Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2015, Article ID 597849, 5 pages
http://dx.doi.org/10.1155/2015/597849

Research Article

Metrics on the Sets of Nonsupersingular Elliptic Curves in Simplified Weierstrass Form over Finite Fields of Characteristic Two

Keisuke Hakuta

Interdisciplinary Graduate School of Science and Engineering, Shimane University, 1060 Nishikawatsu-cho, Matsue-shi, Shimane 690-8504, Japan

Correspondence should be addressed to Keisuke Hakuta; hakuta@cis.shimane-u.ac.jp

Received 25 August 2015; Accepted 19 November 2015

Academic Editor: Aloys Krieg

Elliptic curves have a wide variety of applications in computational number theory such as elliptic curve cryptography, pairing based cryptography, primality tests, and integer factorization. Mishra and Gupta (2008) have found an interesting property of the sets of elliptic curves in simplified Weierstrass form (or short Weierstrass form) over prime fields. The property is that one can induce metrics on the sets of elliptic curves in simplified Weierstrass form over prime fields of characteristic greater than three. Later, Vetro (2011) has found some other metrics on the sets of elliptic curves in simplified Weierstrass form over prime fields of characteristic greater than three. However, to our knowledge, no analogous result is known in the characteristic two case. In this paper, we will prove that one can induce metrics on the sets of nonsupersingular elliptic curves in simplified Weierstrass form over finite fields of characteristic two.

1. Introduction

Elliptic curves have been studied by number theorists for a very long time. Nowadays, elliptic curves have been the focus of much attention due to not only the theoretical aspects but also the practical aspects in computational number theory. In particular, elliptic curves have a wide variety of applications in computational number theory such as elliptic curve cryptography [1, 2], pairing based cryptography [3, 4], primality tests [5, 6], and integer factorization [7, 8].

Mishra and Gupta in [9] have found an interesting property of the sets of elliptic curves in simplified Weierstrass form (or short Weierstrass form) over prime fields of characteristic greater than three. The property is that one can induce metrics on the sets of elliptic curves in simplified Weierstrass form over prime fields of characteristic greater than three. Later, Vetro in [10] has found some other metrics on the sets of elliptic curves in simplified Weierstrass form over prime fields of characteristic greater than three. They have proposed potential applications of the metrics to the protection of side channel attacks [11]. However, to our knowledge, no analogous result is known in the characteristic two case. In this direction, it seems mathematically natural to explore a methodology for constructing metrics on (sub)sets of elliptic curves over finite fields of characteristic two whether there is a cryptographic application or not.

The motivation of this work is to study *the characteristic two case*. We will prove that one can induce metrics on the sets of nonsupersingular elliptic curves in simplified Weierstrass form over finite fields of characteristic two.

The rest of this paper is organized as follows. In Section 2, we recall some basic facts that will be used throughout the paper. In Section 3, we give metrics on the sets of nonsupersingular elliptic curves in simplified Weierstrass form over finite fields of characteristic two. Section 4 concludes the paper.

2. Mathematical Preliminaries

In this section we fix our notation and recall some basic facts that will be used throughout the paper. For more details, we refer the reader to [12, Section 3.3], [13, Appendix A].

Let K be a field. For any field K, we denote by $p = \mathrm{char}(K)$ the characteristic of the field K. We use the symbols $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{F}_q$ to represent the integers, real numbers, and a finite field with q elements, where $q = p^r$ $(r \geq 1)$, $p = \mathrm{char}(\mathbb{F}_q)$. For a finite set S, we denote the cardinality of S by $\sharp S$.

Let E/K: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an algebraic curve over K. We set

$$\begin{aligned} d_2 &= a_1^2 + 4a_2, \\ d_4 &= 2a_4 + a_1a_3, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= d_2^2 - 24d_4, \\ \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6, \\ j(E) &= \frac{c_4^3}{\Delta}. \end{aligned} \tag{1}$$

The next theorem provides a necessary and sufficient condition that E/K is an elliptic curve.

