AN ABSTRACT OF THE THESIS OF

JOHN ARTHUR FURCHA (Name) for the M. A. (Degree) in Mathematics (Major)

Date thesis is presented April 29, 1965

Title A STUDY OF SYMMETRIC MATRICES AND QUADRATIC FORMS OVER FIELDS OF CHARACTERISTIC TWO

Abstract approved Redacted for Privacy
(Major professor)

This thesis has four main results. First we find a reduction form for symmetric matrices over fields of characteristic two. This result parallels the diagonalization theorem for symmetric matrices over fields of characteristic not two.

Secondly we reduce our reduction form to a canonical form in perfect fields of characteristic two.

For our next result we find the number of solutions of an arbitrary quadratic form over a finite field of characteristic two. This result parallels work done by Dickson in fields of characteristic not two.

Finally we make use of our second and third results to find the number of m by t matrices X such that $X'AX = B$, where A and B are nonsingular symmetric matrices of orders m and t respectively. This final result parallels work done by Carlitz in fields of characteristic not two.

A STUDY OF SYMMETRIC MATRICES AND QUADRATIC FORMS OVER FIELDS OF CHARACTERISTIC TWO

by

JOHN ARTHUR FURCHA

A THESIS

submitted to

OREGON STATE UNIVERSITY

in partial fulfillment of
the requirements for the
degree of

MASTER OF ARTS

June 1966

APPROVED:

Redacted for Privacy

Assistant Professor of Mathematics

In Charge of Major

Redacted for Privacy

Chairman of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

Date thesis is presented April 29, 1965

Typed by Carol Baker

ACKNOWLEDGMENTS

The author wishes to acknowledge his wife for her unending faith and patience; also his major professor, Dr. David Carlson, for his invaluable criticisms, comments and assistance.

TABLE OF CONTENTS

A STUDY OF SYMMETRIC MATRICES AND QUADRATIC FORMS OVER FIELDS OF CHARACTERISTIC TWO

CHAPTER I. INTRODUCTION

The number $N_t(A, B)$ of m by t matrices X over $GF[p^n]$, $p > 2$ such that $X'AX = B$, with A and B nonsingular symmetric matrices over $GF[p^n]$, $p > 2$ of rank m and t respectively, was established by L. Carlitz in his article Quadratic Forms in a Finite Field [1]. Later in his article Representations by Skew Forms in a Finite Field [2], Carlitz also found the number $Z_t(A, B)$ of m by t matrices X over $GF[p^n]$, $p > 2$ such that $X'AX = B$, with A and B nonsingular skew symmetric matrices over $GF[p^n]$, $p > 2$, of rank m and t respectively. In both cases, Carlitz assumes $p > 2$. The purpose of this thesis is to find the number of solutions for X when $p = 2$.

We first note that it is sufficient to look only at the case where A and B are nonsingular symmetric matrices since symmetry is equivalent to skew symmetry over fields of characteristic two. That is

$$A = A' \iff A = -A' \quad \text{since} \quad A = -A .$$

We employ in Chapter IV the same method used by Carlitz to find the number $N_t(A, B)$ of m by t matrices X over $GF[2^n]$ such that $X'AX = B$, with A and B nonsingular symmetric matrices

over $GF[2^n]$ of order m and t respectively, $m \geq t$. The analogy is not immediate however, and to illustrate this let's now look at the method used by Carlitz for characteristic $p > 2$ in the symmetric case [1].

Let's assume that $1 \leq t \leq m$. The first step is to find a recursion formula for $N_t(A, B)$. The value of $N_t(A, B)$ is then established by using this recursion formula and mathematical induction on t.

Finding a Recursion Formula

We first show that the matrix B can be assumed in diagonal form using the following theorem [4, p. 166].

Theorem 0.1. Every symmetric matrix with elements in F is congruent over F to a diagonal matrix, provided F does not have characteristic two.

Thus there exists a nonsingular matrix R such that

$$R'BR = \operatorname{diag}(b_1, b_2, \cdots, b_t).$$

Hence, we have

$$(YR)'A(YR) = R'Y'AYR = \operatorname{diag}(b_1, b_2, \cdots, b_t).$$

Since R is nonsingular and the number of matrices YR is the

same as the number of matrices Y, we may assume B to be diagonal and consider solutions $X = YR$.

Let X be a solution of the given matrix equation with first column a such that

$$a'Aa = b_1 .$$

Then there exists a matrix C, m by $m-1$, such that $U = (a|C)$ is unimodular. By properly picking C we have

$$U'AU = \begin{pmatrix} b_1 & z' \\ z & A_1 \end{pmatrix} ,$$

where z represents the column vector $(0, 0, \cdots, 0)$. Now set $X = UY$, where

$$Y = \begin{pmatrix} 1 & \beta' \\ \delta & X_1 \end{pmatrix} , \quad \beta, \delta \text{ column vectors.}$$

Since U is unimodular and a is the first column of X it follows that $\delta = z$; next computing

$$Y'U'AUY$$

we must have $\beta = z$. Hence $X_1'A_1X_1$ is equal to the matrix $B_1 = \text{diag}\,(b_2, \cdots, b_t)$. Thus to find the value of $N_t(A, B)$ we first find all the solutions a of

$$a'Aa = b_1 ;$$

next for each a we choose U and construct A_1. Then we find all solutions X_1 of $X_1'A_1X_1 = B_1$. This may be expressed by the recursion formula

$$N_t(A, B) = \sum_a N_{t-1}(A_1, B_1),$$

for all a's such that $a'Aa = b_1$.

Finding the Value of $N_t(A, B)$

For $t = 1$, we have $B = (b)$ and

$$a'Aa = b ,$$

which is a quadratic form. The number of solutions for a is given by the following two theorems [3, p. 47] (since an arbitrary quadratic form may be reduced to diagonal form [3, p. 157]).

Theorem 0.2. If A is of even $(2m)$ order, the number of solutions $(x_1, x_2, \cdots, x_{2m})$ in $GF[p^n]$, $p > 2$, of the equation

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_{2m}x_{2m}^2 = b,$$

where every a_i is a non-zero element in the field and b belongs

to the field, is

$$q^{2m-1} - \nu q^{m-1} \qquad (\text{if } b \neq 0),$$
$$q^{2m-1} + \nu(q^m - q^{m-1}) \qquad (\text{if } b = 0),$$

where ν is +1 or -1 according as $(-1)^m a_1 a_2 \cdots a_{2m}$ is a square or not-square in the field.

Theorem 0.3. If A is of odd (2m+1) order, the number of solutions $(x_1, x_2, \cdots, x_{2m+1})$ in $GF[p^n]$, $p > 2$, of the equation

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_{2m+1} x_{2m+1}^2 = b$$

where each a_j is a non-zero element in the field and b belongs to the field, is

$$q^{2m} + \omega q^m,$$

where $\omega = +1, -1,$ or zero according as $(-1)^m b a_1 a_2 \cdots a_{2m+1}$ is a square, not-square or zero in the field.

