Canad. Math. Bull. Vol. **44** (2), 2001 pp. 242–256

The Zeta Function of a Pair of Quadratic Forms

Laura Mann Schueller

Abstract. The zeta function of a nonsingular pair of quadratic forms defined over a finite field, k, of arbitrary characteristic is calculated. A. Weil made this computation when $\operatorname{char} k \neq 2$. When the pair has even order, a relationship between the number of zeros of the pair and the number of places of degree one in an appropriate hyperelliptic function field is established.

1 Introduction

The goal of this paper is to calculate the zeta function of a nonsingular pair of quadratic forms, $\{F, G\}$, defined over a finite field of arbitrary characteristic. In 1954, Weil [11] completed this calculation for the case $\operatorname{char} k \neq 2$. Thus, this paper extends Weil's work to arbitrary characteristic.

When the order of the pair is odd, our result is a simple extension of Weil's work. A detailed treatment is included, and the zeta function appears as Theorem 4.1.

When the order of the pair is even and $\operatorname{char} k \neq 2$, Weil gives the zeta function in terms of the number of places of degree one in the hyperelliptic function field defined by $y^2 = \det(uF + G)$.

In order to extend this result to $\operatorname{char} k = 2$, we replace the determinant with the more complicated Arf invariant. We first relate the number of places of degree one in the function field defined by $y^2 + y = \operatorname{Arf}(uF + G)$ to the number of affine solutions of the defining curve. This argument is more technical than the one relating points to places in the $\operatorname{char} k \neq 2$ case. A careful calculation of this relationship in the characteristic two case is given in Theorem 3.4, and the known result, as used by Weil, for the odd characteristic case is given in Equation 4.

Finally, we use these results to calculate the zeta function given in Theorem 4.3.

2 Definitions and Preliminaries

Although our main results are given over finite fields, we make some initial definitions and give some preliminary results for an arbitrary field k. The notation $k^{(t)}$ denotes the set of t-tuples with elements in k, k^* denotes the multiplicative group of nonzero elements of k, and k^{alg} denotes the algebraic closure of k. A quadratic form F in n variables defined over k is a homogeneous polynomial of degree two in the polynomial ring $k[x_1, \ldots, x_n]$. Two quadratic forms, $F, F' \in k[x_1, \ldots, x_n]$, are equivalent

Received by the editors December 11, 1998; revised June 1, 1999.
AMS subject classification: 11G25.

over k if there exists an invertible $n \times n$ matrix

$$E = (e_{ij})_{n\times n}$$

with entries in k such that

$$F'(x_1, \ldots, x_n) = F(y_1, \ldots, y_n), \quad \text{for } y_i = \sum_{j=1}^{n} e_{ij}x_j,\ 1 \le i \le n.$$

The order of F is the minimum m such that there exists a quadratic form $F' = \sum_{1\le i\le j\le m} a'_{ij}x_ix_j$ equivalent to F. If $m < n$, then F is degenerate, and if $m = n$, then F is nondegenerate.

Given

$$F = \sum_{1\le i\le j\le m} a_{ij}x_ix_j,$$

let $[F]$ denote the symmetric $n\times n$ matrix $(\alpha_{ij})_{n\times n}$ where $\alpha_{ij} = \begin{cases} a_{ij} & i < j \\ a_{ji} & j < i \\ 2a_{ii} & i = j \end{cases}$. Thus,

$$[F] = \begin{pmatrix} 2a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & & & \\ \vdots & & & \\ a_{1n} & a_{2n} & \cdots & 2a_{nn} \end{pmatrix}.$$

Let $\det(F) = \det([F])$.

Let $\{F, G\}$ and $\{F', G'\}$ be two pairs of quadratic forms defined over k. The pairs are equivalent over k if both F is equivalent to F' and G is equivalent to G' by the same invertible matrix E. The order of the pair $\{F, G\}$ is the minimum m such that there exists a pair of quadratic forms

$$\left\{F' = \sum_{1\le i\le j\le m} a'_{ij}x_ix_j, G' = \sum_{1\le i\le j\le m} b'_{ij}x_ix_j\right\}$$

equivalent to $\{F, G\}$. If $m < n$, then the pair $\{F, G\}$ is degenerate, and if $m = n$, then the pair $\{F, G\}$ is nondegenerate.

A nontrivial n-tuple, P, with entries in k^{alg} is a singular zero of the pair $\{F, G\}$ if $F(P) = G(P) = 0$ and the Jacobian of the pair $\{F, G\}$ evaluated at P has rank at most one. A pair of quadratic forms $\{F, G\}$ defined over k is singular if there exists a singular zero P of the pair. The pair is nonsingular if it is not singular.

It is easy to check that if $\{F, G\}$ is a degenerate pair of quadratic forms, then the pair $\{F, G\}$ is singular.

For the remainder of this paper, assume that $\{F, G\}$ is a nonsingular pair of quadratic forms in $n \ge 3$ variables defined over $k = F_q$, a finite field with q elements. Let k_r be the unique extension of k of degree r.

The following two results can be found in [7].

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Lemma 2.1 *If $\alpha, \beta \in k^{\text{alg}}$ are not both zero, then $\alpha F + \beta G$ has order at least $n-1$.*

Lemma 2.2 *If u and v are indeterminates over k and* $\operatorname{char} k \neq 2$*, then*

$$\det(uF + vG)$$

splits into distinct linear factors over k^{alg}.

