80. On Certain Numerical Invariants of Mappings over Finite Fields. I

By Takashi ONO
Department of Mathematics, Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1980)

Introduction. Let X be a finite set, Y be a vector space over a finite field $K=\boldsymbol{F}_q$ and F be a mapping $X\to Y$. Using a non-trivial multiplicative character χ of K, we shall define invariants $\rho_F(\chi)$ and $\sigma_F(\chi)$, and prove a simple relation (1.11) between them. If $\dim Y=1$, then $\rho_F(\chi)$ is nothing but the square of the absolute value of the character sum

$$S_F(\chi)=\sum_{x\in X}\chi(F(x)).$$

When X is also a vector space over K, F is a quadratic mapping and χ is a quadratic character, then the computation of $\sigma_F(\chi)$ is generally much easier than that of $\rho_F(\chi)$.*) On the other hand, when the degree of a polynomial mapping F is higher than 2, then, even in the case of the quadratic character, $\sigma_F(\chi)$ involves usually difficult ingredients such as the trace of the Frobenius endomorphism; however, there are cases where $\rho_F(\chi)$ can be computed easily. In such a case, we can use the equality (1.11) to get some informations about the ingredients of $\sigma_F(\chi)$. We shall discuss here a simple example of this type.

§1. Statement of a theorem. Let K be the finite field with q elements: $K=\boldsymbol{F}_q$ and χ be a non-trivial character of the multiplicative group $K^\times$ of K. We extend χ to K by putting $\chi(0)=0$. Let X be a finite set, Y be a vector space over K of finite dimension $m\geqq 1$ and F be any mapping $X\to Y$. For non-zero vectors $u, v\in Y$, we write $u\| v$ when they are propotional to each other, i.e. when there is an $a\in K^\times$ such that $v=au$. When that is so, we write $a=v:u$. Hence, we have $(u:v)(v:u)=1$ and $\chi(u:v)=\bar{\chi}(v:u)$ where $\bar{\chi}$ is the complex conjugate of χ. Denote by P the set of pairs $(x, y)\in X^2$ such that $F(x)\neq 0$, $F(y)\neq 0$ and $F(x)\| F(y)$. In this paper, we shall be interested in the number

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

(1.2) **Remark.** When P is empty, i.e. when $F(x)=0$ for all $x\in X$, we simply put $\rho_F(\chi)=0$.

(1.3) **Remark.** $\rho_F(\chi)$ is an invariant in the sense that, for another

*) In the second paper of the same title as this one, we shall obtain explicit values of the invariants for quadratic mappings arising from pairs of quadratic forms, algebras with involution, Hopf maps, etc.

mapping $G: X \to Y$, and have $\rho_F(\chi)=\rho_G(\chi)$ whenever we have a relation $G\alpha=\beta F$ where α is a bijection of the set X with itself and β is an automorphism of the vector space Y.

(1.4) **Remark.** When $m=1$, for $u\neq 0$, $v\neq 0$ in $Y=K$, we have always $u\| v$ and $\chi(u:v)=\chi(u)\bar{\chi}(v)$. Hence, (1.1) becomes

$$\rho_F(\chi)=|S_F(\chi)|^2$$

where

(1.5) $S_F(\chi)=\sum_{x\in X}\chi(F(x))$,

the character sum of the function $F: X\to K$.

Back to a general mapping $F: X\to Y$, denote by Y^* the dual space of Y. For each $\lambda\in Y^*$, we get a function $F_\lambda: X\to K$ by putting

$$F_\lambda(x)=\lambda(F(x)).$$

Using (1.5), we put

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

(1.7) **Remark.** $\sigma_F(\chi)$ is an invariant in the same sense as (1.3).

(1.8) **Remark.** When $F(x)=0$ for all $x\in X$, we have $\sigma_F(\chi)=0$.

(1.9) **Remark.** When $m=1$, by (1.4), (1.6), we have

(1.10) $\sigma_F(\chi)=(q-1)\rho_F(\chi)$.

In the general case, we shall prove the following

(1.11) **Theorem.** $\sigma_F(\chi)=q^{m-1}(q-1)\rho_F(\chi)$, $m=\dim Y$.

