BULL. AUSTRAL. MATH. SOC. 12C05
VOL. 29(1984), 45-58.

# FORMS OF LOW DEGREE IN FINITE FIELDS

MORRIS ORZECH

It is known that diagonal forms over a finite field have non-trivial zeros if the number of variables, or the size of the field, is large enough. We consider diagonal forms of degree up to five in cases where the size hypotheses are not satisfied. There are finitely many fields not covered by the known results, but a direct computational test of all possible equations is impractical. We describe means of cutting down considerably on the number of fields and the number of equations for which there exist diagonal forms, of degree up to 5 and in 3 variables, with no non-trivial zero.

The study of equations over finite fields, of whether they have solutions, and how many, can be appealing because the questions asked are easy to understand, and conjectures can be vetted by direct computation. An example of a result that has come to be widely known because it is striking, yet elementary to prove is the theorem of Chevalley which states that in a finite field $F$ any equation

$$a_1X_1^d + a_2X_2^d + \ldots + a_nX_n^d = 0 , \quad n > 1 \tag{1}$$

with $a_1, \ldots, a_n$ in $F$ has a solution $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$

Received 23 January 1984. Research supported by NSERC.

provided $n > d$. But what happens if $n \leq d$? Most readers will have seen the remark that for $F_p$ the prime field with $p$ elements the equation

$$x_1^{p-1} + x_2^{p-1} + \ldots + x_{p-1}^{p-1} = 0 \tag{2}$$

cannot have a nontrivial solution in $F_p$ since $b^{p-1} = 1$ for any nonzero $b$ in $F_p$. Though this example shows that the condition $n > d$ cannot be simply dropped in the statement of Chevalley's theorem, it does not indicate whether a weaker condition might suffice. Indeed, an equation seemingly worse than (2) in that the number of variables is strictly less than the degree, namely

$$a_1x_1^p + a_2x_2^p + \ldots + a_{p-1}x_{p-1}^p = 0 \tag{3}$$

has a solution for any $a_1, \ldots, a_{p-1}$ in $F$ as long as $p$ is an odd prime greater than three, and not necessarily equal to the characteristic of $F$. This fact is a special case of a result proved by Gray ([1], Theorem A), and we will indicate later why it is true.

There are other results which provide conditions under which equations such as (1) have solutions even if $n \leq d$. The kind of result we will focus on is that which guarantees that (1) has a solution provided the field $F$ is large enough. Although we will for the reader's information mention facts relating to fairly general and standard equations, our attitude towards these equations will not be the usual one. Rather than dismiss a question once it has been reduced to a computational one, we will persist in answering it completely. It turns out that the computations needed for a complete answer can seem daunting even in special cases because of the many equations to be tested. This leads us to examine ways of reducing to a set of computations which we can implement. The situation in which we will provide a complete answer as to for which $F$ equation (1) always has a nontrivial solution is that where $n = 3$ and $d \leq 5$. Where less is to be lost in simplicity than is to be gained from a more general perspective, we will treat equation (1) without restricting $n$ or $d$.

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

## 1. Notation and basic reductions

Throughout our discussion $F$ will be a finite field with $q$ elements. We will write $F^*$ for the set of nonzero elements of $F$ and $F^d$, $d$ a positive integer, for the set of nonzero elements of the form $x^d$. A solution $(x_1,\dots,x_n)$ to (1) will be called nontrivial if at least one $x_i$ is nonzero. When we refer to a solution of (1) we will assume it is nontrivial unless we specifically say otherwise. It is obvious that if any $a_i$ is zero then (1) has a solution, hence we will also assume all $a_i$ are nonzero. It will then make sense to refer to the coset $a_iF^d$ of $F^d$ in $F^*$ without explicitly writing $a_i \neq 0$. The fundamental way in which the cosets of $F^d$ in $F^*$ play a role is summarized in the next statement, whose proof is immediate:

(1.1) Whether equation (1) has a solution depends only on the cosets $a_iF^d$, and not on the $a_i$ themselves.

