93. *On Certain Numerical Invariants of Mappings over Finite Fields. II*

By Takashi ONO
Department of Mathematics, Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 13, 1980)

Introduction. This is a continuation of the first paper [1] which will be referred to as (I) in this paper.*) Our purpose here is to determine invariants ρ_F, σ_F (see (I.1.1), (I.1.6)) for quadratic mappings $F: X \to Y$ of vector spaces over a finite field $K = F_q$ (q : odd) with respect to the quadratic character of the multiplicative group of K. In particular, we shall obtain explicit values of invariants for such mappings arising from pairs of quadratic forms.

§1. Quadratic mappings. Let K be the finite field with q elements: $K = F_q$ (q : odd). Denote by χ the character of $K^\times$ of order 2. As usual, we extend χ to K by $\chi(0) = 0$. Let X, Y be vector spaces over K of dimension n, m, respectively, and $F: X \to Y$ be a quadratic mapping. By definition, $F_\lambda = \lambda \circ F$ is a quadratic form on X for every linear form $\lambda \in Y^*$. By (I.1.6), we have

(1.1) $\sigma_F = \sum_{\lambda \in Y^*} |S_{F_\lambda}|^2,$

where

(1.2) $S_{F_\lambda} = \sum_{x \in X} \chi(F_\lambda(x)).$

Thanks to the following lemma, proof of which is left to the reader as an exercise, the determination of σ_F is much easier than that of ρ_F.

(1.3) **Lemma.** *Let V be a vector space of dimension r over K and Q be a non-degenerate quadratic form on V. Then we have*

$$S_Q = \sum_{x \in V} \chi(Q(x)) = \begin{cases} 0, & \text{if } r \text{ is even}, \\ (q-1)q^{(r-1)/2}\chi((-1)^{(r-1)/2} \det Q), & \text{if } r \text{ is odd}. \end{cases}$$

(1.4) **Theorem.** *Let $K = F_q$ (q : odd). Let F be a quadratic mapping $X \to Y$ of vector spaces over K, $n = \dim X$, $m = \dim Y$. Let r_λ be the rank of the quadratic form $F_\lambda = \lambda \circ F$, $\lambda \in Y^*$. Then, we have*

$$\rho_F = q^{n-m}(q-1) \sum_{r_\lambda \text{ odd}} q^{n-r_\lambda}.$$

Proof. Write F_λ as a diagonal form $a_1 x_1^2 + \cdots + a_{r_\lambda} x_{r_\lambda}^2$, $a_i \in K^\times$. By (1.3), we have

$$S_{F_\lambda} = \sum_{x \in X} \chi(a_1 x_1^2 + \cdots + a_{r_\lambda} x_{r_\lambda}^2)$$
$$= \sum_{(x_{r_\lambda+1}, \cdots, x_n)} \sum_{(x_1, \cdots, x_{r_\lambda})} \chi(a_1 x_1^2 + \cdots + a_{r_\lambda} x_{r_\lambda}^2)$$

---

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

$$=\begin{cases}0, & \text{if } r \text{ is even},\\ q^{n-(r_\lambda+1)/2}(q-1)\chi((-1)^{(r_\lambda-1)/2}d_\lambda), & \text{if } r_\lambda \text{ is odd},\end{cases}$$

where $d_\lambda=a_1\cdots a_{r_\lambda}$. We have then

$$\sigma_F=(q-1)^2\sum_{r_\lambda\,\text{odd}} q^{2n-r_\lambda-1}$$

and (1.4) follows from (I.1.11). Q.E.D.