Theorem 1 (see [12, Theorem 2.4]). *E is an elliptic curve; that is, the Weierstrass equation is nonsingular, if and only if $\Delta \neq 0$.*

Two elliptic curves E_1 and E_2 are called isomorphic if there exist morphisms (as algebraic varieties) from E_1 to E_2 and from E_2 to E_1 which are inverses of each other. The following theorems (Theorems 2 and 3) tell us when two elliptic curves are isomorphic.

Theorem 2 (see [12, Theorem 2.5]). *If two elliptic curves E_1/K and E_2/K are isomorphic over K, then $j(E_1) = j(E_2)$. The converse is also true if K is an algebraically closed field.*

Theorem 3 (see [12, Theorem 2.1]). *Two elliptic curves E_1/K and E_2/K given by the equations*

$$\begin{aligned} E_1&\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ E_2&\colon y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6 \end{aligned} \tag{2}$$

are isomorphic over K (or K-isomorphic), denoted by $E_1/K \cong E_2/K$, if and only if there exists $u, r, s, t \in K$, $u \neq 0$, such that the change of variables

$$(x, y) \longmapsto \left(u^2x + r, u^3y + u^2sx + t\right) \tag{3}$$

transforms equation E_1 to equation E_2. The relationship of isomorphism is an equivalence relation.

Theorem 4 is the famous Hasse bound for the number of rational points on elliptic curves over finite fields.

Theorem 4 (Hasse). *Let $\sharp E(\mathbb{F}_q) = q + 1 - t$. Then $|t| \leq 2\sqrt{q}$.*

The elliptic curve $E/\mathbb{F}_q$ is called *supersingular* if p divides t. Otherwise, the curve $E/\mathbb{F}_q$ is called *nonsupersingular* (or *ordinary*). It is well-known that if $p = 2$ or $p = 3$, then E is supersingular if and only if $j(E) = 0$. In other words, if $p = 2$ or $p = 3$, E is nonsupersingular if and only if $j(E) \neq 0$. Remark that if $E/K : y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6$ is an elliptic curve with $\mathrm{char}(K) = 2$ and $j(E) \neq 0$, then the admissible change of variables

$$(x, y) \longmapsto \left(\overline{a}_1^2x + \frac{\overline{a}_3}{\overline{a}_1},\ \overline{a}_1^3y + \frac{\overline{a}_1^2\overline{a}_4 + \overline{a}_3^2}{\overline{a}_1^3}\right) \tag{4}$$

transforms E to the nonsupersingular elliptic curve

$$E'/K\colon y^2 + xy = x^3 + a_2x^2 + a_6. \tag{5}$$

An elliptic curve of form (5) is called *simplified Weierstrass form* (or *short Weierstrass form*). Let $E_1/\mathbb{F}_{2^m}, E_2/\mathbb{F}_{2^m}$

$$\begin{aligned} E_1&\colon y^2 + xy = x^3 + a_2x^2 + a_6 \quad (a_6 \neq 0), \\ E_2&\colon y^2 + xy = x^3 + \overline{a}_2x^2 + \overline{a}_6 \quad (\overline{a}_6 \neq 0) \end{aligned} \tag{6}$$

be nonsupersingular elliptic curves over $\mathbb{F}_{2^m}$ in simplified Weierstrass form. If $E_1/\mathbb{F}_{2^m} \cong E_2/\mathbb{F}_{2^m}$, then we have $a_6 = \overline{a}_6$ and the isomorphism is given by

$$\begin{aligned} \phi_s&\colon E_1 \longrightarrow E_2, \\ &(x, y) \longmapsto (x, y + sx), \end{aligned} \tag{7}$$

where s is an element in $\mathbb{F}_{2^m}$ and satisfies the equation

$$s^2 + s = a_2 + \overline{a}_2 \tag{8}$$

(see [12, Section 3.3]).

Remark that if s_1 is a solution of (8) then $s_2 := s_1 + 1$ is the other solution. Furthermore, ϕ_s is an automorphism if and only if $s \in \{0, 1\}$ ([13, Appendix A, Proposition 1.2]).