Now let $\delta = gcd(q-1,d)$. It is easy to see that $F^d = F^\delta$ and that $\delta$ is the minimum positive integer $s$ for which $F^d = F^s$. Let $U_d$ denote the group of $d$th roots of unity in $F^*$. Since $\delta$ divides $q-1$ there is a primitive $\delta$th root of unity in $F^*$ and we have $U_d = U_\delta$ and $|U_d| = \delta$, where $|S|$ denotes the cardinality of the set $S$. The group homomorphism $x \to x^d$ of $F^*$ to itself therefore has kernel of order $\delta$ and it follows that $|F^d| = (q-1)/\delta$. For convenient reference we record these observations below.

(1.2) Let $\delta = gcd(q-1,d)$. Then $F^d = F^\delta$, $U_d = U_\delta$, $|U_d| = \delta$, $|F^d| = (q-1)/\delta$ and $[F:F^d] = \delta$.

We will now introduce a clever device used by Lewis [5] to show that equation (1) has a solution for $d = n = 3$ and extended by Gray [1] to a more general setting. Let $W$ be the set of elements of $F^*$ of the form $x^d-1$, $x$ in $F^*$. By (1.2) $F^d$ has $(q-1)/\delta$ elements, and $W$ has one element less than $F^d$, since zero is certainly of the form $x^d-1$ but is not in $W$. Hence $|W| = -1+(q-1)/\delta$. Then

$$|W \cup F^d \cup W^{-1}| \leq -3+3(q-1)/\delta ,$$

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

where $W^{-1} = \{x^{-1} \mid x \text{ in } W\}$. If $\delta \geq 3$ we have that

$$|W \cup F^d \cup W^{-1}| < q-1 ,$$

so there exists $b$ in $F^*$ not in $W \cup F^d \cup W^{-1}$. It follows that:

(1.3) For $\delta \geq 3$ there exists $b$ in $F^*$ such that the cosets $F^d$, $bF^d$, $(1+b)F^d$ are distinct.

With this at hand, we will show how to analyze equation (3).

THEOREM 1.4. *Suppose $d \geq 4$ and $-1 \in F^d$ (i.e. $char(F) = 2$ or $2\delta \mid (q-1)$). Then any equation*

$$a_1X_1^d + a_2X_2^d + \ldots + a_{d-1}X_{d-1}^d = 0 \tag{4}$$

*has a solution in $F$.*

Proof. If two of the cosets $a_iF^d$ are equal then (1.1) and the hypothesis that $-1$ is a dth power imply that equation (4) has a solution. We therefore assume the cosets $a_1F^d$, ..., $a_{d-1}F^d$ are distinct. Then $[F^* : F^d] \geq d-1$, hence by (1.2) we have $\delta \geq d-1$, and since $\delta$ divides $d$ we must have $\delta = d$.

Let $\zeta$ be a generator of the cyclic group $F^*$. Then the cosets $F^d$, $\zeta F^d$, ..., $\zeta^{d-1}F^d$ are distinct, and must be <u>all</u> the cosets of $F^d$ in $F^*$. By (1.2) we may assume each $a_i$ is in the set $\{1, \zeta, \ldots, \zeta^{d-1}\}$. Since the $a_i$ are distinct, precisely one coset $\zeta^iF^d$, $i = 0, \ldots, d-1$ is missing among the $a_iF^d$. Suppose for example that $\zeta^{d-1}F^d$ is the missing coset, so that equation (4) may be replaced by

$$X_1 + \zeta X_2^d + \ldots + \zeta^{d-2}X_{d-1}^d = 0 .$$

This equation has a solution if and only if that obtained in multiplying by $\zeta$ has a solution. But multiplying by $\zeta$ results in an equation which has a solution if and only if

$$\zeta X_1^d + \zeta^2 X_2^d + \ldots + \zeta^{d-1}X_{d-1}^d = 0$$

has a solution. Here $\zeta^dF^d = F^d$ is the missing coset. Successive

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

multiplications by $\zeta$ lead to equations exhausting all possibilities as to which coset of $F^d$ is not represented among the $a_i F^d$.

