JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Hui June ZHU

On a theorem of Ax and Katz

Tome 29, n° 1 (2017), p. 137-150.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_1_137_0>

Journal de Théorie des Nombres
de Bordeaux **29** (2017), 137–150

On a theorem of Ax and Katz

par Hui June ZHU

Résumé. Le théorème bien connu d'Ax et Katz donne une borne sur la p-divisibilité du nombre de points rationnels sur une variété algébrique $\overline{V}$ sur un corps fini de caractéristique p en termes des degrés et des nombres de variables des polynômes qui definissent $\overline{V}$. Il a été amélioré par Adolphson–Sperber en termes du polytope de Newton du support $\mathscr{G}$ de $\overline{V}$. Dans cet article, nous démontrons que pour toute variété algébrique générique V sur $\overline{\mathbf{Q}}$ de support $\mathscr{G}$, la borne de Adolphson–Sperber peut être réalisée sur la fibre spéciale en p pour un ensemble de nombres premiers p de densité positive dans $\mathrm{Spec}(\mathbf{Z})$. De plus, nous définissons une fonction de $\mathscr{G}$, de nature combinatoire et explicitement calculable, dont la non nullité implique que la borne ci-dessus est réalisée à la fibre spéciale en p pour tout p assez grand.

Abstract. The well-known theorem of Ax and Katz gives a p-divisibility bound for the number of rational points on an algebraic variety $\overline{V}$ over a finite field of characteristic p in terms of the degree and number of variables of defining polynomials of $\overline{V}$. It was strengthened by Adolphson–Sperber in terms of Newton polytope of the support set $\mathscr{G}$ of $\overline{V}$. In this paper we prove that for every generic algebraic variety V over $\overline{\mathbf{Q}}$ supported on $\mathscr{G}$ the Adolphson–Sperber bound can be achieved on special fibre at p for a set of prime p of positive density in $\mathrm{Spec}(\mathbf{Z})$. Moreover, we show that if an explicitly computable combinatorial function on $\mathscr{G}$ is nonzero then the above bound is achieved at special fibre at p for all large enough p.

1. Introduction

In this paper p is a prime number and $q = p^a$ for some integer $a > 0$. Let $\overline{V}$ be an algebraic variety over $\mathbf{F}_q$ defined by a set of non-constant polynomials $\overline{f}_1, \ldots, \overline{f}_r$ in $\mathbf{F}_q[x_1, \ldots, x_n]$ in n variables. We study p-divisibility of the cardinality $|\overline{V}(\mathbf{F}_q)|$ of the set of $\mathbf{F}_q$-rational points on $\overline{V}$. This problem (in a slightly different form) was first proposed by Artin (see [2]) in 1935,

Manuscrit reçu le 18 février 2015, accepté le 7 juillet 2015.
Mathematics Subject Classification. 11G25,14G15.
Mots-clefs. Chevalley–Warning theorem, generic p-divisibility, L-function of exponential sums, zeros of polynomials over finite fields, Ax–Katz bound, weight of support set.

a first bound was given by Chevalley (see [4]) and Warning (see [9]) using elementary method. From then on p-divisibility problem is also known as *Chevalley–Warning problem*. If $q = p^a$ let $\mathrm{ord}_q(\cdot) = \frac{\mathrm{ord}_p(\cdot)}{a}$. Ax (see [3]) and subsequently Katz (see [6]) used Dwork's method to give the following bound which is well known as the *Ax–Katz bound*,

$$\mathrm{ord}_q|\overline{V}(\mathbf{F}_q)| \geq \left\lceil \frac{n - \sum_{j=1}^r \deg(\overline{f}_j)}{\max_{1\leq j\leq r} \deg(\overline{f}_j)} \right\rceil. \tag{1.1}$$

(See also [8] for an elementary proof.) For each integral point $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbf{Z}_{\geq 0}^n$ write $\sigma_p(\mathbf{g}) := \sum_{i=1}^n \sigma_p(g_i)$ where $\sigma(g_i)$ denote the sum of p-adic digits in $g_i \in \mathbf{Z}_{\geq 0}$. Define $\sigma_p(\overline{f}_j) := \max_{\mathbf{g}\in\mathscr{G}_j}(\sigma_p(\mathbf{g}))$. Moreno–Moreno observed that one can always reduce $\overline{V}/\mathbf{F}_q$ to $\overline{V}'/\mathbf{F}_p$ where $\overline{V}'$ is defined by a set of ra polynomials in na variables with degrees $\leq \sigma_p(\overline{f}_j)$ of $\overline{f}_j$. They apply Ax–Katz's bound on $\overline{V}'$ and get the *Moreno–Moreno bound*:

$$\mathrm{ord}_q|\overline{V}(\mathbf{F}_q)| \geq \frac{1}{a}\left\lceil a \cdot \frac{n - \sum_{j=1}^r \sigma_p(\overline{f}_j)}{\max_{1\leq j\leq r} \sigma_p(\overline{f}_j)} \right\rceil. \tag{1.2}$$

This bound only potentially improves Ax–Katz bound for small p, namely for $p < \max_j \deg(\overline{f}_j)$. Let $\overline{f} := z_1\overline{f}_1 + \ldots + z_r\overline{f}_r$ where $z_1, \ldots, z_r$ are new variables and $\Delta(\overline{f})$ its Newton polytope in $\mathbf{R}^{n+r}$. Let $w(\overline{f})$ be the least positive rational number c such that the dilation $c \cdot \Delta(\overline{f})$ contains an integral point of all positive coordinates. Adolphson–Sperber proved in [1] the following *Adolphson–Sperber bound* that strengthens Ax–Katz

$$\mathrm{ord}_q|\overline{V}(\mathbf{F}_q)| \geq w(\overline{f}) - r. \tag{1.3}$$

We prove in this paper that Adolphson–Sperber bound is an asymptotic generic bound in Theorem 1.1 below.

For $1 \leq j \leq r$ let $f_j = \sum_{\mathbf{g}\in\mathscr{G}_j} a_{j,\mathbf{g}}\mathbf{x}^{\mathbf{g}}$ where $a_{j,\mathbf{g}} \neq 0$. Let $V := V(f_1, \ldots, f_r)$ be the algebraic variety defined by the vanishing of $f_1, \ldots, f_r$. Write $\mathbb{A}^{\mathscr{G}_1,\ldots,\mathscr{G}_r}$ for the space of all such algebraic varieties V, and write $\mathbb{A}^{\mathscr{G}_1,\ldots,\mathscr{G}_r}(K)$ for all such V defined over K, that is, $f_j \in K[x_1, \ldots, x_n]$. For any V defined over $\overline{\mathbf{Q}}$, we consider it defined over a number field K that contains all coefficients of $f_1, \ldots, f_r$. Let $\overline{V}$ be the reduction (or special fiber) of V at a prime ideal $\wp$ over p in the ring of integers of K for p large enough. The reduction $\overline{V}$ obviously depends on the choices of K and $\wp$. Assuming the residue field of K at $\wp$ is $\mathbf{F}_q$ for $q = p^a$ then $\overline{V}$ is the algebraic variety over $\mathbf{F}_q$ defined by $\overline{f}_1, \ldots, \overline{f}_r$ in $\mathbf{F}_q[x_1, \ldots, x_n]$.

From now on for any $V = V(f_1, \ldots, f_r)$ over $\overline{\mathbf{Q}}$ we write $\boldsymbol{\mu} := w(f) - r$ where $f = z_1f_1 + \cdots + z_rf_r$ and $w(f)$ is, as above, the least positive rational number c such that $c \cdot \Delta(f)$ contains an integral point of all positive coordinates in $\mathbf{R}^{n+r}$. For p large enough (depending only on coefficients of f)

$w(f) = w(\overline{f})$ and hence $\boldsymbol{\mu} = w(f) - r = w(\overline{f}) - r$. We remark that, for any given V over $\overline{\mathbf{Q}}$ in $\mathbf{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}$ and p large enough, the nonnegative rational number $\boldsymbol{\mu}$ is simply a function on the support set $\mathscr{G}_1,\dots,\mathscr{G}_r$, and nothing else (see also (3.2) for a pure combinatorial definition of $\boldsymbol{\mu}$).

