Dwork Crystals I

Frits Beukers[1] and Masha Vlasenko[2],*

[1]Utrecht University, Department of Mathematics, P.O.Box 80.010, 3508 TA Utrecht, Netherlands and [2]Institute of Mathematics of the Polish Academy of Sciences, Śniadeckich 8, 00-656 Warsaw, Poland

*Correspondence to be sent to: e-mail: f.beukers@uu.nl

We present an elementary elaboration of Dwork's idea of explicit p-adic limit formulas for zeta functions of toric hypersurfaces.

1   Introduction

In his study of zeta-functions of families of algebraic varieties Dwork discovered a number of remarkable congruences for truncated solutions of Picard–Fuchs equations. For example, let

$$F(z) = \frac{1}{\pi} \int_1^\infty \frac{\mathrm{d}x}{\sqrt{x(x-1)(x-z)}} = \sum_{k \geq 0} \left(\frac{(1/2)_k}{k!} \right)^2 z^k$$

be the period function associated to the Legendre family of elliptic curves $y^2 = x(x-1)(x-z)$. Here $(1/2)_k$ denotes the Pochhammer symbol $\Gamma(k+1/2)/\Gamma(1/2)$. Let p be an odd prime and s a positive integer. Let F_{p^s} be the truncation of F given by

$$F_{p^s}(z) = \sum_{k=0}^{p^s-1} \left(\frac{(1/2)_k}{k!} \right)^2 z^k.$$

Let z_0 be a p-adic integer and suppose $F_p(z_0)$ is a p-adic unit. Then $F_{p^s}(z_0)$ is a p-adic unit for all $s \geq 1$ and we have

$$F_{p^{s+1}}(z_0)/F_{p^s}(z_0) \equiv F_{p^s}(z_0)/F_{p^{s-1}}(z_0) (\mathrm{mod}\ p^s).$$

The p-adic unit $\lambda(z_0) = (-1)^{\frac{p-1}{2}} \lim_{s \to \infty} F_{p^s}(z_0)/F_{p^{s-1}}(z_0)$ is a root of the zeta function of the elliptic curve corresponding to $z_0 (\mathrm{mod}\ p)$. (Though it looks slightly different, this fact is a version of [3, (6.29)].)

In a series of papers culminating in [8, Theorem 6.2], Katz developed a general theory of such congruences and their underlying mechanism. However, his congruences involve formal expansion coefficients of differential forms instead of truncated power series solutions of a differential equation. In this paper we consider a 3rd alternative, namely coefficients of certain powers of the polynomial defining a variety. For example, in the case of the Legendre elliptic curve they are given by

$$G_{p^s}(z) = \text{coefficient of } (xy)^{p^s-1} \text{ of } (y^2 - x(x-1)(x-z))^{p^s-1}.$$

Although different from $F_{p^s}(z)$, they both satisfy the hypergeometric differential equation modulo p^s. The congruences read

$$G_{p^{s+1}}(z_0)/G_{p^s}(z_0) \equiv G_{p^s}(z_0)/G_{p^{s-1}}(z_0)(\mathrm{mod}\ p^s)$$

and the quotients converge to the p-adic unit root $\lambda(z_0)$. In this paper we shall deal with a generalized version of the congruences of the latter type. A number of ideas in this paper are already present in [8], but in a very different language. There will also be no smoothness assumptions on the underlying variety. We plan to come back to the case of truncated power series solutions in a later paper.

Let R be a ring of characteristic zero and p a prime number. Suppose that we have a pth power Frobenius lift on R, which is a ring endomorphism $\sigma : R \to R$ with the property that $\sigma(r) \equiv r^p (\mathrm{mod}\ p)$ for all $r \in R$. For example, when $R = \mathbb{Z}$ is the ring of integers we can take $\sigma(r) = r$ for all r. When $R = \mathbb{Z}[t]$ is a polynomial ring we can take $\sigma(g(t)) = g(t^p)$.

Let $f(\mathbf{x}) = \sum_{i=1}^{N} f_i \mathbf{x}^{\mathbf{a}_i}$ be a Laurent polynomial in $x_1, \ldots, x_n$ with $f_i \in R$ for all i. Here we use the vector notation $\mathbf{x}^{\mathbf{e}} = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$. Let $\Delta \subset \mathbb{R}^n$ be the Newton polytope of $f(\mathbf{x})$, which is the convex hull of its support $\{\mathbf{a}_i : f_i \neq 0\}$. Let J be the set of interior lattice points in Δ and set $g = \#J$. We assume that $g > 0$. For any integer $m \geq 1$ we

define the $g \times g$-matrix β_m with entries

$$(\beta_m)_{\mathbf{u},\mathbf{v} \in J} := \text{coefficient of } \mathbf{x}^{m\mathbf{v}-\mathbf{u}} \text{ of } f(\mathbf{x})^{m-1}.$$

When $m = 1$ we take for β_m the identity matrix. We call β_p the *Hasse–Witt matrix* of f. When β_p is invertible modulo p it turns out that β_{p^s} is invertible modulo p for every $s \geq 1$. Note that being invertible modulo p implies being invertible modulo all powers of p.

In [11], it is shown that if the Hasse–Witt matrix is invertible modulo p, then

$$\beta_{p^{s+1}} \sigma(\beta_{p^s})^{-1} \equiv \beta_{p^s} \sigma(\beta_{p^{s-1}})^{-1} \pmod{p^s}$$

for every $s \geq 1$. One may observe that this congruence as similar to the last part of Theorem 6.2 in Katz's paper [8]. We believe that the merit of [11] is that the proof of the congruence is completely elementary.

Let δ be a derivation on R. Again in an elementary way, it is shown in [11] that if β_p is invertible in R, then

$$\delta(\beta_{p^{s+1}}) \beta_{p^{s+1}}^{-1} \equiv \delta(\beta_{p^s}) \beta_{p^s}^{-1} \pmod{p^s}$$

for every $s \geq 1$.

These congruences imply the existence, for each Frobenius lift σ and each derivation δ on R, of p-adic limit matrices Λ_σ and N_δ such that

$$\Lambda_\sigma = \lim_{s \to \infty} \beta_{p^s} \sigma(\beta_{p^{s-1}})^{-1} \text{ and } N_\delta = \lim_{s \to \infty} \delta(\beta_{p^s}) \beta_{p^s}^{-1}.$$

It is the goal of the present paper to give an interpretation of these matrices in terms of operations with regular rational functions on $\mathbb{T}^n \setminus Z_f$, the complement of the set of zeroes $Z_f = \{\mathbf{x} : f(\mathbf{x}) = 0\}$ in the n-dimensional torus $\mathbb{T}^n$. At the same time we provide an alternative proof of the congruences.

To be slightly more precise, we consider the R-module Ω_f of rational functions generated over R by

$$(u_0 - 1)! \frac{\mathbf{x}^{\mathbf{u}}}{f(\mathbf{x})^{u_0}},$$

where u_0 is a positive integer and $\mathbf{u} \in (u_0 \Delta) \cap \mathbb{Z}^n$. Any derivation δ on R can be extended naturally to Ω_f by setting $\delta(x_i) = 0$ for all i.

In this paper we construct the R-linear Cartier operator $\mathscr{C}_p : \widehat{\Omega}_f \to \widehat{\Omega}_{f^\sigma}$, where $\widehat{\Omega}_f = \varprojlim(\Omega_f/p^s\Omega_f)$ is the p-adic completion of Ω_f and $f^\sigma(\mathbf{x}) = \sum_{i=1}^{N} f_i^\sigma \, \mathbf{x}^{\mathbf{a}_i}$ is simply f with σ applied to its coefficients. The Cartier operator commutes with any derivation δ of R.

The main results of this paper are Theorems 4.3 and 5.3. Applied to the open set $\mu = \Delta^\circ$ of interior points of Δ, they describe a free rank g subquotient $Q_f = Q_f(\Delta^\circ)$ of Ω_f to which the Cartier operator descends and Λ_σ is the (transposed) matrix that corresponds to the R-linear map $\mathscr{C}_p : Q_f \to Q_{f^\sigma}$. As a bonus of our considerations we also recover a version of Katz's theorem [8, Theorem 6.2] as Theorem 5.7.

Finally in this introduction we point out the connection with the de Rham cohomology of the complement of Z_f. Define the modules $\Omega_f^n = \Omega_f \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$ and $\Omega_f^{n-1} = \oplus_{i=1}^{n} \Omega_f \frac{dx_1}{x_1} \wedge \cdots \frac{\check{dx_i}}{x_i} \cdots \wedge \frac{dx_n}{x_n}$ of differential n- and $n-1$-forms, respectively. The above-mentioned R-module Q_f is in fact a (p-adic) subquotient of

$$\mathscr{W}_f := \Omega_f^n/d(\Omega_f^{n-1}).$$

We call the latter the *Dwork module*. It is known due to the work of Griffiths and Batyrev that, when R is a field and f satisfies certain regularity conditions (so called Δ-*regularity*), then $\mathscr{W}_f$ is isomorphic to the middle de Rham cohomology $H_{dR}^n(\mathbb{T}^n \setminus Z_f)$ (see Corollary A.4 and [1, Theorem 7.13]). In particular, it is a vector space over R of finite dimension. In this paper we will not assume regularity. We also will not assume that the Newton polytope $\Delta \subset \mathbb{R}^n$ is of maximal dimension.

2   Regular Functions and Formal Expansion

Let R be a characteristic zero domain, $f \in R[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ be a Laurent polynomial and $\Delta \subset \mathbb{R}^n$ be its Newton polytope. By $C(\Delta)$ we denote the subset of $\mathbb{R}^{n+1}$ given by

$$C(\Delta) = \{\lambda(1, u_1, \ldots, u_n) \,|\, (u_1, \ldots, u_n) \in \Delta, \lambda \geq 0\}, \tag{1}$$

the positive cone spanned by the Newton polytope Δ placed in $\mathbb{R}^{n+1}$ in the hyperplane $u_0 = 1$.

The set of integral points $C(\Delta) \cap \mathbb{Z}^{n+1}$ is denoted by $C(\Delta)_\mathbb{Z}$. Let $C(\Delta)_\mathbb{Z}^+ = C(\Delta)_\mathbb{Z} \setminus \{\mathbf{0}\}$ be the set of non-zero integral points in the cone. For any $(u_0, u_1, \ldots, u_n) = \mathbf{u} \in C(\Delta)_\mathbb{Z}$ we denote $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} \cdots x_n^{u_n}$ (we simply drop the component u_0 here, as there is no respective

variable x_0). Consider the R-module Ω_f of regular rational functions generated over R by

$$\omega_{\mathbf{u}} := (u_0 - 1)! \, \frac{\mathbf{x}^{\mathbf{u}}}{f(\mathbf{x})^{u_0}}$$

for all $\mathbf{u} \in C(\Delta)_{\mathbb{Z}}^+$. Note that 1 is an R-linear combination of $\omega_{\mathbf{u}}$ with $u_0 = 1$, so the constant functions are also in Ω_f.

We define the module $d\Omega_f$ as the R-span of all derivatives $x_i \frac{\partial}{\partial x_i} \omega$ with $\omega \in \Omega_f$ and $1 \le i \le n$. Note that $d\Omega_f \subset \Omega_f$. The quotient R-module

$$\mathscr{W}_f := \Omega_f / d\Omega_f,$$

will be called the *Dwork module*.

Remark 2.1. Having the extra factor $(u_0 - 1)!$ in the definition of $\omega_{\mathbf{u}}$ appears to be essential in many ways when working over rings R (rather than fields). At the end of the introduction we mentioned that the Dwork module can be also written in terms of differential forms as $\mathscr{W}_f = \Omega_f^n / d(\Omega_f^{n-1})$. Factors $(u_0 - 1)!$ in $\omega_{\mathbf{u}}$ allow the so-called Griffiths–Dwork reduction when we work in $\mathscr{W}_f$. This is the procedure to reduce the pole order of a form by shifting it by exact forms. More concretely, suppose we have a form of the shape $k! \frac{g(\mathbf{x})}{f^{k+1}} \frac{d\mathbf{x}}{\mathbf{x}}$ and there exist Laurent polynomials $g_0(\mathbf{x}), g_1(\mathbf{x}), \dots, g_n(\mathbf{x})$ with support in $k\Delta$ such that $g = g_0 f + \sum_{i=1}^n g_i x_i \frac{\partial f}{\partial x_i}$. Then

$$
\begin{aligned}
k! \frac{g(\mathbf{x})}{f^{k+1}} \frac{d\mathbf{x}}{\mathbf{x}} &= k! \frac{g_0}{f^k} \frac{d\mathbf{x}}{\mathbf{x}} + \sum_{i=1}^n k! \frac{g_i}{f^{k+1}} x_i \frac{\partial f}{\partial x_i} \frac{d\mathbf{x}}{\mathbf{x}} \\
&= k! \frac{g_0}{f^k} \frac{d\mathbf{x}}{\mathbf{x}} + \sum_{i=1}^n (k-1)! \frac{x_i}{f^k} \frac{\partial g_i}{\partial x_i} \\
&\quad + \sum_{i=1}^n (-1)^i d\left((k-1)! \frac{g_i}{f^k} \frac{dx_1}{x_1} \wedge \cdots \frac{\overset{\vee}{dx_i}}{x_i} \cdots \wedge \frac{dx_n}{x_n} \right) \\
&\equiv k! \frac{g_0}{f^k} \frac{d\mathbf{x}}{\mathbf{x}} + \sum_{i=1}^n (k-1)! \frac{x_i}{f^k} \frac{\partial g_i}{\partial x_i} \quad (\mathrm{mod}\ d(\Omega_f^{n-1})).
\end{aligned}
$$

The final form is again in Ω_f^n. Note that factorials appear in the Laplace transform in [1, §7].

Rational functions can be expanded as formal Laurent series. To that end we fix a vertex $\mathbf{b}$ of Δ and *assume that the coefficient of f at $\mathbf{x}^{\mathbf{b}}$ is a unit in R*. Denote this coefficient by $f_{\mathbf{b}}$ and expand rational functions as

$$\frac{g(\mathbf{x})}{f(\mathbf{x})^m} = \frac{g(\mathbf{x})\mathbf{x}^{-m\mathbf{b}}}{f_{\mathbf{b}}^m(1+\ldots)^m} = \frac{g(\mathbf{x})\mathbf{x}^{-m\mathbf{b}}}{f_{\mathbf{b}}^m}\sum_{k\geq 0} h_k(\mathbf{x}),$$

where $h_k(\mathbf{x})$ are Laurent polynomials supported in $k(\Delta - \mathbf{b})$ for every k. There are only finitely many summands contributing to each monomial in the cone $C(\Delta - \mathbf{b}) \subseteq \mathbb{R}^n$. Observe that when $g(\mathbf{x})$ is supported in $m\Delta$ the formal series in the right-hand side is itself supported in $C(\Delta - \mathbf{b})$. (Here we need a word of caution regarding our notation. In (1) the polytope Δ was placed in the hyperplane $u_0 = 1$ in $\mathbb{R}^{n+1}$, which will be our usual convention throughout the paper. Note that, with this convention, the difference $\Delta - \mathbf{b}$ is a polytope in the hyperplane $u_0 = 0$ and one can view the respective cone $C(\Delta - \mathbf{b})$ as a subset of this hyperplane $\{u_0 = 0\} \cong \mathbb{R}^n$.) Denote the ring of formal Laurent series with support in $C(\Delta - \mathbf{b})$ and coefficients in R by

$$\Omega_{\text{formal}} = \left\{ \sum_{\mathbf{k}\in C(\Delta-\mathbf{b})} a_{\mathbf{k}}\mathbf{x}^{\mathbf{k}} \;\middle|\; a_{\mathbf{k}} \in R \right\}.$$

It is indeed a ring because the cone has $\mathbf{0}$ as a vertex. The above-explained procedure of formal expansion defines an embedding of Ω_f into Ω_{formal} as an R-submodule. Note that we do not include the choice of $\mathbf{b}$ in the notation Ω_{formal}.

Similarly to $\mathrm{d}\Omega_f$, the R-module of *formal derivatives* $\mathrm{d}\Omega_{\text{formal}}$ is defined as the R-span of derivatives $x_i\frac{\partial}{\partial x_i}\omega$ with $1 \leq i \leq n$ and $\omega \in \Omega_{\text{formal}}$.

