Constructing pairing-friendly algebraic curves of genus 2 with small ρ-value

by

Kuo Ming James Chou

A thesis submitted to the
Mathematics and Statistics
in conformity with the requirements for
the degree of Doctor of Philosophy

Queen's University
Kingston, Ontario, Canada
November 2011

Abstract

For pairing-based cryptographic protocols to be both efficient and secure, the underlying genus 2 curves defined over finite fields used must satisfy pairing-friendly conditions, and have small ρ-value, which are not likely to be satisfied with random curves.

In this thesis, we study two specific families of genus 2 curves defined over finite fields whose Jacobians do not split over the ground fields into a product of elliptic curves, but geometrically split over an extension of the ground field of prescribed degree $n = 3, 4$, or 6. These curves were also studied extensively recently by Kawazoe and Takahashi in 2008, and by Freeman and Satoh in 2009 in their searches of pairing-friendly curves.

We present a new method for constructing and identifying suitable curves in these two families which satisfy the pairing-friendly conditions and have ρ-values around 4. The computational results of the ρ-values obtained in this thesis are consistent with those found by Freeman and Satoh in 2009. An extension of our new method has led to a cryptographic example of a pairing-friendly curve in one of the two families which has ρ-value 2.969, and it is the lowest ρ-value ever recorded for curves of this type. Our method is different from the method proposed by Freeman and Satoh, since we can prescribe the minimal degree $n = 3, 4$ or 6 extension of the ground fields which the Jacobians of the curves split over.

Acknowledgments

This thesis would not have been possible without the support of many people. The author wishes to express his gratitude to his supervisor, Dr. Ernst Kani who was abundantly helpful and offered invaluable assistance, support and guidance. Deepest gratitude are also due to the members of the supervisory committee, Dr. Andrew Lewis, Dr. Mike Roth, Dr. Selim Akl, and Dr. Kumar Murty who agreed to host the thesis defense on such a short notice.

Special thanks also to Dr. Andrew Lewis, Dr. Ernst Kani, and Dr. Ram Murty for their continuous encouragement and support, especially during the last three weeks of the thesis submission.

The author also likes to express his gratitude to his parents and grandparents without whose sacrifices in life, the author would not have come to Canada and pursued a postgraduate degree.

A mi hermosa mujer María, tú eres la razón por la que lucho cada día para ser mejor persona. Ni siquiera puedo llegar a imaginar cómo habría vivido mi vida si no te hubiera conocido en Kingston. Gracias por ser como eres y por aceptarme tal y como soy. Esta tesis está dedicada a ti, por todos los sacrificios que has tenido que hacer por mí.

Contents

Chapter 1

Introduction

1.1 Motivation

In 2000, Joux [27] discovered that bilinear pairings can be used for the construction of cryptographic protocols. Using Joux's protocol, it is possible for three parties to share a common key in only a single round of communication, where all previous known protocols take at least two rounds of communication. Another major application of bilinear pairings is the short signature scheme due to Boneh, Lynn, and Shacham [4]. Comparing with previously known signature schemes, their signature scheme produces shorter signatures, while providing similar level of security. Since then, there has been a flurry of activity in the design and analysis of cryptographic protocols using bilinear pairings.

In these pairing-based cryptographic protocols, the underlying bilinear pairings commonly used are the Weil and Tate pairings, and the underlying groups used come from the $\mathbb{F}_q$-rational points $A(\mathbb{F}_q)$ of some abelian varieties $A/\mathbb{F}_q$ with dimension $g \leq 3$. In fact, the underlying groups commonly used are either ordinary elliptic

curves or the Jacobians of some genus two ordinary hyperelliptic curves over finite fields [19]. The advantage of these groups is that on the one hand there are efficient group operations inherited by these group structures, and that on the other hand the discrete logarithm problem (DLP) in these groups is considered to be computationally difficult.

For pairing-based cryptographic protocols to be secure against attacks of the DLP like the Pollard-ρ method or index-calculus [14, 15, 32, 45], the underlying ordinary elliptic curves or genus two ordinary hyperelliptic curves used must satisfy pairing-friendly conditions, which are not likely to be satisfied in general with random curves defined over finite fields [11]. For pairing-based cryptographic protocols to be efficient, the ρ-values associated with the pairing-friendly ordinary elliptic curves or pairing-friendly genus two ordinary hyperelliptic curves must be close to the theoretical minimum of 1.

In the literature, there already exists various efficient constructions of pairing-friendly ordinary elliptic curves defined over finite fields with the associated ρ-value close to 1 [14]. As for genus two curves, the construction of pairing-friendly ordinary curves defined over finite fields with small ρ-value is still not as well developed as for the elliptic curve case.

In [12], Freeman constructed pairing-friendly ordinary genus two hyperelliptic curves defined over finite fields with ρ-value approximately 4, which improved his previous result by half [11]. The ordinary genus two hyperelliptic curves considered by Freeman were such that their Jacobians do not split into product of two elliptic curves over the algebraic closure of the ground field.

The currently best performing of pairing-friendly ordinary genus two hyperelliptic

curves with the associated ρ-value consistently around or below 4 are the Legendre-Satoh curves and Bolza-Freeman-Satoh curves studied by Freeman and Satoh [13]. These are the ordinary genus two hyperelliptic curves such that their Jacobians geometrically split into a product of elliptic curves over a quartic extension or a sextic extension of the ground field. This motivates our interest in designing a method of constructing pairing-friendly ordinary Legendre-Satoh curves and Bolza-Freeman-Satoh curves defined over finite fields, and to study the associated ρ-value of these curves constructed via the method.

In particular, we are interested in constructing pairing-friendly Legendre-Satoh curves and Bolza-Freeman-Satoh curves defined over finite fields whose Jacobians do not split over the ground field, but split into a product of elliptic curves over a specific finite extension of the ground field. The main result of this thesis is the procedure called **Method I** which does just that, and has led to the discovery of several pairing-friendly Legendre-Satoh curves and Bolza-Freeman-Satoh curves with ρ-values around 4. The contributions and the outline of this thesis will be addressed in the following section.

1.2 Contributions and outline of the thesis

In Chapter 2 of this thesis, the necessary background on abelian varieties defined over finite fields and pairing-based cryptography will be introduced. The key concepts in pairing-based cryptography, like the embedding degree with respect to a prime and the associated ρ-value of an algebraic curve, will be presented. In this chapter, the results from Chou and Kani [7] on the classification and existence of abelian surfaces over finite fields which become geometrically split after some finite extension of the

ground fields will be summarized.

In Chapter 3 of this thesis, the families of Legendre-Satoh curves and Bolza-Freeman-Satoh curves defined over finite fields will be presented, and the geometric splitting properties of their Jacobians over a quartic and a sextic extension of the ground field, respectively, will be studied. The first contribution of this chapter is a new proof of Theorem 3.3.1 which answers how the Jacobian of a Legendre-Satoh curve splits over the quartic extension of the ground field. This new proof closes the small gap of the proof presented by Satoh for the same statement in [43] §3, which is summarized in Remark 3.3.2. The second contribution of this chapter is part (b) of Theorem 3.4.1 which gives a new proof of how the Jacobian of a Bolza curve splits over the ground field. The third contribution of this chapter is Corollary 3.4.3 which is a new result on how the Jacobian of a Bolza-Freeman-Satoh curve with certain conditions on its curve coefficients splits over the ground field, over a quadratic extension, and over a cubic extension of the ground field, respectively. The fourth contribution of this chapter is Theorem 3.4.4 which gives necessary and sufficient conditions for the Jacobians of Bolza-Freeman-Satoh curves to be simple over the ground fields. Theorem 3.4.4 fixes a mistake of the proof of theorem 4.5 by Freeman and Satoh [13], which is explained in Remark 3.4.5.

In Chapter 4, the main result of this chapter and of this thesis is Theorem 4.1.1 which gives necessary and sufficient conditions on a tuple of integer values in order to correspond to an isogeny class of abelian varieties of a certain type. More precisely, this class consists of simple geometrically split ordinary abelian surfaces with some prescribed embedding degree with respect to a prime and has the desired geometrical splitting properties over an extension of the ground field of prescribed degree $n = 3, 4$,

or 6. These necessary and sufficient conditions on the integer tuples outlined in Theorem 4.1.1 give rise to the important concept of valid integer tuples for a given $n = 3, 4$ or 6 and their induced isogeny classes of simple geometrically split ordinary abelian surfaces. The second main result of this chapter and of this thesis is Theorem 4.2.3 which gives the necessary conditions on a valid integer tuple for a given $n = 3, 4$ or 6, so that it gives rise to a Legendre-Satoh curve or a Bolza-Freeman-Satoh curve whose Jacobian is isogenous to the simple geometrically split ordinary abelian surfaces induced by the valid integer tuple.

In Chapter 5, the main result of this chapter and the third main result of this thesis is Theorem 5.1.4 which leads to the procedure **Method I** outlined in Section 5.2. The procedure **Method I** searches for valid integer tuples for a given $n = 3, 4$ or 6 that satisfy the necessary conditions mentioned in Theorem 4.2.3, and constructs the desired Legendre-Satoh curve or Bolza-Freeman-Satoh curve. The fourth main result of this thesis is the implementation of **Method I** in Section 5.3, where we found the first example of a pairing-friendly Legendre-Satoh curve whose Jacobian has ρ-value 4.1371, and is not split over a quadratic extension of the ground field. This discovery is summarized in Example 5.3.2. In the same implementation, we also found the first example of a pairing-friendly Bolza-Freeman-Satoh curve whose Jacobian has ρ-value 4.1654 and is not split over a quadratic extension nor over a cubic extension of the ground field. This discovery is summarized in Example 5.3.3. In general, the ρ-values of the pairing-friendly Legendre-Satoh curves and Bolza-Freeman-Satoh curves obtained through our method are around 4, which are consistent with the results obtained by Freeman and Satoh [13]. Our method is different from the method of Freeman and Satoh, since we can prescribe the minimal degree $n = 3, 4$ or 6 extension

of the ground fields which the Jacobians of the curves split over, which is not so clear in the method of Freeman and Satoh.

In Chapter 6, we point out some future lines of research by sketching an extension of **Method I** for searching valid integer tuples for $n = 3$. A preliminary implementation of this new method has led to the discovery of an pairing-friendly Bolza-Freeman-Satoh curve whose Jacobian does not split over the ground field but splits over a cubic extension of the ground field, and has ρ-value less than 3. The ρ-value obtained in this case is 2.969. This discovery is summarized in Example 6.1.5.

Chapter 2

Preliminaries

The purpose of this chapter is to provide the necessary background on abelian varieties defined over finite fields, and to introduce abelian surfaces defined over finite fields which become geometrically split after some finite extension of the ground fields. Some general background on the properties of abelian variety over finite fields will be given in Section 2.1. Those properties of abelian surfaces over finite fields which are important to pairing-based cryptography will be presented in Section 2.2. Finally, the results from Chou and Kani [7] on the classification and existence of abelian surfaces over finite fields which become geometrically split after some finite extension of the ground fields will be summarized in Section 2.3.

2.1 Background and notations

Throughout this thesis, we will follow the convention that is used in Milne [38, 39]. For a scheme $V/\mathbb{F}$ where $\mathbb{F}$ is an arbitrary perfect field and a $\mathbb{F}$-algebra R, $V \otimes R$ denotes $V \times_{\mathrm{spec}(\mathbb{F})} \mathrm{spec}(R)$ and $V(R)$ denotes $\mathrm{Mor}_{\mathbb{F}}(\mathrm{Spec}(R), V)$. By a scheme $V/\mathbb{F}$,

we will always mean that V is a scheme of finite type over $\mathbb{F}$. A *variety* $V/\mathbb{F}$ is a separated scheme such that $V \otimes \overline{\mathbb{F}}$ is integral, where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$. From here and onward, all statements made will be relative to a fixed ground field; namely, if V and W are varieties over $\mathbb{F}$, then a sheaf or a divisor on V or a morphism $V \to W$, is automatically meant to be defined over $\mathbb{F}$. We will use the words "curve" and "surface" to mean a variety of dimension 1 and 2.

A group variety over $\mathbb{F}$ is a variety $V/\mathbb{F}$ together with morphisms

$$m : V \times V \to V \text{ (multiplication)}, \quad inv : V \to V \text{ (inverse)}$$

and an element $\epsilon \in V(\mathbb{F})$ such that the structure on $V(\overline{\mathbb{F}})$ defined by m and inv is that of a group with identity element ϵ. A complete group variety is called an *abelian variety* which is projective and commutative ([38] §2, §7.).

Recall that for a scheme $S/\mathbb{F}$, $\mathrm{Pic}(S)$ denotes the group of isomorphism classes of invertible sheaves on S, and that $S \mapsto \mathrm{Pic}(S)$ is a functor from the category of schemes over $\mathbb{F}$ to that of abeilan groups. Let $C/\mathbb{F}$ be a complete nonsingular curve with genus g_C. The degree of a divisor $D = \sum n_i P_i$ on C is $\sum n_i[\mathbb{F}(P_i) : \mathbb{F}]$ where $n_i \in \mathbb{Z}$. Since every invertible sheaf $\mathcal{L}$ on C is associated to a divisor D on C, we can define $\deg(\mathcal{L}) = \deg(D)$, and write $\mathrm{Pic}^0(C)$ for the group of isomorphism classes of invertible sheaves of degree 0 on C.

