Communications in **M**athematical **A**nalysis
Volume 18, Number 2, pp. 76–85 (2015) www.math-res-pub.org/cma
ISSN 1938-9787

On the Maximality of Certain Hyperellptic Curves with an Application to Character Sums

Peter McCalla*
Department of Mathematics
Morgan State University
Baltimore, MD 21251, USA

François Ramaroson†
Department of Mathematics
Howard University
Washington, DC 20059, USA

(Communicated by En-Bing Lin)

Abstract

In [4], Kodama, Top, Washio studied the maximality of a family of elliptic curves, mostly of genus 3, over a finite field. They used the Jacobians of the curves and differential forms to obtain their results. In this note, in order to prove the maximality of the curves under study, we use analytical tools, namely character and Jacobsthal sums, together with an important result which says that if a curve is the image of a maximal curve under a rational map, then it is itself maximal. Character sums are suitable for counting the number of points on a curve over a finite field, and their use makes the proofs natural and rather elementary. The norm and trace curves are utilized to construct rational maps to the hyperelliptic curves. As an application, the maximality of a certain hyperelliptic curve is used to find the explicit value of a character sum.

AMS Subject Classification: 11G25, 11L10, 14G25, 14G15

Keywords: hyperelliptic curves, character sums, Jacobsthal sums, maximal curves, norm curve, trace curve.

1 Introduction

An affine plane algebraic curve C, defined over a finite field $K = \mathbb{F}_m$, is called *hyperelliptic* if it has an equation of the form

$$C : y^2 = f(x)$$

*E-mail address: peter.mccalla@morgan.edu
†E-mail address: framaroson@howard.edu

where $f(x)$ is a polynomial with coefficients in K, of degree $d > 4$, and whose roots are distinct.

The genus of C is given by ([5])

$$g = \begin{cases} \frac{1}{2}(d-1), & \text{if } d \text{ is odd,} \\ \frac{1}{2}(d-2), & \text{if } d \text{ is even.} \end{cases} \tag{1.1}$$

Let $\mathcal{C}$ be the nonsingular projective model for C. Let $\mathcal{C}(K)$ be the set of K-rational points on $\mathcal{C}$. A fundamental result in the theory of algebraic curves over a finite field is the following inequality, known as the *Hasse-Weil bound*

$$|\mathcal{C}(K)| \leq m + 1 + 2g\sqrt{m}. \tag{1.2}$$

If the equality is attained, then $\mathcal{C}$ is said to be *K-maximal*. We will say that the affine curve C is K-maximal when $\mathcal{C}$ is K-maximal. It is clear that for this notion to make sense, m must be a square.

Maximal curves are of major importance, especially in the areas of Coding Theory and Cryptology. For the remainder of this paper, we will set

$$m = q^2 \text{ with } q = p^n,\ p > 3 \text{ is prime and } n \text{ is an } \textit{odd} \text{ positive integer.}$$

In [4], K-maximality for the following nine hyperelliptic curves has been proven with specific conditions on p:

$$\begin{aligned}
&C_1 : y^2 = x^8 + 1,\ p \equiv -1 (\mathrm{mod}\ 8),\\
&C_2 : y^2 = x^7 + 1,\ p \equiv -1 (\mathrm{mod}\ 7),\\
&C_3 : y^2 = x^8 + x,\ p \equiv -1 (\mathrm{mod}\ 7),\\
&C_4 : y^2 = x^7 + x,\ p \equiv -1 (\mathrm{mod}\ 4),\\
&C_5 : y^2 = (x^2-4)(x^2-2)(x^4-4x^2+1),\ p \equiv -1 (\mathrm{mod}\ 12),\\
&C_6 : y^2 = (x-2)(x^2-2)(x^4-4x^2+1),\ p \equiv 13, -1 (\mathrm{mod}\ 24),\\
&C_7 : y^2 = (x+2)(x^2-2)(x^4-4x^2+1),\ p \equiv 13, -1 (\mathrm{mod}\ 24),\\
&C_8 : y^2 = x^{12} + 1,\ p \equiv -1 (\mathrm{mod}\ 12),\\
&C_9 : y^2 = x^{13} + x,\ p \equiv 13, -1 (\mathrm{mod}\ 24),
\end{aligned}$$

where for $C_1 - C_7$, $g = 3$; and for C_8 and C_9, $g = 5$ and $g = 6$, respectively. The proofs of K-maximality in [4] involve differential forms on the curves together with deep studies of their Jacobians. The aim of this paper is to use another alternative for the proof of K-maximality. The tools that will be used are more analytical and rely on character sums and properties of rational maps that help determine K-maximal curves from known ones. It should be pointed out that more than K-maximality is actually proven in [4].

