cdot w(i_2', j_2') = d-1.$$

It forces $p(i_1' + j_1') \equiv -p_0 \pmod{d}$, which is a contradiction to

$$2(d-p_0) \leqslant i_1 + j_1 < 2d - p_0.$$

By a similar argument, we check that at least one of (i_1, j_1) and (i_2, j_2) belongs to $\mathscr{C}_0$, which completes the proof. □

Notation 5.3. *(1) Let $d = d_1 p_0 + d_0$ and let $0 \leqslant d_2 < p_0$ be the integer such that $d_0 d_2 \equiv 1 \pmod{p_0}$.*

(2) For any two points P_1, P_2 in $\mathbb{Z}^2_{\geqslant 0}$, if they satisfy that $P_1 - P_2 = p_0 Q$ for some point Q in $\mathbb{Z}^2_{\geqslant 0}$, then we denote $P_1 \equiv P_2 \pmod{p_0}$.

Proposition 5.2. *For any $0 < k \leqslant p_0$, we have*

$$\#\big((\mathscr{W}_{2d-k} \cup \mathscr{W}_{2d-p_0-k}) \cap \mathscr{C}_0\big) = \begin{cases} p_0 - 1 & \text{if } k = p_0; \\ k d_2 \% p_0 - 1 & \text{otherwise.} \end{cases}$$

We need some preparations before giving the proof of this proposition after Lemma 5.7.

Lemma 5.5. *Let i, j be two positive integers. If $i + j \leqslant p_0$, then*

$$\big(p(id_1, jd_1)\big)\% \in \mathbb{Y}_0.$$

Proof. Since $p(id_1, jd_1) \equiv (d - id_0, d - jd_0) \pmod{d}$, it is enough to prove

$$1 < w\big((d - id_0, d - jd_0)\big) < 2,$$

which follows directly from $i + j \leqslant d$. □

Notation 5.4. *Put*

$$\mathbb{A} := \Big\{(id_1, jd_1) \;\Big|\; i, j > 0 \text{ and } i + j \leqslant p_0\Big\}.$$

By Lemmas 5.5 and 5.3, for any point $P \in \mathbb{A}$ there exists a point P' in $\mathscr{C}_0$ such that $P' \equiv (pP)\% \pmod{p_0}$. It automatically gives us a map from $\mathbb{A}$ to $\mathscr{C}_0$, denoted by γ. Now we will show that γ is a bijection.

Notation 5.5. *For simplicity of notation, we put* $P_{i,j} := (id_1, jd_1)$.

Lemma 5.6. *The map* γ *is a bijection.*

Proof. Any two points P_{i_1,j_1} and P_{i_2,j_2} in $\mathbb{A}$ satisfy

$$\begin{aligned}\gamma(P_{i_1,j_1}) - \gamma(P_{i_2,j_2}) \equiv& (pP_{i_1,j_1})\% - (pP_{i_2,j_2})\% \\ =& (d - i_1d_0, d - j_1d_0) - (d - i_2d_0, d - j_2d_0) \\ =& ((i_2 - i_1)d_0, (j_2 - j_1)d_0) \pmod{p_0}.\end{aligned}$$

Now if $\gamma(P_{i_1,j_1}) = \gamma(P_{i_2,j_2})$, we know that $((i_2 - i_1)d_0, (j_2 - j_1)d_0) \equiv O \pmod{p_0}$.

Since

$$(d_0, p_0) = 1, |i_2 - i_1| < p_0 \text{ and } |j_2 - j_1| < p_0,$$

we have $i_1 = i_2$ and $j_1 = j_2$, which implies γ is an injection. By Lemma 5.4, there are $\frac{p_0(p_0-1)}{2}$ points in $\mathscr{C}_0$, which is equal to the cardinality of $\mathbb{A}$. Therefore, γ is a bijection. □

Lemma 5.7. *Any two points P_{i_1,j_1} and P_{i_2,j_2} of the same weight satisfy*

$$\Big|d\cdot w\big(\gamma(P_{i_1,j_1})-\gamma(P_{i_2,j_2})\big)\Big| = 0 \text{ or } p_0.$$

Proof. We know easily that

$$\gamma(P_{i_1,j_1})\equiv(d-i_1d_0, d-j_1d_0) \quad \text{and} \quad \gamma(P_{i_2,j_2})\equiv(d-i_2d_0, d-j_2d_0) \pmod{p_0},$$

which implies that

$$d\cdot w\big(\gamma(P_{i_1,j_1})\big)-(d-i_1d_0+d-j_1d_0) \quad \text{and} \quad d\cdot w\big(\gamma(P_{i_2,j_2})\big)-(d-i_2d_0+d-j_2d_0)$$

are both divisible by p_0.

Since P_{i_1,j_1} and P_{i_2,j_2} have the same weight, we know $i_1+j_1=i_2+j_2$. Therefore, we have

$$p_0 \mid d\cdot w\big(\gamma(P_{i_1,j_1})-\gamma(P_{i_2,j_2})\big). \tag{5.2}$$

On the other hand, $\gamma(P_{i_1,j_1})$ and $\gamma(P_{i_2,j_2})$ both belong to $\mathscr{C}_0$, which together with (5.2) force $\big|d\cdot w\big(\gamma(P_{i_1,j_1})-\gamma(P_{i_2,j_2})\big)\big|$ to be 0 or p_0. □

Proof of Proposition 5.2. By Lemma 5.7, we know that

$$\begin{aligned}
\#\big((\mathscr{W}_{2d-k}\cup\mathscr{W}_{2d-p_0-k})\cap\mathscr{C}_0\big) &= \#\Big\{(i,j)\;\Big|\;(i+j)d_0\equiv k \pmod{p_0}, i,j>0 \text{ and } i+j<p_0\Big\}\\
&= \#\Big\{(i,j)\;\Big|\;(i+j)\equiv kd_2 \pmod{p_0}, i,j>0 \text{ and } i+j<p_0\Big\}\\
&= \begin{cases} p_0-1 & \text{if } k=p_0;\\ kd_2\%p_0-1 & \text{otherwise.}\end{cases}
\end{aligned}$$

□

The following proposition is the first stepstone of Theorem 5.1.

Proposition 5.3. *For every integer k with $|k| \geqslant p_0$, we have $\mathscr{D}_k \cap \mathbb{L}_2 = \varnothing$.*

The proof of the proposition will be given after some lemmas.

Lemma 5.8. *Let $\left(P_1, P_2, \ldots, P_{p_0}\right)$ be a sequence of consecutive points in $\mathscr{D}_k \cap \mathbb{Y}$ for some k.*

1. *There are exact $\lfloor \frac{p_0}{2} \rfloor$ points in this sequence belonging to $\mathbb{Y}_0$.*
2. *In particular, if ℓ is an integer with $\lceil \frac{p_0}{2} \rceil < \ell \leqslant p_0$, then at least $\ell - \lceil \frac{p_0}{2} \rceil$ points in the set $\{P_1, P_2, \ldots, P_\ell\}$ belong to $\mathbb{Y}_0$.*

Proof. (1) It follows directly from Lemma 5.4 (1)-(3).

