VFAST Transactions on Mathematics
http://vfast.org/journals/index.php/VTM@ 2024 ISSN(e): 2309-0022, ISSN(p): 2411-6343
Volume 12, Number 1, January-June, 2024 *pp: 92-104*

Quadratic twist of an elliptic curve in a generalized Weierstrass equation over a function field

Fida Hussain Shaikh[1*], **Muhammad Afzal Soomro**[1], **Iqrar Ali Pali**[2*], **Safia Amir Dahri**[1], **Abdul Rahman Soomro**[3]

[1]Department of Mathematics, Dawood university of engineering and technology, Karachi,Sindh, Pakistan.; [2]Department of Telecommunication Engineering, Quaid-e-Awam University of Engineering, Science, and Technology Nawabshah, Pakistan.; [3]Department of Mathematics, Institute of Business Administration, Sukkur, Pakistan.

Keywords: *Elliptic Curve, Twist of Elliptic Curve, Finite Field and Function Field.* ***Subject Classification***: *Galois theory, Commutative Algebra and Algebraic Geometry.*

Journal Info:
Submitted:
Feb 10, 2024
Accepted:
March 15, 2024
Published:
March 25, 2024

Abstract This paper mainly focuses on the construction of a quadratic twist for an elliptic curve represented in a generalized Weierstrass equation over the field $\tilde{\mathbf{F}}_q(t)$. The specific form of the quadratic twist, presented in the generalized Weierstrass equation, is determined by linear algebra approach and discussed in detail.

***Correspondence Author Email Address:**
iqraralipali@quest.edu.pk
DOI: 10.21015/vtm.v12i1.1739

1 Introduction and Preliminaries

In this research article, we embark on a comprehensive exploration of the fundamental concept of elliptic curves, a central topic in mathematics with far-reaching applications across various disciplines. Elliptic curves are algebraic geometric objects defined by cubic equations, possessing unique mathematical properties that render them invaluable in cryptography, number theory, and computer science. As we delve into the intricacies of elliptic curves, we aim to provide the reader with a solid foundation by elucidating their key characteristics, mathematical formulations, and geometric representations.

Furthermore, we extend our discussion to encompass practical examples that illuminate the diverse applications of elliptic curves in real-world scenarios. These examples serve to bridge the theoretical underpinnings of elliptic curves with their tangible implications, showcasing their significance in areas such as secure communication protocols, digital signatures, and error-detecting codes.

Additionally, an exploration into the twist of elliptic curves is undertaken. The concept of a twist in elliptic curve theory is a crucial aspect that enhances our understanding of these mathematical structures. Twists arise from the study of isogenies, which are morphisms between elliptic curves preserving their group structures. By delving into the twist of elliptic curves, we uncover deeper insights into the underlying mathematical principles and connections that contribute to their versatility and utility in diverse applications.

For those seeking a more in-depth understanding of the material presented herein, we recommend referring to the following key sources: [2], [8], [9], and [16]. These references provide additional insights, theoretical frameworks, and empirical evidence that complement and extend the knowledge presented in this article. Moreover, there are many applications of elliptic curves and twists of elliptic curves are in cryptography, coding theory, etc and Boolean functions also play an important role in such applications. some are mentioned in [11], [19], and [5]

Definition 1. *An algebraic curve is called an elliptic curve if it is a smooth, projective curve of genus one, on which there is a rational point at ∞. Elliptic curves hold a distinctive status in algebraic geometry as they belong to the class of abelian varieties, a concept extensively discussed in foundational works such as [7], [21], and [15]. The abelian variety structure of elliptic curves is pivotal in understanding their algebraic and geometric properties, providing a framework for their study and application in various mathematical disciplines. Readers interested in an introduction to the foundational aspects of elliptic curves and abelian varieties may refer to [10] for an in-depth exploration of these mathematical constructs. The explicit Weierstrass equation of elliptic curve $\tilde{\mathbf{E}}/\tilde{\mathbf{K}}$ for the characteristic greater than 3 can be given by*

$$y^2 = x^3 + Ax + B$$

where A, and $B \in \tilde{\mathbf{K}}$. The curve must be non-singular means the curve has no cusps or self-intersections or equivalently we can say

$$4A^3 + 27B^2 \neq 0.$$

The discriminant of $x^3 + Ax + B$ is $\Delta = -(4A^3 + 27B^2)$, so $y^2 = f(x)$ is elliptic curve if Δ is non-zero then it means there are no any multiple roots. If the discriminant is zero then it means the graph of the curve intersects itself. Figure 1 shows some non-singular elliptic curves. For more discussion on singular curves see [15] and [20].

