COMPOSITIO MATHEMATICA

S. SPERBER

Congruence properties of the hyperkloosterman sum

Compositio Mathematica, tome 40, nº 1 (1980), p. 3-33

<http://www.numdam.org/item?id=CM_1980__40_1_3_0>

COMPOSITIO MATHEMATICA, Vol. 40, Fasc. 1, 1980, pag. 3–33

CONGRUENCE PROPERTIES OF THE HYPERKLOOSTERMAN SUM

S. Sperber

Abstract

The article treats p-adically the n-variable Kloosterman exponential sum defined over a finite field of q $(=p^a)$ elements using the method of Dwork. The sum has been treated ℓ-adically $(\ell \neq p)$ by P. Deligne [SGA $4\frac{1}{2}$, Lecture Notes in Mathematics 569, "Applications de la Formule des Traces aux Sommes Trigonométriques", 168–232, Springer-Verlag, Berlin 1977]. New proofs are given for some of Deligne's results, in particular for the functional equation of the associated L-function. The main result is the determination of the Newton polygon of the L-function: if $p \geq n+3$ and if $\{\gamma_i\}_{i=1}^{n+1}$ are the eigenvalues of Frobenius, then their order may be arranged so that ord $\gamma_i = a(i-1)$. In addition, it is proved that an excellent (Tate-Deligne) lifting of Frobenius does not generally exist in the hyperkloosterman example.

0. Introduction

After proving the Riemann hypothesis for curves, Weil [12] applied this result to certain exponential sums in one variable over a finite field, among them the Kloosterman sum, obtaining precise estimates for their absolute value. Recently, Deligne applied his generalization of the Weil result [1] to exponential sums in several variables, treating [2] the hyperkloosterman exponential sum

0010-437X/80/01/0003-32 $00.20/0

$$S_m(f_a) = \sum \psi_m\left(x_1 + \cdots + x_n + \frac{a}{x_1 \cdots x_n}\right) \tag{0.1}$$

(where a belongs to $\mathbb{F}_q$, the finite field with q elements, $\psi_m\colon \mathbb{F}_{q^m} \to \mathbb{C}^*$ is an additive character, and the sum ranges over all elements $(x_1, \ldots, x_n) \in (\mathbb{F}_{q^m}^*)^n$). Using ℓ-adic methods he derived the archimedean estimate $|S_m(f_a)| \leq (n+1)q^{nm/2}$, the eigenvalues of Frobenius $\{\gamma_i\}_{i=1}^{n+1}$ and their conjugates all having complex magnitude $q^{n/2}$. Dwork, in [7], examined the congruence properties of the Kloosterman sums (i.e. $n = 1$ in (0.1)), proving that the eigenvalues of Frobenius may be arranged so that $\operatorname{ord}_q \gamma_1 = 0$, and $\operatorname{ord}_q \gamma_2 = 1$ (where ord_q is the valuation normalized so that $\operatorname{ord}_q q = 1$). The present paper complements Deligne's work [2] and generalizes Dwork's result [7]. We treat the hyperkloosterman exponential sums p-adically.

In a previous article [11], making use of Erdelyi's integral representation formula [8] for the hypergeometric functions ${}_0F_n(1, \ldots, 1; x) = \sum_{j=0}^{\infty} (x^j/(j!))^{n+1}$, we constructed Dwork-type cohomology spaces $\mathfrak{W}_x$ having dimension $n+1$ over Ω, an algebraically closed extension of $\bar{\mathbb{Q}}_p$, having an inverse-Frobenius action: $\bar{\alpha}_x\colon \mathfrak{W}_x \to \mathfrak{W}_{x^p}$. By studying the dual spaces $\mathfrak{N}_x$, we obtained sharp p-adic estimates for the norm of the Frobenius action. Dwork's deformation equation in this case is the hypergeometric differential equation,

$$\delta^{n+1}u - xu = 0, \quad \left(\delta = x\frac{\mathrm{d}}{\mathrm{d}x}\right). \tag{0.2}$$

This equation, like the Bessel equation studied in [7], has an irregular singular point at ∞. In the cases arising in algebraic geometry from a parametrized family of projective hypersurfaces, the deformation equation has only regular singular points. Hence [11], like [7] earlier, extends the domain of definition for p-adic cohomology.

We also examined in [11] the Frobenius action on the solution space of this differential equation at the origin and at infinity using the classical solutions at regular and irregular singular points. The study at the origin, a regular singular point, yielded the result [11(4.2.14)] that for $p \neq 2$, the determinant of the matrix of the Frobenius map $\bar{\alpha}_x$ is $p^{n(n+1)/2}$ for x in Ω satisfying $\operatorname{ord} x > -(n+1)[(p-1)/p^2]$. This result carries important arithmetic information. At a Teichmuller lifting $z = z^q$ of $a \in \mathbb{F}_q$ ($q = p^r$), the Frobenius action $\mathfrak{B}_z(\bar{\alpha}) = \bar{\alpha}_{z^{p^{r-1}}} \cdots \bar{\alpha}_{z^p} \circ \bar{\alpha}_z$ is linear on $\mathfrak{W}_z$ and eigenvalues $\{\gamma_i\}_{i=1}^{n+1}$ are related (via Dwork's theory) to the hyperkloosterman exponential sum by

$$S_m(f_a) = (-1)^n\{\gamma_1^m + \gamma_2^m + \cdots + \gamma_{n+1}^m\} \tag{0.3}$$

In fact, if we form the L-function associated with the hyperkloosterman sum,

$$L(f_a, t) = \exp\Big(\sum_{m=1}^{\infty} \frac{S_m(f_a)}{m} t^m\Big),$$

then

$$L(f_a, t)^{(-1)^{n+1}} = \det(I - tB_z(\bar{\alpha})) \tag{0.4}$$

Hence, the result [11(4.2.14)] on the determinant of the Frobenius matrix implies that for $p \neq 2$,

$$\prod_{i=1}^{n+1} \gamma_i = q^{n(n+1)/2}. \tag{0.5}$$

Deligne, using ℓ-adic etale cohomology, has derived this result with no restrictions on p. As a consequence, since the eigenvalues are known to be algebraic integers, they are ℓ-adic units for $\ell \neq p$. The present article handles the remaining case $\ell = p$, determining the p-adic absolute values of the eigenvalues $\{\gamma_i\}_{i=1}^{n+1}$. The main result is Theorem (2.35). This result shows that the Newton polygon for $\det(I - tB_z(\bar{\alpha}))$ assumes its known lower bound, [11(2.5.11)]. (We remark that corollary (2.5.11) of [11] which gives this lower bound should have been stated, in the language of this introduction, as follows: if $p \geq n+3$, $z = z^q$ a Techmuller lifting of $a \in \mathbf{F}_q$, then the Newton polygon of $\det(I - tB_z(\alpha))$ (using ord_q as the normalized valuation) is contained in the convex closure of the set of points $\{(j, j(j-1)/2\}_{j=0}^{n+1}$.) By an elementary algebraic argument due to Dwork, the theorem is a corollary of Proposition (2.1) which uses the estimates for the norm of the Frobenius map derived in [11] in an essential way.

In addition to the main result, we give in §1 a p-adic proof for the functional equation for $L(f_a, t)$. The proof uses the information provided by our study [11(§5)] of the classical normal solutions at an irregular singular point. Finally, in the last section we show (3.23) that unlike the case of the Bessel equation [7], an excellent (Tate-Deligne) lifting does not exist for $n > 1$ (assuming $p \geq n + 8$).

We will use some of the familiar notation of p-adic analysis. Let Ω be a complete, algebraically closed field of characteristic zero with a non-archimedean valuation normalized so that (unless otherwise

specified) ord $p = 1$. It will be convenient to assume that Ω contains a generic unit t, i.e., a unit whose reduction in the residue class field is transcendental over $\mathbf{F}_p$. It has the important property that for $f(x)$ a polynomial with coefficients algebraic over $\mathbf{Q}_p$,

$$|f(t)| = \sup|f(x)|,$$

where the supremum runs over $x \in D(0, 1^+)$. We are here using the notation

$$D(a, r^-) = \{x \in \Omega \,|\, |x - a| < r\},$$
$$D(a, r^+) = \{x \in \Omega \,|\, |x - a| \leq r\}.$$

We will mean by $D(a, r)$ either of the two above disks. Finally, we note that we will often use the notation, $\mathrm{diag}(a_1, \ldots, a_n)$, to denote the $n \times n$ diagonal matrix with diagonal entries $\{a_1, \ldots, a_n\}$ in that order. As usual π will denote a fixed determination of $(-p)^{1/p-1}$ in Ω.

We thank F. Baldassarri and I. Berkes for several helpful discussions, S. Shatz and W. Messing for their help and encouragement, and B. Dwork for his generous and invaluable assistance.

It is convenient to recapitulate some of the results of [11] which will be useful in the following. We always assume throughout this paper that p denotes an odd prime. Let $b = (p-1)/p$, $b' = b/p$, $e = b - (1/(p-1))$. Define $L(x; b) = \bigcup_{c \in \mathbf{R}} L(x; b, c)$, where

$$L(x; b, c) = \Big\{ \sum_{\alpha \in \mathbf{Z}^n} c(\alpha) t^\alpha \;\Big|\; c(\alpha) \in \Omega,$$
$$\text{ord } c(\alpha) \geq c + b\Sigma(\alpha) + s(\alpha)((n+1)b + \text{ord } x) \Big\}, \quad [11(3.1.1)]$$

(where for $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbf{Z}^n$, $t^\alpha = t_1^{\alpha_1} t_2^{\alpha_2} \cdots t_n^{\alpha_n}$, $\Sigma(\alpha) = \Sigma_{i=1}^n \alpha_i$, and $s(\alpha) = \max\{0, -\alpha_1, -\alpha_2, \ldots, -\alpha_n\}$).

