# 26. *On Certain Numerical Invariants of Mappings over Finite Fields. V*

By Takashi ONO

Department of Mathematics, Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1981)

**Introduction.** This is a continuation of our paper [2] which will be referred to as (I) in this paper.[1] Let $k$ be a finite field with $q$ elements: $k=\boldsymbol{F}_q$, $\chi$ be a non-trivial character of the multiplicative group $k^\times$ (extended by $\chi(0)=0$) and $f$ be a function $k\to k$. We shall put

$$S_f(\chi)=\sum_{x\in k}\chi(f(x)).$$

Consider the polynomial

$$f(x)=x^m+Ax+B,\quad A,\ B\in k,\quad m\geqq 3. \tag{0.1}$$

Denote by $\Delta(A, B)$ the discriminant of $f(x)$, i.e.

$$\Delta(A, B)=(-1)^{m-1}(m-1)^{m-1}A^m+m^mB^{m-1}. \tag{0.2}$$

We assume that $(q, m)=(q, m-1)=1$. The purpose of the paper is to prove the following

**Theorem.** *Let $d$ be an integer $\geqq 2$ such that $(q, d)=(d, m)=(d, m-2)=1$ and let $\chi$ be a non-trivial character of $k^\times$ of exponent $d$. Then, there is a polynomial $f(x)=x^m+Ax+B$ with $A\neq 0$, $B\neq 0$, $\Delta(A, B)\neq 0$ such that*

$$|S_f(\chi)|<\kappa\sqrt{q}, \tag{0.3}$$

*where $\kappa=\sqrt{3}$ if $m=3$ and $\kappa=\sqrt{2(m-1)}$ if $m\geqq 4$.*

**Remark 1.** By the well-known theorem[2] we know that

$$|S_f(\chi)|\leqq(m-1)\sqrt{q} \tag{0.4}$$

for any polynomial $f$ of degree $m$ with $(d, m)=1$.

**Remark 2.** When $d=2$, $m$ can be any odd integer $\geqq 3$ and since there is only one quadratic character $\chi$ we have the relation

$$N=q+S_f(\chi),$$

where $N$ denotes the number of solutions $(x, y)\in k^2$ of the equation

$$y^2=x^m+Ax+B. \tag{0.5}$$

Therefore, our Theorem means that among hyperelliptic curves of type (0.5) with $A\neq 0$, $B\neq 0$, $\Delta(A, B)\neq 0$, there is a curve which satisfies the inequality

$$|N-q|<\kappa\sqrt{q} \tag{0.6}$$

*where $\kappa=\sqrt{3}$ if $m=3$ and $\kappa=\sqrt{2(m-1)}$ if $m\geqq 5$* ($m$: odd). A similar remark can be made for the case $d=3$.

1) For example, we mean by (I.2.3) the item (2.3) in (I).

2) See Theorem 2C on p. 43 of [1].

§1. **Method of the proof.** We first remind the reader the equality

(I.1.11) $$\sigma_F(\chi)=q^{r-1}(q-1)\rho_F(\chi),$$

where $Y$ is a vector space over $k$ of dimension $r$, $F$ is a mapping from a finite set $X$ into $Y$, $\chi$ is a non-trivial character of $k^\times$ and $\sigma_F(\chi)$, $\rho_F(\chi)$ are invariants defined as follows. First, for a function $f: X\to k$, we write

(1.1) $$S_f(\chi)=\sum_{x\in X}\chi(f(x)).$$

Next, the mapping $F: X\to Y$ induces a function $F_\lambda: X\to k$ by $F_\lambda=\lambda\circ F$ for each linear form $\lambda\in Y^*$. We then put

(1.2) $$\sigma_F(\chi)=\sum_{\lambda\in Y^*}|S_{F_\lambda}(\chi)|^2.$$

Now, for non-zero vectors $u, v\in Y$, we write $u\| v$ when they are proportional to each other, i.e. when there is an $a\in k^\times$ such that $v=au$. In this situation, we write $a=v:u$. Finally, we put

(1.3) $$\rho_F(\chi)=\sum_{(x,y)\in P}\chi(F(x):F(y)),$$

where

(1.4) $$P=\Big\{(x, y)\in k^2;\ F(x)\neq 0,\ F(y)\neq 0,\ F(x)\| F(y)\Big\}.$$

Since we consider a fixed character $\chi$ of exponent $d$, we often write $S_f$, $\sigma_F$, $\rho_F$ without $\chi$.