The value of $N_t(A, B)$ is then shown to be, by mathematical induction on t;

$$q^{mt-1/2t(t+1)}\{1-\psi((-1)^{1/2m}\delta_A)q^{-1/2m}\}\{1+\psi((-1)^{1/2(m-t)}\delta_A\delta_B)q^{-1/2(m-t)}\}$$

$$\cdot \prod_{i=1}^{1/2(t-2)} (1-q^{2i-m}) \qquad \text{(for m even, t even)},$$

$$q^{mt-1/2t(t+1)}\{1-\psi((-1))^{1/2m}\delta_A)q^{-1/2m}\} \prod_{i=1}^{1/2(t-1)} (1-q^{2i-m})$$

(for m even, t odd),

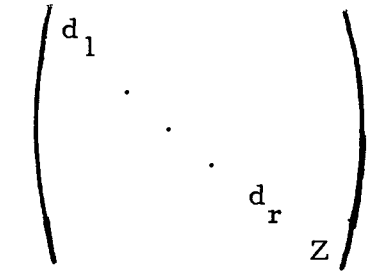
$$q^{mt-1/2t(t-1)}\{1+\psi((-1)^{1/2(m-t)}\delta_A\delta_B)q^{-1/2(m-t)}\} \prod_{i=1}^{1/2(t-1)} (1-q^{2i-m-1})$$

(for m odd, t odd),

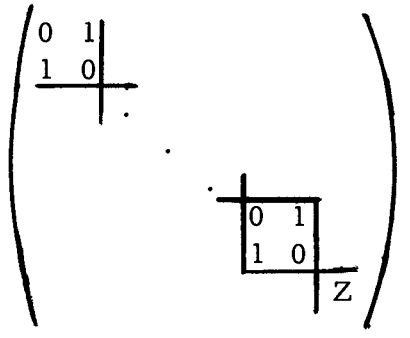
$$q^{mt-1/2t(t-1)} \prod_{i=1}^{1/2\,r} (1-q^{2i-m-1}) \qquad \text{(for m odd, t even)},$$

where δ_A, δ_B are the invariants of A and B, respectively. Notice that theorems 0.1, 0.2, and 0.3 hold only in fields of characteristic not two. Before we can use this method used by Carlitz in fields of characteristic two we must first find analogies to theorems 0.1, 0.2, and 0.3. This is done in Chapters II and III.

We find in Chapter II a reduction form, for symmetric matrices over fields of characteristic two:

a) $B =$  zeros elsewhere and each d_i is a non-zero element,

or

b) $B =$  zeros elsewhere.

This form is not canonical. In answer to the question, "Can it be reduced to a canonical form ?" , we find that only in a perfect field of characteristic two can it be reduced one step further to a canonical form.

We find in Chapter III the analogs of theorems 0.2 and 0.3. We make use of a theorem of L.E. Dickson, in which he finds two canonical forms for quadratic forms in $GF[2^n]$, three lemmas, and the fact that an arbitrary quadratic form over $GF[2^n]$ is equivalent to a form

$$\sum_{1 \leq i \leq j \leq r} a_{ij} x_i x_j \ .$$

The analog is given in theorem 3.1 which states:

The number of solutions of an arbitrary quadratic form over

$GF[2^n]$ can be found in one of the following.

(a) The number of solutions $x = (x_1, x_2, \cdots, x_{2m+1})$ of a quadratic form f, reducible to the canonical form

$$F = x_1x_2 + \cdots + x_{2m-1}x_{2m} + x_{2m+1}^2 = b,$$

is

$$(*)\ q^{2m}$$

(b) The number of solutions $x = (x_1, \cdots, x_{2m})$ of a quadratic form f, reducible to the canonical form

$$F_\lambda = x_1x_2 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}x_{2m} + \lambda x_{2m-1}^2 + \lambda x_{2m}^2 = b,$$

where λ is zero or a particular one of the values λ' for which

$$Q \equiv x_{2m-1}x_{2m} + \lambda' x_{2m-1}^2 + \lambda' x_{2m}^2$$

is irreducible in $GF[2^n]$, is

$$(*)\quad \begin{cases} q^{2m-1} + q^m - q^{m-1} & \text{if } \lambda = 0,\ b = 0, \\ q^{2m-1} - q^{m-1} & \text{if } \lambda = 0,\ b \neq 0, \\ q^{2m-1} - q^m + q^{m-1} & \text{if } \lambda \neq 0,\ b = 0, \\ q^{2m-1} + q^{m-1} & \text{if } \lambda \neq 0,\ b \neq 0. \end{cases}$$

(c) The number of solutions $x = (x_1, x_2, \cdots, x_m)$ of a quadratic form f, expressible over the field as a quadratic form in a minimal number $s\ (s < m)$ of linear homogeneous functions of $x_1, x_2, \cdots, x_m$, is the product of q^{m-s} and (*) of part (a) with $2m+1 = s$, or part (b) with $2m=s$ depending upon whether s is odd or even.

Using the method of Carlitz already described and the method used in [2] together with our results of Chapters II and III we find easily the value of $N_t(A, B)$ in $GF[2^n]$. For B congruent to the form in (a) of our canonical form in Chapter II we find $N_t(A, B)$ has the value

$$q^{mt - \frac{t(t+1)}{2}} .$$

For B congruent to the form in (b) of our canonical form in Chapter II we find $N_t(A, B)$ has the value

$$q^{km-k^2} \prod_{i=0}^{k-1} (q^{m-2i}-1) ,$$

where $t = 2k$.

Before proceeding further, let's explain some of the notation used in this thesis.

i) The capital letters A, B, X, T, etc. are matrices.

ii) A' is the transpose of the matrix A.

iii) $GF[p^n]$ is the unique field with p^n elements. We let $q = p^n$.

iv) $N_t(A, B)$ is the number of matrices X such that $X'AX = B$, where A and B are nonsingular symmetric matrices of rank m and t respectively, $m \geq t$.

v) $\psi(a) = 1, -1, 0$ according as a is a perfect square, not a perfect square, or zero.

vi) $\delta(A)$ is the determinant of the matrix A.

vii) $\oplus$ stands for the direct sum.

viii) P is the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

ix) $U = (a \mid C)$ denotes a matrix C having adjoined to it the new first column a.

CHAPTER II. FINDING A REDUCTION FORM AND A CANONICAL FORM FOR SYMMETRIC MATRICES OVER A FIELD OF CHARACTERISTIC TWO

The first result of this chapter is the establishment of the reduction form,

a) $B = \begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_r & \\ & & & & Z \end{pmatrix}$ zeros elsewhere and each d_i is a non-zero element,

or

b) $B = \begin{pmatrix} \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} & & & \\ & \ddots & & \\ & & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} & \\ & & & Z \end{pmatrix}$ zeros elsewhere,

for symmetric matrices over all fields of characteristic two. Secondly we find for all perfect fields of characteristic two the canonical form,

a) $B = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1 \\ & & & & & Z \end{pmatrix}$ zeros elsewhere,

or

b) $B = \begin{pmatrix} \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} & & & \\ & \ddots & & \\ & & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} & \\ & & & Z \end{pmatrix}$ zeros elsewhere .

We might also point out that our two-case reduction form is reasonable since symmetry and skew symmetry are equivalent in fields of characteristic two. The form in (a) is the same as the form of theorem 0. 1, and if the -1's are replaced by $+1$'s in the canonical form of skew-symmetric matrices over fields of characteristics not two, the result is the form in (b).

Lemma 2. 1. Let A be a symmetric matrix of order r over a field F of characteristic two. Also let i and j be fixed with $1 \leq i < j \leq r$. Then for the matrix $T = (t_{k\ell})$ with

$$t_{ii} = t_{jj} = 0, \qquad t_{ij} = t_{ji} = 1,$$

ones on the rest of the diagonal, and zeros elsewhere

TAT' has;

$$(tat')_{ii} = a_{jj}, \qquad (tat')_{jj} = a_{ii},$$

$$(tat')_{ki} = a_{kj}, \quad \text{and} \quad (tat')_{kj} = a_{ki}, \quad k \neq i, j.$$

Proof. The proof of this lemma follows directly from the fact that T is a permutation matrix.

