Finite Fields and Their Applications 91 (2023) 102254

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Divisibility on point counting over finite Witt rings

Wei Cao [a,*], Daqing Wan [b]

[a] *School of Mathematics and Statistics, Minnan Normal University, Zhangzhou 363000, Fujian Province, PR China*
[b] *Department of Mathematics, University of California, Irvine, 92697-3875, USA*

ARTICLE INFO

Article history:
Received 22 October 2022
Received in revised form 10 April 2023
Accepted 5 June 2023
Available online 26 June 2023
Communicated by Gary L. Mullen

MSC:
11T06
11D88
13F35

Keywords:
Witt vector
Finite field
p-adic number field
Teichmüller box
p-adic estimate

ABSTRACT

Let $\mathbb{F}_q$ denote the finite field of q elements with characteristic p. Let $\mathbb{Z}_q$ denote the unramified extension of the p-adic integers $\mathbb{Z}_p$ with residue field $\mathbb{F}_q$. In this paper, we investigate the q-divisibility for the number of solutions of a polynomial system in n variables over the finite Witt ring $\mathbb{Z}_q/p^m\mathbb{Z}_q$, where the n variables of the polynomials are restricted to run through a box lifting $\mathbb{F}_q^n$. It turns out that in general the answers do depend upon the box chosen. Based on the addition operation of Witt vectors, we prove a q-divisibility theorem for any box of low algebraic complexity, including the simplest Teichmüller box. This extends the classical Ax-Katz theorem over finite field $\mathbb{F}_q$ (the case $m = 1$). Taking $q = p$ to be a prime, our result extends and improves a recent theorem of Grynkiewicz for the unweighted case.

1. Introduction

Let $\mathbb{N}$ denote the set of positive integers. Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $\mathbb{Q}_p$ denote the field of p-adic rational numbers and $\mathbb{Z}_p$ the ring of integers

* Corresponding author.
E-mail addresses: caow2286@mnnu.edu.cn (W. Cao), dwan@math.uci.edu (D. Wan).

https://doi.org/10.1016/j.ffa.2023.102254
1071-5797/

in $\mathbb{Q}_p$. Let $\mathbb{F}_q$ denote the finite field of q elements and $\mathbb{Z}_q$ the unramified extension of the p-adic integers $\mathbb{Z}_p$ with residue field $\mathbb{F}_q$. Let $\mathbb{F}_q[x_1,\dots,x_n]$ denote the ring of the polynomials in n variables $x_1,\dots,x_n$ with coefficients in $\mathbb{F}_q$. The study of the common zeros of a system of polynomials in $\mathbb{F}_q[x_1,\dots,x_n]$ is a classical and important subject in Number Theory and Arithmetic Geometry. In general it is hard to know the exact cardinality of the set of such common zeros in $\mathbb{F}_q$. However, the Chevalley-Warning and Ax-Katz theorems provide estimates of p-divisibility for this problem by utilizing the degrees of the associated polynomials. Given a set S, let $|S|$ denote the cardinality of S. Write $X := (x_1,\dots,x_n)$ and set $[a,b] := \{x \in \mathbb{Z} \mid a \le x \le b\}$ for $a, b \in \mathbb{R}$.

Theorem 1.1. (Chevalley-Warning) *Let $f_1(X),\dots,f_s(X) \in \mathbb{F}_q[x_1,\dots,x_n]$ be a system of nonzero polynomials, and let*

$$V := \{X \in \mathbb{F}_q^n | f_k(X) = 0 \text{ for all } k \in [1,s]\}.$$

If $n > \sum_{k=1}^{s} \deg(f_k)$, then p divides $|V|$.

The Chevalley-Warning theorem also gave an affirmative answer to Artin's conjecture for the homogeneous polynomials (see [13] and [28]), and it was greatly improved by Ax [3] for the case $s = 1$ and Katz [20] for general $s \ge 1$. Let ord_q denote the q-adic additive valuation normalized by $\mathrm{ord}_q q = 1$. If $q = p$, then ord_p is the p-adic additive valuation normalized by $\mathrm{ord}_p p = 1$. For $t \in \mathbb{R}$, let $\lceil t \rceil$ denote the least integer more than or equal to t, and let $\lfloor t \rfloor$ denote the greatest integer less then or equal to t. The Ax-Katz theorem can be stated as follows.

Theorem 1.2. (Ax-Katz) *With the same assumption as in Theorem 1.1, we have*

$$\mathrm{ord}_q(|V|) \ge \left\lceil \frac{n - \sum_{k=1}^{s} \deg(f_k)}{\max_{k\in[1,s]} \deg(f_k)} \right\rceil. \tag{1}$$

An elementary proof of the Ax-Katz theorem is given in [26]. The simplest proof of the Ax-Katz theorem and its extension to character sums are given in [27]. A reduction of the Ax-Katz theorem for a system of equations to Ax's theorem for a single equation has been found by Hou [18]. Besides these, there has been a lot of research work on this topic, including extensions, refinements, variants and alternative proofs (see, for example, [1,2,4–9,11,12,14,15,17,21,22,29]).

Recently, motivated by combinatorial applications, Grynkiewicz [16] proved a version of the Chevalley-Warning and Ax-Katz theorems over the residue class ring $\mathbb{Z}_p/p^m\mathbb{Z}_p$, in which the varying prime power moduli are allowed. The following theorem is just the unweighted case of [16, Theorem 1.3].

Theorem 1.3. *Let p be a prime number and $\mathcal{B} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_n$ with each $\mathcal{I}_j \subseteq \mathbb{Z}_p$ a complete system of residues modulo p for $j \in [1,n]$. Let $m_1,\dots,m_s \in \mathbb{N}$ and $f_1,\dots,f_s \in \mathbb{Z}_p[x_1,\dots,x_n]$ be a system of nonzero polynomials, and let*

$$V := \{X \in \mathcal{B} : \ f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1,s]\}.$$

Then

$$\mathrm{ord}_p(|V|) \geq \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} \deg(f_k)}{\max_{k\in[1,s]}\{p^{m_k-1}\deg(f_k)\}} \right\rceil.$$

Note that each $\mathcal{I}_j$ is a lifting of the prime field $\mathbb{F}_p$ in $\mathbb{Z}_p$ and thus the box $\mathcal{B}$ is a lifting of $\mathbb{F}_p^n$ in $\mathbb{Z}_p^n$. If $m_1 = \cdots = m_s = 1$, then Theorem 1.3 recovers the Ax-Katz theorem for the prime finite field $\mathbb{F}_p$. The box $\mathcal{B}$ in Theorem 1.3 allows many combinatorial applications. As suggested by Grynkiewicz in [16], if there is an $m_k > 1$ for some $k \in [1,s]$, one should appropriately choose the box $\mathcal{B}$ to apply Theorem 1.3 to some problems in Combinatorial Number Theory. In other words, the elements in $\mathcal{I}_i$ should satisfy the proposition below. In our terminology, this just means that one should typically choose the Teichmüller box (cf. Subsection 2.3).

Proposition 1.4. ([16, Proposition 1.4]) *Let p be a prime number and $m \in \mathbb{N}$. There exists a complete system of residues $\mathcal{I} \subseteq [0, p^m - 1]$ modulo p such that*

$$x^{p-1} \equiv \begin{cases} 1 \pmod{p^m} & \text{if } x \not\equiv 0 \pmod{p} \\ 0 \pmod{p^m} & \text{if } x \equiv 0 \pmod{p}, \end{cases} \qquad \text{for every } x \in \mathcal{I}.$$

To prove and apply Theorem 1.3, Grynkiewicz [16] comprehensively utilized the weighted Weisman-Fleck congruence [25] and Wilson's arguments [29]. In fact, Grynkiewicz [16] proved the Ax-Katz theorem over $\mathbb{F}_p$. But it is not clear how to use his method to extend Theorem 1.3 from $\mathbb{Z}_p$ to $\mathbb{Z}_q$ with the box $\mathcal{B}$ being a lifting of $\mathbb{F}_q^n$ so that it would also include the general Ax-Katz theorem. We will give counter-examples showing that the $\mathbb{Z}_q$ generalization of Theorem 1.3 is false. This suggests that the problem is more subtle for $\mathbb{Z}_q$ than for $\mathbb{Z}_p$.

Another restriction in Theorem 1.3 is that the box is in split form, that is, the n-dimensional box $\mathcal{B}$ is the product of one dimensional boxes $\mathcal{I}_j$ for $1 \leq j \leq n$. In general, a box (a lifting of $\mathbb{F}_p^n$ in $\mathbb{Z}_p^n$) will not be in such a split form. We will also give counter-examples showing that Theorem 1.3 is false for general non-split boxes.

Despite all these obstacles, our aim of this paper is to investigate the problem over $\mathbb{Z}_q$ and a general box $\mathcal{B}$ lifting $\mathbb{F}_q^n$, in an attempt to unify and hence extend both the general Ax-Katz theorem and Theorem 1.3. This desired unification is achieved in this paper. Our main result says that the desired q-divisibility theorem holds over $\mathbb{Z}_q$ as long as the box $\mathcal{B}$ (lifting $\mathbb{F}_q^n$) has low algebraic complexity, in the sense that it is close to the Teichmüller box up to a low degree polynomial perturbation. In the case $q = p$, any split box has low algebraic complexity, which explains Theorem 1.3. There are many non-split boxes with low algebraic complexity, and thus our result significantly extends Theorem 1.3 as well, even in the case $q = p$. We now make these more precise. For

simplicity of exposition, we only state some weaker but simpler consequences of our main result in this introduction.

Let T_q be the set of Teichmüller representatives of $\mathbb{F}_q$ in $\mathbb{Z}_q$. The set T_q^n is clearly a lifting of $\mathbb{F}_q^n$, and is called the Teichmüller box. It is the simplest and nicest box for our purpose. Our result for the Teichmüller box is the following statement.