Lemma 2.2.   A series $\sum_{\mathbf{k}\in C(\Delta-\mathbf{b})} a_{\mathbf{k}}\mathbf{x}^{\mathbf{k}}$ is a formal derivative if and only if

$$a_{\mathbf{k}} \equiv 0(\mathrm{mod}\ \gcd(k_1,\ldots,k_n)) \quad \text{for all } \mathbf{k}.$$

Proof.   Notice that for any monomial $\mathbf{x}^{\mathbf{k}}$, any i and any $a \in R$ we have

$$x_i\frac{\partial}{\partial x_i}\left(a\mathbf{x}^{\mathbf{k}}\right) = ak_i\mathbf{x}^{\mathbf{k}} \equiv 0(\mathrm{mod}\ k_i).$$

This shows the $\Rightarrow$ part. To see the reverse implication, write $\gcd(k_1,\ldots,k_n) = \sum_i m_i k_i$ for some $m_i \in \mathbb{Z}$ and note that

$$\sum_i m_i x_i \frac{\partial \mathbf{x}^{\mathbf{k}}}{\partial x_i} = \gcd(k_1,\ldots,k_n)\mathbf{x}^{\mathbf{k}}.$$

$\blacksquare$

3 Cartier Operator

Let us fix a prime number p. We define the Cartier operator $\mathscr{C}_p$ on Ω_{formal} by

$$\mathscr{C}_p\left(\sum_{\mathbf{k}} a_{\mathbf{k}}\mathbf{x}^{\mathbf{k}}\right) := \sum_{\mathbf{k}} a_{p\mathbf{k}}\mathbf{x}^{\mathbf{k}}. \tag{2}$$

Although acting on different spaces, this operation was already used in early papers of Dwork (see ψ in [4, §2]) and Reich (see Ψ in [9, §(b)]).

From now on we *assume that* $\cap_s p^s R = \{0\}$, in which case we have a well defined p-adic valuation

$$\operatorname{ord}_p(r) = \sup\left\{s \in \mathbb{Z}_{\geq 0} : r \in p^s R\right\}$$

on R which extends the usual p-adic valuation on $\mathbb{Z} \subset R$. This valuation takes finite values on all non-zero elements of R and satisfies the inequalities $\operatorname{ord}_p(r_1 r_2) \geq \operatorname{ord}_p(r_1) + \operatorname{ord}_p(r_2)$ and $\operatorname{ord}_p(r_1 + r_2) \geq \min(\operatorname{ord}_p(r_1), \operatorname{ord}_p(r_2))$. We also *assume that R is p-adically complete*. In particular, R is a $\mathbb{Z}_p$-algebra and Lemma 2.2 can be reformulated as

Lemma 3.1. A series $h \in \Omega_{\text{formal}}$ is a formal derivative if and only if $\mathscr{C}_p^s(h) \equiv 0 \pmod{p^s}$ for all integers $s \geq 1$.

One easily shows that $\mathscr{C}_p \circ \theta_i = p\,\theta_i \circ \mathscr{C}_p$ for any $\theta_i = x_i\frac{\partial}{\partial x_i}$. We thus observe that the Cartier operator preserves the submodule of formal derivatives and is divisible by p on it, that is,

$$\mathscr{C}_p : \mathrm{d}\Omega_{\text{formal}} \to p\,\mathrm{d}\Omega_{\text{formal}}. \tag{3}$$

Applying this commutation identity s times yields $\mathscr{C}_p^s \circ \theta_i = p^s \theta_i \circ \mathscr{C}_p^s$, which immediately gives one of the implications in the last lemma. Here is another straightforward property of $\mathscr{C}_p$:

Lemma 3.2. Let $g, h \in \Omega_{\text{formal}}$. Then $\mathscr{C}_p(g(\mathbf{x}^p)h) = g(\mathbf{x})\mathscr{C}_p(h)$.

Since Cartier operators are usually defined mod p in the literature, naming $\mathscr{C}_p$ a Cartier lift might be more appropriate. Nevertheless, we prefer to call it the Cartier operator.

We now like to restrict the Cartier operator to Ω_f. We will need the p-adic completion $\widehat{\Omega}_f := \varprojlim \Omega_f / p^s \Omega_f$. Fix a Frobenius lift σ on R: this is a ring endomophism $\sigma : R \to R$ such that $\sigma(r) \equiv r^p \pmod{p}$ for every $r \in R$. Our main observation is that

Proposition 3.3.   If $p > 2$ then $\mathscr{C}_p(\Omega_f) \subset \widehat{\Omega}_{f^\sigma}$.

Proof.   To see this, rewrite $1/f(\mathbf{x})^{u_0}$ as $f(\mathbf{x})^{p\lceil u_0/p \rceil - u_0}/f(\mathbf{x})^{p\lceil u_0/p \rceil}$. Then note that $f(\mathbf{x})^p = f^\sigma(\mathbf{x}^p) - pG(\mathbf{x})$ for some Laurent polynomial G with coefficients in R and support in $p\Delta$. Then we use the p-adic expansion

$$\frac{\mathbf{x}^\mathbf{u}}{f(\mathbf{x})^{u_0}} = \frac{\mathbf{x}^\mathbf{u} f(\mathbf{x})^{p\lceil u_0/p \rceil - u_0}}{(f^\sigma(\mathbf{x}^p) - pG(\mathbf{x}))^{\lceil u_0/p \rceil}} = \sum_{r \geq 0} p^r \binom{\lceil u_0/p \rceil + r - 1}{r} \frac{G(\mathbf{x})^r}{f^\sigma(\mathbf{x}^p)^{r + \lceil u_0/p \rceil}} \mathbf{x}^\mathbf{u} f(\mathbf{x})^{p\lceil u_0/p \rceil - u_0}.$$

Multiply this with $(u_0 - 1)!$ and apply $\mathscr{C}_p$. Using Lemma 3.2 we find that

$$\mathscr{C}_p(\omega_\mathbf{u}) = \sum_{r \geq 0} \frac{p^r}{r!} \frac{(u_0 - 1)!}{(\lceil u_0/p \rceil - 1)!} (\lceil u_0/p \rceil + r - 1)! \frac{Q_r(\mathbf{x})}{f^\sigma(\mathbf{x})^{r + \lceil u_0/p \rceil}},$$

where the $Q_r(\mathbf{x}) = \mathscr{C}_p(G(\mathbf{x})^r \mathbf{x}^\mathbf{u} f(\mathbf{x})^{p\lceil u_0/p \rceil - u_0})$ are Laurent polynomials in $x_1, \ldots, x_n$ with support in $(\lceil u_0/p \rceil + r)\Delta$ and coefficients in R. The last formula can be rewritten as

$$\mathscr{C}_p(\omega_\mathbf{u}) = \sum_{\mathbf{v} \in C(\Delta)_{\mathbb{Z}}^+} F_{\mathbf{u},\mathbf{v}} \omega_\mathbf{v}^\sigma, \tag{4}$$

where

$$F_{\mathbf{u},\mathbf{v}} = \begin{cases} \frac{p^r}{r!} \frac{(u_0-1)!}{(\lceil u_0/p \rceil - 1)!} \times \text{ coefficient of } \mathbf{x}^\mathbf{v} \text{ in } Q_r(\mathbf{x}), & r := v_0 - \lceil u_0/p \rceil \geq 0, \\ 0, & v_0 < \lceil u_0/p \rceil. \end{cases} \tag{5}$$

To show that $\mathscr{C}_p(\omega_\mathbf{u}) \in \widehat{\Omega}_{f^\sigma}$ it suffices to show that $\mathrm{ord}_p(F_{\mathbf{u},\mathbf{v}}) \to \infty$ as $v_0 \to \infty$. To that end we observe that

$$\mathrm{ord}_p(F_{\mathbf{u},\mathbf{v}}) \geq r - \mathrm{ord}_p(r!) + \mathrm{ord}_p\left(\frac{(u_0 - 1)!}{(\lceil u_0/p \rceil - 1)!}\right).$$

It is straightforward to see that $\frac{(u_0-1)!}{(\lceil u_0/p \rceil - 1)!}$ has order $\geq \lceil u_0/p \rceil - 1$ and that $\mathrm{ord}_p(r!) < \frac{r}{p-1}$. This gives us

$$\mathrm{ord}_p(F_{\mathbf{u},\mathbf{v}}) \geq r + \lceil u_0/p \rceil - 1 - \frac{r}{p-1} = v_0 - 1 - \frac{r}{p-1} \geq \frac{p-2}{p-1}(v_0 - 1). \tag{6}$$

The latter goes to ∞ with v_0 when $p > 2$. ∎

From now on we assume that $p > 2$. By Proposition 3.3 we have a well-defined R-linear map

$$\mathscr{C}_p : \widehat{\Omega}_f \to \widehat{\Omega}_{f^\sigma}. \tag{7}$$

It is in fact given by the explicit formulas (4) and (5), which also show that the map (7) is independent of the choice of vertex $\mathbf{b}$ of Δ at which we are doing formal expansions.

We shall also be interested in regular functions supported in subsets of the cone $C(\Delta)$. For a subset $\mu \subseteq \Delta$ let us denote by

$$\Omega_f(\mu) \subseteq \Omega_f$$

the R-module generated by functions $\omega_{\mathbf{u}}$ with $\mathbf{u} \in C(\mu)_{\mathbb{Z}}^+$. Here $C(\mu) \subseteq C(\Delta)$ is the positive cone spanned by μ placed in $\mathbb{R}^{n+1}$ in the hyperplane $u_0 = 1$, and $C(\mu)_{\mathbb{Z}} = C(\mu) \cap \mathbb{Z}^{n+1}$ is the set of integral points in this cone and $C(\mu)_{\mathbb{Z}}^+ = C(\mu)_{\mathbb{Z}} \setminus \{\mathbf{0}\}$ is the set of non-zero integral points. Note that $\Omega_f(\Delta) = \Omega_f$. The respective p-adic completion is denoted $\widehat{\Omega}_f(\mu) = \varprojlim \Omega_f(\mu)/p^s \Omega_f(\mu)$.

Proposition 3.4. Define a finite topology on Δ, where the closed sets are unions of faces of any dimension. Let $\mu \subset \Delta$ be an open set. Then the Cartier operator $\mathscr{C}_p$ maps $\widehat{\Omega}_f(\mu)$ into $\widehat{\Omega}_{f^\sigma}(\mu)$ and derivations of R map $\Omega_f(\mu)$ to itself.

Proof. Since open sets are intersections of the complements of faces, it is enough to prove our statement for μ being such a complement. Without loss of generality we assume that μ^c is a face of Δ. In this case $C(\mu) = \Sigma^c = C(\Delta) \setminus \Sigma$ where $\Sigma = C(\mu^c)$ is the respective face of the cone $C(\Delta)$. The R-module $\Omega_f(\mu)$ is generated by functions $\omega_{\mathbf{u}}$ with $\mathbf{u} \in \Sigma^c$. To prove our proposition we recall that the Cartier operator (6) is given explicitly by formula (3) and one easily sees that $\mathbf{u} \in \Sigma^c$ and $F_{\mathbf{u},\mathbf{v}} \neq 0$ imply $\mathbf{v} \in \Sigma^c$.

Let δ be a derivation of R and $\mathbf{u} \in C(\mu)_{\mathbb{Z}}$. Observe that in the formula

$$\delta(\omega_{\mathbf{u}}) = -u_0! \frac{\mathbf{x}^{\mathbf{u}} \delta(f)(\mathbf{x})}{f(\mathbf{x})^{u_0+1}} \frac{d\mathbf{x}}{\mathbf{x}}$$

the support of $\mathbf{x}^{\mathbf{u}} \delta(f)$ is in $\mathbf{u} + \Delta$, which again lies in $C(\mu)$ when μ is open in our sense. ∎

Definition 3.5. Fix a non-empty subset $\mu \subseteq \Delta$ that is *open* in the topology from Proposition 3.4. Let $\mu_{\mathbb{Z}} = \mu \cap \mathbb{Z}^n$ be the set of integral points in μ. We assume this set is non-empty and let $h = \#\mu_{\mathbb{Z}}$ be the number of such points. For any integer $m \geq 1$

we define the $h \times h$-matrix $\beta_m = \beta_m(\mu)$ with entries

$$(\beta_m)_{\mathbf{u},\mathbf{v}\in\mu_{\mathbb{Z}}} := \text{coefficient of } \mathbf{x}^{m\mathbf{v}-\mathbf{u}} \text{ of } f(\mathbf{x})^{m-1}. \tag{8}$$

When $m = 1$ we take for $\beta_1(\mu)$ the identity matrix. We call $\beta_p(\mu)$ the *Hasse–Witt matrix of f relative to* μ.

Proposition 3.6.   Suppose that $p > 2$ and $\mu \subseteq \Delta$ is a non-empty subset which is *open* in the topology defined in Proposition 3.4. Then

$$\mathscr{C}_p(\widehat{\Omega}_f(\mu)) \subseteq \text{Span}_R(\omega_{\mathbf{u}}^\sigma)_{\mathbf{u}\in\mu_{\mathbb{Z}}} + p\,\widehat{\Omega}_{f^\sigma}(\mu).$$

Moreover, for any $\mathbf{u} \in \mu_{\mathbb{Z}}$ we have

$$\mathscr{C}_p(\omega_{\mathbf{u}}) \equiv \sum_{\mathbf{v}\in\mu_{\mathbb{Z}}} (\beta_p)_{\mathbf{u},\mathbf{v}}\omega_{\mathbf{v}}^\sigma \quad (\text{mod } p\widehat{\Omega}_{f^\sigma}(\mu)).$$

Proof.   From the proof of Propositions 3.3 and 3.4, in particular equations (4) and (5), we know an expression for $\mathscr{C}_p(\omega_{\mathbf{u}})$ as a linear combination $\sum_{\mathbf{v}\in C(\mu)_{\mathbb{Z}}^+} F_{\mathbf{u},\mathbf{v}}\omega_{\mathbf{v}}^\sigma$ for every $\mathbf{u} \in \mu_{\mathbb{Z}}$. Moreover, it follows from (6) that $F_{\mathbf{u},\mathbf{v}} \equiv 0(\text{mod } p)$ when $v_0 > 1$. Our 1st statement follows immediately. The observation that $(\beta_p)_{\mathbf{u},\mathbf{v}} \equiv F_{\mathbf{u},\mathbf{v}}(\text{mod } p)$ whenever $v_0 = 1$ proves the 2nd statement. ∎

4 The Unit-Root Crystal

In this section we formulate the 1st main result of this paper. But first we need some preparations.

Definition 4.1.   For a non-empty subset $\mu \subseteq \Delta$ that is *open* in the topology from Proposition 3.4, define $U_f(\mu) = \widehat{\Omega}_f(\mu) \cap d\Omega_{\text{formal}}$.

We call $U_f(\mu)$ the *submodule of formal derivatives*. Differential n-forms associated to elements of $U_f(\mu)$ were called forms that "die on formal expansion" by Nick Katz in [8, p.258]. It turns out that one can give a characterization of $U_f(\mu)$, which does not make any reference to Ω_{formal}:

Proposition 4.2.   With the notations as above we have

$$U_f(\mu) = \{\omega \in \widehat{\Omega}_f(\mu) \mid \mathscr{C}_p^s(\omega) \equiv 0 (\mathrm{mod}\ p^s \widehat{\Omega}_{f^{\sigma^s}}(\mu)) \text{ for all } s \geq 1\}. \tag{9}$$

Proof.   Let $\omega \in \widehat{\Omega}_f(\mu)$. Suppose that $\mathscr{C}_p^s(\omega) \equiv 0 (\mathrm{mod}\ p^s \widehat{\Omega}_{f^{\sigma^s}}(\mu))$ for all $s \geq 1$. Then it follows from Lemma 3.1 that $\omega \in d\Omega_{\mathrm{formal}}$.