§2. **Pairs of quadratic forms.** Let A be an $n\times n$ matrix $\in K_n$. Let $E_1,\cdots,E_n$ be elementary divisors of the polynomial matrix $x1_n-A$. For an eigenvalue $\omega\in\bar{K}$ (the algebraic closure of K) of A, suppose that $(x-\omega)^{e_i}$ divides E_i but $(x-\omega)^{e_i+1}$ does not. Since E_i divides E_{i+1}, we get the descending sequence

(2.1) $e_n\geqq e_{n-1}\geqq\cdots\geqq e_2\geqq e_1\geqq 0.$

Omitting zeros from (2.1), we get the sequence of natural numbers

(2.2) $e_n\geqq e_{n-1}\geqq\cdots\geqq e_{n-(k-1)}.$

We write (2.2) as

(2.3) $e(\omega)=(e_n,e_{n-1},\cdots,e_{n-(k-1)})$

and call $e(\omega)$ the set of exponents for the eigenvalue ω of A. We put $k=l(\omega)$ and call this the length of $e(\omega)$. Finally, we put

(2.4) $s(A)=[e(\omega_1),\cdots,e(\omega_t)]$,

where $\omega_1,\cdots,\omega_t$ are all distinct eigenvalues (in $\bar{K}$) of A. The symbol $s(A)$ is known as the Segre characteristic of the matrix A.

For each eigenvalue ω of A, put

(2.5) $$A_\omega=\begin{bmatrix}J_n & & & \\ & J_{n-1} & & \\ & & \ddots & \\ & & & J_{n-(k-1)}\end{bmatrix},\qquad J_i=\begin{bmatrix}\omega & 1 & & & \\ & \omega & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1\\ & & & & \omega\end{bmatrix}\in(\bar{K})_{e_i},$$

where $k=l(\omega)$, $n\geqq i\geqq n-(k-1)$. Then, A is equivalent to the Jordan canonical form, i.e. the direct sum of A_{ω_i}'s.

(2.6) **Lemma.** *Let $A\in K_n$ and $c\in K$. Put* $\mathrm{rk}\,(c)=\mathrm{rank}\,(c1_n-A)$. *Let $\Omega=\{\omega_1,\cdots,\omega_t\}$ be the set of all distinct eigenvalues of A (in $\bar{K}$). Then, we have*

$$\mathrm{rk}\,(c)=\begin{cases}n, & \text{if } c\notin\Omega,\\ n-l(\omega), & \text{if } c\in\Omega,\end{cases}$$

where $l(\omega)$ is the length of the set of exponents for the eigenvalue ω of A.

Proof. The case $c\notin\Omega$ is trivial. If $c=\omega_j\in\Omega$, then, for $i\neq j$, we have $\mathrm{rank}\,(c1_{m_i}-A_{\omega_i})=m_i=$the multiplicity of ω_i in the characteristic polynomial of A. On the other hand, we have $\mathrm{rank}\,(c1_{m_j}-A_{\omega_j})=m_j-l(\omega_j)$ since each block J_i of A_{ω_j} (see (2.5)) loses the rank by 1 by the subtraction. Q.E.D.

Now, let $K=\boldsymbol{F}_q$ (q : odd), $X=K^n$, $Y=K^2$ and $F:X\to Y$ be a quadratic mapping. Hence, a pair of quadratic form (F_1,F_2) is defined by

$F(x)=(F_1(x), F_2(x))$. Using column vectors, we identify quadratic forms $F_1(x), F_2(x)$ with symmetric matrices $A, B \in K_n$ such that $F_1(x)={}^t xAx$, $F_2(x)={}^t xBx$, respectively. A linear form $\lambda \in Y^*$ may be written as $\lambda=(\alpha, \beta)$ when $\lambda(y)=\alpha y_1+\beta y_2$, $y=\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in Y=K^2$. The quadratic form $F_\lambda(x)=\lambda(F(x))$ may be identified with the symmetric matrix $\alpha A+\beta B$ and we have

(2.7) $r_\lambda=\operatorname{rank} F_\lambda=\operatorname{rank}(\alpha A+\beta B)$.

From now on, we assume that the quadratic form $F_1(x)$ is non-degenerate, i.e. $\det A \neq 0$. Then, we have

(2.8) $r_\lambda=\operatorname{rank}(\alpha 1_n+\beta C)$, $\lambda=(\alpha, \beta)$, $C=A^{-1}B$.

