Can. J. Math., Vol. XXXVI, No. 2, 1984, pp. 249-262

DIAGONAL EQUATIONS OVER LARGE FINITE FIELDS

CHARLES SMALL

0. Introduction. We consider polynomials of the form

$$f = \sum_{i=1}^{n} a_i X_i^{d_i}$$

with non-zero coefficients a_i in a finite field F. For any finite extension field $K \supseteq F$, let $f_K:K^n \rightarrow K$ be the mapping defined by f. We say f is *universal* over K if f_K is surjective, and f is *isotropic* over K if f_K has a non-trivial "kernel"; the latter means $f_K(x) = 0$ for some $0 \neq x \in K^n$.

We show (Theorem 1) that f is universal over K provided $|K|$ (the cardinality of K) is larger than a certain explicit bound given in terms of the exponents $d_1, \ldots, d_n$. The analogous fact for isotropy is Theorem 2.

It should be noted that in studying diagonal equations

$$\sum_{i=1}^{n} a_i X_i^{d_i} = b$$

we fix both the number of variables n and the exponents d_i, and ask how large the field must be to guarantee a solution. This is in contrast to the usual approach in additive theory, where one asks how large n must be, compared to the d_i, to guarantee solubility independent of the field. (An example is Chevalley's theorem, discussed briefly in 18 and 20 below.)

Theorems of the type given here are known, but usually in qualitative versions asserting simply that any diagonal equation

$$\sum_{i=1}^{n} a_i X_i^{d_i} = b$$

over a finite field K has a solution (and when $b = 0$ a non-trivial solution) provided K is sufficiently large. What seems not to be spelled out anywhere in the literature (although the results, at least in the prime-field case, are well known to the experts) are explicit bounds which answer the question, how large does K have to be to ensure that f is universal, or isotropic, and which apply to arbitrary diagonal equations without any supplementary hypotheses. It is somewhat surprising that such results

Received May 17, 1982 and in revised form January 12, 1983.

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

have escaped explicit notice, since (as we shall see) they are rather easy consequences of well-known estimates related to the so-called Riemann hypothesis for varieties defined over finite fields. For earlier results along these lines see [**13**] particularly Theorem 7, [**2**], [**15**], [**4**], and of course the pioneer work in this area, [**17**].

1. Statement of the main results.

THEOREM 1. *Let $K \supseteq F$ be finite fields and let*

$$f = \sum_{i=1}^{n} a_iX_i^{d_i} \in F[X_1, \ldots, X_n] \quad \textit{with } a_1a_2 \ldots a_n \neq 0.$$

Assume $n \geqq 2$ and for each i put

$$\delta_i = \text{g.c.d.}(d_i, |K| - 1).$$

If

$$|K| > \prod_{i=1}^{n} (\delta_i - 1)^{2/(n-1)}$$

then f is universal over K.

THEOREM 2. *Let K, F, f and δ_i be as in Theorem* 1, *assume $n \geqq 3$, and put $|K| = q$. If*

$$\frac{q^{n-1} - 1}{(q - 1)q^{(n/2)-1}} > \frac{1}{D} \left| \sum_{l=0}^{D-1} \left(\prod_{\delta_i|l} (1 - \delta_i) \right) \right|$$

where $D = \prod_{i=1}^{n} \delta_i$ then f is isotropic over K.

In the right-hand side of the inequality in Theorem 2, the usual conventions apply: $\delta_i|0$ for all i, and empty products are 1. The expression on the left-hand side of the same inequality is asymptotic to $q^{(n/2)-1}$, and therefore (for $n \geqq 3$) goes to ∞ with q. Thus, Theorem 2 does say that f is isotropic over K as soon as $|K|$ is larger than a certain bound given explicitly in terms of the exponents $d_1, \ldots, d_n$ of f, provided $n \geqq 3$.