If $T/\mathbb{F}$ is a connected scheme, then we can define a group $\mathrm{P}^0_C(T)$ of families of invertible sheaves on C of degree 0 parametrized by T, modulo the trivial families ([39], page 168). This P^0_C is a functor from schemes over $\mathbb{F}$ to abelian groups. The following theorem taken from page 168 of [39] gives rise to the concept of Jacobian variety of C.

Theorem 2.1.1. *There is an abelian variety $J/\mathbb{F}$ and a morphism of functors ι_C :*

$\mathrm{P}^0_C \to J$ *such that* $\iota_C : \mathrm{P}^0_C(T) \to J(T)$ *is an isomorphism whenever* $C(T)$ *is nonempty.*

Let $\mathbb{F}'$ be a finite Galois extention of $\mathbb{F}$ such that $C(\mathbb{F}') \neq \emptyset$, and let G be the Galois group of $\mathbb{F}'$ over $\mathbb{F}$. Then, for every scheme T over $\mathbb{F}$, $C(T \otimes \mathbb{F}')$ is not empty and $\iota_C(T \otimes \mathbb{F}') : \mathrm{P}^0_C(T \otimes \mathbb{F}') \to J(T \otimes \mathbb{F}')$ is an isomorphism ([39], page 168). Since

$$J(T) := \mathrm{Mor}_{\mathbb{F}}(T, J) = \mathrm{Mor}_{\mathbb{F}'}(T \otimes \mathbb{F}', J \otimes \mathbb{F}')^G = J(T \otimes \mathbb{F}')^G,$$

it can be seen that J represents the functor $T \mapsto \mathrm{P}^0_C(T \otimes \mathbb{F}')^G$, and this implies that the pair (J, ι_C) is uniquely determined up to a unique isomorphism by the condition stated in the theorem above. The abelian variety J in the theorem above is called the *Jacobian variety* of C. We will then use J_C to denote the Jacobian variety of C. It is known that $\dim(J_C) = g_C$ ([39], page 171) and, for any field extension $\mathbb{F}'$ of $\mathbb{F}$ in which $C(\mathbb{F}') \neq \emptyset$, the map ι_C defines an isomorphism $\mathrm{Pic}^0(C) \simeq J_C(\mathbb{F}')$ ([39], page 168).

Let $f : A \to B$ be a homomorphism of abelian varieties. Then $\ker(f)$ is a closed subgroup scheme of A of finite type over $\mathbb{F}$. If f is surjective and has finite kernel then f is called an *isogeny*. Two abelian varieties $A/\mathbb{F}$ and $B/\mathbb{F}$ are said to be *isogenous*, denoted by $A \sim B$, if there is an isogeny between $A/\mathbb{F}$ and $B/\mathbb{F}$. The *degree* $\deg(f)$ of an isogeny $f : A \to B$ is defined to be the order of the kernel of f as a finite group scheme. Next, we have the following important definition.

Definition 2.1.2. An abelian variety $A/\mathbb{F}$ is called *simple* or $\mathbb{F}$-simple if it has no nontrivial abelian subvarieties defined over $\mathbb{F}$. If $A \otimes \overline{\mathbb{F}}$ has no nontrivial abelian subvarieties over the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$, then A is said to be *absolutely simple*.

Let $\mathrm{End}(A)$ be the ring of endomorphisms of $A/\mathbb{F}$ defined over $\mathbb{F}$. Then

$$\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is the $\mathbb{Q}$-algebra associated with $\mathrm{End}(A)$, and it is known to be finite-dimensional semisimple algebra ([38], §12). If $A/\mathbb{F}$ is a simple abelian variety and $\alpha \in \mathrm{End}(A)$, then the connected component of $\ker(\alpha)$ containing 0 is an abelian variety, and so it is either A or 0. Hence α is either 0 or an isogeny. In the latter case, there is an isogeny $\beta : A \to A$ such that $\beta \circ \alpha = n$ for some $n \in \mathbb{Q}$. Thus this means that α becomes invertible in $\mathrm{End}^0(A)$. We summarize this observation as follows.

Proposition 2.1.3. *If $A/\mathbb{F}$ is a simple abelian variety, then $\mathrm{End}^0(A)$ is a division algebra.*

The following result is taken from page 54 of Milne and Waterhouse [48], which often allows us to restrict the investigation of abelian varieties to those simple ones.

Theorem 2.1.4. *Given an abelian variety $A/\mathbb{F}$, then*

$$A \sim \prod_{i=1}^{r} A_i^{n_i} \tag{2.1.1}$$

where $n_i \in \mathbb{N}$ and each A_i is $\mathbb{F}$-simple such that $A_i \not\sim A_j$ when $i \neq j$. Furthermore, the integers n_i and the A_i are both uniquely determined up to isogeny.

The map (2.1.1) then induces a ring isomorphism

$$\mathrm{End}^0(A) \simeq \prod_{i=1}^{b} M_{n_i}(\mathrm{End}^0(A_i)) \tag{2.1.2}$$

where each $M_{n_i}(\mathrm{End}^0(A_i))$ denotes the ring of $n_i \times n_i$ matrices over the division algebra $\mathrm{End}^0(A_i)$ ([38], page 122). Recall from Milne [38] (page 125) that every element $f \in \mathrm{End}^0(A)$ satisfies a monic polynomial $h_f(X) \in \mathbb{Q}[X]$ of degree $2g$ where $g = \dim(A)$ and such that, for all rational numbers r, $h_f(r) = \deg(f - r)$. It is a fact that $h_f(X)$ has integer coefficients when $f \in \mathrm{End}(A)$. We call $h_f(X)$ the *characteristic polynomial* of f and define the *trace* of f to be the negative of the integer coefficient of X^{2g-1} in $h_f(X)$.

In the case of a finite field $\mathbb{F}_q$, a given g-dimensional abelian variety $A/\mathbb{F}_q$ has a *Frobenius endomorphism* $\pi_A \in \mathrm{End(A)}$ such that π_A is the identity map on the underlying topological space of A and is the map $a \mapsto a^q$ on the structure sheaf $\mathcal{O}_A$ of A. Let $h_A(X) := h_{\pi_A}(X)$. The following result taken from Milne [38] (page 143) is well known.

Theorem 2.1.5. *Write* $h_A(X) = \prod_{i=1}^{2g}(X - \alpha_i) \in \mathbb{C}[X]$, *and for all* $m \geq 1$ *let* $N_m = \#A(\mathbb{F}_{q^m})$. *Then,*
(1) $N_m = \prod_{i=1}^{2g}(1 - \alpha_i^m) = h_{A\otimes\mathbb{F}_{q^m}}(1)$ *and*
(2) $|\alpha_i| = q^{\frac{1}{2}}$.
Hence,

$$|N_m - q^{mg}| \leq 2g \cdot q^{m(g-\frac{1}{2})} + (2^{2g} - 2g - 1)q^{m(g-1)}.$$

From the theorem above, it is clear that once the characteristic polynomial $h_A(X)$ of $A/\mathbb{F}_q$ is known, then the cardinality of the $\mathbb{F}_{q^m}$-rational points of $A \otimes \mathbb{F}_{q^m}$ can be deduced.

Define a *Weil* q-integer α to be an algebraic integer such that, for every embedding σ of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$, we have $|\sigma(\alpha)| = q^{\frac{1}{2}}$. Two Weil q-integers α and α' are said to belong to the same conjugacy class if α and α' have the same minimum polynomial over $\mathbb{Q}$. From Theorem 2.1.5, it follows that the roots π_A of $h_A(X) \in \mathbb{Z}[X]$ are all Weil q-integers. The following famous result is due to Tate (See Mumford [41], page 253).

Theorem 2.1.6. *(Tate) Let* $A/\mathbb{F}_q$ *and* $A'/\mathbb{F}_q$ *be two abelian varieties. Then* $A \sim A'$ *if and only if* $h_A(X) = h_{A'}(X)$.

In general, the characteristic polynomial $h_A(X)$ of a simple abelian variety $A/\mathbb{F}_q$ may be reducible over $\mathbb{Z}[X]$. The following theorem, taken from page 58 of [48],

addresses the splitting property of $h_A(X)$ over $\mathbb{Z}$ and the relation between $\mathrm{End}^0(A)$ and $\mathbb{Q}(\pi_A)$.

Theorem 2.1.7. *Let $A/\mathbb{F}_q$ be a simple abelian variety, and π_A be its Frobenius endomorphism with the characteristic polynomial $h_A(X)$. Then*
(1) $h_A(X) = m_A(X)^e$ where $e \in \mathbb{N}$ and $m_A(X) \in \mathbb{Z}[X]$ is monic irreducible,
(2) $\mathrm{End}^0(\mathrm{A})$ *is a division algebra with center $\mathbb{Q}(\pi_A)$, and*
(3) $[\mathrm{End}^0(\mathrm{A}) : \mathbb{Q}] = \mathrm{e}^2[\mathbb{Q}(\pi_\mathrm{A}) : \mathbb{Q}]$, *and* $2\mathrm{dim}(\mathrm{A}) = \mathrm{e}[\mathbb{Q}(\pi_\mathrm{A}) : \mathbb{Q}]$.

The following theorem is a consequence of Theorem 2.1.6 and the work of Honda [24].

Theorem 2.1.8. *(Tate-Honda) Let $A/\mathbb{F}_q$ be a $\mathbb{F}_q$-simple abelian variety and $h_A(X)$ be its characteristic polynomial. The map*

$$A \mapsto \quad \textit{roots of } h_A(X) \tag{2.1.3}$$

is a bijection between the set of $\mathbb{F}_q$-isogeny classes of $\mathbb{F}_q$-simple abelian varieties $A/\mathbb{F}_q$ and the set of Galois conjugacy classes of Weil q-integers.

Next, the notions of *ordinary* and *supersingular* abelian varieties will be recalled. Let the characteristic of $\mathbb{F}$ be p. It is known that there exists an integer $0 \leq i \leq g$ such that $A[p](\overline{\mathbb{F}_q}) \simeq (\mathbb{Z}/p\mathbb{Z})^i$, where $A[p](\overline{\mathbb{F}_q}) = \ker([p])(\overline{\mathbb{F}_q})$ with $[p] : A \to A$ being the multiplication by $[p]$ map ([41] page 64). An abelian variety $A/\mathbb{F}_q$ is said to be *ordinary* if $A[p](\overline{\mathbb{F}_q}) \simeq (\mathbb{Z}/p\mathbb{Z})^g$ ([48] page 62). It is said to be *supersingular* if $A \otimes \overline{\mathbb{F}}_q \sim E^g$ where $E/\overline{\mathbb{F}}_q$ is some non-ordinary elliptic curve. The notion of *ordinary curve* and *supersingular curve* $C/\mathbb{F}_q$ is defined similarly; namely, $C/\mathbb{F}_q$ is an ordinary curve or a supersingular curve if its Jacobain variety J_C is ordinary or supersingular.

Let s_A denote the coefficient of X^g in $h_A(X)$. Deligne [10], §2 points out that $A/\mathbb{F}_q$ is ordinary if and only if $\gcd(s_A, q) = 1$. Let tr_A denote the trace of π_A. If $A/\mathbb{F}_q$ is ordinary, then it was shown on page 2367 of Howe [26] that $h_A(X)$ is of the form

$$h_A(X) = X^{2g} + a_1X^{2g-1} + ... + a_{g-1}X^{g+1} + s_AX^g + a_{g-1}qX^{g-1} + ... + a_1q^{g-1}X + q^g, \tag{2.1.4}$$

where $\gcd(s_A, q) = 1$. (Recall that $a_1 = -tr_A$.) Also, it is known that when $A/\mathbb{F}_q$ is any abelian surface, namely $g = 2$, then its characteristic polynomial has similar symmetric property as above, that is,

$$\begin{aligned} h_A(X) &= X^4 - tr_AX^3 + s_AX^2 - tr_AX + q^2 \\ &= (X - \alpha_1)(X - \alpha_2)\left(X - \tfrac{q}{\alpha_1}\right)\left(X - \tfrac{q}{\alpha_2}\right), \end{aligned} \tag{2.1.5}$$

where $\alpha_1, \alpha_2 \in \mathbb{C}$ with $\alpha_i \neq \frac{q}{\alpha_i} = \overline{\alpha_i}$ for $i = 1, 2$. Thus, by Tate's theorem the isogeny class of $A/\mathbb{F}_q$ is characterized by the pair (tr_A, s_A).

The following is the ordinary version of Tate-Honda correspondence which is taken from page 2366 of Howe [26].

Theorem 2.1.9. *The map (2.1.3) induces a bijection between the $\mathbb{F}_q$-isogeny classes of ordinary abelian varieties and Weil polynomials $h_A(X)$ of the form given in (2.1.4) with* $\gcd(s_A, q) = 1$.

Remark 2.1.10. A Weil polynomial is a monic integer polynomial whose roots are all Weil numbers.