Suppose conversely that $\omega \in \widehat{\Omega}_f(\mu) \cap d\Omega_{\mathrm{formal}}$. From the 1st part of Proposition 3.6 it follows that $\mathscr{C}_p(\omega) = \frac{A(\mathbf{x})}{f^\sigma(\mathbf{x})} + p\omega_1$ for some $\omega_1 \in \widehat{\Omega}_{f^\sigma}(\mu)$ and $A(\mathbf{x})$ a Laurent polynomial with support in $\mu_{\mathbb{Z}}$. Since $\omega \in d\Omega_{\mathrm{formal}}$ we have that the Laurent series of $\mathscr{C}_p(\omega)$ is divisible by p. This implies that p divides $A(\mathbf{x})$. Hence, $\mathscr{C}_p(\omega) = p\omega_2$ with $\omega_2 = \omega_1 + A(\mathbf{x})/pf^\sigma(\mathbf{x}) \in \widehat{\Omega}_{f^\sigma}(\mu)$. Applying this observation recursively then yields $\mathscr{C}_p^s(\omega) \in p^s \widehat{\Omega}_{f^{\sigma^s}}(\mu)$, which ends our proof.   ∎

It is clear from Definition 4.1 that the Cartier operator preserves this submodule and is divisible by p on it, that is, we have

$$\mathscr{C}_p : U_f(\mu) \to p\, U_{f^\sigma}(\mu).$$

Recall that the Cartier operator commutes with the connection operations for all derivations δ of R. It is then immediate from Definition 4.1 that all δ preserve $U_f(\mu)$. In other words, $U_f(\mu)$ is a differential submodule of $\widehat{\Omega}_f(\mu)$.

Theorem 4.3.   Assume that the Hasse–Witt matrix $\beta_p(\mu)$ is invertible in R. Then the quotient

$$Q_f(\mu) := \widehat{\Omega}_f(\mu)/d\Omega_{\mathrm{formal}}$$

is a free R-module of rank $h = \#\mu_{\mathbb{Z}}$ with a basis given by the images of $\omega_{\mathbf{u}}, \mathbf{u} \in \mu_{\mathbb{Z}}$.

Strictly speaking, the quotient $\widehat{\Omega}_f(\mu)/d\Omega_{\mathrm{formal}}$ should be read as $\widehat{\Omega}_f(\mu)/U_f(\mu)$ since $U_f(\mu) = \widehat{\Omega}_f(\mu) \cap d\Omega_{\mathrm{formal}}$. We prefer to use the former, more suggestive, notation.

Remark 4.4.   Recall that we work under assumptions that $\cap_s p^s R = \{0\}$ and R is p-adically complete, in which case an element of R is invertible if and only if it is invertible modulo p. Indeed, if $uv = 1 + pw$ then the inverse element is given by $u^{-1} = v(1 + pw)^{-1} = \sum_{k \geq 0}(-p)^k v w^k$. With this observation, we conclude from Theorem 4.3 and

Proposition 3.6 that the Cartier operator on the quotients

$$\mathscr{C}_p : Q_f(\mu) \to Q_{f^\sigma}(\mu)$$

is invertible because its matrix in the bases $\{\omega_{\mathbf{u}}\}, \{\omega_{\mathbf{u}}^\sigma\}$ is congruent modulo p to the (transposed) Hasse–Witt matrix $\beta_p(\mu)$.

Later we will give an explicit p-adic formula for the Cartier matrices on the quotients $Q_f(\mu)$ using matrices $\beta_{p^s}(\mu)$ for $s \geq 1$ (see Theorem 5.3). The proof of Theorem 4.3 exploits the p-adic contraction property of the Cartier operator from Proposition 3.6. The main argument is essentially contained in the following

Proposition 4.5.   Let $M_0, M_1, M_2, \ldots$ be an infinite sequence of R-modules and $\phi_i : M_{i-1} \to M_i$ R-linear maps for all $i \geq 1$. Suppose that $\cap_{s \geq 1} p^s M_i = \{0\}$ for all i. For each i let N_i be a submodule of M_i such that $\phi_i(M_{i-1}) \subset N_i + pM_i$ for all $i \geq 1$. Suppose that $N_i \cap pM_i = pN_i$ (equivalently, M_i/N_i is p-torsion free) and the induced maps $\phi_i : N_{i-1}/pN_{i-1} \to N_i/pN_i$ are isomorphisms for all $i \geq 1$. Define submodules

$$U_i = \{\omega \in M_i | \phi_{i+s} \circ \phi_{i+s-1} \circ \cdots \circ \phi_{i+1}(\omega) \equiv 0 (\mathrm{mod}\ p^s M_{i+s}) \text{ for all } s \geq 1\} \subset M_i.$$

Then, for all i,

(i) $M_i = N_i + U_i$.
(ii) $\phi_i(U_{i-1}) \subset pU_i$.
(iii) $\phi_i(M_{i-1}) \subset N_i + pU_i$.
(iv) $N_i \cap U_i = \{0\}$.

Proof.   Note that (ii) is an immediate consequence of the definition of U_i's. Indeed, for $\omega \in U_{i-1}$ the element $\omega_1 \in M_i$ such that $\phi_i(\omega) = p\omega_1$ satisfies $\phi_{i+s} \circ \cdots \circ \phi_{i+1}(\omega_1) = \frac{1}{p}\phi_{i+s} \circ \cdots \circ \phi_i(\omega) \in p^s M_{i+s}$ for all $s \geq 1$.

Let us show that (iii) follows easily from (i). For any $\omega \in M_{i-1}$ write $\phi_i(\omega) = \omega_1 + p\omega_1'$ with $\omega_1 \in N_i$, $\omega_1' \in M_i$. Using (i) we can write $\omega_1' = v_1 + u_1$ with $v_1 \in N_i$, $u_1 \in U_i$. Thus, we get $\phi_i(\omega) = \omega_1 + v_1 + pu_1 \in N_i + pU_i$.

Proof of (i). Clearly it is enough to do it for $i = 0$.

Consider ϕ_i modulo p, which is a map from M_{i-1}/pM_{i-1} to M_i/pM_i. By the assumption that $\phi_i(M_{i-1}) \subset N_i + pM_i$, the image of $\phi_i (\mathrm{mod}\ p)$ lies in $N_i/(N_i \cap pM_i)$. Since we also assume that $N_i \cap pM_i = pN_i$, the image of $\phi_i (\mathrm{mod}\ p)$ lies in N_i/pN_i. Restricting

$\phi_i(\mathrm{mod}\ p)$ to N_{i-1}/pN_{i-1} we obtain what we call *the induced map* $\phi_i : N_{i-1}/pN_{i-1} \to N_i/pN_i$. It is assumed that this induced map is invertible for each i, and hence the composition $\psi_i := \phi_i \circ \cdots \phi_2 \circ \phi_1 : N_0/pN_0 \to N_i/pN_i$ is an isomorphism for all $i \geq 1$. Define for each $s \geq 1$

$$U_0^{(s)} = \{\omega \in M_0 | \psi_t(\omega) \in p^t M_t \text{ for all } t \leq s\}$$

and $U_0^{(0)} = M_0$. In particular observe that $U_0^{(s+1)} \subset U_0^{(s)}$ for all $s \geq 0$. We first show that $U_0^{(s)} = U_0^{(s+1)} + p^s N_0$ for all $s \geq 0$. Let $\omega \in U_0^{(s)}$. Then $\omega_s := p^{-s}\psi_s(\omega) \in M_s$. By our assumptions there exists $\eta_s \in N_s$ such that $\phi_{s+1}(\eta_s) \equiv \phi_{s+1}(\omega_s)(\mathrm{mod}\ pM_{s+1})$. Choose $\eta_0 \in N_0$ such that $\psi_s(\eta_0) \equiv \eta_s(\mathrm{mod}\ pM_s)$. Then,

$$\begin{aligned}\psi_{s+1}(\omega - p^s\eta_0) &\equiv \phi_{s+1}(p^s\omega_s - p^s\eta_s)(\mathrm{mod}\ p^{s+1}M_{s+1})\\ &\equiv p^s(\phi_{s+1}(\omega_s) - \phi_{s+1}(\eta_s))(\mathrm{mod}\ p^{s+1}M_{s+1})\\ &\equiv 0(\mathrm{mod}\ p^{s+1}M_{s+1}).\end{aligned}$$

Hence, $\omega - p^s\eta_0 \in U_0^{(s+1)}$.

Let $\omega \in M_0$. For $s \geq 1$ we define $\omega_s \in U_0^{(s)}$ inductively via $\omega_s = \omega_{s+1} + p^s\eta_s$, $\eta_s \in N_0$. One easily sees that $\omega - \sum_{s\geq 1} p^s\eta_s \in \cap_{s\geq 1}U_0^{(s)} = U_0$. Hence, we conclude that $M_0 = N_0 + U_0$.

We finally show that $N_0 \cap U_0$ is trivial. Suppose, on the contrary, that $\omega \in N_0 \cap U_0$ and $\omega \neq 0$. Because $\cap_{s\geq 1}p^s M_0 = \{0\}$ there exists $s \geq 0$ such that $p^{-s}\omega \in M_0 \setminus pM_0$. Since M_0/N_0 is p-torsion free this implies that $p^{-s}\omega \in N_0 \setminus pM_0$. Since $\psi_i : N_0/pN_0 \to N_i/pN_i$ is an isomorphism we have that $\psi_i(p^{-s}\omega) \notin pM_i$ for all i. In particular for $i = s + 1$ we get $\psi_{s+1}(p^{-s}\omega) \notin pM_{s+1}$. Hence, $\psi_{s+1}(\omega) \notin p^{s+1}M_{s+1}$. This contradicts the fact that $\omega \in U_0$. Thus, we get a contradiction and conclude that $N_0 \cap U_0$ is trivial. ∎

Proof of Theorem 4.3. We apply Proposition 4.5 to $M_i = \widehat{\Omega}_{f^{\sigma^i}}(\mu)$ and $\phi_i = \mathscr{C}_p$ for all $i \geq 0$. For N_i we take the $\mathrm{Span}_R(\omega_{\mathbf{u}}^{\sigma^i})_{\mathbf{u}\in\mu_{\mathbb{Z}}}$. The property $N_i \cap pM_i = pN_i$ clearly holds. Proposition 3.6 states that $\phi_i(M_i) \subset N_i + pM_i$ and the matrix of $\phi_i : N_{i-1}/pN_{i-1} \to N_i/pN_i$ is given by $\beta_p^{\sigma^{i-1}}(\mu)$ modulo p, which is invertible by the assumption in Theorem 4.3. So the assumptions of Proposition 4.5 are satisfied.

From Proposition 4.2 we find that $U_0 = U_f(\mu)$. Then application of parts (i) and (iv) of Proposition 4.5 shows that

$$\widehat{\Omega}_f(\mu) = \mathrm{Span}_R(\omega_{\mathbf{u}})_{\mathbf{u}\in\mu_{\mathbb{Z}}} \oplus U_f(\mu)$$

as R-modules. Hence, $Q_f(\mu) \cong \mathrm{Span}_R(\omega_{\mathbf{u}})_{\mathbf{u}\in\mu_{\mathbb{Z}}}$. ∎

Remark 4.6.   Parts (iii) and (iv) in Proposition 4.5 imply that

$$\mathscr{C}_p(\widehat{\Omega}_f(\mu)) \subset \mathrm{Span}_R(\omega_{\mathbf{u}}^\sigma)_{\mathbf{u}\in\mu_{\mathbb{Z}}} \oplus p\, U_{f^\sigma}(\mu).$$

Remark 4.7.   Theorem 4.3 is not true if we would have defined $\omega_{\mathbf{u}}$ without the factorial $(u_0 - 1)!$. To see this take the simplest example $f = 1 - x$ in one variable and $R = \mathbb{Z}_p$. Theorem 4.3 implies that every rational function $(k-1)!\,\frac{x^r}{(1-x)^k}$ with $0 \le r \le k$ is modulo (formal) derivatives equivalent to a function of the form $A + \frac{B}{1-x}$. Now drop the factorial, take $k = p + 1, r = 0$ and suppose there exist $A, B \in \mathbb{Z}_p$ such that $A + \frac{B}{1-x} = \frac{1}{(1-x)^{p+1}} + xu'$ for some rational function u. Apply $\mathscr{C}_p$ modulo p on both sides. The derivative xu' is mapped to 0, $\frac{1}{1-x}$ is mapped to itself and we get

$$A + \frac{B}{1-x} \equiv \mathscr{C}_p\left(\frac{1}{(1-x)^p(1-x)}\right) \equiv \mathscr{C}_p\left(\frac{1}{(1-x^p)(1-x)}\right) \equiv \frac{1}{(1-x)^2}(\mathrm{mod}\ p).$$

On the right of this equality we see a rational function with a double pole at $x = 1$ on the left a simple pole. This is clearly contradictory.

Remark 4.8.   Knowledge of the explicit basis in $Q_f(\mu)$ from Theorem 4.3 implies that this R-module is in fact a quotient of $\Omega_f(\mu)$. However, writing it as a quotient of the completion $\widehat{\Omega}_f(\mu)$ yields the Cartier operator on $Q_f(\mu)$. Note also that $Q_f(\mu)$ is a subquotient of the Dwork module $\mathscr{W}_f$ because derivatives are contained in $U_f(\mu)$.

We would like to point out that R-modules $\widehat{\Omega}_f(\mu)$, $U_f(\mu)$, completed Dwork modules $\widehat{\Omega}_f(\mu)/d\widehat{\Omega}_f(\mu)$ and the quotients $Q_f(\mu)$ from Theorem 4.3 together with the Cartier operator $\mathscr{C}_p$ are examples of the following structure. For the scope of this paper, we give the following

Definition 4.9.   A crystal over R is a rule that assigns

- to a polynomial f with coefficients in R a differential R-module M_f, that is, for every derivation δ of R we have maps $\delta : M_f \to M_f$ satisfying $\delta(rm) = \delta(r)m + r\delta(m)$ for $r \in R, m \in M_f$ (*connection maps*);
- to every pth power Frobenius lift $\sigma : R \to R$ an R-linear map $\mathscr{C}_p : M_f \to M_{f^\sigma}$ which commutes with the connection, that is, we have $\mathscr{C}_p \circ \delta = \delta \circ \mathscr{C}_p$ for every derivation δ of R.

Note that over rings R that have no non-trivial derivations, for example, $\mathbb{Z}_p$ and its finite extensions, it still makes sense to consider crystals, though the conditions related to connection are empty.

Following the traditional terminology, see for example [8], one can call $Q_f(\mu)$ the *unit-root quotient* in reflection of the fact that the Cartier operator is divisible by p on $U_f(\mu)$ and invertible on the quotient $Q_f(\mu) = \widehat{\Omega}_f(\mu)/U_f(\mu)$ (see Remark 4.4).

Note also that, when the Hasse–Witt matrix is invertible, $U_f(\mu) \subset \widehat{\Omega}_f(\mu)$ can be characterized as the largest subcrystal on which the Cartier operator is divisible by p.

5   Periods mod m

For any exponent vector $\mathbf{v} \in C(\Delta)_{\mathbb{Z}}$ we define the linear functional $\tau_{\mathbf{v}}$ on Ω_{formal} by

$$\tau_{\mathbf{v}}(\omega) = \text{constant term of } \frac{f^{v_0}}{\mathbf{x}^{\mathbf{v}}}\omega \,.$$

Lemma 5.1.   Let $m \geq 1$ be an integer. For any $\omega \in d\Omega_{\text{formal}}$ we have $\tau_{m\mathbf{v}}(\omega) \equiv 0 (\text{mod } m)$.

For any $\omega \in \Omega_{\text{formal}}$ and any derivation δ of R we have $\delta(\tau_{m\mathbf{v}}(\omega)) \equiv \tau_{m\mathbf{v}}(\delta(\omega))(\text{mod } m)$.

Proof.   Suppose that $\omega = x_i \frac{\partial u}{\partial x_i}$ for some Laurent expansion u. Then

$$
\begin{aligned}
\tau_{m\mathbf{v}}(\omega) &= \text{constant term of } \frac{f(\mathbf{x})^{mv_0}}{\mathbf{x}^{m\mathbf{v}}} x_i \frac{\partial u}{\partial x_i} \\
&\equiv \text{constant term of } x_i \frac{\partial}{\partial x_i}\left(\frac{f(\mathbf{x})^{mv_0}}{\mathbf{x}^{m\mathbf{v}}}u\right)(\text{mod } m) \\
&\equiv 0(\text{mod } m).
\end{aligned}
$$

For any derivation δ of R and any Laurent series ω we have

$$\delta\left(\text{constant term of } \frac{f(\mathbf{x})^{mv_0}}{\mathbf{x}^{m\mathbf{v}}}\omega\right) \equiv \text{constant term of } \frac{f(\mathbf{x})^{mv_0}}{\mathbf{x}^{m\mathbf{v}}}\delta(\omega)$$

because operations δ and taking the constant term commute and derivation of an mth power is zero modulo m.   ∎

The two properties in Lemma 5.1 show that functionals $\tau_{m\mathbf{v}}$ restricted modulo m are what we call *period maps modulo m*. That is, they are R-linear maps from Ω_{formal} to R/mR that vanish on derivatives and commute with derivations of R.