If we define

$$D_{i,x} = t_i \frac{\partial}{\partial t_i} + \pi\left(t_i - \frac{x}{t_1 t_2 \cdots t_n}\right), \quad [11(3.1.3)]$$

then the quotient space $\mathfrak{W}_x = L(x; b)/\Sigma_{i=1}^n D_{i,x} L(x; b)$ is an $(n+1)$-dimensional vector space over Ω with basis $\{(\pi t_1)^i\}_{i=0}^n$, provided ord $x > -(n+1)b$. A linear map (Frobenius) $\tilde{\alpha}_x : \mathfrak{W}_x \to \mathfrak{W}_{x^p}$ is constructed as follows: on the chain level (i.e. on $L(x; b)$), define $\alpha_x = \psi \circ F(x, t)$ where $F(x, t) = \hat{F}(x, t)/\hat{F}(x^p, t^p)$, $\hat{F}(x, t) =$

exp $\pi(t_1+\cdots+t_n+x/t_1t_2\cdots t_n)$, and ψ is linear and defined on monomials by

$$\psi(t^\alpha)=\begin{cases}t^{\alpha/p}, & \text{if } p/\alpha_i, \text{ all } i,\\ 0, & \text{otherwise.}\end{cases}$$

If we define

$$\theta(t)=\exp \pi(t-t^p)=\sum_{m=0}^{\infty} B_m t^m, \tag{0.6}$$

then [3(§4)]

$$\text{ord } B_m \geq mb', \tag{0.7a}$$

and for $0\leq m<p^2$ the stronger estimates

$$\text{ord } B_m \geq \frac{m}{p-1} \tag{0.7b}$$

are valid. If we write

$$F(x,t)=\sum_{\alpha\in Z^n} F(\alpha)t^\alpha,$$

then by definition

$$F(\alpha)=\sum_{\nu\geq s(\alpha)} B_{\alpha_1+\nu}B_{\alpha_2+\nu}\cdots B_{\alpha_n+\nu}B_\nu x^\nu. \tag{0.8}$$

To obtain precise estimates for the norm of $\bar{\alpha}_x$, we constructed the dual space $\mathfrak{R}_x$ of $\mathfrak{W}_x$ with basis $\{\xi^*_{i,x}\}_{i=0}^n$ dual to $\{\pi t_1^i\}_{i=0}^n$ under a pairing defined so that in terms of the Kronecker delta,

$$\delta_{ij}=\langle \pi t_1^j, \xi^*_{i,x}\rangle = \text{coefficient of } t^0 \text{ in } \pi t_1^j\cdot \xi^*_{i,x}. \tag{0.9}$$

Furthermore, we constructed a dual map $\alpha_x^*\colon \mathfrak{R}_{x^p}\to\mathfrak{R}_x$ whose matrix with respect to the dual basis is the transpose of the matrix of $\bar{\alpha}_x$ taken with respect to the bases $\{\pi t_1^i\}_{i=0}^n$ of $\mathfrak{W}_x$ and $\mathfrak{W}_{x^p}$. We may write $\xi^*_{i,x}=\Sigma\, b^{(i)}(\alpha)x^\gamma t^\alpha$ where the sum runs over $(\gamma;\alpha)\in Z^{n+1}$ satisfying $\gamma=s^*(\alpha)$ where by definition $s^*(\alpha)=\min\{0,-\alpha_1,\ldots,-\alpha_n\}$ and the coefficients $b^{(i)}(\alpha)\in\Omega$ satisfy

$$\text{(0.10)} \qquad \operatorname{ord} b^{(i)}(\alpha) \geq \min\left\{\left(\frac{-\Sigma(\alpha)}{n+1} - s^*(\alpha)\right)\operatorname{ord} x, \right.$$
$$\left. \frac{\Sigma(\alpha) + (n+1)s^*(\alpha)}{p-1}\right\}. \qquad [11(2.2.6)]$$

By use of the dual pairing, explicit formulas for the entries $\{A_{\lambda,k}\}_{\lambda,k=1}^{n+1}$ of the matrix A of α_x^* are computed: let $U_i \in Z^n$, $(1 \leq i \leq n)$, be the vector with 1 in the i^{th} position and 0 elsewhere, let $U = \Sigma_{i=1}^n U_i$, then

$$\text{(0.11)} \qquad A_{\lambda,k} = \pi^{k-1} \cdot b^{(\lambda-1)}(0)F(-(k-1)U_1)$$
$$+ \pi^{k-1} \sum_{i=1}^{n} \sum b^{(\lambda-1)}(\alpha)\Gamma_{i,k}^{(n)}(\alpha), \qquad [11(2.5.4)]$$

where the inner sum in the second term on the right side runs over $\alpha = -\Sigma_{\ell=1}^{i} j_\ell U_\ell$, $j_\ell \in \mathbb{N}$, ($\mathbb{N}$ denotes the set of positive integers), and

$$\Gamma_{i,k}^{(n)}(\alpha) = \binom{n}{i} x^{k-1} F(-p\alpha + (k-1)U) + \binom{n}{i-1} F(-p\alpha - (k-1)U_1).$$

Using these formulae, we deduced for $p \geq n+3$ and $\operatorname{ord} x > -(n+1)/p(p-1)$, the factorization

$$\text{(0.12)} \qquad A(x) = \operatorname{diag}(1, p, \ldots, p^n) \cdot \tilde{A}(x) \qquad [11(2.5.9)]$$

where $\tilde{A}(x)$ is a matrix with coefficients taking values in the integers $\mathcal{O}_\Omega$ for x in the given disk.

For x and z sufficiently close, a deformation isomorphism exists, $T_{x,z}: \mathfrak{W}_x \to \mathfrak{W}_z$. Viewing z as fixed and x as variable, and extending coefficients from Ω to the field of germs of meromorphic functions at z, we defined the connection ϵ so that the following diagram commutes:

$$\begin{array}{ccc} \mathfrak{W}_x & \xrightarrow{T_{x,z}} & \mathfrak{W}_z \\ {\scriptstyle\epsilon}\downarrow & & \downarrow{\scriptstyle x\frac{d}{dx}} \\ \mathfrak{W}_x & \xrightarrow{T_{x,z}} & \mathfrak{W}_z \end{array}$$

The horizontal sections of the connection satisfy a differential equation, Dwork's deformation equation, which was identified by Katz [9] (in the cases arising in geometry) as the classical Picard-Fuchs differential equation. After the change of bases

$$\text{(0.13)} \qquad (1, \epsilon^1(1), \ldots, \epsilon^n(1)) = V \cdot (1, \pi t_1, \ldots, (\pi t_1)^n), \qquad [11(3.2.15)]$$

this differential equation is just the hypergeometric differential equation, (0.2), which may be written in matrix form

$$xY' = YG \tag{0.14}$$ [11(4.1.1)]

where G is an $(n+1)\times(n+1)$ matrix of the form

$$G = \left(\begin{array}{c|c} 0 & \pi^{n+1}x \\ \hline I_n & 0 \end{array}\right) \tag{0.15}$$ [11(3.2.16)]

in which I_n denotes the $n \times n$ identity matrix. The change of basis matrix $V = (v_{ij})$ is lower triangular and has the properties: $v_{ii} = 1$ for all i, $v_{1j} = v_{j1} = 0$ for $j > 1$; and $v_{ij} = (j-1)v_{i-1,j} + v_{i-1,j-1}$, for $i, j > 1$. If we write $W = V^{-1}$ then [11(3.2.15)] $w_{ii} = 1$ for all i, and in all other cases

$$w_{ij} = (-1)^{i+j}E^{(j-2)}(i-2) \tag{0.16}$$ [11(2.2.12)]

where $E^{(k)}(r) = 0$ unless $0 \le k \le r$ and in this case $E^{(k)}(r)$ is the sum of all products taken $r-k$ at a time from $\{1, 2, \ldots, r\}$, i.e.

$$E^{(k)}(r) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le r} (r!/i_1 i_2 \cdots i_k).$$

Let $\mathscr{A}^t(x)$ be the Frobenius matrix with respect to the new bases $\{\epsilon^i(1)\}_{i=0}^n$ of $\mathfrak{W}_x$ and $\mathfrak{W}_{x^p}$. Let $\mathscr{A}(x) = (\mathscr{A}_{ij}(x))$. Then for $\operatorname{ord} x > -(n+1)b$, (and recalling $e = b - (1/(p-1))$,

$$\begin{aligned} &\operatorname{ord} \mathscr{A}_{11} = 0; \\ &\operatorname{ord} \mathscr{A}_{i1} \ge (i-1)e; \\ &\operatorname{ord} \mathscr{A}_{ij} \ge (i-1)e + \left(\frac{1}{p-1} - b'\right), \quad \text{for } i \ge 1, j > 1. \end{aligned} \tag{0.17}$$ [11(3.3.2)]

Furthermore, for $\operatorname{ord} x > -(n+1)/p(p-1)$, the factorization (0.12) holds here as well,

$$\mathscr{A}(x) = \operatorname{diag}(1, p, \ldots, p^n) \cdot \tilde{\mathscr{A}}(x), \tag{0.18}$$

where $\tilde{\mathscr{A}}(x)$ takes values in the integers for x in the given disk. At $x = 0$, for $\lambda > 1$,

$$\mathscr{A}_{\lambda 1}(0) = \sum_{i=1}^{\lambda-1} \binom{n+1}{i} \sum_{\alpha_1,\ldots,\alpha_i>0} (-1)^{\Sigma(\alpha)+\lambda-1} \pi^{-\Sigma(\alpha)} B_{p\alpha_1} B_{p\alpha_2} \cdots B_{p\alpha_i}$$

$$\times \sum_{d_1+d_2+\cdots+d_i=\lambda-i-1} E^{d_1}(\alpha_1-1)\cdots E^{d_i}(\alpha_i-1), \qquad \text{(0.19)} \quad [11(3.3.3)]$$

The Frobenius action extends to the solution space of the hypergeometric differential equation. Let $\mathscr{T}$ be the maximal unramified extension of $\mathbb{Q}_p$ in Ω. Let σ be the Frobenius automorphism of $\mathscr{T}$ over $\mathbb{Q}_p$, and we extend σ to $\mathscr{T}(\pi)$ by setting $\sigma(\pi) = \pi$. If a is a unit in $\mathscr{T}$ and Y is a fundamental solution matrix at a, then so is $Y^{\sigma\varphi}\mathscr{A}(x)$, where φ denotes the p-power map on the argument. Hence,

$$Y^{\sigma\varphi}\mathscr{A}(x) = MY \qquad \text{(0.20)} \quad [11(3.4.4)]$$

for a locally constant matrix M.