(2) Combining (1) with Pigeonhole principle, we complete the proof of (2). □

Lemma 5.9. *There do not exist two points $P_0 \in \mathbb{L}_2$ and $Q_0 \in m(\mathbb{L}_3)$ such that $\overrightarrow{Q_0P_0}$ is a diagonal vector of weight less or equal to 1.*

Proof. Suppose the lemma were false. Then there exists an integer k such that

$$\left\{(P, Q) \in (\mathbb{L}_2 \cap \mathscr{D}_k) \times (m(\mathbb{L}_3) \cap \mathscr{D}_k) \;\middle|\; w(\overrightarrow{QP}) \leqslant 1\right\}$$

is not empty. We put (P_1, Q_1) to be a pair of points in this set which maximize the weight $w(\overrightarrow{Q_1P_1})$. By the inductive definition of $\widetilde{\beta}_1$, we can define $\widetilde{\beta}_1$ on P_1 by $\widetilde{\beta}_1(P_1) = Q_1$, which contradicts to the assumption that P_1 does not belong to $\mathbb{L}_1$. □

Lemma 5.10. *For any integer k, there do not exist two points $P \in (\mathbb{Y}_0 \backslash \mathbb{L}_1) \cap \mathscr{D}_k$ and $P' \in \mathbb{L}_1 \cap \mathscr{D}_k$ such that*

$$w(P' - \widetilde{\beta}_1(P')) < w(P - \widetilde{\beta}_1(P')) \leqslant 1. \tag{5.3}$$

Proof. Suppose that P and P' are two points which satisfy conditions in this lemma. We easily see that inequality (5.3) violates the requirement in construction of $\widetilde{\beta}_1$ that $(P', \widetilde{\beta}_1(P'))$ maximizes $w(P' - \widetilde{\beta}_1(P'))$, a contradiction. □

Lemma 5.11. *For an arbitrary point P in $\mathscr{D}_k \cap \mathbb{Y}_0 \cap \mathscr{W}_{(\frac{3d}{2}, 2d]}$, if it satisfies*

$$\#\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P-Q) \leqslant 1\Big\} \geqslant \#\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) > w(P)\Big\} + 1, \qquad (5.4)$$

then it belongs to $\mathbb{L}_1$.

Proof. Let P be a point which satisfies conditions in this lemma. Suppose that P does not belong to $\mathbb{L}_1$. Then by Lemma 5.9, each element in

$$\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P-Q) \leqslant 1\Big\}$$

is equal to $\widetilde{\beta}_1(P')$ for some $P' \in \mathbb{L}_1 \backslash \{P\}$. From equality (5.4), we know that at least one of these P' does not belong to

$$\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) \geqslant w(P)\Big\}.$$

Then we obtain a contradiction directly from Lemma 5.10. □

Corollary 5.3. *For an arbitrary point P in $\mathscr{D}_k \cap \mathbb{Y}_0 \cap \mathscr{W}_{(\frac{3d}{2}, 2d]}$, if it satisfies*

$$\#\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P-Q) \leqslant 1\Big\} \geqslant \#\Big\{Q \in \mathscr{D}_k \cap \mathbb{Y}_0 \;\Big|\; w(Q) \geqslant w(P)\Big\}, \qquad (5.5)$$

then it belongs to $\mathbb{L}_1$.

Proof. Let P be a point satisfying condition in this lemma. Suppose that P does not belong

to $\mathbb{L}_1$. Then we have

$$\#\Big\{Q \in \mathscr{D}_k \cap \mathbb{Y}_0 \;\Big|\; w(Q) \geqslant w(P)\Big\} \geqslant \#\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) > w(P)\Big\} + 1.$$

Combining it with Lemma 5.11, we get $P \in \mathbb{L}_1$, a contradiction. □

Therefore, in order to show that each point P in $\mathscr{D}_k \cap \mathbb{Y}_0 \cap \mathscr{W}_{(\frac{3d}{2},2d]}$ for $|k| \geqslant p_0$ belongs to $\mathbb{L}_1$, it is enough to prove that P satisfies inequality (5.5). The following functions give a lower bound for cardinality of the first set in (5.5) and an upper bound for the second one.

Definition 5.7. *We define*

$$g_1(2p_0 i + j) := \begin{cases} i\lfloor \frac{p_0}{2} \rfloor & \text{if } 0 \leqslant j \leqslant p_0 \\ i\lfloor \frac{p_0}{2} \rfloor + \lfloor \frac{j}{2} \rfloor - \lceil \frac{p_0}{2} \rceil & \text{if } p_0 < j < 2p_0. \end{cases}$$

Lemma 5.12. *For any integers B_1, B_2 and k with $0 < B_1 < B_2 < d$ and $|k| \leqslant B_1$, by Lemma 5.8, we have*

$$\#\Big(\big\{Q \in \mathscr{D}_k \;\big|\; B_1 \leqslant d \cdot w(Q) \leqslant B_2\big\} \cap m(\mathbb{Y}_0)\Big) \geqslant g_1(B_2 - B_1).$$

Definition 5.8. *Define*

$$g_2(2p_0 i + j) := \begin{cases} i\lfloor \frac{p_0}{2} \rfloor + \lfloor \frac{j}{2} \rfloor & \text{if } 0 \leqslant j \leqslant p_0 \\ (i+1)\lfloor \frac{p_0}{2} \rfloor & \text{if } p_0 < j < 2p_0. \end{cases}$$

Lemma 5.13. *For any integers B_1, B_2 and k with $d < B_1 < B_2 < 2d$, by Lemma 5.8, we have*

$$\#\Big(\big\{Q \in \mathscr{D}_k \;\big|\; B_1 \leqslant d \cdot w(Q) \leqslant B_2\big\} \cap \mathbb{Y}_0\Big) \leqslant g_2(B_2 - B_1).$$

Lemma 5.14. *Both g_2 and g_1 are non-decreasing and $g_1(k + p_0) \geqslant g_2(k)$ for every $k > 0$.*

Proof. It follows from their definitions. □

Proof of Proposition 5.3. Consider a point P_0 in $\mathscr{D}_k \cap \mathbb{Y}_0 \cap \mathscr{W}_{(\frac{3d}{2},2d]}$. We have that

$$\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\} = \Big\{Q \in \mathscr{D}_k \;\Big|\; d \cdot w(P_0) - d \leqslant d \cdot w(Q) \leqslant d\Big\} \cap m(\mathbb{Y}_0).$$

By Lemma 5.12, we know that

$$\#\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\} \geqslant g_1(2d - w(P_0)d). \tag{5.6}$$

On the other hand, since

$$\Big\{Q \in \mathscr{D}_k \cap \mathbb{Y}_0 \;\Big|\; w(Q) \geqslant w(P_0)\Big\} = \Big\{Q \in \mathscr{D}_k \;\Big|\; d \cdot w(P_0) \leqslant d \cdot w(Q) \leqslant 2d - |k|\Big\} \cap \mathbb{Y}_0,$$

by Lemma 5.13, we know that

$$\#\Big\{Q \in \mathscr{D}_k \cap \mathbb{Y}_0 \;\Big|\; w(Q) \geqslant w(P_0)\Big\} \leqslant g_2\big(2d - |k| - d \cdot w(P_0)\big). \tag{5.7}$$

