PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 12, December 2009, Pages 4065–4075
S 0002-9939(09)10017-5
Article electronically published on July 28, 2009

POINT COUNT DIVISIBILITY FOR ALGEBRAIC SETS OVER $\mathbb{Z}/p^\ell\mathbb{Z}$ AND OTHER FINITE PRINCIPAL RINGS

DANIEL J. KATZ

(Communicated by Ted Chinburg)

Abstract. We determine the greatest common divisor of the cardinalities of the algebraic sets generated by collections of polynomials $f_1, \dots, f_t$ of specified degrees $d_1, \dots, d_t$ in n variables over a finite principal ring R. This generalizes the theorems of Ax ($t = 1$, R a field), N. M. Katz (t arbitrary, R a field), and Marshall-Ramage ($t = 1$, R an arbitrary finite principal ring).

1. Introduction and statement of result

We are interested in the number of solutions of a system of equations of the form

$$f_1(x_1, \dots, x_n) = f_2(x_1, \dots, x_n) = \cdots = f_t(x_1, \dots, x_n) = 0,$$

where $f_1, \dots, f_t$ are polynomials in the n variables $x_1, \dots, x_n$ over a finite principal ring. By a *principal ring*, we mean a commutative ring with identity in which all ideals can be generated by a single element. For the rest of this paper R will always denote a finite principal ring; we are particularly interested in the case $R = \mathbb{Z}/p^\ell\mathbb{Z}$, but we shall prove our results in full generality. We let $V(f_1, \dots, f_t; R)$ denote the set of simultaneous zeroes of $f_1, \dots, f_t$ for $(x_1, \dots, x_n) \in R^n$, and we let $N(f_1, \dots, f_t; R) = |V(f_1, \dots, f_t; R)|$. We are interested in divisibility properties of $N(f_1, \dots, f_t; R)$. For nonnegative integers $d_1, \dots, d_t$, we set $D(d_1, \dots, d_t; R)$ to be the greatest common divisor of all values of $N(f_1, \dots, f_t; R)$ obtained when each f_i is allowed to vary (independently of the others) over the set of all polynomials of degree d_i in $R[x_1, \dots, x_n]$. In this paper, we take the degree of the zero polynomial to be zero (rather than $-\infty$, as is more usual).

Our problem has already been addressed extensively for R a field. The first results concern the case of the zeroes of a single polynomial ($t = 1$) when $R = \mathbb{F}_q$, the finite field of characteristic p with $q = p^e$ elements. Chevalley [6] showed that if $f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$ is a polynomial with $\deg(f) < n$ and without constant coefficient, then f must have a zero other than $(0, 0, \dots, 0)$. Warning [25] improved this result by showing that $N(f; \mathbb{F}_q)$ is divisible by p when $\deg(f) < n$ (and he showed that this remains true even if we allow f to have a constant coefficient). Ax strengthened Warning's result to show that the cardinality of the zero set can be divisible by higher powers of p if the degree is significantly less than n.

Received by the editors July 10, 2007, and, in revised form, April 26, 2009.
2000 *Mathematics Subject Classification.* Primary 11T06; Secondary 13M10.

Theorem 1.1 (Ax [3]). *If f is a nonconstant polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$, then we have $q^{\max\left\{0, \left\lceil \frac{n-\deg(f)}{\deg(f)} \right\rceil\right\}} \mid N(f; \mathbb{F}_q)$.*

This was generalized by N. M. Katz to a result about the p-divisibility of the cardinality of the zero set of a family of polynomials.

Theorem 1.2 (N. M. Katz [10]). *If $f_1, \ldots, f_t$ are polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$, not all of which are constant, then $q^{\max\left\{0, \left\lceil \frac{n-\sum_i \deg(f_i)}{\max_i \deg(f_i)} \right\rceil\right\}} \mid N(f_1, \ldots, f_t; \mathbb{F}_q)$.*

Both Ax's theorem and N. M. Katz's generalization give lower bounds on the p-divisibility of the cardinality of the zero set that are sharp in a certain sense.

Proposition 1.3 (N. M. Katz [10]). *For any t nonnegative integers $d_1, \ldots, d_t$, not all of which are zero, there are polynomials $f_1, \ldots, f_t \in \mathbb{F}_q[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$ for each i such that $pq^{\max\left\{0, \left\lceil \frac{n-\sum_i d_i}{\max_i d_i} \right\rceil\right\}} \nmid N(f_1, \ldots, f_t; \mathbb{F}_q)$, where p is the characteristic of $\mathbb{F}_q$.*

Note that the original statement of this proposition by N. M. Katz also asserts that one can choose $f_1, \ldots, f_t$ to be homogeneous, but the proof that he supplies only establishes the above proposition as stated, for he reduces the general case to the case $t = 1$ and then relies on Ax's proof [3] of the $t = 1$ case, which unfortunately does not always provide a homogeneous polynomial. However, it is not difficult to modify Ax's proof of the $t = 1$ case to invariably furnish homogeneous polynomials and thus to substantiate N. M. Katz's claim (see [9] for such a modification). Although Proposition 1.3 shows that the lower bounds on p-divisibility established by Ax and Katz cannot be improved if we are given only the degrees of the polynomials, there are many improvements and extensions that concern polynomials of specific forms or use information other than or in addition to the degrees of the polynomials [20], [8], [1], [24], [13], [7], [18], [14], [22], [21], [16], [15], [19], [17], [4], [5].

We may unify Theorem 1.2 and Proposition 1.3 into a statement about the greatest common divisor of cardinalities of algebraic sets.

