Journal of Number Theory 143 (2014) 82–101

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Generic A-family of exponential sums

Hui June Zhu

Department of Mathematics, State University of New York at Buffalo, Buffalo, NY 14260, United States

A R T I C L E   I N F O

Article history:
Received 9 August 2013
Received in revised form 1 January 2014
Accepted 9 March 2014
Available online 14 May 2014
Communicated by D. Wan

MSC:
11,14

Keywords:
Exponential sums
Artin–Schreier curves
L functions
Dwork theory
Frobenius problem

A B S T R A C T

Let $\vec{s} := (s_1, s_2, \ldots, s_m)$ with $s_1 < \cdots < s_m$ being positive integers. Let $\mathbf{A}(\vec{s})$ be the space of all 1-variable polynomials $f(x) = \sum_{\ell=1}^{m} a_\ell x^{s_\ell}$ parameterized by coefficients $\vec{a} = (a_1, \ldots, a_m)$ with $a_m \neq 0$. We study the p-adic valuation of the roots of the L-function of exponential sum of $\overline{f}$ for modulo p reduction of any generic point $f \in \mathbf{A}(\vec{s})(\overline{\mathbf{Q}})$. Let $\mathrm{NP}(\overline{f})$ be the normalized p-adic Newton polygon of the L function of exponential sums of $\overline{f}$. Let $\mathrm{GNP}(\mathbf{A}(\vec{s}), \overline{\mathbf{F}}_p)$ be the generic Newton polygon for $\mathbf{A}(\vec{s})$ over $\overline{\mathbf{F}}_p$, and let $\mathrm{HP}(\mathbf{A}(\vec{s})) := \mathrm{NP}_p(\prod_{i=1}^{d-1}(1 - p^{\frac{i}{d}} T))$ be the absolute lower bound of $\mathrm{NP}(\mathbf{A}(\vec{s}))$. One knows that $\mathrm{NP}(\overline{f}) \prec \mathrm{GNP}(\mathbf{A}(\vec{s}); \overline{\mathbf{F}}_p) \prec \mathrm{HP}(\overline{f})$ for all prime p and for all $\overline{f} \in \mathbf{A}(\vec{s})(\overline{\mathbf{Q}})$, and these equalities hold only when $p \equiv 1 \bmod d$. In the case $\vec{s} = (s, d)$ with $s < d$ coprime we provide a computational method to determine $\mathrm{GNP}(\mathbf{A}(s, d), \overline{\mathbf{F}}_p)$ explicitly by constructing its generating polynomial $H_r \in \mathbf{Q}[X_{r,1}, X_{r,2}, \ldots, X_{r,d-1}]$ for each residue class $p \equiv r \bmod d$. For $p \equiv r \bmod d$ (with $2 \le r \le d-1$ coprime to d) large enough $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ with $\prod_{n=1}^{d-1} h_{r,n,k_{r,n}} \neq 0$ if and only if $\mathrm{GNP}(\mathbf{A}(s, d), \overline{\mathbf{F}}_p)$ has its breaking points after the origin at

$$\left(\left(n, \frac{n(n+1)}{2d} + \frac{(1 - \frac{s}{d}) k_{r,n}}{p-1}\right)\right)_{n=1,2,\ldots,d-1}.$$

If $a \neq 0$ then for any $f = x^d + a x^s \in \mathbf{A}(s, d)(\overline{\mathbf{Q}})$ and for any prime $p \equiv r \bmod d$ large enough we have that $\mathrm{NP}(\overline{f}) = \mathrm{GNP}(\mathbf{A}(s, d), \overline{\mathbf{F}}_p)$ and

E-mail address: hjzhu@math.buffalo.edu.

http://dx.doi.org/10.1016/j.jnt.2014.03.013

$$\lim_{p\to\infty} \mathrm{NP}(\bar{f}) = \mathrm{HP}\big(\mathbf{A}(s,d)\big).$$

Our method applies to compute the generic Newton polygon of Artin–Schreier family $y^p - y = x^d + ax^s$ parameterized by a for p large enough.

1. Introduction

Let $\vec{s} := (s_1, s_2, \ldots, s_m)$ with $s_1 < \cdots < s_m$ being positive integers. Let $\mathbf{A}(\vec{s})$ be the space of all 1-variable polynomials $f(x) = \sum_{\ell=1}^{m} a_\ell x^{s_\ell}$ parameterized by coefficients $\vec{a} = (a_1, \ldots, a_m)$ with $a_m \neq 0$. Without loss of generality we set $a_m = 1$. Fix a primitive p-th root of unity ζ_p. Let $f = \sum_{\ell=1}^{m} a_\ell x^{s_\ell} \in \mathbf{A}(\vec{s})(\overline{\mathbf{Q}})$ be a closed point, that is, $\vec{a} \in \overline{\mathbf{Q}}^m$. Let $\wp$ be a prime ideal in the number field $\mathbf{Q}(a_1, \ldots, a_m)$ lying over p, suppose its residue field is $\mathbf{F}_q$ for some p-power q. For any $k \in \mathbf{Z}_{\geq 1}$ the k-th exponential sum of $\bar{f} := f \bmod \wp$ in $\mathbf{F}_q[x]$ is defined to be

$$S_k(\bar{f}) = \sum_{x \in \mathbf{F}_{q^k}} \zeta_p^{\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(\bar{f}(x))}$$

and the L function of the exponential sum of $\bar{f}/\mathbf{F}_q$ is defined to be

$$L(\bar{f}/\mathbf{F}_q; T) = \exp \sum_{k=1}^{\infty} S_k(\bar{f}) T^k / k.$$

It is known that $L(\bar{f}/\mathbf{F}_q; T) = \sum_{i=0}^{d-1} c_i T^i$ lies in $\mathbf{Z}[\zeta_p][T]$ with $c_0 = 1$. The normalized p-adic Newton polygon of $L(\bar{f}/\mathbf{F}_q; T)$ is denoted by $\mathrm{NP}(\bar{f}) := \mathrm{NP}_q(L(\bar{f}/\mathbf{F}_q; T))$, that is, the lower convex hull of the points $(i, \mathrm{ord}_q c_i)$ for $i = 0, 1, \ldots, d-1$ in the real plane $\mathbf{R}^2$, where $\mathrm{ord}_q c = \mathrm{ord}_p c / \log_p q$. Consider all (lower convex) Newton polygons with the same domain as piece-wise linear functions, we define a partial order $\mathrm{NP}_1 \prec \mathrm{NP}_2$ if NP_1 lies over NP_2. For each prime p, there exists a lower bound for all $\mathrm{NP}(\bar{f})$ by the Grothendieck–Katz specialization theorem (see [Katz]), that is, there exists $\bar{f}_0 \in \mathbf{A}(\vec{s})(\overline{\mathbf{F}}_p)$ such that $\mathrm{NP}(\bar{f}) \prec \mathrm{NP}(\bar{f}_0)$ for all $\bar{f}$ in $\mathbf{A}(\vec{s})(\overline{\mathbf{F}}_p)$. The generic Newton polygon is defined by $\mathrm{GNP}(\mathbf{A}(\vec{s}); \overline{\mathbf{F}}_p) := \mathrm{NP}(\bar{f}_0)$.

In this paper we shall always represent a Newton polygon by its breaking points coordinates in $\mathbf{R}^2$ after origin. Let

$$\mathrm{HP}\big(\mathbf{A}(\vec{s})\big) := \mathrm{NP}_p\left(\prod_{i=1}^{d-1}\big(1 - p^{\frac{i}{d}} T\big)\right).$$

In the literature $\mathrm{HP}(\mathbf{A}(\vec{s}))$ is often called the Hodge polygon of $\mathbf{A}(\vec{s})$ (due to its intimate relation to the Hodge polygon in related toric geometry), and its breaking points after origin are $(n, \frac{n(n+1)}{2d})$ for $n = 1, \ldots, d-1$. It is known that

$$\mathrm{NP}(\bar{f}) \prec \mathrm{GNP}\big(\mathbf{A}(\vec{s}); \overline{\mathbf{F}}_p\big) \prec \mathrm{HP}\big(\mathbf{A}(\vec{s})\big) \tag{1}$$

and their endpoints coincide (see [AS89]). In fact this inequality holds for more general families of Laurent polynomials in multivariables (see for instance [AS89]). For $p \equiv 1 \bmod d$ we have all three polygons coincide, but it is not the case for other residue classes of the prime p. In fact, GNP generally depends not only on the residue class of p but also p itself, and from experimental data for lower degree cases one observes that GNP has a formula for each residue families for p large enough, and we prove this in this paper and give explicit formulas.

For $\vec{s} = (1, 2, \ldots, d)$, Wan has conjectured that a generic polynomial of degree d in $\mathbf{A}(\vec{s})(\overline{\mathbf{Q}})$ has its Newton polygon at each mod p reduction approaching to the absolute lower bound $\mathrm{HP}(\mathbf{A}(\vec{s}))$ as p approaches infinity (see [Wan04]). This conjecture was proved in [Zhu03] and [Zhu04] where it is also proved that Wan's conjecture applies to a 1-parameter family $\mathbf{A}(1, d)$. See also [Yan03]. In this paper we generalize a main theorem of [Zhu03] from $\mathbf{A}(1, d)$ to the more general family $\mathbf{A}(s, d)$. Our major contribution of the current paper is to provide an explicit method allowing one to compute $\mathrm{GNP}(\mathbf{A}(s, d), \overline{\mathbf{F}}_p)$ for every prime p large enough. We prove in this paper the generic Newton polygon at each prime p may be computed globally over $\mathbf{Q}$ instead, and for p large enough it has a formula depending only on the residue of p mod d. Our method is under further development for families of more parameters and for T-adic exponential sums families [LW09].

