74. Note on the Mean Value of V(f). II

By Saburô UCHIYAMA

Mathematical Institute, Tokyo Metropolitan University, Tokyo

(Comm. by Z. SUETUNA, M.J.A., June 13, 1955)

1. Let $GF(q)$ denote a finite field of order $q=p^{\nu}$. In the following we shall consider polynomials of the form

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

where $1<n<p$, and the number $V(f)$ of distinct values $f(x)$, $x\in GF(q)$. L. Carlitz [1][1] has proved that we have

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

where the summation is over the coefficient of the first degree term in $f(x)$. It is also known [2] that

(1.3) $$\sum_{\deg f=n} V(f)=\sum_{r=1}^{n}(-1)^{r-1}\binom{q}{r}q^{n-r}$$

or

(1.4) $$\sum_{\deg f=n} V(f)=c_nq^n+O(q^{n-1}),$$

where the summation on the left-hand side of (1.3) or (1.4) is over all polynomials of degree n of the form (1.1) and

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

In fact, the sum on the left-hand side of (1.3) is equal to the number of distinct polynomials, of degree n,

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \qquad (a_j\in GF(q))$$

having at least one linear polynomial factor in $GF[q,x]$. In this point of view the relation (1.3) is almost obvious.[2]

2. The purpose of this note is to prove the following

Theorem. *We have*

(2.1) $$\sum_{(r)} V(f)=q^{-r}\sum_{\deg f=n} V(f)+R_{n,r} \qquad (1<n<p),$$

where the summation on the left-hand side is over the coefficients a_1, $a_2,\ldots,a_{n-r-1}$ *in* $f(x)$ *and*

$$R_{n,r}=\begin{cases}0 & \text{if } r=1,\\ O(q^{\theta n}) & \text{if } r\geqq 2,\end{cases}$$

with $\theta=1-\dfrac{1}{r}$. *In particular, if* $n\geqq r(r+1)$ *then*

(2.2) $$\sum_{(r)} V(f)=c_nq^{n-r}+O(q^{n-r-1}),$$

where c_n *is the number given by* (1.5).

1) Numbers in brackets refer to the references at the end of this note.

2) Thus we may get a simple proof of (1.3). The idea was suggested to the author by K. Takeuchi.

We may prove analogous results to the inequality (2.2), summing over the coefficients $a_{t+1}, a_{t+2}, \ldots, a_{n-r-1}$ with $r+t \geqq 2$.

It is not difficult to see that the relation (2.1) holds for $r=1$: so we shall prove the theorem only for $r \geqq 2$.

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

$$e(x)=e^{2\pi i S(x)/p}, \quad S(x)=x+x^p+\cdots+x^{p^{\nu-1}}; \tag{3.1}$$

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

$$\sum_x e(xy)=\begin{cases} q & (y=0), \\ 0 & (y\neq 0). \end{cases} \tag{3.2}$$

Given a primary polynomial

$$M=M(x)=x^m+c_{m-1}x^{m-1}+\cdots+c_1x+c_0 \qquad (c_j \in GF(q)),$$

we put $c(M)=-c_{m-1}$ and

$$M^{(1)}(x)=M(x), \quad M^{(k)}(x)=\prod_\omega M(\omega x^{1/k}) \qquad (1<k<p),$$

where ω in the product runs over the kth roots of unity in $GF(q)$. As is easily seen, $M^{(k)}(x)$ is a polynomial of degree m in x, whose coefficients belong to the $GF(q)$.

Put for $1 \leqq k \leqq r$, $2 \leqq r < p$,

$$\lambda^{(k)}(M)=\lambda_\beta^{(k)}(M)=\begin{cases} 1 & (\deg M=0),^{3)} \\ e(\beta c(M^{(k)})) & (\deg M \geqq 1), \end{cases}$$

where $\beta \in GF(q)$, and

$$\lambda(M)=\prod_{k=1}^{r} \lambda^{(k)}(M).$$

Then we have $\lambda(AB)=\lambda(A)\lambda(B)$ for any two primary polynomials A and B in $GF[q,x]$.