§ 2. **Proof of the theorem.** We begin with a lemma:

(2.1) **Lemma.** *Let V be a vector space over $K=F_q$ of dimension $r\geqq 1$ and ξ,η be non-zero linear forms on V: $\xi,\eta\in V^*$. Then, we have*

$$\sum_{x\in V}\chi(\xi(x))\bar{\chi}(\eta(x))=\begin{cases}0, & \xi\nparallel\eta,\\ q^{r-1}(q-1)\chi(\xi:\eta), & \xi\| \eta,\end{cases}$$

Proof. Assume first that $\xi\|\eta$. Hence, we have $\xi=c\eta$, $c=\xi:\eta$. We have then

$$\sum_{x\in V}\chi(\xi(x))\bar{\chi}(\eta(x))=\chi(c)\sum_{x\in V}|\chi(\eta(x))|^2=\chi(c)\sum_{\eta(x)\neq 0}1=\chi(c)(q^r-q^{r-1}),$$

since $\operatorname{Ker}\eta$ contains q^{r-1} elements. Next, assume that $\xi\nparallel\eta$. Since then $\operatorname{Ker}\xi$ and $\operatorname{Ker}\eta$ span V, we have $\dim(\operatorname{Ker}\xi\cap\operatorname{Ker}\eta)=r-2$. One can find a basis $\{e_1,\cdots,e_r\}$ of V such that the first $r-2$ e_i's span $\operatorname{Ker}\xi\cap\operatorname{Ker}\eta$ and that $\xi(e_{r-1})=\eta(e_r)=1$, $\xi(e_r)=\eta(e_{r-1})=0$. Write a vector $x\in V$ as $x=x_1e_1+\cdots+x_re_r$, $x_i\in K$. Then, we have

$$\begin{aligned}\sum_{x\in V}\chi(\xi(x))\bar{\chi}(\eta(x))&=\sum_{(x_1,\cdots,x_r)}\chi(x_{r-1})\bar{\chi}(x_r)\\ &=\sum_{(x_1,\cdots,x_{r-2})}\Big(\sum_{a\in K}\chi(a)\Big)\Big(\sum_{b\in K}\bar{\chi}(b)\Big)=0,\end{aligned}$$

since χ is non-trivial. Q.E.D.

Proof of (1.11). From (1.6), it follows that

$$\begin{aligned}\sigma_F(\chi)&=\sum_{\lambda\in Y^*}|S_{F_\lambda}(\chi)|^2=\sum_{\lambda\in Y^*}\sum_{(x,y)\in X^2}\chi(F_\lambda(x))\bar{\chi}(F_\lambda(y))\\ &=\sum_{(x,y)}\sum_{\lambda\in Y^*}\chi(\lambda(F(x)))\bar{\chi}(\lambda(F(y))),\end{aligned}$$

where we only have to sum over (x, y) such that $F(x)\neq 0$, $F(y)\neq 0$. By applying (2.1) to the inner sum, with $V=Y^*$, $x=\lambda$, $\xi=F(x)$, $\eta=F(y)$ and $r=m$, we have

$$\sum_{\lambda\in Y^*}\chi(\lambda(F(x)))\bar{\chi}(\lambda(F(y)))=\begin{cases}0, & \text{if } F(x)\nparallel F(y),\\ q^{m-1}(q-1)\chi(F(x):F(y)), & \text{if } F(x)\parallel F(y),\end{cases}$$

and so

$$\sigma_F(\chi)=q^{m-1}(q-1)\sum_{(x,y)\in P}\chi(F(x):F(y)),$$

which proves (1.11).