By Lemma 5.14 and $|k| \geqslant p_0$, the terms on the right side of these inequalities above satisfy

$$\begin{aligned} g_2\big(2d - |k| - w(P_0)d\big) \leqslant & g_2\big(2d - p_0 - w(P_0)d\big) \\ \leqslant & g_1\big(2d - w(P_0)d\big). \end{aligned}$$

Hence, we have

$$\#\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\} \geqslant \#\Big\{Q \in \mathscr{D}_k \cap \mathbb{Y}_0 \;\Big|\; w(Q) \geqslant w(P_0)\Big\}. \tag{5.8}$$

Combining it with Corollary 5.3, we prove this proposition. □

Proposition 5.4. *The intersection $\mathscr{W}_{[d,2d-3p_0]} \cap \mathbb{L}_2$ is empty.*

Proof. By Lemma 5.11, it is enough to prove that each point P_0 in $\mathscr{W}_{(\frac{3}{2}d,2d-3p_0]}$, say $P_0 \in \mathscr{D}_k$, satisfies

$$\#\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) > w(P_0)\Big\} + 1 \leqslant \#\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\}. \quad (5.9)$$

Now we estimate the size of the two sets in (5.9) as follows.

By Proposition 5.3 and the assumption of P_0, we are reduced to proving (5.9) for P_0 in $\mathscr{D}_{(-p_0,p_0)} \cap \mathscr{W}_{(\frac{3}{2}d,2d-3p_0]}$, which guarantees us a point P_0' in $\mathscr{C}_0$ such that

$$P_0' = P_0 + (ip_0, ip_0) \quad (5.10)$$

for some integer $i \geqslant 1$. Assume that P_0' belongs to $\mathscr{W}_j$. Put

$$\mathbb{B}(P_0) := \Big\{P \in \mathscr{C}_0 \cap \mathbb{L}_1 \cap \mathscr{D}_k \;\Big|\; w(P) \geqslant w(P_0')\Big\}.$$

Then we give the following estimations.

1. Estimation of $\#\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\}$.

By definition of $\mathbb{B}(P_0)$, we know that $\widetilde{\beta}_1(\mathbb{B}(P_0))$ is contained in

$$\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\} \cap \mathscr{W}_{[j-d,d)}.$$

On the other hand, by (5.10), we know easily that

$$\mathscr{D}_k \cap m(\mathbb{Y}_0) \cap \mathscr{W}_{[j-d-2ip_0,j-d)} \subset \Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\}.$$

Therefore, $\widetilde{\beta}_1(\mathbb{B}(P_0))$ and $\mathscr{D}_k \cap m(\mathbb{Y}_0) \cap \mathscr{W}_{[j-d-2ip_0,j-d)}$ are two disjoint subsets of $\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\}$. By Lemma 5.8, we know that

$$\#\Big(\mathscr{D}_k \cap m(\mathbb{Y}_0) \cap \mathscr{W}_{[j-d-2ip_0,j-d)}\Big) = i\lfloor\frac{p_0}{2}\rfloor,$$

which implies

$$\#\Big\{Q \in \mathscr{D}_k \cap m(\mathbb{Y}_0) \;\Big|\; w(P_0 - Q) \leqslant 1\Big\} \leqslant \#\mathbb{B}(P_0) + i\lfloor\frac{p_0}{2}\rfloor.$$

2. Estimation of $\#\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) > w(P)\Big\}$.

Consider the disjoint decomposition

$$\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) > w(P)\Big\} = \Big(\mathscr{D}_k \cap \mathbb{L}_1 \cap \mathscr{W}_{(j-2ip_0,j]}\Big) \cup \Big(\mathbb{B}(P_0)\backslash P_0'\Big). \tag{5.11}$$

We need consider the following two cases:

Case 1: When P_0' belongs to $\mathbb{L}_1$, we have $\#\Big(\mathbb{B}(P_0)\backslash P_0'\Big) = \#\mathbb{B}(P_0) - 1$, which implies

$$\begin{aligned}
&\#\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) > w(P)\Big\}\\
\leqslant&\#\Big(\mathscr{D}_k \cap \mathscr{W}_{(j-2ip_0,j]}\Big) + \#\Big(\mathbb{B}(P_0)\backslash P_0'\Big)\\
=&i\lfloor\frac{p_0}{2}\rfloor + \#\mathbb{B}(P_0) - 1.
\end{aligned}$$

Case 2: When P_0' does not belong to $\mathbb{L}_1$, we have

$$\#\Big(\mathscr{D}_k \cap \mathbb{L}_1 \cap \mathscr{W}_{(j-2ip_0,j]}\Big) \leqslant \#\Big(\mathscr{D}_k \cap \mathscr{W}_{(j-2ip_0,j]}\Big) - 1,$$

which implies

$$\begin{aligned}
&\#\Big\{Q \in \mathscr{D}_k \cap \mathbb{L}_1 \;\Big|\; w(Q) > w(P)\Big\} \\
\leqslant &\#\Big(\mathscr{D}_k \cap \mathscr{W}_{(j-2ip_0,j]}\Big) - 1 + \#\Big(\mathbb{B}(P_0)\backslash P_0'\Big) \\
= &i\lfloor\frac{p_0}{2}\rfloor + \#\mathbb{B}(P_0) - 1.
\end{aligned}$$

In either case, it is easy to check (5.9), which completes this proposition. □

5.4 Definition of $\widetilde{\beta}$.

We next construct a map $\overline{\beta}_2 : \mathbb{L}_2 \to m(\mathbb{L}_3)$. Put $\widetilde{J} = \{d-3p_0, d-3p_0+1, \ldots, d-1\}$. Write

$$\mathbb{K}_2 := \left\{P \;\middle|\; P \in \mathscr{W}_{\widetilde{J}} \cap \mathscr{D}_{\left[\lceil\frac{d}{2}\rceil,\lceil\frac{d}{2}\rceil+2p_0\right)}\right\} \quad \text{and} \quad \mathbb{K}_2^0 := \mathbb{K}_2 \cap m(\mathbb{Y}_0). \tag{5.12}$$

The general idea of constructing $\overline{\beta}_2$ is to map $\mathbb{L}_2$ to disjoint sets $(\mathbb{K}_2 + (i_k p_0, -i_k p_0)) \cap m(\mathbb{Y}_0)$, where $(i_1, \ldots, i_{\#\mathbb{L}_2})$ is a certain sequence of numbers in some range, such that for any two points P_1 and P_2 in $\mathbb{L}_2$ if $\overline{\beta}_2(P_1)$ and $\overline{\beta}_2(P_2)$ belong to $(\mathbb{K}_2 + (i_k p_0, -i_k p_0)) \cap m(\mathbb{Y}_0)$ for a same k, then $P_1 - \overline{\beta}_2(P_1) = P_2 - \overline{\beta}_2(P_2)$.

Remark 5.1. *An easy computation shows that $\mathscr{W}_{d-1} \cap m(\mathbb{Y}_0)$ is not empty, say that Q is a point in it. The most naive construction of $\overline{\beta}_2$ is to make an injection from $\mathbb{L}_2$ to $\{Q + (2ip_0, -2ip_0)\}_{i=1}^{\#\mathbb{L}_2}$. However, the construction requires a very stronge condition that $d = O(p_0^3)$. In order to weaken this condition, we need a more detailized construction (see Construction 5.1).*

We start the construction of $\overline{\beta}_2$ with giving more details of its codomain. Recall that we defined the numbers d_0, d_1 and d_2 in Notation 5.3.