It will be the interest of Chapters 4 and 5 of this thesis to construct the characteristic polynomials $h_A(X)$ of isogeny classes of ordinary abelian surfaces $A/\mathbb{F}_q$ where $A/\mathbb{F}_q$ satisfies special properties and furthermore is isogenous to some Jacobian varieties of smooth curves $C/\mathbb{F}_q$.

2.2 Application to pairing-based cryptography

In order to introduce the notion of pairing-based cryptography, we first introduce two bilinear pairing maps. Let $C/\mathbb{F}_q$ be a nonsingular projective curve of genus g_C. Let r be a prime coprime to q such that $r|\#J_C(\mathbb{F}_q)$ and $k \in \mathbb{N}$ such that $ord_{\mathbb{F}_r^\times}(q) = k$. The subgroup of r-th roots of unity of $\mathbb{F}_{q^k}^\times$ is denoted by $\mu_r = \{z \in \mathbb{F}_{q^k}^\times | z^r = 1\}$. The first commonly used bilinear pairing map in cryptographic protocols is the following non-degenerate *Weil pairing* [**?**, 49]

$$J_C[r](\overline{\mathbb{F}_q}) \times J_C[r](\overline{\mathbb{F}_q}) \to \mu_r.$$

The second commonly used bilinear map is the following non-degenerate *Tate-Lichtenbaum pairing* [16]

$$J_C[r](\mathbb{F}_{q^k}) \times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r.$$

For cryptographic applications, it is preferable to work with unique representatives of the algebraic objects rather than with their equivalence classes. To achieve this, two simplifications for the Tate-Lichtenbaum pairing will be needed [19]. First, if we assume that $J_C(\mathbb{F}_{q^k})$ contains no elements of order r^2, then $J_C(\mathbb{F}_{q^k})\ /rJ_C(\mathbb{F}_{q^k})$ can be identified with $J_C[r](\mathbb{F}_{q^k})$. Second, we can map the image of Tate-Lichtenbaum pairing into μ_r by raising to the power of $(q^k - 1)/r$. With these simplifications, the pairing arguments and the values of the Tate-Lichtenbaum pairing, like the Weil pairing, will be given by points and finite field elements instead of equivalence classes. The Tate-Lichtenbaum pairing with these simplifications are called the *reduced Tate-Lichtenbaum pairing*.

In 2000, Joux [27] discovered that both the Weil and the reduced Tate-Lichtenbaum pairings can be used for the construction of cryptographic protocols. Using Joux's

protocol, it is possible for three parties to share a common key in only a single round of communication, where all previous known protocols take at least two rounds of communication. Another major application of these bilinear pairings is the short signature schemes due to Boneh, Lynn, and Shacham [4]. Compared to previously known signature scheme, their signature scheme produces shorter signatures, while providing a similar level of security. Since then, there has been a flurry of activity in the design and analysis of cryptographic protocols using the Weil and reduced Tate-Lichtenbaum pairing. The term *pairing-based cryptography* is then used to describe crytographic protocols that use these two non-degenerated bilinear pairings or in general other bilinear pairing maps.

For the cryptographic schemes in pairing-based cryptography to be both secure and efficient, there are certain criteria which the parameters k, r, and q associated with the Jacobain variety $J_C/\mathbb{F}_q$ of $C/\mathbb{F}_q$ mentioned above must satisfy. The rest of this section is devoted to introduce these criteria. We begin with the following definition for general abelian varieties.

Definition 2.2.1. Let $A/\mathbb{F}_q$ be an abelian variety. Let r be a prime such that $\gcd(r, q) = 1$. An abelian variety $A/\mathbb{F}_q$ is said to have *embedding degree* $k \in \mathbb{N}$ *with respect to* r if

(1) $ord_{\mathbb{F}_r^\times}(q) = k$ and

(2) $r|\#A(\mathbb{F}_q)$.

Similarly, given a prime r and an algebraic curve $C/\mathbb{F}_q$ where $\gcd(r, q) = 1$, then $C/\mathbb{F}_q$ *has embedding degree* $k \in \mathbb{N}$ *with respect to* r if and only if $J_C/\mathbb{F}_q$ does.

Due to the following elementary fact about the kth cyclotomic polynomial $\Phi_k(X)$ ([34], page 62), the condition (1) in the above definition is equivalent to $\Phi_k(q) \equiv 0$

$(\text{mod } r)$.

Proposition 2.2.2. *Let r be a prime, $k \in \mathbb{N}$ such that $r \nmid k$, and $a \in \mathbb{Z}$. Then $\Phi_k(a) \equiv 0 \pmod{r}$ if and only if $ord_{\mathbb{F}_r^*}(a) = k$.*

Together with the property of $h_A(X)$ stated in (1) of Theorem 2.1.5 and the above proposition, the proof of part (a) of the following theorem is clear, while that of part (b) of the following theorem is not so trivial, which is due to Freeman [11].

Proposition 2.2.3. *Let $A/\mathbb{F}_q$ be an abelian variety and $h_A(X) \in \mathbb{Z}[X]$ be its characteristic polynomial. Let $r \nmid q$ be a prime number and k a positive integer such that $r \nmid k$.*

(a) A has embedding degree k with respect to r if and only if

$$h_A(1) \equiv 0 \pmod{r}, \quad \text{and} \quad \Phi_k(q) \equiv 0 \pmod{r}.$$

(b) If $k > 1$ then $A(\mathbb{F}_{q^k})$ contains two linearly independent r-torsion points.

Observe that if the hypotheses of Proposition 2.2.3 hold, and if dim $A = 1$, namely if A is an elliptic curve, then, since $A[r](\overline{\mathbb{F}_q})$ is known to be a two-dimensional $\mathbb{F}_r$-vector space ([41], page 64), we must have $A[r](\overline{\mathbb{F}_q}) \subseteq A(\mathbb{F}_{q^k})$, where k is the embedding degree defined above. However, if dim $A > 1$, then in general $A[r](\overline{\mathbb{F}_q}) \simeq (\mathbb{Z}/r\mathbb{Z})^{2g}$ ([41], page 64) will not be contained in $A(\mathbb{F}_{q^k})$ where $g = \dim(A)$. On the other hand, if the embedding degree of A with respect to a prime r is 1 and if dim $A = 1$, then it is still possible that $A[r](\overline{\mathbb{F}_q}) \not\subseteq A(\mathbb{F}_q)$. The following is an example of this.

Example 2.2.4. Consider the curve given by Weierstrass equation $E/\mathbb{F}_{29} : Y^2 = X^3 + 7X + 15$. By the discriminant formula ([46], page 45) we have $\Delta_E = 9$, thus $E/\mathbb{F}_{29}$ is an elliptic curve. A naive point counting algorithm shows that $\#E(\mathbb{F}_{29}) = 28$.

Note that $29 \equiv 1 \pmod 7$ and $7|28$. Thus $E/\mathbb{F}_{29}$ has embedding degree 1 with respect to 7. However, $7^2 \nmid 28$ and hence $E[7](\overline{\mathbb{F}_{29}}) \simeq (\mathbb{Z}/7\mathbb{Z})^2 \not\subseteq E(\mathbb{F}_{29})$.

Clearly, the condition (2) of Definition 2.2.1 implies that $A(\mathbb{F}_q)$ contains a cyclic subgroup of order r. Due to the work of Frey and Rück [16] and Menezes, Okamoto, and Vanstone [37], a careful application of the bilinear pairing maps mentioned earlier can "embed" and transport the discrete logarithm problem (DLP) in the cyclic subgroup of order r in $E(\mathbb{F}_q)$ to the DLP in $\mathbb{F}_{q^k}^\times$ where $E/\mathbb{F}_q$ is an elliptic curve. For pairing-based cryptographic schemes to be secure, both the prime parameter r and the embedding degree $k \in \mathbb{N}$ need to be chosen sufficiently large so that the DLP in the cyclic subgroup of order r in $A(\mathbb{F}_q)$ is resistant to generic attacks like the Pollard-ρ method ([36] §3.6.3) and so that the DLP in $\mathbb{F}_{q^k}^\times$ can withstand the index-calculus attack, which is considered the best known attack for the DLP in $\mathbb{F}_q^\times$ ([36] §3.6.5). On the other hand, it is also important to choose $k \in \mathbb{N}$ small enough so that the implementation of pairings is efficient.

There has been much speculation ([14], page 2) about the exact sizes of r and q^k required for cryptosystems of various security levels, and the problem is also complicated by the fact that the effectiveness of index-calculus attacks is not yet fully understood, especially over extension fields. The following definition is based on the parameter recommendations suggested by Freeman, Scott, and Teske [14] (page 2) and Galbraith, Hess, and Vercauteren [19] (page 9).

Definition 2.2.5. A g-dimensional abelian variety $A/\mathbb{F}_q$ is called *pairing-friendly* if there is a prime r such that $r|\#A(\mathbb{F}_q)$ with $\log_2(r) \geq 160$, and the embedding degree k with respect to r is such that $2 \leq k \leq 30g$. Similarly, an algebraic curve $C/\mathbb{F}_q$ of genus g_C is said to be pairing-friendly if and only if its g-dimensional Jacobian variety

$J_C/\mathbb{F}_q$ is.

The parameter ranges of $\log_2(r) \geq 160$ and $2 \leq k \leq 30g$ in the above definition are currently believed to be the range such that the DLP in both $A[r](\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^{\times}$ are computationally infeasible under the attacks like Pollard-ρ method and index-calculus [32, 14, 15, 45]. In general the embedding degree k with respect to a large prime divisor r of $\#A(\mathbb{F}_q)$ will usually be of the same size as r ([15], page 2). It is an active area of research for pairing-based cryptographers to construct pairing-friendly algebraic curves $C/\mathbb{F}_q$ with prescribed embedding degrees satisfying the range given in Definition 2.2.5.

In [20], Gaudry developed a version of the index-calculus attack which may be applied to solve the DLP in $J_C[r](\mathbb{F}_q)$ faster than the Pollard-ρ method if $g_C > 3$. More recent developments based on the work of Theriault [47], Nagao [42], and Gaudry and Thomé [21] even suggested that, for curves of genus three, the index-calculus attacks might lead to security decrease. This leads to the candidates of algebraic curves $C/\mathbb{F}_q$ with genus one or two. On the other hand, due to the fact that in the supersingular case there exist the known upper bounds $k \leq 6$ and $k \leq 12$ on the embedding degree for elliptic curves defined over finite fields [37] and for genus two curves defined over finite fields [17], respectively, cryptographers often avoid using supersingular curves with genus one or two. As a consequence, non-supersingular curves of genus one and two over finite fields become better curve candidates in pairing-based cryptography.

The following is another important parameter crucial to pairing-based cryptography.

Definition 2.2.6. Let $A/\mathbb{F}_q$ be a g-dimensonal abelian variety. Suppose r is a prime

number such that $r|\#A(\mathbb{F}_q)$. The *ρ-value of $A/\mathbb{F}_q$ with respect to r* is defined to be

$$\rho(A(\mathbb{F}_q)) = \frac{g \log q}{\log r}.$$

Similarly, an algebraic curve $C/\mathbb{F}_q$ of genus g_C is said to have ρ-value with respect to a prime r equal to $\beta \in \mathbb{R}$ if and only if $J_C/\mathbb{F}_q$ has ρ-value with respect to r equal to β.

In cryptographic terms, the ρ-value measures the ratio of a pairing-based cryptosystem's required bandwidth to its security level. From Theorem 2.1.5, it follows that $\#A(\mathbb{F}_q) \approx q^g$, and hence the definition of ρ-value implies that the theoretical minimum is $\rho \approx 1$. For pairing-based cryptosystems to be efficient, it is desirable for the underlying pairing-friendly abelian varieties $A/\mathbb{F}_q$ to have ρ-values as close to 1 as possible. Hence, for both security and efficiency concerns, pairing-based cryptographers are particularly interested in constructing ordinary pairing-friendly algebraic curves $C/\mathbb{F}_q$ of genus one or two with small ρ-values and with various prescribed small embedding degrees satisfying $2 \leq k \leq 30 \cdot g_C$.

In the literature, there already exist efficient constructions of pairing-friendly ordinary elliptic curves over finite fields (i.e. genus one) with ρ-values close to 1, and with various prescribed small embedding degrees [14]. As for genus two curves, the construction of pairing-friendly curves $C/\mathbb{F}_q$ with small ρ-values and various prescribed small embedding degrees is still not as well developed as for elliptic curves.

Freeman [11] found pairing-friendly ordinary curves of genus two over large prime fields whose Jacobian is absolutely simple and has ρ-value approximately 8 with $2 \leq k \leq 5$. Later Freeman [12] was able to reduce the ρ-value down to around 4 with $5 \leq k \leq 16$.

Hitt [23] gave a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of pairing-friendly genus 2 non-ordinary and non-supersingular curves defined over $\mathbb{F}_q$ where $q = 2^m$. In the same paper, Hitt showed that this family of curves have ρ-values between 1 and 2. The main drawback of Hitt's method is the lack of an efficient and systematic way of determining the explicit coefficients of a curve when given the parameter (tr_A, s_A) that distinguish the isogeny class of its Jacobian. Hence her method did not lead to any cryptographic examples of pairing-friendly genus 2 non-ordinary and non-supersingular curves.

