ACTA ARITHMETICA
130.2 (2007)

On a class of equations with special degrees over finite fields

by

Wei Cao and Qi Sun (Chengdu)

1. Introduction. Let $\mathbb{F}_q$ be the finite field of q elements, where $q = p^r$ and p is the characteristic of $\mathbb{F}_q$. Let $f(x_1, \dots, x_n)$ be a nonzero polynomial in n variables over $\mathbb{F}_q$ and let $N(f = 0)$ denote the number of $\mathbb{F}_q$-rational points on the affine hypersurface $f = 0$ in $\mathbb{A}^n(\mathbb{F}_q)$, that is,

$$N(f = 0) = \#\{(x_1, \dots, x_n) \in \mathbb{A}^n(\mathbb{F}_q) \mid f(x_1, \dots, x_n) = 0\}.$$

One of the main objectives of arithmetic of finite fields is to study the value of $N(f = 0)$. In general, it is difficult to give an explicit formula for $N(f = 0)$. Hence there are various estimates for $N(f = 0)$. The degree of f, denoted $\deg f$, plays an important role in these estimates. An elementary upper bound for $N(f = 0)$ (see [10, p. 147]) is

$$N(f = 0) \le q^{n-1} \deg f.$$

Let ord_p be the p-adic additive valuation normalized so that $\mathrm{ord}_p\, p = 1$. The classical Chevalley–Warning theorem asserts that $\mathrm{ord}_p(N(f = 0)) \ge 1$ if $n > \deg f$. Further, Ax [2] showed that

$$\mathrm{ord}_p(N(f = 0)) \ge r \left\lceil \frac{n - \deg f}{\deg f} \right\rceil.$$

Ax's result was extended by Katz [6] to a system of equations. Note that in [12] Katz's theorem was proved by using elementary methods based on Gauss sums, which is also a useful tool adopted in this paper. The Chevalley–Warning–Ax–Katz-type estimates can be improved in many special cases; see [1, 4, 5, 9].

However, the effort to find the formula for $N(f = 0)$ under certain conditions has never been given up. By observing that the explicit formula for $N(f = 0)$ can be obtained if the degrees of the variables in f satisfy

2000 *Mathematics Subject Classification*: 11T06, 11T24, 11S99, 05A10.

Key words and phrases: finite field, number of zeros, p-adic, Gauss sum, degrees of equations.

This work was partially supported by the NNSF of China (10128103).

certain conditions, Sun [11] gave the following result. Its generalizations as well as a short proof to them are given in [3]. In what follows, let det denote the determinant of a square matrix and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$.

THEOREM 1.1 (see [11, Theorem 2] or [3, Theorem 1.1]). *Suppose*

$$f = a_1 x_1^{d_{11}} x_2^{d_{21}} \cdots x_n^{d_{n1}} + \cdots + a_n x_1^{d_{1n}} x_2^{d_{2n}} \cdots x_n^{d_{nn}}$$

where $d_{ij} > 0$, $a_i \in \mathbb{F}_q^*$. *Let* $D = (d_{ij})$ *be an* $n \times n$ *matrix with* $1 \le i, j \le n$. *If* $\gcd(\det(D), q-1) = 1$, *then for* $b \in \mathbb{F}_q$ *we have*

$$N(f = b) = \begin{cases} q^n - (q-1)^n + \dfrac{(q-1)^n + (-1)^n (q-1)}{q} & \text{if } b = 0, \\ \dfrac{(q-1)^n - (-1)^n}{q} & \text{if } b \neq 0. \end{cases}$$

For the so-called "triangular equations", Wang and Sun [14] showed

THEOREM 1.2 (see [14, Corollary]). *Suppose*

$$f = a_1 x_1^{d_{11}} + a_2 x_1^{d_{12}} x_2^{d_{22}} + \cdots + a_n x_1^{d_{1n}} x_2^{d_{2n}} \cdots x_n^{d_{nn}},$$

where $d_{ij} > 0$, $\gcd(d_{11} d_{22} \cdots d_{nn}, q-1) = 1, a_i \in \mathbb{F}_q^*$. *Then*

$$N(f = b) = \begin{cases} (-1)^{n-1} + 2 \sum\limits_{k=0}^{n-1} (-1)^{n-k-1} q^k & \text{if } b = 0, \\ \sum\limits_{k=0}^{n-1} (-1)^{n-k-1} q^k & \text{if } b \neq 0. \end{cases}$$

It is known that the coefficient matrix of a system of linear equations can be used to find the solutions of the system. Inspired by Theorems 1.1 and 1.2, we will show that in some special cases the matrix formed by the degrees of the variables of a "nonlinear" equation over finite fields can be used to count the number of solutions of the equation. Thus the concept of *degree matrix of a given polynomial* naturally arises.

