THE NUMBER OF SOLUTIONS OF CERTAIN SYSTEMS OF EQUATIONS IN A FINITE FIELD

BY ROBERT G. VAN METER

1. Introduction. Let $Z(Z^+)$ be the set of integers (positive integers). We restrict h, i, j, k and l to Z and restrict m, n and r to Z^+. Let K be a finite field with q elements. If $a \in K$, f is a polynomial in $X_1, \cdots, X_r$ over K, $\mathbf{y} =_{\mathrm{df}} (y_1, \cdots, y_r)$ and each y_i is a variable with domain K, then

$$N_r[f(\mathbf{y}) = a] = \#\{\mathbf{c} \in K^r : f(\mathbf{c}) = a\}.$$

We often abbreviate "$N_r[f(\mathbf{y}) = a]$" to "$N_r[f = a]$" or "$N[f = a]$". Similar notation is used for the number of solutions of any open sentence in r variables each having domain K. In any context, the indeterminates (and corresponding variables) are distinct.

We consider the system of equations

$$\underset{i=1}{\overset{m}{\&}} \left(\sum_{j=1}^{n} a_{ij} f_j(\mathbf{x}_j) = a_{i,n+1} \right), \tag{1.1}$$

where

(1.2) $\quad a_{ij} \in K \quad$ for all $\quad (i, j) \in [1, m] \times [1, n + 1]$,

(1.3) for all $j \in [1, n]$, $r_j \in Z^+$ (and $R(n) =_{\mathrm{df}} \sum_{j=1}^{n} r_j$), $A_j =_{\mathrm{df}} q^{r_j - 1}$, f_j is a κ-polynomial in $X_{j1}, \cdots, X_{jr_j}$ over K with $N_{r_j}[f_j = a] = A_j + \kappa(a) B_j$ for all $a \in K$, $\mathbf{x}_j =_{\mathrm{df}} (x_{j1}, \cdots, x_{jr_j})$, each x_{jk} is a variable with domain K,

and, of course,

(1.4) for all $i \in [1, m]$ ($j \in [1, n]$), there exists $j \in [1, n]$ ($i \in [1, m]$) such that $a_{ij} \neq 0$.

We consider the problem of determining $N_{R(n)}[(1.1)]$ subject to (1.2)–(1.4).

Carlitz [2], making use of exponential sums, determined $N[(1.1)]$ in case $m = 2$, the a_{ij} are subject to certain restrictions and the f_j are specific κ-polynomials (certain quadratic forms).

Corson [4], using entirely different methods, determined $N[(1.1)]$ for arbitrary a_{ij} and f_j subject to (1.2)–(1.4) in case $m = 2$ and $n > 2$.

In this paper we generalize some of Corson's results. We devote §2 to κ-polynomials; in particular, Theorem 2.6 gives $N[(1.1)]$ in case $m = 1$. In

Received June 9, 1969. This paper was written while the author was supported by a faculty research grant from Florida Presbyterian College. It is a revision of a doctoral thesis submitted to Duke University. The author is indebted to Professor Carlitz for suggesting the problem.