Kawazoe and Takahashi [32] found pairing-friendly ordinary genus two curves of the form $Y^2 = X^5 + uX$ with ρ-value approximately 4 with $13 \leq k \leq 32$, and one curve attained ρ-value 2.975 with $k = 24$. Recently Freeman and Satoh considered ordinary genus two curves of types

$$C/\mathbb{F}_q : \ Y^2 = X^5 + uX^3 + vX, \tag{2.2.6}$$

which is a generalization of the curves considered by Kawazoe and Takahashi, and the ρ-value obtained is generally around 4 with $8 \leq k \leq 20$, and they obtained a curve with ρ-value 2.214 and $k = 27$ [13]. Freeman and Satoh [13] also considered pairing-friendly ordinary genus two curves of type

$$C/\mathbb{F}_q : \ Y^2 = X^6 + uX^3 + v, \tag{2.2.7}$$

and they found examples of such curves with general ρ-value around 4 for $6 \leq k \leq 15$ [13]. Both types of curves considered by Freeman and Satoh above have the property that the Jacobians are simple over $\mathbb{F}_q$ but not absolutely simple. This leads to an interesting question about the existence and classification up to isogeny of non-supersingular abelian surface $A/\mathbb{F}_q$ that are simple over $\mathbb{F}_q$ but not absolutely simple, which is the main theme of the next section.

2.3 Simple geometrically split abelian surfaces over finite fields

As was mentioned at the end of previous subsection, the pairing-friendly genus two curves considered by Freeman and Satoh which obtained lowest existing ρ-values have the property that their Jacobians are simple over the ground fields but not absolutely simple. The Jacobians of these curves are examples of simple geometrically split non-supersingular abelian surfaces defined over finite fields. It is then natural to seek existence criteria for such abelian surfaces and their classifications. More precisely, in this section we are interested in the existence and classification up to isogeny of non-supersingular $\mathbb{F}_q$-simple abelian surfaces $A/\mathbb{F}_q$ which are not absolutely simple, namely $A \otimes \overline{\mathbb{F}_q}$ splits into a product of elliptic curves.

The classification of such $\mathbb{F}_q$-simple ordinary abelian surfaces was mostly done by Howe and Zhu [25] and in general by Maisner and Nart [35]. Their results were reproved and compactly reformulated in section 2 of [7]. The existence of such $\mathbb{F}_q$-simple abelian surfaces $A/\mathbb{F}_q$ was addressed in section 3 of [7]. In what follows, the results from [7] will be summarized.

The following result, which is Theorem 3 of [7], is the first step toward the classification of non-supersingular $\mathbb{F}_q$-simple abelian surfaces $A/\mathbb{F}_q$ which are geometrically split.

Theorem 2.3.1. *Let $A/\mathbb{F}_q$ be a simple, non-supersingular abelian surface such that $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \sim E_1 \times E_2$ for some integer $n > 1$ and some elliptic curves $E_i/\mathbb{F}_{q^n}$, where $i = 1, 2$. Then*

(a) A, E_1, and E_2 are ordinary, and $E_1 \sim E_2$,

(b) $h_A(X)$ is irreducible over $\mathbb{Q}$ and $K := \mathbb{Q}[X]/(h_A(X))$ is a biquadratic extension of $\mathbb{Q}$,

i.e. $K/\mathbb{Q}$ is Galois with $Gal(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and

(c) if n is minimal, then $n = 2, 3, 4$ or 6.

Since it will help to illuminate the fundamental ideas in this section, a sketch of the proof as given in [7] is provided here.

Proof. (Sketch).

(a) This is verified by examining the structure of the endomorphism algebra $\mathrm{End}^0(A \otimes \mathbb{F}_{q^n})$. It then can be deduced that $E_1 \sim E_2$ and $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \sim E_1^2$ is ordinary and that this is the only possibility of splitting.

(b) The first half of the statement follows from the fact that $A/\mathbb{F}_q$ is simple and ordinary (by part (a)). To examine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, let $A_n := A \otimes \mathbb{F}_{q^n}$ and observe that

$$\begin{aligned} h_{A_n}(X) &= X^4 - tr_{A_n}X^3 + s_{A_n}X^2 - tr_{A_n}qX + q^2 \\ &= (X - \alpha_1^n)(X - \alpha_2^n)\left(X - \tfrac{q^n}{\alpha_1^n}\right)\left(X - \tfrac{q^n}{\alpha_2^n}\right) \\ &= h_E(X)^2, \end{aligned} \tag{2.3.8}$$

where $\alpha_i^n \neq \frac{q^n}{\alpha_i^n}$ and $E \sim E_i$ over $\mathbb{F}_{q^n}$ for $i = 1, 2$. Since E is ordinary and $\pi_{E\times E} = \pi_{A_n} = \pi_A^n$, and since π_E and $\pi_{E\times E}$ have the same minimal polynomial, it follow that

$$K_E := \mathbb{Q}(\pi_A^n) \tag{2.3.9}$$

is an imaginary quadratic field. On the other hand, since $A/\mathbb{F}_q$ is simple and ordinary, it can be checked that $\Delta_A := tr_A^2 - 4s_A + 8q \notin \mathbb{Z}^2$ and

$$K_0 := \mathbb{Q}(\Delta_A) \tag{2.3.10}$$

is the maximal real subfield of K. Thus, K has two distinct quadratic subfields and

so it follows that $K/\mathbb{Q}$ is biquadratic.

(c) Since $\alpha_i^n \neq \frac{q^n}{\alpha_i^n}$ (by the proof of part (b)), it may be assumed that $\alpha_1^n = \alpha_2^n$ and hence

$$\zeta_n = \frac{\alpha_1}{\alpha_2} \in K. \tag{2.3.11}$$

It then follows that $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq 2$ and hence $n = 2, 3, 4, 6$, which proves the desired statement. □

Remark 2.3.2. (1) Note that if $\eta \in \mathrm{Gal}(K/\mathbb{Q})$ denotes the automorphism induced by complex conjugation, then its fixed field is $K^\eta = K_0$. If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the unique automorphism such that $\sigma(\alpha_1) = \alpha_2$, and if $n > 2$, then the third quadratic subfield of K is

$$K^{\sigma\eta} = \mathbb{Q}(\zeta_n). \tag{2.3.12}$$

(2) If $n = 3$ or 6 , then $K_E \neq \mathbb{Q}(\zeta_3)$ and similarly, if $n = 4$, then $K_E \neq \mathbb{Q}(i)$. The former case implies that $E \not\sim E_0$ for any elliptic curve with $j(E_0) = 0$, whereas in the latter case we have that $E \not\sim E_0$ for any elliptic curve with $j(E_0) = 1728$.

Recall from p.13 that the coefficient pair (tr_A, s_A) of the characteristic polynomial $h_A(X)$ characterizes the isogeny class of an abelian surface $A/\mathbb{F}_q$. It is then clear from equation (2.3.8) that to address the classification (up to isogeny) of $\mathbb{F}_q$-simple ordinary abelian surfaces $A/\mathbb{F}_q$ that are geometrically split, it suffices to investigate the explicit conditions on which the coefficient pair (tr_A, s_A) of $h_A(X)$ may have. The following theorem is Theorem 1 from [7].

Theorem 2.3.3. *Let $A/\mathbb{F}_q$ be a simple, non-supersingular abelian surface. Then $A \otimes \mathbb{F}_{q^n}$ splits for some $n > 1$ if and only if A is ordinary and if there is an integer c*

such that

$$tr_A^2 = c(s_A - cq + 2q) \tag{2.3.13}$$

with $0 \leq c \leq 3$. *If this is the case, then* $A \otimes \mathbb{F}_{q^n} \sim E^2$ *for some elliptic curve* $E/\mathbb{F}_{q^n}$, *where* $n = c + 2$ *for* $c < 3$ *and* $n = 6$ *for* $c = 3$. *Moreover,* n *is minimal in the sense that* $A \otimes \mathbb{F}_{q^m}$ *is simple for all* $m|n$, $m \neq n$.

In the proof of Theorem 2.3.3 in [7], the relation (2.3.13) is obtained by applying Newton's formula to $h_A(X)$ and studying the connections between the coefficient pair (tr_A, s_A) and the coefficient pair (tr_{A_n}, s_{A_n}) with $n = 2, 3, 4$, or 6 respectively.

To address the existence up to isogeny of simple abelian surfaces $A/\mathbb{F}_q$ that are not absolutely simple, we will need to work with quartic polynomials of a certain type. Let $h(X)$ be quartic polynomial of the form

$$h(X) = X^4 - tX^3 + sX^2 - tqX + q^2 \in \mathbb{Z}[X], \tag{2.3.14}$$

where q is some prime power. The next result gives the relations on the coefficients $s, t \in \mathbb{Z}$ so that the given polynomial $h(X)$ is indeed the characteristic polynomial of some $\mathbb{F}_q$-simple ordinary abelian surface $A/\mathbb{F}_q$ which splits over $\mathbb{F}_{q^n}$ but not over $\mathbb{F}_{q^m}$, where $n = 2, 3, 4$ or 6, respectively, and $m|n$ with $m \neq n$. Furthermore, the relations on the integer coefficients this result gives is complete. This result is Theorem 2 of [7].

Theorem 2.3.4. *(a) Let* $s \in \mathbb{Z}$. *Then there is a simple, ordinary abelian surface* $A/\mathbb{F}_q$ *with* $s_A = s$ *such that* $A \otimes \mathbb{F}_{q^2}$ *splits if and only if*

$$|s| \leq 2q, \quad \gcd(s, q) = 1, \quad \textit{and} \quad 2q - s \neq x^2, \quad \forall x \in \mathbb{Z}. \tag{2.3.15}$$

If these conditions hold, then we have that

$$h_A(X) = X^4 + sX^2 + q^2. \tag{2.3.16}$$

(b) Let $n = 3, 4$ *or* 6 *and put* $c = \lfloor \frac{n}{2} \rfloor$. *If* $t \in \mathbb{Z}$, *then there is a simple, ordinary abelian surface* $A/\mathbb{F}_q$ *with* $tr_A = t$ *such that* $A \otimes \mathbb{F}_{q^n}$ *splits (but* $A \otimes \mathbb{F}_{q^m}$ *is simple for* $m|n$, $m \neq n$*) if and only if*

$$t^2 \leq 4cq, \quad \gcd(t, q) = 1, \quad c|t, \quad \textit{and} \quad 4cq - t^2 \neq \epsilon x^2, \quad \forall x \in \mathbb{Z}, \tag{2.3.17}$$

where $\epsilon = 1$ *if* $n = 4$ *and* $\epsilon = 3$ *otherwise. If these conditions hold, then*

$$h_A(X) = X^4 - tX^3 + \left(\frac{t^2}{c} + (c-2)q\right) X^2 - tqX + q^2. \tag{2.3.18}$$

(c) If $A/\mathbb{F}_q$ *is any simple, non-supersingular abelian surface which is geometrically split, then it is one of the surfaces listed in part (a) and (b).*

A second *existence question* which was addressed in [7] is the following. For which ordinary elliptic curves $E/\mathbb{F}_{q^n}$ with $n \in \{2, 3, 4, 6\}$, does there exist a $\mathbb{F}_q$-simple abelian surface $A/\mathbb{F}_q$ such that $A \otimes \mathbb{F}_{q^n} \sim E^2$? For $n = 2$, the answer to this question is related to whether or not $2q + tr_E$ is a square in $\mathbb{Z}$. To state the result for $n > 2$, let

$$E^\chi/\mathbb{F}_{q^n}$$

denote the unique (up to isomorphism) nontrivial *quadratic twist* of $E/\mathbb{F}_{q^n}$ ([46], page 343). For $n = 3, 4, 6$ the answer to this question is then related to whether or not there exists an elliptic curve $E_0/\mathbb{F}_{q^d}$ such that $E_0 \otimes \mathbb{F}_{q^n} \sim E^\chi$ where $d = \lfloor \frac{n+2}{3} \rfloor$. The answer to this second existence question is given by the following theorem which is Theorem 20 of [7].

Theorem 2.3.5. *(a) If* $E/\mathbb{F}_{q^2}$ *is an ordinary elliptic curve, then there exists an*

abelian surface $A/\mathbb{F}_q$ such that $A \otimes \mathbb{F}_{q^2} \sim E^2$. Moreover, A is simple if and only if $2q+tr_E$ is not a square or, equivalently, if $E_1 \otimes \mathbb{F}_{q^2} \not\sim E$, for any elliptic curve $E_1/\mathbb{F}_q$. (b) Let $n = 3, 4,$ or 6 and put $c = \lfloor \frac{n}{2} \rfloor$ and $d = \lfloor \frac{n+2}{3} \rfloor$. If $E/\mathbb{F}_q$ is an ordinary elliptic curve, then the following conditions are equivalent:

(i) there is an abelian surface $\mathbb{A}/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^n} \sim E^2$ such that $A \otimes \mathbb{F}_{q^m}$ is simple for

all $m|n$, $m \neq n$;

(ii) there is an integer $t \in \mathbb{Z}$ such that $(4-c)(4q - \frac{t^2}{c})$ is not a square in $\mathbb{Z}$ and such that

$-tr_E = t_0^{\frac{n}{d}} - \frac{n}{d} q^k t_0^{\frac{n}{d}-2}$, where $t_0 = \frac{t^d}{c} - 2(d-1)q$;

(iii) there is an elliptic curve $E_0/\mathbb{F}_{q^d}$ with $E_0 \otimes \mathbb{F}_{q^n} \sim E^\chi$ and an integer $t \in \mathbb{Z}$ such that

$tr_{E_0} = \frac{t^d}{c} - 2(d-1)q$ but $(4-c)(4q - \frac{t^2}{c})$ is not a square in $\mathbb{Z}$.