Next, we look at the behaviour of these linear functionals under the Cartier operator:

Proposition 5.2.   Let p be a prime and $\sigma : R \to R$ be a pth power Frobenius lift. Denote by $\tau_{m\mathbf{v}}^{\sigma}$ the linear functional obtained by multiplication with $(f^{\sigma})^{mv_0}/\mathbf{x}^{m\mathbf{v}}$ and then taking the constant term. Then

$$\tau_{m\mathbf{v}} \equiv \tau_{m\mathbf{v}/p}^{\sigma} \circ \mathscr{C}_p (\mathrm{mod}\ p^{\mathrm{ord}_p(m)}).$$

Proof.   For any $\omega \in \Omega_{\mathrm{formal}}$ we have

$$
\begin{aligned}
\tau_{m\mathbf{v}}(\omega) &= \text{constant term of } \frac{f(\mathbf{x})^{mv_0}}{\mathbf{x}^{m\mathbf{v}}}\omega \\
&\equiv \text{constant term of } \frac{f^{\sigma}(\mathbf{x}^p)^{mv_0/p}}{(\mathbf{x}^p)^{m\mathbf{v}/p}}\omega\ (\mathrm{mod}\ p^{\mathrm{ord}_p(m)}) \\
&\equiv \text{constant term of } \mathscr{C}_p \left(\frac{f^{\sigma}(\mathbf{x}^p)^{mv_0/p}}{(\mathbf{x}^p)^{m\mathbf{v}/p}}\omega \right)\ (\mathrm{mod}\ p^{\mathrm{ord}_p(m)}) \\
&\equiv \text{constant term of } \frac{f^{\sigma}(\mathbf{x})^{mv_0/p}}{\mathbf{x}^{m\mathbf{v}/p}}\mathscr{C}_p(\omega)\ (\mathrm{mod}\ p^{\mathrm{ord}_p(m)}).
\end{aligned}
$$

The 2nd step uses the obvious fact that the constant term equals the constant term of the Cartier transform. In the last step we used a variant of Lemma 3.2 in the bigger ring $R[\mathbf{x}] \otimes_R \Omega_{\mathrm{formal}}$.   ∎

The period maps introduced here are useful when working in Ω_f. Note that to compute $\tau_{\mathbf{v}}(\omega_{\mathbf{u}})$ we simply take the constant coefficient of the product $\frac{f^{v_0}}{\mathbf{x}^{\mathbf{v}}}\omega_{\mathbf{u}}$, which is a Laurent polynomial when $u_0 \leq v_0$. In the particular case when $u_0 = v_0 = 1$ we observe that $\tau_{m\mathbf{v}}(\omega_{\mathbf{u}}) = (\beta_m)_{\mathbf{u},\mathbf{v}}$ for each $m \geq 1$, where β_m are the matrices defined in (8).

The following theorem is our 2nd main result.

Theorem 5.3.   Let $\mu \subseteq \Delta$ be a set open in the topology defined in Proposition 3.4. Suppose that R is p-adically complete and the Hasse–Witt matrix $\beta_p(\mu)$ is invertible in R. Then $\beta_{p^s}(\mu)$ is invertible for all $s \geq 1$.

Let $\mathcal{Q}_f(\mu)$ be the unit-root crystal from Theorem 4.3 and let $\Lambda_{\sigma} = (\lambda_{\mathbf{u},\mathbf{w}})$ be the transposed matrix of $\mathscr{C}_p : \mathcal{Q}_f(\mu) \to \mathcal{Q}_{f^{\sigma}}(\mu)$ with respect to the standard bases $\{\omega_{\mathbf{u}}\}, \{\omega_{\mathbf{w}}^{\sigma}\}$. More precisely, it is the $h \times h$-matrix with entries in R such that

$$\mathscr{C}_p(\omega_{\mathbf{u}}) \equiv \sum_{\mathbf{w} \in \mu_{\mathbb{Z}}} \lambda_{\mathbf{u},\mathbf{w}} \omega_{\mathbf{w}}^{\sigma}\ (\mathrm{mod}\ U_{f^{\sigma}}(\mu)) \tag{10}$$

for all $\mathbf{u} \in \mu_{\mathbb{Z}}$. Then, for all $s \geq 1$ and all $m \geq 1$, it satisfies the congruences

$$\beta_{mp^s}(\mu) \equiv \Lambda_\sigma \beta^\sigma_{mp^{s-1}}(\mu) (\mathrm{mod}\ p^s). \tag{11}$$

In particular, when $m = 1$,

$$\Lambda_\sigma \equiv \beta_{p^s}(\mu)\, \beta^\sigma_{p^{s-1}}(\mu)^{-1}\ (\mathrm{mod}\ p^s). \tag{12}$$

Similarly, for every derivation δ of R Theorem 4.3 implies that there exists a unique matrix $N_\delta = (\nu_{\mathbf{u},\mathbf{v}})_{\mathbf{u},\mathbf{v}\in\mu_{\mathbb{Z}}}$ with entries in R such that

$$\delta(\omega_{\mathbf{u}}) \equiv \sum_{\mathbf{w}\in\mu_{\mathbb{Z}}} \nu_{\mathbf{u},\mathbf{w}}\, \omega_{\mathbf{w}}\ (\mathrm{mod}\ U_f(\mu)). \tag{13}$$

This matrix then satisfies congruences

$$\delta(\beta_{mp^s}(\mu)) \equiv N_\delta\, \beta_{mp^s}(\mu)\ (\mathrm{mod}\ p^s)$$

for all $m, s \geq 1$. In particular, when $m = 1$,

$$N_\delta \equiv \delta(\beta_{p^s}(\mu))\, \beta_{p^s}(\mu)^{-1}\ (\mathrm{mod}\ p^s).$$

Proof. Using (iii) in Proposition 4.5, the congruence (10) can be refined to

$$\mathscr{C}_p(\omega_{\mathbf{u}}) \equiv \sum_{\mathbf{w}\in\mu_{\mathbb{Z}}} \lambda_{\mathbf{u},\mathbf{w}}\omega^\sigma_{\mathbf{w}}\ (\mathrm{mod}\ p\, U_{f^\sigma}(\mu)) \tag{14}$$

(see Remark 4.6). We apply $\tau^\sigma_{mp^{s-1}\mathbf{v}}$ with $\mathbf{v} \in \mu_{\mathbb{Z}}$ to (5). By Proposition 5.2 we have

$$\tau^\sigma_{mp^{s-1}\mathbf{v}}(\mathscr{C}_p(\omega_{\mathbf{u}})) \equiv \tau_{mp^s\mathbf{v}}(\omega_{\mathbf{u}})\ =\ (\beta_{mp^s})_{\mathbf{u},\mathbf{v}}\ (\mathrm{mod}\ p^s)$$

in the left-hand side. Since elements of $U_{f^\sigma}(\mu)$ are formal derivatives (see Proposition 4.2), in the right-hand side Lemma 5.1 yields $p\, \tau^\sigma_{mp^{s-1}\mathbf{v}}(U_{f^\sigma}(\mu)) \equiv 0 (\mathrm{mod}\ p^s)$. So we obtain congruence

$$(\beta_{mp^s})_{\mathbf{u},\mathbf{v}} \equiv \sum_{\mathbf{w}\in\mu_{\mathbb{Z}}} \lambda_{\mathbf{u},\mathbf{w}}(\beta^\sigma_{mp^{s-1}})_{\mathbf{w},\mathbf{v}}\ (\mathrm{mod}\ p^s).$$

It follows that $\beta_{mp^s}(\mu) \equiv \Lambda_\sigma \beta^\sigma_{mp^{s-1}}(\mu) (\mathrm{mod}\ p^s)$. By Proposition 3.6, $\Lambda_\sigma \equiv \beta_p(\mu)(\mathrm{mod}\ p)$ and we find that $\beta_{p^s}(\mu) \equiv \beta_p(\mu)\beta^\sigma_{p^{s-1}}(\mu)(\mathrm{mod}\ p)$. By iteration then obtain

$$\beta_{p^s}(\mu) \equiv \beta_p(\mu)\beta^\sigma_p(\mu) \cdots \beta^{\sigma^{s-1}}_p(\mu)(\mathrm{mod}\ p).$$

Hence, invertibility of all $\beta_{p^s}(\mu)$ modulo p follows from the case $s = 1$. After inversion of $\beta^\sigma_{p^{s-1}}(\mu)$ (it is invertible over R, see Remark 4.4) we find that $\Lambda_\sigma \equiv \beta_{p^s}(\mu)\,\beta^\sigma_{p^{s-1}}(\mu)^{-1}\ (\mathrm{mod}\ p^s)$.

The proof of the 2nd congruence runs similarly: we apply $\tau_{mp^s\mathbf{v}}$ with $\mathbf{v} \in \mu_{\mathbb{Z}}$ to (13). Since $\tau_{mp^s\mathbf{v}}(U_f(\mu)) \equiv 0\,(\mathrm{mod}\ p^s)$ and δ commutes with $\tau_{mp^s\mathbf{v}}$ modulo p^s (see Lemma 5.1) we obtain

$$\delta((\beta_{mp^s})_{\mathbf{u},\mathbf{v}}) = \sum_{\mathbf{w}\in\mu_{\mathbb{Z}}} \nu_{\mathbf{u},\mathbf{w}}(\beta_{mp^s})_{\mathbf{w},\mathbf{v}}\ (\mathrm{mod}\ p^s).$$

Hence, we conclude that $\delta(\beta_{mp^s}(\mu)) \equiv N_\delta\,\beta_{mp^s}(\mu)(\mathrm{mod}\ p^s)$, as desired.   ∎

Remark 5.4.   In [11, §1] the 2nd author conjectured vaguely that the p-adic limits

$$\lim_{s\to\infty} \beta_{p^s}(\Delta^\circ)\,\beta^\sigma_{p^{s-1}}(\Delta^\circ)^{-1}, \quad -\lim_{s\to\infty} \delta(\beta_{p^s}(\Delta^\circ))\,\beta_{p^s}(\Delta^\circ)^{-1} \tag{15}$$

describe, respectively, the Frobenius operator and the Gauss–Manin connection on *the* unit-root crystal attached to the Laurent polynomial $f(\mathbf{x})$. However, the precise meaning of the unit-root crystal in the conjecture was not specified. Moreover, it looked challenging to define this object using as little assumptions on $f(\mathbf{x})$ as one needs for existence of the p-adic limiting matrices (15). Theorem 5.3 implies that this conjecture is true with the unit-root crystal being the dual $Q^\vee_f = \mathrm{Hom}_R(Q_f(\Delta^\circ), R)$ of the crystal defined in Theorem 4.3 with the Frobenius operator $\mathscr{C}^\vee_p : Q^\vee_{f^\sigma} \to Q^\vee_f$. Note that in addition to the invertibility of the Hasse–Witt matrix, which is needed to define (15), we only use one extra assumption: there is a vertex $\mathbf{b}$ of Δ such that the coefficient of $f(\mathbf{x})$ at $\mathbf{b}$ is a unit in R. The latter is a technical assumption that was made in Section 2 for the purposes of doing formal expansion at $\mathbf{b}$ with integral coefficients; it is most likely that one could drop this condition as the Cartier operator (7) can be defined directly by formulas (4) and (5).

A different proof of the conjecture was given recently in [6, §5] under certain geometric assumptions.

Example 5.5. Consider $f(x,y) = y^2 - x(x-1)(x-z) \in R[x,y]$ as a polynomial with coefficients in a ring R containing $\mathbb{Z}[z]$, which we will specify in a moment. We would like to apply Theorem 5.3 with $\mu = \Delta^\circ \subset \mathbb{R}^2$, the interior of the Newton polytope of $f(x,y)$. In this case $\mu_\mathbb{Z} = \{(1,1)\}$, $h = \#\mu_\mathbb{Z} = 1$ and we have

$$\beta_m(\mu) = \text{ the coefficient of } x^{m-1}y^{m-1} \text{ in } \left(y^2 - x(x-1)(x-z)\right)^{m-1}$$

$$= \begin{cases} 0, & m \text{ even}, \\ \binom{m-1}{(m-1)/2} \sum_{k=0}^{(m-1)/2} \binom{(m-1)/2}{k}^2 z^k, & m \text{ odd}. \end{cases}$$

To shorten our notation, we will write $\beta_m(\mu)$ simply as β_m throughout this Example. Now fix a prime $p > 2$. Let $R = \mathbb{Z}[z, \beta_p^{-1}]\widehat{\ } \subset \mathbb{Z}_p[\![z]\!]$ be the p-adic completion of $\mathbb{Z}[z, \beta_p^{-1}]$. This ring consists of power series $g(z) \in \mathbb{Z}_p[\![z]\!]$ that can be approximated p-adically by rational functions whose denominators are powers of the Hasse–Witt polynomial $\beta_p \in \mathbb{Z}[z]$. One can check that the Frobenius lift σ given by $(\sigma g)(z) = g(z^p)$ preserves R. We claim that the respective Cartier matrix (10), which is now a 1×1-matrix, is given by

$$\Lambda_\sigma = (-1)^{\frac{p-1}{2}} \frac{F(z)}{F(z^p)}, \tag{16}$$

where

$$F(z) = {}_2F_1\left(\frac{1}{2}, \frac{1}{2}, 1 \Big| z\right) = \sum_{k \geq 0} \left(\frac{(1/2)_k}{k!}\right)^2 z^k$$

is the hypergeometric series mentioned in the Introduction. Note in particular, that this statement implies that $F(z)/F(z^p) \in \mathbb{Z}[z, \beta_p^{-1}]\widehat{\ }$.

To prove (16) we notice that $\frac{(1/2)_k}{k!} = \frac{\Gamma(k+\frac{1}{2})}{\Gamma(k+1)\Gamma(\frac{1}{2})} = \frac{(-1)^k\Gamma(\frac{1}{2})}{\Gamma(k+1)\Gamma(\frac{1}{2}-k)} = (-1)^k\binom{-\frac{1}{2}}{k}$ and

$$\binom{(p^s-1)/2}{k} \equiv \binom{-\frac{1}{2}}{k} \pmod{p^{s-\mathrm{ord}_p(k!)}}.$$

The latter congruence can be checked by induction on k. Since $\mathrm{ord}_p(k!) \leq \frac{k}{(p-1)}$, it follows that

$$\sum_{k=0}^{(p^s-1)/2} \binom{(p^s-1)/2}{k}^2 z^k \equiv F(z) \pmod{(z^s, p^{\lfloor s\frac{p-2}{p-1}\rfloor})\mathbb{Z}_p[\![z]\!]}.$$

This congruence is much weaker than the one in (12). However, it is sufficient to conclude that the p-adic limit $\Lambda_\sigma = \lim_{s\to\infty} \beta_{p^s}/\sigma(\beta_{p^{s-1}})$ equals $F(z)/F(z^p)$ times the p-adic limit of the ratios $\binom{p^s-1}{(p^s-1)/2}/\binom{p^{s-1}-1}{(p^{s-1}-1)/2}$. One can check that such a ratio is congruent

to $(-1)^{\frac{p-1}{2}}$ modulo p^s, which completes our proof of (16). In a similar vein, one can show that $N_\delta = (\delta F)(z)/F(z)$ for a derivation δ of R.

Let us mention an application of congruence (11) to integrality of formal group laws. Consider an h-tuple of formal powers series $l(z) = (l_\mathbf{u}(z))_{\mathbf{u} \in \mu_\mathbb{Z}}$ in h variables $z = (z_\mathbf{v})_{\mathbf{v} \in \mu_\mathbb{Z}}$ given by

$$l_\mathbf{u}(z) \;=\; \sum_{m=1}^\infty \frac{1}{m} \sum_{\mathbf{w} \in \mu_\mathbb{Z}} \beta_m(\mu)_{\mathbf{u},\mathbf{w}} \, z_\mathbf{w}^m \,.$$

These power series have coefficients in $R \otimes \mathbb{Q}$ and satisfy $l_\mathbf{u}(z) \equiv z_\mathbf{u}$ modulo terms of degree ≥ 2.

Corollary 5.6.   Under the assumptions of Theorem 5.3, the h-dimensional formal group law

$$G(z, z') = l^{-1}(l(z) + l(z'))$$

has coefficients in R.