The classical solutions at $a = 0$ may be written,

$$Y(x) = x^H \cdot P(x), \qquad \text{(0.21)} \quad [11(4.2.1)]$$

where $P(x)$ is analytic in a neighborhood of 0, and $H = (H_{ij})$ is defined in terms of the Kronecker delta by $H_{ij} = \delta_{i-1,j}$. We may assume $P(x)$ normalized so that

$$P_{11}(x) = {}_0F_n(1,\ldots,1;\pi^{n+1}x) = \sum_{i=0}^{\infty} \frac{(\pi^{n+1}x)^i}{(i!)^{n+1}};$$

$$P_{i1}(0) = 0, \quad \text{for } i > 1. \qquad \text{(0.22)} \quad [11(4.2.7)]$$

Furthermore,

$$Y_{-\pi}\mathscr{A}(x) = x^H P((-1)^{n+1}x) \qquad \text{(0.23)} \quad [11(4.2.3)]$$

is a fundamental solution matrix to the adjoint differential equation

$$xY' = YG_{-\pi} \qquad \text{(0.24)} \quad [11(4.1.2)]$$

where $G_{-\pi}$ is the image of the matrix G above, (0.15), under the action of the element of the galois group of $\mathscr{T}(\pi)/\mathscr{T}$, which takes π into $-\pi$. If

$$\Theta = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & -1 & 0 \\ \vdots & & & \\ (-1)^n \cdots & & 0 & 0 \end{pmatrix}, \qquad \text{(0.25)} \quad [11(4.1.5)]$$

then for Y, $Y_{-\pi}$ given above

$$Y\Theta Y^{t}_{-\pi} = \Theta \tag{0.26}$$ [11(4.2.8)]

in $D(0, 1^-)$. Furthermore, in $D(0, 1^-)$,

$$Y^{\varphi}\mathscr{A}(x) = MY, \tag{0.27}$$ [11(4.2.11)]

where

$$M = \mathscr{A}(0) = \begin{pmatrix} 1 & 0 & 0 & \cdots 0 \\ a_1 & p & 0 & \cdots 0 \\ a_2 & pa_1 & p^2 & \cdots 0 \\ \vdots & & & \\ a_n & pa_{n-1} & p^2a_{n-2}\cdots & p^n \end{pmatrix} \tag{0.28}$$

in which $a_i = \mathscr{A}_{i+1,1}(0)$. It follows (taking determinants in (0.27)) that for $\operatorname{ord} x > -(n+1)b'$, and $p \neq 2$,

$$\det \mathscr{A}(x) = p^{n(n+1)/2}. \tag{0.29}$$ [11(4.2.14)]

1. Duality

The form in which we will prove the functional equation is as follows:

$$\mathscr{A}\Theta\mathscr{A}^{t}_{-\pi} = p^n\Theta \tag{1.1}$$

where Θ is the constant matrix (0.25). Denote $\zeta_i(t) = \epsilon^i(1)$, so that

$$(\zeta_0(t), \zeta_1(t), \ldots, \zeta_n(t)) = V(1, \pi t_1, \ldots, (\pi t_1)^n) \tag{1.2}$$

where V is the change of basis matrix, (0.13). The subscript $-\pi$ will indicate the effect of choosing $-\pi$ as $(p-1)$st root of $-p$ (instead of π) in the preceding theory. It follows from (1.2) that $\zeta_{i,-\pi}(-t) = \zeta_i(t)$. Since $F_{-\pi}((-1)^{n+1}x, -t) = F(x, t)$,

$$\mathscr{A}_{-\pi}(x) = \mathscr{A}((-1)^{n+1}x). \tag{1.3}$$

As a consequence $\mathscr{A}_{-\pi}(0) = \mathscr{A}(0)$, so that by (0.27)

$$Y^{\varphi}_{-\pi}\mathscr{A}_{-\pi} = M_{-\pi}Y_{-\pi} \tag{1.4}$$

where $Y_{-\pi}$ is the solution matrix at 0 (0.23), and $M_{-\pi} = \mathscr{A}(0) = M$. Hence to prove (1.1) it is sufficient by (1.4), (0.27), and (0.26) to prove

$$M\Theta M^{t}_{-\pi} = p^{n}\Theta. \tag{1.5}$$

Using (0.27) and computing directly, we find

$$M\Theta M^{t}_{-\pi} = p^{n}\left\{\Theta + \sum_{i=0}^{[\frac{n}{2}]} c_i \Theta T^{2i}\right\} \tag{1.6}$$

where the c_i's are constants and where $T = (T_{ij})$ is the $(n+1)\times(n+1)$ shift matrix with entries (in terms of the Kronecker delta) given by $T_{ij} = \delta_{i,j-1}$. More precisely, if in abbreviated notation $a_i^{(n)} = \mathscr{A}^{(n)}_{i+1,1}(0)$, (where the superscript denotes the n-variable case) then the constant $c_i(a^n)$ is a quadratic form in the $a_i^{(n)}$:

$$c_i(= c_i(a^{(n)})) = \sum_{j=0}^{2i} (-1)^j a^{(n)}_{2i-j} a^{(n)}_j. \tag{1.7}$$

It is sufficient for the proof of (1.5), to prove $c_i(a^{(n)}) = 0$, for $1 \le i \le [\frac{n}{2}]$. By (0.19), if

$$u_i = \sum_{\alpha>0} (-1)^{\alpha+i} \pi^{-\alpha} E^{(i-1)}(\alpha - 1) B_{p\alpha'} \quad (i > 0),$$

then

$$a_i^{(n)} = \sum_{\lambda=1}^{i} \binom{n+1}{\lambda} \sum u_{d_1} u_{d_2} \cdots u_{d_\lambda}, \tag{1.8}$$

the inner sum running over subscripts $d_j > 0$ satisfying $d_1 + d_2 + \cdots + d_\lambda = i$. Set $u_0 = 1$. Then

$$\begin{aligned} \left(\sum_{j=0}^{\infty} u_j x^j\right)^{n+1} &= \sum_{j=0}^{n} a_j^{(n)} x^j + x^{n+1} g_1(x), \\ \left(\sum_{j=0}^{\infty} (-1)^j u_j x^j\right)^{n+1} &= \sum_{j=0}^{n} (-1)^j a_j^{(n)} x^j + x^{n+1} g_2(x), \end{aligned} \tag{1.9}$$

where $g_1(x)$ and $g_2(x)$ belong to $\mathbb{Q}_p(\pi)[[x]]$. Multiplying the two equations of (1.9) together yields

$$\left(\sum_{i=0}^{\infty} c_i(u) x^{2i}\right)^{n+1} = \sum_{i=0}^{[\frac{n}{2}]} c_i(a^n) x^{2i} + h(x) x^{2[\frac{n}{2}]+1} \tag{1.10}$$

where $h(x) \in \mathbb{Q}_p(\pi)[[x]]$. If we compare coefficients on both sides of (1.10), then for $1 \leq j \leq [\frac{n}{2}]$,

$$c_j(a^{(n)}) = (n+1)c_j(u) + q_j(c_1(u), \ldots, c_{j-1}(u)), \tag{1.11}$$

where $q_j \in Z[Y_1, \ldots, Y_{j-1}]$, and $q_j(0, \ldots, 0) = 0$. If we assume by induction that $c_i(a^{(n-1)}) = 0$ for $i \leq [\frac{n-1}{2}]$, then by (1.11) $c_i(u) = 0$ for $i \leq [\frac{n-1}{2}]$ so that $c_i(a^{(n)}) = 0$ for $i \leq [\frac{n-1}{2}]$ again by (1.11). It remains to prove $c_i(a^{(n)}) = 0$ for n even and $i = n/2$.

In this case, since $M^{-1}\Theta T^n(M^t_{-\pi})^{-1} = p^{-2n}\Theta T^n$, we compute by (1.6),

$$Y^{-1}M^{-1}\Theta M^t_{-\pi}(Y^t_{-\pi})^{-1} - p^{-n}\Theta = p^{-2n}c_{n/2}(a^{(n)})Y^{-1}\Theta T^n(Y^t_{-\pi})^{-1}. \tag{1.12}$$

Since the first term on the left-side is simply $\mathcal{A}^{-1}\Theta(\mathcal{A}^t_{-\pi})^{-1}$, the left side is convergent for x, $\operatorname{ord} x > -(n+1)b'$. Using (0.22) to compute Y^{-1} and $(Y^t_{-\pi})^{-1}$, we find that the (i, j) entry in $Y^{-1}\Theta T^n(Y^t_{-\pi})^{-1}$ is

$$(-1)^{i+j}(\delta^{n+1-i}P_{11,-\pi}(x))(\delta^{n+1-j}P_{11}(x)) \tag{1.13}$$

where $P_{11}(x)$ is given by (0.22) and $P_{11,-\pi}(x) = P_{11}((-1)^{n+1}x)$. In particular, (1.12) implies that the $(n+1, n+1)$ entry, $R(x) = P_{11}((-1)^{n+1}x) \cdot P_{11}(x)$ converges in a disk $D(0, 1+\epsilon)$, $\epsilon > 0$. Given Deligne's Riemann hypothesis result in this example [2], we obtain a contradiction of $c_{n/2}(a^{(n)}) \neq 0$ as follows. If $\pi_1, \ldots, \pi_{n+1}$ are the eigenvalues of Frobenius, then by Deligne,

$$|\pi_i| = p^{n/2}, \tag{1.14}$$

for π_i and all its conjugates ($i = 1, 2, \ldots, n+1$). On the other hand, $\lambda(x) = P_{11}(x)/P_{11}(x^p)$ has continuation to $D(0, 1^+)$ [4(Theorem 3)] and at a Teichmüller unit a, $a = a^p$, $\alpha = \lambda(a)$ is an eigenvalue of Frobenius equal to π_i for some i. If $P_{11}(x) \cdot P_{11,-\pi}(x)$ converges on $D(0, 1+\epsilon)$, then $\alpha\alpha_{-\pi} = \lambda(a)\lambda_{-\pi}(a)$ may be evaluated by substituting a into $P_{11}(x)P_{11,-\pi}(x)/P_{11}(x^p)P_{11,-\pi}(x^p)$, obtaining $\alpha\alpha_{-\pi} = 1$ since $a^p = a$. Since α and $\alpha_{-\pi}$ are both algebraic integers, they are ℓ-adic units for all finite primes ℓ. Together with (1.14), this contradicts the product formula. Thus $c_{n/2}(a^{(n)}) = 0$ and this completes the proof of duality.