Let $D_1, \ldots, D_m$ be m distinct lattice points in $\mathbb{Z}_{\ge 0}^n$. For $D_j = (d_{1j}, \ldots, d_{nj})$, write $x^{D_j} = x_1^{d_{1j}} \cdots x_n^{d_{nj}}$. Let f be written in the form

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{m} a_j x^{D_j}, \qquad a_j \in \mathbb{F}_q^*.$$

The *degree matrix* of f, denoted D_f, is defined to be the $n \times m$ matrix

$$D_f = (D_1, \ldots, D_m) = (d_{ij})_{1 \le i \le n, 1 \le j \le m},$$

where each D_j is written as a column vector.

This paper will give the formulae for $N(f = 0)$ provided the degree matrix D_f satisfies certain conditions. Note that in Theorems 1.1 and 1.2 the requirements for D_f are similar: a) all the entries in D_f are nonnegative integers, which case will be denoted by $D_f \ge 0$ for short; b) D_f is a square

matrix, i.e. $n = m$; and c) $\gcd(\det(D_f), q-1) = 1$, which means that $\det(D_f)$ is invertible in the residue ring $\mathbb{Z}/(q-1)$. The main theorem of this paper, Theorem 2.1 in the next section, will weaken these constraints and hence cover more general cases than Theorems 1.1 and 1.2.

2. The main result. Let us start by deriving a well known formula for $N(f = 0)$ in terms of Gauss sums. To do this, some knowledge of p-adic analysis and character sums of finite fields are needed; those unfamiliar with these subjects should consult the standard references [7] and [8].

Let $\mathbb{Q}_p$ be the field of p-adic numbers and let $\mathbb{C}_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$. Let χ be the Teichmüller character of the multiplicative group $\mathbb{F}_q^*$. For $a \in \mathbb{F}_q^*$, the value $\chi(a)$ is just the $(q-1)$th root of unity in $\mathbb{C}_p$ such that $\chi(a)$ modulo p reduces to a. Define the $(q-2)$ Gauss sums over $\mathbb{F}_q$ by

$$G(k) = \sum_{a \in \mathbb{F}_q^*} \chi(a)^{-k} \zeta_p^{\mathrm{Tr}(a)}, \quad 1 \le k \le q-2,$$

where ζ_p is a primitive pth root of unity in $\mathbb{C}_p$ and Tr denotes the trace map from $\mathbb{F}_q$ to the prime field $\mathbb{F}_p$. We claim that for all $a \in \mathbb{F}_q$, the Gauss sums satisfy the following interpolation relation:

$$\zeta_p^{\mathrm{Tr}(a)} = \sum_{k=0}^{q-1} \frac{G(k)}{q-1} \chi(a)^k,$$

where

$$G(0) = q-1, \qquad G(q-1) = -q.$$

In fact, by the Vandermonde determinant, there are numbers $C(k)$ $(0 \le k \le q-1)$ such that for all $a \in \mathbb{F}_q$, one has

$$\zeta_p^{\mathrm{Tr}(a)} = \sum_{k=0}^{q-1} \frac{C(k)}{q-1} \chi(a)^k.$$

It suffices to prove that $C(k) = G(k)$ for all k. Taking $a = 0$, one finds that $C(0)/(q-1) = 1$. This proves that $C(0) = q-1 = G(0)$. For $1 \le k \le q-2$, one computes that

$$G(k) = \sum_{a \in \mathbb{F}_q^*} \chi(a)^{-k} \zeta_p^{\mathrm{Tr}(a)} = \frac{C(k)}{q-1} (q-1) = C(k).$$

Finally,

$$0 = \sum_{a \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(a)} = \frac{C(0)}{q-1} q + \frac{C(q-1)}{q-1} (q-1).$$

This gives $C(q-1) = -q = G(q-1)$. The claim is proved.

With the notation as introduced in Section 1, write $\widetilde{D}_j = (1, D_j) \in \mathbb{Z}_{\geq 0}^{n+1}$. Then

$$x_0 f(x_1, \ldots, x_n) = \sum_{j=1}^{m} a_j x^{\widetilde{D}_j} = \sum_{j=1}^{m} a_j x_0 x_1^{d_{1j}} \cdots x_n^{d_{nj}},$$

where x now has $n+1$ variables $\{x_0, \ldots, x_n\}$.