2.1 Counting Simultaneous Zeroes of Pairs of Quadratic Forms

Theorem 2.3 *Let H be a quadratic form in n variables defined over k. Then H is equivalent over k to a nondegenerate quadratic form in m variables, for some $1 \leq m \leq n$, of exactly one of the following three types.*

1. $x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m$
2. $x_1x_2 + x_3x_4 + \cdots + x_{m-3}x_{m-2} + (a_0x_{m-1}^2 + a_1x_{m-1}x_m + a_2x_m^2)$, $a_i \in k$, $(a_0x_{m-1}^2 + a_1x_{m-1}x_m + a_2x_m^2$ *irreducible over k*)
3. $x_1x_2 + x_3x_4 + \cdots + x_{m-2}x_{m-1} + ax_m^2$, $a \in k^*$.

From here on, a quadratic form equivalent over k to one of these forms shall be called Type 1, Type 2, or Type 3, respectively. This well known classification can be found in [8] or [9].

Definition 2.4 Let $\chi_r \colon k_r \to \mathbb{C}$ be given by $\chi_r(a) = 0, 1, -1$ as a is 0, a nonzero square, or a nonsquare in k_r, respectively.

For ease of notation, we write $\chi(a)$ for $\chi_1(a)$. For later use, note that

$$\chi(-1)^r = \chi_r(-1).$$

Definition 2.5 The pencil, $P_r(F, G)$, of the pair $\{F, G\}$ is the set of all k_r-linear combinations of F and G. That is,

$$P_r(F, G) = \{uF + vG \mid u, v \in k_r\}.$$

Definition 2.6 For each r, we define a function $s_r : P_r(F, G) \to \mathbb{C}$ by

$$s_r(uF + vG) = \begin{cases} 1 & \text{if } uF + vG \text{ is Type 1 over } k_r \\ -1 & \text{if } uF + vG \text{ is Type 2 over } k_r \\ 0 & \text{if } uF + vG \text{ is Type 3} \\ 1 & \text{if } u, v = 0. \end{cases}$$

We note that since a Type 2 form remains Type 2 in a field extension if and only if the degree of the extension is odd, it follows that

$$s_r(uF + vG) = \left(s_d(uF + vG)\right)^{\frac{r}{d}}$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

for all $d|r$.

For ease of notation, we write $s(uF + vG)$ for $s_1(uF + vG)$.

Given r, let

$$N = \left|\{P \in k_r^{(n)} \mid F(P) = G(P) = 0\}\right|,$$

the number of affine zeros of the pair over k_r.

An argument given in [6] gives

$$N = (q^r)^{-2}\Big[(q^r)^n + \sum_{(u,v)\neq(0,0)\in k_r^{(2)}} s_r(uF + vG)(q^r)^{n-\frac{m_{(u,v)}}{2}}\Big]$$

where $m_{(u,v)}$ is the order of the form $uF + vG$.

We now consider projective zeros. Let N_r denote the number of simultaneous projective zeros of the pair $\{F, G\}$ over k_r. Then,

$$N_r = \sum_{h=0}^{n-3}(q^r)^h + \frac{(q^r)^{-2}}{q^r - 1}\sum_{(u,v)\neq(0,0)\in k_r^{(2)}} s_r(uF + vG)(q^r)^{n-\frac{m_{(u,v)}}{2}}.$$

Since the pair $\{F, G\}$ is nonsingular, it follows from Lemma 2.1 that if $m_{(u,v)} \neq 0$, then $m_{(u,v)}$ is either $n-1$ or n. Since $s_r(uF + vG) = 0$ if $m_{(u,v)}$ is odd, it follows that if n is odd, then

$$N_r = \sum_{h=0}^{n-3}(q^r)^h + \frac{(q^r)^{\frac{n-3}{2}}}{q^r - 1}\sum_{\substack{(u,v)\in k_r^{(2)}\\ m_{(u,v)}=n-1}} s_r(uF + vG), \tag{1}$$

and if n is even, then

$$N_r = \sum_{h=0}^{n-3}(q^r)^h + \frac{(q^r)^{\frac{n-4}{2}}}{(q^r) - 1}\sum_{(u,v)\neq(0,0)\in k_r^{(2)}} s_r(uF + vG). \tag{2}$$

2.2 The Arf Invariant

Recall that k is finite and we will assume for this subsection that $\operatorname{char} k = 2$; thus k is perfect. Also for this subsection, assume n is even. Then, for any quadratic form H in n variables defined over k, one can check that $\det(H) = 0$ if and only if H is degenerate.

Denote $\{x^2 + x \mid x \in k\}$, the Artin-Schreier subgroup of k, by $\wp(k)$. Given a nondegenerate quadratic form H in n variables defined over k, the Arf invariant of H, $\operatorname{Arf}(H)$, lies in k. If H' is a nondegenerate quadratic form in n variables defined over k equivalent to H, then $\operatorname{Arf}(H) - \operatorname{Arf}(H') \in \wp(k)$.

A direct calculation gives that $\operatorname{Arf}(H) \in \wp(k)$ if H is Type 1 and $\operatorname{Arf}(H) \notin \wp(k)$ if H is Type 2.