For any c in $\overline{\mathbf{Q}}$ we use $\mathrm{MaxPrime}(c)$ to denote the maximal prime factor of $N_{\mathbf{Q}(c)/\mathbf{Q}}(c)$ in $\mathbf{Q}$ (in both numerator and denominator). Let $\mathrm{MaxPrime}(c_1, c_2, \ldots, c_N)$ be the maximum of $\mathrm{MaxPrime}(c_i)$'s for $i = 1, \ldots, N$.

For any $2 \le r \le d-1$ coprime to d, we construct a generating polynomial $H_r \in \mathbf{Q}[X_{r,1}, \ldots, X_{r,d-1}]$ for $\mathrm{GNP}(\mathbf{A}(s, d), \overline{\mathbf{F}}_p)$ in Section 2, see (8). Key result of this paper lies in the following theorem:

Theorem 1.1. *Let $s < d$ be coprime positive integers.*

Suppose $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$. Let

$$N_{s,d,r} := \max\big(s(d-1), d + \max_n(k_{r,n}), 2(d-s)\max_n(k_{r,n}), \mathrm{MaxPrime}_n(h_{r,n,k_{r,n}})\big)$$

where $1 \le n \le d-1$. For every prime $p \equiv r \bmod d$ and $p > N_{s,d,r}$, the generic Newton polygon $\mathrm{GNP}(\mathbf{A}(s, d), \overline{\mathbf{F}}_p)$ has its breaking points after the origin at

$$\left(\left(n, \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}\right)\right)_{n=1,\ldots,d-1}.$$

Conversely, suppose $\mathrm{GNP}(\mathbf{A}(s,d),\overline{\mathbf{F}}_p)$ *has its breaking points after the origin at* $((n,\frac{n(n+1)}{2d}+\frac{(1-\frac{s}{d})k_{r,n}}{p-1}))_{n=1,\dots,d-1}$ *for all prime* $p>N_{s,d,r}$ *then we have* $H_r=\sum_{n=1}^{d-1}h_{r,n,k_{r,n}}X_{r,n}^{k_{r,n}}$ *with* $\prod_{n=1}^{d-1}h_{r,n,k_{r,n}}\neq 0$.

Let $f=x^d+ax^s\in\mathbf{A}(s,d)(\overline{\mathbf{Q}})$ *and we write* $\overline{f}$ *for its reduction modulo a prime in* $\mathbf{Q}(a)$ *over* p. *Suppose* $a\neq 0$. *Then for all prime* $p\equiv r \bmod d$ *and* $p>\max(N_{s,d,r},\mathrm{MaxPrime}(a))$ *we have*

$$\mathrm{NP}(\overline{f})=\mathrm{GNP}\bigl(\mathbf{A}(s,d);\overline{\mathbf{F}}_p\bigr)$$

and $\lim_{p\to\infty}\mathrm{NP}(\overline{f})=\mathrm{HP}(\mathbf{A}(s,d))$.

If $s<d$ are not coprime, then the statements relating to $\mathrm{HP}(\mathbf{A}(s,d))$ in Theorem 1.1 are false. However, there exists $\mathrm{GNP}(\mathbf{A}(s,d),\overline{\mathbf{F}}_p)$ in that case and the situation was carried out in [BFZ08].

As a byproduct we show that the generic Newton polygon $\mathrm{GNP}(\mathbf{A}(s,d),\overline{\mathbf{F}}_p)$ for $p\equiv r \bmod d$ and p is large enough has a formula. We shall also see that each of these generic Newton polygons can be achieved by some $\overline{f}$ in $\mathbf{F}_p[x]$.

For our family $\mathbf{A}(s,d)$ we construct a semi-linear Fredholm A-matrix M' (where A is our parameter) which represents Dwork's Frobenius matrix over $\mathbf{F}_p$. The L function of a closed special point $\overline{f}\in\mathbf{A}(s,d)(\mathbf{F}_q)$ with $q=p^c$ is determined by the Fredholm A-matrix $M'_c:=M'\cdot(M')^{-\tau}\cdot\dots\cdot(M')^{-\tau^{c-1}}$ where τ is the Frobenius map. However, this infinite matrix is notoriously messy to compute if one ever can, and furthermore c can be arbitrarily large and this changes the corresponding L-function fundamentally. Meanwhile, the Fredholm determinant of M'_c also depends on the prime p intricately. Our method here is: we first work out complete solution set to the Frobenius problem in 2-dimensional case (it is not yet known one can explicitly compute all such complete solution set for higher than 2 dimensional cases, see [Ram05]). Then for p large enough we approximate our Fredholm A-matrix by a finite one. This finite Fredholm A-matrix can be explicitly written down, and most remarkably its p-adic order has a formula for each residue of $p \bmod d$. We prove in this paper that the generic A-families over $\overline{\mathbf{F}}_p$ for p large enough are all the images of a global generic object over $\overline{\mathbf{Q}}$.

Our theorem has application to Artin–Schreier families. The most intensively studied question has been the first slope for Artin–Schreier curves or families. First generic slopes have been studied in the literature (see for instance [Bla11]). For any $f=x^d+ax^s\in\mathbf{A}(s,d)(\overline{\mathbf{Q}})$ let $X_f: y^p-y=f(x) \bmod \wp$ be the corresponding mod p reduction over some finite field $\mathbf{F}_q$. It is known that the Zeta function $\mathrm{Zeta}(X_f/\mathbf{F}_q;T)$ of $X_f/\mathbf{F}_q$ in variable T lies in $\mathbf{Q}[T]$ and its numerator (as the core factor) is a polynomial of degree $(d-1)(p-1)$. In fact it is known that

$$\mathrm{Zeta}(X_f/\mathbf{F}_q;T)=\frac{N_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(L(\overline{f}/\mathbf{F}_q;T))}{(1-T)(1-qT)}$$

where the norm being defined as the product of all Galois conjugates of the polynomial $L(\overline{f}/\mathbf{F}_q;T) \in \mathbf{Q}[\zeta_p][T]$ where the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ acts trivially on the variable T. Let the Newton polygon $\mathrm{NP}(X_f/\mathbf{F}_q)$ of $X_f/\mathbf{F}_q$ be the q-adic Newton polygon of the numerator of $\mathrm{Zeta}(X_f/\mathbf{F}_q;T)$. Thus $\mathrm{NP}(\overline{f}/\mathbf{F}_q)$ is equal to $\mathrm{NP}(X_f/\mathbf{F}_q)$ shrunk by a factor of $p-1$ horizontally and vertically, which we denote by $\mathrm{NP}(\overline{f}/\mathbf{F}_q) = \mathrm{NP}(X_f/\mathbf{F}_q)/(p-1)$. Then the following geometric application is an immediate corollary of Theorem 1.1.

Corollary 1.2. *Let $2 \le r \le d-1$. Let $H_r \in \mathbf{Q}[X_{r,1},\dots,X_{r,d-1}]$ be the generating polynomial constructed in Theorem 1.1. Suppose $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ with $\prod_{n=1}^{d-1} h_{r,n,k_{r,n}} \neq 0$. If $a \neq 0$ then for any $f = x^d + ax^s$ in $\mathbf{A}(s,d)(\overline{\mathbf{Q}})$ and for any prime p large enough we have $\frac{\mathrm{NP}(X_f/\mathbf{F}_q)}{p-1} = \mathrm{GNP}(\mathbf{A}(s,d),\overline{\mathbf{F}}_p)$ whose breaking points after origin are*

$$\left(\left(n, \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}\right)\right)_{n=1,\dots,d-1}$$

and

$$\lim_{p\to\infty} \frac{\mathrm{NP}(X_f/\mathbf{F}_q)}{p-1} = \mathrm{HP}\big(\mathbf{A}(s,d)\big).$$

This paper is organized as follows. We first have some preliminary preparation in Section 2 and define generating polynomials H_r for every $2 \le r \le d-1$. These polynomials in $\mathbf{Q}[X_{r,1},\dots,X_{r,d-1}]$ depend only on s, d and r essentially. In fact, the most technical procedure in this paper is the construction of these global (p-free!) generating polynomials that are linked to p-adic Fredholm determinant of the Frobenius for all primes p large enough. Section 3 provides the bridge between these global polynomials H_r over $\mathbf{Q}$ and the p-adic local analysis, especially under the condition that p is large enough. Section 4 develops Dwork theory for our 1-parameter a-family $\mathbf{A}(s,d)(\overline{\mathbf{F}}_p)$ for p large enough. We prove our main result Theorem 1.1 in Section 4.

2. Frobenius problem and generating polynomials for GNP

2.1. Preliminaries

In this section we develop combinatorial and number theoretic preparations for our main theorem. These two lemmas are elementary yet essential in the arguments of this paper.