Let $R = \{0, 1, \ldots, q-1\} \subset \mathbb{Z}$ and $R^m = \prod_{j=1}^{m} R$ be the direct product of R. For any $k = (k_1, \ldots, k_m) \in R^m$, define

$$\sigma(k) = \#\{1 \leq j \leq m \mid k_j > 0\},$$

and let $s(k)$ be the number of nonzero entries in $k_1\widetilde{D}_1 + \cdots + k_m\widetilde{D}_m$. Let $d_{0j} = 1$ for $j = 1, \ldots, m$. Then we have

$$s(k) = \#\{0 \leq i \leq n \mid k_j d_{ij} > 0 \text{ for some } 1 \leq j \leq m\}.$$

Using the formula

$$\sum_{t \in \mathbb{F}_q} \chi(t)^k = \begin{cases} 0 & \text{if } (q-1) \nmid k, \\ q-1 & \text{if } (q-1) \mid k \text{ and } k > 0, \\ q & \text{if } k = 0, \end{cases}$$

one then calculates that

$$\begin{aligned} qN(f=0) &= \sum_{x_0, \ldots, x_n \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(x_0 f(x))} = \sum_{x_0, \ldots, x_n \in \mathbb{F}_q} \prod_{j=1}^{m} \zeta_p^{\mathrm{Tr}(a_j x^{\widetilde{D}_j})} \\ &= \sum_{x_0, \ldots, x_n \in \mathbb{F}_q} \prod_{j=1}^{m} \sum_{k_j=0}^{q-1} \frac{G(k_j)}{q-1} \chi(a_j)^{k_j} \chi(x^{\widetilde{D}_j})^{k_j} \\ &= \sum_{k_1=0}^{q-1} \cdots \sum_{k_m=0}^{q-1} \left(\prod_{j=1}^{m} \frac{G(k_j)}{q-1} \chi(a_j)^{k_j} \right) \sum_{x_0, \ldots, x_n \in \mathbb{F}_q} \chi(x^{k_1\widetilde{D}_1 + \cdots + k_m\widetilde{D}_m}) \\ &= \sum_{\sum_{j=1}^{m} k_j \widetilde{D}_j \equiv 0 \,(\mathrm{mod}\, q-1)} \frac{(q-1)^{s(k)} q^{n+1-s(k)}}{(q-1)^m} \prod_{j=1}^{m} \chi(a_j)^{k_j} G(k_j). \end{aligned}$$

The above deduction can also be found in [13]. Now we can state the main theorem of this paper.

THEOREM 2.1. *With the notation as above, if there is an $m \times m$ $(m \leq n)$ submatrix of D_f with determinant coprime to $q-1$, then $R = \{0, q-1\}$ and*

$$N(f=b) = \begin{cases} \displaystyle\sum_{k \in R^m} (-1)^{\sigma(k)} (q-1)^{s(k)-\sigma(k)} q^{n-s(k)+\sigma(k)} & \text{if } b = 0, \\ \displaystyle q^n (q-1)^{-1} - \sum_{k \in R^m} (-1)^{\sigma(k)} (q-1)^{s(k)-\sigma(k)-1} q^{n-s(k)+\sigma(k)} & \text{if } b \neq 0. \end{cases}$$

In this case, for any $b \in \mathbb{F}_q$ the value of $N(f = b)$ is completely determined by the degree matrix D_f.

Proof. Suppose there exists an $m \times m$ submatrix of D_f whose determinant is coprime to $q-1$. Then from linear algebra, we know that the following congruence system has only the zero solution, i.e., $k_1 \equiv \cdots \equiv k_m \equiv 0 \pmod{q-1}$:

$$k_1\widetilde{D}_1 + \cdots + k_m\widetilde{D}_m \equiv 0 \pmod{q-1}.$$

Note that $\chi(a_j)^0 = \chi(a_j)^{q-1} = 1$ for $a_j \in \mathbb{F}_q^*$ and $G(0) = q-1, G(q-1) = -q$. Thus we have

$$N(f=0) = \sum_{k \in R^m} (-1)^{\sigma(k)}(q-1)^{s(k)-\sigma(k)}q^{n-s(k)+\sigma(k)}.$$