Theorem 1.1. *Fix $\mathscr{G}_1,\dots,\mathscr{G}_r$ in $\mathbf{Z}^n_{\geq 0}$, and let $\mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}$ be the space of all algebraic varieties supported on $\mathscr{G}_1,\dots,\mathscr{G}_r$.*

(1) *For every generic V in $\mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}(\overline{\mathbf{Q}})$ there exists a set of prime numbers p of positive density in* $\mathrm{Spec}(\mathbf{Z})$ *such that for any special fiber $\overline{V}$ at any prime ideal $\wp$ over p with residue field $\mathbf{F}_q$*

$$\mathrm{ord}_q|\overline{V}(\mathbf{F}_q)| = \boldsymbol{\mu}.$$

(2) *Let $\mathbf{c}(\mathscr{G}_1,\dots,\mathscr{G}_r)$ be a combinatorial function defined explicitly in* (3.12)*. If $\mathbf{c}(\mathscr{G}_1,\dots,\mathscr{G}_r) \neq 0$, then for every V in $\mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}(\overline{\mathbf{Q}})$ for every prime p large enough and for any special fiber $\overline{V}$ at any prime ideal $\wp$ over p that has residue field $\mathbf{F}_q$, we have*

$$\mathrm{ord}_q|\overline{V}(\mathbf{F}_q)| = \boldsymbol{\mu}$$

This theorem shows that the Adolphson–Sperber p-divisibility bound $\boldsymbol{\mu}$ is *asymptotically generically* sharp in the sense it can be achieved for a generic V over $\overline{\mathbf{Q}}$ at infinitely many special fibers. Furthermore, our statement implies that even though these special fibers $\overline{V}$ of V depend on the choice of base field K for V and prime $\wp$ in K over p, for a generic V over $\overline{\mathbf{Q}}$ we have $\mathrm{ord}_q|\overline{V}(\mathbf{F}_q)| = \boldsymbol{\mu}$ that is independent of all these choices for a set of primes p of positive density in $\mathrm{Spec}(\mathbf{Z})$. When the support set $(\mathscr{G}_1,\dots,\mathscr{G}_r)$ satisfies certain combinatorial condition a generic V over $\mathbf{Q}$ achieves the p-divisibility bound for all but finitely many p.

Examples 1.2. Suppose $V(f)$ is any hypersurface defined by $f = \sum_{\mathbf{g}\in\mathscr{G}} a_{\mathbf{g}}\mathbf{x}^{\mathbf{g}}$ in $\mathbf{Q}[x_1,\dots,x_n]$ where $a_{\mathbf{g}} \in \mathbf{Q}^*$ and $\mathscr{G}$ consists of all $\mathbf{g} = (g_1,\dots,g_n) \in \mathbf{Z}^n_{\geq 0}$ with $|\mathbf{g}| := \sum_{i=1}^n g_i = d$. Let $n \geq d$. Then Theorem 1.1 implies that $\mathrm{ord}_p|\overline{V}(\mathbf{F}_p)| \geq \lceil \frac{n-d}{d} \rceil$, the same as the Ax–Katz bound. A consequence of Theorem 1.1(1) is that for all generic such $V(f)$ over $\mathbf{Q}$ we have $\mathrm{ord}_p|\overline{V}(\mathbf{F}_p)| = \lceil \frac{n-d}{d} \rceil$ for primes p in a set of positive density in $\mathrm{Spec}(\mathbf{Z})$. In comparison, Katz showed in [6, Section 5] there is an explicit algebraic surface over $\mathbf{F}_p$ for every prime p that his bound is achieved.

Examples 1.3. Suppose $V(f)$ is any hypersurface with $f = a_1x_1^3x_2^3 + a_2x_2^2x_3^2$ where $a_1, a_2 \in \mathbf{Z} - \{0\}$. One can check by direct computation that $|\overline{V}(\mathbf{F}_p)| = p(2p-1)$ for all p, hence $\mathrm{ord}_p|\overline{V}(\mathbf{F}_p)| = 1$. By Theorem 1.1(2) we have $\mathrm{ord}_p(|\overline{V}(\mathbf{F}_p)|) \geq 1$ and the equality holds for all $V(f)$ and at all prime p large enough. In comparison, Ax–Katz bound says that $\mathrm{ord}_p(|\overline{V}(\mathbf{F}_p)|) \geq 0$ which is weaker in this example.

Our proof uses Dwork method. We first briefly recall necessary p-adic theory to study the number of rational points $|\overline{V}(\mathbf{F}_q)|$ of algebraic variety $\overline{V}$ over $\mathbf{F}_q$ in Section 2, then we prepare some $\mathbf{A}$-polynomials where variables $\mathbf{A}$ parametrize the coefficients of defining polynomials of V over $\overline{\mathbf{Q}}$ in Section 3. This section is technical and combinatorial. We start to prove our theorem for algebraic variety V over $\mathbf{Q}$ and then reduce the general case V over $\overline{\mathbf{Q}}$ to that over $\mathbf{Q}$ immediately. Our proof of the main Theorem 1.1 lies in Section 4.

Acknowledgments. We thank Regis Blache and Kiran Kedlaya for very helpful comments on earlier versions of this paper.

2. Rational points and the trace

For the rest of the paper we fix nonempty subsets $\mathscr{G}_1, \ldots, \mathscr{G}_r$ in $\mathbf{Z}_{\geq 0}^n$. They may or may not be distinct. Let $\overline{f}_1, \ldots, \overline{f}_r$ be any polynomials in $\mathbf{F}_q[x_1, \ldots, x_n]$ with supporting coefficient sets $\mathscr{G}_1, \ldots, \mathscr{G}_r$ respectively. That is, for each $j = 1, \ldots, r$ one can write $\overline{f}_j = \sum_{\mathbf{g} \in \mathscr{G}_j} \overline{a}_{j,\mathbf{g}} \mathbf{x}^{\mathbf{g}}$ for $\overline{a}_{j,\mathbf{g}} \in \mathbf{F}_q^*$. Let $\overline{f} = z_1\overline{f}_1 + \ldots + z_r\overline{f}_r \in \mathbf{F}_q[x_1, \ldots, x_n, z_1, \ldots, z_r]$. Let C be a nonempty subset of $\{1, \ldots, n\}$ and we write $\mathbf{Z}_{>0}^C$ (resp. $\mathbf{Z}_{\geq 0}^C$) for the subset of $\mathbf{Z}_{\geq 0}^n$ with i-th component in $\mathbf{Z}_{\geq 1}$ (resp. $\mathbf{Z}_{\geq 0}$) if $i \in C$ and equal to 0 if $i \notin C$. Let B be a nonempty subset of $\{1, \ldots, r\}$, and let $\mathbf{Z}_{>0}^B$ be defined similarly. Let $\mathscr{G}_{j,C} := \mathscr{G}_j \cap \mathbf{Z}_{\geq 0}^C$. Write $\mathbf{v} = (v_i)_{i=1}^n$ and $\mathbf{t} = (t_j)_{j=1}^r$. Let

$$\mathscr{Z}_{B,C} := \Bigg\{ (\mathbf{t}, \mathbf{v}) \in \mathbf{Z}_{>0}^B \times \mathbf{Z}_{>0}^C \;\Bigg|\; \mathbf{v} = \sum_{j \in B} \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}} \mathbf{g}, u_{\mathbf{g}} \in \mathbf{Q}_{\geq 0}, \; t_j = \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}} \in \mathbf{Z}_{\geq 1} \text{ for each } j \in B \Bigg\}. \tag{2.1}$$

For every pair $(\mathbf{t}, \mathbf{v})$ in $\mathscr{Z}_{B,C}$ we write $\mathbf{z}^{\mathbf{t}}\mathbf{x}^{\mathbf{v}} = \prod_{j \in B} z_j^{t_j} \prod_{i \in C} x_i^{v_i}$. Let

$$\mathscr{Q}_{B,C} := \Bigg\{ (\mathbf{u}, \mathbf{v}) \in \mathbf{Q}_{\geq 0}^{\sum_{j \in B} |\mathscr{G}_{j,C}|} \times \mathbf{Z}_{>0}^C \;\Bigg|\; \mathbf{v} = \sum_{\mathbf{g}} u_{\mathbf{g}} \mathbf{g}, u_{\mathbf{g}} \in \mathbf{Q}_{\geq 0}, \; \mathbf{u} = (u_{\mathbf{g}})_{\mathbf{g} \in \cup_{j \in B} \mathscr{G}_{j,C}}, \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}} \in \mathbf{Z}_{\geq 1} \text{ for each } j \in B \Bigg\}. \tag{2.2}$$

Write the subset of integral points in $\mathscr{Q}_{B,C}$ by $(\mathscr{Q}_{B,C})_{\mathbf{Z}}$. Then we have the natural surjective map

$$\iota : \mathscr{Q}_{B,C} \twoheadrightarrow \mathscr{Z}_{B,C} \tag{2.3}$$

that sends all $(\mathbf{u}, \mathbf{v})$ to $(\mathbf{t}, \mathbf{v})$ with $t_j = \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}}$. Let $|\mathbf{t}| := \sum_{j=1}^r t_j$ and $|\mathbf{u}| := \sum_{j \in B} \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}}$. For $(\mathbf{u}, \mathbf{v})$ in $\mathscr{Q}_{B,C}$ and $(\mathbf{t}, \mathbf{v}) = \iota(\mathbf{u}, \mathbf{v})$ in $\mathscr{Z}_{B,C}$, we have $|\mathbf{t}| = |\mathbf{u}|$.