Remark 2.3.6. In the proof of the above theorem, the existence of an abelian surface $A/\mathbb{F}_q$ such that $A \otimes \mathbb{F}_{q^n} \sim E^2$ with $n \in \{2, 3, 4, 6\}$ is given implicitly by exhibiting its characteristic polynomial $h_A(X)$. Namely, for $n = 2$, it is shown that

$$(tr_A, s_A) = (0,\ -tr_E).$$

For $n = 3, 4, 6$, we have that

$$(tr_A, s_A) = \left(t,\ \frac{t^2}{c} + (c-2)q\right), \text{ where } c = \lfloor \frac{n}{2} \rfloor.$$

The following result, which is Proposition 30 of [7], will be used in the following section.

Proposition 2.3.7. *Let $E/\mathbb{F}_{q^n}$ be an ordinary elliptic curve, where $n = 3, 4$ or 6.*

Then the equivalent conditions (i)-(iii) of Theorem 2.3.5 (b) are equivalent to condition $(iv)_n$ which is given by

$(iv)_3$ $\mathrm{End}^0(E) \not\simeq \mathbb{Q}(\sqrt{-3})$ *and* $E \sim E_1 \otimes \mathbb{F}_{q^3}$*, for some elliptic curve* $E_1/\mathbb{F}_q$*;*

$(iv)_4$ $\mathrm{End}^0(E) \not\simeq \mathbb{Q}(i)$*,* $E^\chi \sim E_0 \otimes \mathbb{F}_{q^4}$ *, for some elliptic curve* $E_0/\mathbb{F}_{q^2}$*, and* $E^2 \sim A \otimes \mathbb{F}_{q^4}$ *for some abelian surface* $A/\mathbb{F}_q$*.*

$(iv)_6$ $\mathrm{End}^0(E) \not\simeq \mathbb{Q}(\sqrt{-3})$ *and* $E \sim E_1 \otimes \mathbb{F}_{q^6}$*, for some elliptic curve* $E_1/\mathbb{F}_{q^2}$ *but* $E \not\sim E_1' \otimes \mathbb{F}_{q^6}$*, for any elliptic curve* $E_1'/\mathbb{F}_{q^3}$*, and* $E^2 \sim A \otimes \mathbb{F}_{q^6}$ *for some abelian surface* $A/\mathbb{F}_q$ *with* $tr_A \neq 0$*.*

Remark 2.3.8. For $n = 3, 6$, the $E_1/\mathbb{F}_{q^c}$ above is in fact the quadratic twist of the $E_0/\mathbb{F}_{q^c}$ in (iii) of Theorem 2.3.5, and hence $tr_{E_1} = -\frac{t^d}{c} + 2(d-1)q$. On the other hand, for $n = 4$ the $E_0/\mathbb{F}_{q^2}$ above is the same as in (iii) of Theorem 2.3.5. The $A/\mathbb{F}_q$ mentioned in $(iv)_4$ and $(iv)_6$ of Proposition 2.3.7 is indeed the $A/\mathbb{F}_q$ mentioned in (i) of Theorem 2.3.5.

Finally, we recall a result from [7] on the classification of all the abelian surfaces $B/\mathbb{F}_q$ with $B \otimes \mathbb{F}_{q^n} \sim E^2$, where $E/\mathbb{F}_{q^n}$ is as in Theorem 2.3.5. Note that for $n = 2$, this has been addressed in Theorem 2.3.5 (a) and in Theorem 2.3.4 (a). To state the result for $n = 3, 4, 6$, the notation of E^χ needs to be extended analogously to A^χ. If $A/\mathbb{F}_q$ is an abelian variety, then let

$$A^\chi/\mathbb{F}_q$$

denote *any* abelian variety such that

$$h_{A^\chi}(X) = h_A(-X).$$

Observe that $A^\chi/\mathbb{F}_q$ exists by the Honda-Tate correspondence. Unlike the notion of E^χ as an isomorphism class, here A^χ is an isogeny class. For $n = 3, 4, 6$, the following

result is Proposition 29 of [7].

Proposition 2.3.9. *Let $E/\mathbb{F}_{q^n}$ be an ordinary elliptic curve, where $n = 3, 4,$ or 6. If E satisfies the equivalent conditions of Theorem 2.3.5 (b), then there are $\lfloor \frac{n+1}{2} \rfloor$ isogeny classes of abelian surfaces $B/\mathbb{F}_q$ such that $B \otimes \mathbb{F}_{q^n} \sim E^2$. More precisely, if $A/\mathbb{F}_q$ and $E_0/\mathbb{F}_{q^d}$ satisfy the conditions (i) and (iii) of Theorem 2.3.5 (b), respectively, and if $t_0 = tr_{E_0}$ and t are as in Theorem 2.3.5 (b), then these isogeny classes are given by the following table:*

n	(tr_B, s_B)	*condition*
3	$(t, t^2 - q)$, $(-2t, t^2 + 2q)$	$t_0^3 - 3qt_0 = -tr_E$, $t = t_0$
4	$(\pm t, \frac{1}{2}t^2)$	$t_0^2 - 2q^2 = -tr_E$, $t^2 = 4q + 2t_0$
6	$(\pm t, \frac{t^2}{3} + q)$, $(0, t_0)$	$t_0^3 - 3q^2t_0 = -tr_E$, $t^2 = 12q + 6t_0$

(2.3.19)

Furthermore, B is simple except in the case that $n = 3$ and $(tr_B, s_B) = (-2t, t^2 + 2q)$.

Chapter 3

Genus two curves with geometrically split Jacobian

The purpose of this chapter is to introduce two families of genus two curves defined over finite fields, called here the Legendre-Satoh curves and the Bolza-Freeman-Satoh curves. The family of Legendre-Satoh curves has the property that their Jacobians split over a quartic extension of the ground field, while the family of Bolza-Freeman-Satoh curves has the property that their Jacobians split over a sextic extension of the ground field.

The material presented in both Section 3.1 and Section 3.2 are a summary of unpublished notes from Kani [29, 30]. In Section 3.1, the concept of subcovers and involutions will be introduced. In Section 3.2, some splitting criteria for the Jacobian J_C of a projective, smooth, and geometrically irreducible curve C/K will be introduced where K is a perfect field. In Section 3.3, the family of Legendre-Satoh curves will be introduced. In Section 3.4, the family of Bolza-Freeman-Satoh curves will be introduced.

The new results in this Chapter are the proof of Theorem 3.3.1, part (b) of Theorem 3.4.1, Corollary 3.4.3, and Corollary 3.4.6.

3.1 Subcovers and involutions

By a *curve over* K we will always mean projective, smooth, and geometrically irreducible K-variety of dimension one. In this section, let K be a perfect field and C/K be a curve with genus g_C. Its function field $K(C)$ is then a finitely generated, regular extension of K of transcendence degree one. Recall from page 20 of Silverman [46] that if $\varphi : C \to E$ is a non-constant morphism map over K where E/K is also a curve, then it induces an injection $\varphi^* : K(E) \hookrightarrow K(C)$ of the respective function fields such that φ^* fixes K. The following theorem is from Silverman [46] (page 20).

Theorem 3.1.1. *Let C/K and E/K be curves.*
(a) Let $\varphi : C \to E$ be a non-constant map defined over K. Then $[K(C) : \varphi^* K(E)] < \infty$.
(b) Let $\iota : K(E) \hookrightarrow K(C)$ be an injection of function fields fixing K. Then there exists a unique non-constant map $f : C \to E$ defined over K such that $\varphi^* = \iota$.
(c) Let $\mathbb{F} \subset K(C)$ be a subfield of finite index containing K. Then there exists a smooth curve E/K, unique up to K-isomorphism, and a non-constant map $\varphi : C \to E$ defined over K such that $\varphi^* K(E) = \mathbb{F}$.

Parts (b) and (c) of Theorem 3.1.1 above show the close connection between smooth curves over field K and their functions fields. As it was remarked in [46] (page 22), the following map is an equivalence of categories.

$$\left[\begin{array}{l}\text{Objects: smooth curves}\\ \text{ defined over } K\\ \text{Maps: non-constant, surjective}\\ \text{ morphisms defined over } K\end{array}\right] \to \left[\begin{array}{l}\text{Objects: finitely generated}\\ \text{extensions } \mathbb{F}/K \text{ of transcendence}\\ \text{degree one with } \mathbb{F}\cap\overline{K}=K\\ \text{Maps: field injections fixing } K\end{array}\right] \tag{3.1.1}$$

$$\begin{array}{rcl} C/K & \mapsto & K(C) \\ \phi : C \to E & \mapsto & \phi^* : K(E) \to K(C). \end{array} \tag{3.1.2}$$

The following definition of a subcover of a curve C/K is needed for the subsequent discussion.

Definition 3.1.2. A *subcover* of a curve C/K is a non-constant morphism $\phi : C \to E$ where E/K is some curve. Two covers $\varphi_i : C \to E_i$ of C are *equivalent* if there exists an isomorphism $\psi : E_1 \to E_2$ such that $\varphi_2 = \psi \circ \varphi_1$.

From the map indicated in (3.1.2), it induces a bijection between:

$$\begin{array}{l}\text{(i) the set of equivalence classes of subcovers of } C.\\ \text{(ii) the set of subfields } \mathbb{F} \subseteq K(C) \text{ with } K \subset \mathbb{F}.\end{array} \tag{3.1.3}$$

If we consider the automorphism group $\mathrm{Aut}(C)$ of C/K, then by Theorem 3.1.1 the map $\phi \mapsto \phi_* := (\phi^*)^{-1}$ induces the following isomorphism of groups:

$$\alpha_C : \mathrm{Aut}(C) \tilde{\to} \mathrm{Aut}(K(C)),$$

where the latter group is the group of field automorphisms of the function field $K(C)$ which are trivial on K. Furthermore, if $\varphi : C \to E$ is any subcover, then the map α_C above restricts to an isomorphism

$$\alpha_{C,\varphi} : \mathrm{Aut}_C(\varphi) \to \mathrm{Aut}_{K(E)}(K(C)), \tag{3.1.4}$$

where $\mathrm{Aut}_C(\varphi) := \{\sigma \in \mathrm{Aut}(C) : \varphi \circ \sigma = \varphi\} \subseteq \mathrm{Aut}(C)$ and $K(E)$ is the function

field of E/K.

Recall from page 20 of [46] that if $\phi : C \to E$ is a morphism of curves then ϕ is either constant or surjective. The following definition is motivated by part (a) of Theorem 3.1.1 which associates the notion of *degree* to a morphism map between curves and defines the notion of *Galois subcover*.

Definition 3.1.3. Let $\phi : C \to E$ be a morphism of curves defined over K. If ϕ is constant, then the *degree of* ϕ is defined to be 0. Otherwise, ϕ is non-constant and said to be a *finite* subcover. The *degree of the given finite subcover* ϕ is defined to be $\deg(\phi) = [K(C) : \phi^* K(E)]$. The finite subcover ϕ is said to be *separable, inseparable, and purely inseparable* if the field extension $K(C)/\phi^* K(E)$ has the corresponding properties. Furthermore, the finite subcover $\phi : C \to E$ is called *Galois* if $|\mathrm{Aut}_C(\varphi)| = \deg(\varphi)$.

It follows from the bijection (3.1.3), the map (3.1.4), and Galois theory that the rule $\varphi \mapsto \alpha_{C,\varphi}(\mathrm{Aut}_C(\varphi))$ defines a bijection between:

$$\begin{aligned} &\text{(i) the set of equivalence classes of Galois subcovers of } C, \\ &\text{(ii) the set of finite subgroups of } \mathrm{Aut}(K(C)). \end{aligned} \tag{3.1.5}$$

Of all the automorphisms of C/K, those automorphisms that have order two under composition in $\mathrm{Aut}(C)$ will be our main interest.

Definition 3.1.4. An involution on a curve C/K is an element $\sigma \in \mathrm{Aut}(C)$ of order two under composition, and the set of involutions in $\mathrm{Aut}(C)$ is denoted by $\mathrm{Inv}(C)$.

Note that since every separable subcover of degree two is automatically Galois,

the following bijection follows from the bijection indicated in (3.1.5).

(i) the set $\mathrm{Inv}(C)$ of involutions of C;

(ii) the set of equivalent classes of separable subcovers of C of degree two;

(iii) the set of subfields $K \subseteq \mathbb{F} \subseteq K(C)$ with $[K(C) : \mathbb{F}] = 2$.

(3.1.6)

Next we introduce the notion of a hyperelliptic curve.