(2.2) **Remark.** Notation being as above, let L be an injective linear mapping of Y into another vector space Z over K. We may then speak of $\rho_{L\circ F}(\chi)$ and $\sigma_{L\circ F}(\chi)$. By definition (1.1), since L is injective, we see easily that $\rho_{L\circ F}(\chi)=\rho_F(\chi)$ which shows that $\rho_F(\chi)$ is independent of the embedding of the image of the mapping F. As for $\sigma_F(\chi)$, by (1.11) we get

$$\sigma_{L\circ F}(\chi)=q^{l-m}\sigma_F(\chi), \qquad \text{where } l=\dim Z.$$

§ 3. An application. Let $K=F_q$, q: odd. In this section, we consider only quadratic character χ. Since there is only one such character, we simply write ρ_F, σ_F instead of $\rho_F(\chi), \sigma_F(\chi)$, respectively. Let X be the field K and f be a function $K\to K$. Since χ takes values ± 1, the character sum

(3.1) $\quad S_f=\sum_{x\in K}\chi(f(x))$

is an integer. Denote by N the number of solutions $(x, y)\in K^2$ of the equation

$$y^2=f(x).$$

Since, for each $x\in X$, the number of y's is $1+\chi(f(x))$, we have

(3.2) $\quad N=q+S_f.$

The following formulas of S_f for linear and quadratic functions on $X=K$ are well-known and easy to prove.

(3.3) $\quad S_f=\sum_{x\in K}\chi(ax+b)=\begin{cases}0, & \text{if } a\neq 0,\\ q\chi(b), & \text{if } a=0.\end{cases}$

(3.4) $\quad S_f=\sum_{x\in K}\chi(ax^2+bx+c)=\begin{cases}-\chi(a), & \text{if } b^2-4ac\neq 0,\\ \chi(a)(q-1), & \text{if } b^2-4ac=0.\end{cases}$

From now on, we assume that q is not divisible by 3, too.

Consider the mapping $F: K\to K^3$ given by

(3.5) $\quad F(x)=(x^3, x, 1).$

Identifying the linear form $\lambda\in(K^3)^*$ with $\lambda=(\alpha, \beta, \gamma)\in K^3$, we have

$$F_\lambda(x)=\alpha x^3+\beta x+\gamma.$$

From (3.5), we have

$$F(x)\parallel F(y)\Longleftrightarrow x=y, \qquad x, y\in K.$$

Therefore, by (1.1), (1.11), we have

(3.6) $\quad \rho_F=q, \qquad \sigma_F=\sum S_{F_\lambda}^2=q^3(q-1).$

When $\alpha=0$, we have, by (3.3),

$$S_{F_\lambda}=\sum_{x\in K}\chi(\beta x+\gamma)=\begin{cases}0, & \text{if } \beta\neq 0,\\ q\chi(\gamma), & \text{if } \beta=0,\ \gamma\neq 0,\\ 0, & \text{if } \beta=\gamma=0,\end{cases}$$

and so $\sum_{\alpha=0}S_{F_\lambda}^2=q^2(q-1)$. Then, from (3.6), we get

(3.7) $\sum_{\alpha\neq 0}S_{F_\lambda}^2=q^2(q-1)^2$.

As for the terms for which $\alpha\neq 0$, we split the sum (3.7) into two parts

(3.8) $\sum_{\alpha\neq 0}S_{F_\lambda}^2=(\mathrm{I})+(\mathrm{II})$,

where (I) (resp. (II)) is the sum over $\lambda=(\alpha,\beta,\gamma)$ with $4\beta^3+27\alpha\gamma^2\neq 0$ (resp. $4\beta^3+27\alpha\gamma^2=0$). For $\lambda=(\alpha,\beta,\gamma)$, $\alpha\neq 0$, we put

(3.9) $A=\beta/\alpha$, $B=\gamma/\alpha$, $\Delta=4A^3+27B^2$.

Then we have

$$S_{F_\lambda}=\chi(\alpha)\sum_{x\in K}\chi(x^3+Ax+B)$$

and it follows that

(3.10) $(\mathrm{II})=(q-1)(\mathrm{II})^*$ with $(\mathrm{II})^*=\sum_{\substack{(A,B)\in K^2\\ \Delta=0}}\left(\sum_{x\in K}\chi(x^3+Ax+B)\right)^2$.

Since $\sum\chi(x^3)=\sum\chi(x)=0$ and $\Delta=0$, we may assume that $A\neq 0$, $B\neq 0$ in (3.10). The condition $\Delta=4A^3+27B^2=0$ implies that $\chi(A)=\chi(-3)$ and that

(3.11) $A=-3C^2$, $B=+2C^3$ for some $C\in K^\times$.