Now use (1.3) to obtain $b$ such that $F^d$, $bF^d$, $(1+b)F^d$ are distinct cosets. Since $d \geq 4$ there exists $i$ with $0 \leq i \leq d-1$ such that $\zeta^i F^d$ is distinct from the cosets $F^d$, $bF^d$, $(1+b)F^d$. Our comments above clearly imply that after suitable renumbering of the $X_i$ and $a_i$ we may assume equation (4) is of the form

$$X_1^d + bX_2^d + (1+b)X_3^d + a_4X_4^d + \ldots + a_{d-1}X_{d-1}^d = 0 .$$

Since $-1$ is in $F^d$ this equation has a solution with $X_1 = X_2 = 1$, hence (4) has a solution. This proves Theorem 1.4.

There are variants of Theorem 1.4 in which stronger hypothesis leads to better conclusions. For example, if $d$ is an odd prime the equation

$$a_1X_1^d + a_2X_2^d + \ldots + a_sX_{d-t}^d = 0$$

has a solution whenever $t \leq [2(d+2)^{\frac{1}{2}}]-4$, where $[m]$ is the largest integer less than or equal to $m$. For $d$ not necessarily prime, with $-1$ in $F^d$, and $d$ sufficiently large, the same equation has a solution if $t \leq d-1\log_2 d^2$. The methods involved in proving these results are more sophisticated than ours. The interested reader is referred to [1] and [9].

## 2. Reduction to a computational problem

Our original equation (1) is the homogeneous case of the more general diagonal equation

(5) $$a_1X_1^{d_1} + a_2X_2^{d_2} + \ldots + a_nX_n^{d_n} = 0 .$$

Weil [10] used standard and fairly elementary facts involving Gauss and Jacobi sums to provide an estimate for $N$, the number of solutions $(x_1, \ldots, x_n)$ (including the trivial one) to (5) with $x_1, \ldots, x_n$ in $F$. For $F$ a field with $q$ elements we have:

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

(2.1) $|N - q^{n-1}| \leq M(d_1,\ldots,d_n)(q-1)q^{(n/2)-1}$ , where

$M(d_1,\ldots,d_n)$ is the number of n-tuples $(j_1,\ldots,j_n)$ with $j_i$ an integer, $0 < j_i \leq d_i - 1$ for $i=1,\ldots,n$ and $(j_1/d_1 + \ldots + j_n/d_n)$ an integer.

This result was proved by Hua and Vandiver as well - the reader may find a pleasant exposition and historical comments in [3, pp. 103-105]. When we specialize to equation (1) we have that each $d_i$ is $d$. We write $M_n(d)$ for $M(d,\ldots,d)$. In this case there is a concise formula for $M_n(d)$ [7, p. 169]:

(2.2) $$M_n(d) = ((d-1)^{n-1} + (-1)^n)(d-1)/d .$$

This formula can be proved thus: To have $(j_1,\ldots,j_n)$ be a suitable n-tuple we may choose $j_1,\ldots,j_{n-1}$ almost arbitrary integers between $1$ and $d-1$ , and let $j_n = dk - (j_1 + \ldots + j_{n-1})$, where $k$ is the least positive integer $m$ with $dm \geq (j_1 + \ldots + j_{n-1})$. Among the $(d-1)^{n-1}$ $(n-1)$-tuples $(j_1,\ldots,j_{n-1})$, the only ones which do not give a suitable $(j_1,\ldots,j_n)$ are those for which $j_1 + \ldots + j_{n-1} = dm$ for some integer $m$. But there are $M_{n-1}(d)$ of these and (2.2) follows by induction on $n$.

Let us now specialize further to the situation where $n = 3$. We will then be considering the equation

(6) $$a_1X_1^d + a_2X_2^d + a_3X_3^d = 0 .$$

We will write $M(d)$ for $M_3(d)$, which equals $(d-1)(d-2)$. If equation (6) has only the trivial solution then $N = 1$ and (2.1) implies that $(q+1) \leq (d-1)(d-2)q^{\frac{1}{2}}$. By use of the quadratic formula it is straightforward to obtain the following result.