Theorem 1.4 (Restatement of N. M. Katz's Results [10]). *For any t nonnegative integers $d_1, \ldots, d_t$, we have $D(d_1, \ldots, d_t; \mathbb{F}_q) = q^{\max\left\{0, \left\lceil \frac{n-(d_1+\cdots+d_t)}{\max\{1, d_1, \ldots, d_t\}} \right\rceil\right\}}$.*

Proof. Clearly the stated power of q, and no higher power of the characteristic of $\mathbb{F}_q$, divides $D(d_1, \ldots, d_t; \mathbb{F}_q)$ by Theorem 1.2 and Proposition 1.3. (Provided some $d_i > 0$; if all $d_i = 0$, then our claim is immediate.) If we set each $f_i = x_{\min\{i,n\}}^{d_i}$ when $d_i > 0$ and set $f_i = 0$ when $d_i = 0$, then we obtain an algebraic set $V(f_1, \ldots, f_t; \mathbb{F}_q)$ whose cardinality is a power of q and which is generated by polynomials of the relevant degrees. Thus no prime other than the characteristic of the field $\mathbb{F}_q$ can divide $D(d_1, \ldots, d_t; \mathbb{F}_q)$. □

Marshall and Ramage [11] generalized Ax's theorem in a different direction. They continued to consider only a single polynomial, but they generalized from polynomials over finite fields to polynomials over finite principal rings. Before stating their full result, we must make a brief consideration of the structure of finite principal rings and show that one can reduce the problem to the consideration of local finite principal rings.

A finite principal ring R can be decomposed as a direct sum $R^{(1)} \oplus \cdots \oplus R^{(r)}$ of local finite principal rings $R^{(i)}$ (see [2, p. 90] or [12, Chapter VI]). Then every element $a \in R$ decomposes as $a = a^{(1)} + \cdots + a^{(r)}$ with each $a^{(i)} \in R^{(i)}$, and each polynomial g decomposes as $g = g^{(1)} + \cdots + g^{(r)}$ with each $g^{(i)} \in R^{(i)}[x_1, \ldots, x_n]$ in such a manner that $\deg(g) = \max\{\deg(g^{(1)}), \ldots, \deg(g^{(r)})\}$. Furthermore $g(a_1, \ldots, a_n) = 0$ if and only if $g^{(i)}(a_1^{(i)}, \ldots, a_n^{(i)}) = 0$ for $i = 1, \ldots, r$, so that $N(f_1, \ldots, f_t; R) = \prod_{i=1}^{r} N(f_1^{(i)}, \ldots, f_t^{(i)}; R^{(i)})$. Then $D(d_1, \ldots, d_t; R)$ is the greatest common divisor of $\prod_{i=1}^{r} N(f_1^{(i)}, \ldots, f_t^{(i)}; R^{(i)})$ when we allow each $f_j^{(i)}$ to run through the polynomials of degree d_j or less over $R^{(i)}$, with the condition that for each j at least one $f_j^{(i)}$ must have degree d_j. If we define $D(\leq d_1, \ldots, \leq d_t; R^{(i)})$ to be the greatest common divisor of $N(f_1^{(i)}, \ldots, f_t^{(i)}; R^{(i)})$ as each $f_j^{(i)}$ varies (independently of the rest) over those polynomials in $R^{(i)}[x_1, \ldots, x_n]$ of degree d_j or less, then we have

$$\prod_{i=1}^{r} D(\leq d_1, \ldots, \leq d_t; R^{(i)}) \leq D(d_1, \ldots, d_t; R) \leq \prod_{i=1}^{r} D(d_1, \ldots, d_t; R^{(i)}).$$

Finally, we shall see below that $D(d_1, \ldots, d_t; R^{(i)})$ is nonincreasing (in the multiplicative ordering of the integers) in each argument d_i (considered with the normal ordering of the integers), so that $D(\leq d_1, \ldots, \leq d_t; R^{(i)}) = D(d_1, \ldots, d_t; R^{(i)})$, and so

$$D(d_1, \ldots, d_t; R) = \prod_{i=1}^{r} D(d_1, \ldots, d_t; R^{(i)}). \tag{1.1}$$

We already have observed this monotonicity of $D(d_1, \ldots, d_t; R^{(i)})$ in the results of N. M. Katz (Theorem 1.4) when $R^{(i)}$ is a finite field, and we shall see that it is true for any local finite principal ring below.

Before stating the result of Marshall and Ramage, we should also state a few pertinent facts about our local finite principal rings $R^{(i)}$. Each such ring (being local) has a maximal ideal generated by a prime π_i (since our ring is principal), and $R^{(i)}/(\pi_i)$ is the residue field $\mathbb{F}_{q_i}$. By locality, all elements not in the maximal ideal (π_i) must be units. The sequence of powers of π_i must repeat since R is finite and $\pi_i^j = \pi_i^{j+k}$ means $\pi_i^j(1 - \pi_i^k) = 0$. Note that $1 - \pi_i^k \notin (\pi_i)$ and hence is a unit. Thus there is some least integer ℓ_i such that $\pi_i^{\ell_i} = 0$. If we let T_i be a set of q representatives modulo π_i, then each element of $a \in R^{(i)}$ can be written uniquely as $a = \sum_{j=0}^{\ell_i - 1} \pi_i^j a_j$ with each $a_j \in T_i$, and thus $\left|R^{(i)}\right| = q_i^{\ell_i}$. Now we may state the result of Marshall and Ramage.

Theorem 1.5 (Marshall-Ramage [11])**.** *Let R be a finite principal ring with decomposition $R^{(1)} \oplus \cdots \oplus R^{(r)}$ into local finite principal rings $R^{(i)}$, each with residue field $\mathbb{F}_{q_i}$ and $\left|R^{(i)}\right| = q_i^{\ell_i}$. Then for any nonnegative integer d, we have $D(d, R) = \prod_{i=1}^{r} D(d, R^{(i)})$, and each $D(d, R^{(i)})$ is equal to $q_i^{\max\left\{0, \left\lceil \frac{n-d}{\max\{1,d\}} \right\rceil\right\}}$ if $\ell_i = 1$ (i.e., if $R^{(i)} = \mathbb{F}_{q_i}$); and if $\ell_i > 1$, then*

$$D(d, R^{(i)}) = \begin{cases} q_i^{\left\lfloor \frac{n\ell_i - 1}{2} \right\rfloor} & \text{if } d > 1, \\ q_i^{(n-1)\ell_i} & \text{if } d = 1, \\ q^{n\ell_i} & \text{if } d = 0. \end{cases}$$

In this paper we present a generalization of the Marshall-Ramage result to zero sets of multiple polynomial equations over R. This generalization is analogous (in content, not method) to N. M. Katz's generalization (Theorem 1.2) of Ax's Theorem (Theorem 1.1).