Since the homogeneous case $d_1 = d_2 = \ldots = d_n = d$, say, is of particular interest, we record the appropriate special cases of Theorems 1 and 2:

COROLLARY 3. *Let $K \supseteq F$ be finite fields with*

$$|K| = q, \quad f = \sum_{i=1}^{n} a_iX_i^{d_i} \in F[X_1, \ldots, X_n]$$

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

with $a_1a_2 \dots a_n \neq 0$, *and put*

$$\delta = \text{g.c.d.}(d, |K| - 1).$$

Then:

(a) *if* $n \geqq 2$ *and* $|K| > (\delta - 1)^{2n/(n-1)}$ *then* f *is universal over* K, *and*
(b) *if* $n \geqq 3$ *and*

$$\frac{q^{n-1} - 1}{(q - 1)q^{(n/2)-1}} > \frac{\delta - 1}{\delta} \left((\delta - 1)^{n-1} + (-1)^n \right)$$

then f *is isotropic over* K.

It is perhaps not immediate (although it is true) that Corollary 3 (b) is a special case of Theorem 2. In Section 2 we indicate a proof of 3 (b) independent of Theorem 2 (see Corollary 10).

Before proceeding to the proofs of Theorems 1 and 2 we indicate some additional corollaries; further consequences and examples are discussed in Section 3 (13 through 21).

COROLLARY 4. *Given a positive integer* d *choose* $n = n(d)$ *large enough to ensure*

$$(d - 1)^{2n/(n-1)} < (d - 1)^2 + 1,$$

and let

$$f = \sum_{i=1}^{n} a_iX_i^d \quad \text{where } 0 \neq a_i \in \mathbf{Q}.$$

Let K *be a finite field with* $|K| > (d - 1)^2$ *and with* $p \nmid a_i \ \forall\, i$, *where* $p =$ char$K$. (*Here* $p \nmid a_i$ *means* p *divides neither numerator nor denominator of* a_i *in lowest terms.*) *Then* f *is universal over* K.

Proof. Since $p =$ char$K$ divides none of the a_i we can read these coefficients as non-zero elements of K. Thus Corollary 3(a) applies, and since $|K| > (d - 1)^2$ implies

$$|K| \geqq (d - 1)^2 + 1 > (d - 1)^{2n/(n-1)} \geqq (\delta - 1)^{2n/(n-1)}$$

where $\delta = \text{g.c.d.}(d, |K| - 1)$ we conclude that f is universal over K.

COROLLARY 5. *Let* d *be a positive integer and* K *a finite field. If* $|K| > (d - 1)^2$ *then every element of* K *is a sum of* d^{th} *powers.*

Proof. Apply Corollary 4 to the case where all the a_i are 1.

A remark at the end of this section shows that $(d - 1)^2$ is best possible in Corollary 5.

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

For any finite field K and positive integer d let $K(d)$ denote the set of all sums of d^{th} powers in K. It is an easy exercise to see that $K(d)$ is a subfield of K and Corollary 5 shows that, for fixed d, $K(d) = K$ except possibly for finitely many K with $|K| \leqq (d - 1)^2$. It is known [**16**] that, whenever $K(d) = K$, every element of K is in fact a sum of δ d^{th} powers where

$$\delta = \text{g.c.d.}(d, |K| - 1) \leqq d.$$

For large finite fields this can be improved:

COROLLARY 6. *Let d be a positive integer and K a finite field. If $|K| > (d - 1)^4$ then every element of K is a sum of two d^{th} powers. More precisely and more generally, if $|K| > (\delta - 1)^4$ where $\delta = \text{g.c.d.}(d, |K| - 1)$ then any $f = a_1X_1^d + a_2X_2^d$, with $0 \neq a_1a_2 \in K$, is universal over K.*

Corollary 6 is just a special case ($n = 2$) of Corollary 3(a). This special case was noted in [**12**] and proved there by a technique which generalizes immediately to prove Theorem 1 as in Section 2 below. Corollary 6 is best possible in the sense that there are arbitrarily large finite fields, for example the prime fields $\mathbf{F}_p$ with $p \equiv 1 \pmod{d}$, in which it is not true that every element is a single d^{th} power; indeed, there are only $(p - 1)/d$ non-zero d^{th} powers in $\mathbf{F}_p$.