(2.3) Equation (6) has a solution if $F$ has $q$ elements, where $q > \frac{1}{2}[M(d)^2 - 2 + M(d)(M(d)^2 - 4)^{\frac{1}{2}}]$ and $M(d) = (d-1)(d-2)$.

Tietäiväinen [9, Theorem 7, p. 27] proved a result in the spirit of (2.3) but which also applies to equations with more than three unknowns.

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

He showed that if $-1$ is in $F^d$ and $q \geq n^{-1}d(d-1)^{n/(n-2)}$ then equation (1) has a solution. For $n=3$ and $d$ ranging through the small values we will examine, (2.3) gives a smaller value of $q$ than this result.

The information that (2.3) yields when $d$ is $2$ or $3$ can be obtained without use of formula (2.1). When $d=2$ it is simple to see that every equation (6) has a solution by recalling that in a finite field every element is a sum of two squares, and using (1.1) along with the observation that $[F^*:F^2] \leq 2$. When $d=3$ we have that $\delta$, the greatest common divisor of $d$ and $q-1$ is $1$ or $3$. Then (1.2) and (1.3) imply that every equation (6) has a solution.

For $d=4$, (2.3) implies that every equation (6) has a solution if $q > 34$. To decide for which $q \leq 34$ there are equations (6) admitting only the trivial solution we need a computational device for checking all such equations without going through every case. This concern will be the focus of the next section.

## 3. The computations

The values of $q$ for which the equation

$$a_1X_1^4 + a_2X_2^4 + a_3X_3^4 = 0 \tag{7}$$

may fail to have a solution have been shown to be among $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32$. If $gcd(4,q-1) < 4$ then every equation (7) has a solution, by (1.2) and our analysis of (6) for $d = 2$. This reduces our work to considering only $q = 5, 9, 13, 17, 25, 29$. If $8$ divides $q-1$ then there is a primitive eighth root of unity, $\zeta$, in $F^*$. Then $\zeta^4 = -1$ and Theorem 1.4 implies that equation (7) has a solution. Thus we eliminate $q = 9, 17$ and $25$ from consideration. We cannot eliminate $q = 5, 13, 29$ since in these cases there are equations such as (7) with only the trivial solution, namely those with $a_1 = a_2 = a_3 = 1$ for $q=5$ and $q=29$ and with $a_1 = a_2 = -a_3 = 1$ for $q = 13$. The search for these examples among the fields $F_5$, $F_{13}$ and $F_{29}$ can be shortened so that in each case only a few equations need to be tested. The following discussion shows how this is done.

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

For $q = 5, 13, 29$ we have a primitive fourth root of unity $\zeta$ in $F^*$, with $\zeta$ not in $F^2$ since $8$ does not divide $q-1$. The cosets $F^4$, $-F^4$, $\zeta F^4$, $-\zeta F^4$ are therefore distinct and since by (1.2) there are four cosets of $F^4$ in $F^*$, we have listed them all. We now use (1.1) to observe that if the cosets $a_i F^4$, $i = 1, 2, 3$ are distinct, there are two of them such that one contains $1$, the other $-1$, or one contains $\zeta$, the other $-\zeta$. In either case equation (7) has a solution. We may therefore consider only the case where the cosets $a_i F^4$ are not distinct. Solving (7) is then equivalent to solving an equation of the form

$$X_1^4 + X_2^4 + cX_3^4 = 0 , \tag{8}$$

where $c$ is one of $1, -1, \zeta, -\zeta$. Checking each of the four equations (8) in each of the three fields $F_5$, $F_{13}$, $F_{29}$ is not a difficult or onerous task, and the offending equations can be readily detected.

Having shown that $F_5$, $F_{13}$, $F_{29}$ are the only fields for which (6) can fail to have a solution when $d = 4$, we will attack the case $d = 5$. Using (2.3) we see that the equation

$$a_1X_1^5 + a_2X_2^5 + a_3X_3^5 = 0 \tag{9}$$

has a solution when $q > 142$. We can eliminate those $q$ with $gcd(5,q-1) = 1$, leaving only the cases $q = 11, 16, 31, 41, 61, 71, 81, 101, 121, 131$.