Lemma. *Let*

$$A=A(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_0,$$
$$B=B(x)=x^m+b_{m-1}x^{m-1}+\cdots+b_0$$

be arbitrary primary polynomials in $GF[q,x]$. *In order that we have*

$$a_{m-j}=b_{m-j} \quad \textit{for} \quad j=1,2,\ldots,r,$$

it is necessary and sufficient that

$$\sum_\lambda \bar{\lambda}(A)\lambda(B) \neq 0,$$

where $\bar{\lambda}$ *denotes the conjugate complex of* λ.

In fact, this is a particular case of Lemma 1.3 in [3].

If we write

$$\tau_j(\lambda)=\sum_{\deg M=j} \lambda(M), \tag{3.3}$$

then $\tau_j(\lambda)=0$ $(j \geqq r)$ for $\lambda \neq \lambda_0=\prod \lambda_0^{(k)}$, and

$$\tau_j(\lambda)=O(q^{\theta j}), \tag{3.4}$$

where $\theta=1-\dfrac{1}{r}$.[4]

3) The functions $\lambda^{(k)}$ are substantially the same ones defined in [3, §1]. The restriction $\lambda^{(k)}(M)=0$ for $M(x)\equiv 0 \pmod{x}$, which was imposed there, is inessential. See also [4].

4) Cf. [4].

Now put

$$C_n(\lambda)=\sum_{\deg M=n}{}' \lambda(M),$$

where, in the summation $\sum'$, $M=M(x)$ runs over the distinct primary polynomials $\in GF[q,x]$ of degree n having at least one linear polynomial factor in $GF[q,x]$. Thus, as is noted in §1, $C_n(\lambda)$ is the sum of

$$\sum_{k=1}^{n}(-1)^{k-1}\binom{q}{k}q^{n-k}$$

members $\lambda(M)$, and we can write it as

$$C_n(\lambda)=\sum_{j=1}^{n}(-1)^{j-1}s_j(\lambda(P_1),\dots,\lambda(P_q))\tau_{n-j}(\lambda),$$

where P_j's are the linear primary polynomials in $GF[q,x]$ and $s_j(x_1,\dots,x_q)$ is the elementary symmetric function of $x_1,\dots,x_q$ of degree j. It is not difficult to show, using (3.4), that

$$C_n(\lambda)=O(q^{\theta n}) \qquad (\lambda\neq\lambda_0).$$

Given a set $(a_{n-1},\dots,a_{n-r})$ of elements of $GF(q)$, we put

$$f_0(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_{n-r}x^{n-r}$$

and consider the sum $\sum_\lambda\bar{\lambda}(f_0)C_n(\lambda)$. By the lemma above we have, using (3.2),

$$\begin{aligned} q^r\sum_{(r)}V(f)&=\sum_{\lambda}\bar{\lambda}(f_0)C_n(\lambda)\\ &=\sum_{k=1}^{n}(-1)^{k-1}\binom{q}{k}q^{n-k}+\sum_{\lambda\neq\lambda_0}\bar{\lambda}(f_0)C_n(\lambda)\\ &=c_nq^n+O(q^{n-1})+O(q^r\cdot q^{\theta n}). \end{aligned}$$

Hence we obtain

$$\sum_{(r)}V(f)=c_nq^{n-r}+O(q^{n-r-1})+O(q^{\theta n}),$$

which completes the proof of the theorem.

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: Note on the mean value of $V(f)$, Proc. Japan Acad., **31**, 199–201 (1955).

[3] ——: Sur les polynômes irréductibles dans un corps fini. I, Proc. Japan Acad., **30**, 523–527 (1954).

[4] ——: Sur les polynômes irréductibles dans un corps fini. II, Proc. Japan Acad., **31**, 267–269 (1955).