Let $E_p(x)$ be the p-adic Artin–Hasse exponential function. We write $E_p(x) = \sum_{i=0}^{\infty} \delta_i x^i$ where $\delta_i \in \mathbf{Z}_p \cap \mathbf{Q}$. For $0 \le i \le p-1$, $\delta_i = \frac{1}{i!}$. Let γ be a root of $\log E_p(x) = \sum_{i=0}^{\infty} \frac{x^{p^i}}{p^i}$ with $\mathrm{ord}_p \gamma = \frac{1}{p-1}$ in $\overline{\mathbf{Q}}_p$. Notice that

$$\frac{\gamma^{p-1}}{p} \equiv -1 \bmod \gamma. \tag{2.4}$$

For each (B, C) as defined above, we define a $\mathbf{Z}_q[\gamma]$-algebra

$$\mathscr{H}_{B,C} := \left\{ \sum_{(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C}} c_{\mathbf{t},\mathbf{v}} \gamma^{|\mathbf{t}|} \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}} \;\middle|\; c_{\mathbf{t},\mathbf{v}} \in \mathbf{Z}_q \right\}. \tag{2.5}$$

This is a subalgebra of $\mathbf{Z}_q[x_1, \ldots, x_n, \gamma z_1, \ldots, \gamma z_r]$. Let $\overline{f}_{B,C}$ be the restriction of $\overline{f}$ for $j \in B$ and $i \in C$, namely,

$$\overline{f}_{B,C} = \sum_{j \in B} \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} \overline{a}_{j,\mathbf{g}} z_j \mathbf{x}^{\mathbf{g}}.$$

Let $\widehat{a}_{j,\mathbf{g}}$ be the Teichmüller lifting of $\overline{a}_{j,\mathbf{g}}$ to $\mathbf{Z}_q^*$, then Dwork's splitting function of $\overline{f}_{B,C}$ is $G_{\overline{f}_{B,C}} := \prod_{j \in B} \prod_{\mathbf{g} \in \mathscr{G}_{j,C}} E_p(\gamma \widehat{a}_{j,\mathbf{g}} z_j \mathbf{x}^{\mathbf{g}})$, which lies in $\mathscr{H}_{B,C}$. Write $\mathbf{a}^{\mathbf{u}} = \prod_{j \in B} \prod_{\mathbf{g} \in \mathscr{G}_{j,C}} a_{j,\mathbf{g}}^{u_{\mathbf{g}}}$ and write $\widehat{\mathbf{a}}^{\mathbf{u}}$ for the corresponding Teichmüller lifting similarly. Then its expansion is

$$G_{\overline{f}_{B,C}} = \sum_{(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C}} G_{\mathbf{t},\mathbf{v}} \gamma^{|\mathbf{t}|} \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}$$

where its coefficients are given by

$$G_{\mathbf{t},\mathbf{v}} = \sum_{(\mathbf{u},\mathbf{v})} \Big(\prod_{\mathbf{u}} \delta_{u_{\mathbf{g}}} \Big) \widehat{\mathbf{a}}^{\mathbf{u}} \tag{2.6}$$

and the sum ranges over all $(\mathbf{u}, \mathbf{v}) \in (\iota^{-1}(\mathbf{t}, \mathbf{v})) \cap (\mathscr{Q}_{B,C})_{\mathbf{Z}}$. Notice that $G_{\mathbf{t},\mathbf{v}} = 0$ if and only if $(\iota^{-1}(\mathbf{t}, \mathbf{v})) \cap (\mathscr{Q}_{B,C})_{\mathbf{Z}} = \emptyset$.

Define an operator ψ_p on $\mathscr{H}_{B,C}$ by

$$\psi_p \left(\sum_{(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C}} c_{\mathbf{t},\mathbf{v}} \gamma^{|\mathbf{t}|} \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}} \right) = \sum_{(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C}} c_{p\mathbf{t},p\mathbf{v}} \gamma^{p|\mathbf{t}|} \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}. \tag{2.7}$$

One can check that $\mathscr{H}_{B,C}$ is closed under ψ_p. Indeed, suppose $(\mathbf{t}, \mathbf{v}) \in \mathscr{Z}_{B,C}$ and $(\mathbf{t}, \mathbf{v}) = (p\mathbf{t}', p\mathbf{v}')$ with $(\mathbf{t}', \mathbf{v}')$ with all corresponding entries of $\mathbf{t}'$ and $\mathbf{v}'$ in $\mathbf{Z}_{\ge 1}$, then $p\mathbf{v}' = \mathbf{v} = \sum u_{\mathbf{g}} \mathbf{g}$ and $pt'_j = t_j = \sum_{\mathbf{g} \in \mathscr{G}_{C,j}} u_{\mathbf{g}} \in \mathbf{Z}_{\ge 1}$ with $u_g \in \mathbf{Q}_{\ge 0}$. We have $\mathbf{v}' = \sum (u_{\mathbf{g}}/p)\mathbf{g}$ and $t'_j = \sum_{\mathbf{g} \in \mathscr{G}_{C,j}} (u_{\mathbf{g}}/p) \in \mathbf{Z}_{\ge 1}$, so $(\mathbf{t}', \mathbf{v}') \in \mathscr{Z}_{B,C}$ and hence $\mathscr{H}_{B,C}$ is closed under the operator ψ_p.

Let τ be the Frobenius automorphism of $\mathbf{Q}_q(\gamma)$ over $\mathbf{Q}_p(\gamma)$ and its induced map on $\mathscr{H}_{B,C}$ is $\tau^{-1}(\sum c_{\mathbf{t},\mathbf{v}} \gamma^{|\mathbf{t}|} \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}) = \sum \tau^{-1}(c_{\mathbf{t},\mathbf{v}} \gamma^{|\mathbf{t}|}) \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}$. Let

$\boldsymbol{\alpha}_{\overline{f}_{B,C}}$ be the Dwork operator on $\mathscr{H}_{B,C}$ defined by

$$\boldsymbol{\alpha}_{\overline{f}_{B,C}} := \tau^{-1} \circ \psi_p \circ G_{\overline{f}_{B,C}}. \tag{2.8}$$

Let $\mathscr{H}_{B,C}^{(\ell)}$ denote the sub-algebra of $\mathscr{H}_{B,C}$ with $|\mathbf{t}| = \ell$, we have a decomposition $\mathscr{H}_{B,C} = \oplus_{\ell \in \mathbf{Z}_{\geq 0}} \mathscr{H}_{B,C}^{(\ell)}$. Note that $\psi_p(\sum c_{\mathbf{t},\mathbf{v}} \gamma^\ell \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}) = \gamma^{(p-1)\ell} \sum c_{p\mathbf{t},p\mathbf{v}} \gamma^\ell \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}$. Then $\psi_p(\mathscr{H}_{B,C}) \subseteq \oplus_{\ell \in \mathbf{Z}_{\geq 0}} p^\ell \mathscr{H}_{B,C}^{(\ell)}$. Since $G_{\overline{f}_{B,C}}$ lies in $\mathscr{H}_{B,C}$, we have $G_{\overline{f}_{B,C}} \cdot \mathscr{H}_{B,C} \subseteq \mathscr{H}_{B,C}$. Then it follows

$$\boldsymbol{\alpha}_{\overline{f}_{B,C}}(\mathscr{H}_{B,C}) \subseteq \oplus_{\ell \in \mathbf{Z}_{\geq 0}} p^\ell \mathscr{H}_{B,C}^{(\ell)}.$$