(1.15) THEOREM: *For $p \neq 2$, if $\mathcal{A}$ is the Frobenius matrix, then*

$$\mathcal{A}\Theta\mathcal{A}^t_{-\pi} = p^n\Theta.$$

Under the additional hypothesis that $p > n+1$, the result may also be proved via p-adic analysis. In fact, in no case does $R(x) = P_{11}(x)P_{11}((-1)^{n+1}x)$ converge in a disk $D(0, 1+\epsilon)$, $\epsilon > 0$. For n odd, $R(x) = P_{11}(x)^2$. In this case the non-extendability of $R(x)$ is implied by the non-extendability of the logarithmic derivative η_2 of $P_{11}(x)$ beyond $D(0, 1^+)$ [11(5.1.20)]. In the case of interest, n is even, and $R(x) = P_{11}(x)P_{11}(-x)$ is the product of a solution to (0.2) at 0 and a solution to the adjoint equation [11(4.1.4)] at 0. It follows that if $R(x)$ can be extended to a point b, then at b, $R(x)$ is a linear combination of products of local solutions at b of (0.2) and its adjoint [11(4.1.4)]. If b is a point of the annulus

$$U(1, 1+\epsilon) = D(0, 1+\epsilon) - D(0, 1^+), \quad \epsilon > 0$$

then modulo the substitution $x \to x^{n+1}$, the local solutions at b are given in [11(§5)]. Hence, we may write

$$R(x^{n+1}) = x^{-n} \sum_{j,j'=0}^{n} C_{j,j'} v_j(x) v_{j'}(x) \exp((\zeta^j - \zeta^{j'})\pi' x) \tag{1.16}$$

where $C_{j,j'} \in \Omega$, $v_j(x)$ converges on the complement of $D(0, 1^+)$ in Ω, $\pi' = (n+1)\pi$, ζ is a primitive $(n+1)$st root of 1 in Ω, and $\exp(cx)$ (for $c \in \Omega$) represents a local determination at b of a solution to the differential equation $y' = cy$, say $\exp(c(x-b))$. Note that by assumption $p > n+1$ so that ord $\pi' = 1/(p-1)$. If $c_1, \ldots, c_k$ are integers in Ω which lie in distinct residue classes, then $\{\exp(\pi' c_j x)\}_{j=1}^{k}$ are linearly independent over the field of functions meromorphic on $U(1, 1+\epsilon)$. (In fact, they are linearly independent over the larger field of functions meromorphic on $D(b, 1^+)$.) We may therefore equate coefficients on both sides of (1.16) as follows. Consider all pairs (j, j') of indices $0 \le j, j' \le n$ such that

$$\zeta^j - \zeta^{j'} \equiv 0 \bmod \mathcal{P}_\Omega \tag{1.17}$$

where $\mathcal{P}_\Omega$ denotes the maximal ideal in the valuation ring $\mathcal{O}_\Omega$ of Ω. Since p and $n+1$ are relatively prime (1.17) is equivalent to $j = j'$. Therefore, the assumption that $R(x)$ continues to $D(0, 1+\epsilon)$ implies

$$x^n R(x^{n+1}) = \sum_j C_{j,j} v_j(x) v_j(-x).$$

The left side converges for $|x| < 1+\epsilon'$, $\epsilon' > 0$; the right side converges for $|x| > 1$. Hence $x^n R(x^{n+1})$ converges on the sphere. By Liouville's

theorem, $x^n R(x^{n+1})$ is constant. Therefore, evaluating at $x = 0$, it is identically zero. Hence $R(x)$ is identically zero, which contradicts $R(x) = P_{11}(x)P_{11}(-x)$. ■

The functional equation may also be expressed as follows: let $a \in \mathbf{F}_q$, let $b = (-1)^{n+1}a$, then

$$\gamma_i \to q^n/\gamma_i$$

is a one-one correspondence from the set $\{\gamma_i\}_{i=1}^{n+1}$ of reciprocal zeros of $L(f_a, t)^{(-1)^{n+1}}$ onto the set $\{\gamma_{i,-\pi}\}_{i=1}^{n+1}$ of reciprocal zeros of $L(f_b, t)^{(-1)^{n+1}}$.

2. Eigenvalues of Frobenius

The main theorem (2.35) is a corollary of the following proposition.

(2.1) PROPOSITION: *If* $x \in \mathcal{T}(\pi)$, $\operatorname{ord} x \geq -(n+1)/p(p-1)$, $p \geq n+3$, *then the coefficients of the Frobenius matrix* $\mathcal{A}$ *satisfy*

$$\mathcal{A}_{\lambda\lambda}(x)/p^{\lambda-1} \equiv 1 \pmod{\pi} \quad \lambda = 1, 2, \ldots, n+1.$$

$$\mathcal{A}_{\lambda j}(x)/p^{\lambda-1} \equiv 0 \pmod{\pi}, \quad \text{for } j > \lambda.$$

REMARK: This result may also be formulated in terms of the matrix $\tilde{\mathcal{A}}(x)$, (0.18). The proposition then states

$$\tilde{\mathcal{A}}(x) \equiv \begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ * & & & 1 \end{pmatrix} \pmod{\pi}.$$

PROOF: By definition [11(§3.3)], $\mathcal{A} = W^t A V^t$ where A^t is the matrix of the Frobenius map with respect to the basis $\{(\pi t_1)^i\}_{i=0}^n$, $W = V^{-1}$, and V is the change of basis matrix (0.13). Thus,

$$\mathcal{A}_{\lambda j} = \sum_{\ell=\lambda}^{n+1} \sum_{k=1}^{j} v_{jk} W_{\ell\lambda} A_{\ell k}. \tag{2.2}$$

Define

$$r(\mathcal{A}_{\lambda j}) = \sum_{k=1}^{j} v_{jk} A_{\lambda k}. \tag{2.3}$$

Then $r(\mathscr{A}_{\lambda j})$ has the property by (0.18)

$$\operatorname{ord}(\mathscr{A}_{\lambda j} - r(\mathscr{A}_{\lambda j})) \geq \lambda. \tag{2.4}$$

We are reduced, therefore, to showing

$$\begin{aligned} r(\mathscr{A}_{\lambda\lambda})/p^{\lambda-1} &\equiv 1 \pmod{\pi} \\ r(\mathscr{A}_{\lambda j})/p^{\lambda-1} &\equiv 0 \pmod{\pi}, \quad \text{for } j > \lambda. \end{aligned} \tag{2.5}$$

By [11(§1.3)], both are known for $\lambda = 1$. For $j > 1$, $v_{j1} = 0$ so that

$$r(\mathscr{A}_{\lambda j}) = \sum_{k=2}^{j} v_{jk} A_{\lambda k}. \tag{2.6}$$

By (0.11), for $\lambda > 1$, $b^{(\lambda-1)}(0) = 0$, so that

$$A_{\lambda k} = \pi^{k-1} \sum_{i=1}^{n} \sum b^{(\lambda-1)}(\alpha) \Gamma_{ik}^{(n)}(\alpha),$$

where the inner sum runs over $\alpha = -\sum_{\ell=1}^{i} j_\ell U_\ell$, $j_\ell \in \mathbb{N}$,

$$\Gamma_{ik}^{(n)}(\alpha) = \binom{n}{i} x^{k-1} F(-p\alpha + (k-1)U) + \binom{n}{i-1} F(-p\alpha - (k-1)U_1),$$

and the $b^{(\lambda)}(\alpha)$ are the coefficients of the member of the dual basis, ξ^*_{λ, x^p}, (0.10). Following the argument of [11(2.5.9)], we write

$$\binom{n}{i} x^{k-1} F(-p\alpha + (k-1)U) = \sum r_j(\alpha) x^{j+k-1}$$

where the sum runs over $j \geq s(-p\alpha + (k-1)U)$. Hence

$$r_j(\alpha) = \binom{n}{i} B_j \prod_{i=1}^{n} B_{j+k-1-p\alpha_i}$$

and for all j (by (0.7a))

$$\operatorname{ord} r_j(\alpha) \geq (-p\Sigma(\alpha) + (n+1)j + n(k-1))b' \tag{2.7}$$

Note that for α as above $s^*(\alpha) = 0$ and (0.10) (with variable equal to x^p) becomes

$$\text{ord } b^{(\lambda-1)}(\alpha) \geq \Sigma(\alpha)/(p-1).$$

Using this and (2.7) when $j \geq p$, then

$$\text{ord } \pi^{k-1} b^{(\lambda-1)}(\alpha) r_j(\alpha) x^{j+k-1} \geq (n+2)e > n,$$

in which the strict inequality makes use of the assumption $p \geq n+3$. By utilizing the sharper estimate (0.7b) when $j < p$, and the fact [11(2.5.9)] that $b^{(\lambda-1)}(\alpha) = 0$ for α in the index set with $-\Sigma(\alpha) < \lambda - 1$, we show, as in [11(2.5.9)] that for $k > 1$ and under the hypotheses of the proposition

$$\text{ord } \pi^{k-1} b^{(\lambda-1)}(\alpha) r_j(\alpha) x^{j+k-1} > \lambda - 1$$

with strict inequality a consequence of the assumption $k > 1$. This shows that for $k > 1$,

$$\text{ord } \pi^{k-1} b^{(\lambda-1)}(\alpha) \binom{n}{i} x^{k-1} F(-p\alpha + (k-1)U) > \lambda - 1.$$

(We take this opportunity to note that contrary to the assertion [11(p.569)], for $k > 1$, we only get the weak inequality

$$\text{ord } \pi^{k-1} b^{(\lambda-1)}(\alpha) \binom{n}{i-1} F(-p\alpha - (k-1)U_1) \geq \lambda - 1$$

arising from the second term of $\Gamma_{ik}^{(n)}(\alpha)$.) Hence

$$A_{\lambda k} \equiv \pi^{k-1} \sum_{i=1}^{n} \binom{n}{i-1} \sum_{\alpha} b^{(\lambda-1)}(\alpha) F(-p\alpha - (k-1)U_1) \pmod{p^{\lambda-1}\pi}$$

where the inner sum runs over $\alpha = -\Sigma_{\ell=1}^{i} j_\ell U_\ell$, $j_\ell \in \mathbb{N}$. This may be improved somewhat since we know by the proof of [11(2.5.9)] that $b^{(\lambda-1)}(\alpha) = 0$ for those α, $-\Sigma(\alpha) < \lambda - 1$, and it is easy to show that

$$\text{ord } \pi^{k-1} \binom{n}{i-1} b^{(\lambda-1)}(\alpha) F(-p\alpha - (k-1)U_1) > \lambda - 1$$

for those α, $-\Sigma(\alpha) > \lambda - 1$. Hence

$$A_{\lambda,k} \equiv \pi^{k-1} \sum_{i=1}^{\lambda-1} \binom{n}{i-1} \sum_{\alpha \in K^{(i)}} b^{(\lambda-1)}(\alpha) F(-p\alpha - (k-1)U_1) \pmod{p^{\lambda-1}\pi}$$

where the index set $K^{(i)}$ of the inner sum is the set

$$K^{(i)} = \left\{\alpha \in \mathbf{Z}^{n+1} \;\middle|\; \alpha = \sum_{\ell=1}^{i} j_\ell U_\ell,\ j_\ell \in \mathbf{N},\ -\Sigma(\alpha) = \lambda - 1\right\}.$$