Definition 2 (Quadratic twist of an elliptic over a field)**.** *Let $E/\mathbb{F}$ be an elliptic curve over finite field. A quadratic twist E^{tw} of E over the field $\mathbb{F}$ is again an elliptic curve over the same field such that it is isomorphic to the curve E but on the quadratic extension of the $\mathbb{F}$.*

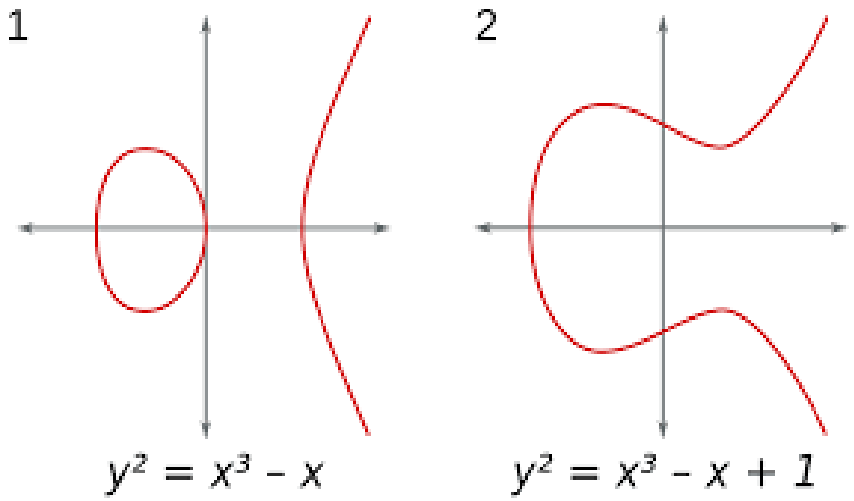

Figure 1 Non-singular Elliptic Curves

For example suppose we have elliptic curve over a field of characteristic greater than 3 defined by the following equation

$$y^2 = x^3 + ax + b$$

where right side doesn't have repeated roots. To find the equation of a quadratic twist suppose we have a square free element d in the field over which the elliptic curve is defined. The following equation defines the quadratic twist of the elliptic curve.

$$dy^2 = x^3 + ax + b.$$

This curve is define over $\mathbb{F}$ but it is not isomorphic to the original function on the base field. The above curve is isomorphic to the original curve on quadratic extension of field $\mathbb{F}$, i.e., $\mathbb{F}(\sqrt{d})$. For more detail on the isomorphism the reader is referred to [1], [12], [6], and [18]. For finite fields specially for even characteristics we give few examples. These examples will help us in learning about the general case that is given in this article. Lets see the definition of quadratic twist in the case of function field over finite field.

Definition 3 (Quadratic twist of an elliptic over rational function field)**.** *Let $\tilde{E}$ be an elliptic curve defined over a rational function field $\tilde{\mathbb{F}}_q(t)$, where q is a power of prime number. Choose a non-square element $s \in \tilde{\mathbb{F}}_q(t)$. Define a new rational function field $\tilde{K} = \tilde{\mathbb{F}}_q(t, s)$, which is an extension of $\tilde{\mathbb{F}}_q(t)$ obtained by adjoining the square root of s. You can then consider the elliptic curve $\tilde{E}'$ defined over $\tilde{K}$ by using the same equation as $\tilde{E}$ but with coefficients from $\tilde{K}$ instead of $\tilde{\mathbb{F}}_q(t)$. This is called the quadratic twist of $\tilde{E}/\tilde{\mathbb{F}}_q(t)$ by s, where t and s are rational functions whose coefficients are from $\tilde{\mathbb{F}}_q$.*

2 Some examples of the known quadratic twists

Here we explain the method of finding the twist by some examples. Essentially we are to describe the method of finding the quadratic twist used in the elementary proof of Manin [4]. This method is applicable in all the characteristics even or odd. Also this method works in both the cases of ordinary and

supersingular elliptic curves. These techniques use linear algebra, field extensions, and some aspects of Galois theory.