From now on we order elements $(\mathbf{t}, \mathbf{v})$ in $\mathscr{Z}_{B,C}$ so that $|\mathbf{t}|$ is nondecreasing, and in this way $\mathscr{Z}_{B,C}$ becomes a partially ordered set. Choose the weighted monomial basis $\{\gamma^{|\mathbf{t}|} \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}\}$ for $\mathscr{H}_{B,C}$ over $\mathbf{Z}_q$ with the pairs $(\mathbf{t}, \mathbf{v})$ ranging in (the partially ordered set) $\mathscr{Z}_{B,C}$. Then

$$\boldsymbol{\alpha}_{\overline{f}_{B,C}}(\gamma^{|\mathbf{t}'|} \mathbf{z}^{\mathbf{t}'} \mathbf{x}^{\mathbf{v}'}) = \sum_{(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C}} (\tau^{-1} \gamma^{(p-1)|\mathbf{t}|} G_{p\mathbf{t}-\mathbf{t}',p\mathbf{v}-\mathbf{v}'}) \gamma^{|\mathbf{t}|} \mathbf{z}^{\mathbf{t}} \mathbf{x}^{\mathbf{v}}, \tag{2.9}$$

where $G_{-,-}$ is as defined in (2.6). Write the infinite matrix

$$M_{B,C} := \left(\gamma^{(p-1)|\mathbf{t}|} G_{p\mathbf{t}-\mathbf{t}',p\mathbf{v}-\mathbf{v}'}\right)_{(\mathbf{t}',\mathbf{v}'),(\mathbf{t},\mathbf{v})} \tag{2.10}$$

where the row and column are indexed by the pairs $(\mathbf{t}', \mathbf{v}')$ and $(\mathbf{t}, \mathbf{v})$ in $\mathscr{Z}_{B,C}$, respectively. This matrix lies over $\mathbf{Q}_q[\gamma]$. Then the matrix of $\boldsymbol{\alpha}_{\overline{f}_{B,C}}$ with respect to the above weighted monomial basis is $\mathrm{Mat}(\boldsymbol{\alpha}_{\overline{f}_{B,C}}) = \tau^{-1} M_{B,C}$. For any matrix M we write

$$M^{[a]} := M^{\tau^{a-1}} \cdots M^\tau M. \tag{2.11}$$

For a compositions of the Dwork operator $\boldsymbol{\alpha}^a_{\overline{f}_{B,C}} = \boldsymbol{\alpha}_{\overline{f}_{B,C}} \circ \cdots \circ \boldsymbol{\alpha}_{\overline{f}_{B,C}}$, we have

$$\mathrm{Mat}(\boldsymbol{\alpha}^a_{\overline{f}_{B,C}}) = M^{[a]}_{B,C}.$$

Theorem 2.1. *Let $\overline{V}$ be algebraic variety defined by the polynomials $\overline{f}_1, \ldots, \overline{f}_r \in \mathbf{F}_q[x_1, \ldots, x_n]$ with $q = p^a$. For any nonempty subsets B, C in $\{1, \ldots, r\}$ and $\{1, \ldots, n\}$ respectively let $M_{B,C}$ be the nuclear matrix defined in* (2.10)*. Then*

$$|\overline{V}(\mathbf{F}_q)| = q^n + \sum_{B,C} (q-1)^{|B|+|C|} q^{n-|B|-|C|} \mathrm{Tr}(M^{[a]}_{B,C}). \tag{2.12}$$

Proof. We have already shown above that $\boldsymbol{\alpha}_{\overline{f}_{B,C}}$ is a nuclear operator on $\mathscr{H}_{B,C}$ (see [5] or [7]). Our statement follows the same standard counting argument as that for (3.5.4) in [6]. □

For a nuclear matrix M over a p-adic valuation ring R, we write $\mathrm{ord}_p M$ for the minimum p-adic order of all entries of M.

Lemma 2.2. *Let $q = p^a$ and $k \in \mathbf{Z}_{\geq 0}$. Let M be a nuclear matrix over a p-adic valuation ring of the block form*

$$\frac{M}{p^k} = \begin{pmatrix} M_{11} & M_{12} \\ p^{>0}M_{21} & p^{>0}M_{22} \end{pmatrix} + (p^{>0})$$

where M_{11} is a square submatrix, M_{ij} are all submatrix such that $\mathrm{ord}_p M_{ij} \geq 0$. Let $M^{[a]}$ be as defined in (2.11)*. Then we have $\frac{\mathrm{Tr}(M^{[a]})}{q^k} \equiv \mathrm{Tr}(M_{11}^{[a]}) \bmod (p^{>0})$. In particular, if $\mathrm{ord}_q \mathrm{Tr}(M_{11}^{[a]}) = 0$ then $\mathrm{ord}_q \mathrm{Tr}(M^{[a]}) = k$.*

Proof. Notice that

$$\frac{M^{[a]}}{p^{ak}} = \frac{M^{\tau^{a-1}}}{p^k} \cdots \frac{M^{\tau}}{p^k} \frac{M}{p^k} \equiv \begin{pmatrix} M_{11}^{[a]} & \star \\ 0 & 0 \end{pmatrix} \bmod (p^{>0})$$

where $\mathrm{ord}_p \star \geq 0$. Thus

$$\frac{M^{[a]}}{q^k} \equiv \begin{pmatrix} M_{11}^{[a]} & \star \\ 0 & 0 \end{pmatrix} \bmod (p^{>0}).$$

Taking trace on both sides, we get $\frac{\mathrm{Tr}(M^{[a]})}{q^k} \equiv \mathrm{Tr}(M_{11}^{[a]}) \bmod (p^{>0})$ which proves our statement. □

As the nuclear matrix $M_{B,C}$ has its entries as polynomials in coefficients $\overline{\mathbf{a}} = (\overline{a}_{j,\mathbf{g}})$ of the defining polynomials $\overline{f}_j = \sum_{\mathbf{g} \in \mathscr{G}_j} \overline{a}_{j,\mathbf{g}} \mathbf{x}^{\mathbf{g}}$, we shall *deform* each entry to polynomials in variables $\mathbf{A} := (A_{j,\mathbf{g}})$. Subsequently, the trace of $M_{B,C}$ is also *deformed* to a polynomial in $\mathbf{A}$. This idea is pronounced in the following Section 3.

3. A-deformations and A-polynomials

The sets $\mathscr{G}_1, \ldots, \mathscr{G}_r$ in $\mathbf{Z}_{\geq 0}^n$ are fixed. Recall that B, C are nonempty subsets in $\{1, \ldots, r\}$ and $\{1, \ldots, n\}$, respectively. Define an integral weight of each pair (B, C) by

$$w_{\mathbf{Z}}(B,C) := \min_{\mathbf{v} \in \mathbf{Z}_{>0}^n} \Bigg\{ \sum_{j \in B} \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}} \,\Bigg|\, \mathbf{v} = \sum_{j \in B} \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}} \mathbf{g}, \text{ with } u_{\mathbf{g}} \in \mathbf{Q}_{\geq 0}, \sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}} \in \mathbf{Z}_{\geq 1} \text{ for every } j \in B \Bigg\}. \tag{3.1}$$

If no representation of $\mathbf{v}$ as described in (3.1) exists, then assign $w_{\mathbf{Z}}(B,C) = +\infty$. Otherwise $|B| \leq w_{\mathbf{Z}}(B,C) \leq r$ where $|B|$ denotes the cardinality of B. From the definition $\mathscr{Z}_{B,C}$ from (2.1) one observes clearly $w_{\mathbf{Z}}(B,C) = \min\{|\mathbf{t}| | (\mathbf{t}, \mathbf{v}) \in \mathscr{Z}_{B,C}\}$. Let $\mathscr{Z}_{B,C}^{min}$ be the (finite) subset of $\mathscr{Z}_{B,C}$ consisting

of all $(\mathbf{t},\mathbf{v})$ in that the minimal bound $w_{\mathbf{Z}}(B,C)$ is realized, that is $|\mathbf{t}| = w_{\mathbf{Z}}(B,C)$. We can show by combinatorics that

$$\boldsymbol{\mu} = \min_{B,C}\Big\{n - |B| - |C| + w_{\mathbf{Z}}(B,C)\Big\}. \tag{3.2}$$

Let $\mathscr{K}$ be the (nonempty) set of all (B,C) with $n-|B|-|C|+w_{\mathbf{Z}}(B,C) = \boldsymbol{\mu}$. By this definition one observes that $\mathscr{Z}^{min}_{B,C} \neq \emptyset$ for each $(B,C) \in \mathscr{K}$. Hence

$$\mathscr{Z}^{min} := \bigcup_{(B,C)\in\mathscr{K}} \mathscr{Z}^{min}_{B,C} \tag{3.3}$$

is a nonempty set consisting of all $(\mathbf{t},\mathbf{v}) \in \mathbf{Z}^B_{>0} \times \mathbf{Z}^C_{>0}$ with $|\mathbf{t}| = \boldsymbol{\mu} - n + |B| + |C| = w_{\mathbf{Z}}(B,C)$.