In his proof of theorem 0.1, which states that every symmetric matrix over a field F of characteristic not two is congruent to a diagonal matrix, Finkbeiner [4, p. 166] treats first the case where all of the diagonal elements are zero. Lemma 2.2 reasonably then deals with matrices having all diagonal elements zero.

Lemma 2.2. Let A be a nonsingular symmetric matrix of order r over a field F of characteristic two with all the diagonal elements zero. Then there exists a nonsingular matrix T such that TAT' is of the form

$$\oplus P_j \quad \text{for } P_j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad j = 1, 2, \cdots, k,$$

and A must be of even order $r = 2k$.

Proof. Since A is nonsingular at least one element of the first row of A (excluding a_{11}) must be non-zero. By lemma 2.1 we can assume a_{12} is non-zero. Now let's choose $T = (t_{ij})$ with

$$t_{22} = 1/a_{12}, \quad t_{i2} = a_{1i}/a_{12} \quad \text{for } i = 3, \cdots, r$$

ones on the rest of the diagonal, and zeros elsewhere.

Now let's calculate TAT' .

$$TAT' = \begin{pmatrix} 1 & & & & & \\ \frac{1}{a_{12}} & & & & & \\ \frac{a_{13}}{a_{12}} & 1 & & & & \\ \vdots & & \ddots & & & \\ \frac{a_{1j}}{a_{12}} & & & \ddots & & \\ \vdots & & & & \ddots & \\ \frac{a_{1r}}{a_{12}} & & & & & 1 \end{pmatrix} \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1j} & \cdots & a_{1r} \\ a_{12} & 0 & a_{23} & \cdots & a_{2j} & \cdots & a_{2r} \\ a_{13} & a_{23} & 0 & \cdots & a_{3j} & \cdots & a_{3r} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ a_{1j} & a_{2j} & a_{3j} & \cdots & 0 & \cdots & a_{jr} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ a_{1r} & a_{2r} & a_{3r} & \cdots & a_{jr} & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 & & & & & \\ \frac{1}{a_{12}} & \frac{a_{13}}{a_{12}} & \cdots & \frac{a_{1j}}{a_{12}} & \cdots & \frac{a_{1r}}{a_{12}} \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ 1 & 0 & \frac{a_{23}}{a_{12}} & \cdots & \frac{a_{2j}}{a_{12}} & \cdots & \frac{a_{2r}}{a_{12}} \\ 0 & \frac{a_{23}}{a_{12}} & 0 & \cdots & \frac{a_{1j}a_{23}+a_{2j}a_{13}}{a_{12}} + a_{3j} & \cdots & \frac{a_{1r}a_{23}+a_{2r}a_{13}}{a_{12}} + a_{3r} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \frac{a_{2j}}{a_{12}} & \frac{a_{1j}a_{23}+a_{2j}a_{13}}{a_{12}} + a_{3j} & \cdots & 0 & \cdots & \frac{a_{2j}a_{1r}+a_{2r}a_{1j}}{a_{12}} + a_{jr} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \frac{a_{2r}}{a_{12}} & \frac{a_{1r}a_{23}+a_{2r}a_{13}}{a_{12}} + a_{3r} & \cdots & \frac{a_{2j}a_{1r}+a_{2r}a_{1j}}{a_{12}} + a_{jr} & \cdots & 0 \end{pmatrix}.$$

Thus we can always find TAT' of the form

$$B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & & & & \\ 0 & & & & \\ \vdots & & & B_1 & \\ 0 & & & & \end{pmatrix}$$

where B_1 has all zeros on the diagonal and has dimension $r - 1$.

Repeating this procedure on B_1 and finding a matrix T_1 in the same manner, then acting on B with $I \oplus T_1$ yields

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & & & & \\ 0 & 0 & & & & \\ \vdots & \vdots & & C_1 & & \\ 0 & 0 & & & & \end{pmatrix}$$

where C_1 has all zeros on the diagonal and has dimension $r - 2$.

Note: $I \oplus T_1$ leaves the elements of the first row of B unchanged.

Now multiplying on the left by the matrix $S = (s_{k\ell})$ with

$$s_{kk} = 1 \text{ for all } k, \quad s_{31} = 1, \quad \text{and zeros elsewhere,}$$

we have

$$SCS' = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & C_1 & \\ 0 & 0 & & & \end{pmatrix}$$

where C_1 is non-singular of rank $r-2$ with all zeros on the diagonal.

Repeating this process on C_1 and continuing we will eventually arrive at

$$\oplus P_j \oplus R$$

where $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $j = 1, 2, \cdots, k$ and R has dimension zero if A was of even rank or one if A was of odd rank. The latter case is impossible since A was nonsingular and R of dimension one on the diagonal would have to be the zero block. This could only happen if A were singular, thus A must be of even rank, $2k$ where k is the number of P blocks.

Looking at a nonsingular symmetric matrix A with all zeros on the diagonal we see that by choosing T as the matrix which adds the i^{th} row to the j^{th} row for some non zero a_{ij} we would have

$$TAT' = B, \quad \text{with} \quad b_{jj} = a_{ij} + a_{ij} = 2a_{ij}.$$

But over a field of characteristic two we have (with this choice of T) $b_{jj} = 0$ since $2a_{ij} = 0$. It is not surprising then that we have the following lemma.

Lemma 2.3. Let A be a nonsingular symmetric matrix of rank r over a field F of characteristic two with all zeros on the diagonal. Then there exists no matrix T such that TAT'

has a nonzero diagonal element.

Proof. Let's first look at the case where A is of the form $\oplus P_j$ for $j = 1, 2, \cdots, k$, and A has rank $r = 2k$. Suppose we now let $k = 1$, and $r = 2$. Then A is merely P and for arbitrary $T = (t_{ij})$ we have

$$TPT' = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} t_{11} & t_{21} \\ t_{12} & t_{22} \end{pmatrix} = \begin{pmatrix} t_{12} & t_{11} \\ t_{22} & t_{21} \end{pmatrix} \begin{pmatrix} t_{11} & t_{21} \\ t_{12} & t_{22} \end{pmatrix} = \begin{pmatrix} 0 & t_{12}t_{21}+t_{11}t_{22} \\ t_{11}t_{22}+t_{12}t_{21} & 0 \end{pmatrix}.$$

Suppose now that $k > 1$, then $A = \oplus P_j$, $j = 1, 2, \cdots, k$. Let's represent an arbitrary $2k$ by $2k$ matrix T in block form as $T = (T_{ij})$ where each T_{ij} is a 2×2 block. Since we are interested only in the diagonal elements of TAT' we need only look at the blocks on the diagonal of TAT';

$$TAT'_{ii} = \sum_{j=1}^{k} T_{ij} P_j T'_{ij}, \quad \text{for} \quad i = 1, 2, \cdots, k \ .$$

But from our calculations for $k = 1$ we see that each diagonal block of TAT' will be a sum of k matrices each with all zeros on the diagonal. Thus each diagonal block TAT'_{ii} will have zeros on the diagonal which is equivalent to TAT' having no non-zero diagonal elements.

If A is not of the form of lemma 2.2 then by lemma 2.2

there exists a nonsingular matrix R such that RAR' is of the form $\oplus P_j$ $j = 1, 2, \cdots, k$. We have already shown that there exists no matrix S such that $S(\oplus P_j)S'$ $j = 1, 2, \cdots, k$ has non-zero elements on the diagonal. This means that

$$SRAR'S' = (SR)A(SR)'$$

has no non-zero elements on the diagonal. Letting $T = SR$, there exists no T such that TAT' has non-zero diagonal elements.