Suppose u and v are indeterminates over k, then $uF + vG$ is a quadratic form in n variables defined over $k(u, v)$. In characteristic two, $\det[F]$ is always a square.

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Therefore, $\det(uF + vG)$ is a square in $k[u, v]$, and it factors into linear factors over k^{alg}. Therefore, there is a factorization $\det(uF + vG) = \delta^2 v^{2l_0} \Pi_{i=1}^{r} (u + a_i v)^{2l_i} \neq 0$ for some $\delta \in k$, a_i distinct in k^{alg}, $l_0 \geq 0$, and $l_i \geq 1$ for $1 \leq i \leq r$. The following result for nonsingular pairs $\{F, G\}$ can be found in [7], (4.3) and (5.10).

Proposition 2.7 *Suppose $\{F, G\}$ is a nonsingular pair over k in n variables. Using the notations above,*

$$\operatorname{Arf}(uF + vG) = \sum_{i=1}^{r} \sum_{j=0}^{2l_i - 1} \frac{c_{ij}(u + a_i v)^j v^{2l_i - j}}{(u + a_i v)^{2l_i}} + \sum_{j=0}^{2l_0 - 1} \frac{c_{0j} u^{2l_0 - j} v^j}{v^{2l_0}} + c_{0,2l_0},$$

where each $c_{ij} \in k^{\text{alg}}$ is uniquely determined and

$$c_{i1} \neq \begin{cases} 0 & \text{if } l_i \geq 2 \\ \sqrt{c_{i0}} & \text{if } l_i = 1. \end{cases}$$

Sometimes we set $v = 1$. In this case, we write

$$\operatorname{Arf}(uF + G) = \frac{f(u)}{g(u)^2}$$

where $g(u)^2 = \det(uF + G)$, $f(u) \in k[u]$, and for any a_i, $1 \leq i \leq r$, $(u + a_i)^2$ doesn't divide $f(u)$ since c_{i0} and c_{i1} are not both zero.

Proposition 2.8

$$\operatorname{Arf}(uF + G) \notin \wp\left(k(u)\right).$$

Proof Suppose, in contradiction, that

$$\operatorname{Arf}(uF + G) = \frac{f(u)}{g(u)^2} = \frac{h_1(u)}{h_2(u)} + \left(\frac{h_1(u)}{h_2(u)}\right)^2$$

for $h_1, h_2 \in k[u]$ with h_1 and h_2 having no common factors over k^{alg}.

By Proposition 2.7, we can write

$$\operatorname{Arf}(uF + G) = \frac{f(u)}{g(u)^2} = \sum_{i=1}^{r} \sum_{j=0}^{2l_i - 1} \frac{c_{ij}(u + a_i)^j}{(u + a_i)^{2l_i}} + \sum_{j=0}^{2l_0} c_{0j} u^{2l_0 - j},$$

where each $c_{ij} \in k^{\text{alg}}$ is uniquely determined and

$$c_{i1} \neq \begin{cases} 0 & \text{if } l_i \geq 2 \\ \sqrt{c_{i0}} & \text{if } l_i = 1. \end{cases}$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

For $1 \leq i \leq r$, $(u+a_i)^{l_i} | g$. By cross multiplying, $(u+a_i)^{2l_i} | f h_2^2$. Since $(u+a_i)^2$ does not divide $f(u)$, it follows that $(u+a_i)^{2l_i-1} | h_2(u)^2$ and $(u+a_i)^{l_i} | h_2(u)$. Thus, $g | h_2$. Since h_1 and h_2 are relatively prime, it is easy to show that $h_2 | g$. Thus, without loss of generality, we can assume $h_2 = g$.

There exist unique $d_{ij} \in k^{\text{alg}}$ such that

$$\frac{h_1}{g} = \sum_{i=1}^{r} \sum_{j=0}^{l_i-1} \frac{d_{ij}(u+a_i)^j}{(u+a_i)^{l_i}} + \sum_{j=0}^{l_0} d_{0j} u^{l_0-j}.$$

Since $\sum_{i=0}^{r} 2l_i = n$, it follows for some i, $0 \leq i \leq r$, that $l_i \geq 1$. We now argue by equating coefficients in $\frac{f}{g^2}$ and $\frac{h_1(u)}{g(u)} + (\frac{h_1(u)}{g(u)})^2$. If $l_i = 1$, then $c_{i1} = d_{i0}$ and $c_{i0} = d_{i0}^2$. If $l_i \geq 2$, then $c_{i1} = 0$. Thus

$$c_{i1} = \begin{cases} 0 & \text{if } l_i \geq 2 \\ \sqrt{c_{i0}} & \text{if } l_i = 1. \end{cases}$$

This is a contradiction, and the result follows. ∎

2.3 The Half Determinant

For this subsection, assume n is odd. Knus, [4], states that the notion of the half-determinant was first introduced by Kneser, [3]. Given a quadratic form H in n variables defined over k of arbitrary characteristic, Knus, [4], defined the half determinant of H, $(\frac{1}{2} - \det)(H)$. A careful discussion of the half determinant and its properties can be found in [7]. Here we are interested only in the following two results.