Write $\mathbf{A} = (A_{j,\mathbf{g}})_{j\in B,\mathbf{g}\in\mathscr{G}_{j,C}}$ for variables. Let $G_{\mathbf{t},\mathbf{v}}(\mathbf{A})$ be the polynomial obtained via replacing each $\widehat{\mathbf{a}}$ in $G_{\mathbf{t},\mathbf{v}}$ in (2.6) by variables $\mathbf{A}$.

$$G_{\mathbf{t},\mathbf{v}}(\mathbf{A}) := \sum_{(\mathbf{u},\mathbf{v})} \prod_{\mathbf{u}} \Big(\prod_{\mathbf{g}} \delta_{u_{\mathbf{g}}}\Big)\mathbf{A}^{\mathbf{u}} \tag{3.4}$$

where $(\mathbf{u},\mathbf{v}) \in (\iota^{-1}(\mathbf{t},\mathbf{v})) \cap (\mathscr{Q}_{B,C})_{\mathbf{Z}}$. Since all $\delta_i \in \mathbf{Z}_p \cap \mathbf{Q}$ for all i we have $G_{\mathbf{t},\mathbf{v}}(\mathbf{A})$ lies in $(\mathbf{Z}_p \cap \mathbf{Q})[\mathbf{A}]$. For any $(\mathbf{t}',\mathbf{v}')$ and $(\mathbf{t},\mathbf{v})$ in $\mathscr{Z}_{B,C}$ we have

$$G_{p\mathbf{t}-\mathbf{t}',p\mathbf{v}-\mathbf{v}'}(\mathbf{A}) = \sum_{(\mathbf{u}'',p\mathbf{v}-\mathbf{v}')} \prod_{\mathbf{u}''} \Big(\prod_{\mathbf{g}} \delta_{u''_{\mathbf{g}}}\Big)\mathbf{A}^{\mathbf{u}''} \tag{3.5}$$

where the sum is over all $(\mathbf{u}'', p\mathbf{v}-\mathbf{v}') \in (\iota^{-1}(p\mathbf{t}-\mathbf{t}', p\mathbf{v}-\mathbf{v}')) \cap (\mathscr{Q}_{B,C})_{\mathbf{Z}}$. That is, $u''_{\mathbf{g}} \in \mathbf{Z}_{\geq 0}$ and $p\mathbf{v}-\mathbf{v}' = \sum_{\mathbf{g}} u''_{\mathbf{g}}\mathbf{g}$. Let $M_{B,C}(\mathbf{A})$ be the paramaterized nuclear matrix over $(\mathbf{Z}_p \cap \mathbf{Q})[\gamma][\mathbf{A}]$ deforming $M_{B,C}$ in (2.10)

$$M_{B,C}(\mathbf{A}) := \Big(\gamma^{(p-1)|\mathbf{t}|} G_{p\mathbf{t}-\mathbf{t}',p\mathbf{v}-\mathbf{v}'}(\mathbf{A})\Big)_{(\mathbf{t}',\mathbf{v}'),(\mathbf{t},\mathbf{v})}, \tag{3.6}$$

where the subindices range over $\mathscr{Z}_{B,C}$. Let

$$N_{B,C}(\mathbf{A}) := \big(G_{p\mathbf{t}-\mathbf{t}',p\mathbf{v}-\mathbf{v}'}(\mathbf{A})\big)_{(\mathbf{t}',\mathbf{v}'),(\mathbf{t},\mathbf{v})}$$

where $(\mathbf{t},\mathbf{v})$ and $(\mathbf{t}',\mathbf{v}')$ lie in $\mathscr{Z}^{min}_{B,C}$. Then by (2.4) and the definitions,

$$(-1)^{w_{\mathbf{Z}}(B,C)} \frac{M_{B,C}(\mathbf{A})}{p^{w_{\mathbf{Z}}(B,C)}} = \begin{pmatrix} N_{B,C}(\mathbf{A}) & M_{12} \\ p^{>0}M_{21} & p^{>0}M_{22}\end{pmatrix} + (p^{>0}) \tag{3.7}$$

for some submatrices M_{12}, M_{21}, M_{22} all with $\mathrm{ord}_p(M_{ij}) \geq 0$.

For any matrix $M(\mathbf{A})$ over $K[\mathbf{A}]$ where K is any field with τ-action, we define $\tau(\mathbf{A}) := \mathbf{A}^p$ and

$$M(\mathbf{A})^{[a]} := M(\mathbf{A})^{\tau^{a-1}} \cdots M(\mathbf{A}) = M^{\tau^{a-1}}(\mathbf{A}^{p^{a-1}}) \cdots M(\mathbf{A}). \tag{3.8}$$

Lemma 3.1. *Let $M_{B,C}(\mathbf{A})^{[a]}$ and $N_{B,C}(\mathbf{A})^{[a]}$ be defined as in* (3.8)*. Then we have*

$$\frac{\mathrm{Tr}(M_{B,C}(\mathbf{A})^{[a]})}{q^{w_{\mathbf{Z}}(B,C)}} \equiv (-1)^{aw_{\mathbf{Z}}(B,C)} \mathrm{Tr}(N_{B,C}(\mathbf{A})^{[a]}) \bmod p^{>0}.$$

Proof. By (3.7), we may apply Lemma 2.2 to the matrix $M_{11} := (-1)^{w_{\mathbf{Z}}(B,C)} N_{B,C}(\mathbf{A})$ and $M := M_{B,C}(\mathbf{A})$ to conclude. □

For any p-adic valuation ring R and polynomial $F(\mathbf{A})$ in $R[\mathbf{A}]$ let $\mathrm{ord}_p(F(\mathbf{A}))$ be the minimum of the p-adic orders of all coefficients of $F(\mathbf{A})$. Since $|\mathbf{t}| \geq w_{\mathbf{Z}}(B,C)$ for all $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C}$, we have

$$\mathrm{ord}_q \mathrm{Tr}(M_{B,C}(\mathbf{A})^{[a]}) \geq \mathrm{ord}_q M_{B,C}(\mathbf{A})^{[a]} \geq w_{\mathbf{Z}}(B,C). \tag{3.9}$$

Definition 3.2. Let $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C}$ where $\mathscr{Z}_{B,C}$ is defined as in (2.1). Consider the set of all *rational representations* of $(\mathbf{t},\mathbf{v})$ in terms of $\mathscr{G}_1,\dots,\mathscr{G}_r$, namely, $\mathbf{v} = \frac{1}{d}\sum_{j\in B}\sum_{\mathbf{g}\in\mathscr{G}_{j,C}} r_{\mathbf{g}}\mathbf{g}$ with $d, r_{\mathbf{g}} \in \mathbf{Z}_{\geq 0}$ and all $r_{\mathbf{g}}$'s are coprime such that $\frac{1}{d}\sum_{\mathbf{g}\in\mathscr{G}_{j,C}} r_{\mathbf{g}} = t_j \in \mathbf{Z}_{\geq 1}$ for all $j \in B$ and $|\mathbf{t}| = \sum_{j\in B} t_j = w_{\mathbf{Z}}(B,C)$.

Let $\mathscr{D}$ be the nonempty finite set of all denominators d of rational representations of all $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}^{min}$.

Lemma 3.3. *(1) For each $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}_{B,C} \cap \iota((\mathscr{Q}_{B,C})_{\mathbf{Z}})$, there is 1-1 correspondence between a term with monomial $\prod_{\mathbf{g}} A_{\mathbf{g}}^{u_{\mathbf{g}}}$ in the expansion of $G_{\mathbf{t},\mathbf{v}}(\mathbf{A})$ as in* (3.4) *and $(\mathbf{u},\mathbf{v}) \in \iota^{-1}(\mathbf{t},\mathbf{v}) \cap (\mathscr{Q}_{B,C})_{\mathbf{Z}}$ such that $\mathbf{v} = \sum_{\mathbf{g}} u_{\mathbf{g}}\mathbf{g}$. In particular $\sum_{\mathbf{g}} u_{\mathbf{g}} = |\mathbf{t}|$.*

(2) Let $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}^{min}$. For each prime p, there is a 1-1 correspondence between a nonzero term with monomial $\prod_{\mathbf{g}} A_{\mathbf{g}}^{u''_{\mathbf{g}}}$ in the expansion of $G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A})$ and a rational representation of $(\mathbf{t},\mathbf{v})$

$$\mathbf{v} = \frac{1}{d}\sum_{j\in B}\sum_{\mathbf{g}\in\mathscr{G}_{j,C}} r_{\mathbf{g}}\mathbf{g}$$

with all $d|(p-1)$, in which $u''_{\mathbf{g}} = \frac{(p-1)}{d} r_{\mathbf{g}} \leq p-1$ and $\sum_{\mathbf{g}} u''_{\mathbf{g}} = (p-1)w_{\mathbf{Z}}(B,C)$.