If $\alpha \in K^{(i)}$, then $1 \le j_\ell \le p-3$ (since $p \ge n+3$). Hence we may apply the estimates (0.7b) obtaining

$$F(-p\alpha - (k-1)U_1) \equiv B_{pj_1-(k-1)}B_{pj_2}\cdots B_{pj_i} \pmod{\pi^{p(\lambda-1)-(k-1)+1}}.$$

Thus,

$$A_{\lambda k} \equiv \pi^{k-1}\sum_{i=1}^{\lambda-1}\binom{n}{i-1}\sum_{\alpha\in K^{(i)}} b^{(\lambda-1)}(\alpha)B_{pj_1-(k-1)}B_{pj_2}\cdots B_{pj_i} \pmod{p^{\lambda-1}\pi}$$

(2.8)

For each $\alpha = -\Sigma_{\ell=1}^{i} j_\ell U_\ell \in K^{(i)}$, define

$$D(j;\alpha) = \sum_{k=2}^{j} v_{jk}\pi^{k-1}\cdot b^{(\lambda-1)}(\alpha)B_{pj_1-(k-1)}B_{pj_2}\cdots B_{pj_i}, \tag{2.9}$$

so that

$$r(\mathscr{A}_{\lambda j}) \equiv \sum_{i=1}^{\lambda-1}\binom{n}{i-1}\sum_{\alpha\in K^{(i)}} D(j;\alpha). \tag{2.10}$$

We claim that for $\alpha \in K^{(i)}$, $i > 1$,

$$D(j;\alpha) \equiv 0 \pmod{p^{\lambda-1}\pi}. \tag{2.11}$$

We know by (0.10) that for such α (x and p as in the hypotheses)

$$\operatorname{ord} b^{(\lambda-1)}(\alpha) \ge \frac{-(\lambda-1)}{p-1},$$

and by (0.7)

$$\operatorname{ord} B_{pj_\ell} \ge \frac{pj_\ell}{p-1},$$

since $j_\ell < \lambda - 1 \le n < p$. Hence to show (2.11) it is sufficient to prove

$$\operatorname{ord}\left(\sum_{k=2}^{j} v_{jk}B_{pj_1-(k-1)}\right) > \frac{pj_1-(k-1)}{p-1}.$$

By definition (0.6),

$$B_m = \sum_{j+pk=m} (-1)^k \frac{\pi^{j+k}}{j!k!},$$

so that

$$B_{pj_1-(k-1)} = \sum_{s=0}^{j_1-1} \frac{(-1)^s \pi^{pj_1-(k-1)-sp+s}}{s![(j_1-s)p-(k-1)]!}. \tag{2.12}$$

It suffices, therefore, to demonstrate

$$\operatorname{ord} \sum_{k=2}^{j} \frac{v_{jk}}{s![(j_1-s)p-(k-1)]!} > s. \tag{2.13}$$

Using $VW = I$, and the definition of w_{ij} in terms of elementary symmetric functions (0.16), we conclude that

$$v_{j2} + \sum_{k=3}^{j} v_{jk}(X-1)\cdots(X-(k-2)) = X^{j-2}. \tag{2.14}$$

Hence, letting $X = \ell p$,

$$\sum_{k=2}^{j} \frac{v_{jk}}{(\ell p-(k-1))!} = \frac{(\ell p)^{j-2}}{(\ell p-1)!}. \tag{2.15}$$

Using (2.15) with $\ell = j_1 - s$, we derive that the left side of (2.13) is precisely $s + j - 1 - j_1$. For $j \geq \lambda$, this is strictly greater than s, since in the case $i > 1$, j_ℓ and in particular j_1 is strictly less than $\lambda - 1$. This establishes (2.11), and (2.10) becomes

$$r(\mathscr{A}_{\lambda j}) \equiv D(j; -(\lambda-1)U_1) \pmod{p^{\lambda-1}\pi}. \tag{2.16}$$

By definition of the dual basis $b^{(\lambda-1)}(-(\lambda-1)U_1) = \pi^{-(\lambda-1)}$. Hence substituting (2.12) into (2.16) and recalling the definition $\pi^{p-1} = -p$, we obtain

$$\frac{1}{p^{\lambda-1}} r(\mathscr{A}_{\lambda j}) \equiv (-1)^{\lambda-1} \sum_{s=0}^{\lambda-2} \frac{p^{-s}}{s!} \sum_{k=2}^{j} \frac{v_{jk}}{[(\lambda-1-s)p-(k-1)]!} \pmod{\pi}.$$

By (2.15), we are reduced to

$$\frac{1}{p^{\lambda-1}} r(\mathscr{A}_{\lambda j}) \equiv (-1)^{\lambda-1} \sum_{s=0}^{\lambda-2} \frac{p^{j-2-s}(\lambda-1-s)^{j-2}}{s![(\lambda-1-s)p-1]!} \pmod{\pi}. \tag{2.17}$$

But, clearly

$$\operatorname{ord} \frac{p^{j-2-s}}{[(\lambda-1-s)p-(k-1)]!} = j-\lambda$$

so that the proof of the proposition in the case $j > \lambda$ is complete. If $j = \lambda$, we use Wilson's theorem repeatedly, so that

$$\frac{1}{p^{\lambda-1}} r(\mathscr{A}_{\lambda\lambda}) \equiv \sum_{s=0}^{\lambda-2} \frac{(-1)^s(\lambda-1-s)^{\lambda-2}}{s!(\lambda-2-s)!} \pmod{\pi}. \tag{2.18}$$

However there is an elementary identity from the calculus of finite differences,

$$m! = \sum_{s=0}^{m} \binom{m}{s} (-1)^s (m+1-s)^m \quad (m \in \mathbb{N}) \tag{2.19}$$

which states that the m^{th} successive difference of the consecutive m^{th} powers $1^m, 2^m, \ldots, (m+1)^m$ is $m!$ The proof of proposition for $j = \lambda$, now follows from (2.18) by taking $m = \lambda - 2$ in (2.19). ■

Now suppose $a \in \mathbb{F}_q$, $(q = p^r)$, and $z = z^q$ is a Teichmüller lifting of a in Ω. If $\mathscr{T}_r$ denotes the unique unramified extension of Q_p of degree r in Ω, then $z \in \mathscr{T}_r$. We wish to evaluate p-adically the eigenvalues of the Frobenius map

$$B_z(\bar{\alpha}) = \bar{\alpha}_{z^{q/p}} \circ \cdots \bar{\alpha}_{z^p} \circ \bar{\alpha}_z \colon \mathfrak{W}_z \to \mathfrak{W}_z,$$

viewed as an endomorphism of $\mathfrak{W}_z$ over the field $k_r = \mathscr{T}_r(\pi)$. These eigenvalues are related to the hyperkloosterman exponential sum by the equivalent relations (0.3) and (0.4). Let $\mathscr{O}_r$ and $\mathscr{O}_\infty$ be the respective rings of integers of the fields k_r and $k_\infty = \mathscr{T}(\pi)$; let $\mathscr{P}_r$ and $\mathscr{P}_\infty$ be the respective maximal ideals. Let σ denote the lifting of the absolute Frobenius to k_r and k_∞ defined by setting $\sigma(\pi) = \pi$. Recall that for z a Teichmüller unit, $\sigma(z) = z^p$.

Our original proof of theorem (2.35) was an induction proof on n, utilizing the normalization of the solution matrix as in [6]. We hope to return to this argument in a future article to present a (p-adic) analytic formula for the unit eigenvalue of Frobenius. We are indebted to B. Dwork for the following argument which shows that the theorem is indeed a corollary of proposition (2.1). To see this we proceed with (semi-) linear algebra. With an eye toward future applications, we employ greater generality than necessary for the theorem.

(2.20) PROPOSITION: *Let D be an $N \times N$ matrix with entries in $\mathcal{O}_\infty$ and let $\bar{D}$ be the reduction of D mod $\mathcal{P}_\infty$. Assume $\bar{D}$ is block lower-triangular and invertible, so we may write*

$$\bar{D} = \begin{pmatrix} \bar{D}_1 & & 0 \\ & \bar{D}_2 & \\ & & \ddots \\ * & & \bar{D}_s \end{pmatrix}$$

where the $\bar{D}_j$ are invertible $i_j \times i_j$ matrices, and $\Sigma_{j=1}^{s} i_j = N$. Let

$$\Delta = \operatorname{diag}(\underbrace{p^{r_1}, \ldots, p^{r_1}}_{i_1}, \underbrace{p^{r_2}, \ldots, p^{r_2}}_{i_2}, \ldots, \underbrace{p^{r_s}, \ldots, p^{r_s}}_{i_s})$$

where $0 \leq r_1 < r_2 < \cdots < r_s$ are integers. Let $\mathcal{D} = \Delta D$. Then

(a) *there exists $M \in GL(N, \mathcal{O}_\infty)$ such that*

$$M^\sigma \mathcal{D} = \Delta M, \tag{2.21}$$

(b) *under the additional hypotheses that $\bar{D}$ is lower triangular (so that $i_1 = i_2 \cdots = i_s = 1$) with 1's on the main diagonal, and that*

$$\Delta = \operatorname{diag}(p^{r_1}, p^{r_2}, \ldots, p^{r_N})$$

with $0 \leq r_1 < r_2 < \cdots < r_N$, then M may be chosen so that

$$M \equiv I_N \pmod{\mathcal{P}_\infty}.$$

PROOF: We may assume without any loss of generality that $r_1 = 0$. Suppose $s = 1$, so that Δ is the $N \times N$ identity matrix. We wish to find M so that

$$M^\sigma \mathcal{D} = M.$$

We can view

$$\rho: x \to x^\sigma \mathcal{D} \tag{2.22}$$

as a semi-linear transformation on k_∞^N, stable on $\mathcal{O}_\infty^n$. Then by Dieudonné's theorem [5(Theorem 1)], [10], there exists $B = (B_{ij}) \in GL(N, k_\infty)$ such that

$$B^\sigma \mathcal{D} = \operatorname{diag}(p^{m_1}, \ldots, p^{m_N}) B.$$

Taking determinants of both sides, we deduce from $\det \bar{\mathscr{D}} \neq 0$ that $m_1 = m_2 \cdots = m_N = 0$. Let $b \in k_1$, $|b| = \max_{i,j} |B_{ij}|$. If we set $M = (1/b)B$, then $M \in GL(N, \mathcal{O}_\infty)$ is as desired.