Theorem 1.6. *Let R be a finite principal ring with decomposition $R^{(1)} \oplus \cdots \oplus R^{(r)}$ into local finite principal rings $R^{(i)}$, each with residue field $\mathbb{F}_{q_i}$ and $\left|R^{(i)}\right| = q_i^{\ell_i}$. Let $d_1, \ldots, d_t$ be nonnegative integers, and let T be the number of d_j not equal to zero. Then we have $D(d_1, \ldots, d_t; R) = \prod_{i=1}^{r} D(d_1, \ldots, d_t; R^{(i)})$. Each $D(d_1, \ldots, d_t; R^{(i)})$ is equal to $q_i^{\max\left\{0, \left\lceil \frac{n-(d_1+\cdots+d_t)}{\max\{1, d_1, \ldots, d_t\}} \right\rceil\right\}}$ if $\ell_i = 1$ (i.e., if $R^{(i)} = \mathbb{F}_{q_i}$). If $\ell_i > 1$ and $n \leq T$, then $D(d_1, \ldots, d_t; R^{(i)}) = 1$; while if $\ell_i > 1$ and $n > T$, then*

$$D(d_1, \ldots, d_t; R^{(i)}) = \begin{cases} q_i^{\left\lfloor \frac{(n-T+1)\ell_i - 1}{2} \right\rfloor} & \text{if any } d_j > 1, \\ q_i^{(n-T)\ell_i} & \text{otherwise.} \end{cases}$$

In the commentary leading up to (1.1), we proved that the product formula in the above theorem for $D(d_1, \ldots, d_t; R)$ will hold if we can prove that $D(d_1, \ldots, d_t; R^{(i)})$ is nonincreasing (in the integers multiplicatively ordered) as each d_i increases (in the usual ordering). So the first assertion of the theorem follows from the rest, and of course the second assertion (the $\ell_i = 1$ case) is just the result of N. M. Katz (Theorem 1.4). So it remains for us to prove the $\ell_i > 1$ case, as we shall do in Section 3 after some preliminary work in Section 2. We included the possibility of zero values for the degrees d_i in the formal statement of our theorem only because it is important to establish the monotonicity of $D(d_1, \ldots, d_t; R^{(i)})$; in all other respects this a triviality and a nuisance. Before we proceed to proofs, let us consider the specialization of our theorem to $R = \mathbb{Z}/p^{\ell}\mathbb{Z}$ (and all d_i positive) and two brief examples.

Corollary 1.7. *Let $\ell > 1$ and let $d_1, \ldots, d_t$ be positive integers. If $n \leq t$, then we have $D(d_1, \ldots, d_t; \mathbb{Z}/p^{\ell}\mathbb{Z}) = 1$; while if $n > t$, then*

$$D(d_1, \ldots, d_t; \mathbb{Z}/p^{\ell}\mathbb{Z}) = \begin{cases} p^{\left\lfloor \frac{(n-t+1)\ell - 1}{2} \right\rfloor} & \text{if any } d_j > 1, \\ p^{(n-t)\ell} & \text{if } d_1 = \cdots = d_t = 1. \end{cases}$$

Example 1.8. Suppose that we consider systems of polynomial equations in the polynomial ring $\mathbb{Z}/12\mathbb{Z}[v, w, x, y, z]$ of the form

$$f(v, w, x, y, z) = g(v, w, x, y, z) = 0,$$

where $\deg(f) = 3$ and $\deg(g) = 1$. We claim that Theorem 1.6 shows that the number of solutions will always be divisible by 24, and indeed, the greatest common divisor $D(3, 1; \mathbb{Z}/12\mathbb{Z})$ of all solution set cardinalities is 24.

Our ring of coefficients $R = \mathbb{Z}/12\mathbb{Z}$ is isomorphic to $R^{(1)} \oplus R^{(2)} = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and so $D(3, 1; \mathbb{Z}/12\mathbb{Z}) = D(3, 1; \mathbb{Z}/4\mathbb{Z}) \cdot D(3, 1; \mathbb{Z}/3\mathbb{Z})$. Now $R^{(1)} = \mathbb{Z}/4\mathbb{Z}$ has residue field $\mathbb{F}_2$ and $\ell_1 = 2$, and we have $n = 5$ variables and $T = 2$ nonconstant equations, one of which is of degree greater than 1, so that $D(3, 1; \mathbb{Z}/8\mathbb{Z}) = 2^3 = 8$. On the other hand $R^{(2)} = \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$, so that $\ell_2 = 1$, and so $D(3, 1; \mathbb{Z}/3\mathbb{Z}) = 3^1$. Therefore $D(\mathbb{Z}/12\mathbb{Z}) = 8 \cdot 3 = 24$ according to Theorem 1.6.

If we set $f(v, w, x, y, z) = v(wx + yz)$ and $g(v, w, x, y, z) = v - 1$, then the simultaneous zeroes are the 5-tuples $(1, w, x, y, z)$ with $wx + yz = 0$. It is not hard to calculate that as w and x run through the elements of $\mathbb{Z}/12\mathbb{Z}$, the product wx

takes each value $\pm 1, \pm 5$ four times, each value ± 2 eight times, each value ± 3 ten times, each value ± 4 sixteen times, the value 6 twenty times, and the value 0 forty times. The same can be said of the product yz as y and z run through $\mathbb{Z}/12\mathbb{Z}$. Thus $wx + yz$ has

$$\begin{aligned} 4 \cdot 4^2 + 2 \cdot 8^2 + 2 \cdot 10^2 + 2 \cdot 16^2 + 1 \cdot 20^2 + 1 \cdot 40^2 &= 2904 \\ &= 2^3 \cdot 3 \cdot 11^2 \end{aligned}$$

zeroes in $(\mathbb{Z}/12\mathbb{Z})^4$, which, as we have seen, is equal to the number of solutions of the system $f(v, w, x, y, z) = g(v, w, x, y, z) = 0$.