The subfield $K(d)$ can easily be characterized in general (compare [**1**]):

PROPOSITION 7. *Let K be a finite field with $|K| = q = p^n$ (p prime, $n \geqq 1$) and let d be a positive integer. Then $|K(d)| = p^m$ where m is the smallest divisor of n such that $(q - 1)/\text{g.c.d.}(d, q - 1)$ divides $p^m - 1$.*

The proof of Proposition 7 is an easy exercise: note that $K(d)$ is characterized as the smallest subfield of K containing the subgroup $\{x^d | 0 \neq x \in K\}$ of the (cyclic) multiplicative group of non-zero elements of K.

It follows from Proposition 7, for example, that with $d = p + 1$ and $|K| = p^2$ we have $K(d) = \mathbf{F}_p \subsetneq K$. Thus in every characteristic, the conclusion of Corollary 5 fails if we have $|K| = (d - 1)^2$ rather than $|K| > (d - 1)^2$.

2. Proofs of theorems 1 and 2.

Consider

$$f = \sum_{i=1}^{n} a_iX_i^{d_i}$$

with $0 \neq a_1a_2 \ldots a_n \in F \subseteq K$ as in the Introduction. For $b \in K$ let $N(b) = |f_K^{-1}(b)| \geqq 0$ be the cardinality of $\{x \in K^n | f(x) = b\}$. Thus $N(b)$ is the "number of times f represents b" over K; f is universal over K if and only if $N(b) > 0 \; \forall \; 0 \neq b \in K$, and f is isotropic over K if and only if $N(0) > 1$.

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

For each $i (1 \leqq i \leqq n)$ put

$$\delta_i = \text{g.c.d.}(d_i, |K| - 1).$$

Since the multiplicative group of K is cyclic of order $|K| - 1$ we have

$$\{x^{d_i} | 0 \neq x \in K\} = \{x^{\delta_i} | 0 \neq x \in K\}.$$

Thus changing the d_i to δ_i changes the mapping $f_K:K^n \to K$ without changing its image; in particular the $N(b)$, $b \in K$, are not affected. It is for this reason that Theorems 1 and 2 are expressed in terms of the δ_i rather than the d_i.

Theorem 1 will follow from the following classical estimate:

PROPOSITION 8. *With $n \geqq 2$ and notation as above we have, for all* $0 \neq b \in K$,

$$|N(b) - q^{n-1}| \leqq \left(\prod_{i=1}^{n} (\delta_i - 1)\right) q^{(n-1)/2}$$

where $q = |K|$.

A proof of Proposition 8, via Gauss and Jacobi sums, can be found in **[6]** where it appears as Corollary 1 on p. 57.

From Proposition 8 we have, for any $0 \neq b \in K$,

$$N(b) - q^{n-1} \geqq - \left(\prod_{i=1}^{n} (\delta_i - 1)\right) q^{(n-1)/2}.$$

Hence

$$N(b) \geqq q^{(n-1)/2}\left(q^{(n-1)/2} - \prod_{i=1}^{n} (\delta_i - 1)\right),$$

and $N(b) > 0$ provided

$$q^{(n-1)/2} > \prod_{i=1}^{n} (\delta_i - 1),$$

which (for $n > 1$) is the same as

$$q > \prod_{i=1}^{n} (\delta_i - 1)^{2/(n-1)}.$$

This proves Theorem 1.

In order to give the analogue of Proposition 8 for $b = 0$ from which Theorem 2 will follow, we need a little more notation. Given integers n and $\delta_1, \ldots, \delta_n$, all $\geqq 2$, put

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

$$\begin{aligned} J &= J(\delta_1, \dots, \delta_n) \\ &= \{j = (j_1, \dots, j_n) \in \mathbf{Z}^n \mid 1 \leqq j_i \leqq \delta_i - 1 \ \forall\, i\}. \end{aligned}$$

For $j = (j_1, \dots j_n) \in J$ define

$$w(j) = \sum_{i=1}^{n} j_i/\delta_i;$$

thus $w{:}J \to \mathbf{Q}$. Put

$$\begin{aligned} I &= I(\delta_1, \dots, \delta_n) = w^{-1}(\mathbf{Z}) \\ &= \{j \in J \mid w(j) \in \mathbf{Z}\}. \end{aligned}$$

I am indebted for the following result to Professor Richard Stanley of M.I.T.

