171. *On a Multiple Exponential Sum*

By Saburô UCHIYAMA
Department of Mathematics, Hokkaidô University, Sapporo, Japan

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

Let k be a finite field with $q=p^{\nu}$ elements and $k[x_1,\cdots,x_m]$ denote the ring of polynomials in m indeterminates $x_1,\cdots,x_m$ with coefficients in k. For $\alpha\in k$, we write as usual

$$e(\alpha)=e^{2\pi i t(\alpha)/p},$$

where

$$t(\alpha)=\alpha+\alpha^{p}+\cdots+\alpha^{p^{\nu-1}}.$$

Given a polynomial $f=f(x_1,\cdots,x_m)\in k[x_1,\cdots,x_m]$ of degree n, not equivalent to a polynomial with indeterminates less than m in number, we construct the exponential sum

$$S_m(f)=\sum_{x_1,\cdots,x_m\in k} e(f(x_1,\cdots,x_m)),$$

where $x_1,\cdots,x_m$ run independently over all elements of k. It is assumed throughout that $1<n<p$.

Recently L. Carlitz and S. Uchiyama [1] have proved the inequality

$$(1)\qquad |S_1(f)|\leqq(n-1)q^{\frac{1}{2}},$$

which can be used, as we shall see, to obtain

$$(2)\qquad S_m(f)=O(q^{m-\frac{1}{2}}),$$

in general. Here and henceforth the constant implied by O depends only upon m and n. The inequality (2) may be compared with a result of S.-H. Min [3], who proved that

$$S_m(f)=O(q^{m\left(1-\frac{1}{n}\right)})$$

for a certain class of polynomials $f\in k[x_1,\cdots,x_m]$ of degree $n\geqq 2m$. Also, in the case of $m=2$, L.-K. Hua and S.-H. Min [2] proved that

$$S_2(f)=O(q^{2-\frac{2}{n}})$$

and that, if $n=3$, then

$$S_2(f)=O(q^{\frac{5}{4}}).$$

This last inequality is better than that in (2) with $m=2$, $n=3$.

Our proof of (2) is highly simple except for the use of the inequality (1). In fact, denoting by l the degree of the polynomial $f(x_1,\cdots,x_m)$ with respect to x_m, we write

$$f(x_1,\cdots,x_m)=\sum_{j=0}^{l} g_j x_m^{l-j},$$

where the $g_j=g_j(x_1,\cdots,x_{m-1})$ are polynomials independent of x_m. By the assumption, there exists, among the g_j $(0\leqq j\leqq l-1)$, one at least that is not identically zero in $k[x_1, \cdots, x_{m-1}]$, and it follows from this that the number of solutions $(x_1, \cdots, x_{m-1})$ in k of the simultaneous equations

(3) $$g_0 = g_1 = \cdots = g_{l-1} = 0$$

is $O(q^{m-2})$. Now, denoting by E the set of the solutions $(x_1, \cdots, x_{m-1})$ in k of (3), we thus obtain

$$\begin{aligned} S_m(f) &= \sum_{x_1, \cdots, x_m \in k} e(f(x_1, \cdots, x_m)) \\ &= \sum_{x_m \in k} \sum_{(x_1, \cdots, x_{m-1}) \in E} + \sum_{x_m \in k} \sum_{(x_1, \cdots, x_{m-1}) \notin E} \\ &= O(q^{m-2}) \cdot q + (q^{m-1} - O(q^{m-2})) \cdot O(q^{\frac{1}{2}}) \\ &= O(q^{m-\frac{1}{2}}), \end{aligned}$$

which completes the proof of (2).

We note that the exponent $m - \dfrac{1}{2}$ of q on the right-hand side of (2) is independent of n, the degree of the polynomial f.

References

[1] L. Carlitz and S. Uchiyama: Bounds for exponential sums, to appear in Duke Math. Jour.

[2] L.-K. Hua and S.-H. Min: On a double exponential sum, Science Reports of National Tsing Hua University, Ser. A, Mathematical, Physical and Engineering Sciences, **4** (1947).

[3] S.-H. Min: On systems of algebraic equations and certain multiple exponential sums, Quart. Jour. Math., Oxford Ser., **18** (1947).