Lemma 5.15. *We have*

$$\#(\mathbb{K}_2^0 \cap \mathscr{W}_{d-i}) = \begin{cases} p_0 - 1 & \text{if } i \equiv d_0 \pmod{p_0}; \\ \big(i(p_0 - d_2)\big)\%p_0 & \text{otherwise} \end{cases}$$

for all $1 \leqslant i \leqslant p_0 - 1$.

Proof. Since $\mathbb{Y}_0$ and $m(\mathbb{Y}_0)$ are symmetric about $y = d - x$, we have

$$\#\Big(\mathbb{K}_2^0 \cap \mathscr{W}_{d-i}\Big) = \#\Big(\mathscr{W}_{d+i} \cap \mathbb{Y}_0 \cap \mathscr{D}_{\left[\lceil \frac{d}{2} \rceil, \lceil \frac{d}{2} \rceil + 2p_0\right)}\Big).$$

Find $p_0 < j \leqslant 2p_0$ such that $2d - j \equiv d + i \pmod{p_0}$. By Corollary 5.2, we have

$$\#\Big(\mathscr{W}_{d+i} \cap \mathbb{Y}_0 \cap \mathscr{D}_{\left[\lceil \frac{d}{2} \rceil, \lceil \frac{d}{2} \rceil + 2p_0\right)}\Big) = \#\Big(\mathscr{W}_{2d-j} \cap \mathscr{D}_{[-p_0, p_0)} \cap \mathbb{Y}_0\Big).$$

From Corollary 5.1, we know

$$\#\Big(\mathscr{W}_{2d-j} \cap \mathscr{W}_{[-p_0, p_0)}\Big) = \#\Big((\mathscr{W}_{2d-j} \cup \mathscr{W}_{2d-p_0-j}) \cap \mathscr{C}_0\Big).$$

Therefore, by Proposition 5.2, if $j = p_0$, then we have

$$\#((\mathscr{W}_{2d-j} \cup \mathscr{W}_{2d-p_0-j}) \cap \mathscr{C}_0) = p_0 - 1.$$

It is not hard to see from the relation between i and j that $i \equiv d_0 \pmod{p_0}$. Combining all these equlities above, we get $\#(\mathbb{K}_2^0 \cap \mathscr{W}_{d-i}) = p_0 - 1$.

For the case that $j \neq p_0$, we have

$$\begin{aligned}
&\#((\mathscr{W}_{2d-j} \cup \mathscr{W}_{2d-p_0-j}) \cap \mathscr{C}_0) \\
=&jd_2\%p_0 - 1 \\
=&(d_0 - i)d_2\%p_0 - 1 \\
=&i(p_0 - d_2)\%p_0.
\end{aligned}$$

By a similar argument, we complete the proof immediately. □

In order to support our construction of $\overline{\beta}_2$, we need several technical lemmas.

Notation 5.6. *For any subset $\mathbb{K}_2'$ of $\mathbb{K}_2$ and any integer $k \in [0, p_0 - 1]$, we put*

$$\mathbb{K}_2'(k) := \begin{cases} P + (-k, k) & \text{if } P + (-k, k) \in \mathbb{K}_2; \\ P + (p_0 - k, -(p_0 - k)) & \text{otherwise.} \end{cases}$$

Lemma 5.16. *Let J be a subset of $\widetilde{J}$. Suppose that there are at least $\mathtt{n}$ points in $\mathscr{W}_j \cap \mathbb{K}_2'$ for each $j \in J$. Then*

(1) *for every subset $\mathbb{S}$ of $\mathscr{W}_J \cap \mathbb{K}_2$ of cardinality $\mathtt{m}$, there exists at least an integer i in $[0, p_0 - 1]$ such that*

$$\#\Big(\mathbb{S} \cap \mathbb{K}_2'(i)\Big) \geqslant \lceil \frac{\mathtt{mn}}{p_0} \rceil.$$

(2) *For the set of lattice points $\mathscr{W}_J \cap \mathbb{K}_2$, there exists a subset I of $\{1, 2, \ldots, p_0\}$ of cardinality less than or equal to $\big\lceil -\log_{(1-\frac{\mathtt{n}}{p_0})}\big(p_0(\#J)\big)\big\rceil$ such that*

$$\bigcup_{i \in I} \mathbb{K}_2'(i) \cap \mathscr{W}_J = \mathscr{W}_J \cap \mathbb{K}_2. \tag{5.13}$$

Proof. (1). Since $\biguplus_{i=0}^{p_0-1} (\mathscr{W}_J \cap \mathbb{K}_2'(i))^\star$ covers $\mathbb{S}$ at least $\mathtt{n}$ times, by Pigeonhole principle, there

exists some i such that $\mathbb{S} \cap \mathbb{K}_2'(i) \geqslant \lceil \frac{\mathbb{m}\mathbb{n}}{p_0} \rceil$.

(2). By (1), we can choose a sequence $(i_1, i_2, \dots)$ from $\{1, 2, \dots, 3p_0\}$ such that

$$\mathbb{m}_k \leqslant \mathbb{m}_{k-1} - \lceil \frac{\mathbb{n}\mathbb{m}_{k-1}}{p_0} \rceil \leqslant \mathbb{m}_{k-1}(1 - \frac{\mathbb{n}}{p_0}), \tag{5.14}$$

where $\mathbb{m}_k := \#(\mathscr{W}_J \cap \mathbb{K}_2 - \bigcup_{j=1}^{k} \mathbb{K}_2'(i_j) \cap \mathscr{W}_J)$.

Write $t = \Big\lfloor -\log_{\left(1-\frac{\mathbb{n}}{p_0}\right)}(p_0(\#J)) \Big\rfloor + 1$. Repeated application of (5.14) gives

$$\mathbb{m}_t \leqslant \mathbb{m}_0(1 - \frac{\mathbb{n}}{p_0})^t = p_0(\#J)(1 - \frac{\mathbb{n}}{p_0})^t < 1.$$

It implies $\mathbb{m}_t = 0$. Therefore, the length of this sequence cannot be longer than $t - 1$, which completes the proof of (2). □

Let u be a real number in $(0, 1)$. Depending on u, we decompose $\widetilde{J}$ into three groups:

1. $J_1(u) = \Big\{ j \in \widetilde{J} \;\Big|\; j > d - \frac{p_0^u}{p_0 - d_2} \Big\}$,
2. $J_2(u) = \Big\{ j \in \widetilde{J} \;\Big|\; \#(\mathscr{W}_j \cap \mathbb{K}_2^0) \geqslant p_0^u \Big\}$, and
3. $J_3(u) := \widetilde{J} \backslash \Big(J_2(u) \cup J_1(u) \Big)$.

By Lemma 5.15, we know that

$$3p_0 - 3p_0^u \leqslant \#J_2(u) \leqslant 3p_0. \tag{5.15}$$

Notation 5.7. *Set* $h = \log_{p_0}(p_0 - d_2)$.