Lemma 2.1. *Let r, d be two coprime positive integers with $r < d$. Let $h(z)$ be a fixed nonzero polynomial in $\overline{\mathbf{Q}}[z]$. Then $h(-\frac{r}{d}) \neq 0$ if and only if for all large enough prime $p \equiv r \bmod d$ we have $h(\lfloor \frac{p}{d} \rfloor) \in \overline{\mathbf{Z}}_p^*$.*

Proof. For all prime p large enough we have $h(z) \in \overline{\mathbf{Z}}_p[z]$ obviously. For such p notice that $p \nmid d$, so we have $\lfloor \frac{p}{d} \rfloor \equiv -\frac{r}{d} \bmod p$ and hence $h(\lfloor \frac{p}{d} \rfloor) \in \overline{\mathbf{Z}}_p^*$ if and only if $h(-\frac{r}{d}) \in \overline{\mathbf{Z}}_p^*$.

If $\theta := h(-\frac{r}{d}) \in \overline{\mathbf{Q}}^*$ then it is clear that $h(-\frac{r}{d}) \in \overline{\mathbf{Z}}_p^*$ for all $p > \operatorname{MaxPrime}(\theta)$. That is $h(\lfloor \frac{p}{d} \rfloor) \in \overline{\mathbf{Z}}_p^*$ for all such p. The converse is clear. $\square$

When $h(z)$ lies in $\mathbf{Z}[z]$ we have the following lemma that yields an effective bound for p. For any $h \in \mathbf{Q}[z]$ let $h^o := h/\operatorname{cont}(h)$ where $\operatorname{cont}(h)$ is the content of the polynomial h.

Lemma 2.2. *Let r, d be two positive integers with $r < d$. Let $h(z) \in \mathbf{Z}[z]$.*

(1) *If $h(-\frac{r}{d}) \neq 0$ then $dz_0 + r \nmid h(z_0)$ for all integers $z_0 \geq d^{\deg(h)-1}|h(-\frac{r}{d})|$.*
(2) *Suppose prime $p \nmid \operatorname{cont}(h)$ and $p > d$. If $h(-\frac{r}{d}) \neq 0$ then $h(\lfloor \frac{p}{d} \rfloor) \in \mathbf{Z}_p^*$ for all $p > \operatorname{MaxPrime}(h^o(-\frac{r}{d}))$; conversely, if $h(\lfloor \frac{p}{d} \rfloor) \in \mathbf{Z}_p^*$ for any prime p, then $h(-\frac{r}{d}) \neq 0$.*

Proof. (1) Without loss of generality we assume $h(z)$ has its leading coefficient > 0. Taking long division algorithm in $\mathbf{Q}[z]$ we have $h(z) = (dz + r)g(z) + R$ for unique $R = h(-\frac{r}{d}) \in \mathbf{Q}$ and unique $g(z) \in \mathbf{Q}[z]$ with leading coefficient > 0. Suppose for $z_0 \in \mathbf{Z}_{>0}$ we have $h(z_0) = (dz_0 + r)C$ for some nonzero integer C depending on z_0 of course. Then we have

$$h\left(-\frac{r}{d}\right) = (dz_0 + r)\big(C - g(z_0)\big).$$

Let $h(z) = \sum_{i=0}^{m} h_i z^i$ for $h_i \in \mathbf{Z}$ and write $g(z) = \sum_{i=0}^{m-1} g_i z^i$, then we have $g_{m-1} = h_m/d$ and $g_{i-1} = (h_i - rg_i)/d$ for all $1 \leq i \leq m-1$. Hence we have $d^m g_i \in \mathbf{Z}$ for all i. Rewrite the above equation below

$$d^m h\left(-\frac{r}{d}\right) = (dz_0 + r)\big(d^m C - d^m g(z_0)\big).$$

Since the left-hand-side is a fixed integer, and the factor $d^m C - d^m g(z_0)$ is also an integer, we have that $dz_0 + r \leq d^m|h(-\frac{r}{d})|$. This says that if $dz_0 + r > d^m|h(-\frac{r}{d})|$ or equivalently $z_0 \geq d^{m-1}|h(-\frac{r}{d})|$, then we have $dz_0 + r \nmid h(z_0)$.

(2) Write $c = \operatorname{cont}(h)$. Assume that prime $p = dz_0 + r$ is coprime to c with $z_0 := \lfloor p/d \rfloor$. Then $C = cC^o$ for some $C^o \in \mathbf{Z}$ as in Part (1) of the proof. Write $g = cg^o$ for $g^o \in \mathbf{Q}[x]$, we have $h^o(z) = (dz + r)g^o(z) + h^o(-\frac{r}{d}) \in \mathbf{Z}[z]$ implies that $d^m g^o(z) \in \mathbf{Z}[z]$. We have

$$d^m h^o\left(-\frac{r}{d}\right) = p\big(d^m C^o - d^m g^o(z_0)\big).$$

Since the left-hand-side is a fixed integer, and the factor $d^m C^o - d^m g^o(z_0)$ is also an integer, we have that $p \leq \operatorname{MaxPrime}(h^o(-\frac{r}{d}))$. This says that if prime $p > \operatorname{MaxPrime}(h^o(-\frac{r}{d}))$ then we have $p \nmid h^o(\lfloor \frac{p}{d} \rfloor)$, i.e. $p \nmid h(\lfloor \frac{p}{d} \rfloor)$. The converse is clear since $\lfloor \frac{p}{d} \rfloor \equiv -\frac{r}{d} \bmod p$ for $p > d$. $\square$

Below we shall study solutions to the Frobenius problem with given two coprime integers. We shall fix two coprime positive integers d, s with $d > s$. Given a positive integer v every nonnegative integral pair (m, n) with $dn + sm = v$ is called a solution to the Frobenius problem of (s, d) in this paper. For any nonnegative integers v with $v > ds - d - s$, let $\beta_v(d, s) := \min(m + n)$ where the minimum is taking over all nonnegative integers m, n such that $dn + sm = v$. Such minimum $\beta_v(d, s)$ exists and is achieved uniquely at $m = (s^{-1}v \bmod d)$ and $n = \frac{v}{d} - \frac{sm}{d}$. The following lemma should be known in the literature but we provide its statement and proof here for the paper to be self-contained.

Lemma 2.3. *Let p be a prime number. Let $v = pi - j$ with $1 \le i, j \le d - 1$ and let $v > ds - d - s + 1$ (or $p > s(d - 1)$). Let $r = (p \bmod d)$.*

(1) *Then the minimum is achieved uniquely $\beta_{pi-j}(s, d) = m_{ij} + n_{ij}$ at*

$$m_{ij} = \big(s^{-1}(ri - j) \bmod d\big),$$
$$n_{ij} = \frac{pi - j}{d} - \frac{sm_{ij}}{d} = \left\lfloor \frac{p}{d} \right\rfloor i + \frac{ri - j - sm_{ij}}{d}.$$

(2) *We have $\beta_{pi-j}(s, d) = \frac{pi-j}{d} + (1 - \frac{s}{d})m_{ij} \ge \lceil \frac{pi-j}{d} \rceil \ge \lfloor \frac{pi}{d} \rfloor$.*
(3) *We have $0 \le m_{ij} \le d - 1$ and $\lfloor \frac{pi}{d} \rfloor - s + 1 \le n_{ij} \le \lfloor \frac{pi}{d} \rfloor$.*
(4) *A general solution to this Frobenius problem is*

$$n_{ij}^\ell := n_{ij} - s\ell, \qquad m_{ij}^\ell := m_{ij} + d\ell$$

for some $0 \le \ell \le \lfloor \frac{pi-j}{ds} \rfloor$. (The minimum β is achieved if and only if $\ell = 0$.) The sum of these solutions is

$$m_{ij}^\ell + n_{ij}^\ell = \beta_{pi-j}(s, d) + (d - s)\ell.$$

Proof. We prove our statements for general integer $v > 0$ first as the specialization to $v = pi - j$ does not alter the argument. It follows from that $d > s$ that this minimum of $m_v + n_v$ is uniquely achieved when m_v is minimal. Let $m_v := (s^{-1}v \bmod d)$ be the least nonnegative residue mod d. It is clear that m_v is the minimal nonnegative solution possible to the equation $dn_v + sm_v = v$. Let $n_v := (v - sm_v)/d$. Since $v > ds - d - s + 1$, we have $v > (d - 1)(s - 1) \ge m_v(s - 1)$. Thus $v - sm_v > -m_v \ge -(d - 1)$. Since n_v is an integer with $n_v > -(d - 1)/d$ and hence $n_v \ge 0$. Therefore, m_v, n_v are nonnegative integers satisfying the equation $dn_v + sm_v = v$. The rest of the statements follow from the definition. □

Observe from Lemma 2.3 that matrix (m_{ij}) is bounded in each entry by $d - 1$, and it varies and exhausts the residue class on each row and each column. Its value depends on $r = (p \bmod d)$. On the other hand, each n_{ij} lies in the small neighborhood of $\frac{pi}{d}$, and hence it increases as p increases, but each $n_{ij}^{\ell} < p$ for all $1 \le i, j \le d-1$.

2.2. *Generating polynomials for* GNP

Recall $s < d$ are two coprime positive integers. The goal of this subsection is to define the generating polynomial H_r in $\mathbf{Q}[X_{r,1}, \ldots, X_{r,d-1}]$ for every residue $2 \le r \le d-1$ exponents of whose nonzero terms give us $\mathrm{GNP}(\mathbf{A}(\vec{s}), \overline{\mathbf{F}}_p)$. This subsection is a dry run. The readers who seek motivation should read Section 4 first.

The case for $r = 1$ is known hence we will omit it entirely, in fact one can also write $H_1 = 1$ for completeness. The idea is that the generic A-determinant in the focus of our study depends only on the residue $r = (p \bmod d)$, not on p itself. There is a generating polynomial for the generic A-family whose (nonzero) terms encode the information of $\mathrm{GNP}(\mathbf{A}(s,d), \overline{\mathbf{F}}_p)$.