Considering now nonsingular symmetric matrices with at least one non-zero element on the diagonal we have lemma 2.4.

Lemma 2.4. If A is a nonsingluar symmetric matrix of rank r over a field F of characteristic two with at least one non-zero diagonal element, then there exists a nonsingular matrix T such that TAT' is of the form

$$\oplus d_i \oplus P_j \quad \text{for} \quad i = 1, 2, \cdots, n, \quad j = 1, 2, \cdots, k$$

with each d_i a non-zero element and $n = r-2k$.

Proof. Since there is at least one non-zero element on the diagonal of A we may assume a_{11} is a non-zero element as a result of lemma 2.1. Suppose also that some a_{1j}, $1 < j \leq r$ is a non-zero element. Then choose $T = (t_{k\ell})$ with

$$t_{kk} = 1 \quad \text{for all} \quad k, \quad t_{jl} = \frac{a_{lj}}{a_{ll}}, \quad \text{zeros elsewhere.}$$

$$TAT' = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ \frac{a_{1j}}{a_{11}} & & & & 1 & \\ & & & & & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1r} \\ a_{12} & a_{22} & \cdots & a_{2j} & \cdots & a_{2r} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{1j} & a_{2j} & \cdots & a_{jj} & \cdots & a_{jr} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{1r} & a_{2r} & \cdots & a_{jr} & \cdots & a_{rr} \end{pmatrix} \begin{pmatrix} 1 & & & \frac{a_{1j}}{a_{11}} & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & 0 & \cdots & a_{1r} \\ a_{12} & a_{22} & \cdots & \frac{a_{12}a_{1j}}{a_{11}} + a_{2j} & \cdots & a_{2r} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & \frac{a_{12}a_{1j}}{a_{11}} + a_{2j} & \cdots & \frac{a_{1j}}{a_{11}}{}^{2} + a_{jj} & \cdots & \frac{a_{1j}a_{1r}}{a_{11}} + a_{rj} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{1r} & a_{2r} & \cdots & \frac{a_{ij}a_{1r}}{a_{11}} + a_{rj} & \cdots & a_{rr} \end{pmatrix}$$

We see that the first rows of A and TAT' are identical except for the j^{th} position where A has a non-zero element and TAT' has a zero. Thus with similar choices of T for any non-zero elements of the first row of A (excluding of course a_{11}) we can obtain a matrix of the form

$$a_{11} \oplus B \ .$$

Continuing with B as we did for A, we first assume that b_{11} is a non-zero element and then find a nonsingular matrix T which will transform B into $b_{11} \oplus C$. If we then apply $I_1 \oplus T$ to $a_{11} \oplus B$ we will obtain

$$a_{11} \oplus b_{11} \oplus C \ .$$

Continuation of the process will bring us eventually to the following form

$$\oplus d_i \oplus K \quad \text{for } i = 1, 2, \cdots, n$$

with each d_i a non-zero element and where K has all zeros on the diagonal and is nonsingular of rank $r-n$. By lemma 2.2, there exists a nonsingular matrix T such that $TKT' = \oplus P_j$ $j = 1, 2, \cdots, k$ and K has rank $2k$. Thus acting on $\oplus d_i \oplus K$ by $I_n \oplus T$ we will have

$$\oplus d_i \oplus P_j \quad \text{for } i=1, 2, \cdots, n, \quad j=1, 2, \cdots, k,$$

with each d_i a non-zero element and $n = r-2k$.

We will now find our reduction form for all symmetric matrices over any field of characteristic two in the following theorem.

Theorem 2.1. Let A be a symmetric matrix over a field F of characteristic two. Then there exists a nonsingular matrix T such that;

a) $TAT' = \oplus d_i \oplus Z$ for $i = 1, 2, \cdots, r$

each d_i is a non-zero element and the rank of A is r,

or

b) $TAT' = \oplus P_j \oplus Z$ for $j = 1, 2, \cdots, k$

and the rank of all A is $2k$.

Proof. Let A be a symmetric matrix of order m and rank $r \leq m$. For A singular $(r < m)$, there are r linearly independent row vectors of A and $m-r$ dependent row vectors of A. For a nonsingular matrix T, TAT' will also have r linearly independent and $m-r$ dependent row vectors [4, p. 78]. Thus there exists a nonsingular matrix T such that TAT' has r non-zero, linearly independent row vectors, and the other $m-r$ rows are the zero vector. But since A is symmetric, $(TAT')' = T'A'T' = TAT'$, and TAT' is also symmetric. Thus TAT' has $m-r$ zero column vectors also. Without loss of generality we can assume that the first r rows (columns) are the non-zero rows (columns), thus

$$TAT' = \begin{pmatrix} A_r & Z \\ Z & Z \end{pmatrix} = A_r \oplus Z$$

where Z is the zero matrix, and A_r is nonsingular of rank r. For A nonsingular clearly the dimension of Z is zero.

Let's look now at only the nonsingular block A_r of rank r. We have the following two cases.

Case I. If A_r has no non-zero elements on the diagonal.

Case II. If A_r has at least one non-zero element on the diagonal.

Case I. By lemma 2.2 there exists a nonsingular matrix T such that TA_rT' is of the form

$$\oplus P_j \text{ for } P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } j = 1, 2, \cdots, k ,$$

where the rank of A_r is $2k$.

Case II. By lemma 2.4 there exists a nonsingular matrix T such that TA_rT' is of the form

$$\oplus d_i \oplus P_j \quad i = 1, 2, \cdots, n, \quad j = 1, 2, \cdots, k ,$$

with each d_i a non-zero element and $n = r-2k$.

i) If k equals zero we have

$$TAT' = \oplus d_i \quad i = 1, 2, \cdots, r .$$

ii) If k does not equal zero we have

$$TA_rT' = \oplus d_i \oplus P_j \quad i = 1, 2, \cdots, n, \quad j = 1, 2, \cdots, k$$

with each d_i a non-zero element and $n = r-2k$. Let $TA_rT' = B$. We first assume $n = 1$, $k = 1$. Then

$$B = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

and for T we choose

$$T_1 = \begin{pmatrix} 1 & 0 & d_1 \\ 1 & 1 & d_1 \\ 1 & 1 & 0 \end{pmatrix} .$$

We have

$$T_1BT_1' = \begin{pmatrix} 1 & 0 & d_1 \\ 1 & 1 & d_1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} d_1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ d_1 & d_1 & 0 \end{pmatrix} = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_1 & 0 \\ 0 & 0 & d_1 \end{pmatrix} .$$

Now let's look at $B = \oplus d_i \oplus P_j$ for $i = 1, 2, \cdots, n$; $j = 1, 2, \cdots, k$ $(k > 1)$.

Rewriting we get $B = \oplus d_i \oplus d_n \oplus P_1 \oplus P_j$ for $i = 1, 2, \cdots, n-1$; $j = 2, \cdots, k$.