Theorem 1.5 *(Corollary 3.5). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $f_1, \ldots, f_s \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in T_q^n \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1, s]\}.$$

Then

$$\mathrm{ord}_q(|V|) \geq \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} \deg(f_k)}{\max_{k\in[1,s]}\{p^{m_k-1}\deg(f_k)\}} \right\rceil.$$

In the case $m_1 = \cdots = m_s = 1$, this reduces to the Ax-Katz theorem over $\mathbb{F}_q$. To be precise, our proof in the general case uses the Ax-Katz theorem over $\mathbb{F}_q$, which is a special case of our result.

The possible extension from the Teichmüller box to a general box is more subtle. Let us define a box $\mathcal{B}$ to be a subset of $\mathbb{Z}_q^n$ with q^n elements such that $\mathcal{B}$ modulo p is equal to $\mathbb{F}_q^n$. That is, $\mathcal{B}$ is a complete system of representatives of $\mathbb{F}_q^n$ in $\mathbb{Z}_q^n$, equivalently, $\mathcal{B}$ is a lifting of $\mathbb{F}_q^n$ in $\mathbb{Z}_q^n$. In order to apply algebraic methods, we would like to give an algebraic presentation of the box $\mathcal{B}$, using the image of a polynomial map, following the spirit in [19]. As proved in Section 4, for any box $\mathcal{B}$, there exists a unique system of polynomials $g_j(X) \in \mathbb{Z}_q[x_1, \ldots, x_n]$ $(1 \leq j \leq n)$ whose degree in each variable is at most $q-1$ such that for any $Y = (y_1, \ldots, y_n) \in \mathcal{B}$, we have

$$Y = X + (g_1(X), \ldots, g_n(X))p, \tag{2}$$

where $X = (x_1, \ldots, x_n) \in T_q^n$ is the Teichmüller lifting of the modulo p reduction of Y. In other words, the box $\mathcal{B}$ is simply the image of the Teichmüller box T_q^n under the polynomial map $X \longrightarrow X + (g_1(X), \ldots, g_n(X))p$. This polynomial representation of the box $\mathcal{B}$ is unique since we require the polynomials $g_j(X)$ to be reduced and thus have degrees at most $q-1$ in each variable, that is, we have reduced the polynomials modulo the ideal $(x_1^q - x_1, \cdots, x_n^q - x_n)$. The total degree of g_j is then bounded by $(q-1)n$. The box $\mathcal{B}$ is called in split form or a split box if $\mathcal{B} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_n$, where each $\mathcal{I}_j$ is a 1-dimensional box in $\mathbb{Z}_q$ lifting $\mathbb{F}_q$. The box $\mathcal{B}$ is in split form if and only if (2) becomes

$$Y = X + (g_1(x_1), \ldots, g_n(x_n))p,$$

where each $g_j(x_j)$ depends only on the one variable x_j. In this case, each g_j has total degree at most $q-1$, much smaller than $n(q-1)$.

The degrees of the representing polynomials g_j's provide a crude measure for the algebraic complexity of the box $\mathcal{B}$, see [19] for a discussion of this in the case of finite fields. A random box $\mathcal{B}$ has high algebraic complexity, and hence algebraic methods have limited values. One expects that a box of low algebraic complexity has some algebraic structure and hence suitable for study using algebraic methods. This explains why we need a low degree bound on the representing polynomials g_j for the box $\mathcal{B}$ in the following theorems.

A polynomial $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ is called a Teichmüller polynomial if all of its coefficients are Teichmüller elements in T_q. Any polynomial $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ has the unique expansion

$$f(X) = \sum_{i=0}^{\infty} p^i f_i(X),$$

where each $f_i(X)$ is a Teichmüller polynomial. This is called the Teichmüller expansion of f. It is obtained from the Teichmüller expansion of the coefficients of f. Our result for a general box $\mathcal{B}$ in $\mathbb{Z}_q^n$ is as follows.

Theorem 1.6 *(Corollary 4.7). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $\mathcal{B}$ be a general box in $\mathbb{Z}_q^n$ defined by the reduced polynomials $g_j \in \mathbb{Z}_q[x_1, \cdots, x_n]$ with $j \in [1, n]$ as above. Let $f_1, \ldots, f_s \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in \mathcal{B} \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1, s]\}.$$

For $1 \le j \le n$, write the Teichmüller expansion $pg_j(X) = \sum_{i=1}^{\infty} p^i g_{ij}(X)$. Let $m = \max_{i \in [1,s]}\{m_i\}$. If $\deg(g_{ij}) \le p^{h\lfloor \frac{i}{h} \rfloor}$ for all $j \in [1, n], i \in [1, m-1]$, then

$$\mathrm{ord}_q(|V|) \ge \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} \deg(f_k)}{\max_{k \in [1,s]}\{p^{m_k-1} \deg(f_k)\}} \right\rceil.$$

If $\mathcal{B}$ is the Teichmüller box, then $g_{ij} = 0$ for all $i, j \ge 1$, and the condition $\deg(g_{ij}) \le p^{h\lfloor \frac{i}{h} \rfloor}$ is trivially satisfied. Theorem 1.6 is thus a generalization of Theorem 1.5 from the Teichmüller box to a general box of low algebraic complexity.

In the case $q = p$ and thus $h = 1$, we obtain the following simpler consequence of Corollary 4.8.

Theorem 1.7. *Let p be a prime number. Let $\mathcal{B}$ be a general box as defined above by the reduced polynomials $g_j(x_1, \cdots, x_n) \in \mathbb{Z}_p[x_1, \cdots, x_n]$ with $j \in [1, n]$. Let $f_1, \ldots, f_s \in \mathbb{Z}_p[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in \mathcal{B} \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1, s]\}.$$

If $\deg(g_j) \le p$ *for all* $j \in [1,n]$, *then*

$$\mathrm{ord}_p(|V|) \ge \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} \deg(f_k)}{\max_{k\in[1,s]}\{p^{m_k-1}\deg(f_k)\}} \right\rceil. \tag{3}$$

In this theorem, if the box $\mathcal{B}$ is in split form, then $\deg(g_j) \le p-1$ and hence the degree condition $\deg(g_j) \le p$ is automatically satisfied. In particular, (3) holds true for all split boxes $\mathcal{B}$, recovering Theorem 1.3. Note that the above theorem is also true for many non-split boxes as long as the degrees of the g_j are bounded by p.

We emphasize that Theorems 1.5, 1.6 and 1.7 presented above are simplified (and thus weaker) versions of our results. For their strong versions, which depend on the degree bounds in the p-adic expansion of the polynomials g_j's and f_k's, see Theorems 3.4 and 4.6. Our basic idea is to use the addition operation of Witt vectors to reduce the congruence solution counting in the box $\mathcal{B}$ to point counting of a system of equations over $\mathbb{F}_q$ for which the Ax-Katz theorem can be applied. The key is to control the degrees of the resulting polynomial equations over $\mathbb{F}_q$. This leads to the assumption on the degree bounds for the g_j's, or more generally the degree bounds in the p-adic Teichmüller expansions of the polynomials g_j's and f_k's.

The paper is organized as follows. Some basic knowledge about the Witt vectors is reviewed in Section 2. Then we apply the ring of Witt vectors over $\mathbb{F}_q$ to study the polynomials in $\mathbb{Z}_q[x_1,\dots,x_n]$, which is divided into two parts: the generalization of Theorem 1.3 to $\mathbb{Z}_q[x_1,\dots,x_n]$ for the Teichmüller box case is given in Section 3, and that for the general box is given in Section 4. In Section 5, we give examples showing that all the theorems are false without the degree bounds of the representing polynomials g_j's.

2. Preliminaries

Witt vector rings and their variants are a useful tool in many branches of mathematics ranging from algebra and algebraic number theory to arithmetic geometry and homotopy theory. In this section, we only review the construction and simple properties of the classical p-typical Witt vectors of Witt and Teichmüller [30]; for generalized or big Witt vectors, refer to [10,23,24]. Using the p-typical Witt vectors one may pass from a perfect field K of characteristic p to unramified complete discrete valuation ring with the residue field K and quotient field of characteristic zero.

2.1. The ring of p-typical Witt vectors

Let R be a commutative ring with identity and $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$. The underlying set of the ring of p-typical Witt vectors over R is the set

$$W(R) = R^{\mathbb{N}_0} = \{(a_0, a_1, \dots) \mid a_i \in R\}.$$

Now we explore the mysterious algebraic structure of $W(R)$. For $n \in \mathbb{N}_0$, the n-th Witt polynomial is defined to be

$$\omega_n(x_0, x_1, \dots, x_n) := x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n. \tag{4}$$

Remark 2.1. If we define $\mathrm{wt}(x_i) = p^i$, then ω_n is weighted homogeneous of weighted degree p^n.

Using the Witt polynomials, we can establish the so-called ghost (or phantom) map

$$\omega : W(R) \to R^{\mathbb{N}_0}, \quad \mathbf{a} = (a_0, a_1, \dots) \mapsto \omega(\mathbf{a}) = (\omega_0(a_0), \omega_1(a_0, a_1), \dots), \tag{5}$$

where $\omega_n(a_0, a_1, \dots, a_n)$ is called the n-th ghost (or phantom) component of $\mathbf{a}$. The ring $W(R)$ of p-typical Witt vectors over R is defined by componentwise addition and multiplication via the ghost components, which was found by the pioneering and ingenious work of Witt [30]. Let $\oplus$ and $\odot$ denote the addition and multiplication in the ring $W(R)$, respectively.

Theorem 2.2 *(Witt). There are two families of polynomials with integer coefficients*

$$S_n(x_0, y_0; x_1, y_1; \dots; x_n, y_n), \quad M_n(x_0, y_0; x_1, y_1; \dots; x_n, y_n), \quad n \in \mathbb{N}_0,$$

such that for $\mathbf{a} = (a_0, a_1, \dots), \mathbf{b} = (b_0, b_1, \dots) \in W(R)$*, we have*

(i) $\mathbf{a} \oplus \mathbf{b} = (S_0(a_0, b_0), S_1(a_0, b_0; a_1, b_1), \dots)$,
(ii) $\mathbf{a} \odot \mathbf{b} = (M_0(a_0, b_0), M_1(a_0, b_0; a_1, b_1), \dots)$,
(iii) $\omega(\mathbf{a} \oplus \mathbf{b}) = \omega(\mathbf{a}) + \omega(\mathbf{b})$,
(iv) $\omega(\mathbf{a} \odot \mathbf{b}) = \omega(\mathbf{a})\omega(\mathbf{b})$.