From now on we fix r, s with $2 \le r \le d-1$ is coprime to d and $1 \le n \le d-1$. For each $1 \le i \le d-1$ we define a linear function in variable z

$$\psi_{r,i}(z) := iz + \left\lfloor \frac{ri}{d} \right\rfloor. \tag{2}$$

For any positive integer t we denote the t-th *falling factorial power* of Y by $[Y]_t := Y(Y-1)\cdots(Y-t+1)$, where Y lies in any ring containing $\mathbf{Z}$. Below our Y is either a rational number or a rational function in $\mathbf{Q}[z]$. For $1 \le i, j \le d-1$ recall $m_{ij} = (s^{-1}(ri-j) \bmod d)$ from Lemma 2.3 and let

$$t_{ij} := \left\lfloor \frac{ri}{d} \right\rfloor - \frac{ri - j - sm_{ij}}{d} + s\ell_{ij}. \tag{3}$$

Let

$$k_{r,n}^{\bullet} := \min_{\sigma \in S_n} \sum_{i=1}^{n} m_{i,\sigma(i)}. \tag{4}$$

For any $k \ge k_{r,n}^{\bullet}$ let $\mathcal{S}(k)$ be the set of all $(\sigma, (\ell_{i,\sigma(i)})_i)$ in $S_n \times \mathbf{Z}_{\ge 0}^n$ such that

$$\sum_{i=1}^{n} m_{i,\sigma(i)} + d \sum_{i=1}^{n} \ell_{i,\sigma(i)} = k.$$

Suppose $\mathcal{S}(k)$ is not empty, then for each $(\sigma, (\ell_{i,\sigma(i)})_i)$ in $\mathcal{S}(k)$ we define

$$\Theta_n := \prod_{i=1}^{n} \frac{(d-1+(k-k_{r,n}^{\bullet}))!}{(m_{i,\sigma(i)} + d\ell_{i,\sigma(i)})!} \in \mathbf{Q}.$$

In fact we shall see below in Lemma 2.5 below that $\Theta_n \in \mathbf{Z}$. Then we define a polynomial in variable z:

$$\widetilde{h}_{r,n,k}(z) := \sum_{(\sigma,(\ell_{i,\sigma(i)})_i)\in\mathcal{S}(k)} \operatorname{sgn}(\sigma)\Theta_n \prod_{i=1}^n \left[\psi_{r,i}(z)\right]_{t_{i,\sigma(i)}}. \tag{5}$$

If $\mathcal{S}(k)$ is empty, define $\widetilde{h}_{r,n,k}(z) := 0$.

We remark that in practice it is not necessary to compute $k^\bullet_{r,n}$ as one can replace Θ_n by

$$\Theta'_n := \prod_{i=1}^n \frac{(d-1+k)!}{(m_{i,\sigma(i)} + d\ell_{i,\sigma(i)})!},$$

and define $\widetilde{h}'_{r,n,k}(z)$ as that in (5) accordingly as follows:

$$\widetilde{h}'_{r,n,k}(z) := \sum_{(\sigma,(\ell_{i,\sigma(i)})_i)\in\mathcal{S}(k)} \operatorname{sgn}(\sigma)\Theta'_n \prod_{i=1}^n \left[\psi_{r,i}(z)\right]_{t_{i,\sigma(i)}}. \tag{6}$$

The following proposition shows that this replacement only changes the function up to a constant factor in $\mathbf{Q}$. Its proof follows immediately from the very definition in (5) and hence we omit.

Proposition 2.4. *Let notation be as above. Then*

$$\widetilde{h}'_{r,n,k}(z) = \left(\frac{(d-1+k)!}{(d-1+k-k^\bullet_{r,n})!}\right)^n \widetilde{h}_{r,n,k}(z).$$

Define

$$\widetilde{h}^o_{r,n,k}(z) := \frac{\widetilde{h}_{r,n,k}(z)}{\operatorname{cont}(\widetilde{h}_{r,n,k}(z))} = \frac{\widetilde{h}'_{r,n,k}(z)}{\operatorname{cont}(\widetilde{h}'_{r,n,k}(z))}. \tag{7}$$

Obviously $\widetilde{h}^o_{r,n,k}(z) \in \mathbf{Z}[z]$.

Lemma 2.5. *Let notation be as above. Fix $2 \le r \le d-1$ coprime to d and $1 \le n \le d-1$.*

(1) *If $(\sigma,(\ell_{i,\sigma(i)})_i)$ lies in $\mathcal{S}(k)$, let $b := k - k^\bullet_{r,n} \ge 0$, then $\ell_{i,\sigma(i)} \le \lfloor b/d \rfloor$.*
(2) *Then $0 \le t_{ij} \le s(b+1)$ is an integer for all $1 \le i,j \le d-1$.*
(3) *We have $\widetilde{h}_{r,n,k}(z) \in \mathbf{Z}[z]$. Furthermore, $\widetilde{h}^o_{r,n,k}(z)$ depends only on d, s, r, b and $\deg(\widetilde{h}^o_{r,n,k}(z)) \le s(n+b/d)$.*

Proof. (1) Since $k = \sum_{i=1}^n m_{i,\sigma(i)} + d\sum_{i=1}^n \ell_{i,\sigma(i)}$ we have $d\sum_{i=1}^n \ell_{i,\sigma(i)} \leq b$. Hence $\ell_{i,\sigma(i)} \leq \lfloor b/d \rfloor$.

(2) Combining the result in Part (1) it remains to show that $t^\bullet_{ij} := \lfloor \frac{ri}{d} \rfloor - \frac{ri-j-sm_{ij}}{d}$ satisfies that $0 \leq t^\bullet_{ij} \leq s$. Since $m_{ij} = (s^{-1}(ri-j) \bmod d)$ and $\gcd(s,d) = 1$ we have $sm_{ij} \equiv ri - j \bmod d$. Hence $\frac{sm_{ij}-ri+j}{d} \in \mathbf{Z}$ and so $t^\bullet_{ij} \in \mathbf{Z}$. By Lemma 2.3 we have that

$$t^\bullet_{ij} \leq \frac{j + sm_{ij}}{d} \leq \frac{(d-1) + s(d-1)}{d} \leq \frac{(s+1)(d-1)}{d}$$

and hence $t^\bullet_{ij} \leq s$ since $t^\bullet_{ij} \in \mathbf{Z}$. Notice that

$$\left\lfloor \frac{ri}{d} \right\rfloor d \geq \left\lfloor \frac{ri-j}{d} \right\rfloor d = ri - j - (ri - j \bmod d) \geq ri - j - sm_{ij}.$$

This proves that $\lfloor \frac{ri}{d} \rfloor \geq \frac{ri-j-sm_{ij}}{d}$. That is, $t^\bullet_{ij} \geq 0$.

(3) Let $b := k - k^\bullet_{r,n}$. Write $\delta_{i,\sigma(i)} := (d-1+b) - (m_{i,\sigma(i)} + d\ell_{i,\sigma(i)})$, then

$$\delta_{i,\sigma(i)} = (d - 1 - m_{i,\sigma(i)}) + (b - d\ell_{i,\sigma(i)}) \geq 0$$

by Lemma 2.3 and Part (1) above. Hence Θ_n is just the product of $\delta_{i,\sigma(i)}$-th falling factorial power of $(d-1+b)$

$$\begin{aligned}\Theta_n &= \prod_{i=1}^n \frac{(d-1+b)!}{(m_{i,\sigma(i)} + d\ell_{i,\sigma(i)})!} \\ &= \prod_{i=1}^n [d-1+b]_{\delta_{i,\sigma(i)}} \\ &= \prod_{i=1}^n (d+b-1)(d+b-2)\cdots(d+b-1-\delta_{i,\sigma(i)}).\end{aligned}$$

It is clear that this is an integer depending only on d, s, r and b.

On the other hand, the $t_{i,\sigma(i)}$-th falling factoring power of $\psi_{r,i}(z)$ is

$$\begin{aligned}\left[\psi_{r,i}(z)\right]_{t_{i,\sigma(i)}} &= \psi_{r,i}(z)\left(\psi_{r,i}(z) - 1\right)\cdots\left(\psi_{r,i}(z) - t_{i,\sigma(i)} + 1\right) \\ &= \left(iz + \left\lfloor \frac{ri}{d} \right\rfloor\right)\left(iz + \left\lfloor \frac{ri}{d} \right\rfloor - 1\right)\cdots\left(iz + \left\lfloor \frac{ri}{d} \right\rfloor - t_{i,\sigma(i)} + 1\right).\end{aligned}$$

It lies in $\mathbf{Z}[z]$ of degree $t_{i,\sigma(i)} \leq s(b+1)$ (by Part (2)), and coefficients are determined by d, s, r, b. Thus by definition, $\widetilde{h}^o_{r,n,k}(z) \in \mathbf{Z}[z]$ is of degree $\leq \max_\sigma \sum_{i=1}^n t_{i,\sigma(i)} \leq \max_\sigma \sum_i s(\ell_{i,\sigma(i)} + 1) = s(n + b/d)$ by definition. $\square$

Fix $2 \le r \le d-1$ and $1 \le n \le d-1$. Let k range over integers $\ge k^\bullet_{r,n}$ and compute $h_{r,n,k} := \widetilde{h}^o_{r,n,k}(-\frac{r}{d})$. Let $k_{r,n} \ge k^\bullet_{r,n}$ be the least integer (if exists) such that $h_{r,n,k_{r,n}} \ne 0$. Let $X_{r,n}$ be a variable, let

$$H_r := \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}. \tag{8}$$

Notice that $H_r \in \mathbf{Q}[X_{r,1}, \ldots, X_{r,d-1}]$.