The paper is organized as follows. In Section 2 we introduce the analytical tools, namely the Jacobsthal sums associated with the quadratic character and we collect the results concerning these sums. In Section 3, we state the theorem which allows the determination of a maximal curve from a known one via a rational map. The norm curve and the trace curve are introduced and we prove their maximality. In Section 4, the proofs of maximality for the nine curves are given. Finally in Section 5, we give an application of maximality to the evaluation of a character sum.

2 Jacobsthal Sums

Character sums play a vital role in counting the number of K-rational points on an algebraic curve, and conversely, knowledge of the number of K-rational points can allow to solve the important problem of evaluating character sums over K.

Let K^* be the multiplicative group of non-zero elements in K. It is well known that this group is cyclic, so let ς be a generator for K^*. For each positive integer k, $1 \leq k \leq q^2 - 1$, we define

$$\rho : K^* \longrightarrow \mathbb{C}$$

by

$$\rho(\varsigma^k) = e^{i\pi k}.$$

The function ρ is well-defined and independent of the chosen generator ς. The following proposition is easily proved.

Proposition 2.1. *The mapping ρ is a* character*, called the quadratic character of K, and it satisfies the following:*

$$\text{For } \alpha \in K^*,\ \rho(\alpha) = \begin{cases} +1 & \text{if } \alpha \text{ is a square in } K^*, \\ -1 & \text{if } \alpha \text{ is not a square in } K^*. \end{cases}$$

It is practical to extend ρ to the whole of K by setting $\rho(0) = 0$.

Definition 2.2. Let ρ be the quadratic character of K. For $r \in \mathbb{N}$ and $\beta \in K^*$, the Jacobsthal sums are defined by

$$\phi_r(\beta) = \sum_{\alpha \in K} \rho(\alpha)\rho(\alpha^r + \beta),$$

$$\psi_r(\beta) = \sum_{\alpha \in K} \rho(\alpha^r + \beta).$$

Theorem 2.3. $\psi_{2r}(\beta) = \phi_r(\beta) + \psi_r(\beta)$.

Proof. We start with the right hand side

$$\begin{aligned} \phi_r(\beta) + \psi_r(\beta) &= \sum_{\alpha \in K} (\rho(\alpha) + 1)\rho(\alpha^r + \beta) \\ &= \rho(\beta) + 2 \sum_{\alpha \in K^+} \rho(\alpha^r + \beta), \end{aligned}$$

where $K^+ = \{\alpha^2 : \alpha \in K^*\}$. Next, for the left side

$$\begin{aligned} \psi_{2r}(\beta) &= \sum_{\alpha \in K} \rho(\alpha^{2r} + \beta) \\ &= \rho(\beta) + \sum_{\alpha \in K^*} \rho\left((\alpha^2)^r + \beta\right) \\ &= \rho(\beta) + 2 \sum_{\gamma \in K^+} \rho(\gamma^r + \beta) \end{aligned}$$

as $(-\alpha)^2 = \alpha^2$ for $\alpha \in K^*$. Therefore the two sides are equal. □

We end this section with a theorem involving the evaluation of the Jacobsthal sum ϕ_6 over the field $\mathbb{F}_{p^2}$ for whose proof we refer to [1].

Theorem 2.4. *If $p \equiv -1 (mod\ 4)$, then*

$$\phi_6(\beta) = \begin{cases} 6p & \text{if } \beta \text{ is a } 12\text{th power in } \mathbb{F}_{p^2}, \\ -6p & \text{if } \beta \text{ is a } 6\text{th power, but not a } 12\text{th power in } \mathbb{F}_{p^2}, \\ 0 & \text{otherwise.} \end{cases}$$

3 K-Maximality of Hyperelliptic Curves

Let $C : y^2 = f(x)$ be a hyperelliptic curve of genus g. If (α,β) is a K-rational point of C and $\beta \neq 0$, then it follows that $(\alpha, -\beta) \in C$. If $\beta = 0$, then $(\alpha, 0) \in C$. Finally, if $f(\alpha)$ is not a square in K, then there is no K-rational point with α as the first coordinate. To put this altogether, for each $\beta \in K$, the number of K-rational points of C is $\sum_{\alpha\in K}(1 + \rho(f(\alpha))) = q^2 + \sum_{\alpha\in K}\rho(f(\alpha))$.

