46. Note on the Mean Value of $V(f)$

By Saburô UCHIYAMA

Mathematical Institute, Tokyo Metropolitan University, Tokyo

(Comm. by Z. SUETUNA, M.J.A., April 12, 1955)

1. Let $GF(q)$ be a fixed finite field of order $q=p^\nu$ and put the polynomial

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

where $1<n<p$. By $V(f)$ we denote the number of distinct values $f(x)$, $x \in GF(q)$. L. Carlitz [1] has recently proved by an elementary method, that the sum

$$\sum_{a_1 \in GF(q)} V(f) \geqq \frac{q^3}{2q-1} > \frac{q^2}{2}, \tag{1.2}$$

the summation being over the coefficient of the first degree term in $f(x)$; in other words, we have

$$V(f) > \frac{q}{2}$$

on the average. This result may be compared with a theorem of the present author (cf. [2]).

In this note we wish to present the following analogue to (1.2):

Theorem. *We have*

$$\sum_{\deg f=n} V(f)=\sum_{r=1}^{n}(-1)^{r-1}\binom{q}{r}q^{n-r} \qquad (1\leqq n<p), \tag{1.3}$$

where the summation on the left-hand side extends over all primary polynomials of degree n of the form (1.1).

As an immediate consequence of (1.3) we get

$$\sum_{\deg f=n} V(f) \geqq \frac{q^{n-1}(q+1)}{2} > \frac{q^n}{2}$$

with the equality only for $n=2$.

2. For $x \in GF(q)$, we define, as in [1, §2],

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

It is clear that $e(x+y)=e(x)e(y)$ and

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

The theorem being true for $n=1$, we may suppose that $n>1$. If we denote by M_r $(1\leqq r\leqq n)$ the number of $y \in GF(q)$ for which the equation $f(x)=y$ has precisely r distinct roots in $GF(q)$, then we have

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

Further, if $N_k(f)$ $(1\leqq k\leqq n-1)$ is the number of solutions $(x_1, x_2, \dots, x_{k+1})$ in $GF(q)$ of the system of equations

$$f(x_1)=f(x_2)=\cdots=f(x_{k+1})$$

with the condition

$$x_{j_1}\neq x_{j_2} \quad \text{if} \quad j_1\neq j_2, \tag{2.4}$$

then

$$N_k(f)=\sum_{r=1}^{n} r(r-1)\cdots(r-k)M_r,$$

and using (2.3) we get (writing N_k for $N_k(f)$)

$$V(f)=q-\frac{N_1}{2!}+\frac{N_2}{3!}-\cdots+(-1)^{n-1}\frac{N_{n-1}}{n!}. \tag{2.5}$$

On the other hand, by repeating use of (2.2), it is easy to see that

$$q^kN_k(f)=\sum_{t_1,\dots,t_k}\ \sum_{x_1,\dots,x_{k+1}}' e\Big(\sum_{j=1}^{k} t_j(f(x_j)-f(x_{j+1}))\Big),$$

where $\sum'$ indicates that the summation implied is over all x_j's that x_{k+1} satisfy (2.4).

We need the following lemma.

Lemma. *If not all of the t_j are zero, then we have*

$$\sum_{a_{n-1},\dots,a_1}\ \sum_{x_1,\dots,x_{k-1}}' e\Big(\sum_{j=1}^{k} t_j(f(x_j)-f(x_{j+1}))\Big)=0 \tag{2.6}$$

for $1\leqq k\leqq n-1$.

In fact, if the sum on the left-hand side of (2.6) were not zero, there would be certain elements $x_1, x_2, \dots, x_{k+1}$ in $GF(q)$, satisfying (2.4), such that

$$\sum_{j=1}^{k} t_j(x_j^s-x_{j+1}^s)=0$$

for $s=1, 2, \dots, n-1$, and *a fortiori* for $s=1, 2, \dots, k$. However, this is impossible since the determinant

$$\begin{vmatrix} x_1-x_2 & x_2-x_3 & \cdots & x_k-x_{k+1} \\ x_1^2-x_2^2 & x_2^2-x_3^2 & \cdots & x_k^2-x_{k+1}^2 \\ \cdots & \cdots & \cdots & \cdots \\ x_1^k-x_2^k & x_2^k-x_3^k & \cdots & x_k^k-x_{k+1}^k \end{vmatrix}=(-1)^{\frac{k(k+1)}{2}}\prod_{j_1<j_2}(x_{j_1}-x_{j_2})\neq 0.$$

Now, by virtue of the lemma, we have

$$q^k\sum_{a_{n-1},\dots,a_1} N_k(f)=q^{n-1}\cdot q(q-1)\cdots(q-k).$$

Hence we obtain finally

$$\begin{aligned}\sum_{a_{n-1},\dots,a_1} V(f)&=q^n+\sum_{a_{n-1},\dots,a_1}\ \sum_{k=2}^{n}(-1)^{k-1}\frac{N_{k-1}}{k!}\\ &=q^n+\sum_{k=2}^{n}(-1)^{k-1}\frac{q^{n-k}\cdot q(q-1)\cdots(q-k+1)}{k!}\\ &=\sum_{k=1}^{n}(-1)^{k-1}\binom{q}{k}q^{n-k},\end{aligned}$$

which completes the proof of (1.3).

3. As is easily seen from (1.3), we have

$$V(f)=c_nq+O(1) \tag{3.1}$$

on the average, where

$$c_n=1-\frac{1}{2!}+\frac{1}{3!}-\cdots+(-1)^{n-1}\frac{1}{n!}.$$

It will be interesting to note that the coefficient c_n gives, in some known cases, the actual *size* of $V(f)$, e.g. $c_1=1$, $c_2=1/2$, $c_3=2/3$, $c_4=5/8$, and $c_n>5/8$ for $n\geqq 5$. Therefore, it may be worth while to decide under what circumstances the relation (3.1) can in fact hold for a certain polynomials of higher degree. To assume the absolute irreducibility of the associated polynomial

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

in $GF[q, u, v]$ seems sufficient.

References

[1] L. Carlitz: On the number of distinct values of a polynomial with coefficients in a finite field, Proc. Japan Acad., **31**, 119–120 (1955).

[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).