Now choosing $T = I_{n-1} \oplus T_1 \oplus I_{2(k-1)}$ we have

$$TBT' = \oplus d_i \oplus T_1(d_n \oplus P_1)T_1' \oplus P_j, \quad i = 1, \cdots, n-1; \; j = 2, \cdots, k$$

which by our calculations for the case where $k = 1$, $n = 1$ reduces to

$$\oplus d_i \oplus d_n \oplus d_n \oplus d_n \oplus P_j, \quad i=1,\cdots,n-1;\ j=2,\cdots,k\ .$$

Continuing this process using similar choices for T with respective changes in the dimensions of the I blocks we will eventually arrive at the following form.

$$\oplus d_i \oplus d_n \oplus d_n \oplus \cdots \oplus d_n, \quad i = 1,\cdots,n-1$$

and there are $2k+1$ d_n's. Thus for Case II there always exists a nonsingular matrix T such that

$$TA_rT' = \oplus d_i \quad i = 1,2,\cdots,r\ .$$

If we now choose $S = T \oplus I_{n-r}$ where T is the nonsingular matrix reducing A_r to either the form of Case I or of Case II then,

$$S(A_r \oplus Z)\,S'$$

is either of the form

(a) $\oplus d_i \oplus Z$ for $i = 1,2,\cdots,r$

with each d_i a non-zero element,

or

$$\text{(b)} \quad \oplus P_j \oplus Z \quad \text{for} \quad j = 1, 2, \cdots, k$$

and the proof of our theorem is complete.

Certainly the reduced form in (a) of theorem 2. 1 is not canonical: For $T = \lambda I$ where $\lambda^2 \neq 1$,

$$T(\oplus d_i \oplus Z)T' = \oplus \lambda^2 d_i \oplus Z \neq \oplus d_i \oplus Z.$$

In a perfect field of characteristic two, however, we do have a canonical form and we find it in the following theorem.

Theorem 2. 2. Every symmetric matrix A of rank r over a perfect field F of characteristic two is congruent to one and only one matrix B of the following forms;

a) $B = I_r \oplus Z$, where A has rank r

b) $B = \oplus P_j \oplus Z$, $j = 1, 2, \cdots, k$ and A has rank $r=2k$.

If the matrix A has at least one non-zero element on the diagonal then by theorem 2. 1 there exists a nonsingular matrix T such that TAT' is of the form $\oplus d_i \oplus Z$ $i = 1, 2, \cdots, r$, where each d_i is a non-zero element. Since our field F is a perfect field of characteristic two for each d_i; there exists a uniquely

determined element $\sqrt{d_i}$ contained in F. Choosing $S = (s_{ij})$ with

$$s_{ii} = \frac{1}{\sqrt{d_i}} \qquad i = 1, 2, \cdots, r ,$$

ones on the rest of the diagonal, zeros elsewhere ,

we have

$$STAT'S' = I_r \oplus Z .$$

If A has no non-zero elements on the diagonal, then by theorem 2.1 there exists a nonsingular matrix T such that TAT' is of the form $\oplus P_j \oplus Z$, $j = 1, 2, \cdots, k$.

It follows immediately from lemma 2.3 that no matrix of the form in (a) can be congruent to a matrix of the form in (b) since one has some non-zero diagonal elements and the other has no non-zero diagonal elements. Also, congruent matrices have the same rank. Hence the theorem is proved.

Since all finite fields are perfect [5, p. 124], we then have a canonical form for all symmetric matrices over $GF[2^n]$.

CHAPTER III. SOLUTIONS OF QUADRATIC FORMS IN $GF[2^n]$

The results of this chapter, theorem 3. 1, as stated in the introduction is an analog of theorems 0. 2 and 0. 3. We find the number of solutions of an arbitrary quadratic form in a finite field of characteristic two. Before we proceed to the proof of theorem 3. 1 we prove the following three lemmas.

Lemma 3. 1. The number of solutions $x = (x_1, x_2, \cdots, x_m)$ in $GF[2^n]$ of the equation

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_mx_m^2 = b,$$

where every a_i is a non-zero element in $GF[2^n]$ and b is any given element in $GF[2^n]$, is q^{m-1}.

Proof. Rewriting our given equation as

$$a_1x_1^2 = b + a_2x_2^2 + \cdots + a_ma_m^2$$

and solving for x_1 (our choice of x_1 was completely arbitrary) we get

$$x_1 = \left(\frac{b+a_2x_2^2 + \cdots + a_mx_m^2}{a_1} \right)^{1/2}$$

which in $GF[2^n]$ is uniquely determined. Since b was given,

any choice for the $x_2, x_3, \cdots, x_m$ will completely determine x_1 and the number of solutions x is just the total number of these choices. There are q choices for each of the $m-1$ unknowns $x_2, x_3, \cdots, x_m$ giving us a total of q^{m-1} choices. Notice that for $a_1 x_1^2 = b$ we have one solution.

Lemma 3.2. The number of solutions $x = (x_1, x_2, \cdots, x_{2m})$ in $GF[2^n]$ of the equation

$$x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m} = b,$$

is

$$q^{2m-1} + q^m - q^{m-1} \qquad (\text{if } b = 0)$$

$$q^{2m-1} - q^{m-1} \qquad (\text{if } b \neq 0).$$

Proof by mathematical induction. For the case $m = 1$ we have

$$x_1x_2 = b.$$

If $b = 0$, for $x_1 = 0$ we have q choices for x_2. For each of the $q-1$ non-zero choices of x_1 we have one choice for x_2, giving us a total of $q + q - 1$ solutions.

If $b \neq 0$, for each of the $q-1$ non-zero choices for x_1 we have one choice for x_2, thus we have $q-1$ solutions and our

lemma is true for $m = 1$.

Assuming the lemma is true for equations in $2(m-1)$ variables, we would have

$$q^{2m-3} - q^{m-2} \qquad (\text{if } b \neq 0),$$

$$q^{2m-3} + q^{m-1} - q^{m-2} \qquad (\text{if } b = 0),$$

solutions $x = (x_1, x_2, \cdots, x_{2(m-1)})$. Now let's look at the given equation in $2m$ variables.

If $b = 0$, we have the given equation equivalent to

$$x_1x_2 + x_3x_4 + \cdots + x_{2m-3}x_{2(m-1)} = x_{2m-1}x_{2m}.$$

This equation is equivalent to the system of two equations

$$(1) \quad x_1x_2 + x_3x_4 + \cdots + x_{2m-3}x_{2(m-1)} = c$$

$$(2) \quad x_{2m-1}x_{2m} = c. \quad (c \in GF[2^n])$$

If $c = 0$, we have $q^{2m-3} + q^{m-1} - q^{m-2}$ solutions for (1) and $2q-1$ solutions for (2). If $c \neq 0$, we have for each of the $q-1$ non-zero choices of c, $q^{2m-3} - q^{m-2}$ solutions for (1) and $q-1$ solutions for (2). The total number of solutions $x = (x_1, x_2, \cdots, x_{2m})$ is therefore

$$(2q-1)(q^{2m-3}+q^{m-1}-q^{m-2}) + (q-1)^2(q^{2m-3}-q^{m-2})$$

$$=2q^{2m-2}+2q^{m}-2q^{m-1}-q^{2m-3}-q^{m-1}+q^{m-2}+q^{2m-1}-q^{m}-qa^{2m-2}+2q^{m-1}+q^{2m-3}-q^{m-2}$$

$$= q^{m}-q^{m-1} + q^{2m-1} .$$

If $b \neq 0$, our given equation is equivalent to the system of two equations

$$(3) \qquad x_1x_2 + x_3x_4 + \cdots + x_{2m-3}x_{2(m-1)} = b+c$$

$$(4) \qquad x_{2m-1}x_{2m} = c .$$

If $c = 0$, we have $2q-1$ solutions for (4) and $q^{2m-3}-q^{m-2}$ solutions for (3). If $c = b$, we have $q-1$ solutions for (4) and $q^{2m-3} + q^{m-1} - q^{m-2}$ solutions for (3). If $c \neq b$, and $c \neq 0$, we have for each one of the $q-2$ choices of c, $q-1$ solutions for (4) and $q^{2m-3}-q^{m-2}$ solutions for (3). The total number of solutions $x = (x_1, x_2, \cdots, x_{2m})$ is therefore