Therefore, we have

$$\begin{aligned}(\mathrm{II})^*&=\sum_{C\neq 0}\left(\left(\sum_{x\in K}\chi(x^3-3C^2x+2C^3)\right)^2\right)\\ &=\sum_{C\neq 0}\left(\left(\sum_{x\in K}\chi((x-C)^2(x+2C))\right)^2\right)\\ &=\sum_{C\neq 0}\left(\left(\sum_{x\neq C}\chi(x+2C)\right)^2\right).\end{aligned}$$

Since we have $\sum_{x\neq C}\chi(x+2C)=\sum_x\chi(x+2C)-\chi(3C)=-\chi(3C)$, we get $(\mathrm{II})^*=(q-1)$. In view of (3.8), (3.10), we have

(3.12) $(\mathrm{I})=\sum_{\alpha\neq 0,\beta\neq 0}S_{F_\lambda}^2=(q-1)^2(q^2-1)$.

When $\alpha\neq 0$ and $\Delta=4A^3+27B^2\neq 0$, the equation

(3.13) $y^2=\alpha x^3+\beta x+\gamma=\alpha(x^3+Ax+B)$

represents an elliptic curve E_λ defined over $K=F_q$.*) Consider E_λ in the projective plane and denote by ν_λ the number of points of E_λ rational over K. Since (3.13) has only one point at infinity, we see from (3.1), (3.2) that

(3.14) $\nu_\lambda=q+1+S_{F_\lambda}$.

*) As for basic facts on elliptic curves, see J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc., **41**, 193–291 (1966).

According to custom, we denote by a_λ the trace of the Frobenius endomorphism of E_λ. We have

(3.15) $\nu_\lambda = q+1-a_\lambda$,

which implies that

(3.16) $S_{F_\lambda} = -a_\lambda$.

The inequality

(3.17) $|a_\lambda| \leqq 2\sqrt{q}$

is famous, but we do not use it here. By (3.16), one can modify (3.12) as

(3.18) $(\mathrm{I}) = (q-1)(\mathrm{I})^*$ with $(\mathrm{I})^* = \sum_{\lambda=(A,B)} a_\lambda^2 = (q-1)(q^2-1)$,

where we identified $\lambda=(1, A, B)$ with (A, B). Now, put

(3.19) $M = \{\lambda=(A,B) \in K^2;\ \Delta = 4A^3+27B^2 \neq 0\}$.

The group $K^\times$ acts on M by

(3.20) $c(\lambda) = \lambda' = (c^4A, c^6B)$ when $\lambda=(A,B)$.

As one verifies easily, the elliptic curves E_λ and $E_{\lambda'}$ are isomorphic over K and so we have $S_{F_\lambda} = S_{F_{\lambda'}}$. Denote by H_λ the isotropy group at $\lambda=(A,B)$: $H_\lambda = \{c \in K^\times;\ c(\lambda)=\lambda\}$. It is easy to see that

$$(3.21)\quad H_\lambda = \begin{cases} \{c \in K^\times;\ c^4=1\}, & \text{if } A\neq 0,\ B=0, \\ \{c \in K^\times;\ c^6=1\}, & \text{if } A=0,\ B\neq 0, \\ \{\pm 1\}, & \text{if } A\neq 0,\ B\neq 0. \end{cases}$$

Let us split the sum $(\mathrm{I})^*$ in (3.18) into 3 parts according to the structure of H_λ in (3.21):

(3.22) $(\mathrm{I})^* = (\mathrm{I})_1 + (\mathrm{I})_2 + (\mathrm{I})_3$

where $(\mathrm{I})_1$ is the sum over $\lambda=(A,B)$ with $A\neq 0$, $B=0$, $(\mathrm{I})_2$ is the sum over $\lambda=(A,B)$ with $A=0$, $B\neq 0$ and $(\mathrm{I})_3$ is the sum over $\lambda=(A,B)$ with $A\neq 0$, $B\neq 0$.