If p is invertible in the ring R, then the ring homomorphism $\omega : W(R) \to R^{\mathbb{N}_0}$ induced by the ghost map (5) is an isomorphism, i.e., $W(R) \cong R^{\mathbb{N}_0}$. It is obvious that the polynomials S_n and M_n are determined by the first $n+1$ coordinates of the Witt vectors and their coefficients do not depend upon the ring R. In particular, one can calculate

$$S_0 = x_0 + y_0, \quad S_1 = x_1 + y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x_0^i y_0^{p-i},$$

$$M_0 = x_0 y_0, \quad M_1 = x_0^p y_1 + x_1 y_0^p + p x_1 y_1.$$

2.2. Polynomials S_n and M_n for r-fold operation

The calculations of S_n and M_n for big n are very complicated. However, for the purpose of this paper, we are more concerned with the degree of the polynomial S_n for

r-fold addition. We also give the degree of the polynomial M_n for r-fold multiplication for completeness.

Let $r \in \mathbb{N}$. For $j \in [1, r]$, write $X_j = (x_{0j}, \dots, x_{nj}, \dots)$, and

$$\begin{aligned} X_1 \oplus \cdots \oplus X_r &= (S_0^{(r)}, \dots, S_n^{(r)}, \dots), \\ X_1 \odot \cdots \odot X_r &= (M_0^{(r)}, \dots, M_n^{(r)}, \dots). \end{aligned} \tag{6}$$

Lemma 2.3. *Both $S_n^{(r)}$ and $M_n^{(r)}$ are polynomials with integer coefficients in $(n+1)r$ variables $x_{ij} (i \in [0, n], j \in [1, r])$. If we set $\mathrm{wt}(x_{ij}) = p^i$ for $i \in [0, n]$ and $j \in [1, r]$, then $S_n^{(r)}$ is weighted homogeneous of weighted degree p^n, and $M_n^{(r)}$ is weighted homogeneous of weighted degree rp^n. More generally, let $d \in \mathbb{N}$, if we set $\mathrm{wt}(x_{ij}) \le dp^i$ for $i \in [0, n]$ and $j \in [1, r]$, then $S_n^{(r)}$ is of weighted degree $\le dp^n$, and $M_n^{(r)}$ is of weighted degree $\le rdp^n$.*

Proof. It immediately follows from (6) and Theorem 2.2 that the polynomial $S_n^{(r)}$ has integer coefficients and that

$$\omega_n(S_0^{(r)}, \dots, S_n^{(r)}) = \omega_n(X_1) + \cdots + \omega_n(X_r),$$

which in expansion by (4) is

$$\begin{aligned} &(S_0^{(r)})^{p^n} + p(S_1^{(r)})^{p^{n-1}} + \cdots + p^n(S_n^{(r)}) \\ &= (x_{01}^{p^n} + \cdots + x_{0r}^{p^n}) + p(x_{11}^{p^{n-1}} + \cdots + x_{1r}^{p^{n-1}}) + p^n(x_{n1} + \cdots + x_{nr}). \end{aligned} \tag{7}$$

Thus we have

$$S_n^{(r)} = \frac{1}{p^n} \left(\sum_{i=1}^{r} \omega_n(X_i) - \sum_{i=0}^{n-1} p^i (S_i^{(r)})^{p^{n-i}} \right). \tag{8}$$

Since $S_n^{(r)}$ has integer coefficients, the factor $\frac{1}{p^n}$ in (8) will be cancelled eventually. Set $\mathrm{wt}(x_{ij}) = p^i$ for $i \in [0, n]$, $j \in [1, r]$. We make use of induction on n to show that $S_n^{(r)}$ is a weighted homogeneous polynomial of weighted degree p^n in $(n+1)r$ variables $x_{ij} (i \in [0, n], j \in [1, r])$. The case of $n = 0$ in which $S_0^{(r)} = x_{01} + \cdots + x_{0r}$ is trivially verified. We assume that $S_k^{(r)}$ is a weighted homogeneous polynomial of weighted degree p^k in $(k+1)r$ variables $x_{ij} (i \in [0, k], j \in [1, r])$ for $0 \le k \le n-1$. Then the sum $\sum_{i=0}^{n-1} p^i (S_i^{(r)})^{p^{n-i}}$ in (8) is a weighted homogeneous polynomial of weighted degree p^n in nr variables $x_{ij} (i \in [0, n-1], j \in [1, r])$. Note that by (7) the sum $\sum_{i=1}^{r} \omega_n(X_i)$ in (8) is weighted homogeneous of weighted degree p^n in $(n+1)r$ variables $x_{ij} (i \in [0, n], j \in [1, r])$ with the variables $x_{nj} (j \in [1, r])$ not occurring in $\sum_{i=0}^{n-1} p^i (S_i^{(r)})^{p^{n-i}}$, which implies that $S_n^{(r)} \neq 0$. Thus we conclude that $S_n^{(r)}$ is a weighted homogeneous polynomial of weighted degree p^n in $(n+1)r$ variables $x_{ij} (i \in [0, n], j \in [1, r])$. The other results can be similarly deduced. □

Remark 2.4. (i) The weighted degree of $S_n^{(r)}$ does not depend upon r, but the weighted degree of $M_n^{(r)}$ does.

(ii) To indicate explicitly the variables as well as their order in $S_n^{(r)}$ and $M_n^{(r)}$, we write

$$S_n^{(r)} := S_n^{(r)}(x_{01}, \dots, x_{0r}; x_{11}, \dots, x_{1r}; \dots; x_{n1}, \dots, x_{nr}), \text{ and}$$
$$M_n^{(r)} := M_n^{(r)}(x_{01}, \dots, x_{0r}; x_{11}, \dots, x_{1r}; \dots; x_{n1}, \dots, x_{nr}).$$

(iii) For later applications, we record the following explicit formulae for $S_0^{(r)}$ and $S_1^{(r)}$.

$$S_0^{(r)} = x_{01} + \cdots + x_{0r},$$
$$S_1^{(r)} = x_{11} + \cdots + x_{1r} - \frac{1}{p} \sum_{t_1+\cdots+t_r=p,\ 0\le t_i\le p-1} \binom{p}{t_1, \cdots, t_r} x_{01}^{t_1} \cdots x_{0r}^{t_r}.$$

2.3. Perfect rings with characteristic p

In this subsection, we always let R be a perfect ring with characteristic p, which means that the Frobenius map $\phi : a \mapsto a^p$ is an automorphism. Let $W(R)$ denote the ring of Witt vectors over R. The Teichmüller lifting is defined by

$$\tau : R \hookrightarrow W(R), \quad a \mapsto \tau(a) = (a, 0, 0, \dots),$$

and $\tau(a)$ is called the Teichmüller representative of the element a. Let

$$K_R := \{\tau(a_0) + \tau(a_1)p + \tau(a_2)p^2 + \cdots \mid a_i \in R, i = 0, 1, 2, \dots\}.$$

Then K_R will be a p-adic ring under the usual addition and multiplication via its isomorphism with $W(R)$. Moreover, if R is a field, then K_R is a complete discrete valuation ring of zero characteristic with residue field R and maximal ideal pK_R. Each element $(a_0, a_1, a_2 \dots) \in W(R)$ can be uniquely represented in K_R as

$$\tau(a_0) + \tau(a_1)p + \tau(a_2)p^2 + \cdots$$

However, this bijection is not a ring isomorphism between $W(R)$ and K_R because it does not respect the addition. Since R is a perfect ring with characteristic p, we have $R \cong R^p$ via the Frobenius map $\phi : a \mapsto a^p$. The true ring isomorphism between $W(R)$ and K_R is denoted by τ again and given explicitly by

$$\tau : W(R) \to K_R, \quad (a_0, a_1, a_2, \dots) \mapsto \tau(a_0) + \tau(a_1)^{p^{-1}} p + \tau(a_2)^{p^{-2}} p^2 + \cdots$$

We usually adopt the alternative expression for τ given as below

$$\tau : W(R) \to K_R, \quad (a_0, a_1^p, a_2^{p^2}, \dots) \mapsto \tau(a_0) + \tau(a_1)p + \tau(a_2)p^2 + \cdots \tag{9}$$

The advantage of the expression (9) lies in that it makes the Witt polynomials become homogenous (cf. Remark 2.1) and hence the polynomial $S_n^{(r)}$ is weighted homogeneous of weighted degree p^n by Lemma 2.3.

Example 2.5. A well-known example is that $W(\mathbb{F}_q) \cong \mathbb{Z}_q$. In particular, the finite Witt ring $W(\mathbb{F}_q)/p^m W(\mathbb{F}_q)$ becomes $\mathbb{Z}_q/p^m\mathbb{Z}_q$.

Now let $r \in \mathbb{N}$, we dicuss the r-fold addition and the r-fold multiplication in K_R. For $j \in [1, r]$, let

$$X_j = (x_{0j}, x_{1j}^p, x_{2j}^{p^2}, \cdots) \in W(R).$$

Then,

$$\tau(X_j) = \sum_i^{\infty} \tau(x_{ij})p^i \in K_R,$$

where τ denotes the ring isomorphism between $W(R)$ and K_R given by (9). We want to find two functions $\widetilde{s}_n^{(r)}$ and $\widetilde{m}_n^{(r)}$, which behave like $S_n^{(r)}$ and $M_n^{(r)}$ as defined in Lemma 2.3, such that

$$\begin{aligned} \sum_{j=1}^{r} \left(\sum_{i=0}^{\infty} \tau(x_{ij})p^i \right) &= \sum_{n=0}^{\infty} \tau(\widetilde{s}_n^{(r)})p^n, \\ \prod_{j=1}^{r} \left(\sum_{i=0}^{\infty} \tau(x_{ij})p^i \right) &= \sum_{n=0}^{\infty} \tau(\widetilde{m}_n^{(r)})p^n. \end{aligned} \tag{10}$$

The formulae for $\widetilde{s}_n^{(r)}$ and $\widetilde{m}_n^{(r)}$ are given below, and the proof for $r = 2$ can also be found in [23, Theorem 1.5].