For $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}^{min}$, we have

$$\begin{aligned} G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A}) &= \sum_{(\mathbf{u}'',(p-1)\mathbf{v})} \left(\prod_{\mathbf{g}} \delta_{u''_{\mathbf{g}}}\right) \mathbf{A}^{\mathbf{u}''} \\ &= \sum_{d\in\mathscr{D}, d|(p-1)} \sum_{(\mathbf{u},\mathbf{v})} \left(\prod_{\mathbf{g}} \delta_{u''_{\mathbf{g}}}\right) \left(\prod_{\mathbf{g}} A_{j,\mathbf{g}}^{u''_{\mathbf{g}}}\right) \end{aligned}$$

where the last sum ranges over all rational representations of $(\mathbf{t},\mathbf{v})$ with denominator $d|(p-1)$. Each term has coefficient in $\mathbf{Z}_p^*$ and $A_{j,\mathbf{g}}$-degree $\leq p-1$.

Proof. The proof of Part (1) is elementary hence we omit it here. Notice that since $|\mathbf{t}|$ is minimal we have $\frac{r_{\mathbf{g}}}{d} \leq 1$. From Part (1) and the observation

above we have $u''_{\mathbf{g}} = (p-1)\frac{r_{\mathbf{g}}}{d} \leq p-1$. This implies that $\delta_{u''_{\mathbf{g}}} = \frac{1}{u''_{\mathbf{g}}!} \in \mathbf{Z}_p^*$. Then Part (2) follows. □

Define a Hasse polynomial in $(\mathbf{Q}\cap\mathbf{Z}_p)[\mathbf{A}]$ for the trace of $\boldsymbol{\alpha}^a_{f_{B,C}}$ as follows

$$H_p^{[a]}(\mathbf{A}) := \sum_{(B,C)\in\mathscr{K}} (-1)^{|B|+|C|+aw_{\mathbf{Z}}(B,C)} \mathrm{Tr}(N_{B,C}(\mathbf{A})^{[a]}). \tag{3.10}$$

Write $H_p(\mathbf{A}) := H_p^{[1]}(\mathbf{A})$ for simplicity then

$$H_p(\mathbf{A}) = \sum_{(B,C)\in\mathscr{K}} (-1)^{|B|+|C|+w_{\mathbf{Z}}(B,C)} \sum_{(\mathbf{t},\mathbf{v})\in\mathscr{Z}^{min}_{B,C}} G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A}).$$

Lemma 3.4. *Let p be any prime with $p \equiv 1 \bmod d$ for all d in $\mathscr{D}$. Let $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}^{min}$.*

(1) Then the expansion of $G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A})$ in Lemma 3.3(2) has each term in $(\mathbf{Z}_p^*\cap\mathbf{Q})[\mathbf{A}]$ with $A_{j,\mathbf{g}}$-degree $\leq p-1$ and homogenous of total degree $(p-1)w_{\mathbf{Z}}(B,C)$. Furthermore, $H_p(\mathbf{A}) \not\equiv 0 \bmod p$.

(2) There is a constant $\theta(\mathscr{G}_1,\ldots,\mathscr{G}_r)$ such that for $p > \theta(\mathscr{G}_1,\ldots,\mathscr{G}_r)$ we have $\mathrm{Tr}(N_{B,C}(\mathbf{A})^{[a]}) \not\equiv 0 \bmod p$ and $H_p^{[a]}(\mathbf{A}) \not\equiv 0 \bmod p$ is homogenous of total degree $(p^a-1)w_{\mathbf{Z}}(B,C)$,

Proof. (1) Notice that

$$H_p(\mathbf{A}) = \sum_{(B,C)\in\mathscr{K}} \sum_{(\mathbf{t},\mathbf{v})\in\mathscr{Z}^{min}} (-1)^{|B|+|C|+w_{\mathbf{Z}}(B,C)} G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A}).$$

The first statement is simply rephrasing the statement in Lemma 3.3(2).

By Lemma 3.3(2) and our hypothesis, each term of the expansion of $G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A})$ is nonzero mod p. Now we claim that for any $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}^{min}_{B,C}$ and $(\mathbf{t}',\mathbf{v}') \in \mathscr{Z}^{min}_{B',C'}$ where $(B,C) \neq (B',C')$ the corresponding $G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}$ and $G_{(p-1)\mathbf{t}',(p-1)\mathbf{v}'}$ do not have common terms to cancel. Indeed, suppose $B \neq B'$, then there exists $j \in B\backslash B'$ where $A_{j,\mathbf{g}}^{\frac{p-1}{d}r_{\mathbf{g}}}$ lies in a monomial of $G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A})\backslash G_{(p-1)\mathbf{t}',(p-1)\mathbf{v}'}(\mathbf{A})$. On the other hand suppose $C \neq C'$. Then there is $i \in C\backslash C'$ such that $v_i \neq 0$ while $v'_i = 0$. Take its corresponding rational representation $\mathbf{v} = \sum_{\mathbf{g}} \frac{r_{\mathbf{g}}}{d}\mathbf{g}$ has $r_{\mathbf{g}} \neq 0$ for some $\mathbf{g} \in \cup_{j\in B}\mathscr{G}_{j,C}$ while $\mathbf{v}' = \sum_{\mathbf{g}} \frac{r'_{\mathbf{g}}}{d'}\mathbf{g}$ has $r'_{\mathbf{g}} = 0$ for $\mathbf{g} \in \cup_{j\in B}\mathscr{G}_{j,C}$. This proves our claim. Therefore $H_p(\mathbf{A}) \not\equiv 0 \bmod p$.

(2) To ease notation we omit subindex (B,C) and j for the rest of the proof. Notice that

$$\mathrm{Tr}(N(\mathbf{A})^{[a]}) = \sum G_{p\mathbf{t}_1-\mathbf{t}_2,p\mathbf{v}_1-\mathbf{v}_2}(\mathbf{A}^{p^{a-1}}) \cdots G_{p\mathbf{t}_a-\mathbf{t}_1,p\mathbf{v}_a-\mathbf{v}_1}(\mathbf{A})$$

where $(\mathbf{t}_i,\mathbf{v}_i)$ ranges over all of $\mathscr{Z}^{min}_{B,C}$. By Lemma 3.3(2) and our hypothesis each term in $G_{p\mathbf{t}-\mathbf{t},p\mathbf{v}-\mathbf{v}}(\mathbf{A})$ lies in $(\mathbf{Z}_p^*\cap\mathbf{Q})[\mathbf{A}]$ and $A_{j,\mathbf{g}}$-degree $\leq p-1$.

Write $\mathrm{Tr}(N(\mathbf{A})^{[a]}) = T_1(\mathbf{A}) + T_2(\mathbf{A})$ where $T_1(\mathbf{A})$ consists of all summands with all equal $(\mathbf{t}_i, \mathbf{v}_i)$ and $T_2(\mathbf{A})$ with at least one not equal. Each monomial in $T_1(\mathbf{A})$ is of the form $\prod_{\mathbf{g}} A_{\mathbf{g}}^{\sum_{i=0}^{a-1} p^i u''_{\mathbf{g},i}}$ where $p\mathbf{v} - \mathbf{v} = \sum_{\mathbf{g}} u''_{\mathbf{g},i}\mathbf{g}$ and $0 \le u''_{\mathbf{g},i} \le p-1$. Coefficient of such monomial lies in $\mathbf{Z}_p^*$. Notice that $T_1(\mathbf{A})$ is homogenous of total degree $(p^a-1)w_{\mathbf{Z}}(B,C)$, where each $A_{\mathbf{g}}$-degree is $\sum_{i=0}^{a-1} p^i u''_{\mathbf{g},i}$.

On the other hand each monomial of $T_2(\mathbf{A})$ is of the form $\prod_{\mathbf{g}} A_{\mathbf{g}}^{\sum_{i=0}^{a-1} p^i u'_{\mathbf{g},i}}$; Suppose this monomial form coincides with one lying in $T_1(\mathbf{A})$ then $p\mathbf{v}' - \mathbf{v}'' \equiv p\mathbf{v} - \mathbf{v} \bmod p$, and hence $\mathbf{v}'' \equiv \mathbf{v} \bmod p$. But $\mathbf{v}'', \mathbf{v}$ are bounded points by our hypothesis so there is a constant $\theta(\mathscr{G}_1, \dots, \mathscr{G}_r)$ such that for all $p > \theta(\mathscr{G}_1, \dots, \mathscr{G}_r)$ we have $\mathbf{v}'' = \mathbf{v}$ and hence $p\mathbf{v}' - \mathbf{v}'' = p\mathbf{v}' - \mathbf{v}$. By comparing $A_{\mathbf{g}}$-degrees we have $\sum_{i=0}^{a-1} p^i u''_{\mathbf{g},i} = \sum_{i=0}^{a-1} p^i u'_{\mathbf{g},i}$ where $0 \le u''_{\mathbf{g},i} \le p-1$ and $u'_{\mathbf{g},i} \in \mathbf{Z}_{\ge 0}$; moreover, $\sum_{i=0}^{a-1} u''_{\mathbf{g},i} = \sum_{i=0}^{a-1} u'_{\mathbf{g},i}$. This implies that $u''_{\mathbf{g},i} = u'_{\mathbf{g},i}$ for all i and hence $p\mathbf{v}' - \mathbf{v} = p\mathbf{v} - \mathbf{v}$ and $\mathbf{v} = \mathbf{v}'$ constradicting our assumption above. Therefore $T_2(\mathbf{A})$ has no monomial terms in common with $T_1(\mathbf{A})$.