Proof.   Since R is a $\mathbb{Z}_p$-algebra, congruences (11) are equivalent to the statement that the tuple of power series $l(z) - p^{-1} \Lambda_\sigma \, l^\sigma(z^p)$ has coefficients in R. Integrality of $G(z, z')$ then follows from Hazewinkel's functional equation lemma [5, §10.2].   ∎

Formal group laws $G(z, z')$ in Corollary 5.6 include coordinalizations of some Artin–Mazur formal groups of algebraic varieties, see [10, Theorem 1]. In the very particular example $f = y^2 - x(x-1)(x-z)$ from the introduction with $\mu = \Delta^\circ$ it follows from [10, p. 924] that the formal group is simply the formal law of addition on the elliptic curve $f = 0$.

Now we would like to explain the connection between our results and [8]. For that purpose, consider linear functionals on Ω_{formal} given by

$$\alpha_\mathbf{k}(\omega) \;=\; \text{coefficient of } \mathbf{x}^\mathbf{k} \text{ in } \omega$$

for $\mathbf{k} \in C(\Delta \setminus \mathbf{b})_\mathbb{Z}$. Just as we had above with $\tau_\mathbf{v}$, for any $\mathbf{k}$ and $m \geq 1$ functional $\alpha_{m\mathbf{k}}$ is a period modulo m. Indeed, by Lemma 2.2 this functional takes values in mR on formal derivatives and, since derivations of R act on Ω_{formal} simply by applying them to coefficients, we clearly have $\alpha_{m\mathbf{k}} \circ \delta = \delta \circ \alpha_{m\mathbf{k}}$. These periods have an obvious property

with respect to the Cartier operator:

$$\alpha_{m\mathbf{k}} = \alpha_{m\mathbf{k}/p} \circ \mathscr{C}_p \tag{17}$$

for all m divisible by p. Combining these observations with Theorem 4.3 we obtain the following version of [8, Theorem 6.2]:

Theorem 5.7. Let $\mu \subseteq \Delta$ be a set open in the topology defined in Proposition 3.4 and $h = \#\mu_{\mathbb{Z}}$. For $\mathbf{k} \in C(\Delta \setminus \mathbf{b})_{\mathbb{Z}}$ consider the column vector $\mathbf{a_k} \in R^h$ with components

$$(\mathbf{a_k})_{\mathbf{u} \in \mu_{\mathbb{Z}}} = \text{ coefficient of } \mathbf{x^k} \text{ in the formal expansion of } \omega_{\mathbf{u}}.$$

Assume that R is p-adically complete and the Hasse–Witt matrix $\beta_p(\mu)$ is invertible in R. For any Frobenius lift σ and any derivation δ of R, let Λ_σ and N_δ $\Lambda_\sigma, N_\delta \in R^{h \times h}$ be the matrices defined in (10) and (13) respectively. (These matrices correspond to the Cartier operator and connection on the unit-root crystal $Q_f(\mu)$ defined in Theorem 4.3.) We then have

$$\mathbf{a}_{p^s\mathbf{k}} \equiv \Lambda_\sigma \, \mathbf{a}^\sigma_{p^{s-1}\mathbf{k}} \ (\mathrm{mod} \ p^s) \tag{18}$$

and

$$\delta(\mathbf{a}_{p^s\mathbf{k}}) \equiv N_\delta \, \mathbf{a}_{p^s\mathbf{k}} \ (\mathrm{mod} \ p^s) \tag{19}$$

for all $\mathbf{k} \in C(\Delta - \mathbf{b})_{\mathbb{Z}}$.

Proof. Consider the equality

$$\mathscr{C}_p(\omega_{\mathbf{u}}) \equiv \sum_{\mathbf{w} \in \mu_{\mathbb{Z}}} \lambda_{\mathbf{u},\mathbf{w}} \omega^\sigma_{\mathbf{w}} (\mathrm{mod} \ p U^\sigma_f(\mu)).$$

Expand all terms in a Laurent series with respect to the vertex $\mathbf{b}$ and determine the coefficient of $\mathbf{x}^{\mathbf{k}p^{s-1}}$ on both sides. For the term in $p U^\sigma_f$ we get a value $0(\mathrm{mod} \ p^s)$. The other terms give us

$$a_{\mathbf{k}p^s}(\omega_{\mathbf{u}}) \equiv \sum_{\mathbf{w} \in \mu_{\mathbb{Z}}} \lambda_{\mathbf{u},\mathbf{w}} a_{\mathbf{k}p^{s-1}}(\omega^\sigma_{\mathbf{w}}) (\mathrm{mod} \ p^s),$$

which gives us the 1st statement.

For the 2nd statement we start with

$$\delta(\omega_{\mathbf{u}}) \equiv \sum_{\mathbf{w} \in \mu_{\mathbb{Z}}} \nu_{\mathbf{u},\mathbf{w}} \omega_{\mathbf{w}} (\mathrm{mod} \ U_f(\mu)).$$

Expand as Laurent series and take the coefficient of $\mathbf{x}^{\mathbf{k}p^s}$ on both sides. We get

$$\delta(a_{\mathbf{k}p^s}(\omega_{\mathbf{u}})) \equiv \sum_{\mathbf{w} \in \mu_{\mathbb{Z}}} v_{\mathbf{u},\mathbf{w}} a_{\mathbf{k}p^s}(\omega_{\mathbf{w}})(\mathrm{mod}\ p^s),$$

which proves our 2nd statement. ∎

We end with an application of Theorems 5.3 and 5.7.

Corollary 5.8.   Suppose that μ is an open set that consists of one vertex point $\mathbf{v} \in \Delta$. Let $f_{\mathbf{v}}$ be the coefficient of $\mathbf{x}^{\mathbf{v}}$ in f and suppose it is a unit in R. Then we have the equality $\mathscr{C}_p(\omega_{\mathbf{v}}) \equiv \frac{f_{\mathbf{v}}^{\sigma}}{f_{\mathbf{v}}}\omega_{\mathbf{v}}^{\sigma}(\mathrm{mod}\ U_{f^{\sigma}}(\mu))$.

Proof.   This follows almost immediately from Theorem 5.3. Note that $\beta_{p^s}(\mu)$ is a 1×1-matrix with entry $f_{\mathbf{b}}^{p^s-1}$. The matrix Λ_{σ} has the entry $\lim_{s\to\infty} f_{\mathbf{b}}^{p^s-1}/(f_{\mathbf{b}}^{\sigma})^{p^{s-1}-1} = f_{\mathbf{b}}^{\sigma}/f_{\mathbf{b}}$. ∎

Note that the situation when one vertex is an open set in the topology from Proposition 3.4 can occur if all lattice points in Δ are vertices. The complement of all but one of these vertices gives us an open one-point set μ.

The following corollary is a generalization of Theorem 5.6 in [2], which deals with congruences for coefficients of power series expansions of rational functions.

Corollary 5.9.   Let $f(\mathbf{x})$ be a Laurent polynomial with coefficients in $\mathbb{Z}_p$ such that all lattice points in its Newton polytope $\Delta \subset \mathbb{R}^n$ are vertices. Suppose that all coefficients of $f(\mathbf{x})$ are p-adic units. Let $g(\mathbf{x})$ be a Laurent polynomial with coefficients in $\mathbb{Z}_p$ and support in Δ. Choose any vertex $\mathbf{b} \in \Delta$ and consider the respective formal expansion

$$\frac{g(\mathbf{x})}{f(\mathbf{x})} = \sum_{\mathbf{k} \in C(\Delta - \mathbf{b})} a_{\mathbf{k}}\mathbf{x}^{\mathbf{k}}.$$

Then, for every $\mathbf{k} \in C(\Delta - \mathbf{b})$ and $s \geq 1$ we have $a_{p^s\mathbf{k}} \equiv a_{p^{s-1}\mathbf{k}}(\mathrm{mod}\ p^s)$.

Proof.   It is sufficient to give a proof for a monomial $g(\mathbf{x}) = \mathbf{x}^{\mathbf{v}}$, $\mathbf{v} \in \Delta_{\mathbb{Z}}$. Application of Theorem 5.7 with $\mu = \{\mathbf{v}\}$, which is an open set due to our assumption on Δ, yields the congruence $a_{p^s\mathbf{k}} \equiv \Lambda_{\sigma} a_{p^{s-1}\mathbf{k}}(\mathrm{mod}\ p^s)$ with $\Lambda_{\sigma} \in \mathbb{Z}_p^{\times}$. Since $R = \mathbb{Z}_p$ we have that $f_{\mathbf{v}}^{\sigma} = f_{\mathbf{v}}$ and hence $\Lambda_{\sigma} = 1$ as in Corollary 5.8. ∎

In [2] the polytope Δ is a subset of the unit hypercube in $\mathbb{R}^n$, hence the conditions of Corollary 5.9 are satisfied.

6 Semi-simple Decomposition

Let $\tilde{n} \leq n$ be the dimension of Δ. For $0 \leq l \leq \tilde{n}$ let $\mu^{(l)} \subset \Delta$ be the complement of the union of faces of codimension $> l$; this is an open set in the topology defined in Proposition 3.4. The inclusions

$$\Delta^\circ = \mu^{(0)} \subset \mu^{(1)} \subset \ldots \subset \mu^{(\tilde{n})} = \Delta$$

give rise to a filtration on the module of regular functions given by

$$\Omega_f(\mu^{(0)}) \subset \Omega_f(\mu^{(1)}) \subset \ldots \subset \Omega_f(\Delta) = \Omega_f. \tag{20}$$

Note that this filtration is preserved by the connection and its p-adic completion is preserved by the Cartier operator, that is, $\mathscr{C}_p : \widehat{\Omega}_f^n(\mu^{(l)}) \rightarrow \widehat{\Omega}_{f^\sigma}^n(\mu^{(l)})$ for each l (see Proposition 3.4). We quotient the p-adic completions by formally exact forms and obtain

$$Q_f(\mu^{(0)}) \subset Q_f(\mu^{(1)}) \subset \ldots \subset Q_f(\Delta).$$

Let $\beta_p^{(l)}$ be the Hasse–Witt matrix of f relative to $\mu^{(l)}$. We shall call $\beta_p^{(0)}$ simply *the Hasse–Witt matrix of f*. The following fact is a straightforward corollary of the congruences stated in Theorem 5.3. As in this theorem, we assume that $\cap_{s \geq 0} p^s R = \{0\}$ and R is p-adically complete. Recall that in this case an element is invertible if and only if it is invertible modulo p. Note also that for any face $\eta \subset \Delta$ the Newton polytope of the restriction $f|_\eta$ is given by η.

Theorem 6.1.   Assume that the coefficients of f at all vertices of Δ are units in R. Let $l \geq 1$. The matrix $\beta_p^{(l)}$ is invertible if and only if $\beta_p^{(l-1)}$ and the Hasse–Witt matrices of all restrictions $f|_\eta$ to the faces $\eta \subset \Delta$ of codimension l are invertible. If this is the case, one has the following decomposition of the quotient crystal

$$Q_f(\mu^{(l)})/Q_f(\mu^{(l-1)}) = \bigoplus_{\substack{\text{faces } \eta \subset \Delta \\ \operatorname{codim}(\eta) = l}} Q_{f|_\eta}(\eta^\circ),$$

where η° is the interior of the face η, and we make the convention that an interior of a vertex is the vertex itself.

Proof.   We write $\mu^{(\ell)} = \eta_1^\circ \cup \eta_2^\circ \cup \ldots \cup \mu^{(\ell-1)}$, where $\eta_1, \eta_2, \ldots$ are all faces of Δ of codimension ℓ, and claim that for any $m \geq 1$ matrices $\beta_m(\mu^{(\ell)})$ have the following block structure

$$\beta_m(\mu^{(\ell)}) = \begin{pmatrix} \beta_m(\eta_1^\circ) & 0 & 0 & \ldots & & * \\ 0 & \beta_m(\eta_2^\circ) & 0 & \ldots & & * \\ & & & \ldots & & * \\ 0 & 0 & 0 & \ldots & \beta_m(\mu^{(\ell-1)}) \end{pmatrix}$$

with diagonal blocks corresponding to all faces of codimension ℓ and $\mu^{(\ell-1)}$ and possibly non-zero off-diagonal blocks only in the last column. This claim follows from the following observation: if $\eta \subsetneq \Delta$ is a face, $\mathbf{v} \in \eta$ and $\mathbf{u} \notin \eta$, then the coefficients of $m\mathbf{v} - \mathbf{u}$ in $f(\mathbf{x})^{m-1}$ is zero. Indeed, choose a linear functional $\kappa : \mathbb{R}^n \to \mathbb{R}$ such that $\kappa|_\eta \equiv c$, and $\kappa(\Delta) \subset \mathbb{R}_{\leq c}$ and $\kappa(\mathbf{u}) < c$ for some $c \in \mathbb{R}$. Then $\kappa(m\mathbf{v} - \mathbf{u}) = mc - \kappa(u) > (m-1)c$ and therefore $m\mathbf{v} - \mathbf{u} \notin (m-1)\Delta$.

Taking $m = p$ we see that the Hasse–Witt matrix $\beta_p(\mu^\ell)$ is invertible if and only if all $\beta_p(\eta_i^\circ)$ and $\beta_p(\mu^{\ell-1})$ are invertible. Since the above-mentioned block structure is preserved under taking the inverse, by the congruences in Theorem 5.3 matrices Λ_σ and N_δ for $\mu^{(\ell)}$ have the same block structure and the direct sum decomposition of the quotient crystal follows immediately.   ∎

Remark 6.2.   Corollaries 5.8 and 5.9 deal with the situation when the only lattice points in the Newton polytope Δ are its vertices. In this case filtration (1) has only one step (the set $\mu_{\mathbb{Z}}^{(\tilde{n}-1)}$ is empty) and, assuming that the coefficients of $f(\mathbf{x}) = \sum_{\mathbf{v}} f_{\mathbf{v}} \mathbf{v} \mathbf{x}^{\mathbf{v}}$ at all vertices are units in R, Theorem 6.1 states that the unit-root crystal $Q_f = Q_f(\Delta)$ is a direct sum of crystals of rank 1.

Let us mention that in the regular case (i.e., when f is Δ-regular) under the identification of the Dwork module $\mathcal{W}_f = \Omega_f/d\Omega_f$ with the cohomology group $H^n(\mathbb{T}^n \setminus Z_f)$ (after tensoring with the field of fractions of R) the image of the filtration (1) is the weight filtration of the respective mixed Hodge structure (see [1, Theorem 8.2]). Theorem 6.1 thus gives a semi-simple decomposition of unit-root crystals corresponding to the graded pieces of the weight filtration.