With $\mathcal{C}$, the non-singular projective model of C, and setting $d = \deg(f)$, the following proposition holds ([5]).

Proposition 3.1. *The number of K-rational points on $\mathcal{C}$ is given by*

$$|\mathcal{C}(K)| = \begin{cases} q^2 + 1 + \sum_{\alpha\in K}\rho(f(\alpha)) & \text{if } d \text{ is odd}, \\ q^2 + 2 + \sum_{\alpha\in K}\rho(f(\alpha)) & \text{if } d \text{ is even}. \end{cases}$$

Combining Proposition 3.1 with (1.1) and (1.2), we obtain the following corollary:

Corollary 3.2. *C is K-maximal if and only if*

$$\sum_{\alpha\in K}\rho(f(\alpha)) = \begin{cases} q(d-1) & \text{if } d \text{ is odd}, \\ q(d-2) - 1 & \text{if } d \text{ is even}. \end{cases}$$

The next two theorems will help us obtain the K-maximality of curves either from the extension $K/\mathbb{F}_{p^2}$ or from rational maps.

Theorem 3.3. *If C is $\mathbb{F}_{p^2}$-maximal, then it is K-maximal.*

Proof. First, recall that $K = \mathbb{F}_{p^{2n}}$, where n is odd. From [3], if C is $\mathbb{F}_{p^2}$-maximal, then

$$|\mathcal{C}(K)| = p^{2n} + 1 + (-1)^{n-1}2gp^n.$$

Since n is odd, the result follows from (1.2). □

Theorem 3.4 (Serre)**.** *Let $f : C \longrightarrow D$ be a surjective morphism of irreducible nonsingular curves where f, C, and D are defined over K. If C is K-maximal, then D is K-maximal.*

Proof. See [3], where it is explained that the result follows from the fact that the L-polynomial of D divides that of C. □

In practice, we will find a surjective rational map on the irreducible plane affine model which, by Algebraic Geometry, extends to the nonsingular projective model ([2]).

We now introduce the norm and trace.

Definition 3.5. The *norm curve* is the hyperelliptic curve N whose equation is given by

$$N : y^2 = x^{q+1} + 1$$

and the *trace curve* is the hyperelliptic curve T whose equation is given by

$$T : y^2 = x^q + x.$$

These curves derived their names from the *field norm* and *field trace* on K.

Theorem 3.6. *The curves N and T are K-maximal.*

Proof. By Corollary 3.2, it is enough to show that, for N,

$$\sum_{\alpha \in K} \rho(\alpha^{q+1} + 1) = q^2 - q - 1$$

and for T,

$$\sum_{\alpha \in K} \rho(\alpha^q + \alpha) = q^2 - q$$

(**for** N) Since $N_{K/\mathbb{F}_q}(\alpha) = \alpha^{q+1}$, $\alpha^{q+1} + 1 \in \mathbb{F}_q$. It follows that $\rho(\alpha^{q+1} + 1)$ is either 0 or 1. Let ν_{q+1} be the set of $(q+1)$-st roots of -1 that lie in the algebraic closure of K. We claim that $\nu_{q+1} \subset K$. Indeed, if $\alpha \in \nu_{q+1}$, then $\alpha^{q^2-1} = (\alpha^{q+1})^{q-1} = 1$, hence $\alpha \in K$. Therefore,

$$\sum_{\alpha \in K} \rho(\alpha^{q+1} + 1) = \sum_{\alpha \in K \setminus \nu_{q+1}} \rho(\alpha^{q+1} + 1) = q^2 - (q+1)$$