Using the same argument as that in Part (1) we find that the summands in the expansion of $H_p^{[a]}(\mathbf{A})$ in (3.10) do not cancel out with each other for distinct $(B,C) \in \mathscr{K}$, and hence $H_p^{[a]}(\mathbf{A}) \not\equiv 0 \bmod p$. □

Below we shall single out a special case of $\mathscr{G}_1, \dots, \mathscr{G}_r$ in which $H_p(\widehat{a}) \bmod p$ is a constant polynomial. Let $\mathscr{D}$ be the set of all denominators of rational representations of $(\mathbf{t}, \mathbf{v}) \in \mathscr{Z}^{min}$. Suppose $\mathscr{D} = \{1\}$, that is, for all $(\mathbf{t}, \mathbf{v}) \in \mathscr{Z}^{min}$

$$G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\mathbf{A}) = \sum_{(\mathbf{u},\mathbf{v}) \in \mathscr{Z}^{min}_{B,C}} \prod_{j \in B} \prod_{\mathbf{g} \in \mathscr{G}_{j,C}} \left(\frac{A_{j,\mathbf{g}}^{p-1}}{(p-1)!}\right)^{r_{\mathbf{g}}} \tag{3.11}$$

where $r_{\mathbf{g}} = 0$ or 1 by Lemma 3.3(2). Let $m_{(\mathbf{t},\mathbf{v})}$ be the number of all such rational representations of $(\mathbf{t}, \mathbf{v}) \in \mathscr{Z}^{min}_{B,C}$, and

$$\mathbf{c}(\mathscr{G}_1, \dots, \mathscr{G}_r) := \sum_{(B,C) \in \mathscr{K}} (-1)^{w_{\mathbf{Z}}(B,C)} \sum_{(\mathbf{t},\mathbf{v}) \in \mathscr{Z}^{min}_{B,C}} m_{(\mathbf{t},\mathbf{v})}. \tag{3.12}$$

One can compute and verify that Example 1.3 satisfies the condition $\mathbf{c}(\mathscr{G}) \neq 0$.

Proposition 3.5. *Suppose $\mathscr{D} = \{1\}$. Then $\mathbf{c}(\mathscr{G}_1, \dots, \mathscr{G}_r) \neq 0$ if and only if for all $\mathbf{a} \in \mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}(\mathbf{Q})$ and for p large enough, we have $H_p(\widehat{\mathbf{a}}) \in \mathbf{Z}_p^*$.*

Proof. Below we assume $\mathbf{a}$ is integral by letting p be large enough. Combining with Wilson's theorem $(p-1)! \equiv -1 \bmod p$ and $\widehat{\mathbf{a}}^p \equiv \widehat{\mathbf{a}} \bmod p$, we

have by (3.11)

$$\begin{aligned} G_{(p-1)\mathbf{t},(p-1)\mathbf{v}}(\widehat{\mathbf{a}}) &= \sum \prod_{j\in B} \prod_{\mathbf{g}\in\mathscr{G}_{j,C}} (\frac{\widehat{a}_{j,\mathbf{g}}^{p-1}}{(p-1)!})^{r_{\mathbf{g}}} \\ &\equiv \sum \prod_{j\in B} \prod_{\mathbf{g}\in\mathscr{G}_{j,C}} (-1)^{r_{\mathbf{g}}} \\ &\equiv \sum (-1)^{w_{\mathbf{Z}}(B,C)} \\ &\equiv (-1)^{w_{\mathbf{Z}}(B,C)} m_{(\mathbf{t},\mathbf{v})} \bmod p \end{aligned}$$

where the sum is over all rational representations of $(\mathbf{u},\mathbf{v})$. Then by (3.10)

$$\begin{aligned} H_p(\widehat{\mathbf{a}}) &\equiv \sum_{(B,C)\in\mathscr{K}} (-1)^{|B|+|C|} \sum_{(\mathbf{t},\mathbf{v})\in\mathscr{Z}_{B,C}^{min}} m_{(\mathbf{t},\mathbf{v})} \\ &\equiv (-1)^{n-\boldsymbol{\mu}} \sum_{(B,C)\in\mathscr{K}} (-1)^{w_{\mathbf{Z}}(B,C)} \sum_{(\mathbf{t},\mathbf{v})\in\mathscr{Z}_{B,C}^{min}} m_{(\mathbf{t},\mathbf{v})} \\ &\equiv (-1)^{n-\boldsymbol{\mu}} \mathbf{c}(\mathscr{G}_1,\dots,\mathscr{G}_r) \bmod p. \end{aligned}$$

As $\mathbf{c}(\mathscr{G}_1,\dots,\mathscr{G}_r)$ is a nonzero integer by our hypothesis, this proves that $\mathbf{c}(\mathscr{G}_1,\dots,\mathscr{G}_r) \not\equiv 0 \bmod p$ if and only if $H_p(\widehat{\mathbf{a}}) \in \mathbf{Z}_p^*$. □

4. Proof of main theorem

Let $\mathscr{G}_1,\dots,\mathscr{G}_r$ be fixed subsets in $\mathbf{Z}_{\geq 0}^n$. Let $\mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}$ be the space of all algebraic varieties $V(f_1,\dots,f_r)$ where $f_1,\dots,f_r$ are supported on $\mathscr{G}_1,\dots,\mathscr{G}_r$, respectively. Namely, $f_j = \sum_{\mathbf{g}\in\mathscr{G}_j} a_{j,\mathbf{g}}\mathbf{x}^{\mathbf{g}}$ where $a_{j,\mathbf{g}} \neq 0$ for all $\mathbf{g} \in \mathscr{G}_j$. For any field K containing $\mathbf{Q}$ (resp. $\mathbf{F}_p$) we shall identify each algebraic variety V (resp. $\overline{V}$) in $\mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}(K)$ by $\mathbf{a} = (a_{j,\mathbf{g}})_{j,\mathbf{g}}$ (resp. $\overline{\mathbf{a}}$) with $a_{j,\mathbf{g}} \in K$ (resp. $\overline{a}_{j,\mathbf{g}}$) and $\mathbf{g} \in \mathscr{G}_j$ for $1 \leq j \leq r$. In this section $V_{\mathbf{a}}$ denote the variety defined by $\mathbf{a}$.

This section is devoted to prove our main Theorem 1.1. It is clear that Theorems 4.3 and 4.4 below proves Parts (1) and (2) of Theorem 1.1, respectively.

In the following proposition we show that the polynomial $H_p^{[a]}(\mathbf{A}) \in \mathbf{Q}[\mathbf{A}]$ defined in (3.10) is indeed a Hasse polynomial for the p-adic valuation of $|V_{\mathbf{a}}(\mathbf{F}_q)|$. For any prime $\wp$ over p of residue degree a let $\overline{V_{\mathbf{a}}}$ denote $V_{\mathbf{a}} \bmod \wp$.

Proposition 4.1. *Let $\overline{\mathbf{Z}}$ denote the ring of integral elements in $\overline{\mathbf{Q}}$. For any $\mathbf{a} \in \mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}(\overline{\mathbf{Z}})$, or for any $\mathbf{a}$ in $\mathbb{A}^{\mathscr{G}_1,\dots,\mathscr{G}_r}(\overline{\mathbf{Q}})$ and p large enough, the following statements are equivalent to each other*

(1) $|H_p^{[a]}(\mathbf{a})|_p = 1$
(2) $H_p^{[a]}(\mathbf{a}) \not\equiv 0 \bmod \wp$
(3) $\mathrm{ord}_q|\overline{V_{\mathbf{a}}}(\mathbf{F}_q)| = \boldsymbol{\mu}$.