LEMMA 9.

$$|I| = \frac{(-1)^n}{D} \sum_{l=0}^{D-1} \left(\prod_{\delta_k | l} (1 - \delta_k) \right)$$

where $D = \prod_{k=1}^{n} \delta_k$.

Proof. Let ζ be the primitive D^{th} root of unity $e^{2\pi i/D}$ and for each $k = 1, 2, \dots, n$ put $\hat{\delta}_k = D/\delta_k$. For any positive integer t we have

$$(1 - \zeta^t) \sum_{l=0}^{D-1} \zeta^{tl} = 0,$$

so that

$$(*) \quad \sum_{l=0}^{D-1} \zeta^{tl} = \begin{cases} D & \text{if } D \mid t \\ 0 & \text{if } D \nmid t \end{cases}.$$

For $j = (j_1, \dots, j_n) \in J$ we have

$$w(j) = \left(\sum_{k=1}^{n} j_k \hat{\delta}_k \right) / D,$$

hence $j \in I$ if and only if $D | \sum j_k \hat{\delta}_k$, if and only if

$$1 = \zeta^{\Sigma j_k \hat{\delta}_k} = \prod_{k=1}^{n} \zeta^{j_k \hat{\delta}_k}.$$

Thus for $j = (j_1, \dots, j_n) \in I$ we have

$$1 = \frac{1}{D} \sum_{l=0}^{D-1} (\zeta^{\Sigma j_k \hat{\delta}_k})^l.$$

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

For $j = (j_1, \ldots, j_n) \in J, j \notin I$, on the other hand, we have $D \nmid \sum j_k \hat{\delta}_k$, hence (by $(*)$) for such j,

$$0 = \frac{1}{D} \sum_{l=0}^{D-1} (\zeta^{\sum j_k \hat{\delta}_k})^l.$$

Therefore

$$(* *) \quad |I| = \frac{1}{D} \sum_{l=0}^{D-1} \sum (\zeta^{\sum j_k \hat{\delta}_k})^l$$

where the unlabeled sum is over all $j = (j_1, \ldots, j_n) \in J$. The right-hand side of $(* *)$ is just

$$\frac{1}{D} \sum_{l=0}^{D-1} \prod_{k=1}^{n} \sum_{m=1}^{\delta_k - 1} \zeta^{\hat{\delta}_k l m},$$

and since $\zeta^{\hat{\delta}_k}$ is a primitive δ_k^{th} root of unity, we can use the analog of $(*)$ to evaluate the inmost sum:

$$\sum_{m=1}^{\delta_k - 1} \zeta^{\hat{\delta}_k l m} = \delta_k - 1 \text{ if } \delta_k | l, \ -1 \text{ if } \delta_k \nmid l.$$

Hence, if we let $\mu(l)$ be the number of k for which $\delta_k \nmid l$, we get from $(* *)$:

$$|I| = \frac{1}{D} \sum_{l=0}^{D-1} (-1)^{\mu(l)} \prod_{\delta_k | l} (\delta_k - 1),$$

which is clearly the same as the result as stated.

COROLLARY 10. *In the homogeneous case,* $\delta_1 = \delta_2 = \ldots = \delta_n = \delta$, *we have*

$$|I| = |I(\delta, \ldots, \delta)| = \frac{\delta - 1}{\delta} \left((\delta - 1)^{n-1} + (-1)^n \right).$$

Proof. This can be extracted from Lemma 9 as a special case. It can also be proved by induction on n; see **[10]**, Lemma 6D, p. 169.