(**for** T) Since $T_{K/\mathbb{F}_q}(\alpha) = \alpha^q + \alpha \in \mathbb{F}_q$, $\rho(\alpha^q + \alpha)$ is either 0 or 1. Let ν_{q-1} is the set of $(q-1)$-st roots of -1. Then, similarly for ν_{q+1}, $\nu_{q-1} \subset K$ and

$$\sum_{\alpha \in K} \rho(\alpha^q + \alpha) = \sum_{\alpha \in K \setminus \nu_{q-1} \cup \{0\}} \rho(\alpha^q + \alpha) = q^2 - q$$

and we are done. □

4 The Maximality of the Nine Curves

Theorem 4.1. *The curves C_1, C_2, and C_8 are K-maximal under the imposed conditions on p.*

Proof. For C_1, since $p \equiv -1 (\mathrm{mod}\ 8)$, $q \equiv -1 (\mathrm{mod}\ 8)$. Similarly, in the cases for C_2 and C_8, $q \equiv -1 (\mathrm{mod}\ 7)$ and $q \equiv -1 (\mathrm{mod}\ 12)$, respectively. Let ℓ be an integer such that $q+1 = 8\ell$ (for C_1), $q+1 = 7\ell$ (for C_2), and $q+1 = 12\ell$ (for C_8). In all cases, consider the map $f : N \longrightarrow C_i$ $(i = 1, 2, 8)$ defined by

$$f(x, y) = (x^\ell, y).$$

The map f is surjective and the conclusion follows from Theorems 3.4 and 3.6. □

Theorem 4.2. *The curve C_3 is K-maximal under the imposed conditions on p.*

Proof. Note that the conditions for C_2 and C_3 are identical. Consider the maps $g : C_2 \longrightarrow C_3$ and $h : C_3 \longrightarrow C_2$ defined by

$$g(x,y) = \left(\frac{1}{x}, \frac{y}{x^4}\right) \qquad h(x,y) = \left(\frac{1}{x}, \frac{y}{x^4}\right).$$

The maps g and h are rational and inverses of each other. It follows that C_2 and C_3 are birationally equivalent and we are done. □

Theorem 4.3. *The curve C_4 is K-maximal under the imposed conditions on p.*

Proof. First, we consider the Jacobsthal sum ϕ_6 on $\mathbb{F}_{p^2}$. Since $p \equiv -1 (\mathrm{mod}\, 4)$, $\phi_6(1) = 6p$ by Theorem 2.4, which makes C_4 $\mathbb{F}_{p^2}$-maximal by Corollary 3.2. Therefore, it is K-maximal by Theorem 3.3. □

Theorem 4.4. *The curve C_9 is K-maximal under the imposed conditions on p.*

Proof. (**Case 1:** $p \equiv 13 (\mathrm{mod}\, 24)$) We have $q \equiv 13 (\mathrm{mod}\, 24)$. Let ℓ be such that $q = 24\ell + 13$. Then by using the map $f : T \longrightarrow C_9$ defined by

$$f(x,y) = (x^{2\ell+1}, x^{\ell} y)$$

along with Theorem 3.4, the conclusion follows.

(**Case 2:** $p \equiv -1 (\mathrm{mod}\, 24)$) By Corollary 3.2, it is enough to show that $\phi_{12}(1) = 12q$. Since $q \equiv -1 (\mathrm{mod}\, 24)$, the curve $y^2 = x^{24} + 1$ is K-maximal (using the same reasoning as in the proof of Theorem 4.1) and $\psi_{24}(1) = 22q - 1$. Since C_8 is K-maximal, $\psi_{12}(1) = 10q - 1$. Therefore, by Theorem 2.3, $\phi_{12}(1) = 12q$. □

Theorem 4.5. *The curve C_5 is K-maximal under the imposed conditions on p.*

Proof. Note that the conditions for C_5 and C_8 are the same. Consider the map $f : C_8 \longrightarrow C_5$ defined by

$$f(x,y) = \left(x + \frac{1}{x}, \frac{y(x^2-1)}{x^4}\right)$$

Then a simple algebraic calculation shows that $f(x,y)$ lies in C_5. By Theorem 4.1, C_8 is K-maximal. Therefore, by Theorem 3.4, C_5 is K-maximal. □

Theorem 4.6. *The curve C_6 is K-maximal under the imposed conditions on p.*

Proof. (**Case 1:** $p \equiv 13 (\mathrm{mod}\, 24)$) We have $q \equiv 13 (\mathrm{mod}\, 24)$. Let k be defined by $q = 24k + 13$ and consider the map $f : T \longrightarrow C_6$ defined by

$$f(x,y) = \left(x^{2k+1} + \frac{1}{x^{2k+1}}, \frac{y(x^{2k+1}-1)}{x^{7k+4}}\right)$$

The result now follows from Theorems 3.4 and 3.6.