Proposition 2.9 *Let $u, v \in k_r$. Then, $(\frac{1}{2} - \det)(uF + vG) = 0$ if and only if $uF + vG$ is degenerate over k_r.*

Proposition 2.10 *Let u, v be indeterminates over k. Then, $(\frac{1}{2} - \det)(uF + vG)$ splits into distinct linear factors over k^{alg}.*

It is interesting to note that if $\operatorname{char} k \neq 2$, then

$$\left(\frac{1}{2} - \det\right)(uF + vG) = \frac{1}{2}\left(\det(uF + vG)\right).$$

3 Places of Degree One

In this section, assume that n is even. We relate the number of solutions, N_p, in $k^{(2)}$ of

$$\begin{cases} y^2 + y = \operatorname{Arf}(uF + G) & \operatorname{char} k = 2 \\ y^2 = \det(uF + G) & \operatorname{char} k \neq 2 \end{cases}$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

to the number of places of degree one in the hyperelliptic function field $k(u, y)$ defined by

$$\begin{cases} y^2 + y = \mathrm{Arf}(uF + G) & \text{char } k = 2 \\ y^2 = \det(uF + G) & \text{char } k \neq 2. \end{cases}$$

Lemma 2.2, when $\text{char } k \neq 2$, and Proposition 2.8, when $\text{char } k = 2$, give that $k(u, y)$ has degree two over $k(u)$.

For $\alpha \in k$, let P_α denote the place of $k(u)$ at α with corresponding valuation v_α. Let v'_α denote a normalized valuation of $k(u, y)$ that lies above v_α, and let e_α be the ramification index of v'_α over v_α. Note that e_α does not depend on the choice of v'_α since $k(u, y)/k(u)$ is a Galois extension. Let $|\mathcal{P}_\alpha|$ denote the number of places of degree one in $k(u, y)$ lying over P_α. Similarly, define v_∞, v'_∞, e_∞, and $|\mathcal{P}_\infty|$ with respect to the infinite place P_∞. Let $N_\mathcal{P}$ denote the total number of places of degree one in $k(u, y)$.

When $\text{char } k = 2$, let N_g denote the number of elements $\alpha \in k$ such that $g(\alpha) = \det(\alpha F + G) = 0$. For later use, note that

$$\begin{aligned} N_g &= \big|\{u \in k \mid \det(uF + G) = 0\}\big| \\ &= \big|\{u \in k \mid uF + G \text{ is Type 3}\}\big|. \end{aligned}$$

We define a quantity N_F that depends on the Type of F over k by

$$N_F = \begin{cases} 1 + \chi(-1)^{\frac{n}{2}} & \text{if } F \text{ is Type 1} \\ 1 - \chi(-1)^{\frac{n}{2}} & \text{if } F \text{ is Type 2} \\ 1 & \text{if } F \text{ is Type 3.} \end{cases} \tag{3}$$

If $\text{char } k = 2$, then $\chi(-1)^{\frac{n}{2}} = 1$ and

$$N_F = \begin{cases} 2 & \text{if } F \text{ is Type 1} \\ 0 & \text{if } F \text{ is Type 2} \\ 1 & \text{if } F \text{ is Type 3.} \end{cases}$$

If $\text{char } k \neq 2$, then $N_F = \chi\big(\det(F)\big) + 1$.

3.1 Characteristic Two

For this subsection, assume that $\text{char } k = 2$.

Lemma 3.1

$$N_p = \sum_{\substack{\alpha \in k \\ v_\alpha(\mathrm{Arf}(uF+G)) \geq 0}} |\mathcal{P}_\alpha|.$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Proof By Proposition 2.7, given $\alpha \in k$, $v_\alpha\big(\mathrm{Arf}(uF+G)\big) \geq 0$ if and only if $g(\alpha) \neq 0$. Choose such an α. The equation $y^2 + y = \mathrm{Arf}(uF+G) = \frac{f(u)}{g(u)^2}$ gives that y is integral over the place P_α. If $\bar{y}$ is the image of y in the residue field, then $\bar{y}^2 + \bar{y} = \frac{f(\alpha)}{g(\alpha)^2}$.

If $\frac{f(\alpha)}{g(\alpha)^2} \in \wp(k)$, then $y^2 + y = \frac{f(\alpha)}{g(\alpha)^2}$ factors into two distinct linear factors. Otherwise, $y^2 + y = \frac{f(\alpha)}{g(\alpha)^2}$ is irreducible.

Using Kummer's theorem (Theorem III.3.7 [10]), we see that if $\frac{f(\alpha)}{g(\alpha)^2} \in \wp(k)$, then $|\mathcal{P}_\alpha| = 2$, and $|\mathcal{P}_\alpha| = 0$ otherwise. Thus $|\mathcal{P}_\alpha|$ is equal to the number of points on $y^2 + y = \frac{f(u)}{g(u)^2}$ with $u = \alpha$. The result follows by summing over all $\alpha \in k$ with $g(\alpha) \neq 0$. ∎

Lemma 3.2

$$N_g = \sum_{\substack{\alpha \in k \\ v_\alpha(\mathrm{Arf}(uF+G))<0}} |\mathcal{P}_\alpha|.$$

Proof Since $g(\alpha) = 0$ if and only if $v_\alpha\big(\mathrm{Arf}(uF+G)\big) < 0$, it is sufficient to show that if $v_\alpha\big(\mathrm{Arf}(uF+G)\big) < 0$, then $|\mathcal{P}_\alpha| = 1$. We consider the cases $v_\alpha\big(\mathrm{Arf}(uF+G)\big)$ odd and even separately.