On the other hand, if we set $f(v, w, x, y, z) = v(1 + 4v^2)$ and $g(v, w, x, y, z) = w$, then the simultaneous zeroes are of the form $(0, 0, x, y, z)$ with x, y, z arbitrary. Thus there are $12^3 = 2^6 \cdot 3^3$ solutions of the system $f(v, w, x, y, z) = g(v, w, x, y, z) = 0$.

Note that the solution set cardinalities in both cases are divisible by 24. Their greatest common divisor is precisely 24.

One may ask whether, when given $d_1, \ldots, d_t$, one can always find a system of polynomials $f_1, \ldots, f_t$, each with $\deg(f_i) = d_i$ and such that $N(f_1, \ldots, f_t; R) = D(d_1, \ldots, d_t; R)$. The following example shows that this is not the case.

Example 1.9. Let $R = \mathbb{Z}/9\mathbb{Z}$, $n = 2$, $t = 1$, and $d_1 = 2$, so that we are considering zero sets of single quadratic polynomials in two variables over $\mathbb{Z}/9\mathbb{Z}$. By Theorem 1.5 (or also by Corollary 1.7 of the more general Theorem 1.6), we have $D(2; \mathbb{Z}/9\mathbb{Z}) = 3$. We shall see that no quadratic polynomial $f(x, y) \in \mathbb{Z}/9\mathbb{Z}[x, y]$ has $N(f; \mathbb{Z}/9\mathbb{Z}) = 3$.

By applying invertible affine transformations of variables to our polynomials, it is not hard to show that any quadratic polynomial $Q(x, y)$ in $\mathbb{Z}/9\mathbb{Z}[x, y]$ can be transformed into a polynomial of the form $f(x, y) = u(g(x) \pm h(y) + c)$, where u is a unit in $\mathbb{Z}/9\mathbb{Z}$; c is a constant in $\mathbb{Z}/9\mathbb{Z}$; $g(x)$ is one of the following: $g_1(x) = x^2$, $g_2(x) = 3x^2 + x$, or $g_3(x) = 3x^2$; and $h(y)$ is one of the following: $h_1(y) = y^2$, $h_2(y) = 3y^2 + y$, $h_3(y) = 3y^2$, $h_4(y) = y$, $h_5(y) = 3y$, or $h_6(y) = 0$.

As x runs through $\mathbb{Z}/9\mathbb{Z}$, the values of $g_2(x) = 3x^2 + x$ run through $\mathbb{Z}/9\mathbb{Z}$, so that $N(f; Z/9\mathbb{Z}) = 9$ if $g = g_2$. The same is true if $h = h_2$ or h_4. So we need consider only $g \in \{g_1, g_3\}$ and $h \in \{h_1, h_3, h_5, h_6\}$.

Note that $x^2 = 0$ for three values of x in $\mathbb{Z}/9\mathbb{Z}$, and x^2 takes each value in the set of quadratic residues $\{1, 4, 7\}$ for precisely two values of x. Thus if $g(x) = g_1(x) = x^2$ and $h(y) = h_1(y) = y^2$, then $N(f; \mathbb{Z}/9\mathbb{Z})$ is either zero or at least $2 \cdot 2 = 4$. The same analysis may be applied with combinations involving $g_3(x) = 3x^2$ or $h_3(y) = 3y^2$ when we realize that $3x^2$ takes the value 0 for three values of x and takes the value 3 for six values of x. Also $h_5(y) = 3y$ takes each value in $\{0, 3, 6\}$ for precisely three values of y and $h_6(y) = 0$ takes the value 0 for all 9 values of y. Therefore any $f(x) = u(g(x) \pm h(y) + c)$ with $g \in \{g_1, g_3\}$ and $h \in \{h_1, h_3, h_5, h_6\}$ must have $N(f; \mathbb{Z}/9\mathbb{Z}) = 0$ or $N(f; \mathbb{Z}/9\mathbb{Z}) \geq 4$.

We have shown that there is no quadratic $f(x, y) \in \mathbb{Z}/9\mathbb{Z}[x, y]$ with $N(f; \mathbb{Z}/9\mathbb{Z}) = D(2; \mathbb{Z}/9\mathbb{Z}) = 3$. Without too much difficulty, one may show that the set of values of $N(f; \mathbb{Z}/9\mathbb{Z})$ as f ranges over all quadratic polynomials in $\mathbb{Z}/9\mathbb{Z}[x, y]$ is $\{0, 6, 9, 12, 18, 21, 27, 36, 45, 54\}$, the greatest common divisor of which is indeed 3, although 3 itself is not in the set.

A result related to Corollary 1.7 can be found in the work of Wilson [26], who counts solutions in $\{0, 1, \ldots, p-1\}^n$ and in $\{0, 1\}^n$ of polynomial equations modulo

prime powers involving n variables. In fact, Wilson allows for different prime power moduli in different equations. Corollary 1.7, on the other hand, involves systems in which all the equations are modulo p^ℓ and solutions are sought in a full set $\{0, 1, \dots, p^\ell - 1\}^n$. Wilson's results, which improve upon earlier results of Schanuel [23], have useful applications in combinatorics (see his paper [26] for details).

2. Row operations and variable reindexing

For this section, and indeed for the rest of the paper, we assume that R is a local finite principal ring whose maximal ideal is generated by the prime π and whose residue field is $\mathbb{F}_q$. We assume that $|R| = q^\ell$, and we use p to denote the characteristic of $\mathbb{F}_q$ and set e so that $q = p^e$. We shall use boldface letters as shorthand for lists of n elements; for example, $\mathbf{x}$ is shorthand for $x_1, \dots, x_n$ and $\mathbf{a}$ is shorthand for $a_1, \dots, a_n$.

If $f_1, \dots, f_t$ is a list of polynomials in $R[x_1, \dots, x_n]$, we shall often find it expedient to transform this list into another list, $g_1, \dots, g_t$, by performing a finite number of modifications of the following types:

(1) We may permute the order of the polynomials in the list.
(2) We may replace any polynomial $\phi(\mathbf{x})$ with $u\phi(\mathbf{x})$, where u is a unit in R.
(3) If $\phi(\mathbf{x})$ and $\psi(\mathbf{x})$ are in the list and $r \in R$, then we may replace $\psi(\mathbf{x})$ with $\psi(\mathbf{x}) - r\phi(\mathbf{x})$.
(4) We may permute the indices of the variables $x_1, \dots, x_n$.