Definition 3.1.5. A nonsingular curve C/K of genus $g_C > 1$ is called a *hyperelliptic curve* if there exists a subcover $\pi : C \to Y$ of degree 2 where Y/K is a complete, smooth, and geometrically irreducible curve with genus $g_Y = 0$.

It follows from (3.1.6) and the definition above that C/K is a hyperelliptic curve if and only if there exists a $\omega_C \in \mathrm{Inv}(C)$ such that the genus $g_{C/\langle\omega_C\rangle}$ of the quotient curve $C/\langle\omega_C\rangle$ equals zero. Furthermore, if this is the case, then Proposition 5.3 in §IV of [22] says that this involution ω_C is unique. This involution is commonly known as the *hyperelliptic involution*, and the subcover π stated in Definition 3.1.5 is called *hyperelliptic subcover*. Note that the hyperelliptic involution commutes with all the elements in $\mathrm{Aut}(C)$. Indeed, if C/K is a hyperelliptic curve with hyperelliptic involution ω_C, then we can consider $\omega := \sigma^{-1} \circ \omega_C \circ \sigma$ for $\sigma \in \mathrm{Aut}(C)$. Thus $\omega \in \mathrm{Inv}(C)$ and σ induces an isomorphism $C/\langle\omega\rangle \simeq C/\langle\omega_C\rangle$. It follows from the definition of hyperelliptic curve and the uniquness of hyperelliptic involution that $g_{C/\langle\omega\rangle} = g_{C/\langle\omega_C\rangle} = 0$ and $\omega = \omega_C$. Thus $\sigma \circ \omega_C = \omega_C \circ \sigma$ for $\sigma \in \mathrm{Aut}(C)$.

As it was explained on page 73 and page 74 by Avanzi, Cohen, Doche, Frey, Lange, and Nguyen [1], the affine part of a hyperelliptic curve C/K can be described by the following equation:

$$C/K : \; Y^2 + h(X) \cdot Y = f(X), \tag{3.1.7}$$

where $h(X), f(X) \in K[X]$ with $\deg(h) \leq g_C + 1$ and $\deg(f) \leq 2g_C + 2$, and $f(X)$ has no repeated roots. Furthermore, if the characteristic of the field K is odd, then the transformation $Y \mapsto Y - h(X)/2$ simplifies the curve equation given by (3.1.7) to

$$C/K : \ Y^2 = f(X), \tag{3.1.8}$$

for some $f(X) \in K[X]$ (page 74, [1]). If a hyperelliptic curve is given by the equation (3.1.8), then the hyperelliptic involution is given by $(X, Y) \mapsto (X, -Y)$ [40] (page 61). We also recall the fact that if $g_C = 2$, then the curve C is hyperelliptic. From now on we will assume that the characteristic of the underlying field K is odd, and describe hyperelliptic curves C/K by their affine parts via the equation given by (3.1.8).

3.2 A splitting criterion for J_C

Once again, let K be a perfect field and C/K be a projective, smooth, and geometrically irreducible curve with genus denoted by g_C. Assume that $C(K) \neq \emptyset$. Recall from Section 2.1 the definition of the Jacobian J_C of a curve C/K as an object representing a functor. Thus, there exists a canonical isomorphism

$$\iota_C : \mathrm{Pic}^0(C) \tilde{\to} J_C(K)$$

which is compatible with base-change. If $\varphi : C \to E$ is a subcover, then by the functoriality of J_C, there is a homomorphism of abelian varieties

$$\varphi^* : J_E \to J_C \tag{3.2.9}$$

such that $\varphi^*(i_E(D)) = i_C(\varphi^*(D))$ for all divisors $D \in \mathrm{Pic}^0(E)$ where $\varphi^* D$ is the pullback of a divisor class [22] (page 137, 148). On the other hand, by the autoduality

of the Jacobian there is also a homomorphism of abelian varieties

$$\varphi_* : J_C \to J_E \tag{3.2.10}$$

such that $\varphi_*(i_C(D)) = i_E(\varphi_*(D))$ for all divisors $D \in \mathrm{Pic}^0(C)$ where $\varphi_* D$ denotes the pushforward of the divisor D ([22] page 306). Observe that $(\varphi_* \circ \varphi^*)(D) = n_\varphi D$ for all divisors D on E where $n_\varphi = \deg(\varphi)$. From this we obtain the relation

$$\varphi_* \circ \varphi^* = [n_\varphi]_{J_E} \tag{3.2.11}$$

where $[n_\varphi]_{J_E}$ is the multiplication by n_φ map on J_E. To see this, verify the relation over an algebraic closed field. Since the multiplication by n_φ map $[n_\varphi]$ on J_E is an isogeny, it follows that the map φ_* is surjective and the map φ^* has finite kernel. If we put

$$e_\varphi := \varphi^* \circ \varphi_* \in \mathrm{End}(J_C), \tag{3.2.12}$$

then it follows from (3.2.11) that we have

$$\varphi_* \circ e_\varphi = n_\varphi \circ \varphi_* \ \text{ and } \ e_\varphi \circ \varphi^* = n_\varphi \circ \varphi^*. \tag{3.2.13}$$

If C/K is a curve of genus $g_C \geq 2$ and $\varphi \in \mathrm{Aut}(C)$, then the map given in (3.2.10) plays an important role in the following lemma taken from page 5 of [29].

Lemma 3.2.1. *If C/K is a curve of genus $g_C \geq 2$, then the following canonical map*

$$\begin{array}{rccc} j_* : & \mathrm{Aut}(C) & \to & \mathrm{Aut}(J_C) \\ & \sigma & \mapsto & \sigma_* \end{array} \tag{3.2.14}$$

is injective, where σ_* is as indicated in (3.2.10).

Proof. Without loss of generality, we assume that K is algebraically closed. We note that the map $j_* : \mathrm{Aut}(C) \to \mathrm{Aut}(J_C)$ is a group homomorphism. We proceed to show that $\mathrm{Ker}(j_*) = \{\mathrm{id}_C\}$ by contradiction. Let $\sigma \in \mathrm{Ker}(j_*)$ be such that $\sigma \neq \mathrm{id}_C$.

Thus $j_*(\sigma) = \sigma_* = \mathrm{id}_{J_C}$. Since $\sigma \neq \mathrm{id}_C$, then there exists a point $P \in C$ such that $\sigma(P) \neq P$. If we choose another point $Q \in C$ such that $P \neq Q$, then $\sigma(P) \neq P, \sigma(Q)$. It follows that $\sigma(P) + Q \neq \sigma(Q) + P$, and hence the dimension of the linear system $|\sigma(Q) + P| \geq 1$. Since $g_C \geq 2$, it follows from the first part of Clifford's theorem (page 343 of [22]) that $\dim|\sigma(Q) + P| \geq 1$. Thus we must have $\dim|\sigma(Q) + P| = 1$. Then the second half of Clifford's theorem says that C must be hyperelliptic curve and hence has hyperelliptic involution ω_C. Thus we also have

$$|\sigma(Q) + P| = |\omega_C(P) + P|.$$

This is clearly a contradiction, since for any fixed point $P \in C$, $|\sigma(Q) + P|_{Q \in C(K)}$ has infinitely many distinct divisors, but $\omega_C(P) + P$ is the only divisor in the linear system $|\omega_C(P) + P|$. Thus the statement is proven. □

The lemma above plays an important role in the following splitting criterion for the Jacobian of a hyperelliptic curve.

Proposition 3.2.2. *If C/K is a hyperelliptic curve of genus $g_C \geq 2$ and $\sigma \in \mathrm{Aut}(C)$ is an automorphism such that the induced $\sigma_* \in \mathrm{Aut}(J_C)$ via the map j_* given in (3.2.14) satisfies $\sigma_* \neq [\pm 1]_{J_C}$ and $\sigma_*^2 = [1]_{J_C}$, then J_C is not K-simple.*

Proof. Let $h_1 := 1_{J_C} - \sigma_*$ and $h_2 := 1_{J_C} + \sigma_*$. By the hypothesis, we have $h_i \neq 0$ where $i = 1, 2$. Since $h_1 \circ h_2 = (1_{J_C} - \sigma_*)(1_{J_C} + \sigma_*) = 1 - \sigma_*^2 = 1_{J_C} - 1_{J_C} = 0$, it follows that h_1 is a nontrivial zero divisor of $\mathrm{End}^0(J_C)$ and hence $\mathrm{End}^0(J_C)$ is not a division algebra. By Proposition 2.1.3, we know that J_C is not K-simple. □

If a subcover $\varphi : C \to E$ is Galois, then a useful formula for the e_φ defined in

(3.2.12) is given by

$$e_\varphi = \sum_{\sigma \in \mathrm{Aut}_C(\varphi)} \sigma_*, \tag{3.2.15}$$

where $\sigma_* \in \mathrm{Aut}(J_C) \subset \mathrm{End}(J_C)$ is the automorphism induced by $\sigma \in \mathrm{Aut}(C)$ indicated in the above theorem via the map j_* (Kani, Rosen [31], page 315). Furthermore, if C/K is a hyperelliptic curve of genus $g_C \geq 2$ and $(\omega_C)_*$ is the automorphism of J_C induced by its hyperelliptic involution $\omega_C \in \mathrm{Inv}(C)$ via the map j_* given in Lemma 3.2.1, then the formula above gives a simple description of $(\omega_C)_*$.

Proposition 3.2.3. *If C/K is a hyperelliptic curve of genus $g_C \geq 2$, then the automorphism $(\omega_C)_*$ of J_C induced by the hyperelliptic involution $\omega_C \in \mathrm{Inv}(C)$ via the map j_* given in (3.2.14) has the form $(\omega_C)_* = [-1]_{J_C}$.*

Proof. Let $\pi : C \to Y$ be the hyperelliptic subcover. Since $\dim(J_Y) = g_y = 0$, we have $J_Y = 0$. Hence we have that $e_\pi = \pi^* \circ (\pi)_* = 0$. On the other hand, by the formula given in (3.2.15) we have $e_\pi = (1_C)_* + (\omega_C)_*$. Hence this implies that $(\omega_C)_* = [-1]_{J_C}$. □

Now suppose that two subcovers $\varphi_i : C \to E_i$ are given. Then there is a homomorphism

$$(\varphi_1, \varphi_2)_* := ((\varphi_1)_*, (\varphi_2)_*) : J_C \to J_{E_1} \times J_{E_2}$$

which is uniquely characterized by the condition

$$\mathrm{proj}_i \circ (\varphi_1, \varphi_2)_* = (\varphi_i)_*, \quad i = 1, 2, \tag{3.2.16}$$

where $\mathrm{proj}_i : J_{E_1} \times J_{E_2} \to J_{E_i}$ denotes the ith projection. Similarly, there is a homomorphism

$$\varphi_1^* + \varphi_2^* : J_{E_1} \times J_{E_2} \to J_C \tag{3.2.17}$$

which is uniquely characterized by the condition

$$(\varphi_1^* + \varphi_2^*) \circ e_i = \varphi_i^*, \;\; i = 1, 2, \tag{3.2.18}$$

where $e_i : J_{E_i} \hookrightarrow J_{E_1} \times J_{E_2}$ denotes the ith inclusion. By the definition of e_φ and relations (3.2.16) and (3.2.18), we have

$$e_{\varphi_i} = \varphi_i^* \circ \varphi_{i*} = (\varphi_1^* + \varphi_2^*) \circ (e_i \circ \mathrm{proj}_i) \circ (\varphi_1, \varphi_2)_*,$$

for $i = 1, 2$. Then it follows that

$$e_{\varphi_1} + e_{\varphi_2} = (\varphi_1^* + \varphi_2^*) \circ (\varphi_1, \varphi_2)_* \tag{3.2.19}$$

since $e_1 \circ \mathrm{pr}_1 + e_2 \circ \mathrm{pr}_2 = [1]_{J_{E_1} \times J_{E_2}}$. If we consider the composite

$$f := (\varphi_1, \varphi_2)_* \circ (\varphi_1^* + \varphi_2^*) \in \mathrm{End}(J_{E_1} \times J_{E_2})$$

then by relations (3.2.16) and (3.2.18) we have

$$\mathrm{pr}_i \circ f \circ e_j = (\varphi_i)_* \circ \varphi_j^*$$

for all $i, j \in \{1, 2\}$, which characterizes $f \in \mathrm{End}(J_{E_1} \times J_{E_2})$ uniquely. Observe that for any point $(D_1, D_2) \in (J_{E_1} \times J_{E_2})(\overline{K})$ we have

$$\begin{aligned} f(D_1, D_2) &= ((\varphi_1)_* \circ (\varphi_1^* + \varphi_2^*)(D_1),\ (\varphi_2)_* \circ (\varphi_1^* + \varphi_2^*)(D_2)) \\ &= (([n_{\varphi_1}] + ((\varphi_1)_* \circ \varphi_2^*))(D_1),\ ((\varphi_2)_* \circ \varphi_1^*) + [n_{\varphi_2}])(D_2)), \end{aligned}$$

where $n_{\varphi_i} = \deg(\varphi_i)$ with $i = 1, 2$. It follows that the two by two matrix representation of $f \in \mathrm{End}(J_{E_1} \times J_{E_2})$ is given by

$$\begin{pmatrix} [n_{\varphi_1}] & (\varphi_1)_* \circ \varphi_2^* \\ (\varphi_2)_* \circ \varphi_1^* & [n_{\varphi_2}] \end{pmatrix}. \tag{3.2.20}$$

Remark 3.2.4. It is clear from (3.2.20) that the two by two matrix representation of f is multiplication by n if and only if $n_{\varphi_1} = n_{\varphi_2} = n$ and $(\varphi_1)_* \circ \varphi_2^* = (\varphi_2)_* \circ \varphi_1^* = 0$.