Now let $b \in \mathbb{F}_q^*$. It is easy to see that the degree matrix D_{f-b} is obtained from D_f by adjoining $(1, 0, \ldots, 0)^{\mathrm{T}}$ as the right most column. Consider the congruence system

$$\begin{pmatrix} 1 & \cdots & 1 & 1 \\ d_{11} & \cdots & d_{1m} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ d_{n1} & \cdots & d_{nm} & 0 \end{pmatrix} \begin{pmatrix} k_1 \\ \vdots \\ k_m \\ k_{m+1} \end{pmatrix} \equiv 0 \pmod{q-1}. \tag{2.1}$$

By the last n congruences of (2.1) and the previous discussion, we have $k_1 \equiv \cdots \equiv k_m \equiv 0 \pmod{q-1}$. So $k_{m+1} \equiv 0 \pmod{q-1}$ by the first congruence of (2.1). This shows that the congruence system (2.1) also has only the zero solution. Thus the value of $N(f = b)$ is completely determined by the degree matrix D_{f-b}, and in particular does not depend on the choice of the concrete value of b. So $N(f = b) = (q^n - N(f = 0))/(q-1)$. The result follows. ∎

3. Corollaries. Finally, we give two corollaries to Theorem 2.1, which generalize Theorems 1.1 and 1.2 respectively. For the convenience of discussion, we introduce some notation. For a zero vector $k = (0, \ldots, 0) \in R^m$, we simply write $k = 0$. Observe that

$$N(f=0) = \Big(\sum_{k=0} + \sum_{k \in R^m \setminus \{0\}}\Big)(-1)^{\sigma(k)}(q-1)^{s(k)-\sigma(k)}q^{n-s(k)+\sigma(k)}.$$

Let $N_0(f = 0)$ denote the former sum on the right side and $N_*(f = 0)$ the latter. Clearly, for $k = 0$ we get $s(k) = \sigma(k) = 0$, implying $N_0(f = 0) = q^n$. Thus $N(f = 0) = q^n + N_*(f = 0)$. So we only need to calculate $N_*(f = 0)$.

COROLLARY 3.1. *With the notation as before, if $D_f > 0$ and there exists an $m \times m$ submatrix of D_f whose determinant is coprime to $q-1$, then*

$$N(f=b) = \begin{cases} q^n - q^{-1}(q-1)^{n-m+1}((q-1)^m - (-1)^m) & \text{if } b = 0, \\ q^{-1}(q-1)^{n-m}((q-1)^m - (-1)^m) & \text{if } b \neq 0. \end{cases}$$

In particular, if $n = m$, then

$$N(f=b) = \begin{cases} q^n - q^{-1}(q-1)((q-1)^n - (-1)^n) & \text{if } b = 0, \\ q^{-1}((q-1)^n - (-1)^n) & \text{if } b \neq 0. \end{cases}$$

Proof. Clearly, $s(k) = n+1$ for any $k \in R^m \setminus \{0\}$. Then by Theorem 2.1 and the binomial theorem, we have

$$\begin{aligned} N_*(f=0) &= \sum_{\sigma(k)=1}^{m} (-1)^{\sigma(k)}(q-1)^{n+1-\sigma(k)} q^{n-(n+1)+\sigma(k)} \\ &= q^{-1}(q-1)^{n-m+1} \sum_{\sigma(k)=1}^{m} (q-1)^{m-\sigma(k)}(-q)^{\sigma(k)} \\ &= -q^{-1}(q-1)^{n-m+1}((q-1)^m - (-1)^m). \end{aligned}$$

The other statements follow. ∎

COROLLARY 3.2. *With the notation as before, suppose that D_f is of the form*

$$D_f = \begin{pmatrix} & M & \\ d_{n-m+1,1} & \cdots & d_{n-m+1,m} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_{nm} \end{pmatrix}$$

where $M > 0$ is an $(n-m) \times m$ matrix and the submatrix $(d_{ij})_{n-m+1 \le i \le n, 1 \le j \le m}$ is upper triangular with $d_{ij} = 0$ for $i - j > n - m$ and $d_{ij} > 0$ otherwise. If there exists an $m \times m$ submatrix of D_f whose determinant is coprime to $q-1$, then

$$N(f=b) = \begin{cases} q^n + (q+1)^{-1}(1-q)^{n-m+1}((-1)^{n-m}q^m - (-1)^n) & \text{if } b = 0, \\ (q+1)^{-1}(1-q)^{n-m}((-1)^{n-m}q^m - (-1)^n) & \text{if } b \neq 0. \end{cases}$$

In particular, if $n = m$, then

$$N(f=b) = \begin{cases} q^n + (q+1)^{-1}(1-q)(q^n - (-1)^n) & \text{if } b = 0, \\ (q+1)^{-1}(q^n - (-1)^n) & \text{if } b \neq 0. \end{cases}$$