$$(2q-1)(q^{2m-3}-q^{m-2})+(q-1)(q^{2m-3}+q^{m-1}-q^{m-2})+(q-2)(q-1)(q^{2m-3}-q^{m-2})$$

$$= 2q^{2m-2}-2q^{m-1}-q^{2m-3}+q^{m-2}+q^{2m-2}+q^{m}-q^{m-1}-q^{2m-3}-q^{m-1}+q^{m-2}$$

$$+ q^{2m-1}-q^{m}-3q^{2m-2}+3q^{m-1}+2q^{2m-3}-2q^{m-2}$$

$$= q^{2m-1}-q^{m-1} .$$

Lemma 3.3. If $x_1x_2 + \lambda x_1^2 + \lambda x_2^2$ is an irreducible polynomial in $GF[2^n]$ then the equation

$$x_1x_2 + \lambda x_1^2 + \lambda x_2^2 = b, \quad \lambda \neq 0,$$

has $q + 1$ solutions $x = (x_1, x_2)$ if $b \neq 0$, and only the obvious solution $(0, 0)$ if $b = 0$.

Proof. If $b = 0$, let's assume (α, β) is another solution to the given equation other than the solution $(0, 0)$ then both α and β cannot be zero. Since the given equation is unchanged if x_1 and x_2 are replaced by $-x_1$ and $-x_2$, if (α, β) is a solution (β, α) is also. In any case there exists a non-zero solution for x_2, let's assume it is β. Then if (α, β) is a solution of the given equation, $\beta x_1 + \alpha x_2$ must divide $\lambda x_1^2 + \lambda x_2^2 + x_1x_2$. (Performing the division leads us to the second factor $\frac{\lambda}{\beta} x_1 + (\frac{\lambda\alpha}{\beta^2} + \frac{1}{\beta}) x_2$.) But this contradicts the statement in our theorem which says the polynomial $\lambda x_1^2 + \lambda x_2^2 + x_1x_2$ is irreducible, so we must have only the trivial solution $(0, 0)$ leaving q^2-1 other possible solutions $x=(x_1, x_2)$ for

$$\lambda x_1^2 + \lambda x_2^2 + x_1x_2 = b, \qquad b \neq 0 .$$

Let's denote this set of q^2-1 other solutions as

$$S = \{x \mid x \neq (0, 0)\}.$$

Let $(\alpha, \beta) \in S$ be a solution of our given equation for some fixed $b_0 \neq 0$ and let's look at the subset of S,

$$T = \{\nu(\alpha, \beta) = (\nu\alpha, \nu\beta) \mid \nu \neq 0\}.$$

T has $q-1$ elements. For any $\nu \neq 0$, $\nu(\alpha, \beta)$ is a solution of

$$\lambda(\nu\lambda)^2 + \lambda(\nu\beta)^2 + (\nu\alpha)(\nu\beta) = \nu^2\lambda\alpha^2 + \nu^2\lambda\beta^2 + \nu^2\alpha\beta = \nu^2 b_0 .$$

Let $\nu^2 b_0 = c$; then solving for ν we get $\nu = (\frac{c}{b_0})^{1/2}$ which is uniquely determined in a field of characteristic two. But we have $q-1$ choices for $\nu \neq 0$, each giving us a different value of $c \neq 0$ since b_0 is fixed. Thus in our subset T we have one solution for every non-zero element c.

Let (γ, δ) be any other element of S. As above, we can define

$$V = \{\nu(\gamma, \delta) = (\nu\gamma, \nu\delta) \mid \nu \neq 0\}$$

and show that the subset V also contains one solution for every non-zero element c. We wish to show that either $T = V$ or they are disjoint. But if $\mu(\alpha, \beta) = \nu(\gamma, \delta) \neq 0$, then $(\gamma, \delta) = (\nu^{-1}\mu)(\alpha, \beta) \in T$ and $V \subset T$. Similarly $T \subset V$, so $T = V$.

If we continue in this manner until we exhaust the q^2-1 solutions contained in S, we will have $q+1$ disjoint subsets of S, each containing one and only one solution for every non-zero element in the field. Thus we will have $q+1$ solutions

$x = (x_1, x_2)$ for the equation

$$\lambda x_1^2 + \lambda x_2^2 + x_1 x_2 = b$$

for each non-zero b contained in $GF[2^n]$.

The following theorem of L. E. Dickson gives us two canonical forms for certain quadratic forms in $GF[2^n]$ [3, p. 197].

Theorem. If a quadratic form with coefficients in $GF[2^n]$ cannot be expressed in the field as a quadratic form in fewer than m linear homogeneous functions of $x_1, x_2, \cdots, x_m$, it can be reduced by a linear homogeneous substitution belonging to the field to one of the canonical forms.

$$F \equiv x_1 x_2 + x_3 x_4 + \cdots + x_{m-2} x_{m-1} + x_m^2 \qquad (m \text{ odd})$$

$$F_\lambda \equiv x_1 x_2 + x_3 x_4 + \cdots + x_{m-3} x_{m-2} + x_{m-1} x_m + \lambda x_{m-1}^2 + \lambda x_m^2 \qquad (m \text{ even})$$

where λ is zero or is a particular one of the values λ' for which

$$Q \equiv x_{m-1} x_m + \lambda' x_{m-1}^2 + \lambda' x_m^2$$

is irreducible in $GF[2^n]$.

In the following theorem we will find the number of solutions for any quadratic form over a field of characteristic two. Those

which can not be reduced to a quadratic form in fewer than m linear homogeneous functions of $x_1, x_2, \cdots, x_m$, we find by finding the number of solutions to the two canonical forms. Those which can be reduced to a quadratic form in fewer than m linear homogeneous functions of $x_1, x_2, \cdots, x_m$, we find in terms of the number of solutions of the canonical form of the quadratic form expressed in the minimal number of linear homogeneous functions of $x_1, x_2, \cdots, x_m$.

Theorem 3.1. The number of solutions of an arbitrary quadratic form over $GF[2^n]$ can be found in one of the following.

(a) The number of solutions $x = (x_1, x_2, \cdots, x_{2m+1})$ of a quadratic form f, reducible to the canonical form

$$F \equiv x_1x_2 + \cdots + x_{2m-1}x_{2m} + x_{2m+1}^2 = b,$$

is

$$(*)q^{2m}$$

(b) The number of solutions $x = (x_1, x_2, \cdots, x_{2m})$ of a quadratic form f, reducible to the canonical form

$$F_\lambda \equiv x_1x_2 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}x_{2m} + \lambda x_{2m-1}^2 + \lambda x_{2m}^2 = b,$$

where λ is zero or is a particular one of the values λ' for which

$$Q \equiv x_{2m-1}x_{2m} + \lambda' x_{2m-1}^2 + \lambda' x_{2m}^2$$

is irreducible in $GF[2^n]$, is

$$(*)\qquad \begin{cases} q^{2m-1} + q^m - q^{m-1} & \text{if } \lambda = 0, \quad b = 0, \\ q^{2m-1} - q^{m-1} & \text{if } \lambda = 0, \quad b \neq 0, \\ q^{2m-1} - q^m + q^{m-1} & \text{if } \lambda \neq 0, \quad b = 0, \\ q^{2m-1} + q^{m-1} & \text{if } \lambda \neq 0, \quad b \neq 0. \end{cases}$$

(c) The number of solutions $x = (x_1, x_2, \cdots, x_m)$ of a quadratic form f, expressible in the field as a quadratic form in a minimal number $s (s < m)$ of linear homogeneous functions of $x_1, x_2, \cdots, x_m$, is the product of q^{m-s} and (*) of part (a) with $2m+1 = s$ or part (b) with $2m = s$ depending upon whether s is odd or even.