To prove our Theorem, we first consider the case where $X=k$, $Y=k^3$ and $F(x)=(x^m, x, 1)$. Since $F(x)\| F(y)$ if and only if $x=y$, we have

(1.5) $$\rho_F=q,$$

and, by (I.1.11), we get

(1.6) $$\sigma_F=q^3(q-1).$$

Identifying the linear form $\lambda\in Y^*$ with $\lambda=(\alpha,\beta,\gamma)\in k^3$ we can write $F_\lambda(x)=\alpha x^m+\beta x+\gamma$. We shall consider in $Y^*$ the following five subsets:

$$\begin{aligned}
\Lambda_{\mathrm{I}} &=\{\lambda=(\alpha,\beta,0);\ \alpha,\beta\in k\},\\
\Lambda_{\mathrm{II}} &=\{\lambda=(\alpha,0,\gamma);\ \alpha,\gamma\in k\},\\
\Lambda_{\mathrm{III}} &=\{\lambda=(\alpha,0,0);\ \alpha\in k\},\\
\Lambda_{\mathrm{IV}} &=\{\lambda=(0,\beta,\gamma);\ \beta,\gamma\in k^\times\},\\
\Lambda_{\mathrm{V}} &=\{\lambda=(\alpha,\beta,\gamma);\ \alpha,\beta,\gamma\in k^\times\}.
\end{aligned}$$

If we put

(1.7) $$\sigma_j=\sum_{\lambda\in\Lambda_j}|S_{F_\lambda}|^2,\qquad I\leqq j\leqq V,$$

we have

(1.8) $$\sigma_F=\sigma_{\mathrm{I}}+\sigma_{\mathrm{II}}-\sigma_{\mathrm{III}}+\sigma_{\mathrm{IV}}+\sigma_{\mathrm{V}}.$$

Among these terms, we have $\sigma_{\mathrm{III}}=\sum_{\alpha\in k}|\sum_{x\in k}\chi(\alpha x^m)|^2=0$ since $\chi$ is non-trivial and $(d, m)=1$, and $\sigma_{\mathrm{IV}}=\sum_{(\beta,\gamma)\in(k^\times)^2}|\sum_{x\in k}\chi(\beta x+\gamma)|^2=0$ since $\beta\neq 0$. Therefore (1.8) becomes

(1.9) $$\sigma_F=\sigma_{\mathrm{I}}+\sigma_{\mathrm{II}}+\sigma_{\mathrm{V}}.$$

In the next two sections, we shall compute the first two terms of (1.9) explicitly.

§ 2. **Computation of $\sigma_{\mathrm{I}}$.** To find

(2.1) $$\sigma_{\mathrm{I}}=\sum_{(\alpha,\beta)\in K^2}|\sum_{x\in k}\chi(\alpha x^m+\beta x)|^2,$$

we use the equality (I.1.11) with $X=k$, $Y=k^2$ and $F(x)=(x^m, x)$. We see easily that

(2.2) $$F(x)\|F(y)\Leftrightarrow y=ax, \quad a^{m-1}=1, \quad x, y\in k^{\times}.$$

Put $\delta'=(m-1, q-1)$ and $\omega=g^{(q-1)/\delta'}$ where $g$ is a generator of the cyclic group $k^{\times}$. Then we have the disjoint union

(2.3) $$\begin{aligned} &P=P_0\cup P_1\cup\cdots\cup P_{\delta'-1} && \text{with} \\ &P_i=\{(x, \omega^i x),\ x\in k^{\times}\}, && 0\leqq i\leqq\delta'-1. \end{aligned}$$