7   Example

Consider $f = y^2 + tx^3 + xy + x$ and R the p-adic completion of $\mathbb{Z}_p[t]$. We have the following sets of exponent vectors with $u_0 = 1$:

1. $\mu_{\mathbb{Z}}^{(2)} = \{(0,2), (1,0), (3,0), (2,0), (1,1)\} = \Delta_{\mathbb{Z}}$

2. $\mu_{\mathbb{Z}}^{(1)} = \{(2, 0), (1, 1)\}$

3. $\mu_{\mathbb{Z}}^{(0)} = \{(1, 1)\}$,

where the $\mu^{(l)}$ are defined in the previous section. The ordering of the exponent vectors in Δ is chosen in decreasing filtration order. Using this ordered basis a straightforward calculation shows that for odd m,

$$\beta_m = \begin{pmatrix} 1 & 0 & 0 & 0 & h_m(t) \\ 0 & 1 & 0 & 0 & \frac{1}{2}h_m(t) \\ 0 & 0 & t^{m-1} & 0 & \frac{1}{2t}h_m(t) \\ 0 & 0 & 0 & \binom{m-1}{\frac{m-1}{2}}t^{\frac{m-1}{2}} & g_m(t) \\ 0 & 0 & 0 & 0 & f_m(t) \end{pmatrix},$$

where

$$f_m(t) = \sum_{k \geq 0} \binom{m-1}{4k}\binom{4k}{2k}\binom{2k}{k}t^k, \quad g_m(t) = \sum_{k \geq 0} \binom{m-1}{4k+1}\binom{4k+1}{2k}\binom{2k}{k}t^k,$$

$$h_m(t) = \sum_{k \geq 1} \binom{m-1}{4k-1}\binom{4k-1}{2k}\binom{2k}{k}t^k.$$

For the invertibility of β_p we extend R to be the p-adic completion of $\mathbb{Z}_p[t, (tf_p(t))^{-1}]$. Then $\beta_{p^s}(\beta_{p^{s-1}}^\sigma)^{-1}$ reads

$$\begin{pmatrix} 1 & 0 & 0 & 0 & (h_{p^s}(t) - h_{p^{s-1}}(t^p))/f_{p^{s-1}}(t^p) \\ 0 & 1 & 0 & 0 & \frac{1}{2}(h_{p^s}(t) - h_{p^{s-1}}(t^p))/f_{p^{s-1}}(t^p) \\ 0 & 0 & t^{p-1} & 0 & \frac{1}{2t}(h_{p^s}(t) - h_{p^{s-1}}(t^p))/f_{p^{s-1}}(t^p) \\ 0 & 0 & 0 & c(p,s)t^{(p-1)/2} & (g_{p^s} - c(p,s)t^{(p-1)/2}g_{p^{s-1}}(t^p))/f_{p^{s-1}}(t^p) \\ 0 & 0 & 0 & 0 & f_{p^s}(t)/f_{p^{s-1}}(t^p) \end{pmatrix},$$

where $c(p, s) = \binom{p^s-1}{(p^s-1)/2}\binom{p^{s-1}-1}{(p^{s-1}-1)/2}^{-1}$. We now take the limit as $s \to \infty$. It is not hard to derive that $c(p, s) \equiv (-1)^{(p-1)/2} \pmod{p^s}$. Also, using $\binom{p^s-1}{m} \equiv \binom{p^{s-1}-1}{\lfloor m/p \rfloor} \pmod{p^s}$, one easily shows that

$$h_{p^s}(t) - h_{p^{s-1}}(t^p) + \frac{1}{2}(f_{p^s}(t) - f_{p^{s-1}}(t^p)) \equiv 0 \pmod{p^s}.$$

Finally, experiment shows that

$$\frac{f_{p^s}(t)}{f_{p^{s-1}}(t^p)} \equiv \frac{F(t)}{F(t^p)} \pmod{p^s},$$

where $F(t) = {}_2F_1(1/4, 3/4, 1|64t)$ and

$$\frac{g_{p^s}(t) - (-t)^{(p-1)/2} g_{p^{s-1}}(t^p)}{f_{p^{s-1}}(t^p)} \equiv \frac{G(t) - (-t)^{(p-1)/2} G(t^p)}{F(t^p)} \pmod{p^s},$$

where $G(t) = {}_3F_2(5/4, 3/4, 1/2; 3/2, 1|64t)$. Putting everything together we find the limit

$$\Lambda = \begin{pmatrix} 1 & 0 & 0 & 0 & \frac{-1}{2}\left(\frac{F(t)}{F(t^p)} - 1\right) \\ 0 & 1 & 0 & 0 & \frac{-1}{4}\left(\frac{F(t)}{F(t^p)} - 1\right) \\ 0 & 0 & t^{p-1} & 0 & \frac{-1}{4t}\left(\frac{F(t)}{F(t^p)} - 1\right) \\ 0 & 0 & 0 & (-t)^{(p-1)/2} & \frac{G(t) - (-t)^{(p-1)/2} G(t^p)}{F(t^p)} \\ 0 & 0 & 0 & 0 & \frac{F(t)}{F(t^p)} \end{pmatrix}.$$

We make a few observations.

    (i) $(1, 1, t, 0, 1)\Lambda = (1, 1, t^p, 0, 1)$

    (ii) $(2, 0, 0, 0, 1)\Lambda = (2, 0, 0, 0, 1)$

    (iii) $(0, 1, 3t, 0, 1)\Lambda = (0, 1, 3t^p, 0, 1).$

These equalities imply that in Q_f we have

$$\mathscr{C}_p\left(\frac{f_i}{f}\right) = \frac{f_i^\sigma}{f^\sigma} \qquad i = 0, 1, 2,$$

where $f_0 = f, f_1 = x\frac{\partial f}{\partial x}, f_2 = y\frac{\partial f}{\partial y}$. This is a general phenomenon, as shown in the following theorem.

Proposition 7.1. Let $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ be a Laurent polynomial with coefficients in a characteristic zero ring R such that at least one vertex coefficient of f is a unit modulo p. Let $f_0 = f$ and $f_i = x_i\frac{\partial f}{\partial x_i}$ for $i = 1, \ldots, n$. Then for all i,

$$\mathscr{C}_p\left(\frac{f_i}{f}\right) \equiv \frac{f_i^\sigma}{f^\sigma} \pmod{p\, d\widehat{\Omega}_{f^\sigma}}.$$

Proof.   The case $i = 0$ comes down to $\mathscr{C}_p(1) = 1$, which is trivial. So let $i > 0$. As earlier, we will use the notation $\theta_i = x_i \frac{\partial}{\partial x_i}$. Notice that

$$
\begin{aligned}
\mathscr{C}_p\left(\frac{f_i}{f}\right) &= \mathscr{C}_p(\theta_i(\log f(\mathbf{x}))) \\
&= p\theta_i\left(\mathscr{C}_p(\log f(\mathbf{x}))\right) \\
&= \theta_i\left(\mathscr{C}_p(\log f(\mathbf{x})^p)\right) \\
&= \theta_i\left(\mathscr{C}_p(\log f^\sigma(\mathbf{x}^p)) + \mathscr{C}_p\left(\log\left(1 + p\frac{G(\mathbf{x})}{f^\sigma(\mathbf{x}^p)}\right)\right)\right),
\end{aligned}
$$

where $pG(\mathbf{x}) = f(\mathbf{x})^p - f^\sigma(\mathbf{x}^p)$. Observe that $\mathscr{C}_p(\log f^\sigma(\mathbf{x}^p)) = \log f^\sigma(\mathbf{x})$. Power series expansion of the log in

$$
\mathscr{C}_p\left(\log\left(1 + p\frac{G(\mathbf{x})}{f^\sigma(\mathbf{x}^p)}\right)\right)
$$

gives us

$$
-\sum_{r\geq 1}\frac{(-p)^r}{r}\frac{\mathscr{C}_p(G(\mathbf{x})^r)}{f^\sigma(\mathbf{x})^r}.
$$

Combining these evaluations gives us the final result

$$
\mathscr{C}_p\left(\frac{f_i}{f}\right) = \frac{f_i^\sigma}{f^\sigma}(\mathbf{x}) - \sum_{r\geq 1}\theta_i\left(\frac{(-p)^r}{r!}(r-1)!\frac{\mathscr{C}_p(G(\mathbf{x})^r)}{f^\sigma(\mathbf{x})^r}\right).
$$

Clearly, the latter summation belongs to $p\,d\widehat{\Omega}_{f^\sigma}$ when $p > 2$. ∎

We now determine the limit of

$$
\theta(\beta_{p^s})\beta_{p^s}^{-1} = \begin{pmatrix}
0 & 0 & 0 & 0 & \frac{\theta h_{p^s}(t)}{f_{p^s}(t)} \\
0 & 0 & 0 & 0 & \frac{\theta h_{p^s}(t)}{2f_{p^s}(t)} \\
0 & 0 & p^s-1 & 0 & \frac{\theta h_{p^s}(t)-p^s h_{p^s}}{2t f_{p^s}(t)} \\
0 & 0 & 0 & \frac{1}{2}(p^s-1) & \frac{2\theta g_{p^s}(t)-(p^s-1)g_{p^s}(t)}{2f_{p^s}(t)} \\
0 & 0 & 0 & 0 & \frac{\theta f_{p^s}(t)}{f_{p^s}(t)}
\end{pmatrix},
$$

where $\theta = t\frac{d}{dt}$. Some experiment suggests the following congruences

$$\frac{\theta f_{p^s}(t)}{f_{p^s}(t)} \equiv \frac{\theta F(t)}{F(t)} \pmod{p^s}, \quad \frac{\theta h_{p^s}(t)}{f_{p^s}(t)} \equiv \frac{-1}{2}\frac{\theta F(t)}{F(t)} \pmod{p^s}$$

and

$$\frac{2\theta g_{p^s}(t) + g_{p^s}(t)}{f_{p^s}(t)} \equiv -\frac{4\theta F(t) + F(t)}{F(t)} \pmod{p^s}.$$

This yields the limit matrix

$$N = \begin{pmatrix} 0 & 0 & 0 & 0 & \frac{-1}{2}\frac{\theta F(t)}{F(t)} \\ 0 & 0 & 0 & 0 & \frac{-1}{4}\frac{\theta F(t)}{F(t)} \\ 0 & 0 & -1 & 0 & \frac{-1}{4t}\frac{\theta F(t)}{F(t)} \\ 0 & 0 & 0 & \frac{-1}{2} & -2\frac{\theta F(t)}{F(t)} - \frac{1}{2} \\ 0 & 0 & 0 & 0 & \frac{\theta F(t)}{F(t)} \end{pmatrix}.$$

From this limit matrix it easily follows that $\frac{f_i}{f}, i = 0, 1, 2$ are horizontal in Q_f, that is, they are annihilated by θ. This is a general phenomenon.

Proposition 7.2.   Let notations be as in Proposition 7.1 and δ be a derivation on R. Then we have

$$\delta\left(\frac{f_i}{f}\right) \equiv 0 \pmod{d\Omega_f}.$$

Proof.   The proof is immediate,

$$\delta\left(\frac{f_i}{f}\right) = \frac{\delta(f)_i \cdot f - f_i \cdot \delta(f)}{f^2} = \theta_i\left(\frac{\delta(f)}{f}\right). \qquad \blacksquare$$

Finally, getting back to our example, we mention the matrix

$$Y = \begin{pmatrix} 1 & 0 & 0 & 0 & \frac{-1}{2}F(t) \\ 0 & 1 & 0 & 0 & \frac{-1}{4}F(t) \\ 0 & 0 & t^{-1} & 0 & \frac{-1}{4t}F(t) \\ 0 & 0 & 0 & t^{-1/2} & G(t) \\ 0 & 0 & 0 & 0 & F(t) \end{pmatrix}.$$

This is a fundamental solution matrix of the system of 1st order equations

$$\theta \mathbf{y}(t) = N \mathbf{y}(t),$$

where $\mathbf{y}$ is a column vector of 5 unknown functions in t.

Note that Propositions 7.1 and 7.2 have nothing to do with the unit-root crystal Ω_f: their statements hold modulo $d\widehat{\Omega}_{f^\sigma}$ and $d\Omega_f$ respectively and not just modulo formal derivatives. These propositions show that $\oplus_{i=0}^{n} R\frac{f_i}{f}$ is a subcrystal in the completed Dwork crystal $\widehat{\mathscr{W}}_f = \widehat{\Omega}_f / d\widehat{\Omega}_f$, on which the Cartier operator acts as the identity. In the geometric situation mentioned at the end of the introductory section, this subcrystal should correspond to the embedding of $H_{dR}^n(\mathbb{T}^n)$ into $H_{dR}^n(\mathbb{T}^n \setminus Z_f) \cong \mathscr{W}_f$.

Acknowledgments

Funding

References

[1] Batyrev, V. "Variations of the mixed Hodge structure of affine hypersurfaces in algebraic tori." *Duke Math. J.* 69, no. 2 (1993): 349–409.

[2] Beukers, F., M. Houben, and A. Straub. "Gauss congruences for rational functions in several variables." *Acta Arith.* 184 (2018): 341–62.

[3] Dwork, B. "p-adic cycles." *Publ. Math. Inst. Hautes Études Sci.* 37 (1969): 27–115.

[4] Dwork, B. "On the congruence properties of the zeta function of algebraic varieties." *J. Reine Angew. Math.* 203 (1960): 130–42.

[5] Hazewinkel, M. *Formal Groups and Applications*, p. 573. Academic Press, New York. 1978.

[6] Huang, A., B. Lian, S.-T. Yau, and C. Yu. "Hasse–Witt matrices, unit roots and period integrals." arXiv:1801.01189 [math.AG]

[7] Katz, N. "On the differential equations satisfied by period matrices." *Publ. Math. Inst. Hautes Études Sci.* 35 (1968): 71–106.

[8]   Katz, N. "Internal reconstruction of unit-root F-crystals via expansion coefficients. With an appendix by Luc Illusie." *Ann. Sci. Éc. Norm. Supér.* 18 (1985): 245–85.

[9]   Reich, D. "A p-adic fixed point formula." *Amer. J. Math.* 91, no. 3 (1969): 835–50.

[10] Stienstra, J. "Formal group laws arising from algebraic varieties." *Amer. J. Math.* 109, no. 5 (1987): 907–25.

[11] Vlasenko, M. "Higher Hasse–Witt matrices." *Indag. Math.* 29 (2018): 1411–24.

Appendix: Point counting and an alternative construction of the Cartier operator

Suppose that $R = \mathbb{Z}_q$ where $q = p^a$ and σ is the standard pth power Frobenius lift satisfying $\sigma^a = id$. Then the ath iteration of the Cartier operator $\mathscr{C}_q := \mathscr{C}_p^a$ maps $\widehat{\Omega}_f$ to itself. It follows from the estimate (5) that modulo every power p^s the image of $\mathscr{C}_p$ has finite rank. By this reason the trace of $\mathscr{C}_q$ is a well defined p-adic value. In this section we will prove the following

Theorem A.1   The trace of $(q^s - 1)^n \times \mathscr{C}_q^s$ on $\widehat{\Omega}_f$ equals the number of points on $\mathbb{T}^n \setminus Z_f$ with coordinates $x_1, \ldots, x_n \in \mathbb{F}_{q^s}^\times$.

Remark A.2.   Since $\mathscr{C}_q$ is divisible by q on the submodule of formal derivatives $U_f \subset \widehat{\Omega}_f$, we conclude from Theorem A.1 that on the quotient $Q_f = \widehat{\Omega}_f / U_f$ one has

$$\mathrm{Tr}(\mathscr{C}_q^s | Q_f) \equiv 1 + (-1)^{n+1} \# Z_f(\mathbb{F}_{q^s}) \pmod{q^s}.$$

The term 1 on the right corresponds to the eigenvector $1 \in \Omega_f$, which has eigenvalue 1. If the Hasse–Witt matrix $\beta_p(\Delta)$ is invertible, then Q_f is a $\mathbb{Z}_q$-vector space of finite dimension and it follows from the above congruence that the polynomial

$$\det(1 - T\mathscr{C}_q | Q_f)/(1 - T) \in \mathbb{Z}_q[T]$$

raised to the power $(-1)^n$ is the unit-root part of the zeta function of the hypersuface $Z_f \subset \mathbb{T}^n$ over $\mathbb{F}_q$. Note that in our standard basis in Q_f (i.e., images of $\omega_{\mathbf{u}} \in \Omega_f, \mathbf{u} \in \Delta_{\mathbb{Z}}$) the operator $\mathscr{C}_q$ is given by the transpose of

$$\Lambda \, \sigma(\Lambda) \, \ldots \, \sigma^{a-1}(\Lambda),$$

where $\Lambda = \Lambda_\sigma$ is the matrix from Theorem 5.3.

We will use a resolution of the module Ω_f. This construction ties our crystals with the exponential modules in the literature, for example in [1], and exhibits a natural lift of our Cartier operator which possesses nice properties and hence might be useful

on its own. With the lifted Cartier operator, the point counting can be done using a version of Dwork's trace formula, which is now a standard technique in p-adic analysis.

From now on R is a characteristic zero ring, we will impose more assumptions when needed. Let us introduce the auxiliary variable x_0 and define the subring

$$R[\Delta] \subset R[x_0, x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$$

as the span of monomials $\mathbf{X^u} = x_0^{u_0} \ldots x_n^{u_n}$ with $\mathbf{u} \in C(\Delta)_{\mathbb{Z}}$. We remind the reader that throughout the paper we denoted $\mathbf{x^u} = x_1^{u_1} \ldots x_n^{u_n}$ for $\mathbf{u} = (u_0, \ldots, u_n)$, so now we shall use the capital letter for $\mathbf{X^u} = x_0^{u_0} \mathbf{x^u}$. We denote $F(\mathbf{X}) = x_0 f(\mathbf{x}) \in R[\Delta]$. The operations

$$\mathscr{D}_{i,f} \ = \ x_i \frac{\partial}{\partial x_i} + x_i \frac{\partial F(\mathbf{X})}{\partial x_i} : R[\Delta] \to R[\Delta], \quad i = 0, \ldots, n$$

are called *twisted derivatives*. Formally, we have $\mathscr{D}_{i,f} = e^{-F} \circ \theta_i \circ e^F$, where $\theta_i = x_i \frac{\partial}{\partial x_i}$. Twisted derivatives commute with each other.