The analogue of Proposition 8 for $b = 0$ is:

PROPOSITION 11. *With notation as above* ($f = \sum_{i=1}^{n} a_i X_i^{d_i}$, $n \geqq 2$, $0 \neq a_1 a_2 \ldots a_n \in F \subseteq K$, $|K| = q$, $\delta_i = \text{g.c.d.}(d_i, q - 1)$) *we have*

$$|N(0) - q^{n-1}| \leqq |I| (q - 1) q^{(n/2)-1}$$

where $I = I(\delta_1, \ldots, \delta_n)$

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

A proof of Proposition 11 can be found in [**6**] where it appears as Corollary 1 on page 54.

COROLLARY 12. *With notation as in Proposition* 11 *we have*

$$\text{(a)}\quad |N(0) - q^{n-1}| \leqq \frac{1}{D}\left|\sum_{k=0}^{D-1}\left(\prod_{\delta_i|k}(1-\delta_i)\right)\right|(q-1)q^{(n/2)-1}$$

where $D = \prod_{i=1}^n \delta_i$

$$\text{(b)}\quad |N(0) - q^{n-1}| \leqq \frac{\delta-1}{\delta}\left((\delta-1)^{n-1} + (-1)^n\right)(q-1)q^{(n/2)-1}$$

in the homogeneous case $\delta_1 = \delta_2 = \ldots = \delta_n = \delta$ *and*

(c) $N(0) = q^{n-1}$ *in the "antihomogeneous" case where one of the* δ_i *is relatively prime to all the others.*

Proof. For (a) and (b), combine Proposition 11 with Lemma 9 and Corollary 10 respectively. Part (c) follows from Proposition 11 and the fact, noted in [**6**] and easily verified, that I is empty in the antihomogeneous case.

We can now prove Theorem 2. From Proposition 11 we have

$$N(0) - q^{n-1} \geqq -|I|(q-1)q^{(n/2)-1},$$

so that $N(0) > 1$ provided

$$q^{n-1} - |I|(q-1)q^{(n/2)-1} > 1,$$

that is,

$$\frac{q^{n-1}-1}{(q-1)q^{(n/2)-1}} > |I|.$$

Using Lemma 9 to evaluate $|I|$ we get Theorem 2, since f is isotropic if and only if $N(0) > 1$.

Note that the parameter $|I| = |I(\delta_1, \ldots, \delta_n)|$ which intervenes in the above results can be interpreted as the degree of the numerator of the zeta function of

$$f = \sum_{i=1}^n a_i X_i^{d_i};$$

see [**7**], Corollary 2.

3. Examples and remarks.

13. From Corollary 10 we see that for $\delta = 2$ and n odd,

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

$$|I(\delta, \dots, \delta)| = 0.$$

It then follows from Proposition 11 that when n is odd the equation

$$\sum_{i=1}^{n} a_iX_i^2 = 0$$

has exactly $|K|^{n-1}$ solutions in any finite field K. In particular, we recover the familiar fact that $a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ is isotropic over any finite field (see [**11**], Corollary 2 of I.2.2). From Corollary 3(a) we recover the (equivalent) fact that $a_1X_1^2 + a_2X_2^2$ is always universal.

14. Theorem 2, stated for $n \geqq 3$, is true (by the same proof) for $n = 2$ as well, but it collapses in this case to the statement that $a_1X_1^{d_1} + a_2X_2^{d_2}$ is isotropic over K when $I = I(\delta_1, \delta_2)$ is empty, since

$$\frac{q^{n-1} - 1}{(q - 1)q^{(n/2)-1}} = 1 \quad \text{when } n = 2.$$

This is weak since Proposition 11 implies $N(0) = q^{n-1}$ whenever I is empty. The statement "$\sum_{i=1}^{n} a_iX_i^{d_i}$ is isotropic over all sufficiently large finite fields", true for $n \geqq 3$ by Theorem 2, is in fact false for $n = 2$. (Example: $X_1^2 + X_2^2$ is isotropic over K if and only if -1 is a square in K, if and only if $|K| \equiv 1 \pmod 4$, so there are arbitrarily large finite prime fields $\mathbf{F}_p$ over which $X_1^2 + X_2^2$ is isotropic and arbitrarily large finite prime fields $\mathbf{F}_p$ over which it is not.)