First, suppose $\alpha \in k$ with $v_\alpha\big(\mathrm{Arf}(uF+G)\big) < 0$ and odd. We have that

$$v'_\alpha(y^2+y) = e_\alpha\left(v_\alpha\left(\frac{f(u)}{g(u)^2}\right)\right) < 0.$$

So, $v'_\alpha(y^2+y) = 2v'_\alpha(y)$. Since $v_\alpha(\frac{f(u)}{g(u)^2})$ is odd, it follows that $e_\alpha = 2$. Thus, there is exactly one (ramified) place of degree one over P_α. That is, $|\mathcal{P}_\alpha| = 1$.

Now, suppose $\alpha \in k$ with $v_\alpha\big(\mathrm{Arf}(uF+G)\big) < 0$ and even. Since $g(\alpha) = 0$, by Proposition 2.7, we can write

$$\mathrm{Arf}(uF+G) = \frac{f(u)}{g(u)^2} = \frac{c_0 + c_1(u-\alpha)}{(u-\alpha)^{2l}} + \frac{(u-\alpha)^2 f_\alpha(u)}{g(u)^2},$$

for some $f_\alpha(u) \in k[u]$ where $l \geq 1$, $(u-\alpha)^l$ is the largest power of $(u-\alpha)$ that divides $g(u)$, and $c_1 \neq \begin{cases} 0 & l \geq 2 \\ \sqrt{c_0} & l = 1 \end{cases}$. Define $z(u) = \frac{\sqrt{c_0}}{(u-\alpha)^l}$.

If $l = 1$, then

$$v_\alpha\big(\mathrm{Arf}(uF+G) + z(u) + z(u)^2\big) = v_\alpha\left(\frac{c_1 + \sqrt{c_0}}{(u-\alpha)} + \frac{(u-\alpha)^2 f_\alpha(u)}{g(u)^2}\right) = -1 = 1 - 2l.$$

If $l \geq 2$, then

$$v_\alpha\big(\mathrm{Arf}(uF+G) + z(u) + z(u)^2\big) = v_\alpha\left(\frac{c_1}{(u-\alpha)^{2l-1}} + \frac{\sqrt{c_0}}{(u-\alpha)^l} + \frac{(u-\alpha)^2 f_\alpha(u)}{g(u)^2}\right).$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Since,

$$v_\alpha\left(\frac{c_1}{(u-\alpha)^{2l-1}}\right) = 1-2l,$$
$$v_\alpha\left(\frac{\sqrt{c_0}}{(u-\alpha)^{l}}\right) = -l > 1-2l,$$

and

$$v_\alpha\left(\frac{(u-\alpha)^2 f_\alpha(u)}{g(u)^2}\right) \geq 2-2l > 1-2l,$$

it follows that

$$v_\alpha\left(\frac{c_1}{(u-\alpha)^{2l-1}} + \frac{\sqrt{c_0}}{(u-\alpha)^{l}} + \frac{(u-\alpha)^2 f_\alpha(u)}{g(u)^2}\right) = 1-2l.$$

Thus, $v_\alpha(\mathrm{Arf}(uF+G)+z^2+z) = 1-2l$ is a negative odd integer. A theorem on Artin-Schreier extensions (Theorem III.7.8 in [10]) implies that all places over P_α must be ramified, and we have that $|\mathcal{P}_\alpha| = 1$. ∎

Lemma 3.3 $N_F = |\mathcal{P}_\infty|$.

Proof We have three cases depending on the Type of F over k.

Suppose F is Type 3. Then, F is degenerate, and by Proposition 2.7 we can write

$$\mathrm{Arf}(uF+G) = \frac{f(u)}{g(u)^2} = \frac{f_0(u)}{g(u)^2} + \sum_{j=0}^{2l} c_j u^{2l-j},$$

where $\deg(f_0) < \deg(g^2) < n$, $2l = n - \deg(g^2) > 0$, and $c_1 \neq \begin{cases} 0 & l \geq 2 \\ \sqrt{c_0} & l = 1 \end{cases}$.

Define $z(u) = \sqrt{c_0}u^l$.

If $l = 1$, then

$$v_\infty\big(\mathrm{Arf}(uF+G)+z(u)+z(u)^2\big) = v_\infty\left((c_1+\sqrt{c_0})u + c_2 + \frac{f_0(u)}{g(u)^2}\right) = -1 = 1-2l.$$

If $l \geq 2$, then

$$\mathrm{Arf}(uF+G)+z(u)+z(u)^2 = (c_1u^{2l-1}+\cdots+c_{2l-1}u^1+c_{2l}) + \sqrt{c_0}u^l + \frac{f_0(u)}{g(u)^2},$$

and

$$v_\infty\big(\mathrm{Arf}(uF+G)+z(u)+z(u)^2\big) = 1-2l.$$

Thus, $v_\infty\big(\mathrm{Arf}(uF+G)+z^2+z\big) = 1-2l$ is a negative odd integer. A theorem on Artin-Schreier extensions (Theorem III.7.8 in [10]) implies that all places over P_∞ must be ramified, and we have that $|\mathcal{P}_\infty| = 1$.