Procedures 1–3 are the standard row operations to a system of equations over a ring. If $g_1, \dots, g_t$ is obtained from $f_1, \dots, f_t$ using a sequence of these operations only, then $V(f_1, \dots, f_t; R) = V(g_1, \dots, g_t; R)$. Operation 4 corresponds to reindexing the variables. If we allow ourselves to use this operation as well in changing $f_1, \dots, f_t$ to $g_1, \dots, g_t$, then $V(f_1, \dots, f_t; R)$ and $V(g_1, \dots, g_t; R)$ are the same up to permutation of coordinates. Thus $N(f_1, \dots, f_t; R) = N(g_1, \dots, g_t; R)$.

We say that our new list $g_1, \dots, g_t$ is *row-reduced in the linear part* to mean that there are integers $\epsilon_1 \le \epsilon_2 \le \cdots \le \epsilon_t \le \ell$ such that for each i, we have

$$g_i(\mathbf{x}) = c_i + \pi^{\epsilon_i} x_i + \pi^{\epsilon_i} L_i(x_{i+1}, \dots, x_n) + Q_i(\mathbf{x}), \tag{2.1}$$

where Q_i has no terms of degree 0 or 1, L_i is homogeneous of degree 1, and c_i is a constant in R. We also insist that if $j > i$ with $\epsilon_j = \epsilon_i$, then x_j does not appear in L_i. It is not hard to see that if we are allowed to use all operations 1–4, then we can always transform a list of polynomials into another list that is row-reduced in the linear part.

3. The p-divisibility of algebraic sets over local finite principal rings

After stating Theorem 1.6, we went on to show that it suffices to demonstrate only the final assertion of the theorem, which we restate here.

Proposition 3.1. *Let R be a local finite principal ring with residue field $\mathbb{F}_q$ and $|R| = q^\ell$ for some $\ell > 1$. Let $d_1, \dots, d_t$ be nonnegative integers, and let T be the number of d_i not equal to zero. If $n \le T$, then $D(d_1, \dots, d_t; R) = 1$; while if $n > T$, then*

$$D(d_1, \dots, d_t; R) = \begin{cases} q^{\lfloor \frac{(n-T+1)\ell - 1}{2} \rfloor} & \text{if any } d_i > 1, \\ q^{(n-T)\ell} & \text{otherwise.} \end{cases}$$

The conventions in the first paragraph of the previous section remain in force: R is a local finite principal ring with maximal ideal generated by the prime π, residue field $\mathbb{F}_q$, $|R| = q^\ell$, $q = p^e$ for the rational prime p, and boldface letters represent lists of n elements. We shall first prove that greatest common divisors of the cardinalities of algebraic sets over R are at least as great as asserted in Proposition 3.1, and then we shall show that they are no greater. We begin with two auxiliary results that will be used in our proof of the proposition. We start with the simple case of counting zeroes of systems of polynomials of the first degree.

Lemma 3.2. *Let $\ell \geq 1$, let $n \geq t$, and let $f_1, \ldots, f_t \in R[x_1, \ldots, x_n]$ be of first degree. Then $q^{(n-t)\ell} \mid N(f_1, \ldots, f_t; R)$.*

Proof. By the comments in Section 2, we may replace $f_1, \ldots, f_t$ with a list $g_1, \ldots, g_t$ that is row-reduced in the linear part and has the same number of simultaneous zeroes. So the polynomials g_i have the form

$$g_i(\mathbf{x}) = c_i + \pi^{\epsilon_i} x_i + \pi^{\epsilon_i} L_i(x_{i+1}, \ldots, x_n),$$

where $\epsilon_1 \leq \cdots \leq \epsilon_t \leq \ell$, each L_i is homogeneous of degree 1, and each c_i is a constant in R. If $c_i \not\equiv 0 \pmod{\pi^{\epsilon_i}}$ for any i, then there is no solution to the system and our claim is proved. Otherwise, select $\gamma_i \in R$ so that $c_i = \pi^{\epsilon_i}\gamma_i$, and note that solving $g_1(\mathbf{x}) = \cdots = g_t(\mathbf{x}) = 0$ is tantamount to simultaneously solving

$$\gamma_i + x_i + L_i(x_{i+1}, \ldots, x_n) \equiv 0 \pmod{\pi^{\ell - \epsilon_i}}$$

for $i = 1, \ldots, t$. The solutions to this system are found by setting $x_{t+1}, \ldots, x_n$ arbitrarily and then setting x_t, x_{t-1} and so on until at last we set x_1. Each such x_i is determined modulo $\pi^{\ell-\epsilon_i}$, and so ranges over a set of q^{ϵ_i} values. So the total number of solutions is $q^{\ell(n-t)+\epsilon_t+\epsilon_{t-1}+\cdots+\epsilon_1}$. □

Now we need to count zeroes when one or more of the polynomials is quadratic or of higher degree. First we consider a very special case wherein the quadratic and higher degree terms of the polynomials are π-adically small when compared with the linear terms.

Lemma 3.3. *Let $\ell \geq 1$ and $n \geq t$, and suppose that $f_1, \ldots, f_t \in R[x_1, \ldots, x_n]$ such that for each i*

$$f_i(\mathbf{x}) = c_i + x_i + L_i(x_{i+1}, \ldots, x_n) + \pi Q_i(\mathbf{x}),$$

where $c_i \in R$, $L_i \in R[x_{i+1}, \ldots, x_n]$ is homogeneous of degree 1 and Q_i has no terms of degree less than 2. Then $N\left(f_1, \ldots, f_t; R/(\pi^j)\right) = q^{(n-t)j}$ for $j = 1, \ldots, \ell$.