Remark 2.6. Notice that in this case the definition clearly indicates that the positive integer $k_{r,n}$ is independent of p. Indeed, by Lemma 2.5 the polynomial $\widetilde{h}^o_{r,n,k}(z)$ is independent of p, hence those k with $\widetilde{h}^o_{r,n,k}(-\frac{r}{d}) = 0$ is independent of p.

We are able to explicitly calculate H_r for all $d \le 5$, in fact the following conjecture is verified for all $d \le 5$.

Conjecture 2.7. *Let H_r be as defined in (8) above. For every r with $2 \le r \le d-1$ and $\gcd(r,d) = 1$, we have $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ with $\prod_{n=1}^{d-1} h_{r,n,k_{r,n}} \ne 0$.*

Lemma 2.8. *Fix $1 \le n \le d-1$ and $2 \le r \le d-1$ coprime to d. Let $b = k - k^\bullet_{r,n} \ge 0$.*

(1) *Let $m_{ij}^{\ell_{ij}}, n_{ij}^{\ell_{ij}}$ be defined as in Lemma 2.3(4). Define*

$$\kappa_{r,n,k} := \big((d-1+b)!\big)^n \prod_{i=1}^{n} \left\lfloor \frac{pi}{d} \right\rfloor !.$$

Then we have $\kappa_{r,n,k} \in \mathbf{Z}$; and $\kappa_{r,n,k} \in (\mathbf{Z} \cap \mathbf{Z}_p^*)$ for prime $p \ge d+b$.

(2) *Define*

$$\mu_{r,n,k} := \sum_{(\sigma,\ell_{i,\sigma(i)}) \in \mathcal{S}(k)} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \frac{1}{m_{i,\sigma(i)}^{\ell_{i,\sigma(i)}}! \, n_{i,\sigma(i)}^{\ell_{i,\sigma(i)}}!}.$$

We have $\mu_{r,n,k} \in \mathbf{Q} \cap \mathbf{Z}_p$ for all prime $p \equiv r \bmod d$ and $p \ge d+b$. Furthermore, we have

$$\widetilde{h}_{r,n,k}\left(\left\lfloor \frac{p}{d} \right\rfloor\right) = \kappa_{r,n,k} \cdot \mu_{r,n,k}.$$

Proof. (1) It is clear that $\kappa_{r,n,k} \in \mathbf{Z}$. Since $n \le d-1$ we have $\lfloor pi/d \rfloor \le p-1$ and hence $\lfloor \frac{pi}{d} \rfloor \in \mathbf{Z}_p^*$ for all p. On the other hand, $d-1+b < p$ by our hypothesis and hence $(d-1+b)! \in \mathbf{Z}_p^*$ too. Hence $\kappa_{r,n,k} \in \mathbf{Z}_p^*$ for $p \ge b+d$.

(2) We first observe that $\psi_{r,i}(\lfloor\frac{p}{d}\rfloor) = i\lfloor\frac{p}{d}\rfloor + \lfloor\frac{ri}{d}\rfloor = \lfloor\frac{pi}{d}\rfloor$ (by writing $p = \lfloor\frac{p}{d}\rfloor d + r$). Secondly we notice that for all i, j

$$t_{ij} = \psi_{r,i}\left(\left\lfloor\frac{p}{d}\right\rfloor\right) - n_{ij}^{\ell_{ij}} = \left\lfloor\frac{pi}{d}\right\rfloor - n_{ij}^{\ell_{ij}}.$$

Thus we have

$$\left[\psi_{r,i}\left(\left\lfloor\frac{p}{d}\right\rfloor\right)\right]_{t_{i,\sigma(i)}} = \frac{\psi_{r,i}(\lfloor p/d\rfloor)!}{n_{i,\sigma(i)}^{\ell_{i,\sigma(i)}}!} = \frac{\lfloor pi/d\rfloor!}{n_{i,\sigma(i)}^{\ell_{i,\sigma(i)}}!}.$$

Therefore

$$\widetilde{h}_{r,n,k}\left(\left\lfloor\frac{p}{d}\right\rfloor\right) = \kappa_{r,n,k}\sum_{(\sigma,\ell_{i,\sigma(i)})\in\mathcal{S}(k)}\operatorname{sgn}(\sigma)\prod_{i=1}^{n}\frac{1}{m_{i,\sigma(i)}^{\ell_{i,\sigma(i)}}!n_{i\sigma(i)}^{\ell_{i,\sigma(i)}}!}$$

which proves our statement.

Since $n_{ij}^{\ell} < p$ by Lemma 2.3 and hence $n_{ij}^{\ell}!$ is in $\mathbf{Z}_p^*$. By Lemma 2.5 we have $\ell_{i,\sigma(i)} \leq \lfloor\frac{b}{d}\rfloor$ and hence $m_{ij}^{\ell} = m_{ij} + d\ell \leq d - 1 + d\lfloor\frac{b}{d}\rfloor < p$ for $p \geq d + b$ and it follows $m_{ij}^{\ell}! \in \mathbf{Z}_p^*$. Thus $\mu_{r,n,k} \in \mathbf{Z}_p$ for $p \geq d + b$. □

Proposition 2.9. *Fix r, n as above.*

(1) *Then $h_{r,n,k} \neq 0$ if and only if $\widetilde{h}_{r,n,k}^{o}(-\frac{r}{d}) \neq 0$.*
(2) *If $\widetilde{h}_{r,n,k}^{o}(\lfloor\frac{p}{d}\rfloor) \in \mathbf{Z}_p^*$ for all prime $p \equiv r \bmod d$ and $p > \max(d, \mathrm{MaxPrime}(h_{r,n,k}))$ then $\widetilde{h}_{r,n,k}^{o}(-\frac{r}{d}) \neq 0$. Conversely if $\widetilde{h}_{r,n,k}^{o}(-\frac{r}{d}) \neq 0$ for $p \equiv r \bmod d$ and $p > d$ then $\widetilde{h}_{r,n,k}^{o}(\lfloor\frac{p}{d}\rfloor) \in \mathbf{Z}_p^*$.*
(3) *For any prime $p \equiv r \bmod d$ and $p > d + k$ we have $\widetilde{h}_{r,n,k}^{o}(\lfloor\frac{p}{d}\rfloor) \in \mathbf{Z}_p^*$ if and only if $\mu_{r,n,k} \in \mathbf{Z}_p^*$.*
(4) *If $h_{r,n,k} \neq 0$ then $k \geq 0$ is the least such that $\mu_{r,n,k} \in \mathbf{Z}_p^*$ for all prime $p \equiv r \bmod d$ and $p > d + k$. Conversely, if $k \geq 0$ is the least such that $\mu_{r,n,k} \in \mathbf{Z}_p^*$ for all prime $p \equiv r \bmod d$ and $p > \max(d + k, \mathrm{MaxPrime}(h_{r,n,k}))$ then we have $h_{r,n,k} \neq 0$.*

Proof. Part (1) follows from the definition of $h_{r,n,k}$. Part (2) follows from Lemma 2.2. Part (3) follows from Lemma 2.8: since for $p > d + k$ we have $\kappa_{r,n,k} \in \mathbf{Z}_p^*$ and by Lemma 2.8 $\mu_{r,n,k} = \widetilde{h}_{r,n,k}(\lfloor\frac{p}{d}\rfloor)/\kappa_{r,n,k}$, we have that $\widetilde{h}_{r,n,k}(\lfloor\frac{p}{d}\rfloor) \in \mathbf{Z}_p^*$ if and only if $\mu_{r,n,k} \in \mathbf{Z}_p^*$. It is clear that Part (4) follows from (1)–(3). □

3. Tame *A*-determinant

This section completely determines the p-adic order of certain finite *tame* A-determinant, whose expansion is a polynomial in variable A (remark: this variable A parameterizes the coefficient a in the family of polynomials $x^d + ax^s$). These tame A-determinants will be used to approximate our Fredholm A-determinant in Section 4. They are the bridge connecting the generating polynomials to the actually p-adic Fredholm determinant in Dwork theory.

Let $E_p(-)$ be the p-adic Artin–Hasse exponential function (see [Kob84, IV.2] or see [Sch84, Section 48]). We pick a root γ of $\log_p E_p(x) = \sum_{i=1}^{\infty} \frac{x^{p^i}}{p^i}$ in $\overline{\mathbf{Q}}_p$ of $\mathrm{ord}_p\gamma = 1/(p-1)$ such that $\zeta_p = E_p(\gamma)$ is the same primitive p-th root of unity as in the beginning and throughout of this paper. For any integer $pi-j$ with $1 \le i,j \le d-1$ we define a polynomial in $\mathbf{Q}[\gamma][A]$ for every $\ell^\bullet \in \mathbf{Z}_{\ge 0}$

$$F_{pi-j,\ell^\bullet}(A) := \sum_{\ell=0}^{\ell^\bullet} \frac{A^{m_{ij}^\ell}\gamma^{m_{ij}^\ell+n_{ij}^\ell}}{m_{ij}^\ell!n_{ij}^\ell!} \tag{9}$$

where m_{ij}^ℓ, n_{ij}^ℓ are defined as in Lemma 2.3(4). Define the n-th tame A-determinant

$$P_{n,\ell^\bullet}(A) := \det\bigl(\bigl(F_{pi-j,\ell^\bullet}(A)\bigr)_{1\le i,j\le n}\bigr). \tag{10}$$

It lies in $\mathbf{Q}[\gamma][A]$ and its key property is provided below in the lemma. Notice that $\mathbf{Z}_p[\gamma] = \mathbf{Z}_p[\zeta_p]$ is the ring of integers in $\mathbf{Q}_p(\gamma) = \mathbf{Q}_p(\zeta_p)$.