15. The homogeneous example $f = a_1X_1^4 + a_2X_2^4 + a_3X_3^4$ is considered in detail in [**9**]. Corollary 3(a) guarantees f is universal over any finite field with more than 27 elements, and Corollary 3(b) guarantees f is isotropic over K if $|K| = q$ satisfies $(q + 1)/\sqrt{q} > 6$. The smallest integer q satisfying this inequality is 34, and since q must be a prime power we conclude f is isotropic except possibly for $q \leqq 32$. However if $q \not\equiv 1 \pmod 4$, f is equivalent to either $a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ or $a_1X_1 + a_2X_2 + a_3X_3$ (replace $d = 4$ by $\delta = \text{g.c.d.}(4, q - 1)$), both of which (as we have already seen) are isotropic over any finite field.

Thus $a_1X_1^4 + a_2X_2^4 + a_3X_3^4$ is isotropic over all finite fields with more than 29 elements. For this particular example ($n = 3$, $d = 4$) the result thus obtained by Corollary 3(b) is best possible, since $X_1^4 + X_2^4 + X_3^4$ is anisotropic over $\mathbf{F}_{29}$.

16. One application of theorems of the type discussed here, on diagonal equations over finite fields, is to similar equations over $\mathfrak{p}$-adic fields, for a basic technique in studying $\mathfrak{p}$-adic fields is to use tools like Hensel's lemma to lift information from the (finite) residue class fields. In [**3**], for

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

example, the ternary form $f = ax^d + by^d + cz^d$ is considered, where a, b, c are non-zero elements in the field with q elements, and [**17**] is cited for the fact that f is isotropic provided $q > d^4$. Applying Corollary 3(b) we see that in fact f is isotropic provided

$$\frac{q^2 - 1}{(q - 1)q^{1/2}} > \frac{d - 1}{d}\left((d - 1)^2 - 1\right),$$

which amounts to

$$\frac{q + 1}{\sqrt{q}} > (d - 1)(d - 2).$$

Putting $m = (d - 1)(d - 2)$ and applying the quadratic formula we conclude f is isotropic provided

$$q > \phi(d) = \frac{m^2 + m\sqrt{m^2 - 4}}{2} - 1.$$

This is a clumsier criterion to write down than $q > d^4$, but it does give significantly lower estimates. Indeed, for large d (hence large m), $\sqrt{m^2 - 4}$ is roughly m, so that $\phi(d)$ is roughly $m^2 - 1$, or $d^4 - 6d^3 + 13d^2 - 12d + 3$, and

$$\lim_{d \to \infty} (d^4 - \phi(d)) = \infty$$

(like $6d^3$).

17. Let

$$f = \sum_{i=1}^{n} a_i X_i^{d_i}, \quad 0 \neq a_1 a_2 \ldots a_n \in F \subseteq K,$$

$$|K| = q,\ n \geqq 2, \text{ and } \delta_i = \text{g.c.d.}(d_i, q - 1),$$

as above. If any two of the δ_i are relatively prime then f is isotropic over K. In particular, if any two of the d_i are relatively prime then f is isotropic over every finite field containing F. To see this, assume without loss of

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

generality that g.c.d.$(\delta_1, \delta_2) = 1$. Then by Corollary 12 (c) we have that $a_1X_1^{d_1} + a_2X_2^{d_2}$ has exactly q zeros in K, and in particular is isotropic; but then so is f.

18. A famous theorem of Chevalley (see [**5**, 10 Section 2] or [**11**, I, 2.2]) asserts that $\sum_{i=1}^n a_iX_i^{d_i} (0 \neq a_1 a_2 \dots a_n \in F)$ is isotropic over every finite field K containing F provided $n > \max d_i$. In [**14**] the homogeneous case is improved as follows: with exactly one exception ($|K| = p$ prime and $d = p - 1$), $\sum_{i=1}^n a_iX_i^d$ is isotropic over every finite field $K \supseteq F$ provided $n \geqq (d + 3)/2$. Thus for a fixed positive integer d, if we leave aside the one exceptional case noted above, the largest n for which an anisotropic form $\sum_{i=1}^n a_iX_i^d$ can exist is $n = \left[\frac{d+2}{2}\right]$. This explains for example why, when $d = 4$, the case $n = 3$ is the one of interest (cf. 15 above); in general the interesting case for isotropy of $f = \sum_{i=1}^n a_iX_i^d$ is $n = \left[\frac{d+2}{2}\right]$. Moreover, this form f is of interest primarily over fields K with $|K| \equiv 1 \pmod{d}$, for over a field K not satisfying this congruence, f is equivalent to a form $\sum_{i=1}^n a_iX_i^\delta$ with smaller exponent