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Now, suppose F is either Type 1 or Type 2. Then, F has order n by Lemma 2.1 and is nondegenerate, and we can write

$$\operatorname{Arf}(uF+G) = \frac{f(u)}{g(u)^2} = \frac{f_0(u)}{g(u)^2} + c_0,$$

where $\deg(f_0) < \deg(g^2) = n$ and $c_0 = \operatorname{Arf}(F)$.

Thus, $v_\infty\big(\operatorname{Arf}(uF+G)\big) \geq 0$, and y is integral over P_∞. If $\bar{y}$ is the image of y in the residue field, then $\bar{y}^2 + \bar{y} = c_0$. By comments from Subsection 2.2, we have that $\bar{y}^2 + \bar{y} = c_0$ splits into distinct linear factors if F is Type 1 and is irreducible if F is Type 2. By Kummer's theorem (Theorem III.3.7 in [10]), we see

$$|\mathcal{P}_\infty| = \begin{cases} 2 & \text{if } F \text{ is type 1} \\ 0 & \text{if } F \text{ is type 2.} \end{cases}$$

■

Theorem 3.4

$$N_{\mathcal{P}} = N_p + N_g + N_F.$$

Proof Since every place of degree one in $k(u,y)$ lies over a place of degree one in $k(u)$, we have

$$N_{\mathcal{P}} = |\mathcal{P}_\infty| + \sum_{\alpha\in k} |\mathcal{P}_\alpha|.$$

Separating the second summation and substituting from Lemmas 3.1, 3.2, and 3.3 gives

$$\begin{aligned} N_{\mathcal{P}} &= |\mathcal{P}_\infty| + \sum_{\substack{\alpha\in k \\ v_\alpha(\operatorname{Arf}(uF+G))<0}} |\mathcal{P}_\alpha| + \sum_{\substack{\alpha\in k \\ v_\alpha(\operatorname{Arf}(uF+G))\geq 0}} |\mathcal{P}_\alpha| \\ &= N_F + N_g + N_p. \end{aligned}$$

■

3.2 Odd Characteristic

If we assume $\operatorname{char} k \neq 2$, then the relationship

$$N_{\mathcal{P}} = N_p + N_F \tag{4}$$

is known. It is used implicitly by Weil, [11], and can be proved using methods similar to those in Subsection 3.1. In particular,

$$N_F = |\mathcal{P}_\infty|, \text{ and } N_p = \sum_{\alpha\in k} |\mathcal{P}_\alpha|.$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

4 Zeta Functions

In this section, we recount the arguments given by Weil in [11] to calculate the zeta function of a nonsingular pair of quadratic forms defined over k when $\operatorname{char} k \neq 2$, and we give the corresponding arguments to find the zeta function of a nonsingular pair of quadratic forms when $\operatorname{char} k = 2$.

4.1 Preliminaries

The zeta function, $Z(u)$, of the pair $\{F, G\}$ is defined by

$$Z(u) = \exp\Big(\sum_{r=1}^{\infty} \frac{N_r u^r}{r}\Big).$$

It is easy to show that if

$$N_r = \sum_i \gamma_i^r - \sum_j \beta_j^r \quad \gamma_i, \beta_j \in \mathbb{C},$$

then

$$Z(u) = \frac{\prod_j (1 - \beta_j u)}{\prod_i (1 - \gamma_i u)}. \tag{5}$$

The converse is also true and the proof of both implications can be found as Proposition 11.1.1 in [2].

4.2 Number of Variables Odd

When n is odd, Weil's calculation of the zeta function of $\{F, G\}$ when $\operatorname{char} k \neq 2$ can be generalized to include k of arbitrary characteristic. Weil defines $\phi(u, v) = \det(uF + vG)$. We define

$$\phi(u, v) = \Big(\frac{1}{2} - \det\Big)(uF + vG).$$

Recall that if $\operatorname{char} k \neq 2$, then $(\frac{1}{2} - \det)(uF + vG) = \frac{1}{2}\big(\det(uF + vG)\big)$. Thus, in this case, we have changed ϕ only by a nonzero constant factor.

In this Subsection (4.2), assume n is odd. Suppose $u, v \in k_r$, not both zero. Then $uF + vG$ has order $n - 1$ over k_r if and only if $\phi(u, v) = 0$. Thus, Equation 1 gives

$$N_r = \sum_{h=0}^{n-3} (q^r)^h + \frac{(q^r)^{\frac{n-3}{2}}}{q^r - 1} \sum_{\substack{(u,v) \neq (0,0) \in k_r^{(2)} \\ \phi(u,v)=0}} s_r(uF + vG).$$

Factoring over k, we have $\phi(u, v) = \prod_{\lambda=1}^{l} p_\lambda(u, v)$, for distinct, irreducible factors $p_\lambda \in k[u, v]$. Define $d_\lambda = \deg p_\lambda$.