Theorem 2.6. *With the above notation, for $n \in \mathbb{N}_0$ we have*

$$\begin{aligned} \widetilde{s}_n^{(r)} &= S_n^{(r)}(x_{01}^{1/p^n}, \dots, x_{0r}^{1/p^n}; x_{11}^{1/p^{n-1}}, \dots, x_{1r}^{1/p^{n-1}}; \dots; x_{n1}, \dots, x_{nr}), \text{ and} \\ \widetilde{m}_n^{(r)} &= M_n^{(r)}(x_{01}^{1/p^n}, \dots, x_{0r}^{1/p^n}; x_{11}^{1/p^{n-1}}, \dots, x_{1r}^{1/p^{n-1}}; \dots; x_{n1}, \dots, x_{nr}). \end{aligned}$$

Let $s_n^{(r)} := (\widetilde{s}_n^{(r)})^{p^n}$ and $m_n^{(r)} := (\widetilde{m}_n^{(r)})^{p^n}$, then we have

$$\begin{aligned} s_n^{(r)} &= S_n^{(r)}(x_{01}, \dots, x_{0r}; x_{11}^p, \dots, x_{1r}^p; \dots; x_{n1}^{p^n}, \dots, x_{nr}^{p^n}), \text{ and} \\ m_n^{(r)} &= M_n^{(r)}(x_{01}, \dots, x_{0r}; x_{11}^p, \dots, x_{1r}^p; \dots; x_{n1}^{p^n}, \dots, x_{nr}^{p^n}). \end{aligned}$$

The polynomials $s_n^{(r)}$ and $m_n^{(r)}$ have integer coefficients. Moreover, $s_n^{(r)}$ is homogeneous of degree p^n and $m_n^{(r)}$ is homogeneous of degree rp^n in the variables x_{ij}.

Proof. We only consider the r-fold addition. Let $\oplus$ denote the addition in the ring $W(R)$. Like in (6), we have

$$(S_0^{[r]}, \dots, S_n^{[r]}, \dots) = X_1 \oplus \cdots \oplus X_r, \tag{11}$$

where

$$S_n^{[r]} = S_n^{(r)}(x_{01}, \dots, x_{0r}; x_{11}^p, \dots, x_{1r}^p; \dots; x_{n1}^{p^n}, \dots, x_{nr}^{p^n}).$$

Applying the map τ to the two sides of (11) and combining (10) yields

$$\sum_{n=0}^{\infty} \tau(S_n^{[r]})^{p^{-n}} p^n = \sum_{j=1}^{r} \tau(X_j) = \sum_{j=1}^{r} \left(\sum_{i=0}^{\infty} \tau(x_{ij}) p^i \right) = \sum_{n=0}^{\infty} \tau(\widetilde{s}_n^{(r)}) p^n.$$

Therefore $\tau(S_n^{[r]})^{p^{-n}} = \tau(\widetilde{s}_n^{(r)})$ and hence $(S_n^{[r]})^{p^{-n}} = \widetilde{s}_n^{(r)}$ for all $n \in \mathbb{N}_0$. That is,

$$\widetilde{s}_n^{(r)} = (S_n^{(r)})^{p^{-n}}(x_{01}, \dots, x_{0r}; x_{11}^p, \dots, x_{1r}^p; \dots; x_{n1}^{p^n}, \dots, x_{nr}^{p^n}). \tag{12}$$

Since R is perfect with characteristic p, we can put the power p^{-n} inside, namely

$$\widetilde{s}_n^{(r)} = S_n^{(r)}(x_{01}^{1/p^n}, \dots, x_{0r}^{1/p^n}; x_{11}^{1/p^{n-1}}, \dots, x_{1r}^{1/p^{n-1}}; \dots; x_{n1}, \dots, x_{nr}).$$

Note the degrees of variables in $\widetilde{s}_n^{(r)}$ are fractions. To apply the Ax-Katz theorem later, we need them to be integers. Let $s_n^{(r)} := (\widetilde{s}_n^{(r)})^{p^n}$. Then by (12), we have

$$s_n^{(r)} = S_n^{(r)}(x_{01}, \dots, x_{0r}; x_{11}^p, \dots, x_{1r}^p; \dots; x_{n1}^{p^n}, \dots, x_{nr}^{p^n}). \tag{13}$$

It follows from Lemma 2.3 that the polynomial $s_n^{(r)}$ has integer coefficients and that $s_n^{(r)}$ is homogeneous of degree p^n. The result for $m_n^{(r)}$ can be deduced similarly. □

Remark 2.7. In the following we simply write $s_n^{(r)}$, which means by default it is in the variables $\{x_{ij}^{p^i} \mid i \in [0, n], j \in [1, r]\}$. As presented in (13) the order of $x_{ij}^{p^i}$ may affect the expression of $s_n^{(r)}$, but it does not affect the homogeneous degree of $s_n^{(r)}$, with which we are most concerned. So we may loosely write $s_n^{(r)} = s_n^{(r)}(x_{ij}^{p^i} \mid i \in [0, n], j \in [1, r])$ when the variables are needed to be indicated.

Lemma 2.8. *Let R be a perfect ring with characteristic p. Let $m \in \mathbb{N}$ and $\sum_{i=0}^{\infty} \tau(x_i)p^i \in K_R$ with $x_i \in R$. Then the following statements are equivalent:*

(i) $\sum_{i=0}^{\infty} \tau(x_i)p^i \equiv 0 \pmod{p^m}$.

(ii) $x_0 = x_1 = \cdots = x_{m-1} = 0$.
(iii) $x_0 = x_1^p = \cdots = x_{m-1}^{p^{m-1}} = 0$.

Proof. It follows directly from that $\tau((0,0,\dots)) = 0$ and that τ is a ring isomorphism between $W(R)$ and K_R. □

The above lemma can be easily extended to the r-fold addition, which will play the crucial role in our later proofs.

Lemma 2.9. *Let R be a perfect ring with characteristic p. Let $m, r \in \mathbb{N}$ and $\sum_{i=0}^{\infty} \tau(x_{ij})p^i \in K_R$ with $x_{ij} \in R, j \in [1,r]$. Suppose $\sum_{j=1}^{r} \left(\sum_{i=0}^{\infty} \tau(x_{ij})p^i\right) = \sum_{n=0}^{\infty} \tau(\widetilde{s}_n^{(r)})p^n$. For $n \in \mathbb{N}_0$, let $s_n^{(r)} := (\widetilde{s}_n^{(r)})^{p^n}$. Then the following statements are equivalent:*

(i) $\sum_{j=1}^{r} \sum_{i=0}^{\infty} \tau(x_{ij})p^i \equiv 0 \pmod{p^m}$.
(ii) $\widetilde{s}_0^{(r)} = \widetilde{s}_1^{(r)} = \cdots = \widetilde{s}_{m-1}^{(r)} = 0$.
(iii) $s_0^{(r)} = s_1^{(r)} = \cdots = s_{m-1}^{(r)} = 0$.

3. q-divisibility theorem for the Teichmüller box

Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. In this section, we always let $R = \mathbb{F}_q$ and denote by $W(\mathbb{F}_q)$ the ring of Witt vectors over $\mathbb{F}_q$. Let T_q be the set of Teichmüller representatives of $\mathbb{F}_q$ in $\mathbb{Z}_q$ and the related Teichmüller lifting be $\tau : \mathbb{F}_q \to \mathbb{Z}_q, a \mapsto \tau(a)$. Then $T_q = \{\tau(a) | a \in \mathbb{F}_q\}$ and for each $a \in \mathbb{F}_q$, we have $\tau(a)^q = \tau(a)$ and $\tau(a) \equiv a \pmod{p}$. Then $T_q = \{\zeta^i | i = 1, 2, \dots, q-1\} \cup \{0\}$ where ζ is a primitive $(q-1)$-th root of unity in $\mathbb{Z}_q$. For any $a \in T_q$, let $\widetilde{a}$ be the unique element in $\mathbb{F}_q$ such that $\tau(\widetilde{a}) = a$. We call T_q^n the Teichmüller box in $\mathbb{Z}_q^n$.

Another construction of $\mathbb{Z}_q$ is using the ring $W(\mathbb{F}_q)$, the Witt vectors over $\mathbb{F}_q$, as described in Section 2. The ring isomorphism between $W(\mathbb{F}_q)$ and $\mathbb{Z}_q$ is given by

$$\tau : W(\mathbb{F}_q) \to \mathbb{Z}_q, \quad (a_0, a_1^p, a_2^{p^2}, \dots) \mapsto \tau(a_0) + \tau(a_1)p + \tau(a_2)p^2 + \cdots \tag{14}$$

If $\mathbb{F}_q = \mathbb{F}_p$, then $W(\mathbb{F}_p) \cong \mathbb{Z}_p$. Moreover, since $a^p = a$ for $a \in \mathbb{F}_p$, the map (14) becomes

$$\tau : W(\mathbb{F}_p) \to \mathbb{Z}_p, \quad (a_0, a_1, a_2, \dots) \mapsto \tau(a_0) + \tau(a_1)p + \tau(a_2)p^2 + \cdots \tag{15}$$

Let $\mathbb{Z}_q[x_1, \dots, x_n]$ denote the ring of polynomials in n variables $x_1, \dots, x_n$ with coefficients in $\mathbb{Z}_q$. Write $X^u = x_1^{d_1} \cdots x_n^{d_n}$ with $u = (d_1, \dots, d_n) \in \mathbb{N}_0^n$. Let $f = \sum_{j=1}^{r} a_j X^{u_j} \in \mathbb{Z}_q[x_1, \dots, x_n]$ with $0 \neq a_j \in \mathbb{Z}_q$. We can write

$$a_j = \sum_{i=0}^{\infty} a_{ij} p^i, \quad a_{ij} \in T_q.$$

This is called the Teichmüller expansion of a_j. Similarly,

$$f = \sum_{j=1}^{r}\sum_{i=0}^{\infty} a_{ij}p^i X^{u_j} = \sum_{j=1}^{r}\sum_{i=0}^{\infty}(a_{ij}X^{u_j})p^i = \sum_{i=0}^{\infty} p^i \sum_{j=1}^{r} a_{ij}X^{u_j}$$

is the Teichmuller expansion of the polynomial f. We first consider the single polynomial case.