(**Case 2:** $p \equiv -1 (\mathrm{mod}\, 24)$) Let k be defined by $q + 1 = 24k$ and consider the map $g : N \longrightarrow C_6$ defined by

$$g(x,y) = \left(x^k + \frac{1}{x^k}, \frac{y(x^{2k}-1)}{x^{7k}}\right)$$

The result now follows from Theorems 3.4 and 3.6. □

Theorem 4.7. *The curve C_7 is K-maximal under the imposed conditions on p.*

Proof. Similar to the proof of Theorem 4.6 using the map $f : T \longrightarrow C_7$ defined by

$$f(x,y) = \left(x^{2k+1} + \frac{1}{x^{2k+1}}, \frac{y(x^{2k+1}+1)}{x^{7k+4}}\right)$$

for $p \equiv 13 (\mathrm{mod}\ 24)$ and $g : N \longrightarrow C_7$ defined by

$$g(x,y) = \left(x^{k} + \frac{1}{x^{k}}, \frac{y(x^{2k}+1)}{x^{7k}}\right)$$

for $p \equiv -1 (\mathrm{mod}\ 24)$. □

5 An Application to the Evaluation of a Character Sum

In this section we evaluate a certain character sum using the maximality of the curve C_5.

We begin with an easy classical transformation formula involving the quadratic character of K.

Theorem 5.1. *Let ρ be the quadratic character of K and $F : K \longrightarrow \mathbb{C}$ any complex-valued function. Then the following holds:*

$$\sum_{\alpha \in K} F(\alpha) + \sum_{\alpha \in K} \rho(\alpha) F(\alpha) = \sum_{\alpha \in K} F(\alpha^2).$$

This transformation formula involving the quadratic character can be generalized as follows:

Theorem 5.2. *Let ρ be the quadratic character of K and $g : K \longrightarrow \mathbb{C}$ any complex valued function. Let a, b, c, A, B, C be elements of K, then*

$$\sum_{\alpha \in K}{}' \rho\left(g\left(\frac{a\alpha^2 + b\alpha + c}{A\alpha^2 + B\alpha + C}\right)\right) = \sum_{\alpha \in K} \rho(g(\alpha)) + \sum_{\alpha \in K} \rho(\theta^*(\alpha))\rho(g(\alpha)) - \begin{cases} \rho(a/A), & \text{if } A \neq 0 \\ 0, & \text{if } A = 0 \end{cases}$$

where

$$\theta^*(x) = Dx^2 + \Delta x + d$$

with

$$D = B^2 - 4AC$$
$$d = b^2 - 4ac$$
$$\Delta = 4aC - 2bB + 4cA$$

and in $\sum'_{\alpha \in K}$, the summation is defined over $\alpha \in K$ in which the summand is defined.

A proof in the case of $\mathbb{F}_p$ can be found in [8] and the general case over K is an easy extension.

Theorem 5.3. *Let* $p \equiv -1 (mod\ 12)$, $f(x) = x^5 - 10x^4 + 33x^3 - 38x^2 + 8x$, *and*

$$S = \sum_{\alpha \in K} \rho(f(\alpha))$$

where ρ *is the quadratic character on* K. *Then* $S = 4q$.

To prove this, we need the following lemma:

Lemma 5.4. $\sum_{\alpha \in K} \rho(3\alpha^3 - 3\alpha^2 + \alpha) = 2q.$

Proof. Consider the elliptic curves

$$E_1 : y^2 = 3x^3 - 3x^2 + x \qquad E_2 : v^2 = u^3 + 1$$

The transformations

$$E_1 \longrightarrow E_2 \text{ by } (x,y) \mapsto (3x - 1, 3y)$$

$$E_2 \longrightarrow E_1 \text{ by } (x,y) \mapsto \left(\frac{u+1}{3}, \frac{v}{3}\right)$$

realize isomorphisms of these curves over K for $p \equiv -1 (\text{mod } 12)$, hence

$$\sum_{\alpha \in K} \rho(3\alpha^3 - 3\alpha^2 + \alpha) = \sum_{\alpha \in K} \rho(\alpha^3 + 1).$$