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

In k_{d_λ}, by Proposition 2.10, $p_\lambda(u,v)$ splits into distinct linear factors, each of the form $(a_i u - b_i v)$, for $1 \leq i \leq d_\lambda$. Each form $b_iF + a_iG$ has order $n-1$ over k_{d_λ}. Further, since the extension is Galois, $b_iF + a_iG$ is equivalent to $b_jF + a_jG$ for all $1 \leq i, j \leq d_\lambda$. Either all of the forms are Type 1 or all of the forms are Type 2. We define $s_\lambda = s_{d_\lambda}(b_iF + a_iG)$. Let $s_\lambda^{\frac{1}{d_\lambda}}$ denote an arbitrary d_λ root of s_λ.

With this notation,

$$N_r = \sum_{h=0}^{n-3} (q^r)^h + (q^r)^{\frac{n-3}{2}} \sum_{\lambda, d_\lambda | r} d_\lambda s_\lambda^{\frac{r}{d_\lambda}}.$$

Defining ν_λ to be a primitive d_λ root of unity gives

$$N_r = \sum_{h=0}^{n-3} (q^r)^h + (q^r)^{\frac{n-3}{2}} \sum_{\lambda=1}^{l} \sum_{i=0}^{d_\lambda - 1} (\nu_\lambda^i s_\lambda^{\frac{1}{d_\lambda}})^r.$$

Using the special form of the zeta function given in Equation 5,

$$Z(u) = \prod_{h=0}^{n-3} (1 - q^h u)^{-1} \prod_{\lambda=1}^{l} \prod_{i=0}^{d_\lambda - 1} (1 - q^{\frac{n-3}{2}} \nu_\lambda^i s_\lambda^{\frac{1}{d_\lambda}} u)^{-1}.$$

Finally, simplifying gives the following result.

Theorem 4.1 *Let $\{F, G\}$ be a nonsingular pair of quadratic forms defined over the finite field F_q in n variables where n is odd. Then, the zeta function, $Z(u)$, of the pair is*

$$Z(u) = \prod_{h=0}^{n-3} (1 - q^h u)^{-1} \prod_{\lambda=1}^{l} (1 - q^{\frac{n-3}{2} d_\lambda} s_\lambda u^{d_\lambda})^{-1}.$$

4.3 Number of Variables Even

In this section, we consider what turns out to be the more interesting case, n even. If $\operatorname{char} k \neq 2$, we follow Weil's work, [11], and consider $k(u,y)$ defined by $y^2 = \det(uF + G)$. If $\operatorname{char} k = 2$, we consider $k(u,y)$ defined by $y^2 + y = \operatorname{Arf}(uF + G)$.

In this Subsection (4.3), assume n is even and keep the notation from Section 3.

Lemma 4.2

$$\sum_{(u,v) \neq (0,0) \in k^{(2)}} s(uF + vG) = \chi(-1)^{\frac{n}{2}} (q-1)[N_{\mathcal{P}} - (q+1)].$$

Proof We will prove the cases $\operatorname{char} k = 2$ and $\operatorname{char} k \neq 2$ separately.

First, suppose $\operatorname{char} k \neq 2$. Given $u, v \in k$ not both zero, let $n_{u,v}$ be the number of solutions in k of

$$y^2 = \det(uF + vG).$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Then for all choices of u, v,

$$n_{u,v} = \chi\big(\det(uF + vG)\big) + 1 = \chi(-1)^{\frac{n}{2}} s(uF + vG) + 1.$$

Thus,

$$\sum_{(u,v)\neq(0,0)\in k^{(2)}} s(uF + vG) = \chi(-1)^{\frac{n}{2}} \Big[\Big(\sum_{(u,v)\neq(0,0)\in k^{(2)}} n_{u,v} \Big) - (q^2 - 1) \Big]. \tag{6}$$

Summing over the choices for u, v, we have

$$\begin{aligned} \sum_{(u,v)\neq(0,0)\in k^2} n_{u,v} &= (q-1)\Big(\sum_{u\in k} n_{u,1} \Big) + (q-1) n_{1,0} \\ &= (q-1)[N_p + N_F]. \end{aligned}$$

Using Equation 4,

$$\sum_{(u,v)\neq(0,0)\in k^{(2)}} n_{u,v} = (q-1)[N_p + N_F] = (q-1) N_{\mathcal{P}}.$$

Substituting this into Equation 6 gives,

$$\begin{aligned} \sum_{(u,v)\neq(0,0)\in k^{(2)}} s(uF + vG) &= \chi(-1)^{\frac{n}{2}} [(q-1) N_{\mathcal{P}} - (q^2 - 1)] \\ &= \chi(-1)^{\frac{n}{2}} (q-1)[N_{\mathcal{P}} - (q+1)]. \end{aligned}$$

Now, suppose $\operatorname{char} k = 2$. Given $u, v \in k$, not both zero, let $n_{u,v}$ be the number of solutions in k of

$$y^2 + y = \operatorname{Arf}(uF + vG).$$

Then

$$n_{u,v} = \begin{cases} 2 & \text{if } uF + vG \text{ is Type 1} \\ 0 & \text{otherwise,} \end{cases}$$

or equivalently

$$n_{u,v} = \begin{cases} s(uF + vG) & \text{if } uF + vG \text{ is Type 3,} \\ s(uF + vG) + 1 & \text{otherwise.} \end{cases}$$