$(\mathrm{I})_1$ and $(\mathrm{I})_2$ can be computed explicitly by using (3.4):

$$\begin{aligned}(\mathrm{I})_1 &= \sum_{A\neq 0}\Big(\sum_{x\in K}\chi(x^3+Ax)\Big)^2 = \sum_{A\in K}\sum_{x,y\in K}\chi(x^3+Ax)\chi(y^3+Ay) \\ &= \sum_{x,y}\chi(xy)\sum_{A}\chi(A^2+(x^2+y^2)A+x^2y^2) \\ &= -\sum_{x,y}\chi(x)\chi(y)+q\sum_{x^2=y^2}\chi(xy) \\ &= -(\textstyle\sum\chi(x))^2+q\sum_{y=\pm x}\chi(xy) = q(q-1)(1+\chi(-1)).\end{aligned}$$

Hence we have

$$(3.23)\quad (\mathrm{I})_1 = \begin{cases} 2q(q-1), & \text{if } q\equiv 1 \pmod 4, \\ 0, & \text{if } q\equiv 3 \pmod 4.\ ^{*)} \end{cases}$$

Similarly, we have

$$(3.24)\quad (\mathrm{I})_2 = \begin{cases} 2q(q-1), & \text{if } q\equiv 1 \pmod 3, \\ 0, & \text{if } q\equiv 2 \pmod 3. \end{cases}$$

From (3.22)–(3.24), it follows that

---

*) This, of course, implies that all $a_\lambda=0$, $\lambda=(A,0)$, when $q\equiv 3 \pmod 4$. The similar remark may be applied to (3.24).

$$(3.25)\quad (\mathrm{I})_3=\begin{cases}(q-1)(q^2-4q-1), & \text{if } q\equiv 1 \pmod{12},\\ (q-1)(q^2-2q-1), & \text{if } q\equiv 5 \text{ or } 7 \pmod{12},\\ (q-1)(q^2-1), & \text{if } q\equiv 11 \pmod{12}.\end{cases}$$

Now, the group $K^\times$ acts on the set

$$(3.26)\quad M^*=\{\lambda=(A,B)\in (K^\times)^2;\ \Delta=4A^3+27B^2\neq 0\}$$

and we have $a_\lambda=a_{\lambda'}$ when λ and λ' belong to the same orbit. Denote by $M^\sharp$ the quotient space of M^* by the action of $K^\times$. Since each orbit consists of $(q-1)/2$ elements by (3.21), it follows from (3.25) that

$$(3.27)\quad \sum_{M^\sharp} a_\lambda^2=\begin{cases}2(q^2-4q-1), & \text{if } q\equiv 1 \pmod{12},\\ 2(q^2-2q-1), & \text{if } q\equiv 5 \text{ or } 7 \pmod{12},\\ 2(q^2-1), & \text{if } q\equiv 11 \pmod{12}.\end{cases}$$

Denoting by $[E]$ the cardinality of a set E, we have

$$(3.28)\quad [M^\sharp]((q-1)/2)=[M^*]=(q-1)^2-(q-1)$$

since the set $(K^\times)^2-M^*=\{(A,B)\in (K^\times)^2;\ \Delta=4A^3+27B^2=0\}$ can be described in terms of $C\in K^\times$ as in (3.11). Hence, we get

$$(3.29)\quad [M^\sharp]=2(q-2).$$

From (3.27), (3.29), we have the following

(3.30) **Proposition.** *Suppose that the characteristic of $K=F_q$ is not 2, 3. Let $k=0$, 2 or 4 according as $q\equiv 11 \pmod{12}$, $q\equiv 5$ or 7 $\pmod{12}$ or $q\equiv 1 \pmod{12}$. For a pair $\lambda=(A,B)\in (K^\times)^2$ with $\Delta=4A^3+27B^2\neq 0$, denote by a_λ the trace of the Frobenius endomorphism of the elliptic curve $E_\lambda: y^2=x^3+Ax+B$. Then, we have*

$$\inf_\lambda |a_\lambda| \leqq \sqrt{\frac{q^2-kq-1}{q-2}} \leqq \sup_\lambda |a_\lambda|.$$