If two of the cosets $a_i F^5$ are equal then (9) has a solution because $(-1)^5 = -1$. We may therefore assume the cosets $a_i F^5$ are distinct for $i = 1, 2, 3$. Hence if $\zeta$ is a primitive fifth root of unity, solving (9) is equivalent to solving one of the six equations

$$\begin{cases} X_1^5 + \zeta X_2^5 + \zeta^2 X_3^5 = 0 & X_1^5 + \zeta X_2^5 + \zeta^3 X_3^5 = 0 \\ X_1^5 + \zeta X_2^5 + \zeta^4 X_3^5 = 0 & X_1^5 + \zeta^2 X_2^5 + \zeta^3 X_3^5 = 0 \\ X_1^5 + \zeta^3 X_2^5 + \zeta^4 X_3^5 = 0 & X_1^5 + \zeta^2 X_2^5 + \zeta^4 X_3^5 = 0 \end{cases} . \tag{10}$$

If we multiply the first equation in each column by a suitable power of $\zeta$

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

we can generate the other equations in the column (after renumbering the $X_i$). We have shown:

(3.1) All equations (9) have a solution if and only if each of the two equations

$$X_1^5 + \zeta X_2^5 + \zeta^2 X_3^5 = 0 \qquad X_1^5 + \zeta X_2^5 + \zeta^3 X_3^5 = 0 \tag{11}$$

or equivalently, each of the two equations

$$1 + \zeta X^5 + \zeta^2 Y^5 = 0 \qquad 1 + \zeta X^5 + \zeta^3 Y^5 = 0 \tag{12}$$

has a solution.

We can now eliminate from consideration those $q$ where $25$ divides $q-1$ (which unfortunately means only the case $q = 101$) since for these $\zeta = \alpha^5$ and each of the equations in (11) has a solution with $X_1 = 1$, $X_2 = -\alpha^{-1}$, $X_3 = 0$.

Our next reduction depends on using (1.3). Since we are assuming $\delta = 5$, there exists $b$ in $F^*$ with $F^5$, $bF^5$, $(1+b)F^5$ distinct cosets. By (3.1) the equation

$$X_1^5 + bX_2^5 + (1+b)X_3^5 = 0 \tag{13}$$

must be equivalent (in the sense of having a solution) to one of the equations in (11). Since (13) has the solution $X_1 = X_2 = -X_3 = 1$, it follows that:

(3.2) At least one of the equation in (11) has a solution.

By using (3.1) and (3.2) we can eliminate the cases in our list where $q = p^f$, $p$ the characteristic of $F$, $f > 1$. For then $(a + b)^p = a^p + b^p$. If the first equation of (11) has a solution $(x_1,x_2,x_3)$ then raising to the $p$th power gives a solution $(x_1^p,x_2^p,x_3^p)$ to the equation:

$$X_1^5 + \zeta^p X_2^5 + \zeta^{2p} X_3^5 = 0 \quad . \tag{14}$$

In the list of the $q$ we are considering the values of $p$ thus arising are $p = 2$, $3$ and $11$. Looking at table (10) we see that equation (14) is

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

in each case in the second column. It follows that the two equations in (11) are equivalent, hence by (3.1) and (3.2) all equations (9) have a solution when $q = 16$, $81$ and $121$.

We are left to consider the two equations in (12) for $q = 11$, $31$, $41$, $61$, $71$, $101$, $131$. For $q = 11$ we can take $\zeta = 4$ as our fifth root of unity, and since $F^5 = \{\pm 1\}$ it is easy to see that the second equation in (12) does not have a solution. Although it turns out that except for $q = 11$ both equations in (12) have solutions, we are not able to offer a pleasant explanation for this fact. However, the computations involved in disposing of the open cases are not particularly burdensome, owing to the nice form of the equations in (12). Indeed, once we choose a fifth root of unity $\zeta$ and compute the cosets $\zeta^i F^5$, $i = 0,\ldots,3$ we need only inspect each of the pairs of cosets $(\zeta F^5, \zeta^2 F^5)$, $(\zeta F^5, \zeta^3 F^5)$ to see if there is an element in the first coset of the pair which differs by $\pm 1$ from an element in the second coset of the pair (we are using the fact that $(-1)^5 = -1$. We will list the results of our computations in a table so the reader can verify them, and after that we will summarize our conclusions about equation (9). In our table we write $n$ for the $n$-fold sum of $1$ in $F$, $(x,y)$ for a solution to the equation heading the column and $\zeta_5$ for a primitive fifth root of unity.