Proof. We induct on j. For $j = 1$, we are solving $c_i + x_i + L_i(x_{i+1}, \ldots, x_n) \equiv 0 \pmod{\pi}$ for all $i \in \{1, \ldots, t\}$, so that we may set $x_{t+1}, \ldots, x_n$ to whatever values we want, but then $x_t, x_{t-1}, \ldots, x_1$ must take unique values modulo π. So $N\left(f_1, \ldots, f_t; R/(\pi)\right) = q^{n-t}$.

Now suppose that $j > 1$ and that $N\left(f_1, \ldots, f_t; R/(\pi^{j-1})\right) = q^{(n-t)(j-1)}$. For each solution modulo π^{j-1} (call it $\mathbf{b}$), we count distinct $\mathbf{y}$ modulo π that make $\mathbf{b} + \pi^{j-1}\mathbf{y}$ solve our system modulo π^j. Note that

$$f_i(\mathbf{b} + \pi^{j-1}\mathbf{y}) \equiv f_i(\mathbf{b}) + \pi^{j-1} y_i + \pi^{j-1} L_i(y_{i+1}, \ldots, y_n) \pmod{\pi^j}.$$

Since $f_i(\mathbf{b}) \equiv 0 \pmod{\pi^{j-1}}$, we can write it as $\pi^{j-1}\alpha_i$ for some $\alpha_i \in R$, and we are essentially solving

$$\alpha_i + y_i + L_i(y_{i+1}, \ldots, y_n) \equiv 0 \pmod{\pi},$$

so that we may set $y_{t+1}, \dots, y_n$ to whatever we wish, but then $y_t, y_{t-1}, \dots, y_1$ are uniquely determined modulo π. So the number of distinct solutions modulo π^j for our system is $q^{n-t}N\left(f_1, \dots, f_t; R/(\pi^{j-1})\right) = q^{(n-t)j}$. □

Now we are ready to prove Proposition 3.1. We start by proving that the greatest common divisors are at least as large as stated there. When $n \leq T$ there is nothing to prove in this regard, so we consider only the case when $n > T$. If any polynomial is a nonzero constant (or if they are all zero constants), then $N(f_1, \dots, f_t; R) = 0$ (or $q^{n\ell}$), which is certainly divisible by what we claim to be the divisor in our proposition. If some polynomials are nonconstant and the rest are zero constants, then we may strike the zero polynomials off our list to obtain a smaller list of polynomials determining the same algebraic set and the same exponents in the statement of our proposition. So we may also assume that all d_i are nonzero, i.e., that $T = t$. If $d_1 = \cdots = d_t = 1$, then we may invoke Lemma 3.2 to obtain the requisite divisor. Therefore, to prove that the divisors are at least as great as stated in Proposition 3.1, it suffices to demonstrate the following reduction.

Lemma 3.4. *Let $\ell > 1$, let $n > t$, and let $f_1, \dots, f_t$ be nonconstant polynomials. Then $q^{\left\lfloor \frac{(n-t+1)\ell-1}{2} \right\rfloor} \mid N(f_1, \dots, f_t; R)$.*

Proof. We induct on ℓ. We group the zeroes of our system into equivalence classes modulo π (called *π-classes*) and show that the cardinality of each π-class is divisible by $q^{\left\lfloor \frac{(n-t+1)\ell-1}{2} \right\rfloor}$. Let $\mathbf{a}$ be a zero of our system, so that

$$f_i(\mathbf{a} + \pi\mathbf{x}) = \pi f_{i,1}(\mathbf{x}) + \pi^2 f_{i,2}(\mathbf{x}) + \pi^3 f_{i,3}(\mathbf{x}) + \cdots$$

for each i, where $f_{i,j}$ is homogeneous of degree j. Set

$$g_i(\mathbf{x}) = f_{i,1}(\mathbf{x}) + \pi f_{i,2}(\mathbf{x}) + \pi^2 f_{i,3}(\mathbf{x}) + \cdots$$

for each i. Note that the size of the π-class of $\mathbf{a}$ is precisely $N\left(g_1, \dots, g_t; R/(\pi^{\ell-1})\right)$, so that it will suffice for us to show that $q^{\left\lfloor \frac{(n-t+1)\ell-1}{2} \right\rfloor} \mid N\left(g_1, \dots, g_t; R/(\pi^{\ell-1})\right)$.

Use the row operations of Section 2 on $g_1, \dots, g_t$ with variable reindexing to obtain a list of polynomials $h_1, \dots, h_t$ that is row-reduced in the linear part and has the same number of distinct zeroes in $R/(\pi^{\ell-1})$. There is some $k \in \{0, 1, \dots, t\}$ such that for $i \leq k$, we have

$$h_i(\mathbf{x}) = x_i + h_{i,1}(x_{k+1}, \dots, x_n) + \pi h_{i,2}(\mathbf{x}) + \pi^2 h_{i,3}(\mathbf{x}) + \cdots,$$

and for $i > k$, we have

$$h_i(\mathbf{x}) = \pi h_{i,1}(x_{k+1}, \dots, x_n) + \pi h_{i,2}(\mathbf{x}) + \pi^2 h_{i,3}(\mathbf{x}) + \cdots,$$

where each $h_{i,j}$ is a homogeneous polynomial in $R[x_1, \dots, x_n]$ of degree j, and where $h_{i,1}$ does not involve $x_1, \dots, x_k$. Since the row operations with variable reindexing do not change the size of the algebraic set, it suffices for us to show that $q^{\left\lfloor \frac{(n-t+1)\ell-1}{2} \right\rfloor} \mid N\left(h_1, \dots, h_t; R/(\pi^{\ell-1})\right)$.

If $k = t$, then we may use Lemma 3.3 to show that $N\left(h_1, \dots, h_t; R/(\pi^{\ell-1})\right)$ is $q^{(n-t)(\ell-1)}$, and since $(n-t)(\ell-1) \geq \left\lfloor \frac{(n-t+1)\ell-1}{2} \right\rfloor$ (because $n > t$ and $\ell \geq 2$), we are done. So henceforth assume that $k < t$.