Let $\tilde{\mathbf{E}}$ is elliptic curve defined over $\tilde{\mathbf{F}}_q(t)$ with characteristic more than or equal to three. The equation of the elliptic curve is

$$y^2 = x^3 + ax^2 + bx + c.$$

Manin found a quadratic twist of elliptic curve in his elementary proof of Hasse inequality. It is given by the following equation.

$$f(t)y^2 = x^3 + ax^2 + bx + c = f(x).$$

One can check that this curve is isomorphic to the previous curve but on the quadratic extension of the base field. On the base field they are not isomorphic.

The case of characteristic 2 is found in two different forms of elliptic curves, namely ordinary and supersingular celliptic curve. The ordinary elliptic curve in characteristic 2 is given by the following equation.

$$y^2 = x^3 + ax^2 + b.$$

The j-invariant of this curve is non-zero and $b \neq 0$. Otherwise the curve will be singular. The second case is super-singular elliptic curve with j-invariant zero. The equation of such curve is given as follows.

$$y^2 + ay = x^3 + bx + c$$

here $a \neq 0$ to make it non-singular. In [17] authors found the twist in both forms. In ordinary case the equation of the quadratic twist is given by

$$y^2 + txy = t^2 f(x) + x^2 f(t).$$

In the case of supersingular case the equation of the quadratic twist is

$$y^2 + ay = x^3 + bx + c.$$

These twists are defined over the field $\tilde{\mathbf{F}}_q(t)$, and specifically, they are quadratic twists. For further information, interested readers are referred to [4] and [17].

2.1 Quadratic twist in odd characteristic

Let $\tilde{\mathbf{E}}$ be an elliptic curve defined over $\tilde{\mathbf{F}}_q(t)$ with characteristic more than two. It is defined by the following equation.

$$\tilde{\mathbf{E}} : y^2 = x^3 + ax^2 + bx + c = f(x).$$

where s satisfies $s^2 = f(t) = t^3 + at^2 + bt + c$.

Let $\tilde{\mathbf{K}} = \tilde{\mathbf{F}}_q(t, x)$ be a function field and its extension is $\tilde{\mathbf{K}}(s, y)$. $\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}}$ is a Galois extension so $\mathbf{Aut}(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$ is a Galois group that is $\{1, \rho, \delta, \rho\delta\}$ and by the action of Galois group $-y$ and $-s$ are the roots of $\tilde{\mathbf{E}} : y^2 = f(x)$ and $s^2 = f(t)$ respectively. Therefore there exists an involution or an automorphism in $G(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$ that is given as

$$A(x, t, s, y) \mapsto (x, t, -s, -y).$$

where $\tilde{\mathbf{K}}(s,y)$ is a vector space over a field $\tilde{\mathbf{K}}$ symbolically represented as $\tilde{\mathbf{K}}^{\tilde{\mathbf{K}}(s,y)}$. The basis of $\tilde{\mathbf{K}}(s,y)$ is $\{1, s, y, sy\}$.

It is well known fact that, every finite n-dimensional vector space is isomorphic to $\mathbb{R}^n$, where $\mathbb{R}$ is a set of real numbers and $\mathbb{R}^n = \{(a_1, a_2, a_3, \cdots, a^{(n)}) \mid a_1, a_2, a_3, \cdots, a^{(n)} \in \mathbb{R}\}$. This implies that $\tilde{\mathbf{K}}(s,y)$ is isomorphic to $\mathbb{R}^4$, hence we can write

$$1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, y = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, sy = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Since, $A(1) = 1, A(s) = -s, A(y) = -y$ and $A(sy) = A(s)A(y) = (-s)(-y) = sy$, then that there exists a 4×4 matrix defined as follows

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The one of the eigen values of A is 1. By taking eigen value 1, to find its corresponding eigen vector we follow the following procedure. Let $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \tilde{\mathbf{K}}(s,y)$ be a vector, then we have $Av = v$ and it further can be explained as follows.

$$(A - I)v = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

It can simply be concluded that, we have

$x_1 = x_2 = x_3 = 0$ and $x_4 = \tilde{k}$ where $\tilde{k}$ is any constant number, this implies

$$v = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \tilde{k} \end{pmatrix} = \tilde{k} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = sy.$$

so sy is an invariant vector under the transformation A. Let $\eta = sy$, and by taking its square on both sides, we get

$$\eta^2 = (sy)^2 = s^2y^2$$

now by dividing both sides by s^4, we obtain

$$(\eta/s^2)^2 = f(x)/s^2$$

let $(\eta/s^2)^2 = y$, then

$$s^2y^2 = f(x).$$

since $s^2 = f(t)$

$$f(t)y^2 = f(x)$$

$f(t)y^2 = f(x)$ is a twist in Manin's case.