| $q$ | $\zeta_5$ | $1 + \zeta X^5 + \zeta^2 Y^5$ | $1 + \zeta X^5 + \zeta^3 Y^5$ |
|---|---|---|---|
| 31 | 2 | (-3,-3) | (3,-3) |
| 41 | -4 | (14,-1) | ( 3,3 ) |
| 61 | -3 | ( -4,8 ) | ( 2,1 ) |
| 71 | 5 | ( 2,-2 ) | (-2,-1) |
| 131 | -42 | (2,-23) | (-6,21) |

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

THEOREM 3.1. *Let $F$ be a finite field with $q$ elements. Let $a_1,a_2,a_3$ be elements of $F$. The equation*

$$a_1X_1^d + a_2X_2^d + a_3X_3^d = 0$$

*has nontrivial solutions for $d = 2$ and $d = 3$. For $d = 4$ there exist $a_1,a_2,a_3$ for which the equation fails to have a nontrivial solution precisely when $q = 5, 13, 29$. For $d = 5$ such $a_i$ exist precisely when $q = 11$.*

## 4. Sums of two dth powers

There is clearly a connection between the existence of solutions to the equation

$$aX_1^d + bX_2^d + cX_3^d = 0 \tag{15}$$

and solutions to the equation

$$aX^d + bY^d = -c\ . \tag{16}$$

If (16) has a solution so does (15), but the reverse need not be true if all solutions $(x_1,x_2,x_3)$ to (15) have $x_3 = 0$. We would therefore expect that if there is an integer $I(d)$ such that every equation (16) has a solution in $F_q$ when $q > I(d)$, then $I(d)$ should be related to, but probably be strictly larger, than the quantity $\frac{1}{2}[M(d)^2 - 2 + M(d)(M(d)^2 - 4)^{\frac{1}{2}}]$ mentioned in (2.3).

We will discuss how to obtain a well-known formula for one such $I(d)$ using the estimate presented in (2.1). The discussion surrounding (2.1) is the only place in our paper where we invoked results that seem to go beyond basic facts about finite fields and groups. However, a perusal of [3, Chapter 7] will convince the reader that this same material is all that is needed to establish and understand (2.1) - although the discussion in [3] is for prime fields, the very same arguments given there apply to all finite fields. Our formula for $I(d)$ can be, and is obtained in various places, from first principles using Gauss and Jacobi sums rather than from (2.1). However, it seems worthwhile to pursue our

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

method hoping to pique the reader's curiosity to consult [3] and compare our recursive use of (2.1) with a similar recursive process used to establish formulas for Gauss sums.

We now drop our convention that solutions are assumed to be non-trivial. Let $F$ have $q$ elements and let

$$N = \{(x_1,x_2,x_3) \in F\times F\times F \mid ax_1^d + bx_2^d + cx_3^d = 0\} ,$$

$$L = \{(x,y) \in F\times F \mid ax^d + by^d = -c\} .$$

Let $N$ denote the cardinality of $N$, $L$ that of $L$. For each element $(x,y)$ in $L$ there are $(q-1)$ elements in $N$, namely $(xu,yu,u)$ as $u$ varies through $F^*$. It is easy to see that $N = (q-1)L + N_o$, where $N_o$ is the cardinality of the set

$$N_o = \{(x_1,x_2) \mid ax_1^d + bx_2^d = 0\} .$$

The equation $aX_1^d + bX_2^d = 0$ is one to which the discussion of (2.1) applies with $n = 2$, so that $M(d,d) = M_2(d) = d-1$, by (2.2). Thus (2.1) implies that

$$|N_o - q| \leqslant (d-1)(q-1). \tag{17}$$

What can we say about $q$ if equation (16) has no solution? We must have $L = 0$ so that $N = N_o$. Then applying (2.1) with $n = 3$ yields

$$|N_o - q^2| \leqslant (d-1)(d-2)(q-1)q^{\frac{1}{2}} . \tag{18}$$

Now use (17) and (18) together with the triangle inequality, then cancel a factor of $(q-1)$, leading to

$$q \leqslant (d-1) + (d-1)(d-2)q^{\frac{1}{2}} .$$

From this inequality we obtain the next result by a straightforward use of the binomial formula.