The remark above will play an important role in the proof of the following splitting

criterion for the Jacobian of a hyperelliptic curve.

Theorem 3.2.5. *Suppose that C/K is a hyperelliptic curve of genus $g_C \geq 2$ and that there exists an involution $\sigma_1 \in \mathrm{Inv}(C)$ with $\sigma_1 \neq w_C$. Put $\sigma_2 := \sigma_1 \circ w_C$ and $E_i := C/\langle \sigma_i \rangle$ where $i = 1, 2$. Let $\varphi_i : C \to E_i$ be the associated subcovers of degree two. Then we have*

$$e_{\varphi_1} + e_{\varphi_2} = [2]_{J_C}, \;\; e_{\varphi_1} \circ e_{\varphi_2} = e_{\varphi_2} \circ e_{\varphi_1} = 0, \tag{3.2.21}$$

and hence

$$\varphi_1^* + \varphi_2^* : J_{E_1} \times J_{E_2} \to J_C, \;\; ((\varphi_1)_*, (\varphi_2)_*) : J_C \to J_{E_1} \times J_{E_2}$$

are isogenies satisfying

$$(\varphi_1^* + \varphi_2^*) \circ ((\varphi_1)_*, (\varphi_2)_*) = [2]_{J_C}, \;\; ((\varphi_1)_*, (\varphi_2)_*) \circ (\varphi_1^* + \varphi_2^*) = [2]_{J_{E_1} \times J_{E_2}}. \tag{3.2.22}$$

Proof. Let $\sigma := (\sigma_1)_* \in \mathrm{Aut}(J_C)$ where $(\sigma_1)_*$ is induced by $\sigma_1 \in \mathrm{Aut}(C)$ via the map j_* given in (3.2.14). It follows from Proposition 3.2.3 and from the definition of the map j_* that $j_*(\sigma_2) = (\sigma_2)_* = (\sigma_1 \circ \omega_C)_* = (\sigma_1)_* \circ (\omega_C)_* = \sigma \circ [-1]_{J_C} = -\sigma$. By (3.2.15), we know that

$$e_{\varphi_i} = 1 + (\sigma_i)_* = 1 + \mu_i \sigma \tag{3.2.23}$$

where $\mu_1 = 1$ and $\mu_2 = -1$. By (3.2.23) and the fact that $\sigma \in \mathrm{Inv}(C)$, we have $e_{\varphi_1} + e_{\varphi_2} = (1 + \sigma) + (1 - \sigma) = [2]_{J_C}$, and $e_{\varphi_1} \circ e_{\varphi_2} = (1 + \sigma)(1 - \sigma) = 1 - \sigma^2 = 0$. Similarly, we have $e_{\varphi_2} \circ e_{\varphi_1} = (1 - \sigma)(1 + \sigma) = \sigma^2 - 1 = 0$. This proves (3.2.21). Since $e_{\varphi_1} \circ e_{\varphi_2} = e_{\varphi_2} \circ e_{\varphi_1} = 0$, it follows that $(\varphi_1)_* \circ e_{\varphi_1} \circ e_{\varphi_2} \circ \varphi_2^* = (\varphi_2)_* \circ e_{\varphi_2} \circ e_{\varphi_1} \circ \varphi_1^* = 0$. Since $\deg(\varphi_i) = 2$, it follows from (3.2.13) that $(\varphi_1)_* \circ e_{\varphi_1} \circ e_{\varphi_2} \circ \varphi_2^* = [4](\varphi_1)_* \circ \varphi_2^*$ and $(\varphi_2)_* \circ e_{\varphi_2} \circ e_{\varphi_1} \circ \varphi_1^* = [4](\varphi_2)_* \circ \varphi_1^*$. This implies that

$$(\varphi_1)_* \circ \varphi_2^* = (\varphi_2)_* \circ \varphi_1^* = 0. \tag{3.2.24}$$

Note that the first part of (3.2.22) follows from (3.2.19) and the first part of (3.2.21). The second part of (3.2.22) follows from Remark (3.2.4) and (3.2.24). Finally, since $[2]_{J_C}$ is isogeny, it follows from (3.2.22) that $(\varphi_1^* + \varphi_2^*)$ and $((\varphi_1)_*, (\varphi_2)_*)$ are both surjective with finite kernel and hence are isogenies. □

Finally, we conclude this section with one more splitting criterion for the Jacobian of a hyperelliptic curve.

Theorem 3.2.6. *Suppose that $C/\mathbb{F}_q$ is a hyperelliptic curve of genus $g_C = 2$ such that its Jacobian $J_C/\mathbb{F}_q$ is ordinary and satisfies $J_C \otimes \overline{\mathbb{F}_q} \sim \overline{E}^2$ for some elliptic curve $\overline{E}/\overline{\mathbb{F}_q}$. Assume that there exists an automorphism $f \in \mathrm{Aut}(C)$ such that $\mathrm{ord}(f) = n \geq 3$, and $\mathrm{End}^0(\overline{E}) \not\supseteq \mathbb{Q}(\zeta_n)$ where ζ_n is the primitive nth root of unity. Let $\overline{\tau} \in \mathrm{Inv}(C \otimes \overline{\mathbb{F}_q})$ be such that $\overline{\tau} \neq w_C$. Then, J_C splits over $\mathbb{F}_q$ if and only if $\overline{\tau} = \tau \otimes \overline{\mathbb{F}_q}$, for some $\tau \in \mathrm{Aut}(C)$.*

Proof. Assume that $\overline{\tau} = \tau \otimes \overline{\mathbb{F}_q} \in \mathrm{Inv}(C \otimes \overline{\mathbb{F}_q})$ for some $\tau \in \mathrm{Aut}(C)$. By Proposition 3.2.3, the injectivity of the map j_* given by Lemma 3.2.1, and the fact that $\tau \neq \omega_C$, we have $\tau_* \neq (\omega_C)_* = [-1]_{J_C}$. On ther other hand, we have $\tau \neq 1_C$. Hence we have $\tau_* \neq [\pm 1]_{J_C}$ via the map j_* given by (3.2.14). Since $\tau_*^2 = [1]_{J_C}$ and $\tau_* \neq [\pm 1]_{J_C}$, it follows from Proposition 3.2.2 that J_C splits over $\mathbb{F}_q$.

Conversely, suppose that $J_C \sim E_1 \times E_2$ splits over $\mathbb{F}_q$. Since J_C is ordinary, it follows that E_i is also ordinary where $i = 1, 2$. Hence for $i = 1, 2$ we know that $\mathrm{End}^0(E_i)$ is a imaginary quadratic number field. Since $E_i \otimes \overline{\mathbb{F}_q} \simeq \overline{E}$, it follows that $\mathrm{End}^0(E_i) \simeq \mathrm{End}^0(\overline{E})$. Now we proceed by considering two different cases.

If $E_1 \sim E_2$, then by (2.1.2) we have $\mathrm{End}^0(J_C) \simeq M_2(\mathrm{End}^0(E_i)) \simeq M_2(\mathrm{End}^0(\overline{E}))$. Hence It follows from Proposition 13 of Kani [28] (page 14) that $\mathrm{End}(J_C) \simeq \mathrm{End}(J_C \otimes \overline{\mathbb{F}_q})$. This implies that $j_*(\overline{\tau})^\phi = (\overline{\tau})_*^\phi = (\overline{\tau})_* = j_*(\overline{\tau})$ for all $\phi \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ where the

map $j_* : \mathrm{Aut}(C \otimes \overline{\mathbb{F}_q}) \to \mathrm{Aut}(J_{C \otimes \overline{\mathbb{F}_q}})$ is given by (3.2.14). On the other hand, we have $j_*(\overline{\tau}^{\phi}) = j_*(\overline{\tau})^{\phi}$. It follows from the injectivity of the map j_* given in Lemma 3.2.1 that $\phi(\overline{\tau}) = \overline{\tau}$ for all $\phi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ and hence $\overline{\tau} = \tau \otimes \overline{\mathbb{F}_q}$ for some $\tau \in \mathrm{Aut}(C)$ as claimed.

Now suppose that $E_1 \not\sim E_2$. Then $\mathrm{End}^0(J_C) \simeq \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2) \simeq K \times K$ where $K = \mathrm{End}^0(\overline{E})$ is some imaginary quadratic number field. This implies that $f = (f_1, f_2)$ where $f_i \in K$ is some root of unity of order n_i where $i = 1, 2$ and $n = \mathrm{lcm}(n_1, n_2)$. Thus we have $n_i \in \{1, 2, 3, 4, 6\}$. If one of $n_i = 4$, then $K \simeq \mathbb{Q}(i)$, and the other n_j must be either 2 or 4 where $i, j \in \{1, 2\}$. Hence we have $n = \mathrm{lcm}(n_1, n_2) = 4$ and $K \simeq \mathrm{End}^0(\overline{E}) \simeq \mathbb{Q}(\zeta_4)$, which is a contradiction. If one of the $n_i = 3$ or 6, then $K \simeq \mathbb{Q}(\zeta_3)$ and the other n_j will have to divide 6 where $i, j \in \{1, 2\}$. It then follows that $K \simeq \mathrm{End}^0(\overline{E}) \simeq \mathbb{Q}(\zeta_n)$ where $n = \mathrm{lcm}(n_1, n_2) = 3$ or 6, which is also a contradiction. Thus we must have $n = \mathrm{lcm}(n_1, n_2)|2$ which contradicts the assumption that $n \geq 3$. We conclude that the case that $J_C \sim E_1 \times E_2$ with $E_1 \not\sim E_2$ cannot occur. This proves the statement. □

3.3 Legendre-Satoh curves

The purpose of this section is to introduce the family of genus two Legendre-Satoh curves defined over $\mathbb{F}_q$ which has the property that the Jacobians split over $\mathbb{F}_{q^4}$. In what follows, we will assume that the characteristics of $\mathbb{F}_q$ is not 2 nor 3.

The family of genus two *Legendre-Satoh curves* [43] is defined as follows:

$$C_{u,v}/\mathbb{F}_q : \; Y^2 = X^5 + uX^3 + vX, \tag{3.3.25}$$

where $u^2 - 4v \neq 0$ and $v \neq 0$. These curves were recently studied and proposed by

Satoh [43] for the purpose of hyperelliptic cryptogarphy and were called Legendre-Satoh curves in [7] for the reason which will be explained presently.

Observe that if we set the changes of variables: $x \mapsto c^{-2}x$ and $y \mapsto c^{-5}y$, then an isomorphic Legendre-Satoh curve $C_{uc^4,vc^8}/\mathbb{F}_q : Y^2 = X^5 + uc^4X^3 + vc^8X$ can be obtained. In [7] it was pointed out that if $u = -(1+v)$, then $C_{u,v}$ has the form

$$C_{(-1-v),v}/\mathbb{F}_q : Y^2 = X(X^2-1)(X^2-v)$$

which is the type of curve studied by Legendre in 1832. Note that if $c \in \mathbb{F}_{q^8}$ is such that it satisfies $c^8v + c^4u + 1 = 0$, then the family of curves $C_{(-1-v),v}$ is geometrically the same as the family of $C_{u,v}$ because of the following isomorphism

$$C_{(-1-c^8v),c^8v} \otimes \mathbb{F}_{q^8} \simeq C_{c^4v,c^8v} \otimes \mathbb{F}_{q^8} \simeq C_{u,v} \otimes \mathbb{F}_{q^8}.$$

Hence the name Legendre-Satoh curve was chosen in [7].

In what follows, $J_{u,v}$ is used to denote the Jacobian of a Legendre-Satoh curve $C_{u,v}$ defined over $\mathbb{F}_q$. Next we present a result regarding the splitting property of $J_{u,v}$ whose proof makes use the tools presented in Section 3.2.

Theorem 3.3.1. *Let $C_{u,v}/\mathbb{F}_q : Y^2 = f(X)$ be a genus two Legendre-Satoh curve defined as in (3.3.25). Fix $\sigma \in \mathbb{F}_{q^4}^{\times}$ such that $\sigma^4 = v$ and put*

$$\gamma = 2\frac{u-6\sigma^2}{u+2\sigma^2} \in \mathbb{F}_{q^2} \text{ and } \chi = \frac{u+2\sigma^2}{64\sigma^3} \in \mathbb{F}_{q^4}. \tag{3.3.26}$$

Then the curves

$$E_\chi/\mathbb{F}_{q^4} : Y^2 = \chi(X-1)(X^2-\gamma X+1) \tag{3.3.27}$$

$$E_{u,v}/\mathbb{F}_{q^2} : Y^2 = (X-1)(X^2-\gamma X+1) \tag{3.3.28}$$

are elliptic curves with j-invariant

$$j(E_\chi) = j(E_{u,v}) = 256\frac{(\gamma+1)^3}{\gamma+2}, \tag{3.3.29}$$

and E_χ is a quadratic twist of $E_{u,v} \otimes \mathbb{F}_{q^4}$. Furthermore, we also have $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_\chi^2$.

