23. Note on the Mean Value of V(f). III

By Saburô UCHIYAMA

Mathematical Institute, Tokyo Metropolitan University, Tokyo

(Comm. by Z. SUETUNA, M.J.A., Feb. 13, 1956)

1. Let $GF(q)$ denote a 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 $V(f)$ denote the number of distinct values assumed by $f(x)$, $x\in GF(q)$. It is known [1] that

$$\sum_{\deg f=n} V(f)=c_nq^n+O(q^{n-1}), \tag{1.2}$$

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

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

In other words, the mean value of $V(f)$ over all polynomials f of degree n is asymptotically equal to c_nq.

Professor Carlitz has proposed, in a written communication to the author, a problem to evaluate the sum

$$\sum_{\deg f=n} V^2(f).$$

Here we wish to present a solution of this problem by proving the following

Theorem. *Under the Riemann hypothesis for L-functions we have*

$$\sum_{\deg f=n} V^2(f)=c_n^2q^{n+1}+O(q^n), \tag{1.3}$$

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

Thus the variance $q^{-n+1}\sum_{\deg f=n}(V(f)-c_nq)^2$ *is of order* $O(q)$.

The L-functions mentioned here were introduced and employed in [3] with certain characters defined over the polynomial ring $GF[q,x]$. For the effect of the Riemann hypothesis, see [3, Proposition 3].

2. Following the notation of [2, §3] we write

$$\lambda=\lambda^{(1)}\lambda^{(2)}\cdots\lambda^{(n-1)}$$

and put

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

the summation being over the primary polynomials in $GF[q,x]$ of degree j. Then, we have, as before,

$$\tau_j(\lambda_0)=q^j,$$

$$\tau_j(\lambda)=0 \qquad (\lambda\neq\lambda_0,\ j\geqq n-1)$$

and

(2.1) $$\tau_j(\lambda)=O(q^{j/2}) \quad (\lambda\neq\lambda_0,\ 1\leqq j<n-1)$$

by the Riemann hypothesis.

Let us consider the sum

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

where, in the summation $\sum'$, $M=M(x)$ runs over the distinct primary polynomials in $GF[q,x]$ of degree n which admit at least one linear polynomial factor in $GF[q,x]$. We have, as in [2, §3],

(2.2) $$C_n(\lambda_0)=c_nq^n+O(q^{n-1})$$

and if $\lambda\neq\lambda_0$, then

(2.3) $$C_n(\lambda)=O(q^{n/2})$$

by virtue of (2.1) (cf. [2, §3]).

3. Now, the number $V(f)$ of the distinct values assumed by

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

is equal to the number of b's in $GF(q)$ for each of which the polynomial

$$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+b$$

admits at least one linear polynomial factor in $GF[q,x]$. Thus

$$q^{n-1}V(f)=\sum_{\lambda}C_n(\lambda)\lambda(f)$$

and hence, using (2.2) and (2.3),

$$\begin{aligned}q^{2(n-1)}\sum_{\deg f=n}V^2(f)&=\sum_{\deg f=n}\sum_{\lambda,\lambda'}C_n(\lambda)C_n(\lambda')\lambda(f)\lambda'(f)\\&=\sum_{\lambda,\lambda'}C_n(\lambda)C_n(\lambda')\sum_{\deg f=n}\lambda(f)\lambda'(f)\\&=q^{n-1}\sum_{\lambda}C_n(\lambda)C_n(\bar\lambda)\\&=q^{n-1}(C_n^2(\lambda_0)+\sum_{\lambda\neq\lambda_0}|C_n(\lambda)|^2)\\&=q^{n-1}(c_n^2q^{2n}+O(q^{2n-1})),\end{aligned}$$

from which follows (1.3) at once.

Concerning the variance we have

$$\begin{aligned}\sum_{\deg f=n}(V(f)-c_nq)^2&=\sum V^2(f)-2c_nq\sum V(f)+c_n^2q^2\cdot q^{n-1}\\&=c_n^2q^{n+1}+O(q^n)-2c_nq(c_nq^n+O(q^{n-1}))+c_n^2q^{n+1}\\&=O(q^n)\end{aligned}$$

by (1.2) and (1.3). This completes the proof of the theorem.

References

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

[2] ——: Ditto. II, Proc. Japan Acad., **31**, 321–323 (1955).

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