$$\delta = \text{g.c.d.}(d, |K| - 1).$$

Now Corollary 3(b) gives a criterion (provided $d \geqq 4$) for f to be isotropic, and shows that if f fails to be isotropic over a field K then $|K| = q$ must satisfy

$$(*) \quad \frac{q^{\left[\frac{d}{2}\right]} - 1}{(q-1)q^{\left[\frac{d-2}{2}\right]/2}} \leqq \frac{d-1}{d}\left((d-1)^{\left[\frac{d}{2}\right]} - (-1)^{\left[\frac{d}{2}\right]}\right).$$

We are thus led to the following question: Given $d > 4$, let q be the largest prime power satisfying $(*)$ and $q \equiv 1 \pmod{d}$, and put $n = \left[\frac{d+2}{2}\right]$. Is there an anisotropic form $\sum_{i=1}^n a_iX_i^d$ over $\mathbf{F}_q$? (For $d = 4$ we have $q = 29$ and $n = 3$, and the answer is yes: see 15 above.)

This is a precise formulation of the question whether the bound given in Corollary 3(b) is best possible in general. Note that the left side of the inequality (*) is asymptotic to

$$q^{\left[\frac{d-2}{2}\right]/2}$$

and the right side is very nearly

$$\frac{(d-1)^{\left[\frac{d+2}{2}\right]}}{d},$$

so that the size q of the field of interest in this question is approximately

$$\left(\frac{(d-1)^n}{d}\right)^{2/(n-2)} \quad \text{where } n = \left[\frac{d+2}{2}\right].$$

For example $d = 12$ gives $n = 7$ and $q \cong 305$.

19. An amusing example arises when we consider $f = \sum_{i=1}^n a_iX_i^d$ over fields K with $q = |K|$ satisfying $(q - 1)|d$. Since $x^d = 1$ for all $0 \neq x \in K$, the mapping $f_K:K^n \to K$ defined by f can be defined as follows: let $\mathbf{a} = (a_1, \ldots, a_n)$ be the vector of coefficients of f, and for each $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ define the "reduction" $\mathbf{x}'$ of $\mathbf{x}$ by $\mathbf{x}' = (x_1', \ldots, x_n')$ with $\mathrm{x}_\mathrm{i}' = 0$ when $x_i = 0$, $x_i' = 1$ when $x_i \neq 0$. Then $f_K(\mathbf{x})$ is the inner product

$$\mathbf{a} \cdot \mathbf{x}' = \sum_{i=1}^n a_ix_i'.$$

Thus f is isotropic if and only if

$$\sum_{i\in T} a_i = 0$$

for some non-empty subset T of $\{1, \ldots, n\}$. Also f represents a non-zero element b if and only if

$$\sum_{i\in T(b)} a_i = b$$

for some subset $T(b)$ of $\{1, \ldots, n\}$, and f is universal if and only if there is such a subset $T(b)$ for each $0 \neq b \in K$.

In one special case it happens that all non-trivial forms $\sum_{i=1}^n a_iX_i^{d_i}$ are of the type just discussed, namely when $q - 1$ is a prime p. (Of course, this forces q to be 3 or a power of 2, and characterizing such q is a notorious unsolved problem.) In this case $q - 1 = p$, given any form $\sum_{i=1}^n a_iX_i^{d_i}$ and setting

$$\delta_i = \text{g.c.d.}(d_i, q - 1)$$

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

as usual, we have (for each i) either $\delta_i = 1$ or $\delta_i = p$. If $\delta_i = 1$ for some i things are trivial, and if $\delta_i = p$ for all i we are in the "geometric" (or "combinatorial") situation described above.