3. Metrics

In this section we assume that $K = \mathbb{F}_{2^m}$ for $m \geq 2$. We consider the set of nonsupersingular elliptic curves over $\mathbb{F}_{2^m}$ in simplified Weierstrass form; namely,

$$\begin{aligned} &\mathscr{E}(m) \\ &\quad := \{E/\mathbb{F}_{2^m}\colon \text{elliptic curve} \mid E \text{ is of the form } (5)\}. \end{aligned} \tag{9}$$

Throughout this section, we assume that $E_i/\mathbb{F}_{2^m} \in \mathscr{E}(m)$ are elliptic curves for $i = 1, 2, 3$. In addition, we denote

$$\begin{aligned} \phi_s&\colon E_1 \longrightarrow E_2, \\ &(x, y) \longmapsto (x, y + sx), \\ \phi_t&\colon E_2 \longrightarrow E_3, \\ &(x, y) \longmapsto (x, y + tx), \\ \phi_u&\colon E_1 \longrightarrow E_3, \\ &(x, y) \longmapsto (x, y + ux), \end{aligned} \tag{10}$$

if $E_1/\mathbb{F}_{2^m} \cong E_2/\mathbb{F}_{2^m}$, $E_2/\mathbb{F}_{2^m} \cong E_3/\mathbb{F}_{2^m}$, and $E_1/\mathbb{F}_{2^m} \cong E_3/\mathbb{F}_{2^m}$, respectively. Let $\widetilde{\mathscr{B}}$ be the set of all basis of a linear space $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. We put

$$\mathscr{B} \coloneqq \left\{\mathbf{v} = \langle \mathbf{v}_1, \ldots, \mathbf{v}_m \rangle \in \widetilde{\mathscr{B}} \mid \text{there exists } j \in \{1, \ldots, m\} \text{ such that } \mathbf{v}_j = 1\right\}, \tag{11}$$

where $1 \in \mathbb{F}_{2^m}$ is the multiplicative identity element. Note that the set $\mathscr{B}$ is a nonempty finite set because a polynomial basis belongs to the set $\mathscr{B}$. We choose a basis $\mathbf{v} = \langle \mathbf{v}_1, \ldots, \mathbf{v}_m \rangle \in \mathscr{B}$ and fixed it. Then there exists $j_0 \in \{1, \ldots, m\}$ such that $\mathbf{v}_{j_0} = 1$. Let

$$\begin{array}{ccccc} f_{j_0}: & \mathbb{F}_{2^m} & \longrightarrow & \mathbb{F}_2^{m-1} \\ & \cup & & \cup \\ & x = \sum_{i=1}^{m} x_i \mathbf{v}_i & \longmapsto & f_{j_0}(x) = \widehat{x}_{j_0} = \left(x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_m\right) \end{array} \tag{12}$$

denote the surjective $\mathbb{F}_2$-linear map, where $x_i \in \mathbb{F}_2$ $(1 \le i \le m)$. For any $x = \sum_{i=1}^{m} x_i \mathbf{v}_i \in \mathbb{F}_{2^m}$ $(x_i \in \mathbb{F}_2)$, we write

$$\begin{aligned} \mathsf{wt}\left(f_{j_0}(x)\right) &= \mathsf{wt}\left(\widehat{x}_{j_0}\right) \\ &\coloneqq \sharp\left\{i \in \{1, \ldots, m\} \mid i \ne j_0,\ x_i \ne 0\right\}. \end{aligned} \tag{13}$$

Note that, for all $x \in \mathbb{F}_{2^m}$, we always have $\mathsf{wt}(f_{j_0}(x)) \le m - 1$. We put $s = \sum_{i=1}^{m} s_i \mathbf{v}_i \in \mathbb{F}_{2^m}$ $(s_i \in \mathbb{F}_2)$, $t = \sum_{i=1}^{m} t_i \mathbf{v}_i \in \mathbb{F}_{2^m}$ $(t_i \in \mathbb{F}_2)$, and $u = \sum_{i=1}^{m} u_i \mathbf{v}_i \in \mathbb{F}_{2^m}$ $(u_i \in \mathbb{F}_2)$ for the isomorphisms of form (10).