Denote by Ω_C the set of all distinct eigenvalues (in $\bar{K}$) of C. Then, (2.6) implies that

$$(2.9) \quad r_\lambda=\begin{cases} 0, & \text{if } \alpha=\beta=0, \\ n, & \text{if } \alpha\neq 0,\ \beta=0, \\ n, & \text{if } \beta\neq 0 \text{ and } -(\alpha/\beta) \notin \Omega_C, \\ n-l(-(\alpha/\beta)), & \text{if } \beta\neq 0 \text{ and } -(\alpha/\beta) \in \Omega_C. \end{cases}$$

Substituting the values r_λ in (2.9) back into (1.4) we obtain the values of ρ_F, σ_F for pair of quadratic forms $F(x)=(F_1(x), F_2(x))$ where $F_1(x)$ is non-degenerate. Namely, put $\Omega_{C,K}=\Omega_C \cap K$, the set of eigenvalues of $C=A^{-1}B$ contained in K. Let $n_{C,K}=[\Omega_{C,K}]$, the cardinality. (It may well happen that $n_{C,K}=0$.) For each $\omega \in \Omega_{C,K}$, $\lambda=(\alpha, \beta)$ with $\beta\neq 0$ and $\alpha=-\beta\omega$ provides a linear form such that $-(\alpha/\beta)=\omega$. Since there are $q-1$ β's each ω contributes $q-1$ λ's. Hence, the number of λ's for which $\alpha\neq 0$, $\beta=0$ is $q-1$, the number of λ's for which $\beta\neq 0$ and $-(\alpha/\beta) \notin \Omega_{C,K}$ is $(q-1)(q-n_{C,K})$ and the number of λ's for which $\beta\neq 0$ and $-(\alpha/\beta) \in \Omega_{C,K}$ is $(q-1)n_{C,K}$. Taking the parity of r_λ into account, we get, from (1.4), the following

(2.10) **Theorem.** *Let $K=F_q$ (q: odd), $F=(F_1, F_2)$ be a quadratic mapping $K^n \to K^2$ such that the quadratic form F_1 is non-degenerate. Let A, B be symmetric matrices corresponding to F_1, F_2, respectively, and let $C=A^{-1}B$. Let $n_{C,K}$ be the number of all distinct eigenvalues of C contained in K and, for each such eigenvalue ω let $l(\omega)$ be the length of the set of exponents for ω. Then, we have*

$$\rho_F=\begin{cases} q^{n-2}(q-1)^2 \sum_{l(\omega)\ \mathrm{odd}} q^{l(\omega)}, & \text{if } n \text{ is even}, \\ q^{n-2}(q-1)^2(1+q-n_{C,K}+\sum_{l(\omega)\ \mathrm{even}} q^{l(\omega)}), & \text{if } n \text{ is odd}. \end{cases}$$

(2.11) **Remark.** Note that ρ_F depends only on the Segre characteristic $s(C)$ of $C=A^{-1}B$ when every eigenvalue of C is in K. Under this assumption, we give here the complete list of ρ_F for $n=3$.

Segre char.	$F=(F_1, F_2)$	ρ_F
[1,1,1]	$F_1=x_1^2+x_2^2+x_3^2,\ F_2=\omega_1x_1^2+\omega_2x_2^2+\omega_3x_3^2$	$q(q-1)^2(q-2)$
[2,1]	$F_1=2x_1x_2+x_3^2,\ F_2=2\omega_1x_1x_2+x_2^2+\omega_2x_3^2$	$q(q-1)^3$
[(1,1),1]	$F_1=x_1^2+x_2^2+x_3^2,\ F_2=\omega_1x_1^2+\omega_1x_2^2+\omega_2x_3^2$	$q(q-1)^2(q^2+q-1)$
[3]	$F_1=2x_1x_3+x_2^2,\ F_2=2\omega_1x_1x_3+\omega_1x_2^2+2x_2x_3$	$q^2(q-1)^2$
[(2,1)]	$F_1=2x_1x_2+x_3^2,\ F_2=2\omega_1x_1x_2+x_2^2+\omega_1x_3^2$	$q^2(q-1)^2(q+1)$
[(1,1,1)]	$F_1=x_1^2+x_2^2+x_3^2,\ F_2=\omega_1x_1^2+\omega_1x_2^2+\omega_1x_3^2$	$q^2(q-1)^2$

Reference

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