Lemma 3.1. *Let $1 \le n \le d-1$ and $b \in \mathbf{Z}_{\ge 0}$.*

(1) *Then $P_{n,\lfloor b/d\rfloor}(A)$ can be written as a polynomial in $\mathbf{Q}[A\gamma^{1-\frac{s}{d}}]$ whose terms are monomials in $A\gamma^{1-\frac{s}{d}}$. Furthermore, we have*

$$P_{n,\lfloor b/d\rfloor}(A) = \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{k_{r,n}^\bullet \le k \le k_{r,n}^\bullet + b} \mu_{r,n,k}\bigl(A\gamma^{1-\frac{s}{d}}\bigr)^k$$
$$+ \gamma^{> \frac{(p-1)n(n+1)}{2d} + (1-\frac{s}{d})(k_{r,n}^\bullet + b)} R$$

for some $R \in \mathbf{Z}_p[\gamma][A]$.

(2) *If $h_{r,n,k_{r,n}} \ne 0$ then for all $p \equiv r \bmod d$ and $p > \max(d + k_{r,n}, \mathrm{MaxPrime}(h_{r,n,k_{r,n}}))$*

$$\mathrm{ord}_p\bigl(P_{n,\lfloor b/d\rfloor}(A)\bigr) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

Conversely, if $\mathrm{ord}_p(P_{n,\lfloor b/d\rfloor}(A)) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}$ for $p > d + k_{r,n}$ then $h_{r,n,k_{r,n}} \ne 0$.

(3) *Let $a \in \overline{\mathbf{Q}}^*$ and let $\bar{a}$ be its residue reduction over p. Let $\widehat{a}$ be the Teichmüller lifting of $\bar{a}$. If $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ then for all prime $p \equiv r \bmod d$ and $p > \max(d + \max_n(k_{r,n}), \mathrm{MaxPrime}_n(h_{r,n,k_{r,n}}), \mathrm{MaxPrime}(a))$, we have for all n*

$$\mathrm{ord}_p\bigl(P_{n,\lfloor b/d\rfloor}(\widehat{a})\bigr) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

Conversely, if $\mathrm{ord}_p(P_{n,\lfloor b/d\rfloor}(\widehat{a})) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}$ *for all* n *and all prime* $p > \max(d + \max_n(k_{r,n}), \mathrm{MaxPrime}(a))$ *then* $H_r = \sum_{n=1}^{d-1} h_{r,n,k} X_{r,n}^{k_{r,n}}$.

Proof. (1) By the formal expansion of determinant and the above identity, we have

$$\begin{aligned} P_{n,\lfloor b/d\rfloor}(A) &= \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} F_{pi-\sigma(i),\lfloor b/d\rfloor} \\ &= \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} \sum_{\ell=0}^{\lfloor b/d\rfloor} \frac{A^{m^{\ell}_{i,\sigma(i)}} \gamma^{m^{\ell}_{i,\sigma(i)}+n^{\ell}_{i,\sigma(i)}}}{m^{\ell}_{i,\sigma(i)}! n^{\ell}_{i,\sigma(i)}!} \\ &= \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \sum_{0\le \ell_{i,\sigma(i)}\le\lfloor b/d\rfloor} \frac{A^{\sum_{i=1}^n m^{\ell_{i,\sigma(i)}}_{i,\sigma(i)}}}{\prod_{i=1}^n m^{\ell_{i,\sigma(i)}}_{i,\sigma(i)}! n^{\ell_{i,\sigma(i)}}_{i,\sigma(i)}!} \gamma^{\sum_{i=1}^n m^{\ell_{i,\sigma(i)}}_{i,\sigma(i)} + n^{\ell_{i,\sigma(i)}}_{i,\sigma(i)}}. \end{aligned}$$

Notice that by Lemma 2.3 for any $\ell_{i,\sigma(i)}$

$$d\sum_{i=1}^{n} n^{\ell_{i,\sigma(i)}}_{i,\sigma(i)} + s\sum_{i=1}^{n} m^{\ell_{i,\sigma(i)}}_{i,\sigma(i)} = (p-1)n(n+1)/2.$$

Write $k = \sum_{i=1}^n m^{\ell_{i,\sigma(i)}}_{i,\sigma(i)}$. Then

$$\sum_{i=1}^{n} m^{\ell_{i,\sigma(i)}}_{i,\sigma(i)} + n^{\ell_{i,\sigma(i)}}_{i,\sigma(i)} = \frac{(p-1)n(n+1)}{2d} + \left(1 - \frac{s}{d}\right)k.$$

Then there are $w_k \in \mathbf{Z}_p^*$ such that

$$\begin{aligned} P_{n,\lfloor b/d\rfloor}(A) &= \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{k^{\bullet}_{r,n}\le k\le k^{\bullet}_{r,n}+b} \mu_{r,n,k} A^k \gamma^{(1-\frac{s}{d})k} \\ &\quad + \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{k\ge k^{\bullet}_{r,n}+b} \sum_{\sigma\in S_n^k} \mathrm{sgn}(\sigma) w_k A^k \gamma^{(1-\frac{s}{d})k} \\ &= \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{k^{\bullet}_{r,n}\le k\le k^{\bullet}_{r,n}+b} \mu_{r,n,k} \left(A\gamma^{(1-\frac{s}{d})}\right)^k \\ &\quad + \gamma^{>\frac{(p-1)n(n+1)}{2d} + (1-\frac{s}{d})k_{r,n}} R \end{aligned}$$

for some $R \in \mathbf{Z}_p[\gamma][A]$.

(2) Fix n. By Proposition 2.9 our hypothesis implies $k_{r,n}$ is the least k such that $\mu_{r,n,k_{r,n}} \in \mathbf{Q} \cap \mathbf{Z}_p^*$ for $p \equiv r \bmod d$ and $p > \max(d + k_{r,n}, \mathrm{MaxPrime}(h_{r,n,k_{r,n}}))$. For all $k^{\bullet}_{r,n} \le k < k_{r,n}$ we have $\mu_{r,n,k_{r,n}} \in \mathbf{Q} \cap p\mathbf{Z}_p$. Hence $\mathrm{ord}_p \mu_{r,n,k_{r,n}} \ge 1$. Thus the p-adic valuations are precisely as displayed by our Part (1).

(3) Fix n. Since $a \neq 0$ we have for $p > \mathrm{MaxPrime}(a)$ then $\widehat{a} \in \overline{\mathbf{Z}}_p^*$. Consider the formula in Part (1)

$$P_{n,\lfloor b/d\rfloor}(\widehat{a}) = \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{k^\bullet_{r,n} \le k \le k^\bullet_{r,n}+b} \mu_{r,n,k}\widehat{a}^k \gamma^{(1-\frac{s}{d})k} + (\text{higher } \gamma\text{-terms}).$$

Then applying an analogous argument of Part (2) we conclude that $k_{r,n}$ is the least positive integer such that $h_{r,n,k_{r,n}} \neq 0$ if and only if $k_{r,n}$ is the least k such that $\mu_{r,n,k}\widehat{a}^k \in \overline{\mathbf{Z}}_p^*$; and hence it is equivalent to

$$\mathrm{ord}_p P_{n,\lfloor b/d\rfloor}(\widehat{a}) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

This proves our statements. $\square$

4. Asymptotic Dwork theory for A-families

In this section we approximate Fredholm A-determinant by those tame determinants defined in Section 3. To keep the paper short we refer the reader to [AS89,Wan93,Wan04] for more thorough treatment of classical Dwork theorem. Let $f(x) = x^d + ax^s$ be a polynomial with $a \in \overline{\mathbf{Q}}$ and $d > s \ge 1$ are coprime integers. Namely, $f(x) \in \mathbf{A}(s,d)(\overline{\mathbf{Q}})$. Let $\bar{a}$ be the reduction mod $\wp$ of a for a prime ideal $\wp$ in the number field $\mathbf{Q}(a)$ lying over p. Let $\widehat{a}$ be the p-adic Teichmüller lifting of $\bar{a}$ in $\overline{\mathbf{Z}}_p$. We recall the Dwork trace formula for the L function of exponential sum of $\overline{f} = f(x) \bmod \wp$, assuming $\wp$ has residue field $\mathbf{F}_q$ for some p-power q. Let ζ_p be the primitive p-th root of unity fixed from the beginning and throughout this paper. Let $\gamma \in \overline{\mathbf{Q}}_p$ be the root of $\log_p E_p(x) = \sum_{i=0}^\infty \frac{x^{p^i}}{p^i}$ with $\mathrm{ord}_p(\gamma) = 1/(p-1)$ such that $E_p(\gamma) = \zeta_p$ (just as in the beginning of Section 3 above). Write $E_p(\gamma X) = \sum_{t=0}^\infty \lambda_t X^t$ for some $\lambda_t \in (\mathbf{Q} \cap \mathbf{Z}_p)[\gamma]$. Then we have $\lambda_t = \gamma^t/t!$ for all $0 \le t \le p-1$, and $\mathrm{ord}_p\lambda_t \ge t/(p-1)$ for all $t \ge 0$. For any integer $v \ge 0$ let

$$F'_v(A) := \sum_{n_v,m_v} \lambda_{n_v}\lambda_{m_v} A^{m_v} \tag{11}$$

where the sum ranges over $m_v, n_v \in \mathbf{Z}_{\ge 0}$ such that $n_v d + m_v s = v$. For the only situation we are studying in this paper $v = pi - j$ with $1 \le i, j \le d-1$ we use the notation from Lemma 2.3 that is, $m_{pi-j} = m_{ij}^\ell$ and $n_{pi-j} = n_{ij}^\ell$ for some ℓ.