Now we define the function $d_{\mathbf{v}}^{(m)}$: $\mathscr{E}(m) \times \mathscr{E}(m) \to \mathbb{R}$ as follows:

$$\begin{array}{ccccc} d_{\mathbf{v}}^{(m)}: & \mathscr{E}(m) \times \mathscr{E}(m) & \longrightarrow & \mathbb{R} & \\ & \cup & & \cup & \\ & (E_1, E_2) & \longmapsto & \mathsf{wt}\left(f_{j_0}(s)\right) & \text{if } E_1/\mathbb{F}_{2^m} \cong E_2/\mathbb{F}_{2^m}, \\ & (E_1, E_2) & \longmapsto & m & \text{otherwise.} \end{array} \tag{14}$$

Remark that the function $d_{\mathbf{v}}^{(m)}$ is well-defined because, for two solutions s_1, s_2 $(s_2 = s_1 + 1)$ of (8), we have $\mathsf{wt}(f_{j_0}(s_1)) = \mathsf{wt}(f_{j_0}(s_2))$. Namely, the function $d_{\mathbf{v}}^{(m)}$ *does not* depend on the choice of isomorphisms.

We are ready to state and prove the main result of this paper, namely, Theorem 5, which states that the set of nonsupersingular elliptic curves over $\mathbb{F}_{2^m}$ in simplified Weierstrass form is a metric space under the metric $d_{\mathbf{v}}^{(m)}$.

Theorem 5 (metric on $\mathscr{E}(m)$). *$(\mathscr{E}(m), d_{\mathbf{v}}^{(m)})$ is a metric space.*

Proof. We prove the nonnegativity, the nondegeneracy, the symmetry, and the triangular inequality.

(1) Nonnegativity. By the definition of the function $d_{\mathbf{v}}^{(m)}$, we have $d_{\mathbf{v}}^{(m)}(E_1, E_2) \ge 0$ for all $E_1, E_2 \in \mathscr{E}(m)$.

(2) Nondegeneracy. Suppose that $d_{\mathbf{v}}^{(m)}(E_1, E_2) = 0$. Since $m \ge 2$, we must have $\mathsf{wt}(f_{j_0}(s)) = \mathsf{wt}(\widehat{s}_{j_0}) = 0$. This implies that $s_i = 0$ for all $i \ne j_0$. Remember that $s_i \in \mathbb{F}_2 = \{0, 1\}$. Setting $s_{j_0} = 0$ (resp., $s_{j_0} = 1$) yields $s = 0$ (resp., $s = 1$). When $s = 0$ or $s = 1$, the isomorphism of form (10) is an automorphism. Thus, $E_1 = E_2$. Conversely, if $E_1 = E_2$, then the isomorphism of form (10) is an automorphism. It then follows that $s = 0, 1$. Hence $s_i = 0$ for all $i \ne j_0$ and therefore $d_{\mathbf{v}}^{(m)}(E_1, E_2) = \mathsf{wt}(f_{j_0}(s)) = 0$.

(3) Symmetry. If $E_1/\mathbb{F}_{2^m} \ncong E_2/\mathbb{F}_{2^m}$, then $d_{\mathbf{v}}^{(m)}(E_1, E_2) = d_{\mathbf{v}}^{(m)}(E_2, E_1) = m$. Otherwise, we define

$$\begin{aligned} &\psi\colon E_2 \longrightarrow E_1, \\ &(x, y) \longmapsto (x, y + sx). \end{aligned} \tag{15}$$

One can easily check that ψ is an isomorphism. Thus $d_{\mathbf{v}}^{(m)}(E_1, E_2) = d_{\mathbf{v}}^{(m)}(E_2, E_1) = \mathsf{wt}(\widehat{s}_{j_0})$.

(4) Triangular Inequality. Let $E_1, E_2, E_3 \in \mathscr{E}(m)$. We claim that

$$d_{\mathbf{v}}^{(m)}(E_1, E_3) \le d_{\mathbf{v}}^{(m)}(E_1, E_2) + d_{\mathbf{v}}^{(m)}(E_2, E_3). \tag{16}$$

There are two cases to consider. Namely, $E_1/\mathbb{F}_{2^m} \ncong E_3/\mathbb{F}_{2^m}$ and $E_1/\mathbb{F}_{2^m} \cong E_3/\mathbb{F}_{2^m}$.