2.2 Quadratic twist in ordinary case

Let $\tilde{\mathbf{E}}$ be an elliptic curve defined over $\tilde{\mathbf{F}}_q(t)$ with characteristic 2 and J.I (j-invariant)of $\tilde{\mathbf{E}}$ is non-zero, defined as

$$\tilde{\mathbf{E}} : y^2 + xy = x^3 + ax^2 + b$$

where s satisfies

$$s^2 + ts = f(t) = t^3 + at^2 + b.$$

Let $\tilde{\mathbf{K}} = \tilde{\mathbf{F}}_q(t, x)$, since extension of $\tilde{\mathbf{K}}$ is $\tilde{\mathbf{K}}(s, y)$, it is known that $\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}}$ is a Galois extension so $\mathbf{Aut}(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$ is a Galois group that is $\{1, \rho, \delta, \rho\delta\}$ and by the action of Galois group $-y - x$ and $-s - t$ are the roots of $\tilde{\mathbf{E}} : y^2 + xy = f(x)$ and $s^2 + ts = f(t)$ respectively. Therefore, there exists an involution or automorphism from $G(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$ that is defined as

$$A(x, t, s, y) \mapsto (x, t, -s - t, -y - x).$$

Since $\tilde{\mathbf{K}}(s, y)$ is a vector space whose coefficients are from fixed field $\tilde{\mathbf{K}}$, the basis of $\tilde{\mathbf{K}}(s, y)$ are $\{1, s, y, sy\}$.

It is understood that $\tilde{\mathbf{K}}(s, y)$ is isomorphic to $\mathbb{R}^4$,

$$1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, y = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, sy = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Since, $A(1) = 1, A(s) = -s - t, A(y) = -y - x$ and $A(sy) = A(s)A(y) = (-s - t)(-y - x) = tx + xs + ty + sy$. We will get 4×4 matrix that is

$$A = \begin{pmatrix} 1 & -t & -x & tx \\ 0 & -1 & 0 & x \\ 0 & 0 & -1 & t \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

since the eigen value of A is 1. For any vector $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \tilde{\mathbf{K}}(s, y)$ can be written as $Av = v$. Therefore

$$(A - I)v = \begin{pmatrix} 0 & -t & -x & tx \\ 0 & -2 & 0 & x \\ 0 & 0 & -2 & t \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The following conclusion is drawn through the upper one

$x_1 = 0, x_2 = x\tilde{k}/2, x_3 = t\tilde{k}/2$ and $x_4 = \tilde{k}$, this implies

$$v = \begin{pmatrix} 0 \\ x\tilde{k}/2 \\ t\tilde{k}/2 \\ \tilde{k} \end{pmatrix} = \tilde{k}/2 \begin{pmatrix} 0 \\ x \\ t \\ 2 \end{pmatrix} = xs + ty + 2sy$$

$xs + ty + 2sy$ is a invariant vector under transformation A.

Let $\eta = xs + ty + 2sy$, since characteristic of $\tilde{\mathbf{K}}(s, y)$ is 2, so $2sy = 0$, this implies $\eta = xs + ty$, take square on both sides of η,

$$\eta^2 = (xs + ty)^2 = x^2s^2 + t^2y^2.$$

Since, $s^2 = f(t) - ts$ and $y^2 = f(x) - xy$ replace these values in η^2

$$\begin{aligned}\eta^2 &= x^2(f(t) - ts) + t^2(f(x) - xy)\\ &= x^2f(t) + t^2f(x) - tx(xs + tx)\\ \eta^2 + tx\eta &= x^2f(t) + t^2f(x)\end{aligned}$$

let $\eta = y$ then,

$$Y^2 + txy = x^2f(t) + t^2f(x)$$

$y^2 + txy = x^2f(t) + t^2f(x)$ is a twist in ordinary case.