From this we have

$$\rho_F=\sum_{(x,y)\in P}\chi(F(x): F(y))=\sum_{i=0}^{\delta'-1}\sum_{P_i}\chi(\omega^{-i})=(q-1)\sum_{i=0}^{\delta'-1}\chi(\omega^{-i}),$$

and so

(2.4) $$\rho_F=\begin{cases}\delta'(q-1), & \text{if } \chi(\omega)=1,\\ 0, & \text{if } \chi(\omega)\neq 1.\end{cases}$$

Hence we have

(2.5) $$\sigma_{\mathrm{I}}=\begin{cases}\delta' q(q-1)^2, & \text{if } \chi(\omega)=1,\\ 0, & \text{if } \chi(\omega)\neq 1.\end{cases}$$

§ 3. **Computation of $\sigma_{\mathrm{II}}$.** To find

(3.1) $$\sigma_{\mathrm{II}}=\sum_{(\alpha,\gamma)\in k^2}\left|\sum_{x\in k}\chi(\alpha x^m+\gamma)\right|^2,$$

we use the equality (I.1.11) with $X=k$, $Y=k^2$ and $F(x)=(x^m, 1)$. We see that

(3.2) $$F(x)\|F(y)\Leftrightarrow y^m=x^m, \qquad x, y\in k.$$

Hence, when $x\neq 0$, there are $\delta''$ $y$'s with $\delta''=(m, q-1)$. If we put $\eta=g^{(q-1)/\delta''}$, then we have the disjoint union

(3.3) $$\begin{aligned} &P=\{(0, 0)\}\cup P_0\cup P_1\cup\cdots\cup P_{\delta''-1} && \text{with} \\ &P_i=\{(x, \eta^i x),\ x\in k^{\times}\}, && 0\leqq i\leqq\delta''-1. \end{aligned}$$

Since $\chi(F(x): F(y))=1$ for $(x, y)\in P$, we have

(3.4) $$\rho_F=1+(q-1)\delta''$$

and hence

(3.5) $$\sigma_{\mathrm{II}}=q(q-1)(1+(q-1)\delta'').$$

§ 4. **$\sigma_{\mathrm{V}}$, $\sigma_{\mathrm{V}}^{*}$ and $\sigma_{\mathrm{V}}^{**}$.** We consider here the most interesting sum

(4.1) $$\sigma_{\mathrm{V}}=\sum_{(\alpha,\beta,\gamma)\in(k^{\times})^3}\left|\sum_{x\in k}\chi(\alpha x^m+\beta x+\gamma)\right|^2.$$

On putting

(4.2) $$A=\frac{\beta}{\alpha}, \qquad B=\frac{\gamma}{\alpha},$$

we have

(4.3) $$\sigma_{\mathrm{V}}=(q-1)\sigma_{\mathrm{V}}^{*} \quad \text{with} \quad \sigma_{\mathrm{V}}^{*}=\sum_{(A,B)\in(k^{\times})^2}\left|\sum_{x\in k}\chi(x^m+Ax+B)\right|^2.$$

Let the group $k^{\times}$ act on the set $(k^{\times})^2$ by the rule:

(4.4) $$(A, B)t=(At^{m-1}, Bt^m), \qquad t \in k^\times.$$

Clearly, the stability group at each point $(A, B)$ is trivial and so each orbit consists of $q-1$ points and there are $q-1$ orbits in $(k^\times)^2$. Since $\sum_{x\in k}\chi(x^m+At^{m-1}x+Bt^m)=\chi(t)^m\sum_{x\in k}\chi(x^m+Ax+B)$, if we call $(A_i, B_i)$, $1\leqq i\leqq q-1$, representatives of orbits, we have

(4.5) $$\sigma_V^* =(q-1)\sigma_V^{**} \quad \text{with} \quad \sigma_V^{**}=\sum_{i=1}^{q-1}|S_{f_i}|^2$$

where $f_i(x)=x^m+A_ix+B_i$.