We proceed by induction on s. Let $\bar{\mathbf{F}}_p$ be the residue class field of K_∞. Consider the reduction mod $\mathscr{P}_\infty$ of the map ρ (2.22) acting on $\mathcal{O}_\infty^N$:

$$\bar{\rho}\colon (\bar{x}_1, \ldots, \bar{x}_N) \to (\bar{x}_1^p, \bar{x}_2^p, \ldots, \bar{x}_N^p)\left(\begin{array}{c|c} \bar{D}_1 & 0 \\ \hline 0 & 0 \end{array}\right).$$

Again by Dieudonné's theorem, there exist i_1 linearly independent fixed points of the map in $(\bar{\mathbf{F}}_p)^N$ say $\bar{\xi}_j = (\bar{x}_{j,1}, \ldots, \bar{x}_{j,i_1}, 0, \ldots, 0)$.

By a standard argument, these fixed points can be lifted to fixed points $\xi_1, \ldots, \xi_{i_1}$ of ρ in $\mathcal{O}_\infty^N$ such that if $\xi_j = (x_{j1}, \ldots, x_{jN})$ then

$$|x_{jk}| < 1, \quad \text{for } k > i_1, \tag{2.23}$$

and if $\Lambda_1 = (x_{jk})$, $j, k = 1, 2, \ldots, i_1$, then $|\det \Lambda_1| = 1$. Set

$$Y_1 = \left(\begin{array}{c|c} \Lambda_1 & \Lambda_2 \\ \hline 0 & I \end{array}\right)$$

where $(\Lambda_1 \mid \Lambda_2)$ has for its rows the vectors ξ_j, Λ_1 is an $i_1 \times i_1$ matrix with $\det \Lambda_1 \neq 0$, and Λ_2 is an $i_1 \times (N - i_1)$ matrix, with $\Lambda_2 \equiv 0 \pmod{\mathscr{P}_\infty}$. Writing $\mathscr{D} = \left(\begin{array}{c|c} D_1 & H_1 \\ \hline H & \Gamma \end{array}\right)$, we have by a straightforward computation

$$Y_1^\sigma \mathscr{D} Y_1^{-1} = \left(\begin{array}{c|c} I_{i_1} & 0 \\ \hline H\Lambda_1^{-1} & \mathscr{D}^{(1)} \end{array}\right)$$

where $\mathscr{D}^{(1)} = -H\Lambda_1^{-1}\Lambda_2 + \Gamma$. Note that we may factor $\mathscr{D}^{(1)} = \Delta^{(1)} D^{(1)}$ where

$$\Delta^{(1)} = \operatorname{diag}(p^{r_2}, \ldots, p^{r_2}, \ldots, p^{r_s}, \ldots, p^{r_s}) \tag{2.24}$$

and $D^{(1)}$ is an $(N - i_1) \times (N - i_1)$ square matrix with entries in $\mathcal{O}_\infty$ whose reduction mod $\mathscr{P}_\infty$ by (2.23) satisfies

$$\bar{D}^{(1)} = \bar{\Gamma} = \begin{pmatrix} \bar{D}_2 & & & 0 \\ & \bar{D}_3 & & \\ * & & \ddots & \\ & & & \bar{D}_s \end{pmatrix} \tag{2.25}$$

It is convenient to call $H\Lambda^{-1} = U$ and use block notation so that

$$Y_1^{\sigma}\mathscr{D}Y_1^{-1} = \left(\begin{array}{c|c} I_{i_1} & 0 \\ \hline \begin{matrix} U_2 \\ \vdots \\ U_s \end{matrix} & \begin{matrix} \mathscr{D}_{22}^{(1)} \cdots \mathscr{D}_{2s}^{(1)} \\ \\ \mathscr{D}_{s2}^{(1)} \cdots \mathscr{D}_{ss}^{(1)} \end{matrix} \end{array}\right)$$

where U_j is an $i_j \times i_1$ matrix with coefficients in $p^{r_j}\mathscr{O}_\infty$, and $\mathscr{D}_{jk}^{(1)}$ is an $i_j \times i_k$ matrix with coefficients in $p^{r_j}\mathscr{O}_\infty$. We wish to find

$$Z_1 = \left(\begin{array}{c|c} I_{i_1} & 0 \\ \hline \begin{matrix} V_2 \\ \vdots \\ V_s \end{matrix} & I_{N-i_1} \end{array}\right)$$

such that

$$Z_1^{\sigma}Y_1^{\sigma}\mathscr{D}Y_1^{-1}Z_1^{-1} = \left(\begin{array}{c|c} I_{i_1} & 0 \\ \hline 0 & \mathscr{D}^{(1)} \end{array}\right).$$

Therefore, we need to solve the simultaneous equations

$$V_k^{\sigma} + U_k - \sum_{j=2}^{s} \mathscr{D}_{kj}^{(1)} V_j = 0, \quad k = 2, \ldots, s,$$

for the matrices V_k. Since p^{r_k} divides both U_k and $\mathscr{D}_{kj}^{(1)}$, it also divides V_k. It is sufficient to show that for every integer ℓ we can find matrices $V_k^{(\ell)}$ such that

$$V_k^{(\ell)} \equiv V_k^{(\ell+1)} \pmod{p^{\ell}\pi} \tag{2.26}$$

and

$$V_k^{(\ell)\sigma} + U_k - \sum_{j=2}^{s} \mathscr{D}_{kj}^{(1)} V_j^{(\ell)} \equiv 0 \pmod{p^{\ell}\pi}. \tag{2.27}$$

For $\ell < r_2$ we take $V_k^{(\ell)} = 0$ for all k. For $\ell = r_2$ we take

$$V_2^{(r_2)} \equiv -U_2^{\sigma^{-1}} \pmod{p^{r_2}\pi},$$

$$V_k^{(r_2)} \equiv 0 \pmod{p^{r_2}\pi}, \quad \text{for } k > 2.$$

Assume for some ℓ, $\ell \geq r_2$, $V_k^{(\ell)}$ has been determined for all k with properties (2.26) and (2.27). Set

$$V_k^{(\ell+1)} = V_k^{(\ell)} + p^{\ell}\pi W_k^{(\ell+1)}.$$

Then letting

$$\delta_k = V_k^{(\ell)\sigma} + U_k - \sum_{j=2}^{s} \mathscr{D}_{kj}^{(1)} V_j^{\ell},$$

we solve

$$\delta_k + p^{\ell}\pi W_k^{(\ell+1)\sigma} - p^{\ell}\pi \sum_{j=2}^{s} \mathscr{D}_{kj}^{(1)} W_j^{(\ell+1)} \equiv 0 \pmod{p^{\ell+1}\pi}$$

by noting that since $r_2 \geq 1$, p divides all $\mathscr{D}_{kj}^{(1)}$, and it suffices to take

$$W_k^{(\ell+1)} \equiv -\frac{1}{p^{\ell}\pi}\,\delta_k^{\sigma^{-1}} \pmod{p}.$$

We complete the construction of Z_1 by setting $V_t = \lim_{\ell\to\infty} V_k^{(\ell)}$.

By induction, there is a matrix $M^{(1)} \in GL(N - i_1, \mathcal{O}_\infty)$ such that

$$M^{(1)\sigma}\mathscr{D}^{(1)} = \Delta^{(1)}M^{(1)}.$$

If we now take

$$M = \left(\begin{array}{c|c} I_{i_1} & 0 \\ \hline 0 & M^{(1)} \end{array}\right) Z_1 Y_1,$$

then the proof of part (a) is complete.

For the proof of part (b) we note that by the additional hypotheses,

$$\bar{\mathscr{D}} = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & 0 \end{array}\right).$$

Hence the fixed point $\xi = (x_1, \ldots, x_N)$ may be taken so that

$$x_1 \equiv 1 \pmod{\mathscr{P}_\infty},$$

$$x_j \equiv 0 \pmod{\mathscr{P}_\infty}, \quad \text{for } j > 1.$$

The conclusion now follows as above but here the induction hypothesis gives $M^{(1)}$ in $GL(N-1, \mathcal{O}_\infty)$ satisfying

$$M^{(1)} \equiv I_{N-1} \pmod{\mathcal{P}_\infty}. \quad \blacksquare$$

(2.28) COROLLARY: *Under the hypotheses of part (a) of the proposition, M is determined up to multiplication by a diagonal matrix in* $GL(N, \mathcal{O}_1)$ *(i.e. up to multiplication by a diagonal matrix whose coefficients are units of* $\mathbb{Q}_p(\pi)$*).*

PROOF: Since $M \in GL(N, \mathcal{O}_\infty)$, any other solution may be written EM for some $E = (E_{ij}) \in GL(N, \mathcal{O}_\infty)$. Substituting in (2.21) and eliminating M gives

$$E^\sigma \Delta = \Delta E.$$

Thus $E_{ij}^\sigma p^{j-1} = E_{ij} p^{i-1}$, and E is diagonal with coefficients fixed by σ. $\blacksquare$

(2.29) COROLLARY: *Let* $\mathcal{D}, \Delta, D, M$ *be as in part (a) of proposition* (2.20). *Assume furthermore the coefficients of D lie in* $\mathcal{O}_r$. *Let*

$$\mathcal{D}_r = \mathcal{D}^{\sigma^{r-1}} \mathcal{D}^{\sigma^{r-2}} \cdots \mathcal{D} \tag{2.30}$$

and

$$E = M^{\sigma^r} M^{-1}. \tag{2.31}$$

Then (i) *E is diagonal with unit coefficients in* $\mathcal{O}_1$.