From now on we assume $p > s(d-1)$ (so as to apply Lemma 2.3). Recall from (9), for $b \in \mathbf{Z}_{\ge 0}$

$$F_{pi-j,\lfloor b/d\rfloor}(A) = \sum_{\ell=0}^{\lfloor b/d\rfloor} \frac{A^{m_{ij}^\ell}\gamma^{m_{ij}^\ell + n_{ij}^\ell}}{m_{ij}^\ell! n_{ij}^\ell!}.$$

Then we have

$$\begin{aligned} F'_{pi-j}(A) &= \sum_{\ell \ge 0} u_{i,j,\ell} A^{m_{ij}^\ell} \gamma^{m_{ij}^\ell + n_{ij}^\ell} \\ &= F_{pi-j,\lfloor b/d \rfloor}(A) + \sum_{\ell > \lfloor b/d \rfloor} u_{i,j,\ell} A^{m_{ij}^\ell} \gamma^{m_{ij}^\ell + n_{ij}^\ell} \end{aligned}$$

for some $u_{i,j,\ell} \in \mathbf{Z}_p[\gamma]$ which is equal to $\frac{1}{m_{ij}^\ell ! n_{ij}^\ell !}$ when $\ell \le \lfloor b/d \rfloor$. Let $P_{n,\lfloor b/d \rfloor}(A) = \det(F_{pi-j,\lfloor b/d \rfloor}(A))_{1 \le i,j \le n}$ for all $1 \le n \le d-1$. We show below that $P_{n,\lfloor b/d \rfloor}(A)$ approximates $P'_n(A) := \det(F'_{pi-j})_{1 \le i,j \le n}$ up to b terms p-adically.

Lemma 4.1. *Let $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ be defined in (8).*

(1) *We write $N_r := \max(s(d-1), d + \max_n(k_{r,n}), \mathrm{MaxPrime}_n(h_{r,n,k_{r,n}}))$, then for all n and for all prime $p \equiv r \bmod d$ with $p > N_r$ we have*

$$\mathrm{ord}_p\big(P'_n(A)\big) = \mathrm{ord}_p\big(P_{n,\lfloor b/d \rfloor}(A)\big) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

Conversely, if $\mathrm{ord}_p(P'_n(A)) = \mathrm{ord}_p(P_{n,\lfloor b/d \rfloor}(A)) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}$ for all n and all prime $p > \max(s(d-1), d+\max_n(k_{r,n}))$ then we have $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$.

(2) *Let $a \in \overline{\mathbf{Q}}^*$ and let $\bar{a}$ be its residue reduction over p. Let $\widehat{a}$ be the Teichmüller lifting of $\bar{a}$. If $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ then for all prime $p \equiv r \bmod d$ and $p > \max(N_r, \mathrm{MaxPrime}(a))$ for all $1 \le n \le d-1$ we have*

$$\mathrm{ord}_p\big(P'_n(\widehat{a})\big) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

Conversely, if for all $1 \le n \le d-1$ and all prime $p \equiv r \bmod d$ and $p > \max(s(d-1), d + \max_n(k_{r,n}), \mathrm{MaxPrime}(a))$ we have $\mathrm{ord}_p(P'_n(\widehat{a})) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}$ then the generating function is of the form $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$.

Proof. (1) Let $1 \le i,j \le d-1$. Let $p > s(d-1)$. Then we have for some $u_{i,\sigma(i),\ell} \in \mathbf{Z}_p$ that

$$P'_n(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^n \sum_{\ell=0}^\infty u_{i,\sigma(i),\ell} A^{m_{i,\sigma(i)}^\ell} \gamma^{m_{i,\sigma(i)}^\ell + n_{i,\sigma(i)}^\ell}.$$

Using the same computational argument as that of Lemma 3.1 we get

$$\begin{aligned} P'_n(A) = {} & \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{k_{r,n}^\bullet \le k \le k_{r,n}^\bullet + b} \Bigg(\sum_{(\sigma, \ell_{i,\sigma(i)}) \in \mathcal{S}(k)} \frac{\mathrm{sgn}(\sigma) A^k}{\prod_{i=1}^n m_{i,\sigma(i)}^{\ell_{i,\sigma(i)}} ! n_{i,\sigma(i)}^{\ell_{i,\sigma(i)}} !} \Bigg) \gamma^{(1-\frac{s}{d})k} \\ & + \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{k > k_{r,n}^\bullet + b} \sum_{(\sigma, \ell_{i,\sigma(i)}) \in \mathcal{S}(k)} \mathrm{sgn}(\sigma) w_k A^k \gamma^{(1-\frac{s}{d})k} \end{aligned}$$

for some $w_k \in \mathbf{Z}_p[\gamma]$. By Lemma 2.8 we can write

$$P'_n(A) = \gamma^{\frac{(p-1)n(n+1)}{2d}} \sum_{0 \le k - k^\bullet_{r,n} \le b} \mu_{r,n,k} A^k \gamma^{(1-\frac{s}{d})k} + \gamma^{> \frac{(p-1)n(n+1)}{2d} + (1-\frac{s}{d})(k^\bullet_{r,n}+b)} R$$

for some $R \in \mathbf{Z}_p[\gamma][A]$. Since $k_{r,n}$ is the minimal k with $\widetilde{h}_{r,n,k}(-\frac{r}{d}) \neq 0$ and $0 \le k - k^\bullet_{r,n} < b$. By Proposition 2.9 for $p \equiv r \bmod d$ with $p > \max(d + \max_n(k_{r,n}), \mathrm{MaxPrime}_n(h_{r,n,k_{r,n}}))$ we have $\mu_{r,n,k} \in \mathbf{Z}_p^*$ and hence

$$\mathrm{ord}_p\big(P'_n(A)\big) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

Comparing with Lemma 3.1

$$\mathrm{ord}_p\big(P_{n,\lfloor b/d \rfloor}(A)\big) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

The converse direction follows by applying Proposition 2.9 again with analogous argument as that of Lemma 3.1.

(2) The proof here is analog to that of Lemma 3.1 by using Proposition 2.9 and applying the extra condition that $p > s(d-1)$ on top of both directions. □

Then we prove Theorem 1.1 below by applying the p-adic Dwork theory and transform theorem we developed in [Zhu12].

Theorem 4.2 *(Theorem 1.1). Let $s < d$ be two coprime positive integers. Let $2 \le r \le d-1$. Suppose $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ be as defined in (8) with $\prod_{n=1}^{d-1} h_{r,n,k_{r,n}} \neq 0$. Let $N_{s,d,r}$ be defined as in Theorem 1.1. Then for $p \equiv r \bmod d$ and $p > N_{s,d,r}$ we have $\mathrm{GNP}(\mathbf{A}(s,d), \overline{\mathbf{F}}_p)$ with breaking points after origin at*

$$\left(\left(n, \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}\right)\right)_{n=1,\ldots,d-1}. \tag{12}$$

Conversely, suppose for all prime $p \equiv r \bmod d$ and $p > \max(s(d-1), d + \max_n(k_{r,n}), 2(d-s)\max_n(k_{r,n}))$, $\mathrm{GNP}(\mathbf{A}(s,d), \overline{\mathbf{F}}_p)$ has its breaking points as above in (12), then H_r has to be of the form $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$.

Given $f = x^d + ax^s \in \mathbf{A}(s,d)(\overline{\mathbf{Q}})$ with $\overline{f} = x^d + \bar{a}x^s \in \mathbf{A}(s,d)(\mathbf{F}_q)$. If $a \in \overline{\mathbf{Q}}^*$, then for all prime $p \equiv r \bmod d$ and $p > \max(N_{s,d,r}, \mathrm{MaxPrime}(a))$ we have

$$\mathrm{NP}(\overline{f}) = \mathrm{GNP}\big(\mathbf{A}(s,d), \overline{\mathbf{F}}_p\big)$$

and

$$\lim_{p\equiv r \bmod d} \mathrm{NP}(\overline{f}) = \mathrm{HP}\big(\mathbf{A}(s,d)\big).$$

Proof. Let $a \neq 0$. We define a twisted matrix $M'' := (F''_{pi-j}) := (F'_{pi-j}\gamma^{\frac{j-i}{d}})$, notice this is the matrix representing the Dwork operator with respect to a weighted monomial basis. For $q = p^c$ for write

$$\big(M''/\mathbf{F}_q\big)(A) := M'' \cdot M''^{\tau^{-1}} \cdot M''^{\tau^{-2}} \cdot \cdots \cdot M''^{\tau^{-(c-1)}}$$

where τ is the Frobenius map on $\mathbf{Q}_q(\zeta_p)$ that fixes $\mathbf{Q}_p(\zeta_p)$ that lifts the Frobenius map $x \mapsto x^p$ over its residue field extension, and $\tau(A) = A^p$. Then Dwork theory states that

$$L(\overline{f}/\mathbf{F}_q, T) = \frac{\det(1 - T(M''/\mathbf{F}_q)(\widehat{a}))}{\det(1 - qT(M''/\mathbf{F}_q)(\widehat{a}))} \tag{13}$$

and it is of the form $1 + C_1T + \cdots + C_{d-1}T^{d-1}$ in $\mathbf{Z}[\zeta_p][T]$.