Construction 5.1 (Construction of $\overline{\beta}_2$)**.** *We construct* $\overline{\beta}_2$ *in three steps:*

Step 1. *Lemma 5.15 shows that $\mathbb{K}_2^0 \cap \mathscr{W}_{d-1}$ is not empty, say that it contains a point Q_1. We put*

$$\mathscr{W}_{J_1+d} \cap \mathbb{L}_2 := \{P_1, P_2, \dots, P_{t_1}\},$$

where t_1 is its cardinality, and define $\overline{\beta}_2$ on $\mathscr{W}_{J_1+d} \cap \mathbb{L}_2$ as

$$\begin{aligned}\overline{\beta}_2 :&\mathscr{W}_{J_1+d} \cap \mathbb{L}_2 \to m(\mathbb{L}_3)\\ &P_i \mapsto Q_1 + \big(p_0(i-1), -p_0(i-1)\big).\end{aligned}$$

Namely, $\overline{\beta}_2$ maps $\mathscr{W}_{J_1+d} \cap \mathbb{L}_2$ into a disjoint union of $\mathbb{K}_2 + (p_0 i, -p_0 i)$ for $0 \leqslant i \leqslant t_1 - 1$.

By the definition of J_1, we know that $\#J_1 = \lfloor \frac{p_0^u}{p_0 - d_2} \rfloor$. Since $\mathscr{W}_{J_1+d} \cap \mathbb{L}_2$ is in an isosceles right triangle with side lengths $\#J_1$, we have $t_1 \leqslant \frac{1}{2}(\lfloor \frac{p_0^u}{p_0-d_2} \rfloor + 1)\lfloor \frac{p_0^u}{p_0-d_2} \rfloor$. It is easily check that $t_1 \leqslant \frac{1}{2}({p_0}^{2(u-h)} + {p_0}^{u-h})$.

Step 2. *We denote by θ the unique map from $\mathbb{K}_1$ to $\mathbb{K}_2$ given by parallel transform. By Lemma 5.16 (2), there is a sequence $(i_1, i_2, \dots, i_{t_2})$ such that*

$$\bigcup_{k=1}^{t_2} \mathbb{K}_2^0(i_k) \cap \mathscr{W}_{J_2} = \mathbb{K}_2 \cap \mathscr{W}_{J_2} \quad \textit{and} \quad t_2 \leqslant \Big\lfloor -\log_{(1-\frac{p_0^u}{p_0})} \big(p_0(\#J_2)\big) \Big\rfloor.$$

Since $\bigcup_{k=1}^{t_2} \mathbb{K}_2^0(i_k)$ depends only on the elements in set $\{i_1, i_2, \dots, i_{t_2}\}$, we can in fact require $(i_1, i_2, \dots, i_{t_2})$ to be increasing.

It is easily seen that

$$t_2 \leqslant \Big\lfloor -\log_{(1-\frac{p_0^u}{p_0})} \big(p_0(\#J_2)\big) \Big\rfloor \leqslant \Big\lfloor -\log_{(1-\frac{p_0^u}{p_0})} (3p_0^2) \Big\rfloor.$$

For each point P in $\mathscr{W}_{J_2+d} \cap \mathbb{L}_2$, we put $k(P)$ to be the smallest number such that $\mathbb{K}_2^0(i_{k(P)}) \cap$

$\mathscr{W}_{J_2}$ contains $\theta(P)$. Then we define

$$\overline{\beta}_2(P) := \theta(P) + (x_2(P), -x_2(P)),$$

where $x_2(P) = t_1 p_0 + i_{k(P)} + k(P)p_0.x$ Namely, $\overline{\beta}_2$ maps $\mathscr{W}_{J_2+d} \cap \mathbb{L}_2$ into a disjoint union of

$$\mathbb{K}_2 + \big[t_1 p_0 + i_k + k p_0\big](1, -1) \quad \textit{for } 1 \leqslant k \leqslant t_2.$$

Step 3. *Write $J_3(u) = \{j_1, j_2, \ldots, j_{s_3}\}$. By (5.15), we know that $s_3 \leqslant 3p_0^u$. Let d_3 be the largest number in $\widetilde{J}$ such that $\#(\mathscr{W}_j \cap \mathbb{K}_2^0) \geqslant \frac{p_0}{2}$. By Lemma 5.15, we have*

$$J_3 \in (d - 3p_0, d_3] \quad \textit{and} \quad \frac{p_0}{2} \leqslant (d - d_3)(p_0 - d_2) < p_0.$$

Replacing J in Lemma 5.16 by $\{d_3\}$, we obtain a sequence $(i'_1, i'_2, \ldots, i'_{t_3})$ from $\{1, 2, \ldots, p_0\}$ such that

$$\bigcup_{k=1}^{t_3} \mathbb{K}_2^0(i_k) \cap \mathscr{W}_{d_3} = \mathbb{K}_2 \cap \mathscr{W}_{d_3} \quad \textit{and} \quad t_3 \leqslant \big\lfloor -\log_{(1-\frac{p_0/2}{p_0})}(p_0) \big\rfloor = \big\lfloor \log_2(p_0) \big\rfloor.$$

*Similar to **Step 2**, we assume that $(i'_1, i'_2, \ldots, i'_{t_3})$ is increasing. Then we define $\overline{\beta}_2$ on $\mathscr{W}_{J_3+d} \cap \mathbb{L}_2$ as follows:*

Consider each $P \in \mathscr{W}_{J_3+d} \cap \mathbb{L}_2$. Suppose that P belongs to $\mathscr{W}_{j_l+d}$ for some $j_l \in J_3$. Let $k(P)$ be the smallest number such that $\mathbb{K}_2^0(i'_{k(P)}) \cap \mathscr{W}_{d_3}$ contains $\theta(P) + (d_3 - j_l, d_3 - j_l)$. Then we define

$$\overline{\beta}_2(P) := \theta(P) + (d_3 - j_l + x_3(P), d_3 - j_l - x_3(P)),$$

where $x_3(P) = p_0[k(P) + (l-1)(t_3+2) + t_1 + t_2 + 2] + i'_{k(P)}$.

Namely, $\overline{\beta}_2$ maps $\mathscr{W}_{J_2+d} \cap \mathbb{L}_2$ into a disjoint union of

$$\mathbb{K}_2 + \big\{p_0[k + (l-1)(t_3+2) + t_1 + t_2 + 2] + i'_k\big\}(1,-1)$$

for $1 \leqslant k \leqslant t_3$ and $1 \leqslant l \leqslant s_3$.

Notice that the codomain of $\overline{\beta}_2$ is both a disjoint union of shifts of $\mathbb{K}_2$ and a subset of $\square_\Delta$. Then for a fixed d, the residue p_0 of p modulo d cannot be too large. The following computation gives p_0 an upper bound such that the construction for $\overline{\beta}_2$ above is realizable. In fact, the complicated conditions in Theorem 4.1 are also from this computation.