3.1. For a single polynomial

A polynomial $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ is called a Teichmüller polynomial if all of its coefficients are Teichmüller elements in T_q. Clearly, any polynomial $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ has the unique expansion

$$f(X) = \sum_{i=0}^{\infty} p^i f_i(X),$$

where each $f_i(X)$ is a Teichmüller polynomial. This is called the Teichmüller expansion of f. It is obtained from the Teichmüller expansion of the coefficients of f.

Theorem 3.1 *(Strong Version). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a nonzero polynomial. Given an $m \in \mathbb{N}$, let*

$$V := \{X \in T_q^n \mid f(X) \equiv 0 \pmod{p^m}\}.$$

Let $f = \sum_{i=0}^{\infty} p^i f_i$ be the Teichmüller expansion of f. Let $d \in \mathbb{N}$. If $\deg(f_i) \le dp^{h\lfloor \frac{i}{h} \rfloor}$ for all $i \in [0, m-1]$, then

$$\mathrm{ord}_q(|V|) \ge \left\lceil \frac{n - \frac{p^m-1}{p-1}d}{p^{m-1}d} \right\rceil. \tag{16}$$

Proof. Let $s_n^{(r)}$ be the polynomial as defined before, which is homogeneous of degree p^n by Theorem 2.6. Write

$$f = \sum_{i=0}^{\infty} p^i f_i = \sum_{i=0}^{\infty} p^i \sum_{j=1}^{r} a_{ij}X^{u_j},\ a_{ij} \in T_q.$$

From Lemma 2.9 we know that for a given $X \in T_q^n$, $f(X) \equiv 0 \pmod{p^m}$ if and only if

$$g_k(\widetilde{X}) := s_k^{(r)}\left((\widetilde{a}_{ij}\widetilde{X}^{u_j})^{p^i} \mid i \in [0,k], j \in [1,r]\right) = 0, \text{ for all } k \in [0, m-1].$$

Note $\widetilde{a}_{ij}, \widetilde{X} \in \mathbb{F}_q^n$ with $X \in T_q^n$. Define

$$\widetilde{V} := \left\{ X \in \mathbb{F}_q^n \mid g_k(X) = 0 \text{ for all } k \in [0, m-1] \right\}.$$

Then $|V| = |\widetilde{V}|$. Note $(\widetilde{a}_{ij} X^{u_j})^{p^i} = (\widetilde{a}_{ij} X^{u_j})^{p^{i-h\lfloor \frac{i}{h} \rfloor}}$ in $\mathbb{F}_q$ with $q = p^h$. Now

$$\deg(a_{ij} X^{u_j}) \le \deg(f_i) \le d p^{h\lfloor \frac{i}{h} \rfloor}.$$

It follows that

$$\deg((\widetilde{a}_{ij} X^{u_j})^{p^{i-h\lfloor \frac{i}{h} \rfloor}}) \le d p^{h\lfloor \frac{i}{h} \rfloor} p^{i-h\lfloor \frac{i}{h} \rfloor} = d p^i.$$

So by Lemma 2.3, $\deg(g_k) \le d p^k$ for $k \in [0, m-1]$. Thus

$$\sum_{k=0}^{m-1} \deg(g_k) \le \sum_{k=0}^{m-1} p^k d = \frac{p^m - 1}{p-1} d. \tag{17}$$

Applying the Ax-Katz Theorem 1.2 to $\widetilde{V}$ and using (17), we obtain

$$\mathrm{ord}_q(|\widetilde{V}|) \ge \left\lceil \frac{n - \sum_{k=0}^{m-1} \deg(g_k)}{\max_{k \in [0,m-1]} \deg(g_k)} \right\rceil \ge \left\lceil \frac{n - \frac{p^m - 1}{p-1} d}{p^{m-1} d} \right\rceil. \tag{18}$$

Then (16) follows from (18) and the equality that $|V| = |\widetilde{V}|$. □

If $\deg(f) = d$, then $\deg(f_i) \le d \le d p^{h\lfloor \frac{i}{h} \rfloor}$ for all i and thus the condition of the theorem is automatically satisfied. This gives the following weaker but simpler consequence.

Corollary 3.2 *(Weak Version). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a nonzero polynomial. Given an $m \in \mathbb{N}$, let*

$$V := \{ X \in T_q^n \mid f(X) \equiv 0 \pmod{p^m} \}.$$

Then

$$\mathrm{ord}_q(|V|) \ge \left\lceil \frac{n - \frac{p^m - 1}{p-1} \deg(f)}{p^{m-1} \deg(f)} \right\rceil.$$

Corollary 3.2, in which the condition is weaker than Theorem 3.1, can be viewed as the generalized $\mathbb{Z}_q$-version of Theorem 1.3 with $s = 1$ for the Teichmüller box case. In other words, Theorem 3.1 not only generalizes but also improves Theorem 1.3 for one polynomial in the Teichmüller box case.

Corollary 3.3 below follows from Theorem 3.1 and the fact that $h\lfloor\frac{i}{h}\rfloor = i$ for $h = 1$.

Corollary 3.3. *Let p be a prime number. Let $f \in \mathbb{Z}_p[x_1, \ldots, x_n]$ be a nonzero polynomial. Given an $m \in \mathbb{N}$, let*

$$V := \{X \in T_p^n \mid f(X) \equiv 0 \pmod{p^m}\}.$$

Let $f = \sum_{i=0}^{\infty} p^i f_i$ be the Teichmüller expansion of f. Let $d \in \mathbb{N}$. If $\deg(f_i) \le dp^i$ for all $i \in [0, m-1]$, then

$$\mathrm{ord}_p(|V|) \ge \left\lceil \frac{n - \frac{p^m-1}{p-1}d}{p^{m-1}d} \right\rceil.$$

Note that the degree condition $\deg(f_i) \le dp^i$ is significantly weaker than the condition $\deg(f) \le d$, which allows those terms of f that are divisible by p have much larger degree than d.

3.2. For a polynomial system

Theorem 3.1 can be extended to the system of polynomials without much more difficulties except for more cumbersome notation. Theorem 3.4 below generalizes as well as improves Theorem 1.3 for the Teichmüller box case.

Theorem 3.4 *(Strong Version). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $f_1, \ldots, f_s \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in T_q^n \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1, s]\}.$$

Write the p-adic Teichmüller expansion

$$f_k = \sum_{i=0}^{\infty} p^i f_{k,i}(X), \ k \in [1, s].$$

Let $d_1, \ldots, d_s \in \mathbb{N}$. If $\deg(f_{k,i}) \le d_k p^{h\lfloor\frac{i}{h}\rfloor}$ for all $i \in [0, m_k - 1]$, $k \in [1, s]$, then

$$\mathrm{ord}_q(|V|) \ge \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} d_k}{\max_{k\in[1,s]}\{p^{m_k-1}d_k\}} \right\rceil.$$

Proof. From the proof of Theorem 3.1, we see that for each modulus p^{m_k}, the polynomial f_k contributes m_k polynomials g_{tk} over $\mathbb{F}_q$ ($t \in [0, m_k - 1]$) whose degree is bounded by $p^t d_k$ and thus $\sum_{t=0}^{m_k-1} \deg(g_{tk}) \le \frac{p^{m_k}-1}{p-1} d_k$. Now given s polynomials f_k and

s moduli p^{m_k}, $k \in [1,s]$, we get $\sum_{k=1}^{s} m_k$ polynomials over $\mathbb{F}_q$ with the sum of degrees $\leq \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} d_k$ and maximal degree bounded by $\max_{k\in[1,s]}\{p^{m_k-1}d_k\}$. Applying the Ax-Katz theorem, we obtain the desired result. □

Let $d_k = \deg(f_k)$. Then trivially we have $\deg(f_{k,i}) \leq d_k \leq d_k p^{h\lfloor \frac{i}{h} \rfloor}$. This gives the following weaker corollary.

Corollary 3.5 *(Weak Version). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $f_1, \ldots, f_s \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in T_q^n \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1,s]\}.$$

Then

$$\mathrm{ord}_q(|V|) \geq \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} \deg(f_k)}{\max_{k\in[1,s]}\{p^{m_k-1}\deg(f_k)\}} \right\rceil.$$

In the case $q = p$, the theorem becomes

Corollary 3.6. *Let p be a prime number. Let $f_1, \ldots, f_s \in \mathbb{Z}_p[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in T_p^n \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1,s]\}.$$

For each $k \in [1,s]$, write the p-adic Teichmüller expansion

$$f_k = \sum_{i=0}^{\infty} p^i f_{k,i}(X).$$

Let $d_1, \ldots, d_s \in \mathbb{N}$. If $\deg(f_{k,i}) \leq d_k p^i$ for all $i \in [0, m_k - 1]$, $k \in [1,s]$, then

$$\mathrm{ord}_p(|V|) \geq \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} d_k}{\max_{k\in[1,s]}\{p^{m_k-1}d_k\}} \right\rceil.$$

Note that in the p-adic expansion of the polynomial f_k, the condition $\deg(f_{k,i}) \leq d_k p^i$ for $i \geq 1$ is significantly weaker than the condition $\deg(f_k) \leq d_k$. Namely, the degree of those terms in f_k which are divisible by p can have much larger degree than d_k.

4. q-divisibility theorem for the general box

The box T_q^n in the previous section is called the Teichmüller box. A natural question is whether our results in Section 3, especially Theorem 3.4, hold true for other non-

Teichmüller boxes $\mathcal{B}$. We address this question in this section. For this purpose, we first need to understand a general box algebraically.