Proof. (a) There is a simple proof of (a) which is similar to the proof of lemma 3.1.

(b) If $\lambda = 0$, we have

$$x_1x_2 + \cdots + x_{2m-1}x_{2m} = b$$

which by lemma 3.2 has

$q^{2m-1} + q^m - q^{m-1}$ solutions if $b = 0$,

$q^{2m-1} - q^{m-1}$ solutions if $b \neq 0$.

If $\lambda \neq 0$, we have

$$x_1x_2+\cdots+x_{2m-1}x_{2m}+\lambda x_{2m-1}^2+\lambda x_{2m}^2 = b.$$

For $m = 1$ this reduces to

$$x_1x_2 + \lambda x_1^2 + \lambda x_2^2 = b$$

which by lemma 3.3 has one solution if $b = 0$, and $q+1$ solutions if $b \neq 0$, and our theorem is true for $m = 1$.

Now let's look at our given equation in more than two variables. If $b = 0$ the given equation is equivalent to

$$x_1x_2+\cdots+x_{2m-3}x_{2m-2}=x_{2m-1}x_{2m}+\lambda x_{2m-1}^2+\lambda x_{2m}^2$$

which is equivalent to the system of two equations

(1) $x_1x_2 + \cdots + x_{2m-3}x_{2m-2} = c$

(5) $x_{2m-1}x_{2m}+\lambda x_{2m-1}^2+\lambda x_{2m}^2 = c$.

If $c = 0$, we have $q^{2m-3} + q^{m-1} - q^{m-2}$ solutions for (1) and one solution for (5). If $c \neq 0$, we have for each of the $q-1$ non-zero choices of c, $q^{2m-3}-q^{m-2}$ solutions for (1) and $q+1$ solutions for (5). The total number of solutions $x = (x_1, \cdots, x_{2m})$ is therefore

$$q^{2m-3}+q^{m-1}-q^{m-2}+(q-1)(q+1)(q^{2m-3}-q^{m-2})$$

$$= q^{2m-3}+q^{m-1}-q^{m-2}+q^{2m-1}-q^{m}-q^{2m-3}+q^{m-2}$$

$$= q^{2m-1}-q^{m}+q^{m-1}.$$

If $b \neq 0$, our given equation is equivalent to the system of two equations

$$(3) \quad x_1x_2 + \cdots + x_{2m-3}x_{2m-2} = b+c$$

$$(6) \quad x_{2m-1}x_{2m}+\lambda x_{2m-1}^2+\lambda x_{2m}^2 = c .$$

If $c = 0$, we have $q^{2m-3} - q^{m-2}$ solutions for (3) and one solution for (6). If $c = b$, we have $q^{2m-3} + q^{m-1} - q^{m-2}$ solutions for (3) and $q+1$ solutions for (6). If $c \neq b, 0$, for each of the $q-2$ choices of c, we have $q^{2m-3} - q^{m-2}$ solutions for (3) and $q+1$ solutions for (6). The total number of solutions $x=(x_1,\cdots,x_{2m})$ is therefore

$$q^{2m-3}-q^{m-2}+(q+1)(q^{2m-3}+q^{m-1}-q^{m-2})+(q-2)(q+1)(q^{2m-3}-q^{m-2})$$

$$= q^{2m-3}-q^{m-2}+q^{2m-2}+q^{m}-q^{m-1}+q^{2m-3}+q^{m-1}-q^{m-2}$$

$$+ q^{2m-1}-q^{m}-q^{2m-2}+q^{m-1}-2q^{2m-3}+2q^{m-2}$$

$$= q^{2m-1} + q^{m-1} .$$

(c) Let's suppose that f is expressible in a minimum number of linear homogeneous functions of $x_1, x_2, \cdots, x_m$, say s. Let's label these s functions $y_1, y_2, \cdots, y_s$. Thus we have

$$y_i = \sum_{j=1}^{m} d_{i_j} x_j \qquad \text{for} \quad i = 1, 2, \cdots, s,$$

which is a system of s equations in m variables $(m > s)$. Suppose the y_i's are linearly dependent functions of the x_j's. Let's assume y_s is a linear combination of the other $s-1$ y's. Then we have

$$y_i = \sum_{j=1}^{m} d_{i_j} x_j \qquad \text{for} \quad i = 1, 2, \cdots, s-1,$$

$$y_s = \sum_{\ell=1}^{s-1} \delta_\ell y_\ell \quad .$$

Looking at the quadratic form in the s y's we have

$$F \equiv \sum_{k,\ell=1}^{s} \gamma_{k\ell} y_k y_\ell$$

$$= \sum_{k,\ell=1}^{s-1} \gamma_{k\ell} y_k y_\ell + \sum_{k=1}^{s-1} \gamma_{ks} y_k y_s + \gamma_{ss} y_s^2 = \sum_{k,\ell}^{s-I} \gamma_{k\ell} y_k y_\ell + \sum_{k=1}^{s-1} \gamma_{ks} y_k \Big(\sum_{\ell=1}^{s-1} \delta_\ell y_\ell\Big)$$

$$+ \gamma_{ss} \Big(\sum_{\ell=1}^{s-1} \delta_\ell y_\ell\Big)^2 = \sum_{k,\ell}^{s-1} \gamma_{k\ell} y_k y_\ell + \sum_{\ell=1}^{s-1} \eta_\ell y_\ell^2 + \sum_{\substack{k,\ell \\ k \neq \ell}}^{s-1} \eta_{k\ell} y_k y_\ell + \gamma_{ss} \sum_{\ell=1}^{s-1} \delta_\ell^2 y_\ell^2 ,$$

where the η's depend upon the constants γ_{ks} and δ_{ℓ}. But this is a quadratic form in $s-1$ y's thus contradicting our supposition that s was the minimal number of linear homogeneous functions of $x_1, x_2, \cdots, x_m$.

Suppose now that the y_i's are linearly independent functions. We can apply part (a) of this theorem, if s is odd or part (b), if s is even and find the number of solutions $(k_1, k_2, \cdots, k_s)$ where $y_i = k_i$ $i = 1, 2, \cdots, s$. Since we are interested in finding the number of solutions $(x_1, x_2, \cdots, x_m)$, for each solution $(k_1, \cdots, k_s)$ of the y_i's we must solve the system of equations

$$k_i = \sum_{j=1}^{m} d_{i_j} x_j \quad \text{for} \quad i = 1, 2, \cdots, s.$$

Since the rank of the coefficient matrix of the system is s, reducing the system to echelon form leaves $m-s+1$ variables in the last equation. This means we have s variables uniquely determined and $m-s$ variables arbitrary, giving us q^{m-s} solutions $(x_1, x_2, \cdots, x_m)$ for each solution $(k_1, k_2, \cdots, k_s)$ of the y's.

We can also have lemma 3.1 as a special case of theorem 3.1 (c). If every $a_{ij} (i, j = 1, 2, \cdots, m;\ i < j)$ were zero f would reduce to

$$(\sqrt{a_{11}} x_1 + \cdots + \sqrt{a_{mm}} x_m)^2 .$$

Thus $s = 1$, and we have

$$q^{m-s} \cdot q^{0} = q^{m-1} .$$

CHAPTER IV. EVALUATING $N_t(A, B)$ IN $GF[2^n]$

The final results of this thesis are given in the following theorem.