From the constructing above, we know that the image of $\overline{\beta}_2$ is included in a union of disjoint shifts of $\mathbb{K}_2$. Moreover, the number of these shifts, denoted by $\mathcal{N}$, is counted and estimated as follows:

$$\begin{aligned}
\mathcal{N} =& t_1 + t_2 + t_3 \times s_3 \\
\leqslant& \frac{1}{2}({p_0}^{2(u-h)} + {p_0}^{u-h}) + \Big\lfloor -\log_{(1-\frac{p_0^u}{p_0})}(3p_0^2)\Big\rceil + \Big\rfloor \log_2(p_0)\Big\rceil \times 3p_0^u \\
\leqslant& \frac{3}{4}{p_0}^{2(u-h)} + \frac{1}{4} + 2\ln(p_0)p_0^{1-u} + \ln 3p_0^{1-u} + \log_2(p_0) \times 3p_0^u.
\end{aligned} \tag{5.16}$$

Recall $\mathbb{K}_2 = \Big\{P \;\Big|\; P \in \mathscr{W}_{\tilde{J}} \cap \mathscr{D}_{\left[\lfloor \frac{d}{2} \rfloor, \lfloor \frac{d}{2} \rfloor + 2p_0\right)}\Big\}$. It is easy to see that the largest x-coordinate of points in the codomain of $\overline{\beta}_2$ is equal to $\frac{3}{4}d + p_0(\mathcal{N} + 2s_3 + 3)$, which obvious is controled by d. Then we get a necessary condition:

$$d \geqslant 4p_0(\mathcal{N} + 2s_3 + 3). \tag{5.17}$$

We write $G(h,u) = \max\{2(u-h), 1-u, u\}$. Recall that $h = \log_{p_0}(p_0 - d_2)$ is fixed by p_0 and d. Therefore, our next goal is to determine the minimum of $G(h,u)$ by varying the value of u inside $[0,1]$.

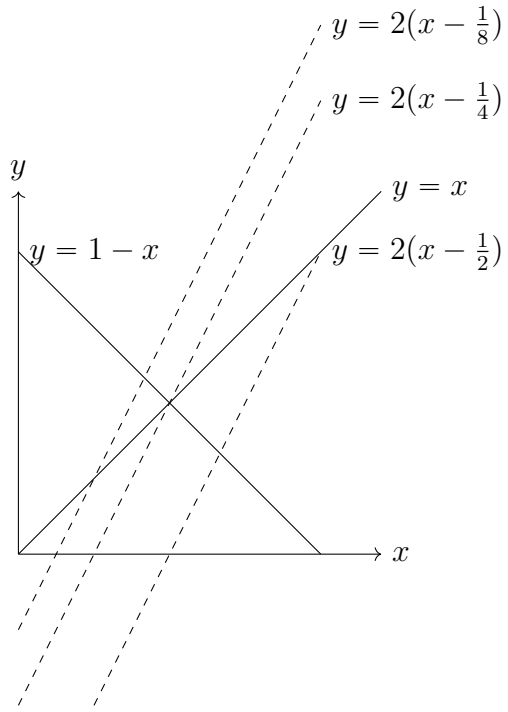

Figure 5.2: Determine the optimizer of h.

Definition 5.9. *We call u' an* optimizer *of h if $G(h, u') = \min_{u \in [0,1]} \big(G(h, u)\big)$.*

In order to get an optimizer of a given $h \in (0, 1]$. We need to consider two cases:.

Case 1. When $\frac{1}{4} \leqslant h \leqslant 1$. From Figure 5.2, the optimizer u of h is the x-coordinate of the point of intersection of lines $y = x$ and $y = 1 - x$. Therefore, we know that $u = \frac{1}{2}$ is the optimizer of this h. Plugging $u = \frac{1}{2}$ into equations (5.16) and (5.17), we have

$$4p_0(\mathcal{N} + 2s_3 + 3) \leqslant 4p_0^{\frac{3}{2}}\Big[\ln 3 + \frac{27}{4} + (2 + \frac{3}{\ln 2})\ln p_0\Big] + 13p_0.$$

Case 2. When $0 < h < \frac{1}{4}$. Based on the same observation of Figure 5.2, an optimizer u of h is the x-coordinate of the point of intersection of lines $y = 2(x - h)$ and $y = 1 - x$. An easy computation shows that $u = \frac{1+2h}{3}$. Combining it with (5.16) and (5.17), we have

$$4p_0(\mathcal{N} + 2s_3 + 3) \leqslant 4p_0^{\frac{5-2h}{3}}\Big[\ln 3 + \frac{27}{4} + (2 + \frac{3}{\ln 2})\ln p_0\Big] + 13p_0.$$

Notation 5.8. *(1) We write*

$$V(\overline{\beta}_2) := \Big\{ P - \overline{\beta}_2(P) \;\Big|\; P \in \mathbb{L}_2 \Big\}. \tag{5.18}$$

(2) The reflection of a vector $\vec{v}$ through a diagonal line $y = x$ is denoted by $\vec{v}^{\vee}$. Let V be a set of vectors. We put $V^{\vee} := \{\vec{v}^{\vee} \mid \vec{v} \in V\}$.

Lemma 5.17. *We know that*

$$\mathrm{Im}(\widetilde{\beta}_1) \cap \Big\{ P - \vec{v} \;\Big|\; P \in \mathbb{L}_2 \text{ and } \vec{v} \in V(\overline{\beta}_2) \cup V(\overline{\beta}_2)^{\vee} \Big\}$$

is empty.

Proof. It is easy to check that any point Q in

$$\Big\{ P - \vec{v} \;\Big|\; P \in \mathbb{L}_2 \text{ and } \vec{v} \in V(\overline{\beta}_2) \cup V(\overline{\beta}_2)^{\vee} \Big\}$$

belongs to $\mathscr{D}_k$ for some $|k| > \frac{d}{2}$. Then this lemma follows simply from the definition of $\widetilde{\beta}_1$. □

Construction 5.2 (Construction of $\widetilde{\beta}_2$)**.** ***Step 1****. Write*

$$\mathscr{E}_2 := \big\{ \beta : \mathbb{L}_2 \hookrightarrow m(\mathbb{Y}_0) \;\big|\; P - \beta(P) \in V(\overline{\beta}_2) \cup V(\overline{\beta}_2)^{\vee} \text{ for all } P \in \mathbb{L}_2 \big\}.$$

We know that $\mathscr{E}_2$ is non-empty, for $\overline{\beta}_2$ is automatically contained in it.

Step 2*. We line up the elements in $V(\overline{\beta}_2)$ to form a sequence, denoted by $(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{\mathcal{N}})$.*

Step 3*. Define a partial order over $\mathscr{E}_2$ as follows:*

For any two maps $\beta_1, \beta_2 \in \mathscr{E}_2$, we denote $\beta_1 \prec_2 \beta_2$, if there exists an integer $1 \leqslant k \leqslant \mathcal{N}$ such

that

- $\#\{P \mid P - \beta_1(P) = \vec{v}_i \text{ or } \vec{v}_i^\vee\} = \#\{P \mid P - \beta_2(P) = \vec{v}_i \text{ or } \vec{v}_i^\vee\}$ *for all* $1 \leqslant i \leqslant k-1$, *and*

- $\#\{P \mid P - \beta_1(P) = v_k \text{ or } v_k^\vee\} < \#\{P \mid P - \beta_2(P) = v_k \text{ or } v_k^\vee\}$.