Recall that a box $\mathcal{B}$ in $\mathbb{Z}_q^n$ is defined to be a complete system of representatives of $\mathbb{F}_q^n$ in $\mathbb{Z}_q^n$. The box $\mathcal{B}$ considered in Theorem 1.3 is a special case in split form, that is, $\mathcal{B} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_n$, where each $\mathcal{I}_i$ is a complete system of representatives of $\mathbb{F}_q$ in $\mathbb{Z}_q/p\mathbb{Z}_q$. Now, we would like to describe the box $\mathcal{B}$ in terms of the image of a polynomial system.

A polynomial $g \in \mathbb{Z}_q[x_1, \ldots, x_n]$ is called a Teichmüller polynomial if all of its coeffcients are Teichmüller elements in T_q. The polynomial g is called reduced if its degree in each variable is at most $q-1$. Thus, a reduced polynomial $g \in \mathbb{Z}_q[x_1, \ldots, x_n]$ has total degree at most $n(q-1)$. For any given box $\mathcal{B}$, the elements in $\mathcal{B}$ can be uniquely determined by a system of reduced polynomials over $\mathbb{Z}_q$.

Lemma 4.1. *Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $\mathcal{B} \subseteq \mathbb{Z}_q^n$ with $|\mathcal{B}| = q^n$ and $\mathcal{B} \mod p = \mathbb{F}_q^n$.*

(i) *There exists a unique system of reduced Teichmüller polynomials $g_{ij} \in \mathbb{Z}_q[x_1, \ldots, x_n]$ depending only on the box $\mathcal{B}$ with $j \in [1, n], i \in \mathbb{N}$ such that for any $Y = (y_1, \ldots, y_n) \in \mathcal{B}$, we have*

$$Y = X + (g_{11}(X), \ldots, g_{1n}(X))p + (g_{21}(X), \ldots, g_{2n}(X))p^2 + \cdots, \tag{19}$$

where $X = (x_1, \ldots, x_n) \in T_q^n$ is the Teichmüller lifting of the modulo p reduction of Y.

(ii) *There exists a unique system of reduced polynomials $g_j \in \mathbb{Z}_q[x_1, \ldots, x_n]$ depending only on the box $\mathcal{B}$ with $j \in [1, n]$ such that for any $Y = (y_1, \ldots, y_n) \in \mathcal{B}$, we have*

$$Y = X + (g_1(X), \ldots, g_n(X))p, \tag{20}$$

where $X = (x_1, \ldots, x_n) \in T_q^n$ is the Teichmüller lifting of the modulo p reduction of Y. In particular, $\mathcal{B}$ is the image of T_q^n under the polynomial map $X \to X + (g_1(X), \ldots, g_n(X))p$.

(iii) *Assume that $\mathcal{B}$ is in split form. Then (19) becomes*

$$Y = X + (g_{11}(x_1), \ldots, g_{1n}(x_n))p + (g_{21}(x_1), \ldots, g_{2n}(x_n))p^2 + \cdots,$$

where each $g_{ij}(x_j) \in \mathbb{Z}_q[x_j]$ is a reduced Teichmüller polynomial in the one variable x_j and hence has degree at most $q-1$ for $j \in [1, n], i \in \mathbb{N}$. Equivalently, (20) becomes

$$Y = X + (g_1(x_1), \ldots, g_n(x_n))p,$$

where each $g_j(x_j) \in \mathbb{Z}_q[x_j]$ is a reduced polynomial in the one variable x_j and hence degree at most $q-1$ for all $1 \le j \le n$.

Proof. (ii) is equivalent to (i) by taking

$$g_j = \sum_{i=1}^{\infty} p^{i-1} g_{ij},\ 1 \le j \le n.$$

Thus, the right side is just the Teichmüller expansion of the left side. (iii) is a consequence of (i) and (ii) by applying them to each one dimensional factor of the split box $\mathcal{B}$. We shall now prove (i).

For a given $Y = (y_1, \ldots, y_n) \in \mathcal{B}$, we can write uniquely

$$(y_1, \ldots, y_n) = (x_{01}, \ldots, x_{0n}) + (x_{11}, \ldots, x_{1n})p,$$

where $X = (x_{01}, \ldots, x_{0n}) \in T_q^n$ and $(x_{11}, \ldots, x_{1n}) \in \mathbb{Z}_q^n$. The vector $X = (x_{01}, \ldots, x_{0n})$ in T_q^n and the vector $Y = (y_1, \ldots, y_n)$ in $\mathcal{B}$ determine each other. In fact, X is just the Teichmüller lifting of the reduction $Y \mod p$, and Y is the unique element in $\mathcal{B}$ with the same mod p reduction as X. In particular, $(x_{11}, \ldots, x_{1n})$ is also uniquely determined by $X = (x_{01}, \ldots, x_{0n})$.

Letting Y run over $\mathcal{B}$, then X runs over T_q^n as $\mathcal{B} \mod p = \mathbb{F}_q^n$ by assumption. For each $1 \le j \le n$, the quantity x_{1j} is a function of X. This establishes a map from T_q^n to $\mathbb{Z}_q$, and we consider the corresponding map from $\mathbb{F}_q^n$ to $\mathbb{F}_q$, namely

$$\widetilde{g}_{1j}: \quad \mathbb{F}_q^n \to \mathbb{F}_q, \quad X \mapsto \widetilde{g}_{1j}(X).$$

Recall the fact that any map from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ can be expressed uniquely by a reduced polynomial in n variables with coefficients in $\mathbb{F}_q$. In particular, our map $\widetilde{g}_{1j}$ is a reduced polynomial in $\mathbb{F}_q[x_1, \cdots, x_n]$. Let g_{1j} be the Teichmüller lifting of $\widetilde{g}_{1j}$ in $\mathbb{Z}_q[x_1, \ldots, x_n]$. Then, we have proved

$$Y = X + (g_{11}(X), \cdots, g_{1n}(X))p + (x_{21}, \cdots, x_{2n})p^2,$$

where $(x_{21}, \cdots, x_{2n}) \in \mathbb{Z}_q^n$ is uniquely determined by X. Continuing this procedure, we find uniquely determined reduced Teichmüller polynomials $g_{ij}(X) \in \mathbb{Z}_q[x_1, \cdots, x_n]$ $(i \ge 1,\ 1 \le j \le n)$ such that (i) holds. The lemma is proved. □

Remark 4.2. For convenience, set $g_{0j}(X) = x_j$ for $j \in [1, n]$. Then, equation (19) becomes

$$Y = \sum_{i=0}^{\infty} (g_{i1}(X), \ldots, g_{in}(X))p^i. \tag{21}$$

We simply write $\mathcal{B} = T_q^n(g_{ij} : j \in [1, n], i \in \mathbb{N})$ provided that the g_{ij}'s are reduced Teichmüller polynomials in $\mathbb{Z}_q[x_1, \ldots, x_n]$.

This completes our discussion on the box $\mathcal{B}$. We now move to the reduction from polynomial congruences in the box $\mathcal{B}$ to equations over the finite field $\mathbb{F}_q$.

Fix a nonzero vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ with $|\alpha| := \alpha_1 + \cdots + \alpha_n$. For an element $\beta \in \mathbb{N}_0^{|\alpha|}$ of the form

$$\beta = (\beta_{11}, \ldots, \beta_{\alpha_1 1}; \beta_{12}, \ldots, \beta_{\alpha_2 2}; \ldots; \beta_{1n}, \ldots, \beta_{\alpha_n n}), \tag{22}$$

we write $\beta = (\beta_{tl})$ for short with β_{tl} arranged as in (22) and define $|\beta| := \sum_{l=1}^{n} \sum_{t=1}^{\alpha_l} \beta_{tl}$. By (19), one has $Y = (y_1, \ldots, y_n)$ with $y_j = \sum_{i=0}^{\infty} g_{ij}(X)p^i$ for $j \in [1, n]$. Then

$$\prod_{l=1}^{n} \left(\sum_{k=0}^{\infty} g_{kl}(X)p^k \right)^{\alpha_l} = \sum \prod_{l=1}^{n} \prod_{t=1}^{\alpha_l} \left(g_{\beta_{tl}l}(X)p^{\beta_{tl}} \right) = \sum \left(\prod_{l=1}^{n} \prod_{t=1}^{\alpha_l} g_{\beta_{tl}l}(X) \right) p^{|\beta|}, \tag{23}$$

where both the sums in (23) run over all the vectors $\beta = (\beta_{tl}) \in \mathbb{N}_0^{|\alpha|}$. In particular, if $\deg(g_{ij}) \le p^{h\lfloor \frac{i}{h} \rfloor}$ for $j \in [1, n], i \in [1, m-1]$, then for any $\beta = (\beta_{tl}) \in \mathbb{N}_0^{|\alpha|}$ with $|\beta| \le m-1$, we have

$$\deg \left(\prod_{l=1}^{n} \prod_{t=1}^{\alpha_l} g_{\beta_{tl}l}(X) \right) = \sum_{l=1}^{n} \sum_{t=1}^{\alpha_l} \deg(g_{\beta_{tl}l}(X)) \le \sum_{l=1}^{n} \sum_{t=1}^{\alpha_l} p^{h\lfloor \frac{\beta_{tl}}{h} \rfloor} \le |\alpha| p^{h\lfloor \frac{|\beta|}{h} \rfloor}. \tag{24}$$

4.1. For a single polynomial

Like in Section 3, we first consider the single polynomial case.