Thus,

$$\sum_{(u,v)\neq(0,0)\in k^2} s(uF + vG) = \Big(\sum_{(u,v)\neq(0,0)\in k^2} n_{u,v} \Big) - (q^2 - 1) + \sum_{\substack{u,v\in k \\ uF+vG \text{ is Type 3}}} (1). \tag{7}$$

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Summing over the choices for u, v, we have $\sum_{(u,v)\neq(0,0)\in k^2} n_{u,v}$ is the number of solutions in $k^{(3)}$ of $y^2 + y = \mathrm{Arf}(uF + vG)$. That is,

$$\sum_{(u,v)\neq(0,0)\in k^2} n_{u,v} = (q-1)[N_p + \text{ (number of solutions of } y^2 + y = \mathrm{Arf}(F))]$$

$$= (q-1)\left[N_p + \begin{cases} 2 & \text{if } F \text{ is Type 1} \\ 0 & \text{otherwise} \end{cases}\right].$$

Next we count the number of forms that are Type 3,

$$\sum_{\substack{u,v\in k \\ uF+vG \text{ is Type 3}}} (1) = (q-1)\left[N_g + \begin{cases} 1 & \text{if } F \text{ is Type 3} \\ 0 & \text{otherwise} \end{cases}\right].$$

Substituting into Equation 7 and using Theorem 3.4 gives,

$$\sum_{(u,v)\neq(0,0)\in k^2} s(uF + vG) = (q-1)[N_p + N_g + N_F] - (q^2 - 1)$$

$$= (q-1)[N_{\mathcal{P}} - (q+1)].$$

Since $\chi(-1)^{\frac{n}{2}} = 1$ when $\mathrm{char}\, k = 2$, the result follows immediately. ∎

By Corollary V.1.16 in [10] and the Hasse-Weil Theorem, there exist α_i, with $|\alpha_i| = \sqrt{q}$, such that

$$N_{\mathcal{P}} - (q+1) = -\sum_{i=1}^{2g} \alpha_i.$$

Here, g is the genus. Further, the number of places of degree one in the function field defined over k_r is equal to $q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$, (see V.1.16 in [10]).

Thus, by Lemma 4.2,

$$\sum_{(u,v)\neq(0,0)\in k_r^{(2)}} s_r(uF + vG) = \left(\chi(-1)^{\frac{n}{2}}\right)^r (q^r - 1)\left(-\sum_{i=1}^{2g} \alpha_i^r\right).$$

By Equation 2,

$$N_r = \sum_{h=0}^{n-3} (q^r)^h + \frac{(q^r)^{\frac{n-4}{2}}}{q^r - 1} \sum_{(u,v)\neq(0,0)\in k_r^{(2)}} s_r(uF + vG)$$

$$= \sum_{h=0}^{n-3} (q^r)^h - (q^r)^{\frac{n-4}{2}} \left(\chi(-1)^{\frac{n}{2}}\right)^r \left(\sum_{i=1}^{2g} \alpha_i^r\right).$$

Using the special form of the zeta function given in Equation 5 gives the following result.

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press

Theorem 4.3 *Let $\{F, G\}$ be a nonsingular pair of quadratic forms defined over the finite field F_q in n variables where n is even. Then, the zeta function, $Z(u)$, of the pair is*

$$Z(u) = \prod_{h=0}^{n-3}(1 - q^h u)^{-1} \prod_{i=1}^{2g}\left(1 - \chi(-1)^{\frac{n}{2}} q^{\frac{n-4}{2}} \alpha_i u\right).$$

References

[1] C. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristic* 2. J. Reine Angew. Math. **183**(1941), 148–167.
[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory 2nd Ed*. Graduate Texts in Math. **84**, Springer-Verlag, New York, 1990.
[3] M. Kneser, *Vorlesung über quadratische Formen*. Göttingen, Math. Institut, 1973–4.
[4] M. Knus, *Quadratic Forms, Clifford Algebras and Spinors*. Seminars in Mathematics, **1**, Campinas, Brazil, 1988.
[5] T. Lam, *The Algebraic Theory of Quadratic Forms*. Mathematics Lecture Note Series, W. A. Benjamin, Inc., Reading, MA, 1973.
[6] D. Leep and L. Schueller, *Zeros of a Pair of Quadratic Forms Defined Over a Finite Field*. Finite Fields Appl. (2) **5**(1999), 157–176.
[7] ———, *A Characterization of Nonsingular Pairs of Quadratic Forms*. submitted, 1998.
[8] R. Lidl and H. Niederreiter, *Finite Fields*. Encyclopedia of Math. and its Applications **20**, Cambridge Univ. Press, New York, 1984.
[9] W. Schmidt, *Equations over finite fields: an elementary approach*. Lecture Notes in Math. **536**, Springer-Verlag, New York, 1976.
[10] H. Stichtenoth, *Algebraic Function Fields and Codes*. Universitext, Springer-Verlag, Berlin, Heidelberg, 1993.
[11] A. Weil, *Footnote to a Recent Paper*. Amer. J. Math. **76**(1954), 347–350.
[12] E. Witt, *Über eine Invariante quadratischer Formen* mod 2. J. Reine Angew. Math. **193**(1954), 119–120.

Department of Mathematics
Whitman College
Walla Walla, Washington 99362
U.S.A.

https://doi.org/10.4153/CMB-2001-024-7 Published online by Cambridge University Press