For $i > k$, set

$$H_i(\mathbf{x}) = h_{i,1}(x_{k+1}, \dots, x_n) + h_{i,2}(\mathbf{x}) + \pi h_{i,3}(\mathbf{x}) + \cdots.$$

Then $N\left(h_1,\dots,h_t;R/(\pi^{\ell-1})\right)$ is equal to the number of distinct $\mathbf{x}$ modulo $\pi^{\ell-1}$ that satisfy the system

$$h_1(\mathbf{x})\equiv\cdots\equiv h_k(\mathbf{x})\equiv 0 \pmod{\pi^{\ell-1}},$$
$$H_{k+1}(\mathbf{x})\equiv\cdots\equiv H_t(\mathbf{x})\equiv 0 \pmod{\pi^{\ell-2}}. \tag{3.1}$$

There are $N\left(h_1,\dots,h_k,H_{k+1},\dots,H_t;R/(\pi^{\ell-2})\right)$ solutions to the system

$$h_1(\mathbf{x})\equiv h_k(\mathbf{x})\equiv H_{k+1}(\mathbf{x})\equiv\cdots\equiv H_t(\mathbf{x})\equiv 0 \pmod{\pi^{\ell-2}}, \tag{3.2}$$

and for each solution $\mathbf{b}$ to system (3.2), we investigate the $\mathbf{y}\in R^n$ that make $\mathbf{b}+\pi^{\ell-2}\mathbf{y}$ a solution of the mixed system (3.1). Clearly any choice of $\mathbf{y}$ will satisfy the congruences modulo $\pi^{\ell-2}$ in (3.1). If $i\le k$, then

$$h_i(\mathbf{b}+\pi^{\ell-2}\mathbf{y})\equiv h_i(\mathbf{b})+\pi^{\ell-2}y_i+\pi^{\ell-2}h_{i,1}(y_{k+1},\dots,y_n) \pmod{\pi^{\ell-1}};$$

and since $h_i(\mathbf{b})\equiv 0 \pmod{\pi^{\ell-2}}$, we can write it as $\pi^{\ell-2}\eta_i$ for some $\eta_i\in R$, so that we are essentially solving

$$\eta_i+y_i+h_{i,1}(y_{k+1},\dots,y_n)\equiv 0 \pmod{\pi}$$

for $i\le k$. Thus we can set $y_{k+1},\dots,y_n$ to whatever values we want, and there will be unique values modulo π of $y_1,\dots,y_k$ that satisfy these congruences. Thus the number of distinct $\mathbf{y}$ modulo π that make $\mathbf{b}+p\mathbf{y}$ a solution of (3.1) is q^{n-k}. Thus the total number of distinct $\mathbf{x}$ modulo $\pi^{\ell-1}$ that solve (3.1) is q^{n-k} times the number of solutions of system (3.2). That is, $N\left(h_1,\dots,h_t;R/(\pi^{\ell-1})\right)=q^{n-k}N\left(h_1,\dots,h_k,H_{k+1},\dots,H_t;R/(\pi^{\ell-2})\right)$.

If $\ell=2$, then $N\left(h_1,\dots,h_k,H_{k+1},\dots,H_t;R/(\pi^{\ell-2})\right)=1$ trivially, so that we have $N\left(h_1,\dots,h_t;R/(\pi^{\ell-1})\right)=q^{n-k}$, which is greater than $q^{\left\lfloor\frac{(n-t+1)\ell-1}{2}\right\rfloor}$ because $\ell=2$ and $k<t$.

If $\ell=3$, then the $h_i \pmod{\pi}$ with $i\le k$ are all of degree 1 or less and the $H_i \pmod{\pi}$ with $i>k$ are of degree 2 or less. Thus, by the theorem of N. M. Katz (Theorem 1.2), we know that $q^{\left\lceil\frac{n-k-2(t-k)}{2}\right\rceil}\mid N\left(h_1,\dots,h_k,H_{k+1},\dots,H_t;R/(\pi^{\ell-2})\right)$. So $N\left(h_1,\dots,h_t;R/(\pi^{\ell-1})\right)$ is divisible by $q^{n-k+\left\lceil\frac{n-2t+k}{2}\right\rceil}=q^{\left\lfloor\frac{3n-2t-k+1}{2}\right\rfloor}$, which is greater than or equal to $q^{\left\lfloor\frac{(n-t+1)\ell-1}{2}\right\rfloor}$ since $\ell=3$ and $k<t$.

If $\ell>3$, then $q^{\left\lceil\frac{(n-t+1)(\ell-2)-1}{2}\right\rceil}\mid N\left(h_1,\dots,h_k,H_{k+1},\dots,H_t;R/(\pi^{\ell-2})\right)$ by induction. So $N\left(h_1,\dots,h_t;R/(\pi^{\ell-1})\right)$ is divisible by $q^{n-k+\left\lfloor\frac{(n-t+1)(\ell-2)-1}{2}\right\rfloor}$, which is greater than or equal to $q^{\left\lfloor\frac{(n-t+1)\ell-1}{2}\right\rfloor}$ since $k<t$.

So in any case, we know that $q^{\left\lfloor\frac{(n-t+1)\ell-1}{2}\right\rfloor}\mid N\left(h_1,\dots,h_t;R/(\pi^{\ell-1})\right)$. We showed that this suffices to complete the proof. □

We have demonstrated that the greatest common divisors of the cardinalities of algebraic sets are at least as great as claimed in Proposition 3.1. Therefore to complete the proof of that proposition, we need to prove that the greatest common divisors are in fact no greater than what is stated.

We assume the hypotheses of Proposition 3.1, and, without loss of generality, we relabel the d_i so that $0<d_1\le d_2\le\ldots\le d_T$ and $d_{T+1}=\cdots=d_n=0$. If $n\le T$, then we can set $f_i(\mathbf{x})=x_{\min\{i,n\}}(1+\pi x_{\min\{i,n\}}^{d_i-1})$ for $i\le T$ and $f_i(\mathbf{x})=0$ for $i>T$. Then note that the only solution of $f_1(\mathbf{x})=\cdots=f_t(\mathbf{x})=0$ is $\mathbf{x}=(0,0,\dots,0)$, which proves that the greatest common divisor of cardinalities of algebraic sets is 1 if $n\le T$.