Step 4. *Let* $\widetilde{\beta}_2$ *be a maximal element in* $\mathscr{E}_2$.

By Hypothesis 5.1, we know that $m(\mathbb{L}_2) \cap \widetilde{\beta}_2(\mathbb{L}_2) = \varnothing$. Combining it with Lemma 5.1, we can simply prove the existence of $\mathbb{s}(\widetilde{\beta}_2)$. Since maps $\widetilde{\beta}_1$ and $\mathbb{s}(\widetilde{\beta}_2)$ are symmetric, we define

$$\begin{aligned}\widetilde{\beta}_3 : \mathbb{Y}_0 \Big\backslash \Big(\mathrm{Dom}(\widetilde{\beta}_1) \cup \mathrm{Dom}(\mathbb{s}(\widetilde{\beta}_2))\Big) &\to m(\mathbb{Y}_0) \Big\backslash \Big(\mathrm{Im}(\widetilde{\beta}_1) \cup \mathrm{Im}(\mathbb{s}(\widetilde{\beta}_2))\Big) \\ P &\mapsto m(P).\end{aligned}$$

Putting $\widetilde{\beta}_1, \mathbb{s}(\widetilde{\beta}_2)$ and $\widetilde{\beta}_3$ together, we define a bijection $\widetilde{\beta} : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$ such that

$$\widetilde{\beta}(P) = \begin{cases} \widetilde{\beta}_1(P) & \text{if } P \in \mathbb{L}_1; \\ \mathbb{s}(\widetilde{\beta}_2)(P) & \text{if } P \in \mathrm{Dom}(\mathbb{s}(\widetilde{\beta}_2)); \\ \widetilde{\beta}_3(P) & \text{otherwise.} \end{cases} \tag{5.19}$$

Since $\mathbb{Y}_0 \Big\backslash \Big(\mathrm{Dom}(\widetilde{\beta}_1) \cup \mathrm{Dom}(\mathbb{s}(\widetilde{\beta}_2))\Big) \subset \mathbb{L}_3$, we know that $w(P - m(P)) \leqslant 1$ for each point $P \in \mathbb{L}_3$. Combining it with the constructive definition of $\widetilde{\beta}_1$ and $\mathbb{s}(\widetilde{\beta}_2)$, we easily check that $\widetilde{\beta}$ is a special bijection (see Definition 4.7).

5.5 Completion of the proofs.

Notation 5.9. *For a bijection $\beta : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$, we write*

$$\mathbb{L}_\beta := \mathbb{L}_2 \cup \beta^{-1}(m(\mathbb{L}_2)).$$

Recall that we defined the meaning of two bijections $\beta, \beta' : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$ to be related in Definition 4.8.

Proposition 5.5. *(a) A bijection $\beta' : \mathbb{Y}_0 \to m(\mathbb{Y}_0)$ is related to $\widetilde{\beta}$ if and only if*

(1) *$P - \beta'(P) = P - \widetilde{\beta}(P)$ or $(P - \widetilde{\beta}(P))^\vee$ for all P in $\mathbb{L}_2$;*

(2) *$\beta'\big|_{\mathbb{L}_1} = \widetilde{\beta}\big|_{\mathbb{L}_1}$;*

(3) *$\beta'(P) = m(P)$ for $P \in \mathbb{Y}_0 \backslash (\mathbb{L}_1 \cup \mathbb{L}_{\beta'})$;*

(4) *β' is symmetric.*

(b) The number of bijections related to $\widetilde{\beta}$ is equal to 2^k, where

$$k = \#\big\{P \in \mathbb{L}_2 \mid P - (P - \widetilde{\beta}_2(P))^\vee \in m(\mathbb{Y}_0)\big\}.$$

Proof of Proposition 5.5. "$\Longrightarrow$". It is straightforward.

"$\Longleftarrow$". By the construction of $\widetilde{\beta}_1$, we know that $P - \beta'(P)$ is not diagonal for each point P in $\mathbb{L}_2$; and $\beta'^{-1}(Q) - Q$ is not diagonal for each point Q in $m(\mathbb{L}_2)$. On the other hand, since β' and $\widetilde{\beta}$ are related, there are exact $2 \bullet \#\mathbb{L}_2$ non-diagonal vectors in $\Big\{P - \beta'(P) \;\Big|\; P \in \mathbb{Y}_0\Big\}$. Therefore, we have

$$\Big\{P - \beta'(P) \;\Big|\; P \in \mathbb{L}_{\beta'}\Big\}^\star = \Big\{P - \widetilde{\beta}(P) \;\Big|\; P \in \mathbb{L}_{\widetilde{\beta}}\Big\}^\star. \tag{5.20}$$

Recall that we denote $V(\overline{\beta}_2) = \{\vec{v}_1, \vec{v}_2, \dots\}$. Assume that β' does not satisfy Property (1). We put i be the smallest number such that there exists some point P_0 which satisfies

$$P_0 - \widetilde{\beta}(P_0) = \vec{v}_i \text{ or } \vec{v}_i^{\vee} \quad \text{and} \quad P_0 - \beta'(P_0) \neq \vec{v}_i \text{ or } \vec{v}_i^{\vee}.$$

It is easy to see that for each point Q in $m(\mathbb{Y}_0) \cap \mathscr{D}_k$, there exists at most one vector $\vec{v}$ in $V(\overline{\beta}_2) \cup V(\overline{\beta}_2)^{\vee}$ such that $P_0 + \vec{v}$ belongs to $\mathbb{L}_2$. Combining it with Lemma 5.17 allows us to induce a injection $\beta_2' : \mathbb{L}_2 \to m(\mathbb{Y}_0)$ from $\widetilde{\beta}_2$ such that

$$\beta_2'(P) = \begin{cases} \widetilde{\beta}_2(P_0) & \text{if } P = P_0; \\ \beta'(P) & \text{else.} \end{cases}$$

It is easy to check that β_2' is greater than $\widetilde{\beta}_2$ with respect to "$\prec_2$", a contradiction. Therefore, β' satisfies Property (1).

Apply the same argument to $m \circ \beta'^{-1} \circ m$, we know that

$$\beta'^{-1}(Q) - Q = \widetilde{\beta}^{-1}(Q) - Q \text{ or } (\widetilde{\beta}^{-1}(Q) - Q)^{\vee} \text{ for all } Q \text{ in } m(\mathbb{L}_2).$$

Recall that we define the partial order "$\prec_1$" and $V^{\star}(\beta)$ in Definitions 5.3 and 5.4. One can check that $V^{\star}(\widetilde{\beta}|_{\mathbb{Y}_0 \backslash \mathbb{L}_{\widetilde{\beta}}})$ is actually the only maximal element in the set

$$\left\{ V^{\star}(\beta) \;\middle|\; \beta : \mathbb{Y}_0 \backslash \mathbb{L}_{\widetilde{\beta}} \to m(\mathbb{Y}_0 \backslash \mathbb{L}_{\widetilde{\beta}}) \text{ and } \beta \text{ is diagonal} \right\}$$

with respect to the partial order " $\prec_1$".