Since $\mathrm{ord}_p(F'_{pi-j}(\widehat{a})) \geq \frac{\lceil \frac{pi-j}{d} \rceil}{p-1}$ by its definition, we have

$$\mathrm{ord}_p\big(F''_{pi-j}(\widehat{a})\big) \geq \frac{i}{d}.$$

Write $P''_n := \det((M'')^{[n]})$, i.e., the first n by n submatrix of M''. Obviously $P''_n(\widehat{a}) = P'_n(\widehat{a})$ since M'' is the result of a simple change of basis for M'. Apply Lemma 4.1, we have that for $p \equiv r \bmod d$ and $p > \max(N_r, \mathrm{MaxPrime}(a))$ and for all $1 \leq n \leq d-1$

$$\mathrm{ord}_p\big(P'_n(\widehat{a})\big) = \mathrm{ord}_p\big(P_{n,\lfloor b/d \rfloor}(\widehat{a})\big) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

In summary, we have

$$\mathrm{ord}_p P''_n(\widehat{a}) = \mathrm{ord}_p P'_n(\widehat{a}) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}. \tag{14}$$

Thus for $p > 2(d-s)k_{r,n} + 1$ we have

$$\sum_{i=1}^{n} \frac{i}{d} = \frac{n(n+1)}{2d} \leq \mathrm{ord}_p P''_n(\widehat{a}) < \frac{n(n+1)+1}{2d}.$$

This verifies that the hypothesis of the transform theorem in Section 5 of [Zhu12] is satisfied, hence we are enabled to conclude that

$$\mathrm{NP}(\overline{f}) = \mathrm{NP}_p\left(\sum_{n=0}^{d-1} P''_n(\widehat{a})T^n\right)$$

and by (14) its breaking points after the origin are given by

$$\big(n, \mathrm{ord}_p P_n''(\widehat{a})\big) = \left(n, \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}\right)$$

for $n = 1, \ldots, d-1$.

Conversely, suppose we know for such prime $p \equiv r \bmod d$ the breaking points of $\mathrm{GNP}(\mathbf{A}(s,d), \overline{\mathbf{F}}_p)$ are as given. Then we may apply the transform theorem of [Zhu12] and conclude that it is equal to $\mathrm{NP}_p(\sum_{n=0}^{d-1} P_n''(\widehat{a})T^n)$, or in other words for all $1 \le n \le d-1$ we have

$$\mathrm{ord}_p P_n''(\widehat{a}) = \frac{n(n+1)}{2d} + \frac{(1-\frac{s}{d})k_{r,n}}{p-1}.$$

Then we apply Lemma 4.1 and find that H_r is of the given form.

The last statement follows by taking limit since by our hypothesis $k_{r,n}$ is independent of p. □

Corollary 4.3. *Let notation be as in Theorem 4.2. Assume Conjecture 2.7 holds (i.e., suppose $H_r = \sum_{n=1}^{d-1} h_{r,n,k_{r,n}} X_{r,n}^{k_{r,n}}$ with $\prod_{n=1}^{d-1} h_{r,n,k_{r,n}} \neq 0$). Let $f = x^d + ax^s \in \mathbf{A}(s,d)(\overline{\mathbf{Q}})$ with $d > s \ge 1$ coprime. Then for all prime $p > \max_r(N_{s,d,r}, \mathrm{MaxPrime}(a))$ we have that*

$$\mathrm{NP}(\overline{f}) = \mathrm{GNP}\big(\mathbf{A}(s,d); \overline{\mathbf{F}}_p\big) \tag{15}$$

and $\lim_{p\to\infty} \mathrm{NP}(\overline{f}) = \mathrm{HP}(\mathbf{A}(s,d))$ if and only if $a \neq 0$.

Proof. Suppose $a \neq 0$ then the statement follows from Theorem 4.2. If $a = 0$ then $f = x^d$ and $\mathrm{NP}(\overline{f})$ is explicitly worked out by Stickelberger theorem (see [Wan04]). For $p \equiv 1 \bmod d$ we have $\mathrm{NP}(\overline{f}) = \mathrm{HP}(\mathbf{A}(s,d))$ but for $2 \le r \le d-1$ we know $\mathrm{NP}(\overline{f})$ lies strictly above $\mathrm{GNP}(\mathbf{A}(s,d), \overline{\mathbf{F}}_p)$. Hence $\lim_{p\to\infty} \mathrm{NP}(\overline{f})$ does not exist. □

For any $s < d$ coprime integers and for any $q = p^c$ ($c \in \mathbf{Z}_{\ge 1}$), define

$$\mathrm{GNP}\big(\mathbf{A}(s,d), \mathbf{F}_q\big) := \inf_{\overline{f} \in \mathbf{A}(s,d)(\mathbf{F}_q)} \mathrm{NP}(\overline{f})$$

if exists. Grothendieck–Katz specialization theorem implies that $\mathrm{GNP}(\mathbf{A}(s,d), \overline{\mathbf{F}}_p)$ exists. Our proof of the main theorem implies the following statement immediately.

Corollary 4.4. *Let notation be as in Theorem 1.1. Assume Conjecture 2.7 holds. For p large enough, $\mathrm{GNP}(\mathbf{A}(s,d), \mathbf{F}_q)$ exists for any p-power q and we have*

$$\mathrm{GNP}\big(\mathbf{A}(s,d), \mathbf{F}_q\big) = \mathrm{GNP}\big(\mathbf{A}(s,d), \overline{\mathbf{F}}_p\big).$$

Remark 4.5. The computation of H_r starts with smallest $k \geq k^{\bullet}_{r,n}$ and increases until we find the next term with $h_{r,n,k} \neq 0$. When $s = 1$ we have $H_r = \sum_{n=1}^{d-1} h_{r,n,k^{\bullet}_{r,n}} X_{r,n}^{k^{\bullet}_{r,n}}$ (it is shown in [Zhu03]) with $\prod_{n=1}^{d-1} k^{\bullet}_{r,n} \neq 0$. But for $s \geq 2$ it is not always true that $H_r = \sum_{n=1}^{d-1} h_{r,n,k^{\bullet}_{r,n}} X_{r,n}^{k^{\bullet}_{r,n}}$. In fact in the case $(s, d) = (2, 5)$ and $r = 3$ one can show directly that H_3 has its least degree monomial of strictly higher degree then $k^{\bullet}_{r,n}$ for at least one n with $1 \leq n \leq d - 2$.

Acknowledgments

We are very grateful to the referee for careful reading and many helpful comments. Research in this paper was partially supported by NSA mathematical science research grant 1094132-1-57192.

References

[AS89] Alan Adolphson, Steve Sperber, Exponential sums and Newton polyhedra: cohomology and estimates, Ann. of Math. 130 (1989) 367–406.

[Bla11] Regis Blache, Valuation of exponential sums and the generic first slope for Artin–Schreier curves, J. Number Theory 132 (10) (2012) 2336–2352.

[BFZ08] Regis Blache, Eric Ferard, Hui June Zhu, Hodge–Stickelberger polygons for L-functions of exponential sums of $P(x^s)$, Math. Res. Lett. 15 (5) (September 2008) 1053–1071.

[Katz] Nicholas Katz, Sommes exponentielles, Astérisque 79 (1980).

[Kob84] Neal Koblitz, p-Adic Numbers, p-Adic Analysis and Zeta-Functions, Grad. Texts in Math., vol. 58, Springer-Verlag, 1984.

[LW09] Chunlei Liu, Daqing Wan, T-adic exponential sums over finite fields, Algebra Number Theory 3 (5) (2009) 489–509.

[Ram05] J.L. Ramírez Alfonsín, The Diophantine Frobenius Problem, Oxford Lecture Ser. Math. Appl., vol. 30, Oxford University Press, 2005.

[Sch84] W.H. Schikhof, Ultrametric Calculus: An Introduction to p-Adic Analysis, Cambridge Stud. Adv. Math., vol. 4, Cambridge University Press, 1984.

[Wan93] Daqing Wan, Newton polygons and zeta functions and L functions, Ann. of Math. 37 (1993) 249–293.

[Wan04] Daqing Wan, Variations of p-adic L functions for exponential sums, Asian J. Math. 8 (2004) 427–470.

[Yan03] Roger Yang, Newton polygons of L-functions of polynomials of the form $x^d + \lambda x$, Finite Fields Appl. 9 (1) (2003) 59–88.

[Zhu03] Hui June Zhu, p-Adic variation of L functions of one variable exponential sums, Amer. J. Math. 125 (2003) 669–690.

[Zhu04] Hui June Zhu, Asymptotic variation of L functions of one-variable exponential sums, J. Reine Angew. Math. 572 (2004) 219–233.

[Zhu12] Hui June Zhu, Asymptotic variations of L-functions of exponential sums, preprint, arXiv:1211.5875.