27. *On the Number of Distinct Values of a Polynomial with Coefficients in a Finite Field*

By Leonard CARLITZ
Department of Mathematics, Duke University, U.S.A.
(Comm. by Z. SUETUNA, M.J.A., March 12, 1955)

1. Let $GF(q)$ denote the finite field of order $q=p^{\nu}$ and put

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x \qquad (a_j\in GF(q)), \tag{1.1}$$

where $1<n<p$. Let $V=V(f)$ denote the number of distinct values $f(x)$, $x\in GF(q)$. Uchiyama [2] has proved the following theorem: Suppose that

$$f^*(u, v)=\frac{f(u)-f(v)}{u-v} \tag{1.2}$$

is absolutely irreducible (that is, irreducible in every finite extension of $GF(q)$); then $V>q/2$ for all $n\geqq 4$. It is pointed out this conclusion cannot be asserted without the hypothesis concerning $f^*(u, v)$; moreover the proof of the theorem makes use of a deep theorem of A. Weil on the number of solutions of equations in two unknowns in a finite field.

In this note we wish to point out that it is easy to prove that $V>q/2$ *on the average*. More precisely we shall prove the following

Theorem. *The sum*

$$\sum_{a_1\in GF(q)} V(f)\geqq\frac{q^3}{2q-1}\geqq\frac{q^2}{2}, \tag{1.3}$$

where the summation is over the coefficient of the first degree term in $f(x)$.

We remark that this theorem is independent of any hypothesis on $f^*(u, v)$ and that the proof is quite elementary.

2. For $x\in GF(q)$, we define

$$e(x)=e^{2\pi i S(x)/p}, \qquad S(x)=x+x^p+\cdots+x^{p^{\nu-1}}. \tag{2.1}$$

Then $e(x+y)=e(x)e(y)$ and

$$\sum_x e(xy)=\begin{cases} q & (y=0)\\ 0 & (y\neq 0).\end{cases} \tag{2.2}$$

Following the notation of [2] we let M_r denote the number of $y\in GF(q)$ such that the equation $f(x)=y$ has precisely r distinct roots in $GF(q)$; then we have

$$V=\sum_{r=1}^n M_r, \qquad q=\sum_{r=1}^n rM_r. \tag{2.3}$$

Also if $N_1=N_1(f)$ is the number of solutions (x, y) of $f(x)-f(y)=0$, then

$$N_1=\sum_{r=1}^n r^2M_r. \tag{2.4}$$

In the Cauchy inequality

(2.5) $$(\sum a_r b_r)^2 \leqq (\sum a_r^2)(\sum b_r^2)$$

take $a_r^2 = r^2 M_r$, $b_r^2 = M_r$, so that $(\sum rM_r)^2 \leqq (\sum r^2 M_r)(\sum M_r)$. Using (2.3) and (2.4) this becomes

(2.6) $$V(f)N_1(f) \geqq q^2.$$

A second application of (2.5) yields

$$\sum_{a_1} (V(f)N_1(f))^{1/2} \leqq (\sum_{a_1} V(f))^{1/2} (\sum_{a_1} N_1(f))^{1/2},$$

and using (2.6) we get

(2.7) $$(\sum_{a_1} V(f))(\sum_{a_1} N_1(f)) \geqq q^4.$$

Now on the other hand it is clear from (2.2) that

$$\begin{aligned} qN_1(f) &= \sum_t \sum_{x,y} e\{t(f(x)-f(y))\} \\ &= q^2 + \sum_{t \neq 0} \sum_{x,y} e\{t(x^n - y^n) + \cdots + ta_1(x-y)\}. \end{aligned}$$

Summing over a_1 and again using (2.2) we get

$$q \sum_{a_1} N_1(f) = q^3 + q \sum_{t \neq 0} \sum_x 1 = 2q^3 - q^2,$$

so that

(2.8) $$\sum_{a_1} N_1(f) = 2q^2 - q.$$

Substituting from (2.8) in (2.7) we have at once

$$\sum_{a_1} V(f) \geqq \frac{q^4}{2q^2 - q} = \frac{q^3}{2q-1} > \frac{q^2}{2},$$

which completes the proof of (1.3).

3. It may be of interest to remark that the method used in proving (2.8) leads easily to the following result. Let $f(x_1, \ldots, x_r)$ denote a polynomial $\in GF[q, x_1, \ldots, x_r]$, where r is an arbitrary integer $\geqq 1$ and put

$$M(f) = \sum_{x_1, \ldots, x_r} e(f(x_1, \ldots, x_r)).$$

Then we have

(3.1) $$\sum_{a_1, \ldots, a_r} |M(f)|^2 = q^{2r},$$

where $f(x_1, \ldots, x_r) = a_1 x_1 + \cdots + a_r x_r +$ terms of higher degree; in other words $M(f)$ is on the average of order $q^{r/2}$. This result may be compared with [1, formula (8.4)].

References

[1] L. Carlitz: Invariantive theory of equations in a finite field, Trans. Amer. Math. Soc., **75**, 405–427 (1953).

[2] S. Uchiyama: Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini, Proc. Japan Acad., **30**, 930–933 (1954).