(ii) $M\mathcal{D}_r M^{-1} = E^{-1}\Delta^r$ *(i.e. M diagonalizes* $\mathcal{D}_r$ *as linear transformation over* k_r*).*

(iii) *If furthermore* $\mathcal{D}$, Δ, *D, and M are as in part (b) of proposition* (2.20), *then the units along the diagonal of E are all principal and*

$$E \equiv I_N \pmod{\pi}.$$

PROOF: Apply σ^i to (2.21) so that

$$M^{\sigma^{i+1}} \mathcal{D}^{\sigma^i} = \Delta M^{\sigma^i} \tag{2.32}$$

But $\mathcal{D}$ is fixed by σ^r, and hence with E as in (2.31), EM satisfies (2.21). Thus (i) follows from corollary (2.28). (iii) follows from the definition of E, (2.31), and the known properties of M, (2.20b). By (2.32),

$$M^{\sigma^i} \mathcal{D}^{\sigma^{i-1}} \cdots \mathcal{D}^\sigma \cdot \mathcal{D} = \Delta^i M.$$

Thus

$$M^{\sigma^r}\mathscr{D}_r = \Delta^r M .$$

(ii) now follows from the definition of E, (2.31). ■

(2.33) COROLLARY: (a) *Let D, Δ, $\mathscr{D}$, M be $N \times N$ matrices satisfying the hypotheses of proposition* (2.20), *part* (a). *If in addition we assume that the coefficients of D belong to $\mathcal{O}_r$, $q = p^r$, then the eigenvalues $\{\gamma_j\}_{j=1}^N$ of $\mathscr{D}_r$* (2.30), *(viewed as a linear map of k_r^N over k_r), belong to $\mathcal{O}_1$, the ring of integers of $\mathbb{Q}_p(\pi)$, and may be ordered so that*

$$\operatorname{ord}_q \gamma_j = r_\ell, \quad \text{for } j \text{ such that } \sum_{k=1}^{\ell} i_k < j \leq \sum_{k=1}^{\ell+1} i_k, \tag{2.34}$$

(the r_ℓ are the integers in the statement of proposition (2.20) *part* (a)).

(b) *If D, Δ, $\mathscr{D}$, M are as in proposition* (2.20) *part* (b) *then the $\{\gamma_j\}_{j=1}^N$ may be ordered so that*

$$\gamma_i / q^{r_i} \equiv 1 \pmod{\pi}. \quad ■$$

In our case, $N = n+1$, $D = \tilde{\mathscr{A}}(z)$, $\Delta = \operatorname{diag}(1, p, \ldots, p^n)$, and by (2.1), D, Δ, $\mathscr{D}$ satisfy the hypotheses of proposition (2.20) part (b).

(2.35) THEOREM: *Let $\{\gamma_i\}_{i=1}^{n+1}$ be the eigenvalues of $B_z(\bar{\alpha})$ acting linearly over k_r on $\mathfrak{W}_z$. Then the $\{\gamma_i\}_{i=1}^{n+1}$ are integers in $\mathbb{Q}_p(\pi)$ and may be so arranged that*

$$\gamma_i / q^{i-1} \equiv 1 \pmod{\pi}. \quad ■$$

3. Non-existence of Tate-Deligne lifting

We treat the possibility of normalization by a good choice of lifting of Frobenius. Let $\varphi_1(x) = x^p + z(x)$ where $z(x)$ is analytic, defined over $\mathbb{Q}_p(\pi)$, and $|z(x)| < 1$. Let $\mathscr{A}^{(\varphi_1)}$ be the matrix of the map $\tilde{\alpha}_x^* = F(x, t) \circ \varphi_1 \mathfrak{R}_{\varphi_1(x)} \to \mathfrak{R}_x$ relative to the bases $\{\zeta_i^*\}$, $0 \leq i \leq n+1$, [11(§3.2)]. Then φ_1 is an excellent (Tate-Deligne) lifting of Frobenius provided the entries $\mathscr{A}_{i1}^{(\varphi_1)}$ $(2 \leq i \leq n+1)$ all vanish. This is equivalent via the Katz identification [9] to the stability of the absolute Frobenius on

holomorphic n-forms in the Monsky-Washnitzer dagger cohomology theory.

We proceed in two steps. First, we prove that there is a unique $z(x)$ as above for which $\mathscr{A}_{21}^{(\varphi_1)}(x) = 0$. In the second step we show that for this z, $\mathscr{A}_{31}^{(\varphi_1)}(x)$ is not identically zero.

If Y is a solution matrix to (0.14) at $a \in \mathscr{T}$, then [5(Prop. 3.1)]

$$Y^{\sigma\varphi}\mathscr{A} = Y^{\sigma\varphi_1}\mathscr{A}^{(\varphi_1)}. \tag{3.1}$$

Thus

$$\mathscr{A}^{(\varphi_1)}(x) = \chi^{\sigma}(x^p, z)\mathscr{A}(x), \tag{3.2}$$

where

$$\chi(x, z) = Y^{-1}(x + z)Y(x), \tag{3.3}$$

χ being defined whenever x and $x + z$ belong to the domain of definition of Y. χ then satisfies the partial differential equation

$$\frac{\partial \chi}{\partial x} - \frac{\partial \chi}{\partial z} = \chi G_0 \tag{3.4}$$

where $G_0 = (1/x)G$, G defined in (0.15). Hence, we may write

$$\chi(x, z) = \sum_{\nu=0}^{\infty} \frac{z^{\nu}}{\nu!} M_{\nu}(x) \tag{3.5}$$

where M_{ν} is a matrix of rational functions of x which satisfies by (3.4) the recursive relation

$$M_{\nu+1} = M_{\nu}' - M_{\nu}G_0, \quad (M_0 = I). \tag{3.6}$$

If $M_{\nu}(x) = (M_{\nu}(i, j; x))$, then (3.6) translates into the following recursions on entries:

$$\begin{aligned} M_{\nu}(i, j) &= M_{\nu-1}'(i, j) - x^{-1}M_{\nu-1}(i, j + 1), \quad (j \neq n + 1), \\ M_{\nu}(i, n + 1) &= M_{\nu-1}'(i, n + 1) - \pi^{n+1}M_{\nu-1}(i, 1). \end{aligned} \tag{3.7}$$

It follows from (3.7) that, given the initial condition $M_0 = I$, $M_{\nu}(i, j)$ $(\in \mathbb{Q}_p(\pi)(x))$ is in fact a homogeneous polynomial of degree ν in π^{n+1} and x^{-1} with coefficients in Z. Furthermore, $M_{\nu}(i, j)$ is divisible by $x^{-r_{\nu}(i,j)}$ where

$$r_\nu(i,j) = \left[\frac{n}{n+1}(\nu+1-i+j)\right] + i - j, \tag{3.8}$$

(in which [ ] denotes the greatest integer function). Therefore, if $\chi(x,z) = (\chi_{ij}(x,z))$, then

$$\chi_{ij}(x,z) = \delta_{ij} + \sum_{\nu \geq t(i,j)} M_\nu(i,j;x)\frac{z^\nu}{\nu!} \tag{3.9}$$

where $t(i,j)$ is the least positive residue of $i-j$ module $n+1$. Clearly $\chi_{ij}^{\sigma} = \chi_{ij}$.

By (3.2),

$$\mathscr{A}_{21}^{(\varphi_1)}(x) = \sum_{i=1}^{n+1} \chi_{2i}(x^p, z)\mathscr{A}_{i1}(x). \tag{3.10}$$

Let $f_i = \mathscr{A}_{i1}/\mathscr{A}_{11}$. Then $\mathscr{A}_{21}^{(\varphi_1)}(x) = 0$ is equivalent to

$$\ell(x,z) = -f_2(x), \tag{3.11}$$

where

$$\ell(x,z) = \frac{1}{\chi_{22}(x^p,z)}\left\{\chi_{21}(x^p,z) + \sum_{j=3}^{n+1}\chi_{2j}(x^p,z)f_j(x)\right\}. \tag{3.12}$$

It is a standard computation to show $\chi_{ij}(x^p,z)$ converges in the region

$$\Delta = \left\{(x,z)\in\Omega^2 \,\middle|\, \operatorname{ord} z > \operatorname{ord} x^p + \frac{1}{p-1}, \quad \text{for } -\frac{(n+1)}{(p-1)} \leq \operatorname{ord} x^p;\right.$$
$$\left.\operatorname{ord} z > \frac{n}{n+1}\operatorname{ord} x^p, \quad \text{for } -(n+1)b < \operatorname{ord} x^p \leq -\frac{(n+1)}{(p-1)}\right\}.$$

Let

$$\epsilon = \begin{cases} 1 & \text{if } \operatorname{ord} x^p > -\left(\dfrac{n+1}{p-1}\right) \\ \dfrac{n}{n+1} & \text{if } \operatorname{ord} x^p \leq -\left(\dfrac{n+1}{p-1}\right). \end{cases}$$

Then the entries $\chi_{ii}(x^p,z)$, $i = 1,2,\ldots,n+1$, are principal units on the region $\Gamma_\epsilon \subset \Delta$,

$$\Gamma_\epsilon = \left\{(x, z) \in \Delta \mid \operatorname{ord} z - \epsilon \cdot \operatorname{ord} x^p > \frac{1}{p-1}\right\}.$$

Let $g(x, z) = x^p \ell(x, z) + z$, so that

$$\frac{g(x, z)}{z} = \chi_{22}(x^p, z)^{-1} \sum_{\nu=2}^{\infty} \frac{z^{\nu-1}}{\nu!} m_\nu(x), \tag{3.13}$$

where

$$\begin{aligned} m_\nu(x) = {} & x^p M_\nu(2, 1; x^p) + \nu M_{\nu-1}(2, 2; x^p) \\ & + \sum_{k=3}^{n+1} x^p f_k(x) M_\nu(2, k; x^p). \end{aligned} \tag{3.14}$$

For $c \in \mathbb{R}_+$, define

$$\Gamma_{c,\epsilon} = \left\{(x, z) \in \Gamma_\epsilon \mid \operatorname{ord} z - \epsilon \cdot \operatorname{ord} x^p - \frac{1}{p-1} \geq c\right\}.$$

Then one sees that there exists a constant k, depending on c, $0 < k < 1$ such that $|g(x, z)| < k|z|$ for $(x, z) \in \Gamma_{c,\epsilon}$. Thus g satisfies the Lipshitz condition

$$|g(x, z_1) - g(x, z_2)| < k \cdot |z_1 - z_2|$$

for pairs $(x, z_1), (x, z_2) \in \Gamma_{c,\epsilon}$. Hence, (cf. [7, Lemma 7.1]), we have the following proposition.