Proof. Let $l = n - m$. For a $k \in R^m \setminus \{0\}$, $s(k)$ can be expressed as follows:

$$s(k) = l + 1 + \max\{1 \le j \le m \mid k_j > 0\}.$$

For a fixed $s(k)$, only the entries in the set of $\{k_1, \dots, k_{s(k)-l-1}\}$ can take nonzero values and $k_{s(k)-l-1}$ must be nonzero. Thus by Theorem 2.1 and the binomial theorem, we obtain

$$
\begin{aligned}
&N_*(f=0)\\
&= \sum_{s(k)=l+2}^{n+1} \sum_{\sigma(k)=1}^{s(k)-l-1} \binom{s(k)-l-2}{\sigma(k)-1} (-1)^{\sigma(k)} (q-1)^{s(k)-\sigma(k)} q^{n-s(k)+\sigma(k)}\\
&= \sum_{s(k)=l+2}^{n+1} \sum_{i=0}^{s(k)-l-2} \binom{s(k)-l-2}{i} (-1)^{i+1} (q-1)^{s(k)-i-1} q^{n-s(k)+i+1}\\
&= \sum_{s(k)=l+2}^{n+1} (-1)(q-1)^{l+1} q^{n-s(k)+1} \sum_{i=0}^{s(k)-l-2} \binom{s(k)-l-2}{i} (q-1)^{s(k)-l-2-i} (-q)^i\\
&= (1-q)^{l+1} q^{n+1} \sum_{s(k)=l+2}^{n+1} (-q^{-1})^{s(k)}\\
&= (q+1)^{-1} (1-q)^{l+1} ((-1)^l q^{n-l} - (-1)^n).
\end{aligned}
$$

The other statements follow. ∎

Remark. We noticed that in [3] and [14], other forms of the generalizations of Theorems 1.1 and 1.2 are given. Similar to the proofs of the above two corollaries, these as well as other possible generalizations can also be derived from Theorem 2.1 via some combinatorial tricks.

Acknowledgements. The authors thank Professor Daqing Wan for kindly providing his course notes at the Arizona Winter School 2004 and the anonymous reviewer for his/her helpful comments and corrections.

References

[1] A. Adolphson and S. Sperber, *p-Adic estimates for exponential sums and the theorem of Chevalley–Warning*, Ann. Sci. École Norm. Sup. 20 (1987), 545–556.

[2] J. Ax, *Zeros of polynomials over finite fields*, Amer. J. Math. 86 (1964), 255–261.

[3] W. Cao, *A short proof to some results of Sun and Wang*, Algebra Colloq. 14 (2007), 177–180.

[4] W. Cao and Q. Sun, *A reduction for counting the number of zeros of general diagonal equation over finite fields*, Finite Fields Appl. 12 (2006), 681–692.

[5] —, —, *Improvements upon the Chevalley–Warning–Ax–Katz-type estimates*, J. Number Theory 122 (2007), 135–141.

[6] N. M. Katz, *On a theorem of Ax*, Amer. J. Math. 93 (1971), 485–499.

[7] N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta Functions*, Grad. Texts in Math. 58, Springer, 1996.

[8] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, Reading, MA, 1983.
[9] O. Moreno and C. J. Moreno, *Improvement of the Chevalley–Warning and the Ax–Katz theorem*, Amer. J. Math. 117 (1995), 241–244.
[10] W. M. Schmidt, *Equations over Finite Fields*: *An Elementary Approach*, Lecture Notes in Math. 536, Springer, New York, 1976.
[11] Q. Sun, *The formula for the number of solutions of a class of equations over a finite field*, Chinese Ann. Math. Ser. A 18 (1997), 403–408.
[12] D. Wan, *An elementary proof of a theorem of Katz*, Amer. J. Math. 111 (1989), 1–8.
[13] —, *Mirror symmetry for zeta functions*, in: AMS/IP Stud. Adv. Math. 38, Amer. Math. Soc., 2006, 159–184.
[14] W. Wang and Q. Sun, *The number of solutions of certain equations over finite fields*, Finite Fields Appl. 2 (2005), 182–192.

Department of Mathematics
Shanghai Jiaotong University
Shanghai 200240, P.R. China

School of Mathematics
Sichuan University
Chengdu 610064, P.R. China

Currently at:

School of Mathematics
Sichuan University
Chengdu 610064, P.R. China
E-mail: caowei433100@vip.sina.com

Received on 17.1.2007
and in revised form on 21.7.2007 (5371)