20. A variant of Chevalley's theorem due to Morlaye [**8**] is perhaps worth mentioning here as it seems not to be widely known:

$$f = \sum_{i=1}^{n} a_i X_i^{d_i}$$

is both universal and isotropic (over all finite fields K containing the coefficients a_i) provided

$$\sum_{i=1}^{n} 1/d_i > 1;$$

in fact for any $b \in K$ the number of solutions in K^n to $f = b$ is divisible by char$K$. In the homogeneous case this is precisely Chevalley's theorem but in non-homogeneous situations it is sometimes stronger: for example $X_1^2 + X_2^4 + X_3^6 + X_4^6$ is universal and isotropic (over all finite fields) by Morlaye's Theorem, but Chevalley's Theorem doesn't apply since $n = 4 < 6 = \max d_i$.

21. In general, universality and isotropy are independent notions, as the following simple examples show: over $\mathbf{F}_7$, $X_1^3 - X_2^3$ is isotropic but not universal; $X_1^2 + 2X_2^2$ is universal but not isotropic; $X_1^2 - X_2^2$ is both; X_1^2 is neither. There are nonetheless some obvious connections: if

$$f = \sum_{i=1}^{n} a_i X_i^{d_i}$$

is universal then

$$f + bX_{n+1}^{d_{n+1}}$$

is isotropic for any $b \neq 0$; if

$$f = \sum_{i=1}^{n} a_i X_i^{d}$$

and $f + bX_{n+1}^d$ is isotropic then either f represents $-b$ or f is itself isotropic; etc. For specific equations, observations of this type occasionally permit use of Theorem 1 (about universality) to derive a result about isotropy which is stronger than what one would get from Theorem 2, and similarly in the other direction.

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press

References

1. D. Anderson, Problem 6201, Amer. Math. Monthly *85* (1978), 203 and *86* (1979), 869-870.
2. M. M. Dodson, *Homogeneous additive congruences*, Phil. Trans. Roy. Soc. A *261* (1967), 163-210.
3. ——— *Some estimates for diagonal equations over p-adic fields*, Acta Arith. *40* (1982), 117-124.
4. L. K. Hua and H. S. Vandiver, *On the existence of solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. *34* (1948), 258-263.
5. K. Ireland and M. Rosen, *Elements of number theory* (Bogden and Quigley, 1972).
6. J.-R. Joly, *Equations et variétés algébriques sur un corps fini*, Ens. Math. *19* (1973), 1-117.
7. ——— *Nombre de solutions de certaines equations diagonales sur un corps fini*, C. R. Acad. Sci. Paris *272* (1971), 1549-1552.
8. B. Morlaye, *Equations diagonales non homogènes sur un corps fini*, C. R. Acad. Sci. Paris *272* (1971), 1545-1548.
9. M. Orzech, *Forms of low degree and sums of d^{th} powers in finite fields*, preprint.
10. W. M. Schmidt, *Equations over finite fields an elementary approach*, Springer Lecture Notes *536* (1976).
11. J.-P. Serre, *A course in arithmetic* (Springer, 1973).
12. C. Small, *Sums of powers in large finite fields*, Proc. A. M. S. *65* (1977), 35-36.
13. A. Tietäväinen, *On the non-trivial solvability of some equations and systems of equations in finite fields*, Ann. Acad. Sci. Fenn. Ser. A, I. *360* (1965), 1-38.

    ——— *On diagonal forms over finite fields*, Ann. Univ. Turku, Ser. A I *118* (1968).

14.
15. ——— *Note on Waring's problem* (mod p), Ann. Acad. Sci. Fenn. A I *554* (1973).
16. L. Tornheim, *Sums of n^{th} powers in fields of prime characteristic*, Duke Math. J. *4* (1938), 359-362.
17. A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. *55* (1949), 497-508.

Queen's University,
Kingston, Ontario

https://doi.org/10.4153/CJM-1984-016-6 Published online by Cambridge University Press