Case 1 $(E_1/\mathbb{F}_{2^m} \ncong E_3/\mathbb{F}_{2^m})$. In this case, we have $d_{\mathbf{v}}^{(m)}(E_1, E_3) = m$. If follows immediately from $E_1/\mathbb{F}_{2^m} \ncong E_3/\mathbb{F}_{2^m}$ that $E_1/\mathbb{F}_{2^m} \ncong E_2/\mathbb{F}_{2^m}$ or $E_2/\mathbb{F}_{2^m} \ncong E_3/\mathbb{F}_{2^m}$. Then $d_{\mathbf{v}}^{(m)}(E_1, E_2) = m$ or $d_{\mathbf{v}}^{(m)}(E_2, E_3) = m$. This shows that $d_{\mathbf{v}}^{(m)}(E_1, E_3) \le d_{\mathbf{v}}^{(m)}(E_1, E_2) + d_{\mathbf{v}}^{(m)}(E_2, E_3)$ as claimed.

Case 2 $(E_1/\mathbb{F}_{2^m} \cong E_3/\mathbb{F}_{2^m})$. There are two possibilities: $E_1/\mathbb{F}_{2^m} \ncong E_2/\mathbb{F}_{2^m}$ and $E_1/\mathbb{F}_{2^m} \cong E_2/\mathbb{F}_{2^m}$. The former case gives $d_{\mathbf{v}}^{(m)}(E_1, E_2) = m$, which shows that $d_{\mathbf{v}}^{(m)}(E_1, E_3) \le d_{\mathbf{v}}^{(m)}(E_1, E_2) \le d_{\mathbf{v}}^{(m)}(E_1, E_2) + d_{\mathbf{v}}^{(m)}(E_2, E_3)$ (or, more precisely, $d_{\mathbf{v}}^{(m)}(E_1, E_2) < d_{\mathbf{v}}^{(m)}(E_1, E_2) + d_{\mathbf{v}}^{(m)}(E_2, E_3)$ since $E_2/\mathbb{F}_{2^m} \ncong E_3/\mathbb{F}_{2^m}$). In the latter case, we have $\phi_u = \phi_t \circ \phi_s$. This yields that $d_{\mathbf{v}}^{(m)}(E_1, E_2) = \mathsf{wt}(f_{j_0}(s))$, $d_{\mathbf{v}}^{(m)}(E_2, E_3) = \mathsf{wt}(f_{j_0}(t))$, and $d_{\mathbf{v}}^{(m)}(E_1, E_3) = \mathsf{wt}(f_{j_0}(u)) = \mathsf{wt}(f_{j_0}(s + t))$, respectively. Since $|s_i + t_i| \le |s_i| + |t_i|$ for all $i \in \{1, \ldots, m\}$, $i \ne j_0$, we obtain

$$\begin{aligned} \left|\mathsf{wt}\left(f_{j_0}(u)\right)\right| &= \left|\mathsf{wt}\left(f_{j_0}(s + t)\right)\right| \\ &\le \left|\mathsf{wt}\left(f_{j_0}(s)\right)\right| + \left|\mathsf{wt}\left(f_{j_0}(t)\right)\right|, \end{aligned} \tag{17}$$

where $|s_i|$ (resp., $|t_i|$) is equal to 1 when $s_i = 1$ (resp., $t_i = 1$) and otherwise $|s_i|$ (resp., $|t_i|$) is equal to 0. Hence we have $d_{\mathbf{v}}^{(m)}(E_1, E_3) \leq d_{\mathbf{v}}^{(m)}(E_1, E_2) + d_{\mathbf{v}}^{(m)}(E_2, E_3)$. This completes the proof. □

Remark 6. The main observation of Theorem 5 is that the isomorphism of form (10) is an automorphism if and only if $s \in \{0, 1\}$. By omitting the j_0th entry of s and by summing up the number of nonzero s_i with $1 \leq i \leq m$ and $i \neq j_0$, one can construct a metric on $\mathscr{E}(m)$. In order to omit the j_0th entry, we use a basis $\mathbf{v}$ which is belonging to the set $\mathscr{B}$. The nonnegativity and the symmetry for $d_{\mathbf{v}}^{(m)}$ are obvious. The nondegeneracy for $d_{\mathbf{v}}^{(m)}$ is followed by the omission of j_0th entry. The triangular inequality for the Hamming distance implies the triangular inequality for $d_{\mathbf{v}}^{(m)}$.