2.3 Quadratic twist in super-singular case

Let $\tilde{\mathbf{E}}$ be an elliptic curve defined over $\tilde{\mathbf{F}}_q(t)$ with characteristic 2 and J.I (j-invariant) of $\tilde{\mathbf{E}}$ is zero, defined as

$$\tilde{\mathbf{E}} : y^2 + ay = x^3 + bx + c = f(x)$$

where s satisfies

$$s^2 + as = f(t) = t^3 + +bt + c.$$

Similarly we will have $-y - a$ and $-s - a$ are the roots of $\tilde{\mathbf{E}} : y^2 + ay = f(x)$ and $s^2 + as = f(t)$ respectively. Therefore there exists an involution or automorphism from $G(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$ that is defined as

$$A(x, t, s, y) \mapsto (x, t, -s - a, -y - a).$$

Since $\tilde{\mathbf{K}}(s, y)$ is a vector space whose coefficients are from fixed field $\tilde{\mathbf{K}}$, the basis of $\tilde{\mathbf{K}}(s, y)$ are $\{1, s, y, sy\}$. $\tilde{\mathbf{K}}(s, y)$ is isomorphic to $\mathbb{R}^4$, therefore

$$1 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, s = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, y = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, sy = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Since,

$A(1) = 1, A(s) = -s - a, A(y) = -y - a$

and

$A(sy) = A(s)A(y) = (-s - a)(-y - a) = a^2 + as + ay + sy.$

It means that there exist a 4×4 matrix

$$A = \begin{pmatrix}1 & -a & -a & a^2\\0 & -1 & 0 & a\\0 & 0 & -1 & a\\0 & 0 & 0 & 1\end{pmatrix}$$

since eigen value of A is 1. For any vector $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \tilde{\mathbf{K}}(s, y)$ can be written as $Av = v$.

Therefore

$$(A - I)v = \begin{pmatrix} 0 & -a & -a & a^2 \\ 0 & -2 & 0 & a \\ 0 & 0 & -2 & a \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \tilde{x}^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The following conclusion is drawn through the upper one
$x_1 = 0$, $x_2 = a\tilde{k}/2$, $x_3 = a\tilde{k}/2$ and $x_4 = \tilde{k}$, this implies

$$v = \begin{pmatrix} 0 \\ a\tilde{k}/2 \\ a\tilde{k}/2 \\ \tilde{k} \end{pmatrix} = a\tilde{k}/2 \begin{pmatrix} 0 \\ 1 \\ 1 \\ 2/a \end{pmatrix} = s + y + \frac{2}{a}sy$$

$s + y + \frac{2}{a}sy$ is a invariant vector under involution A, so let $\eta = s + y + \frac{2}{a}sy$, since characteristic of $\tilde{\mathbf{K}}(s, y)$ is 2, so $\eta = s + y$, by taking square on both sides of η,

$$\begin{aligned} \eta^2 &= (s + y)^2 \\ &= s^2 + y^2 \end{aligned}$$

it is known that

$$s^2 = f(t) - as, y^2 = f(x) - ay$$

so,

$$\begin{aligned} \eta^2 &= f(t) - as + f(x) - ay \\ &= f(t) + f(x) - a(s + y) \\ \eta^2 + a\eta &= f(t) + f(x) \end{aligned}$$

let

$$\eta = y$$

then

$$y^2 + ay = f(t) + f(x).$$

$y^2 + ay = f(t) + f(x)$ is a twist in super-singular case.

3 Results and Discussion

3.1 Derivation of quadratic twist in general Weierstrass form

The primary outcome of this paper is established in this section. The proof follows a similar approach to that presented in Section 2. We identify the quadratic twist of the generalized Weierstrass equation for an elliptic curve. The consideration of the quadratic twist of the elliptic curve is an essential component in Manin's elementary proof of the Hasse inequality.

3.2 Quadratic twist in general Weierstrass form

Theorem 1. *Let* $\tilde{\mathbf{E}}$ *be an elliptic curve defined over* $\tilde{\mathbf{F}}_q(t)$ *field of rational functions in one variables over finite field of any characteristic and of order q, with equation*

$$\tilde{\mathbf{E}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = f(x).$$

Then the quadratic twist of $\tilde{\mathbf{E}}$ *is*

$$y^2 + (a_1x + a_3)(a_1t + a_3)y = (a_1x + a_3)^2f(t) + (a_1t + a_3)^2f(x) + 4f(t)f(x).$$

Proof.

Let $\tilde{\mathbf{E}}$ be an elliptic curve defined over $\tilde{\mathbf{F}}_q(t)$ field of rational functions in one variables over finite field of any characteristic and of order q, with equation

$$\tilde{\mathbf{E}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = f(x).$$

Suppose s satisfies

$$s^2 + a_1ts + a_3s = t^3 + a_2t^2 + a_4t + a_6 = f(t)$$

where a_1, a_2, a_3, a_4 and $a_6 \in \mathbb{F}_q$.