Theorem 4.3 *(Strong Version). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $\mathcal{B} \subseteq \mathbb{Z}_q^n$ with $|\mathcal{B}| = q^n$ and $\mathcal{B} \mod p = \mathbb{F}_q^n$, and $\mathcal{B} = T_q^n(g_{ij} : j \in [1, n], i \in \mathbb{N})$. Let $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a nonzero polynomial. Given an $m \in \mathbb{N}$, let*

$$V := \{X \in \mathcal{B} \mid f(X) \equiv 0 \pmod{p^m}\}.$$

Write the Teichmüller expansion $f = \sum_{i=0}^{\infty} p^i f_i$ with $f_i = \sum_{j=1}^{r} a_{ij} X^{u_j}$. Let $d \in \mathbb{N}$. If for each term $a_{ij}X^{u_j}$, we have

$$\deg \left(a_{ij} \prod_{l=1}^{n} \prod_{t=1}^{\alpha_l} g_{\beta_{tl}l}(X) \right) \le dp^{h\lfloor \frac{i+|\beta|}{h} \rfloor} \tag{25}$$

for all $i \in [0, m-1]$, $j \in [1, r]$, $\beta = (\beta_{tl}) \in \mathbb{N}_0^{|u_j|}$ with the sum $i + |\beta| \le m-1$, then

$$\operatorname{ord}_q(|V|) \ge \left\lceil \frac{n - \frac{p^m - 1}{p-1} d}{p^{m-1} d} \right\rceil.$$

Proof. We follow the notations used in the proof of Theorem 3.1, so we do not explain them more. Choose an arbitrary term of f, say $a_{ij}X^u p^i$ with $u=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}_0^n$ and take any $\beta=(\beta_{tj})\in\mathbb{N}_0^{|u|}$. Let $Y=(y_1,\ldots,y_n)$ with $y_j=\sum_{i=0}^{\infty}g_{ij}(X)p^i$ for $j\in[1,n]$. Substituting Y for X in this term, by (23) we have

$$a_{ij}p^i\prod_{l=1}^{n}\prod_{t=1}^{\alpha_l}\left(g_{\beta_{tl}l}(X)p^{\beta_{tl}}\right)=a_{ij}p^{i+|\beta|}\prod_{l=1}^{n}\prod_{t=1}^{\alpha_l}g_{\beta_{tl}l}(X).$$

This is zero modulo p^m if $i+|\beta|\geq m$. Thus, we can assume $i+|\beta|\leq m-1$. Since $a^{p^h}=a^q=a$ for $a\in\mathbb{F}_q$, we deduce

$$\left(\widetilde{a}_{ij}\prod_{l=1}^{n}\prod_{t=1}^{\alpha_l}\widetilde{g}_{\beta_{tl}l}(X)\right)^{p^{i+|\beta|}}=\left((\widetilde{a}_{ij}\prod_{l=1}^{n}\prod_{t=1}^{\alpha_l}\widetilde{g}_{\beta_{tl}l}(X)\right)^{p^{i+|\beta|-h\lfloor\frac{i+|\beta|}{h}\rfloor}}.$$

By (25), we have

$$\deg\left(a_{ij}\prod_{l=1}^{n}\prod_{t=1}^{\alpha_l}g_{\beta_{tl}l}(X)\right)^{p^{i+|\beta|-h\lfloor\frac{i+|\beta|}{h}\rfloor}}\leq dp^{h\lfloor\frac{i+|\beta|}{h}\rfloor}p^{i+|\beta|-h\lfloor\frac{i+|\beta|}{h}\rfloor}=dp^{i+|\beta|}.$$

The remaining is similar to the proof of Theorem 3.1. □

A weak version is the following result.

Corollary 4.4 *(Weak Version). Let p be a prime number and $q=p^h$ with $h\in\mathbb{N}$. Let $\mathcal{B}\subseteq\mathbb{Z}_q^n$ with $|\mathcal{B}|=q^n$ and $\mathcal{B}\bmod p=\mathbb{F}_q^n$, and $\mathcal{B}=T_q^n(g_{ij}:j\in[1,n],i\in\mathbb{N})$. Let $f\in\mathbb{Z}_q[x_1,\ldots,x_n]$ be a nonzero polynomial. Given an $m\in\mathbb{N}$, let*

$$V:=\{X\in\mathcal{B}\mid f(X)\equiv 0\pmod{p^m}\}.$$

If $\deg(g_{ij})\leq p^{h\lfloor\frac{i}{h}\rfloor}$ for $j\in[1,n],i\in[1,m-1]$, then

$$\mathrm{ord}_q(|V|)\geq\left\lceil\frac{n-\frac{p^m-1}{p-1}\deg(f)}{p^{m-1}\deg(f)}\right\rceil.$$

Proof. Suppose $\deg(g_{ij})\leq p^{h\lfloor\frac{i}{h}\rfloor}$ for $j\in[1,n],i\in[1,m-1]$. Let $d=\deg(f)$. By (24) we see that (25) holds naturally for $\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}_0^n$ and $\beta=(\beta_{tl})\in\mathbb{N}_0^{|\alpha|}$ with $|\beta|\leq m-1$. □

Corollary 4.4 for the case $q=p$ becomes simpler because $h\lfloor\frac{i}{h}\rfloor=i$ for $h=1$.

Corollary 4.5 *(Weak Version). Let p be a prime number. Let $\mathcal{B} \subseteq \mathbb{Z}_p^n$ with $|\mathcal{B}| = p^n$ and $\mathcal{B} \mod p = \mathbb{F}_p^n$, and $\mathcal{B} = T_p^n(g_{ij} : j \in [1,n], i \in \mathbb{N})$. Let $f \in \mathbb{Z}_p[x_1, \ldots, x_n]$ be a nonzero polynomial. Given an $m \in \mathbb{N}$, let*

$$V := \{X \in \mathcal{B} \mid f(X) \equiv 0 \pmod{p^m}\}.$$

If $\deg(g_{ij}) \le p^i$ for all $j \in [1,n], i \in [1, m-1]$, then

$$\mathrm{ord}_p(|V|) \ge \left\lceil \frac{n - \frac{p^m-1}{p-1}\deg(f)}{p^{m-1}\deg(f)} \right\rceil. \tag{26}$$

In particular, (26) holds true for all $\mathcal{B}$ in split form.

4.2. For a polynomial system

We extend the results above to the system of polynomials. The proofs are omitted since they are very similar to the ones given above.

Theorem 4.6 *(Strong Version). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $\mathcal{B} \subseteq \mathbb{Z}_q^n$ with $|\mathcal{B}| = q^n$ and $\mathcal{B} \mod p = \mathbb{F}_q^n$, and $\mathcal{B} = T_q^n(g_{ij} : j \in [1,n], i \in \mathbb{N})$. Let $f_1, \ldots, f_s \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in \mathcal{B} \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1,s]\}.$$

For each $k \in [1,s]$, write the p-adic Teichmüller expansion

$$f_k = \sum_{i=0}^{\infty} p^i f_{k,i}(X),$$

with $f_{k,i}(X) = \sum_{j=1}^{r_k} a_{ij}^{(k)} X^{u_j^{(k)}}$. Let $d_1, \ldots, d_s \in \mathbb{N}$. If for each term $a_{ij}^{(k)} X^{u_j^{(k)}}$, we have

$$\deg\left(a_{ij}^{(k)} \prod_{l=1}^{n} \prod_{t=1}^{\alpha_l} g_{\beta_{tl}l}(X)\right) \le d_k p^{h\lfloor \frac{i+|\beta|}{h} \rfloor}$$

for all $i \in [0, m_k - 1]$, $j \in [1, r_k]$, $\beta = (\beta_{tj}) \in \mathbb{N}_0^{|u_j^{(k)}|}$ with the sum $i + |\beta| \le m_k - 1$, then

$$\mathrm{ord}_q(|V|) \ge \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} d_k}{\max_{k\in[1,s]}\{p^{m_k-1} d_k\}} \right\rceil.$$

A weaker consequence is the following

Corollary 4.7 *(Weak Version). Let p be a prime number and $q = p^h$ with $h \in \mathbb{N}$. Let $\mathcal{B} \subseteq \mathbb{Z}_q^n$ with $|\mathcal{B}| = q^n$ and $\mathcal{B} \mod p = \mathbb{F}_q^n$, and $\mathcal{B} = T_q^n(g_{ij} : j \in [1,n], i \in \mathbb{N})$. Let $f_1, \ldots, f_s \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in \mathcal{B} \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1,s]\}.$$

Let $m = \max_{i\in[1,s]}\{m_i\}$. If $\deg(g_{ij}) \le p^{h\lfloor \frac{i}{h} \rfloor}$ for $j \in [1,n], i \in [1, m-1]$, then

$$\mathrm{ord}_q(|V|) \ge \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} \deg(f_k)}{\max_{k\in[1,s]}\{p^{m_k-1}\deg(f_k)\}} \right\rceil.$$

In the case $q = p$, the above corollary reduces to

Corollary 4.8 *(Weak Version). Let p be a prime number. Let $\mathcal{B} \subseteq \mathbb{Z}_p^n$ with $|\mathcal{B}| = p^n$ and $\mathcal{B} \mod p = \mathbb{F}_p^n$, and $\mathcal{B} = T_p^n(g_{ij} : j \in [1,n], i \in \mathbb{N})$. Let $f_1, \ldots, f_s \in \mathbb{Z}_p[x_1, \ldots, x_n]$ be a system of nonzero polynomials. For given $m_1, \ldots, m_s \in \mathbb{N}$, let*

$$V := \{X \in \mathcal{B} \mid f_k(X) \equiv 0 \pmod{p^{m_k}} \text{ for all } k \in [1,s]\}.$$

Let $m = \max_{i\in[1,s]}\{m_i\}$. If $\deg(g_{ij}) \le p^i$ for all $j \in [1,n], i \in [1, m-1]$, then

$$\mathrm{ord}_p(|V|) \ge \left\lceil \frac{n - \sum_{k=1}^{s} \frac{p^{m_k}-1}{p-1} \deg(f_k)}{\max_{k\in[1,s]}\{p^{m_k-1}\deg(f_k)\}} \right\rceil. \tag{27}$$

In particular, (27) holds true for all boxes $\mathcal{B}$ in split form.

5. Examples

The corollary above shows that Theorem 1.3 extends to any box $\mathcal{B}$ in split form when $q = p$. However, as illustrated in the examples below, Theorem 1.3 cannot be extended to arbitrary $\mathcal{B}$ in general, even when $q = p$ (cf. Example 5.1) or $\mathcal{B}$ in split form if q is a higher power of p, (cf. the last two rows in Table 1 in Example 5.2).