In the definition of $d_{\mathbf{v}}^{(m)}$, we put $d_{\mathbf{v}}^{(m)}(E_1, E_2) = m$ when $E_1/\mathbb{F}_{2^m} \not\cong E_2/\mathbb{F}_{2^m}$. However, the value m does not have any special meanings, and one can use any other positive integer greater than or equal to m in order to define different metrics on $\mathscr{E}(m)$.

Corollary 7 (other metrics on $\mathscr{E}(m)$). *(1) For any integer $n \in \mathbb{Z}$ greater than or equal to m, define the function $d_{\mathbf{v}}^{(n)} : \mathscr{E}(m) \times \mathscr{E}(m) \to \mathbb{R}$ as follows:*

$$\begin{array}{ccccc} d_{\mathbf{v}}^{(n)}: & \mathscr{E}(m) \times \mathscr{E}(m) & \longrightarrow & \mathbb{R} & \\ & \cup & & \cup & \\ & (E_1, E_2) & \longmapsto & \mathrm{wt}\left(f_{j_0}(s)\right) & \text{if } E_1/\mathbb{F}_{2^m} \cong E_2/\mathbb{F}_{2^m}, \\ & (E_1, E_2) & \longmapsto & n & \text{otherwise.} \end{array} \tag{18}$$

Then $(\mathscr{E}(m), d_{\mathbf{v}}^{(n)})$ is a metric space.

(2) We define the function $d_{\mathbf{v}}^{(\infty)}: \mathscr{E}(m) \times \mathscr{E}(m) \to \mathbb{R} \cup \{\infty\}$ as follows:

$$\begin{array}{ccccc} d_{\mathbf{v}}^{(\infty)}: & \mathscr{E}(m) \times \mathscr{E}(m) & \longrightarrow & \mathbb{R} \cup \{\infty\} & \\ & \cup & & \cup & \\ & (E_1, E_2) & \longmapsto & \mathrm{wt}\left(f_{j_0}(s)\right) & \text{if } E_1/\mathbb{F}_{2^m} \cong E_2/\mathbb{F}_{2^m}, \\ & (E_1, E_2) & \longmapsto & \infty & \text{otherwise.} \end{array} \tag{19}$$

Then $(\mathscr{E}(m), d_{\mathbf{v}}^{(\infty)})$ is also a metric space.

(3) Set

$$\mathscr{N}_m := \{m, m+1, m+2, \ldots\} \cup \{\infty\}. \tag{20}$$

We choose a subset $\mathscr{S} \subseteq \mathscr{B}$. Since $\mathscr{B}$ is a finite set, the subset $\mathscr{S}$ is also a finite set. For each $\mathbf{v} \in \mathscr{S}$, we take $n_{\mathbf{v}} \in \mathscr{N}_m$. Then the function

$$\begin{aligned} \sum_{\mathbf{v} \in \mathscr{S}} d_{\mathbf{v}}^{(n_{\mathbf{v}})}: \mathscr{E}(m) \times \mathscr{E}(m) &\longrightarrow \mathbb{R} \cup \{\infty\}, \\ (E_1, E_2) &\longmapsto \sum_{\mathbf{v} \in \mathscr{S}} d_{\mathbf{v}}^{(n_{\mathbf{v}})}(E_1, E_2) \end{aligned} \tag{21}$$

is also a metric on $\mathscr{E}(m)$.

