DIAGONAL FORMS OF ODD DEGREE OVER A FINITE FIELD

James F. Gray

1. A PROBLEM

Throughout this paper, k is a finite field of q^f elements, k^* is the multiplicative group of nonzero elements of k, and k^p the set of p-th powers in k^*.

The literature shows the existence of nontrivial zeros in k of each of the following forms (here p denotes an odd prime):

$$a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 \qquad (a_i \in k), \tag{1}$$

$$a_1 x_1^p + a_2 x_2^p + \cdots + a_p x_p^p \qquad (a_i \in k;\ p \geq 3), \tag{2}$$

$$a_1 x_1^p + a_2 x_2^p + \cdots + a_{p-1} x_{p-1}^p \qquad (a_i \in k;\ p \geq 5). \tag{3}$$

In particular, Lewis [2] established the existence of zeros for (1), and the author [1, Theorems 5, 8] for (2) and (3).

Without change, the proofs for (2) and (3) extend in addition to all odd positive integers p relatively prime to $q^f - 1$. The question naturally arises whether or not a restriction to higher values of p would permit further improvements. More precisely, for a fixed odd positive integer p, either itself prime or relatively prime to $q^f - 1$, what is the maximum value of t for which

$$a_1 x_1^p + a_2 x_2^p + \cdots + a_{p-t} x_{p-t}^p \qquad (a_i \in k) \tag{4}$$

has a nontrivial zero in k? Since (4) is solvable with $t = 0$ by (2), and since t is obviously bounded above by $p - 2$, such a maximum value exists.

This paper proposes the following estimate of t (notation: $[x]$ is the greatest integer not greater than x).

THEOREM A. *If* k *is a finite field of* q^f *elements, and* p *is an odd positive integer, either prime or relatively prime to* $q^f - 1$, *then* (4) *has a nontrivial zero in* k *for* $t = t(p) = [2\sqrt{p+2}] - 4$.

Note that $t(3) = 0$ and $t(5) = 1$, in agreement with results (2) and (3) above. Further, for $p = 1$, although $t(p) = -1$, the theorem is true as stated, by inspection. Henceforth, then, we shall consider only $p \geq 3$.

2. A REFORMULATION OF THE PROBLEM

A few simple observations will suffice to show that Theorem A is a consequence of

THEOREM B. *If* k *is a finite field of* q^f *elements, if* p *is an odd prime such that* $p \mid q^f - 1$, *and if* dk^p *is a generator of* k^*/k^p (k^* the multiplicative group of k;

Received February 13, 1960.