Henceforth we assume that $n > T$. For $i < T$, set $f_i(\mathbf{x}) = x_i(1 + \pi x_i^{d_i-1})$, and for $i > T$, set $f_i(\mathbf{x}) = 0$. Then let $f_T(\mathbf{x})$ range over $R[x_T, \ldots, x_n]$ with $\deg(f_T(\mathbf{x})) = d_T$. Solutions to $f_1(\mathbf{x}) = \cdots = f_t(\mathbf{x}) = 0$ are precisely those elements of R^n of the form $(0, 0, \ldots, 0, x_T, x_{T+1}, \ldots, x_n)$ with $f_T(x_T, \ldots, x_n) = 0$. Thus the number of solutions in R^n to our system is equal to the number of solutions in R^{n-T+1} of the single equation $f_T(x_T, \ldots, x_n) = 0$. By the theorem of Marshall and Ramage (Theorem 1.5), the greatest common divisor of cardinalities of sets of solutions in R^{n-T+1} of $f_T(x_T, \ldots, x_n) = 0$ is $q^{\left\lfloor \frac{(n-T+1)\ell-1}{2} \right\rfloor}$ if $d_T > 1$ or $q^{(n-T)\ell}$ if $d_T = 1$. Thus these are upper bounds (in their respective cases) of $D(d_1, \ldots, d_t; R)$. Since $d_T = 1$ if and only if all $d_i \leq 1$, we have the upper bounds we need to complete the proof of Proposition 3.1, which in turn completes the proof of Theorem 1.6.

Acknowledgements

The author thanks Matthew Gealy for helpful discussions. He also thanks an anonymous referee for enriching the paper by asking the question addressed by Example 1.9.

References

1. Alan Adolphson and Steven Sperber, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning*, Ann. Sci. École Norm. Sup. (4) **20** (1987), no. 4, 545–556. MR932797 (89d:11112)
2. M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802 (39:4129)
3. James Ax, *Zeroes of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261. MR0160775 (28:3986)
4. Wei Cao and Qi Sun, *A reduction for counting the number of zeros of general diagonal equation over finite fields*, Finite Fields Appl. **12** (2006), no. 4, 681–692. MR2257089 (2007f:11033)
5. ———, *Improvements upon the Chevalley-Warning-Ax-Katz-type estimates*, J. Number Theory **122** (2007), no. 1, 135–141. MR2287115
6. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75.
7. Pedro L. del Angel R., *A remark on the Hodge type of projective varieties of low degree*, J. Reine Angew. Math. **449** (1994), 173–177. MR1268584 (95b:14004)
8. Jean-René Joly, *Nombre de solutions de certaines équations diagonales sur un corps fini*, C. R. Acad. Sci. Paris Sér. A-B **272** (1971), A1549–A1552. MR0282949 (44:183)
9. Daniel J. Katz, *On p-adic estimates of weights in Abelian codes over Galois rings*, Ph.D. thesis, California Institute of Technology, Pasadena, CA, 2005.
10. Nicholas M. Katz, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499. MR0288099 (44:5297)
11. Murray Marshall and Garry Ramage, *Zeros of polynomials over finite principal ideal rings*, Proc. Amer. Math. Soc. **49** (1975), 35–38. MR0360541 (50:12989)
12. Bernard R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker Inc., New York, 1974. MR0354768 (50:7245)
13. O. Moreno and C. J. Moreno, *An elementary proof of a partial improvement to the Ax-Katz theorem*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 257–268. MR1251983 (94k:11039)
14. ———, *Improvements of the Chevalley-Warning and the Ax-Katz theorems*, Amer. J. Math. **117** (1995), no. 1, 241–244. MR1314464 (95j:11116)
15. Oscar Moreno and Francis N. Castro, *Divisibility properties for covering radius of certain cyclic codes*, IEEE Trans. Inform. Theory **49** (2003), no. 12, 3299–3303. MR2045808 (2005d:94215)
16. ———, *Improvement on Ax-Katz's and Moreno-Moreno's theorems with coding theory applications*, Proceedings of IEEE International Symposium on Information Theory, 2003, p. 132.

17. ———, *Improvement of Ax-Katz's and Moreno-Moreno's results and applications*, Int. J. Pure Appl. Math. **19** (2005), no. 2, 259–267. MR2138044
18. Oscar Moreno and Carlos J. Moreno, *The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes*, IEEE Trans. Inform. Theory **40** (1994), no. 6, 1894–1907. MR1322391 (96j:94029)
19. Oscar Moreno, Kenneth W. Shum, Francis N. Castro, and P. Vijay Kumar, *Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications*, Proc. London Math. Soc. (3) **88** (2004), no. 3, 545–564. MR2044049 (2005g:11114)
20. Bernard Morlaye, *Équations diagonales non homogènes sur un corps fini*, C. R. Acad. Sci. Paris Sér. A-B **272** (1971), A1545–A1548. MR0282948 (44:182)
21. Marc Perret, *On the number of points of some varieties over finite fields*, Bull. London Math. Soc. **35** (2003), no. 3, 309–320. MR1960941 (2003m:14036)
22. Debin Ren, Qi Sun, and Pingzhi Yuan, *Number of zeros of diagonal polynomials over finite fields*, Finite Fields Appl. **7** (2001), no. 1, 197–204, dedicated to Professor Chao Ko on the occasion of his 90th birthday. MR1803944 (2001k:11055)
23. Stephen H. Schanuel, *An extension of Chevalley's theorem to congruences modulo prime powers*, J. Number Theory **6** (1974), 284–290. MR0349637 (50:2130)
24. Daqing Wan, *Zeros of diagonal equations over finite fields*, Proc. Amer. Math. Soc. **103** (1988), no. 4, 1049–1052. MR954981 (89i:11138)
25. E. Warning, *Bemerkung zur vorstehenden arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 76–83.
26. Richard M. Wilson, *An Ax–Katz-type theorem for congruences modulo powers of a prime*, J. Number Theory (to appear).

Department of Mathematics, Princeton University, Princeton, New Jersey 08544
E-mail address: katz.daniel.j@gmail.com