https://doi.org/10.1017/S0004972700001702 Published online by Cambridge University Press

THEOREM 4.1. *Let $F$ be a field with $q$ elements, $d$ a positive integer. If there exist $a,b,c$ in $F$ such that the equation*

$$aX^d + bY^d = c$$

*fails to have a solution then*

$$q < \tfrac{1}{2}M(d)^2 + (d-1) + \tfrac{1}{2}M(d)(M(d)^2 + 4(d-1))^{\frac{1}{2}} ,$$

*where $M(d) = (d-1)(d-2)$.*

Small [8] showed that for $q > (d-1)^4$ any element of $F$ is a sum of two $d$th powers. Theorem 4.1 gives a smaller bound for $q$, though one that is not so easily remembered. Though smaller, our bound for $q$ still grows like $d^4$, as does that of Small and that of Tietäivänen, referred to following (2.3).

Our methods in Section 3 are at the limit of feasibility for hand-computation when $d = 5$. The (admittedly sparse) evidence we have gathered suggests that the requirement of (2.3) on the size of $q$ is stricter than necessary. Since our basis for restricting $q$ is a count on the number of solutions to our equations, rather than a criterion for whether a single nontrivial solution exists, it may be that an approach involving (2.1) is bound to give too gross an estimate. As previously indicated there are more sophisticated methods that have been used to establish conditions under which solutions exist (see [9] for example). In addition to the book of Ireland and Rosen [3] mentioned earlier we recommend Joly's exposition [4] for an introduction and broad survey of questions about equations in finite fields. We also suggest Mazur's article [6] for those wishing to see the connection between elementary questions about the number of solutions to equations and the deeper concerns leading to the Artin zeta function and the Weil conjectures.

## References

[1] J. F. Gray, "Diagonal forms of odd degree over a finite field", *Michigan Math. J.* 7 (1960), 297-302.

[2] L. K. Hua and H. S. Vandiver, "Characters over certain types of rings, with applications to the theory of equations in a finite field", *Proc. Nat. Acad. Sci. USA* 35 (1949), 94-99.

[3] K. Ireland and M. I. Rosen, *Elements of number theory* (Bogden and Quigley, Tarrytown-on-Hudson, N.Y., 1972).

[4] J.-R. Joly, "Équations et variétiés algébriques sur un corps fini", *L'Enseignement Math.* 19 (1973), 1-117.

[5] D. J. Lewis, "Cubic congruences", *Michigan Math. J.* 4 (1957), 85-95.

[6] B. Mazur, "Eigenvalues of Frobenius acting on algebraic varieties over a finite field", in *Algebraic geometry - Arcata 1974*, 231-262 (Proceedings of Symposia in Pure Mathematics, No. 29, Amer. Math. Soc. Providence, R.I., 1975).

[7] W. M. Schmidt, *Equations over finite fields - an elementary approach* (Lecture Notes in Mathematics No. 536. Springer-Verlag, Berlin, 1976).

[8] C. Small, "Sums of powers in large finite fields", *Proc. Amer. Math. Soc.* 65 (1977), 35-36.

[9] A. Tietäväinen, "On the non-trivial solvability of some equations and systems of equation in finite fields", *Ann. Acad. Sci. Fenn. Ser. A I* 360 (1965), 6-38.

[10] A. Weil, "Number of solutions of equations in a finite field", *Bull. Amer. Math. Soc.* 55 (1949), 497-508.

Department of Mathematics & Statistics,
Queen's University,
Kingston, K7L 3N6,
Canada.