As a corollary of Lemma 5.17, we know that for each k, there does not exist two points in $\mathscr{D}_k$ such that one is from $\mathbb{L}_1$ and the other is from $\beta'(\mathbb{L}_2)$. Therefore, if we put β'' to be a

bijection from $\mathbb{Y}_0$ to $m(\mathbb{Y}_0)$ such that β'' is an element in

$$\Big\{\beta : \mathbb{Y}_0 \to m(\mathbb{Y}_0) \mid \mathbb{L}_\beta = \mathbb{L}_{\beta'} \ \&\ \beta \text{ is diagonal}\Big\},$$

which maximizes $V^\star(\beta'')$ with respect to "$\prec_1$", then we have

$$\beta''|_{\mathbb{L}_1} = \widetilde{\beta}|_{\mathbb{L}_1}.$$

Moreover, we can check that $V^\star(\beta'') \preceq_1 V^\star(\widetilde{\beta})$ and the equation hold if and only if $\mathbb{L}_{\beta'}$ is weakly symmetric and $\beta'(P) = m(P)$ for each $P \in \mathbb{Y}_0 \backslash (\mathbb{L}_1 \cup \mathbb{L}_{\beta'})$.

On the other hand, since β' and $\widetilde{\beta}$ are related, we know that $V^\star(\beta') =_1 V^\star(\widetilde{\beta})$. Hence, we have

$$\beta'|_{\mathbb{Y}_0 \backslash \mathbb{L}_{\beta'}} = \beta''|_{\mathbb{Y}_0 \backslash \mathbb{L}_{\beta''}},$$

which implies that β' satisfies Property (2) and (3).

Then we are left to show that $\beta'|\mathbb{L}_{\beta'}$ is symmetric. First, from the argument above, we know that it is weakly symmetric. Therefore, for any point P in $\mathbb{L}_2$, if we put $P' := m(\beta'(P))$, we know that $\beta'(P') \in m(\mathbb{L}_2)$. Since we checked Property (1) already, we know that $P' - \beta'(P') \in V(\overline{\beta}_2) \cup V(\overline{\beta}_2)^\vee$. As the argument above, there are at most one vector $\vec{v}$ in $V(\overline{\beta}_2) \cup V(\overline{\beta}_2)^\vee$ such that $P' - \vec{v} \in m(\mathbb{L}_2)$, which obviously is $P' - m(P)$. Therefore, we know that β' is symmetric.

(b) It follows directly from (a). □

Proof of Proposition 4.3. (1) By Proposition 5.5, we check that $\widetilde{\beta}$ constructed in (5.19) is exactly the needed $\widetilde{\beta}$ in this proposition. Moreover, we know that the integer i in this

proposition is equal to

$$\#\big\{P \in \mathbb{L}_2 \mid P - (P - \widetilde{\beta}_2(P))^{\vee} \in m(\mathbb{Y}_0)\big\}.$$

(2) From Lemma 4.1, we know that two special bijections contribute a same monomial to $\widetilde{v}^{\mathrm{sp}}_{h(\mathbb{T}_1)}$ in Lemma 4.6 if and only if they are related. By Corollary 4.1 and part (1) of this proposition, we have

$$\widetilde{v}_{h(\mathbb{T}_1)} = \frac{2^i}{\prod\limits_{P\in\mathbb{T}_1}\prod\limits_{i=1}^{\mathbb{x}'_1} b_{P,\tau(\widetilde{\beta}),i}!}\prod_{i=1}^{\mathbb{x}'_1}\widetilde{a}_{Q_i}^{\sum\limits_{P\in\mathbb{T}_1} b_{P,\tau(\widetilde{\beta}),i}} + \text{“other terms”}, \tag{5.21}$$

where “other terms” is a power series in $\mathbb{Z}_p[\widetilde{\underline{a}}]$ which contains no term like $\widetilde{a}_{Q_i}^{\sum\limits_{P\in\mathbb{T}_1} b_{P,\tau(\widetilde{\beta}),i}}$. Since for any $P \in \mathbb{T}_1$ and any $1 \leqslant i \leqslant \mathbb{x}'_1$, we know that $b_{P,\tau(\widetilde{\beta}),i}$ in (5.21) is less than p, we complete the proof of this proposition. □

Bibliography

[AS] A. Adolphson and S. Sperber, Exponential sums and Newton polyhedra: Cohomology and estimates. *Ann. of Math.* **Vol. 130** (1989), 367–406.

[BE] B. Berndt and R. Evans, The determination of Gauss sums, *Bull. Amer. Math. Soc.*, **5** (1981), 107–129.

[BF] R. Blache, E. Ferard, Newton stratification for polynomials: the open stratum, *J. Number Theory.* **123** (2007), 456–472.

[BFZ] R. Blache, E. Ferard, and H. Zhu, Hodge–Stickelberger polygons for L-functions of exponential sums of $P(x^s)$, *Math. Res. Lett.* **15** (2008), no. 5, 1053–1071.

[DWX] C. Davis, D. Wan, and L. Xiao, Newton slopes for Artin–Schreier–Witt towers, *Math. Ann.* **364** (2016), no. 3, 1451–1468.

[H] D. Haessig, L-functions of symmetric powers of Kloosterman sums (unit root L-functions and p-adic estimates), `arXiv:1504.05802`.

[KW] M. Kosters, D. Wan, On the arithmetic of $\mathbb{Z}_p$-extensions, `arXiv:1612.07158`.

[LWan] C. Liu and D. Wan, T-adic exponential sums over finite fields, *Algebra Number Theory* **3** (2009), no. 5, 489–509.

[LWX] R. Liu, D. Wan, and L. Xiao, Slopes of eigencurves over the boundary of the weight space, *to appear in Duke Math. J.*, `arXiv:1412.2584`.

[LWei] C. Liu and D. Wei, The L-functions of Witt coverings, *Math. Z.* **255** (2007), 95–115.

[OY] Y. Ouyang, J. Yang, Newton polygons of L functions of polynomials $x^d + ax$. *J. Number Theory.* **160** (2016), 478–491.

[OZ] Y. Ouyang and S. Zhang, Newton polygons of L-functions of polynomials $x^d + ax^{d-1}$ with $p \equiv -1 \pmod{d}$. *Finite Fields and their Appl.* **37** (2016), 285–294.

[R] R. Ren, Spectral halo for Hilbert modular forms, *in preparation.*

[RWXY] R. Ren, D. Wan, L. Xiao, and M. Yu, Slopes for higher rank Artin–Schreier–Witt Towers, *to appear in Trans. Amer. Math. Soc.*, `arXiv:1605.02254`.

[SZ] J. Scholten and H. Zhu, Slope estimates of Artin-Schreier curves. *Compositio Math.* **137** (2003), no. 3, 275–292.

[W] D. Wan, Variation of p-adic Newton polygons for L-functions of exponential sums, *Asian J. Math.* **8** (2004), no. 3, 427–471.

[WXZ] D. Wan, L. Xiao, and J. Zhang, Slopes of eigencurves over boundary disks, *to appear in Math. Ann.*, `arXiv:1407.0279`.

[Z1] H. Zhu, p-adic variation of L-functions of one variable exponential sums, I. *American Journal of Mathematics.* **125** (2003), 669–690.

[Z2] H. Zhu, Generic Newton Slopes for Artin–Schreier–Witt Tower in two variables, `arXiv:1612.07158`.