Example 5.1. Let $p = 2$. Let $f = x_1 + x_2 + x_3 + x_4 \in \mathbb{Z}_2[x_1, x_2, x_3, x_4]$. Let $V = \{X \in T_2^4 \mid f(X) = 0\}$. By Theorem 3.1, we have $\mathrm{ord}_p(|V|) \ge 1$ (in fact $\mathrm{ord}_p(|V|) = 3$). Given an $a \in T_2$, let $\mathcal{B}_a = \{(a_1 + (a_1a_2a_3a_4 + a)p, a_2, a_3, a_4) \mid a_i \in T_2, i \in [1,4]\}$ and $V_a = \{X \in \mathcal{B}_a \mid f(X) = 0 \pmod{p^2}\}$. Thus, we have $g_1 = x_1x_2x_3x_4 + a$, and $g_i = 0$ for $i \in [2,4]$. Now we consider the cardinality of V_a, that is, the number of solutions of the congruence

$$(x_1 + x_2 + x_3 + x_4) + (x_1x_2x_3x_4 + a)2 \equiv 0 \pmod{2^2}$$

Table 1
$|V_u|$ and $\mathrm{ord}_p(|V_u|)$ for some $u \in \mathbb{N}_0^5$.

u	$3u \mod q-1$	$\lvert V_u\rvert$	$\mathrm{ord}_p(\lvert V_u\rvert)$
$(4,4,4,4,4)$	$(4,4,4,4,4)$	1206	2
$(5,5,5,5,5)$	$(7,7,7,7,7)$	2601	2
$(6,6,6,6,6)$	$(2,2,2,2,2)$	864	3
$(7,7,7,7,7)$	$(5,5,5,5,5)$	1881	2
$(8,8,8,8,8)$	$(8,8,8,8,8)$	606	1
$(4,7,2,5,8)$	$(4,5,6,7,8)$	660	1

with $x_i \in T_2$. By Lemma 2.9 and Remark 2.4, it is equivalent to counting the number of solutions in $\mathbb{F}_2$ of the system

$$\begin{cases} y_1+y_2+y_3+y_4=0, \\ y_1y_2y_3y_4+\widetilde{a}-\sum \frac{1}{2}\binom{2}{t_1,\ldots,t_4} y_1^{t_1}\cdots y_4^{t_4}=0, \end{cases}$$

where $y_i=\widetilde{x}_i$ for $i\in[1,4]$ and the sum in the second equation is over all the tuples $(t_1,\ldots,t_4)$ satisfying that $t_1+\cdots+t_4=2$ and $0\le t_i<2$ for all i. By easy calculation, we get $|V_0|=1$ and $|V_1|=7$ respectively, to both of which Theorem 3.1 cannot be applied as $\deg(g_1)=4$ is larger than $p=2$.

Example 5.2. Let $p=3$ and $q=p^2=9$. Let $f=x_1+\cdots+x_5\in\mathbb{Z}_q[x_1,\ldots,x_5]$. Given a vector $u=(d_1,\ldots,d_5)\in\mathbb{N}_0^5$, let the box $\mathcal{B}_{(d_1,\ldots,d_5)}$ be the set $\{(a_1+a_1^{d_1}p,\ldots,a_5+a_5^{d_5}p)\mid a_i\in T_q, i\in[1,5]\}$, or in concise notation,

$$\mathcal{B}_u=\{(X,\cdots,X_5)+(X_1^{d_1},\cdots,X_5^{d_5})p \mid X_i\in T_q\}.$$

Define $V_u:=\{X\in\mathcal{B}_u \mid f(X)\equiv 0 \pmod{p^2}\}$. By Theorem 3.1, we have $\mathrm{ord}_p(|V_{\mathbf{0}}|)\ge 2$ (in fact $\mathrm{ord}_p(|V_{\mathbf{0}}|)=8$). Now we consider the cardinality of V_u for $u=(d_1,\ldots,d_5)\neq\mathbf{0}$, that is, the number of solutions of the congruence

$$(x_1+\cdots+x_5)+(x_1^{d_1}+\cdots+x_5^{d_5})p\equiv 0 \pmod{p^2}$$

with $x_i\in T_q$. By Lemma 2.9 and Remark 2.4, it is equivalent to counting the number of solutions in $\mathbb{F}_q$ of the system

$$\begin{cases} y_1+\cdots+y_5=0, \\ y_1^{3d_1}+\cdots+y_5^{3d_5}-\sum \frac{1}{3}\binom{3}{t_1,\ldots,t_5} y_1^{t_1}\cdots y_5^{t_5}=0, \end{cases}$$

where $y_i=\widetilde{x}_i$ for $i\in[1,5]$ and the sum in the second equation is over all the tuples $(t_1,\ldots,t_5)$ satisfying that $t_1+\cdots+t_5=3$ and $0\le t_i<3$ for all i. Randomly choosing some vectors $u\in\mathbb{N}_0^5$ in which some components are greater than p (so Theorem 3.1 is not valid for them), and computing via computer, we get the results listed in Table 1.

The last two rows in Table 1 show that Theorem 4.6 is false without the degree bound condition on g_{ij}, even for split boxes.

Data availability

The authors are unable or have chosen not to specify which data has been used.

Acknowledgments

The authors thank the anonymous reviewers for carefully reading the manuscript and providing the constructive comments. The authors also thank Weihua Li for providing the data in Example 5.2 by computer program. The first author is jointly supported by the National Natural Science Foundation of China (Grant No. 11871291), and Natural Science Foundation of Fujian Province, China (Grant No. 2022J02046). The second author is partially supported by NSF.

References

[1] A. Adolphson, S. Sperber, p-adic estimates for exponential sums and the theorem of Chevalley–Warning, Ann. Sci. Éc. Norm. Supér. 20 (1987) 545–556.
[2] E. Aichinger, J. Moosbauer, Chevalley Warning type results on abelian groups, J. Algebra 569 (2021) 30–66.
[3] J. Ax, Zeros of polynomials over finite fields, Am. J. Math. 86 (1964) 255–261.
[4] I. Baoulina, A. Bishnoi, P. Clark, A generalization of the theorems of Chevalley-Warning and Ax-Katz via polynomial substitutions, Proc. Am. Math. Soc. 147 (10) (2019) 4107–4122.
[5] D. Brink, Chevalley's theorem with restricted variables, Combinatorica 31 (1) (2011) 127–130.
[6] W. Cao, A partial improvement of the Ax–Katz theorem, J. Number Theory 132 (2012) 485–494.
[7] W. Cao, Dilation of Newton polytope and p-adic estimate, Discrete Comput. Geom. 45 (2011) 522–528.
[8] W. Cao, p-adic valuations associated to fibers and images of polynomial functions, Finite Fields Appl. 77 (2022) 101951.
[9] W. Cao, Q. Sun, Improvements upon the Chevalley-Warning-Ax-Katz-type estimate, J. Number Theory 122 (2007) 135–141.
[10] P. Cartier, Groupes formels associés aux anneaux de Witt généralisés, C. R. Acad. Sci. Paris, Sér. A–B 265 (1967) A129–A132.
[11] F.N. Castro, O. Moreno, I. Rubio, An improvement of a theorem of Carlitz, J. Pure Appl. Algebra 224 (5) (2020) 106246.
[12] J.M. Chen, W. Cao, Degree matrices and divisibility of exponential sums over finite fields, Arch. Math. (Basel) 94 (2010) 435–441.
[13] C. Chevalley, Démonstration d'une hypothése de M. Artin, Abh. Math. Semin. Univ. Hamb. 11 (1935) 73–75.
[14] P. Clark, T. Genao, F. Saia, Chevalley-Warning at the boundary, Expo. Math. 39 (4) (2021) 604–623.
[15] P. Clark, A. Forrow, J.R. Schmitt, Warning's second theorem with restricted variables, Combinatorica 37 (3) (2017) 397–417.
[16] D.J. Grynkiewicz, A generalization of the Chevalley-Warning and Ax-Katz theorems with a view towards combinatorial number theory, arXiv:2208.12895, 2022.
[17] D.R. Heath-Brown, A note on the Chevalley-Warning theorems, Russ. Math. Surv. 66 (2) (2011) 427–436.
[18] X.D. Hou, A note on the proof of a theorem of Katz, Finite Fields Appl. 11 (2005) 316–319.
[19] T. Lai, A. Marino, A. Robinson, D.Q. Wan, Moment subset sums over finite fields, Finite Fields Appl. 62 (2020) 101607.
[20] N.M. Katz, On a theorem of Ax, Am. J. Math. 93 (1971) 485–499.

[21] O. Moreno, C.J. Moreno, Improvement of the Chevalley-Warning and the Ax-Katz theorem, Am. J. Math. 117 (1995) 241–244.
[22] O. Moreno, K. Shum, F.N. Castro, V.P. Kumar, Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications, Proc. Lond. Math. Soc. 88 (3) (2004) 545–564.
[23] J. Rabinoff, The theory of Witt vectors, arXiv:1409.7445, 2014.
[24] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by M.J. Greenberg.
[25] Z.W. Sun, D.Q. Wan, Lucas type congruences for cyclotomic Ψ-coefficients, Int. J. Number Theory 4 (2) (2008) 155–170.
[26] D.Q. Wan, An elementary proof of a theorem of Katz, Am. J. Math. 111 (1989) 1–8.
[27] D.Q. Wan, A Chevalley-Warning approach to the p-adic estimates of character sums, Proc. Am. Math. Soc. 123 (1995) 45–54.
[28] E. Warning, Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, Abh. Math. Semin. Univ. Hamb. 11 (1935) 76–83.
[29] R. Wilson, A lemma on polynomials modulo p^m and applications to coding theory, Discrete Math. 306 (23) (2006) 3154–3165.
[30] E. Witt, Zyklische körper und algebren der charakteristik p vom grad p^n. Struktur diskret bewerteter perfekter körper mit vollkommenem restklassenkörper der charakteristik p, J. Reine Angew. Math. 176 (1937) 126–140.