Theorem 4. 1. (i) The value of $N_t(A, B)$ in $GF[2^n]$ if B is congruent to the form in (a) of theorem 2. 2 is,

$$q^{mt-\frac{t(t+1)}{2}}, \quad (t \leq m).$$

ii) The value of $N_t(A, B)$ in $GF[2^n]$ if B is congruent to the form in (b) of theorem 2. 2 is,

$$q^{km-k^2} \prod_{i=0}^{2k-1} (q^{m-2i}-1), \quad (t = 2k \leq m = 2r).$$

Proof. We have already shown that a symmetric matrix A over a finite field of characteristic two is congruent to either the form in (a) or in (b) of theorem 2. 2.

i) Suppose that B is reducible to the diagonal form in (a) I_t and that $t \geq 1$, we shall first set up a recursion formula for $N_t(A, B)$. Let X be a solution of our equation

$$X'AX = I_t$$

with first column a so that

$$a'Aa = 1 .$$

Then we note from our work in Chapter II that there exists an m by $m-1$ matrix C such that $U = (a|C)$ is unimodular. By properly picking C we have

$$U'AU = \begin{pmatrix} 1 & z' \\ z & A_1 \end{pmatrix}$$

where z represents the column vector $(0, 0, \cdots, 0)$. Now we set $X = UY$, where

$$Y = \begin{pmatrix} 1 & \beta' \\ \delta & X_1 \end{pmatrix}$$

with β and δ column vectors. Since U is unimodular and a is the first column of X it follows that $\delta = z$; next calculating

$$X'AX = Y'U'AUY = \begin{pmatrix} 1 & z' \\ \beta & X_1' \end{pmatrix} \begin{pmatrix} 1 & z' \\ z & A_1 \end{pmatrix} \begin{pmatrix} 1 & \beta' \\ z & X_1 \end{pmatrix} = \begin{pmatrix} 1 & \beta' \\ \beta & X'A_1X_1 \end{pmatrix}$$

$$= I_t ,$$

we conclude that $\beta = z$. Hence we have $X_1'A_1X_1$ equal to the diagonal matrix $B_1 = I_{t-1}$. To find all solutions X we must first find all solutions a of

$$a'Aa = 1 ;$$

next for each a we choose U and construct A_1 as described above. This procedure can be expressed by means of the recursion formula

$$N_t(A, B) = \sum_a N_{t-1}(A_1, B_1),$$

where the summation is over all a satisfying

$$a'Aa = 1 .$$

Using mathematical induction on t we have for $t = 1$,

$$q^{mt - \frac{t(t+1)}{2}} = q^{m-1},$$

and the theorem is true.

For $t > 1$ assume the truth of the theorem with t replaced by $t-1$. Then we have

$$N_{t-1}(A, B) = q^{(m-1)(t-1) - \frac{(t-1)(t)}{2}} .$$

From our construction of A_1 we have, for unimodular U,

$$U'AU = I_1 \oplus A_1$$

thus $\delta(A) = \delta(A_1)$, but this means that every summation in our recursion formula will be summed over the same number of solutions,

namely the solutions of

$$a'Aa = 1,$$

which we have already found to be q^{m-1}. Thus

$$N_t(A,B) = N_{t-1}(A,B)\cdot q^{m-1}$$

$$= q^{m-1}\cdot q^{(m-1)(t-1)-\frac{(t-1)(t)}{2}}$$

$$= q^{tm-\frac{2t+(t-1)t}{2}} = q^{tm-\frac{t(t+1)}{2}} .$$

ii) Suppose that B is reducible to the P block-diagonal form in (b) of theorem 2.2 and $k \geq 1$. Following L. Carlitz method [2] we find a recursion formula for $N_t(A,B)$. Now let X be a solution of our equation

$$X'AX = B$$

with first column a and second column b so that

$$(ab)'A(ab) = P .$$

Then we can find an m by $m-2$ matrix C such that $U = (ab|C)$ is nonsingular. We can pick C such that

$$U'AU = \begin{pmatrix} P & Z \\ Z' & A_1 \end{pmatrix} ,$$

where Z represents a 2 by m-2 zero matrix. Now let $X = UY$, where

$$Y = \begin{pmatrix} I_2 & K \\ H & X_1 \end{pmatrix},$$

H is m-2 by 2 and K is 2 by t-2 while X_1 is m-2 by t-2. Since a and b are the first two columns of X and U is nonsingular it follows that $H = Z$. Calculating

$$X'AX = Y'U'AUY = \begin{pmatrix} I_2 & Z \\ K' & X_1' \end{pmatrix} \begin{pmatrix} P & Z \\ Z' & A_1 \end{pmatrix} \begin{pmatrix} I_2 & K \\ Z & X_1 \end{pmatrix}$$

$$= \begin{pmatrix} P & PK \\ K'P & K'PK + X_1'A_1X_1 \end{pmatrix} = B,$$

we must have $K = Z$ also. Hence $X_1'A_1X_1$ is equal to $\oplus P_j$ for $j = 2, 3, \cdots, k$. Thus to find all the solutions of our given equation we first find all solutions V of

$$V'AV = P,$$

where $V = (ab)$ is an m by 2 matrix; next for each V we choose U and construct A_1 as described above. This process can be expressed by the recursion formula

$$N_t(A, B) = \sum_V N_{t-2}(A_1, B_1).$$

Using mathematical induction on k we have for $k = 1$,

$$q^{km-k^2} \prod_{i=0}^{k-1} (q^{m-2i}-1) = q^{m-1} \cdot (q^m-1).$$

Since we can also assume A in our canonical form,

$$V'AV = P$$

reduces to

$$\eta_1\mu_2+\eta_2\mu_1 + \cdots + \eta_{m-1}\mu_m+\eta_m\mu_{m-1} = 1,$$

where $a = (\eta_1\eta_2\cdots\eta_m)$ and $b = (\mu_1\mu_2\cdots\mu_m)$. The number of solutions of this equation given by lemma 3.2 is

$$q^{m-1} \cdot (q^m-1).$$

Thus the theorem is true for $k = 1$.

Now let $k > 1$ and assume the theorem true with r replaced by $r-1$. We notice that each one of the summands on the right side of our recursion formula has the same value. Namely the number of solutions V of the equation

$$V'AV = P$$

which we found to be $q^{m-1} \cdot (q^m-1)$. Therefore from our recursion formula and our inductive hypothesis we have,

$$N_t(A, B) = N_{t-2}(A_1, B_1) \cdot q^{m-1} \cdot (q^m - 1)$$

$$= q^{m-1} \cdot (q^m - 1) \cdot q^{(k-1)(m-2)-(k-1)^2} \prod_{i=0}^{k-2} (q^{m-2-2i} - 1)$$

$$= q^{(km-k^2)} \cdot (q^m - 1) \cdot \prod_{i=0}^{k-2} (q^{m-2-2i} - 1)$$

$$= q^{km-k^2} \cdot \prod_{i=0}^{k-1} (q^{m-2i} - 1) .$$

BIBLIOGRAPHY

1. Carlitz, L. Representations by quadratic forms in a finite field. Duke Mathematical Journal 21: 123-137. 1954.

2. Carlitz, L. Representations by skew forms in a finite field. Archives of Mathematics 5: 19-31. 1954.

3. Dickson, L. E. Linear groups. New York, Dover, 1958. 312 p.

4. Finkbeiner, Daniel T. Matrices and linear transformations. San Francisco, Freeman, 1960. 246 p.

5. Van Der Waerden. Modern algebra. Vol. I. New York, Ungar, 1953. 264 p.