Let $R[\Delta]^+$ be the free R-module generated by $\mathbf{X^u}$ with $\mathbf{u} \in C(\Delta)_Z^+$. It is an ideal in $R[\Delta]$ and twisted derivatives preserve $R[\Delta]^+$. The *Laplace transform* is the R-linear map $\mathscr{R} : R[\Delta]^+ \to \Omega_f$ given by

$$\mathbf{X^u} \mapsto (-1)^{u_0}(u_0 - 1)! \, \frac{\mathbf{x^u}}{f(\mathbf{x})^{u_0}} \ = \ (-1)^{u_0} \omega_{\mathbf{u}}.$$

This Laplace transform was basically defined in [7, p.244] and [1, §7]. See also our Remark 2.1. It is clear that $\mathscr{R}$ is surjective.

Proposition A.3. The kernel of the Laplace transform is given by $\mathscr{D}_{0,f}(R[\Delta]^+)$. Under the induced isomorphism

$$\mathscr{R} : R[\Delta]^+ / \mathscr{D}_{0,f}(R[\Delta]^+) \xrightarrow{\sim} \Omega_f$$

the twisted derivative $\mathscr{D}_{i,f}$ corresponds to the usual derivative θ_i for each $1 \leq i \leq n$.

Proof. Under the Laplace transform the elements $\mathscr{D}_{0,f}(\mathbf{X^u}) = u_0 \mathbf{X^u} + x_0 f(\mathbf{x}) \mathbf{X^u}$ are mapped to

$$(-1)^{u_0} u_0! \, \frac{\mathbf{x^u}}{f(\mathbf{x})^{u_0}} + (-1)^{u_0+1} u_0! \, \frac{\mathbf{x^u} f(\mathbf{x})}{f(\mathbf{x})^{u_0+1}} \ = \ 0.$$

It is clear that these elements generate all relations in Ω_f and therefore they span the kernel of $\mathscr{R}$.

Let $1 \leq i \leq n$. Since twisted derivatives commute, $\mathscr{D}_{i,f}$ maps $\mathrm{Ker}(\mathscr{R}) = \mathrm{Im}(\mathscr{D}_{0,f})$ to itself. The fact that the induced map on Ω_f coincides with θ_i can be easily checked on

monomials:

$$\mathscr{R}\left(\mathscr{D}_{i,f}(\mathbf{X^u})\right) = \mathscr{R}\left(u_i\mathbf{X^u} + \theta_i F(\mathbf{X})\mathbf{X^u}\right) = (-1)^{u_0}(u_0 - 1)!\left(u_i\frac{\mathbf{X^u}}{f(\mathbf{x})^{u_0}} - u_0\frac{\mathbf{X^u}\theta_i f(\mathbf{x})}{f(\mathbf{x})^{u_0+1}}\right)$$

$$= (-1)^{u_0}\theta_i\omega_{\mathbf{u}} = \theta_i\mathscr{R}(\mathbf{X^u}). \qquad\blacksquare$$

Corollary A.4. $R[\Delta]^+/\sum_{i=0}^{n}\mathscr{D}_{i,f}(R[\Delta]^+) \cong \mathscr{W}_f.$

We would like to remark that in [1, Theorem 7.13] the quotient module on the left in this corollary was identified with $H_{dR}^n(\mathbb{T}^n \setminus Z_f)$ under the condition that R is a field and $f(\mathbf{x})$ is Δ-regular. At the end of the introductory section we mentioned the relation between Dwork modules and de Rham cohomology having in mind Corollary A.4.

To define the Cartier operator, we turn on our usual assumptions that $\cap_s p^s R = \{0\}$ and R is p-adically complete. Let $R[\![\Delta]\!]$ be the ring of formal power series with coefficients in R and support in $C(\Delta)$. The p-adic completion $\widehat{R[\Delta]} = \lim_s R[\Delta]/p^s R[\Delta]$ consists of power series with infinitely growing p-adic valuation of coefficients:

$$\widehat{R[\Delta]} = \left\{\sum_{\mathbf{u}\in C(\Delta)_{\mathbb{Z}}} a_{\mathbf{u}}\mathbf{X^u} \ : \ a_{\mathbf{u}}\in R, \quad \mathrm{ord}_p(a_{\mathbf{u}})\to\infty \ \mathrm{as}\, u_0\to\infty\right\} \subset R[\![\Delta]\!].$$

We denote by $\widehat{R[\Delta]}^+$ the ideal of power series with zero constant term ($a_{\mathbf{0}} = 0$). It follows from Proposition A.3 that $\widehat{\Omega}_f \cong \widehat{R[\Delta]}^+/\mathscr{D}_{0,f}\left(\widehat{R[\Delta]}^+\right)$.

Theorem A.5.   Consider the operator on power series given by

$$V_p\left(\sum_{\mathbf{u}} a_{\mathbf{u}}\mathbf{X^u}\right) = \sum_{\mathbf{u}}(-p)^{u_0}a_{p\mathbf{u}}\mathbf{X^u}.$$

Let $p > 2$. For every pth power Frobenius lift $\sigma : R \to R$, the operator

$$\mathscr{V}_\sigma = e^{-F^\sigma} \circ V_p \circ e^F$$

maps $R[\![\Delta]\!]$ to itself. Operator $\mathscr{V}_\sigma$ preserves $R[\![\Delta]\!]^+$ and it is divisible by p on this submodule. The following commutation relation with twisted derivatives

$$\mathscr{D}_{i,f^\sigma} \circ \mathscr{V}_\sigma = p\,\mathscr{V}_\sigma \circ \mathscr{D}_{i,f} \qquad\qquad (A.1)$$

holds for each $0 \le i \le n$.

The operator $\mathscr{V}_\sigma$ preserves $\widehat{R[\Delta]}$ and the induced map $p^{-1}\mathscr{V}_\sigma : \widehat{\Omega}_f \to \widehat{\Omega}_{f^\sigma}$ coincides with the Cartier operator $\mathscr{C}_p : \widehat{\Omega}_f \to \widehat{\Omega}_{f^\sigma}$ constructed in Section 3.

Proof.   Fix any $\mathbf{u} \in C(\Delta)^+_{\mathbb{Z}}$ and denote $v_0 = p\lceil \frac{u_0}{p} \rceil - u_0$. Observe that

$$V_p\left(e^{x_0 f(\mathbf{x})} \mathbf{X}^{\mathbf{u}}\right) = \sum_{n \geq 0,\, p\,|(n+u_0)} \frac{(-px_0)^{\frac{n+u_0}{p}} \mathscr{C}_p(f(\mathbf{x})^n \mathbf{x}^{\mathbf{u}})}{n!}$$

$$= \sum_{m \geq 0} \frac{(-px_0)^{m+\lceil \frac{u_0}{p} \rceil} \mathscr{C}_p(f(\mathbf{x})^{pm+v_0} \mathbf{x}^{\mathbf{u}})}{(pm + v_0)!}$$

and therefore

$$\mathscr{V}_\sigma \mathbf{X}^{\mathbf{u}} = \sum_{k \geq 0} \frac{(-x_0)^k f^\sigma(\mathbf{x})^k}{k!} \sum_{m \geq 0} \frac{(-px_0)^{m+\lceil \frac{u_0}{p} \rceil} \mathscr{C}_p(f(\mathbf{x})^{pm+v_0} \mathbf{x}^{\mathbf{u}})}{(pm + v_0)!}$$

$$= \sum_{r \geq 0} (-px_0)^{r+\lceil \frac{u_0}{p} \rceil} \mathscr{C}_p\left(\mathbf{x}^{\mathbf{u}} \sum_{m+k=r} \frac{f(\mathbf{x})^{pm+v_0} f^\sigma(\mathbf{x}^p)^k}{(pm+v_0)!\; k!\; p^k} \right)$$

$$= \sum_{r \geq 0} (-px_0)^{r+\lceil \frac{u_0}{p} \rceil} \mathscr{C}_p\left(\mathbf{x}^{\mathbf{u}} \sum_{s=0}^{r} \frac{G(\mathbf{x})^{r-s} f(\mathbf{x})^{ps+v_0}}{(r-s)!} \gamma_{ps+v_0} \right),$$

where we substituted $f^\sigma(\mathbf{x}^p) = f(\mathbf{x})^p + pG(\mathbf{x})$ and recognised the sums

$$\gamma_{ps+v_0} = \sum_{m=0}^{s} \frac{1}{(pm+v_0)!\; (s-m)!\; p^{s-m}}$$

as coefficients of the *Dwork exponential* $e^{x_0 + \frac{x_0^p}{p}} = \sum_{n \geq 0} \gamma_n x_0^n$. The following standard estimate of their p-adic order

$$\mathrm{ord}_p(\gamma_n) \geq \left(\frac{p-1}{p^2} - \frac{1}{p-1} \right) n \tag{A.2}$$

implies that the matrix coefficients given by $\mathscr{V}_\sigma \mathbf{X}^{\mathbf{u}} = \sum_{\mathbf{v}} \mathscr{F}_{\mathbf{u},\mathbf{v}} \mathbf{X}^{\mathbf{v}}$ have p-adic valuations bounded by

$$\mathrm{ord}_p(\mathscr{F}_{\mathbf{u},\mathbf{v}}) \geq r + \left\lceil \frac{u_0}{p} \right\rceil + \min_{0 \leq s \leq r}\left(\left(-\frac{1}{p-1} \right)(r-s) + \left(\frac{p-1}{p^2} - \frac{1}{p-1} \right)(ps+v_0) \right)$$

$$= r + \left\lceil \frac{u_0}{p} \right\rceil - \frac{r}{p-1} + \min_{0 \leq s \leq r}\left(-\frac{s}{p} \right) + \left(\frac{p-1}{p^2} - \frac{1}{p-1} \right)\left(p\left\lceil \frac{u_0}{p} \right\rceil - u_0 \right)$$

$$= \left(\frac{p-1}{p} - \frac{1}{p-1} \right)\left(r + \left\lceil \frac{u_0}{p} \right\rceil \right) - \left(\frac{p-1}{p^2} - \frac{1}{p-1} \right) u_0$$

$$= \left(\frac{p-1}{p} - \frac{1}{p-1} \right) v_0 + \left(\frac{1}{p-1} - \frac{p-1}{p^2} \right) u_0,$$

where we used $r = v_0 - \lceil \frac{u_0}{p} \rceil$. Since this valuation is non-negative, we conclude that all $\mathscr{F}_{\mathbf{u},\mathbf{v}} \in R$ and hence $\mathscr{V}_\sigma$ maps the module of formal series $R[\![\Delta]\!]$ to itself. We also observe

that $\mathscr{V}_\sigma$ is divisible by p on $R[\![\Delta]\!]^+$. Moreover, $\mathscr{V}_\sigma$ preserves $\widehat{R[\Delta]}$ because when $v_0 \to \infty$ we have $\mathrm{ord}_p(\mathscr{F}_{\mathbf{u},\mathbf{v}} \in R) \to \infty$ uniformly in u_0.

The commutation relation (A.1) follows immediately from $\theta_i \circ V_p = p\,\theta_i \circ V_p$ and the fact that $\mathscr{D}_{i,f} = e^{-F} \circ \theta_i \circ e^F$. Since $\widehat{\Omega}_f = \widehat{R[\Delta]}^+ / \mathscr{D}_{0,f}(\widehat{R[\Delta]}^+)$, we have a well defined induced map $p^{-1}\mathscr{V}_\sigma : \widehat{\Omega}_f \to \widehat{\Omega}_f^\sigma$. Let us show that this induced map coincides with the Cartier operator $\mathscr{C}_p$ defined in Proposition 3.3. Since $\mathscr{R}(\mathbf{X}^{\mathbf{w}}) = (-1)^{u_0}\omega_{\mathbf{w}}$, we consider

$$
p^{-1}\mathscr{V}_\sigma \mathbf{X}^{\mathbf{u}} - \sum_{\mathbf{v} \in C(\Delta)_{\mathbb{Z}}^+} (-1)^{v_0+u_0} F_{\mathbf{u},\mathbf{v}}\mathbf{X}^{\mathbf{v}}
$$
$$
= \frac{1}{p}\sum_{r \geq 0}(-px_0)^{r+\lceil \frac{u_0}{p}\rceil}\mathscr{C}_p\left(\mathbf{x}^{\mathbf{u}}\sum_{s=0}^{r} G(\mathbf{x})^{r-s}f(\mathbf{x})^{ps+v_0}\frac{\gamma_{ps+v_0} - \delta_{s,0}\Gamma_p(u_0)}{(r-s)!}\right),
\tag{A.3}
$$

where we used formula (5) and substitution $\frac{(u_0-1)!}{(\lceil\frac{u_0}{p}\rceil-1)!} = (-1)^{u_0}p^{\lceil\frac{u_0}{p}\rceil-1}\Gamma_p(u_0)$. It is easy to check that the difference (A.3) equals

$$
\mathscr{D}_{0,f^\sigma}\left(\frac{1}{p}\sum_{r \geq 0}(-px_0)^{r+\lceil\frac{u_0}{p}\rceil}\mathscr{C}_p\left(\mathbf{x}^{\mathbf{u}}\sum_{s=0}^{r}G(\mathbf{x})^{r-s}f(\mathbf{x})^{ps+v_0}\frac{\mu_s}{(r-s)!}\right)\right),
\tag{A.4}
$$

where the coefficients $\mu_s \in \mathbb{Q}$ are determined by the recurrence

$$
\left(s + \left\lceil \frac{u_0}{p}\right\rceil\right)\mu_s = p^{-1}\mu_{s-1} + \gamma_{ps+v_0} - \Gamma_p(u_0)\delta_{s,0}.
$$

(The initial term μ_0 is also determined by this formula and convention $\mu_{-1} = 0$.) We claim that

$$
\mathrm{ord}_p(\mu_s) \geq \left(-\frac{1}{p} - \frac{1}{p-1}\right)s + 1 - \left\lceil\frac{u_0}{p}\right\rceil,
\tag{A.5}
$$

and hence inside of $\mathscr{D}_{0,f^\sigma}(\ldots)$ in (A.4) the p-adic valuation of coefficients of the polynomial next to $x_0^{r+\lceil\frac{u_0}{p}\rceil}$ can be estimated from below as

$$
-1 + r + \lceil\frac{u_0}{p}\rceil + \min_{0 \leq s \leq r}\mathrm{ord}_p\left(\frac{\mu_s}{(r-s)!}\right) \geq r + \min_{0 \leq s \leq r}\left(\left(-\frac{1}{p} - \frac{1}{p-1}\right)s - \frac{1}{p-1}(r-s)\right)
$$
$$
= r + \left(-\frac{1}{p} - \frac{1}{p-1}\right)r = \left(\frac{p-1}{p} - \frac{1}{p-1}\right)r.
$$

Since this valuation is non-negative and grows infinitely as $r \to \infty$, we conclude that (A.4) belongs to $\mathscr{D}_{0,f^\sigma}\left(\widehat{R[\Delta]^+}\right)$ and therefore $p^{-1}\mathscr{V}_\sigma = \mathscr{C}_p$ on $\widehat{\Omega}_f$.