Next we observe that the curve E_2 is supersingular at p since $p \equiv -1 (\text{mod } 3)$ and it is well-known that

$$|E_2(\mathbb{F}_p)| = p + 1$$

It then follows from the theory of elliptic curves (nonsingular curves of genus 1) over a finite field ([6]) that

$$|E_2(\mathbb{F}_{p^2})| = p^2 + 1 + 2p = (p+1)^2$$

hence E_2 is $\mathbb{F}_{p^2}$-maximal. Since $q^2 = p^{2n}$ with n odd, E_2 is K-maximal by Theorem 3.3 and we have

$$|E_2(K)| = q^2 + 1 + 2q$$

It follows that

$$\sum_{\alpha \in K} \rho(\alpha^3 + 1) = |E_2(K)| - (q^2 + 1) = 2q$$

and we are done. □

Proof of Theorem 5.3. Consider the curve

$$C_5 : y^2 = (x^2 - 4)(x^2 - 2)(x^4 - 4x^2 + 1) = (x^4 - 6x^2 + 8)(x^4 - 4x^2 + 1)$$

By Theorem 3.5, C_5 is K-maximal and by Corollary 3.2

$$\sum_{\alpha \in K} \rho((\alpha^4 - 6\alpha^2 + 8)(\alpha^4 - 4\alpha^2 + 1)) = 6q - 1$$

Setting $f(x) = (x^2-6x+8)(x^2-4x+1)$, by Theorem 5.1 with $F(x) = \rho(f(x))$, the following holds:

$$\sum_{\alpha\in K}\rho((\alpha-2)(\alpha-4)(\alpha^2-4\alpha+1))+S = \sum_{\alpha\in K}\rho((\alpha^2-2)(\alpha^2-4)(\alpha^4-4\alpha^2+1)) = 6q-1. \quad (5.1)$$

We now evaluate the sum

$$\sum_{\alpha\in K}\rho((\alpha-2)(\alpha-4)(\alpha^2-4\alpha+1)) = \sum_{\alpha\in K}\rho((\alpha^2-6\alpha+8)(\alpha^2-4\alpha+1)).$$

Using Theorem 5.2 with

$$\begin{aligned} g(x) &= x \\ (a,b,c) &= (1,-6,8) \\ (A,B,C) &= (1,-4,1) \\ (D,\Delta,d) &= (12,-12,4) \\ \theta^*(x) &= 4(3x^2-3x+1) \end{aligned}$$

and using the fact that $\sum_{\alpha\in K}\rho(\alpha) = 0$, we obtain

$$\sum_{\alpha\in K}\rho((\alpha^2-6\alpha+8)(\alpha^2-4\alpha+1)) = \sum_{\alpha\in K}\rho(3\alpha^3-3\alpha^2+\alpha)-1.$$

By Lemma 5.4, the resulting character sum is 2q. Solving for S in (5.1), we get

$$S = 6q-1-(2q-1) = 4q$$

and we are done. □

Corollary 5.5. *Under the same conditions as in Theorem 5.4, the curve of genus 2,*

$$C_{10}: y^2 = x^5-10x^4+33x^3-38x^2+x = x(x-2)(x-4)(x^2-4x+1)$$

is K-maximal.

Proof. Follows from Corollary 3.2. □

References

[1] B. Berndt, R. Evans, and K. Williams, Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer. *Illinois Journal of Mathematics* **23** no. 3 (1979), pp. 374-437.

[2] W. Fulton, Algebraic Curves. Online, 2008.

[3] J.W.P. Hirschfeld, G. Korchmaros, and F Torres, Algebraic Curves over a Finite Field. Princeton Univ. Press, New Jersey, 2008.

[4] T. Kodama, J. Top, and T. Washio, Maximal Hyperelliptic Curves of Genus Three. *Finite Fields and Their Applications* **15** (2009), pp. 392-403.

[5] G. Orzech and M. Orzech, Plane Algebraic Curves. Marcel Dekker Inc, New York, NY, 1991.

[6] J. Silverman, The Arithmetic of Elliptic Curves, 2nd ed.. Springer, New York, NY, 1986.

[7] H. Stichtenoth, Algebraic Function Fields and Codes. Springer, Berlin, 2009.

[8] K. Williams, Finite Transformation Formulae Involving the Legendre Symbol. *Pacific J. Math.* **34** (1970), pp. 559-568.