REPRESENTATIONS BY QUADRATIC FORMS IN A FINITE FIELD

By L. Carlitz

1. **Introduction.** Let $q = p^n$, $p > 2$ and let

$$A(x) = \sum_{i,j=1}^{m} \alpha_{ij}x_ix_j , \qquad B(x) = \sum_{i,j=1}^{t} \beta_{ij}x_ix_j \tag{1.1}$$

be quadratic forms with coefficients in $GF(q)$. We consider the following problem. Put

$$u_i = \sum_{j=1}^{t} \xi_{ij}x_j \qquad (i = 1, \cdots, m; \xi_{ij} \in GF(q)); \tag{1.2}$$

then we seek the number $N_t(A, B)$ of linear forms (1.2) such that

$$A(u) = B(x). \tag{1.3}$$

An equivalent formulation of the problem is to find the number of $m \times t$ matrices X with elements in $GF(q)$ such that

$$X'AX = B, \tag{1.4}$$

where A and B are the matrices of the quadratic forms (1.1). There is no loss in generality in assuming A non-singular; however the rank r of B is arbitrary ($r \leq m, t$).

In order to determine $N_t(A, B)$, we first evaluate $N_r(A, B)$ and $N_t(A, 0)$. Suppose B reduced to diagonal form $(\beta_1 , \cdots , \beta_r , 0, \cdots , 0)$, and put $\delta_B = \beta_1\beta_2 \cdots \beta_r$; also for $\alpha \in GF(q)$ define $\psi(\alpha) = 0, 1, -1$ according as $\alpha = 0$, square or non-square of $GF(q)$. We put $\lambda_A = \psi(\delta_A)$, $\lambda_B = \psi(\delta_B)$. Then $N_r(A, B)$ is a function of $\lambda_A , \lambda_B , m$ and r, while $N_t(A, 0)$ is a function of λ_A , m and t. We find (see Theorem 1 below) that $N_r(A, B)$ can be expressed as a fairly simple product. The explicit results for $N_t(A, 0)$ are of a different kind; the final formulas are in terms of certain terminating q-hypergeometric series (see Theorem 4 below). For example for m odd we get

$$q^{\frac{1}{2}t(t+1)-mt}N_t(A, 0) = {}_2\Phi_2[q^{-\frac{1}{2}t}, q^{-\frac{1}{2}(t-1)}; q^{\frac{1}{2}(m+1)}]',$$

where the prime indicates that q is to be replaced by q^{-2}. As for $N_t(A, B)$ we have the formula (Theorem 5)

$$N_t(A, B) = N_r(A, B^*)N_{t-r}(A_r , 0), \tag{1.5}$$

where A_r is symmetric of order $m - r$, non-singular with $\lambda_A = \lambda_B\lambda_{A_r}$ and B^* is symmetric of order r, non-singular with $\lambda_{B^*} = \lambda_B$. As an incidental result we find (Theorem 3) the number $N(m, r, \lambda)$ of symmetric matrices A of order m, rank r and such that $\lambda_A = \lambda$.

Received March 25, 1953.