It only remains to prove (A.5). For this purpose we consider $f(\mathbf{x}) = 1$ in (3) and (A.4). In this case $\mathscr{V}_\sigma$ is multiplication by the Dwork exponential $e^{x_0+p^{-1}x_0^p}$, followed by $\mathscr{C}_p$ and the substitution $x_0 \mapsto -px_0$. We shall denote $\mathscr{V}_\sigma$ simply by $\mathscr{V}$ and $\mathscr{D}_{0,f^\sigma} = x_0\frac{d}{dx_0} + x_0$

by $\mathscr{D}$. The equality of (A.4) and (A.3) can be written as

$$\mathscr{D}\left(p^{-1}\sum_{r\geq 0}(-px_0)^{r+\lceil\frac{u_0}{p}\rceil}\mu_r\right) = p^{-1}\mathscr{V}(x_0^{u_0}) - p^{-1}\Gamma_p(u_0)(-px_0)^{\lceil\frac{u_0}{p}\rceil}$$

$$= p^{-1}\mathscr{V}\left(x_0^{u_0} - \Gamma_p(u_0)x_0^{p\lceil\frac{u_0}{p}\rceil}e^{-x_0-p^{-1}x_0^p}\right).$$

Note that $\mathscr{D}$ is invertible on $\mathbb{Q}_p[\![x_0]\!]^+ = x_0\mathbb{Q}_p[\![x_0]\!]$, and hence the commutation relation $\mathscr{V}\mathscr{D} = p\mathscr{D}\mathscr{V}$ can be rewritten as $p^{-1}\mathscr{D}^{-1}\mathscr{V} = \mathscr{V}\mathscr{D}^{-1}$. Applying $\mathscr{D}^{-1}$ to the last identity and using the commutation relation, we get

$$p^{-1}\sum_{r\geq 0}(-px_0)^{r+\lceil\frac{u_0}{p}\rceil}\mu_r = \mathscr{V}\mathscr{D}^{-1}\left(x_0^{u_0} - \Gamma_p(u_0)x_0^{p\lceil\frac{u_0}{p}\rceil}e^{-x_0-p^{-1}x_0^p}\right). \tag{A.6}$$

Let

$$L_{\alpha,\beta} = \left\{\sum_{m\geq 1}a_mx_0^m \in x_0\mathbb{Q}_p[\![x_0]\!] \mid \mathrm{ord}_p(a_m) \geq \alpha m + \beta\right\}.$$

Let $\alpha_0 = \frac{p-1}{p^2} - \frac{1}{p-1}$ and $\alpha_1 = \frac{p-1}{p} - \frac{1}{p-1}$. Note that (A.5) precisely means that the series in (A.6) belongs to $L_{\alpha_1,0}$. In order to demonstrate this fact, we first notice that for any $\alpha \geq \alpha_0$ and any β we have $\mathscr{V}: L_{\alpha,\beta} \to L_{\alpha_1,\beta}$. Indeed, since $e^{x_0+p^{-1}x_0^p} \in L_{\alpha_0,0}$ we decompose $\mathscr{V}$ into three steps and check that

$$L_{\alpha,\beta} \stackrel{\cdot e^{x_0+p^{-1}x_0^p}}{\to} L_{\min(\alpha_0,\alpha),\beta} = L_{\alpha_0,\beta} \stackrel{\mathscr{C}_p}{\to} L_{p\alpha_0,\beta} \stackrel{x_0\mapsto -px_0}{\to} L_{p\alpha_0+1,\beta} = L_{\alpha_1,\beta}.$$

In the view of (A.6), it now suffices to show that

$$\mathscr{D}^{-1}\left(x_0^{u_0} - \Gamma_p(u_0)x_0^{p\lceil\frac{u_0}{p}\rceil}e^{-x_0-p^{-1}x_0^p}\right) \in L_{\alpha_0,0}. \tag{A.7}$$

It is useful to observe that $\mathscr{D}(x_0^m) = mx_0^m + x_0^{m+1}$ and

$$\mathscr{D}(x_0^m e^{-x_0-p^{-1}x_0^p}) = e^{-x_0}x_0\frac{\mathrm{d}}{\mathrm{d}x_0}(x_0^m e^{-p^{-1}x_0^p}) = (mx_0^m - x_0^{m+p})e^{-x_0-p^{-1}x_0^p}.$$

Using these two rules one can easily check that

$$\mathscr{D}\left((-1)^{u_0-1}(u_0-1)!\sum_{m=0}^{u_0-1}\frac{(-x_0)^m}{m!}\right) = x_0^{u_0} \tag{A.8}$$

and

$$\mathscr{D}\left((n-1)!\,p^{n-1}\sum_{m=0}^{n-1}\frac{x_0^{pm}}{m!\,p^m}e^{-x_0-p^{-1}x_0^p}\right) = -x_0^{pn}e^{-x_0-p^{-1}x_0^p}. \tag{A.9}$$

Note that under $\mathscr{D}(\ldots)$ the polynomial in (A.8) has integral coefficients and the series in (A.9) belongs to $L_{\alpha_0,0}$ if one cuts off its constant term. We shall use (A.9) with $n = \lceil\frac{u_0}{p}\rceil$.

Since $(-1)^{u_0}(u_0 - 1)! = \Gamma_p(u_0)(\lceil \frac{u_0}{p} \rceil - 1)! \, p^{\lceil \frac{u_0}{p} \rceil - 1}$, we get

$$\mathscr{D}^{-1}\left(x_0^{u_0} - \Gamma_p(u_0)x_0^{p\lceil \frac{u_0}{p} \rceil} e^{-x_0 - p^{-1}x_0^p}\right)$$

$$= (-1)^{u_0 - 1}(u_0 - 1)! \left(\sum_{m=0}^{u_0-1} \frac{(-x_0)^m}{m!} - \sum_{m=0}^{\lceil \frac{u_0}{p} \rceil - 1} \frac{x_0^{pm}}{m! \, p^m} e^{-x_0 - p^{-1}x_0^p}\right).$$

Note that the constant term of the series in the right-hand side vanishes, which means that we integrated (A.7) in $x_0 \mathbb{Q}_p[\![x_0]\!]$ explicitly. Since $\Gamma_p(u_0)$ is a p-adic integer and $\alpha_0 < 0$, this series belongs to $L_{\alpha_0,0}$ due to the remarks made after (A.8) and (A.9). This completes our proof of (A.5). ∎

Remark A.6.   One can easily define a connection on $R[\Delta]$ in a way and it commutes with the twisted derivatives. Namely, for every derivation $\delta : R \to R$ we define its action on $R[\Delta]$ as

$$\nabla_\delta := \delta + \delta F,$$

where the 1st summand simply means that the derivation δ is applied to the coefficients and the 2nd one means multiplication by the polynomial $\delta F(\mathbf{X}) = x_0 (\delta f)(\mathbf{x})$. Formally, one can write $\nabla_\delta = e^{-F} \cdot \delta \cdot e^F$. To see that ∇_δ commutes with the twisted derivatives, recall that $\mathscr{D}_{i,f} = e^{-F} \cdot \theta_i \cdot e^F$ and note that δ and θ_i commute. Operations ∇_δ preserve $R[\Delta]^+$ and descend to its quotients by the images of twisted derivatives, particularly to Ω_f and $\mathscr{W}_f$. It is easy to check that ∇_δ acts on Ω_f as the natural extension of δ to rational functions, the operation that we simply denoted by the same letter δ earlier in this paper.

Finally, observe that the operator $\mathscr{V}_\sigma = e^{-F^\sigma} \cdot V_p \cdot e^F$ defined in Theorem A.5 commutes with the connection operators. Namely, it is obvious that V_p commutes with δ as operators on power series, and after twisting by exponentials we obtain

$$\mathscr{V}_\sigma \cdot \nabla_\delta = \nabla_\delta^\sigma \cdot \mathscr{V}_\sigma,$$

where $\nabla_\delta^\sigma = \delta + \delta F^\sigma = e^{-F^\sigma} \cdot \delta \cdot e^{F^\sigma}$. This observation turns quotients of $\widehat{R[\Delta]}^+$ by twisted derivatives into crystals.

From now on we consider $R = \mathbb{Z}_q$ with $q = p^a$. Here we have the standard pth power Frobenius lift $\sigma : \mathbb{Z}_q \to \mathbb{Z}_q$, which satisfies $\sigma^a = id$. Consider the operator on power series $Z_q[\![\Delta]\!]$ given by

$$\mathscr{V}_q := e^{-F} \circ V_p^a \circ e^F.$$

Below we compute the traces of powers of $\mathscr{V}_q$ using a few standard tricks in p-adic analysis, which are basically due to Dwork.

Remark A.7. The traces are well-defined p-adic numbers because modulo every p^s the operator $\mathscr{V}_q$ has finite-dimensional image (see the p-adic estimate of the matrix entries in the proof of Theorem A.5). Note also that the traces only depend on the mod p reduction of the polynomial $F(\mathbf{X}) = x_0 f(\mathbf{x})$. Indeed, if $F'(\mathbf{X}) - F(\mathbf{X}) = pG(\mathbf{X})$ then the respective operators on power series are conjugate $\mathscr{V}'_q = e^{-pG} \circ \mathscr{V}_q \circ e^{pG}$ and modulo each power of p this identity can be written using matrices of finite size.

Proposition A.8. For all $s \geq 1$ one has

$$(1 - q^s)^{n+1} \mathrm{Tr}\left(\mathscr{V}_q^s \mid \mathbb{Z}_q[\![\Delta]\!]\right) \ = \ q^s \, \#Z_f(\mathbb{F}_{q^s}) - (q^s - 1)^n.$$

Proof. Let $\pi \in \overline{\mathbb{Q}_p}$ be a number satisfying $\pi^{p-1} = -p$. We will work with Laurent series with coefficients in $R = \mathbb{Q}_q(\pi)$ and support in the cone $C(\Delta)$. Let $\rho : R[\![\Delta]\!] \to R[\![\Delta]\!]$ be the operation given by $\rho(\mathbf{X}^{\mathbf{u}}) = \pi^{u_0} \mathbf{X}^{\mathbf{u}}$. Note that $V_p = \rho^{-1} \circ \mathscr{C}_p \circ \rho$ and $e^{\pm F} = \rho^{-1} \circ e^{\pm \pi F} \circ \rho$, and hence

$$\rho \circ \mathscr{V}_q^s \circ \rho^{-1} = e^{-\pi F} \circ \mathscr{C}_q^s \circ e^{\pi F} \ = \ \mathscr{C}_q^s \circ \Theta_{F,s}, \tag{A.10}$$

where we used the power series

$$\Theta_{F,s}(\mathbf{X}) := \exp\left(\pi F(\mathbf{X}) - \pi F(\mathbf{X}^{q^s})\right) = \sum_{u \in C(\Delta)_\mathbb{Z}} b_{\mathbf{u}} \mathbf{X}^{\mathbf{u}}. \tag{A.11}$$

From (A.10) it is clear that $\mathrm{Tr}(\mathscr{V}_q^s) = \sum_{\mathbf{u} \in C(\Delta)_\mathbb{Z}} b_{(q^s-1)\mathbf{u}}$. Since

$$\sum_{x \in \mathbb{Z}_q : x^{q-1} = 1} x^u \ = \ \begin{cases} q - 1, & \text{if } (q-1)|u, \\ 0, & \text{otherwise,} \end{cases}$$

this trace can be computed by summation of values of (A.11) over tuples of Teichmüller units in $\mathbb{Z}_{q^s}$:

$$\sum_{\mathbf{X} \in \mathbb{Z}_{q^s}^{n+1} : x_i^{q^s-1} = 1} \Theta_{F,s}(\mathbf{X}) \ = \ (q^s - 1)^{n+1} \sum_{\mathbf{u} \in C(\Delta)_\mathbb{Z}} b_{(q^s-1)\mathbf{u}} \ = \ (q^s - 1)^{n+1} \mathrm{Tr}(\mathscr{V}_q^s). \tag{A.12}$$

To evaluate the sum on the left, consider the *Dwork exponential* $\theta_p(z) = \exp(\pi z - \pi z^p)$. This series has p-adic radius of convergence > 1 and $\zeta_p := \theta_p(1) = 1 + \pi \pmod{\pi^2}$ is a pth root of unity. For $k \geq 1$, let $\theta_{p^k}(z) = \exp(\pi z - \pi z^{p^k}) = \prod_{i=0}^{k-1} \theta_p(z^{p^i})$. The additive character $\psi_k : \mathbb{F}_{p^k} \to \mathbb{Q}_p(\pi)^\times$ given by $\psi_k(\bar{x}) = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(\bar{x})}$ is related to the Dwork exponential via $\psi_k(\bar{x}) = \theta_{p^k}(\mathrm{Teich}(\bar{x}))$.

Write $F(\mathbf{X}) = x_0 f(\mathbf{x}) = \sum a_{\mathbf{u}} \mathbf{X}^{\mathbf{u}}$ and let $\bar{F}(\mathbf{X}) = \sum \bar{a}_{\mathbf{u}} \mathbf{X}^{\mathbf{u}}$ with $\bar{a}_{\mathbf{u}} \in \mathbb{F}_q$ be the reduction of F modulo p. Denote $a'_{\mathbf{u}} = \mathrm{Teich}(\bar{a}_{\mathbf{u}})$ and $F'(\mathbf{X}) = \sum a'_{\mathbf{u}} \mathbf{X}^{\mathbf{u}}$. For any vector

$\bar{X} = (\bar{x}_0, \ldots, \bar{x}_n) \in \mathbb{F}_{q^s}^{n+1}$ we have

$$\psi_{as}(\bar{F}(\bar{\mathbf{X}})) = \psi_{as}\left(\sum \bar{a}_{\mathbf{u}} \bar{\mathbf{X}}^{\mathbf{u}}\right) = \prod \theta_{q^s}(a'_{\mathbf{u}} \mathrm{Teich}(\bar{\mathbf{X}})^{\mathbf{u}}) = \Theta_{F'}(\mathrm{Teich}(\bar{\mathbf{X}})).$$

Therefore, the left-hand sum in (A.12) for F' can be evaluated as

$$\sum_{\mathbf{X} \in \mathbb{Z}_{q^s}^{n+1} \,:\, x_i^{q^s-1}=1} \Theta_{F',s}(\mathbf{X}) = \sum_{\bar{\mathbf{X}} \in (F_{q^s}^{\times})^{n+1}} \psi_{as}(\bar{F}(\bar{\mathbf{X}})) = \sum_{\bar{\mathbf{x}} \in (F_{q^s}^{\times})^n} \sum_{x_0 \in F_{q^s}} \psi_{as}(\bar{x}_0 f(\bar{\mathbf{x}}))$$

$$= \sum_{\bar{\mathbf{x}} \in (F_{q^s}^{\times})^n} \begin{cases} q^s - 1, & \text{if } \bar{f}(\bar{\mathbf{x}}) = 0 \\ -1, & \text{if } \bar{f}(\bar{\mathbf{x}}) \neq 0 \end{cases} = q^s \, \#Z_f(\mathbb{F}_{q^s}) - (q^s - 1)^n.$$

(A.13)

By Remark A.7, since $F' \equiv F \pmod{p}$ traces of powers of $\mathscr{V}'_q = e^{-F'} \circ V_p^a \circ e^{F'}$ and $\mathscr{V}_q = e^{-F} \circ V_p^a \circ e^F$ are equal. Hence, our claim follows from (A.12) and (A.13). ∎

Proof of Theorem A.1. By Theorem A.5, we have

$$q^s \mathrm{Tr}(\mathscr{C}_q^s | \widehat{\Omega}_f) = \mathrm{Tr}(\mathscr{V}_q^s | \widehat{R[\Delta]}^+) - \mathrm{Tr}(\mathscr{V}_q^s | \mathscr{D}_{0,f}(\widehat{R[\Delta]}^+)) = (1 - q^s) \mathrm{Tr}(\mathscr{V}_q^s | \widehat{R[\Delta]}^+). \qquad (14)$$

Here the 2nd equality follows from the commutation relation $\mathscr{V}_q^s \circ \mathscr{D}_{0,f} = q^s \mathscr{D}_{0,f} \circ \mathscr{V}_q^s$. Traces on $\widehat{R[\Delta]}^+$ and $R[\![\Delta]\!]^+$ are the same. It is clear from the definition of $\mathscr{V}_q$ that for every $s \geq 1$ one has $\mathscr{V}_q^s(\mathbf{X}^{\mathbf{0}}) = \mathbf{X}^{\mathbf{0}} +$ terms with $u_0 \geq 1$, and hence $\mathrm{Tr}(\mathscr{V}_q^s | R[\![\Delta]\!]^+) = \mathrm{Tr}(\mathscr{V}_q^s | R[\![\Delta]\!]) - 1$. Finally, we combine (A.14) with Proposition A.8 and get

$$(q^s - 1)^n \mathrm{Tr}(\mathscr{C}_q^s | \widehat{\Omega}_f) = -q^{-s}(q^s - 1)^{n+1} \left(\mathrm{Tr}(\mathscr{V}_q^s | R[\![\Delta]\!]) - 1 \right)$$

$$= -q^{-s} \left(q^s \, \#Z_f(\mathbb{F}_{q^s}) - (q^s - 1)^n - (q^s - 1)^{n+1} \right)$$

$$= (q^s - 1)^n - \#Z_f(\mathbb{F}_{q^s}) = \#Z_{\mathbb{T}^n \setminus Z_f}(\mathbb{F}_{q^s}). \qquad ∎$$