From (1.6), (1.9), (2.5), (3.5), (4.3), (4.5), it follows that

(4.6) $$\sigma_V^{**}=\begin{cases} q(q+1-\delta'-\delta''), & \text{if } \chi(\omega)=1, \\ q(q+1-\delta''), & \text{if } \chi(\omega)\neq 1. \end{cases}$$

§5. **End of the proof.** Let $\Delta=\Delta(A, B)$ be the discriminant of $x^m+Ax+B$, $A\neq 0$, $B\neq 0$. By (0.2), it is clear that $\Delta(A, B)=0$ if and only if $\Delta((A, B)t)=0$ for all $t\in k^\times$. Hence the vanishing of $\Delta$ is a property of an orbit. We call an orbit singular (resp. non-singular) if it contains a point $(A, B)$ such that $\Delta(A, B)=0$ (resp. $\Delta(A, B)\neq 0$). As is easily verified, we have $\Delta(A, B)\neq 0$ if and only if the affine plane curve $y^d=x^m+Ax+B$ is non-singular.[3] There is always a singular orbit, say, the one which contains the point $((-1)^m m, m-1)$. We claim that there is only one singular orbit. In fact, assume that $\Delta(A, B)=(-1)^{m-1}(m-1)^{m-1}A^m+m^mB^{m-1}=0$. Then, a simple computation shows that $(A, B)=((-1)^m m, m-1)t$ with $t=(-1)^m mB/(m-1)A$, which means that every singular curve is in the orbit of the curve $((-1)^m m, m-1)$. From now on, we assume that $q-2$ curves $(A_i, B_i)$, $1\leqq i\leqq q-2$, are non-singular and the last curve $(A_{q-1}, B_{q-1})=((-1)^m m, m-1)$ is singular.

We now consider the sum

(5.1) $$S_{f_{q-1}}=\sum_{x\in k}\chi(f_{q-1}(x)), \qquad f_{q-1}(x)=x^m+(-1)^m mx+(m-1).$$

First, note the factorization:

(5.2) $f_{q-1}(x)=(x-e)^2h(x)$, where $e=1$ if $m$ is odd, $e=-1$ if $m$ is even and $h(x)=x^{m-2}+2ex^{m-3}+3x^{m-4}+\cdots+(m-2)ex+(m-1)$.

Therefore, we have

(5.3) $$S_{f_{q-1}}=S_h(\chi)-\chi(h(e)), \qquad h(e)=(1/2)m(m-1)\neq 0.$$

Since $\chi$ is of exponent $d$ and $(d, m-2)=1$, by the well-known result (Theorem 2C on p. 43 of [1]) we have

(5.4) $$|S_h(\chi)|\leqq(m-3)\sqrt{q}.$$

On the other hand, call $f(x)=x^m+Ax+B$ one of the $f_i(x)$'s, $1\leqq i\leqq q-2$, such that $|S_f|=\inf|S_{f_i}|$. Then, from (4.5), (5.3), (5.4), we get

(5.5) $$\begin{aligned}\sigma_V^{**}&\geqq(q-2)|S_f|^2+|S_{f_{q-1}}|^2\geqq(q-2)|S_f|^2+(|S_h(\chi)|-1)^2\\ &\geqq(q-2)|S_f|^2-2|S_h(\chi)|+1\geqq(q-2)|S_f|^2-2(m-3)\sqrt{q}+1,\end{aligned}$$

3) When $\Delta(A, B)=0$, the point $((-1)^m mB/(m-1)A, 0)$ is the only singular point of the affine curve $y^d=x^m+Ax+B$.

which implies that

$$|S_f(\chi)| \leqq \sqrt{\frac{\sigma_V^{**} + 2(m-3)\sqrt{q} - 1}{q-2}}.\text{[4]} \tag{5.6}$$

Note that $\sigma_V^{**} \leqq q^2$ since $\delta'$, $\delta'' \geqq 1$ and that $q-2 \geqq q/3$, $q^{3/2} > 3$ since $q \geqq 3$. On substituting the values of $\sigma_V^{**}$ of (4.6) in (5.6) we obtain the inequality (0.3) of Theorem.

## References

[1] Schmidt, W. M.: Equations over finite fields. Lect. Notes in Math., vol. 536, Springer-Verlag (1976).

[2] Ono, T.: On certain numerical invariants of mappings over finite fields. I. Proc. Japan Acad., **56**A, 342–347 (1980).

4) (5.6) is a generalization of (I.3.30).