(4) We put $\mathbb{R}_{>0} := \{c \in \mathbb{R} \mid c > 0\}$. For each $\mathbf{v} \in \mathscr{S}$, we take $c_{\mathbf{v}}^{(n_{\mathbf{v}})} \in \mathbb{R}_{>0}$. Then as in (3), we can define the metric

$$\begin{aligned} \sum_{\mathbf{v} \in \mathscr{S}} c_{\mathbf{v}}^{(n_{\mathbf{v}})} d_{\mathbf{v}}^{(n_{\mathbf{v}})}: \mathscr{E}(m) \times \mathscr{E}(m) &\longrightarrow \mathbb{R} \cup \{\infty\}, \\ (E_1, E_2) &\longmapsto \sum_{\mathbf{v} \in \mathscr{S}} c_{\mathbf{v}}^{(n_{\mathbf{v}})} d_{\mathbf{v}}^{(n_{\mathbf{v}})}(E_1, E_2) \end{aligned} \tag{22}$$

on $\mathscr{E}(m)$.

Proof. The proofs are very similar to the proof of Theorem 5; thus we omit them. □

Remark 8 (topological properties of a metric space $\mathscr{E}(m)$). We recall that a metric space gives rise to a topology. Here, we make sure of the properties of the topology on $\mathscr{E}(m)$ induced by a metric. Given a metric space $(\mathscr{E}(m), d)$, let $\mathscr{O}_d$ be the topology on $\mathscr{E}(m)$ induced by the metric d. Note that the facts shown below *do not* depend on the metric d. A metric space is a Hausdorff space [14, p. 110, Proposition 11.5]. A finite subset of a topological space is compact [14, p. 128, Example 13.8(a)]. These two facts indicate that $(\mathscr{E}(m), \mathscr{O}_d)$ is a compact Hausdorff space. If a finite space is Hausdorff then its topology is discrete [14, p. 111, Exercise 11.2(b)]. Therefore $\mathscr{O}_d$ is discrete, and hence $(\mathscr{E}(m), \mathscr{O}_d)$ is totally disconnected. Any finite metric space is compact, therefore $(\mathscr{E}(m), \mathscr{O}_d)$ is a complete metric space.

4. Conclusion

In this paper, we have defined some metrics on the sets of nonsupersingular elliptic curves in simplified Weierstrass form over finite fields of characteristic two. In order to derive analogous results for the case of *supersingular elliptic curves of characteristic two* and for the case of *elliptic curves of characteristic three*, some deep observation on the properties of elliptic curves over finite fields will be needed.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by a grant for young researchers from Shimane University in 2015.

References

[1] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[2] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO '85 Proceedings*, vol. 218 of *Lecture Notes in Computer Science*, pp. 417–426, Springer, Berlin, Germany, 1986.

[3] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[4] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[5] A. O. L. Atkin and F. Morain, "Elliptic curves and primality proving," *Mathematics of Computation*, vol. 61, no. 203, pp. 29–68, 1993.

[6] S. Goldwasser and J. Kilian, "Primality testing using elliptic curves," *Journal of the ACM*, vol. 46, no. 4, pp. 450–472, 1999.

[7] H. W. Lenstra Jr., "Factoring integers with elliptic curves," *Annals of Mathematics*, vol. 126, no. 3, pp. 649–673, 1987.

[8] P. L. Montgomery, "Speeding the Pollard and elliptic curve methods of factorization," *Mathematics of Computation*, vol. 48, no. 177, pp. 243–264, 1987.

[9] P. K. Mishra and K. C. Gupta, "A metric on the set of elliptic curves over $\mathbb{F}_p$," *Applied Mathematics Letters*, vol. 21, no. 12, pp. 1330–1332, 2008.

[10] F. Vetro, "Metrics on the set of elliptic curves over $\mathbb{F}_p$," *International Journal of Contemporary Mathematical Sciences*, vol. 1, no. 1, pp. 22–24, 2011.

[11] M. Joye and C. Tymen, "Protections against differential analysis for elliptic curve cryptography: an algebraic approach," in *Cryptographic Hardware and Embedded Systems—CHES 2001 Proceedings*, vol. 2162 of *Lecture Notes in Computer Science*, pp. 377–390, Springer, Berlin, Germany, 2011.

[12] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston, Mass, USA, 1993.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 2nd edition, 2009.

[14] W. A. Sutherland, *Introduction to Metric and Topological Spaces*, Oxford University Press, 2nd edition, 2009.