Proof. For each $\mathbf{a}$ we may choose for the rest of the proof that p is large enough so that $\mathrm{ord}_p\mathbf{a} \geq 0$. Then let $\widehat{\mathbf{a}}$ be the Teichmüller lifting of $\overline{\mathbf{a}}$. The first two statements are clear. We claim that Parts (2) and (3) are equivalent. Applying (2.12) and Lemma 3.1 we have

$$\begin{aligned}\frac{|\overline{V_{\mathbf{a}}}(\mathbf{F}_q)|}{q^{\boldsymbol{\mu}}} - q^{n-\boldsymbol{\mu}} &\equiv \sum_{(B,C)\in\mathscr{K}} (q-1)^{|B|+|C|}\frac{\mathrm{Tr}(M_{B,C}(\widehat{\mathbf{a}})^{[a]})}{q^{w_{\mathbf{Z}}(B,C)}} \bmod \wp \\ &\equiv \sum_{(B,C)\in\mathscr{K}} (-1)^{|B|+|C|+aw_{\mathbf{Z}}(B,C)}\mathrm{Tr}(N_{B,C}(\widehat{\mathbf{a}})^{[a]}) \bmod \wp.\end{aligned}$$

Comparing to definition (3.10) we have

$$\frac{|\overline{V_{\mathbf{a}}}(\mathbf{F}_q)|}{q^{\boldsymbol{\mu}}} \equiv H_p^{[a]}(\widehat{\mathbf{a}}) \equiv H_p^{[a]}(\mathbf{a}) \bmod \wp.$$

Our claim follows. □

Let $\mathscr{Z}^{min}$ be as in (3.3). Let $\mathscr{D}$ be the set of all denominators d of rational representations of all $(\mathbf{t},\mathbf{v}) \in \mathscr{Z}^{min}$. Let $\theta(\mathscr{G}_1,\ldots,\mathscr{G}_r)$ be as in Lemma 3.4. We shall write $\mathscr{P}$ for the set of primes $p \equiv 1 \bmod d$ for all d lying in $\mathscr{D}$ and $p > \theta(\mathscr{G}_1,\ldots,\mathscr{G}_r)$. Observe that it is of positive density in $\mathrm{Spec}(\mathbf{Z})$ by Dirichlet's theorem on arithmetic progressions. The following theorem shows that for prime p in $\mathscr{P}$, a subset of Spec$\mathbf{Z}$ of positive density, there is a *Hasse polynomial* $H_p^{[a]}(\mathbf{A})$ defined over $\mathbf{Q}$ that $H_p^{[a]}(\mathbf{A}) \bmod p$ is a nonzero polynomial in $\mathbf{F}_p[\mathbf{A}]$ of homogenous degree $(p-1)w_{\mathbf{Z}}(B,C)$ (as seen in Lemma 3.4).

Theorem 4.2. *Let K be a number field and $\mathscr{O}_K$ its ring of integers. For any $p \in \mathscr{P}$ let $\mathscr{U}_p$ be the subset in $\mathbb{A}^{\mathscr{G}_1,\ldots,\mathscr{G}_r}$ consisting of all $\mathbf{a}$ with $|H_p^{[a]}(\mathbf{a})|_p = 1$ where a is corresponding residue degree over p. Write $V_{\mathbf{a}}$ for the algebraic variety defined by $\mathbf{a}$ and $\overline{V_{\mathbf{a}}}$ for its reduction $V_{\mathbf{a}} \bmod \wp$ with residue degree a. Then for every $V_{\mathbf{a}} \in \mathbf{A}^{\mathscr{G}_1,\ldots,\mathscr{G}_r}(\mathscr{O}_K)$ we have $V_{\mathbf{a}}$ in $\mathscr{U}_p(\mathscr{O}_K)$ if and only if $\mathrm{ord}_q|\overline{V_{\mathbf{a}}}(\mathbf{F}_q)| = \boldsymbol{\mu}$. In particular, if $V_{\mathbf{a}} \in \mathscr{U}_p(K)$ and p is large enough we have $\mathrm{ord}_q|\overline{V_{\mathbf{a}}}(\mathbf{F}_q)| = \boldsymbol{\mu}$.*

Proof. It follows immediately from Proposition 4.1. □

Theorem 4.3. *Let K be a number field. Let $\mathscr{U}$ be the subset of $\mathbb{A}^{\mathscr{G}_1,\ldots,\mathscr{G}_r}$ consisting of all $\mathbf{a}$ over K satisfying that $\prod_{p\in\mathscr{P}}|H_p^{[a(p)]}(\mathbf{a})| = 1$ where $a(p)$ denote the corresponding residue degree over p. If $V_{\mathbf{a}} \in \mathscr{U}(\mathscr{O}_K)$ then $\mathrm{ord}_q|\overline{V_{\mathbf{a}}}(\mathbf{F}_q)| = \boldsymbol{\mu}$ for all $p \in \mathscr{P}$. If $V_{\mathbf{a}} \in \mathscr{U}(K)$ then $\mathrm{ord}_q|\overline{V_{\mathbf{a}}}(\mathbf{F}_q)| = \boldsymbol{\mu}$ for all $p \in \mathscr{P}$ and p large enough.*

Proof. It follows from Theorem 4.2 above. □

In general the above defined Hasse polynomials $H_p^{[a]}(\mathbf{A})$ in $\mathbf{Q}[\mathbf{A}]$ depends on p. However, for special occasions like (but not limited to) $\mathscr{D} = \{1\}$ we found that $H_p^{[a]}(\mathbf{A}) \bmod p$ is a constant independent of p.

Theorem 4.4. *Suppose* $\mathscr{D} = \{1\}$. *Suppose* $\mathbf{c}(\mathscr{G}_1, \ldots, \mathscr{G}_r) \neq 0$ *where* $\mathbf{c}(\cdot)$ *is defined in* (3.12). *Then for all* V *in* $\mathbb{A}^{\mathscr{G}_1,\ldots,\mathscr{G}_r}(\mathbf{Q})$ *and* p *large enough we have* $\operatorname{ord}_p|\overline{V}(\mathbf{F}_p)| = \boldsymbol{\mu}$.

Proof. By Proposition 3.5 we know that for all $\mathbf{a}$ in $\mathbb{A}^{\mathscr{G}_1,\ldots,\mathscr{G}_r}(\mathbf{Q})$ for p large enough $H_p(\mathbf{a}) \in \mathbf{Z}_p^* \cap \mathbf{Q}$. Thus by Proposition 4.1 we have $\operatorname{ord}_p|\overline{V}(\mathbf{F}_p)| = \boldsymbol{\mu}$. □

We remark that the condition $\mathscr{D} = \{1\}$ is an indicator of how sparse the given system $\mathscr{G}_1, \ldots, \mathscr{G}_r$ is. We have the following more explicit criterion in constructing such supporting sets.

Proposition 4.5. *Let* $\mathscr{G}_1, \ldots, \mathscr{G}_r$ *be given subsets of points in* $\mathbf{Z}_{\geq 0}^n$. *If* $\sum_{\mathbf{g} \in \mathscr{G}_{j,C}} u_{\mathbf{g}} \mathbf{g} \in \mathbf{Z}_{\geq 1}^C$ *for each* $1 \leq j \leq r$ *with* $\sum_{\mathbf{g} \mathscr{G}_{j,C}} u_{\mathbf{g}} \in \mathbf{Z}_{\geq 1}$ *and* $u_{\mathbf{g}} \in \mathbf{Q}_{\geq 0}$ *implies that* $u_{\mathbf{g}} \in \mathbf{Z}$ *then* $\mathscr{D} = \{1\}$.

Remark 4.6. Applying Proposition 4.5, we have $\mathscr{D} = \{1\}$ for Example 1.3.

References

[1] A. Adolphson & S. Sperber, "p-adic estimates for exponential sums and the theorem of Chevalley–Warning", *Ann. Sci. École. Norm. Sup.* **20** (1987), p. 545-556.

[2] E. Artin, *The collected papers of Emil Artin*, Addison-Wesley Publishing Company, 1965, xvi+560 pages.

[3] J. Ax, "Zeros of polynomials over finite fields", *Amer. J. Math.* **86** (1964), p. 255-261.

[4] C. Chevalley, "Démonstration d'une hypothèse de M. Artin", *Abh. Math. Sem. Univ. Hamburg* **11** (1935), p. 73-75.

[5] B. Dwork, "On the rationality of the zeta function of an algebraic variety", *Amer. J. Math.* **82** (1960), p. 631-648.

[6] N. M. Katz, "On a theorem of Ax", *Amer. J. Math.* **93** (1971), p. 485-499.

[7] J.-P. Serre, "Endomorphismes complètements continus des espaces de Banach p-adiques", *Inst. Hautes. Études Sci. Publ. Math.* **12** (1962), p. 69-85.

[8] D. Wan, "An elementary proof of a theorem of Katz", *Amer. J. Math.* **111** (1989), p. 1-8.

[9] E. Warning, "Bemerkung zur vorstehenden Arbeit von Herrn Chevalley", *Abh. Math. Sem. Univ. Hamburg* **11** (1935), p. 76-83.

Hui June Zhu
Department of mathematics
SUNY at Buffalo
Buffalo, NY 14260, USA
E-mail: hjzhu@math.buffalo.edu