Let $\tilde{\mathbf{K}} = \tilde{\mathbf{F}}_q(t, x)$ be the extension of $\tilde{\mathbf{F}}_q(t)$. Since the extension of $\tilde{\mathbf{K}}$ is $\tilde{\mathbf{K}}(s, y)$, it is known that $\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}}$ is a Galois extension so $\mathbf{Aut}(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$ is a Galois group.

Let $G(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}}) = \{1, \rho, \delta, \rho\delta\}$, by the action of $G(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$, $-y - a_1x - a_3$ and $-s - a_1t - a_3$ are the roots of $\tilde{\mathbf{E}} : y^2 + a_1xy + a_3y = f(x)$ and $s^2 + a_1ts + a_3s = f(t)$, respectively.

Therefore there exist a involution or automorphism from Galois group $G(\tilde{\mathbf{K}}(s, y)/\tilde{\mathbf{K}})$ that is defined as

$$A(x, t, s, y) \mapsto (x, t, -s - a_1t - a_3, -y - a_1x - a_3).$$

Since $\tilde{\mathbf{K}}(s, y)$ is a vector space whose coefficients are from fixed field $\tilde{\mathbf{K}}$, the basis of $\tilde{\mathbf{K}}(s, y)$ are $\{1, s, y, sy\}$. It is understood that $\tilde{\mathbf{K}}(s, y)$ is isomorphic to $\mathbb{R}^4$

$$1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, y = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, sy = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Since,

$A(1) = 1, A(s) = -s - a_1t - a_3, A(y) = -y - a_1x - a_3$

and

$A(sy) = A(s)A(y) = (-s - a_1t - a_3)(-y - a_1x - a_3)$

$= (a_1t + a_3)(a_1x + a_3) + (a_1x + a_3)s + (a_1t + a_3)y + sy.$

Therefore, there exist a 4×4 matrix

$$A = \begin{pmatrix} 1 & -(a_1t + a_3) & -(a_1x + a_3) & (a_1t + a_3)(a_1x + a_3) \\ 0 & -1 & 0 & (a_1x + a_3) \\ 0 & 0 & -1 & (a_1t + a_3) \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since the eigen value of A is 1. For any vector $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \tilde{\mathbf{K}}(s, y)$ can be written as $Av = v$. Therefore

$$(A - I)v = \begin{pmatrix} o & -(a_1t + a_3) & -(a_1x + a_3) & (a_1t + a_3)(a_1x + a_3) \\ 0 & -2 & 0 & (a_1x + a_3) \\ 0 & 0 & -2 & (a_1t + a_3) \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The following conclusion is drawn through the upper one

$x_1 = 0$, $x_2 = (a_1x + a_3)\tilde{k}/2$, $x_3 = (a_1t + a_3)\tilde{k}/2$ and $x_4 = \tilde{k}$, this implies

$$v = \begin{pmatrix} 0 \\ (a_1x + a_3)\tilde{k}/2 \\ (a_1t + a_3)\tilde{k}/2 \\ \tilde{k} \end{pmatrix} = \tilde{k}/2 \begin{pmatrix} 0 \\ (a_1x + a_3) \\ (a_1t + a_3) \\ 2 \end{pmatrix}$$

$$= (a_1x + a_3)s + (a_1t + a_3)y + 2sy$$

$(a_1x + a_3)s + (a_1t + a_3)y + 2sy$ is a invariant vector under involution A.

Let $\eta = (a_1x + a_3)s + (a_1t + a_3)y + 2sy$, take square on η

$$(\eta)^2 = ((a_1x + a_3)s + (a_1t + a_3)y + 2sy)^2.$$

Let $\gamma = (a_1x + a_3)$ and $\theta = (a_1t + a_3)$

$$\begin{aligned} (\eta)^2 &= (\gamma s + \theta y + 2sy)^2 \\ &= (\gamma)^2(s)^2 + (\theta)^2y^2 + 4s^2y^2 + 2\gamma\theta sy \\ &+ 4\theta sy^2 + 4\gamma s^2y. \end{aligned}$$