(3.15) PROPOSITION: *The equation* $w = \ell(x, z)$ *has a unique holomorphic solution* $z = z(x, w)$ *for* (x, w) *in the region* $\Gamma_{\epsilon-1}$. *In this region* $|z(x, w)| = |x| \cdot |w|$. ■

If $w = -f_2(x)$, by (0.17) $\operatorname{ord} f_2(x) \geq e$ for $\operatorname{ord} x^p > -(n+1)b$. Hence a holomorphic solution z exists for (3.11) in the region

$$T = \left\{x \in \Omega \mid e - (\epsilon - 1) \operatorname{ord} x^p - \frac{1}{p-1} > 0, \right.$$
$$\left. \operatorname{ord} x^p > -(n+1)b\right\}.$$

The condition $(\epsilon - 1) \cdot \operatorname{ord} x^p < e - (1/(p-1))$ is equivalent to $p > 3$ and $\operatorname{ord} x^p > -(n+1)b - (2/(p-1))$. Therefore,

$$T = \left\{ x \in \Omega \mid \operatorname{ord} x^p > -(n+1)\left(b - \frac{2}{p-1}\right) \right\}, \tag{3.16}$$

for $p > 3$. Note $T \supset D(0, 1^+)$. We summarize the above results.

(3.17) COROLLARY: *There exists a unique lifting of the Frobenius map*

$$\varphi_1(x) = x^p + z(x),$$

(where $z(x)$ is analytic and $|z(x)| < 1$ for $x \in T$) for which $\mathscr{A}_{21}^{(\varphi_1)}(x) = 0$ for $x \in T$. φ_1 is defined over $\mathbb{Q}_p(\pi)$. ■

As the second step, we prove that $\mathscr{A}_{31}^{(\varphi_1)}$ is congruent to a non-zero polynomial mod p^{3e}. As a consequence, for x a generic unit, $\mathscr{A}_{31}^{(\varphi_1)}(x) \neq 0$. Since $\mathscr{A}_{31}^{(\varphi_1)}(x)$ is a power-series, this implies it does not vanish identically in any neighborhood.

By (3.15), for x a unit, $|z| = |f_2(x)|$. Hence ord $z \geq e$. By (3.13), ord $g(x, z) >$ ord z. Evaluating (3.14) for x a unit, ord $m_\nu(x) \geq 0$. For $2 \leq \nu < p$, ord$(z^\nu/\nu!) > \nu e$. For $\nu \geq p$,

$$\operatorname{ord}\left(\frac{z^\nu}{\nu!}\right) > \frac{\nu e}{2} \tag{3.18}$$

for $p > 3$. Hence,

(3.19) LEMMA: *If $p > 3$, then* ord $g(x, z) \geq 2e$. ■

By (3.2) and (3.9),

$$\begin{aligned} \mathscr{A}_{31}^{(\varphi_1)}(x) = \frac{z^2}{2x^{2p}}\mathscr{A}_{11}(x) + \left(\frac{-z}{x^p} + \frac{z^2}{2x^{2p}}\right)\mathscr{A}_{21}(x) \\ + \mathscr{A}_{31}(x) + \sum_{\nu \geq 3} \frac{z^\nu}{\nu!} a_\nu(x) \end{aligned} \tag{3.20}$$

where ord $a_\nu(x) \geq 0$. By (3.18) for $p > 5$,

$$\mathscr{A}_{31}^{(\varphi_1)}(x) \equiv \frac{z^2}{2x^{2p}}\mathscr{A}_{11}(x) + \left(-\frac{z}{x^p} + \frac{z^2}{2x^{2p}}\right)\mathscr{A}_{21}(x) + \mathscr{A}_{31}(x) \pmod{p^{3e}}.$$

Since, ord $\mathscr{A}_{21}(x) > e$, ord $\mathscr{A}_{31}(x) > 2e$, and

$$z = x^p \frac{\mathscr{A}_{21}(x)}{\mathscr{A}_{11}(x)} + g(x, z)$$

with ord $g(x, z) \geq 2e$, therefore,

$$\mathscr{A}_{31}^{(\varphi_1)} \equiv \frac{2\mathscr{A}_{11}\mathscr{A}_{31} - \mathscr{A}_{21}^2}{2\mathscr{A}_{11}} \pmod{p^{3e}}.$$

In terms of the Frobenius matrix A [11(§1.4)],

$$\mathscr{A}_{31}^{(\varphi_1)} \equiv \frac{2A_{11}A_{31} - A_{21}^2}{2\mathscr{A}_{11}} \pmod{p^{3e}}.$$

By [11(§1.2)], the coefficients A_{i1} may be approximated by $\tilde{A}_{i1}$, ord $\tilde{A}_{i1} > (i-1)e$, ord$(A_{i1} - \tilde{A}_{i1}) \geq ie$ for ord $x > -(n+1)b$, where explicitly

$$\tilde{A}_{i1} = \pi^{-(i-1)} \sum_{t=0}^{\infty} \sum_{\ell} \sum (B_{p\alpha_1+\ell} B_{p\alpha_2+\ell} \cdots B_{p\alpha_n+\ell} B_\ell) x^t,$$

in which for each t, ℓ runs from 0 to $(n+1)t + p(i-1)$, and for $j = (t-\ell)/p \in \mathbf{Z}$, the inner sum ranges over n-tuples $(\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}^n$ such that $\Sigma_{k=1}^n \alpha_k = (n+1)j + (i-1)$, $p\alpha_k \geq -\ell$ for all k. It follows that

$$\mathscr{A}_{31}^{(\varphi_1)} \equiv \frac{2\tilde{A}_{11}\tilde{A}_{31} - \tilde{A}_{21}^2}{2\mathscr{A}_{11}} \pmod{p^{3e}}$$

for x a unit.

(3.21) LEMMA: *For $p \geq n+8$, $2\tilde{A}_{11}\tilde{A}_{31} - \tilde{A}_{21}^2$ is congruent* mod p^{3e} *to a non-trivial polynomial.*

PROOF: The usual estimates (0.7) for the constants B_i yield

$$2\tilde{A}_{11}\tilde{A}_{31} - \tilde{A}_{21}^2 \equiv \sum_{\mu=0}^{[p/(n+1)]} C_\mu x^\mu (= C(x)) \pmod{p^{3e}}$$

where

$$C_\mu = \frac{n+1}{\pi} \sum (2B_{2p+\lambda} B_\lambda^2 B_\gamma^{n+1} + nB_{p+\lambda}^2 B_\lambda^{n-1} B_\gamma^{n+1} - (n+1) B_{p+\lambda} B_{p+\gamma} B_\lambda^n B_\gamma^n) \tag{3.22}$$

the sum running over all $\lambda, \gamma \in \mathbf{Z}$, $\lambda + \gamma = \mu$, $0 \leq \lambda, \gamma \leq [p/(n+1)]$.

By (3.21), $C_0 = ((n+1)/\pi^2)\,(2B_{2p} - B_p^2)$ which is easily shown to be trivial mod p^{3e} (for $p \neq 2$). Similarly, C_1 may be computed from (3.20). Using the explicit values of the B_m, we compute

$$C_1 = (n+1)\pi^{2p+n-1}\left\{2\left(\frac{1}{(2p+1)!}+\frac{1}{(2p)!}-\frac{1}{p!(p+1)!}\right)\right.$$
$$\left. + n\left(\frac{1}{(p+1)!}-\frac{1}{p!}\right)^2\right\}.$$

Let $D = C_1/(n+1)\pi^{2p+n-1}$. It follows that $D \equiv n+2 \pmod p$, and D is a unit for $p > n+2$. Hence,

$$\operatorname{ord} C_1 = 2 + \frac{n+1}{p-1} < 3e$$

for $p \geq n+8$. ■

(3.23) THEOREM: *For $p \geq n+8$, an excellent lifting of Frobenius does not exist.*

PROOF: Since the coefficients of $C(x)$ belong to $\mathbb{Q}_p(\pi)$, therefore if t is a generic unit, then $|C(t)| = |C|_0(1)$ where the right side denotes the Gauss norm, the supremum of the p-adic magnitudes of the coefficients of C. Since C_1 is non-trivial mod p^{3e} clearly $C(t)$ is nontrivial mod p^{3e}. It follows that $\mathscr{A}_{31}^{(\varphi_1)}(t)$ is nontrivial and $\mathscr{A}_{31}^{(\varphi_1)}(x)$, a power series, is not identically zero. ■

REFERENCES

[1] P. DELIGNE: La Conjecture de Weil, I. *Publ. Math. I.H.E.S., 43,* (1973) 273–308.

[2] P. DELIGNE: Applications de la Formule des Traces aux Sommes Trigonométriques. *SGA* $4\frac{1}{2}$ *Springer Lectures Notes 569* (1977) Berlin.

[3] B. DWORK: On the Zeta Function of a Hypersurface. *Publ. Math. I.H.E.S., 12* (1962) 5–68.

[4] B. DWORK: p-Adic Cycles. *Publ. Math. I.H.E.S., 37* (1969) 27–115.

[5] B. DWORK: Normalized Period Matrices I. *Ann. of Math., 94* (1971) 337–388.

[6] B. DWORK: Normalized Period Matrices II. *Ann. of Math., 98* (1973) 1–57.

[7] B. DWORK: Bessel Functions as p-adic Functions of the Argument. *Duke Math. J., 41* (1974) 711–738.

[8] A. ERDELYI: Integraldarstellungen Hypergeometrisches Funktionen. *Quart. J. of Math., 8* (1937) 267–277.

[9] N. KATZ: On the Differential Equations Satisfied by Period Matrices. *Publ. Math. I.H.E.S., 35* (1968) 223–258.

[10] YU. MANIN: Theory of Commutative Formal Groups over Fields of Finite Characteristic. *Russian Math. Survey, 18* (1963) 1–83.

[11] S. SPERBER: p-Adic Hypergeometric Functions and Their Cohomology I. *Duke Math. Journal, 44* (1977) 535–589.
[12] A. WEIL: On Some Exponential Sums. *Proc. N.A.S., 31* (1948) 204–207.

(Oblatum 4-IV-1977 & 18-IX-1978)

Department of Mathematics
University of Illinois
Urbana, Illinois 61801

Current Address:
Department of Mathematics
University of Minnesota
Minneapolis, Minnesota 55455