Since, $s^2 = f(t) - (\theta)s$ and $y^2 = f(x) - (\gamma)y$, so

$$\begin{aligned} \eta^2 &= (\gamma)^2(f(t) - (\theta)s) + (\theta)^2(f(x) - (\gamma)y) \\ &+ 4(f(y) - (\gamma)y)(f(t) - (\theta)s) + 4\gamma(f(t) - (\theta)s)y \\ &+ 4\theta s(f(x) - (\gamma)y) + 2\gamma\theta sy. \end{aligned}$$

$$
\begin{aligned}
&= \gamma^2 f(t) - \gamma^2\theta s + \theta^2 f(x) - \gamma\theta^2 y \\
&+ 4f(t)f(x) - 4\gamma y f(t) - 4\theta s f(x) + 4\gamma\theta s y \\
&+ 4\gamma y f(t) - 4\gamma\theta s y + 4\theta s f(x) \\
&- 4\gamma\theta s y + 2\gamma\theta s y.
\end{aligned}
$$

$$
\begin{aligned}
&= \gamma^2 f(t) + \theta^2 f(x) - \gamma\theta(\gamma s + \theta y + 2sy) + 4f(t)f(x) \\
&= \gamma^2 f(t) + \theta^2 f(x) - \gamma\theta\eta + 4f(t)f(x) \\
\eta^2 + \gamma\theta\eta &= \gamma^2 f(t) + \theta^2 f(x) + 4f(t)f(x).
\end{aligned}
$$

Replace the values of γ and θ

$$
\eta^2 + (a_1x + a_3)(a_1t + a_3)\eta = (a_1x + a_3)^2 f(t) + (a_1t + a_3)^2 f(x) + 4f(t)f(x).
$$

let $\eta = y$, then

$$
y^2 + (a_1x + a_3)(a_1t + a_3)y = (a_1x + a_3)^2 f(t) + (a_1t + a_3)^2 f(x) + 4f(t)f(x).
$$

Twist in general case is,

$$
y^2 + (a_1x + a_3)(a_1t + a_3)y = (a_1x + a_3)^2 f(t) + (a_1t + a_3)^2 f(x) + 4f(t)f(x).
$$

3.3 Conclusion

In Manin's exploration, the focus shifted towards revealing the quadratic twist of an elliptic curve defined over the field $\tilde{\mathbf{F}}_q(t)$ within the context of an odd characteristic of $\mathbf{F}_q$. The specific quadratic twist in Manin's case is elucidated as follows:

$$
f(t)y^2 = x^3 + ax^2 + bx + c = f(x).
$$

Having employed the quadratic twist as a pivotal element in his elementary proof, the researcher proceeded to extend the proof by deriving an isomorphism map. This map, in turn, led to the identification of two key points—one being the identity point and the other the Frobenius point. Subsequently, the researcher rigorously demonstrated the validity of four lemmas, each playing an indispensable role in the elementary proof of Hasse's inequality.

In contrast, when examining elliptic curves over fields of even characteristics, other scholars explored two distinct curve types: ordinary elliptic curves and super-singular elliptic curves. In both instances, these researchers encountered different quadratic twists. The quadratic twist specific to ordinary elliptic curves is delineated as follows:

$$
y^2 + txy = t^2 f(x) + x^2 f(t)
$$

and the quadratic twist for super-singular case is given as follows

$$
y^2 + ay = f(t) + f(x).
$$

They also followed Manin's approach in presenting the elementary proof of Hasse's inequality. Consequently, from the preceding discussion, we can deduce that a crucial element in the elementary proof

of Hasse's inequality involves a concept known as a quadratic twist. Even in the more general Weierstrass case, the proof of Hasse's inequality remains applicable. In our investigation, we have identified the quadratic twist for the general Weierstrass form, and the precise results of our study are detailed here. This includes a comprehensive understanding of the general Weierstrass equation.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is defined over $\tilde{\mathbf{F}}_q(t)$. Here, we reveal a special version of the equation:

$$Y^2 + (a_1x + a_3)(a_t + a_3)Y = (a_1x + a_3)^2f(t) + (a_1t + a_3)^2f(x) + 4f(x)f(t)$$

defined over $\tilde{\mathbf{F}}_q(t)$.

This equation is defined over the field $\tilde{\mathbf{F}}_q(t)$. Understanding this version is a key step in proving Hasse's inequality in a simpler way. What makes it interesting is that the method used to find this special version in other cases hasn't been explained in existing writings. You can explore more about this in works like [4], [3], [13], [14], and [17] for a better grasp of the concept.

Author Contributions

Fida Hussain Shaikh: as first author wrote first draft of the manuscript. **Muhammad Afzal Soomro**: Editing and final revision of manuscript and whole supervision. **Iqrar Ali Pali**: Designed the study, reviewed the relevant literature and analysis of study. **Safia Amir Dahri**: Reviewing and writing. **Abdul Rehman Soomro**: Supported in writing.

Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest.

Funding Information

Author Information

ORCID:
Iqrar Ali Pali: 0009-0004-6286-3714
Muhammad Afzal Soomro: 0000-0002-2398-1716

References

[1] Adj, G., Ahmadi, O. and Menezes, A. [2019], 'On isogeny graphs of supersingular elliptic curves over finite fields', *Finite Fields and Their Applications* **55**, 268–283.

[2] Calger, C. S. [2023], 'Elliptic curves over finite fields'.

[3] Chahal, J. S. [1988], *Topics in number theory*, The University Series in Mathematics, Plenum Press, New York.

[4] Chahal, J. S., Soomro, A. and Top, J. [2014], 'A supplement to Manin's proof of the Hasse inequality', *Rocky Mountain J. Math.* **44**(5), 1457–1470.
URL: *https://projecteuclid.org/euclid.rmjm/1420071550*

[5] Flori, J.-P. [2012], Boolean functions, algebraic curves and complex multiplication, PhD thesis, Télécom ParisTech.

[6] Griffon, R. and Ulmer, D. [2020], 'On the arithmetic of a family of twisted constant elliptic curves', *Pacific Journal of Mathematics* **305**(2), 597–640.

[7] Hartshorne, R. [1977], *Algebraic geometry*, Springer-Verlag, New York.

[8] Hayat, U., Ullah, I., Azam, N. A. and Azhar, S. [2022], 'A novel image encryption scheme based on elliptic curves over finite rings', *Entropy* **24**(5), 571.

[9] Khalid, I., Shah, T., Almarhabi, K. A., Shah, D., Asif, M. and Ashraf, M. U. [2022], 'The spn network for digital audio data based on elliptic curve over a finite field', *IEEE Access* **10**, 127939–127955.

[10] Landesman, A. and Litt, D. [2023], 'An introduction to the algebraic geometry of the putman–wieland conjecture', *European Journal of Mathematics* **9**(2), 40.

[11] Pali, I. A., Soomro, M. A., Memon, M., Maitlo, A. A., Dehraj, S. and Umrani, N. A. [2023], 'Construction of an s-box using suppersingular elliptic curve over finite field', *Journal of Hunan University Natural Sciences* **50**(7).

[12] Park, S. W. and Wang, N. [2023], 'On the average of p-selmer ranks in quadratic twist families of elliptic curves over global function fields', *International Mathematics Research Notices* p. rnad095.

[13] Peter Roquette [2018], *The Riemann hypothesis in characteristic P in historical perspective*, Springer Berlin Heidelberg, New York, NY.

[14] Roquette, P. [2002], 'The Riemann hypothesis in characteristic p, its origin and development. I. The formation of the zeta-functions of Artin and of F. K. Schmidt', *Mitt. Math. Ges. Hamburg* **21**(2), 79–157.

[15] Silverman, J. H. [2009], *The arithmetic of elliptic curves. Graduate Text in Mathematics 106*, second edn, Springer- Verlag, New York.

[16] Silvestri, E. [2020], 'Elliptic curves with complex multiplication and applications to class field theory'.

[17] Soomro, M. [2013], *Algebraic curves over finite fields*, s.n.] ; University of Groningen Library] [Host, S.l.; Groningen. OCLC: 846890796.
URL: *http://irs.ub.rug.nl/ppn/35797039X*

[18] Tan, K.-S. [2023], 'The frobenius twists of elliptic curves over global function fields', *arXiv preprint arXiv:2301.00518* .

[19] Umrani, N. A., Pali, I. A. and Dahri, S. A. [2023], 'Construction of substitution boxes using finite fields', *VFAST Transactions on Mathematics* **11**(2), 01–15.

[20] Washington, L. C. [2008], *Elliptic curves*, Discrete Mathematics and its Applications (Boca Raton), second edn, Chapman & Hall/CRC, Boca Raton, FL.
URL: *http://dx.doi.org/10.1201/9781420071474*

[21] Waterhouse, W. C. [1969], 'Abelian varieties over finite fields', *Ann. Sci. École Norm. Sup. (4)* **2**, 521–560.