Proof. The fact that E_χ and $E_{u,v}$ are elliptic curves, that E_χ and $E_{u,v} \otimes \mathbb{F}_{q^4}$ are quadratic twists of each other, and the formulae of the j-invariants of both curves were all explained on pages 22–23 of [7]. Let $E_1 := E_\chi$ and $E_2 := E_{-\chi}$ where $E_{-\chi}/\mathbb{F}_{q^4}$ is defined as in (3.3.27) with χ being replaced by $-\chi$. We proceed to show that $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_1 \times E_2$ by first showing that there exist injections $f_i : \mathbb{F}_{q^4}(E_i) \hookrightarrow \mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4})$, where $\mathbb{F}_{q^4}(E_i)$ and $\mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4})$ are the function fields of $E_i/\mathbb{F}_{q^4}$ and $C_{u,v} \otimes \mathbb{F}_{q^4}$, respectively. Consider the two functions X and Y in the function field $\mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4})$ such that they satisfy the curve equation $Y^2 = f(X)$ and define the following functions in $\mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4})$:

$$\begin{cases} U_1 := \left(\frac{X+\sigma}{X-\sigma}\right)^2 \\ V_1 := \frac{Y}{(X-\sigma)^3} \end{cases}, \quad \begin{cases} U_2 := \left(\frac{X-\sigma}{X+\sigma}\right)^2 \\ V_2 := \frac{Y}{(X+\sigma)^3}. \end{cases}$$

Thus $\mathbb{F}_{q^4}(U_i, V_i)$ is a subfield of $\mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4})$ where $i = 1, 2$. Through a tedious computation we can verify that the elements U_i and V_i defined above satisfy the following relations in $\mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4})$:

$$\begin{aligned} V_1^2 &= \chi(U_1 - 1)(U_1^2 - \gamma U_1 + 1), \\ V_2^2 &= -\chi(U_2 - 1)(U_2^2 - \gamma U_2 + 1). \end{aligned}$$

From these relations, it follows that $\mathbb{F}_{q^4}(E_i) \simeq \mathbb{F}_{q^4}(U_i, V_i)$ and hence has the following injection

$$f_i : \mathbb{F}_{q^4}(E_i) \simeq \mathbb{F}_{q^4}(U_i, V_i) \hookrightarrow \mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4}).$$

From Proposition 3.1.1 in Section 3.1 (page 25 of [46]), we know that there exist unique non-constant morphisms

$$\begin{array}{rccc} \varphi_1 : & C_{u,v} & \to & E_1 \\ & (X, Y) & \mapsto & \left((\frac{X+\sigma}{X-\sigma})^2, \frac{Y}{(X-\sigma)^3}\right) \end{array} \qquad \begin{array}{rccc} \varphi_2 : & C_{u,v} & \to & E_2 \\ & (X, Y) & \mapsto & \left((\frac{X-\sigma}{X+\sigma})^2, \frac{Y}{(X+\sigma)^3}\right) \end{array}$$

such that $\varphi_i^* = f_i$. Since $U_1 = \left(\frac{X+\sigma}{X-\sigma}\right)^2$ and $U_2 = \left(\frac{X-\sigma}{X+\sigma}\right)^2$, by multiplying $(X-\sigma)^2$ and $(X+\sigma)^2$ to both sides of these equations respectively and grouping like terms in X we obtain the following relations

$$(U_1 - 1)X^2 - 2\sigma(U_1 + 1)X + \sigma^2(U_1 - 1) = 0 \quad (3.3.30)$$

$$(U_2 - 1)X^2 + 2\sigma(U_2 + 1)X + \sigma^2(U_2 - 1) = 0. \quad (3.3.31)$$

From these relations, it follows that

$$\deg(\varphi_i) = [\mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4}) : \mathbb{F}_{q^4}(E_i)] = [\mathbb{F}_{q^4}(X, Y) : \mathbb{F}_{q^4}(U_i, V_i)] = 2.$$

Indeed, since the definitions of U_i and V_i show that $\mathbb{F}_{q^4}(X, Y) = \mathbb{F}_{q^4}(U_i, V_i, X)$, it follows from (3.3.30) and (3.3.31) that $[\mathbb{F}_{q^4}(X, Y) : \mathbb{F}_{q^4}(U_i, V_i)] = [\mathbb{F}_{q^4}(U_i, V_i)(X) : \mathbb{F}_{q^4}(U_i, V_i)] = 1$ or 2. If it is equal to 1, then we must have $\mathbb{F}_{q^4}(X, Y) \simeq \mathbb{F}_{q^4}(U_i, V_i) \simeq \mathbb{F}_{q^4}(E_i)$, which is a contraction.

Next we proceed to find the involutions that give rise to the subcovers $\varphi_i : C_{u,v} \to E_i$. Note that the two roots of the quadratic equation given in (3.3.30) are X and $\frac{\sigma^2}{X}$, hence the non-trivial automorphism of the extension $\mathbb{F}_{q^4}(X)$ over $\mathbb{F}_{q^4}(U_1)$ is given by the map $X \mapsto \frac{\sigma^2}{X}$. By applying this map to the polynomial $f(X)$, we obtain

$$\frac{\sigma^6(v + uX^2 + X^4)}{X^5}.$$

Observe that in $\mathbb{F}_{q^4}(C \otimes \mathbb{F}_{q^4})$ we have $\frac{Y^2}{X} = v + uX^2 + X^4$, and hence we have

$$\frac{\sigma^6(v + uX^2 + X^4)}{X^5} = \left(\frac{\sigma^3 Y}{X^3}\right)^2.$$

This leads us to the choice of the map

$$s_1(X, Y) = \left(\frac{\sigma^2}{X}, -\frac{\sigma^3 Y}{X^3}\right)$$

which is an automorphism of $C_{u,v}$. Indeed, this follows from the fact that the pair $\left(\frac{\sigma^2}{X}, -\frac{\sigma^3 Y}{X^3}\right)$ satisfies the curve equation $Y^2 = f(X)$ in the function field $\mathbb{F}_{q^4}(C_{u,v} \otimes \mathbb{F}_{q^4})$.

On the other hand, observe that $s_1^2(X,Y) = s_1\left(\frac{\sigma^2}{X}, -\frac{\sigma^3 Y}{X^3}\right) = (X,Y)$, and hence it is an involution. Finally, we verify that the cover $\varphi_1 : C_{u,v} \to E_1$ is s_1-invariant

$$s_1(\varphi_1(X)) = s_1\left(\left(\tfrac{X+\sigma}{X-\sigma}\right)^2\right) = \left(\frac{\frac{\sigma^2}{X}+\sigma}{\frac{\sigma^2}{X}-\sigma}\right)^2 = \left(\tfrac{X+\sigma}{X-\sigma}\right)^2 = \varphi_1(X)$$
$$s_1(\varphi_1(Y)) = s_1\left(\tfrac{Y}{(X-\sigma)^3}\right) = \tfrac{-\sigma^3 Y}{\sigma^3(\sigma-X)^3} = \tfrac{Y}{(X-\sigma)^3} = \varphi_1(Y).$$

Thus it follows that the involution s_1 gives rise to the subcover φ_1. If we put $s_2 := s_1 \circ \omega_{C_{u,v}}$, where $\omega_{C_{u,v}}$ denotes the hyperelliptic involution of $C_{u,v}$, then clearly

$$s_2(X,Y) = \left(\frac{\sigma^2}{X}, \frac{\sigma^3 Y}{X^3}\right)$$

is an automorphism of $C_{u,v}$ and of order 2, since both s_1 and $\omega_{C_{u,v}}$ are automorphisms of $C_{u,v}$ of order 2. Furthermore, we observe that the subcover φ_2 is s_2-invariant because

$$s_2(\varphi_2(X)) = s_2\left(\left(\tfrac{X-\sigma}{X+\sigma}\right)^2\right) = \left(\frac{\frac{\sigma^2}{X}-\sigma}{\frac{\sigma^2}{X}+\sigma}\right)^2 = \left(\tfrac{X-\sigma}{X+\sigma}\right)^2 = \varphi_2(X),$$
$$s_2(\varphi_2(Y)) = s_2\left(\tfrac{Y}{(X+\sigma)^3}\right) = \tfrac{\sigma^3 Y}{\sigma^3(\sigma+X)^3} = \tfrac{Y}{(X+\sigma)^3} = \varphi_2(Y).$$

Thus it follows that the involution s_2 gives rise to the subcover φ_2. Since the involutions s_i give rise to the two subcovers φ_i with degree two which satisfy the hypotheses of Theorem 3.2.5, it follows from Theorem 3.2.5 that $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_1 \times E_2$. Since $E_\chi = E_1 \sim E_2$ over $\mathbb{F}_{q^4}$, we then have $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_\chi^2$ as claimed. □

Remark 3.3.2. Although the proof presented above is more or less known to Satoh [43] §3, there is a small gap in Satoh's proof where he showed $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_1 \times E_2$. On page 6 of [43], Satoh argued that $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_1 \times E_2$ follows only from $(\varphi_i)_* \circ \varphi_i^*$ being a multiplication by two map on E_i without any further clarification. In the proof presented above, this gap is closed by Theorem 3.2.5.

The result $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_\chi^2$ of Theorem 3.3.1 can be further refined by giving some explicit congruence conditions on the prime power q, or by specifying the square

condition on the coefficient v of curve $C_{u,v}/\mathbb{F}_q$. This refinement of Theorem 3.3.1 is summarized below which is Theorem 31 in [7].

Theorem 3.3.3. *Let $C_{u,v}/\mathbb{F}_q$ be a genus two Legendre-Satoh curve and let $E_{u,v}/\mathbb{F}_{q^2}$ be the elliptic curve defined in (3.3.28).*
(a) If $q \equiv 3 \pmod 4$ or if v is a square in $\mathbb{F}_q^\times$ or if $\mathrm{End}^0(E_{u,v} \otimes \overline{\mathbb{F}_q}) \not\simeq \mathbb{Q}(i)$, then $J_{u,v}$ splits over $\mathbb{F}_{q^2}$. Moreover, the converse holds if $E_{u,v}$ is ordinary.
(b) Suppose that $q \equiv 1 \pmod 4$ and that v is not a square in $\mathbb{F}_q^\times$, and that $E_{u,v}$ is ordinary. Then $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple if and only if precisely one of $4q \pm 2tr_{E_{u,v}}$ is a square in $\mathbb{Z}$. If this is the case and if $t \in \mathbb{Z}$ and $\epsilon = \pm 1$ are such that $4q + 2\epsilon tr_{E_{u,v}} = t^2$, then

$$h_{J_{u,v}}(X) = X^4 \pm tX^3 + \frac{t^2}{2}X^2 \pm tqX + q^2.$$

Note that if the hypotheses of part (b) of Theorem 3.3.3 are fulfilled and precisely one of $4q \pm 2tr_{E_{u,v}}$ is a square in $\mathbb{Z}$, then $J_{u,v}$ must be $\mathbb{F}_q$-simple. On the other hand, suppose one of the hypotheses of part (a) of Theorem 3.3.3 is fulfilled. Then knowing $J_{u,v}$ splits over $\mathbb{F}_{q^2}$ does not help us in determining whether $J_{u,v}$ is $\mathbb{F}_q$-simple or not. The following result is Corollary 32 of [7] which addresses the $\mathbb{F}_q$-simplicity issue of $J_{u,v}$ in the case of $v \in (\mathbb{F}_q^\times)^2$.

Corollary 3.3.4. *(a) If $v \in (\mathbb{F}_q^\times)^4$, then $\gamma, \chi \in \mathbb{F}_q$ and $J_{u,v} \sim E_\chi \otimes E_{-\chi}$, where E_χ is defined in (3.3.27) and $E_{-\chi}/\mathbb{F}_{q^4}$ is defined as in (3.3.27) with χ being replaced by $-\chi$, then $h_{J_{u,v}}(X) = h_{E_\chi}(X) h_{E_\chi}((-1)^{\frac{q-1}{2}}X)$.*
(b) If $v \in (\mathbb{F}_q^\times)^2 \backslash (\mathbb{F}_q)^4$, then $\gamma \in \mathbb{F}_q$ and $J_{u,v} \otimes \mathbb{F}_{q^2} \sim ((E_{u,v} \otimes \mathbb{F}_{q^2})^\chi)^2$, where $E_{u,v}$ is the elliptic curve defined as in (3.3.28). If $E_{u,v}$ is ordinary, then $J_{u,v}$ is simple if and only if $4q - tr_{E_{u,v}}^2 \notin \mathbb{Z}^2$ or, equivalently, if and only if $\mathrm{End}^0(E_{u,v}) \not\simeq \mathbb{Q}(i)$. If this is the case, then $h_{J_{u,v}}(X) = X^4 + (tr_{E_{u,v}}^2 - 2q)X^2 + q^2$.

Using the above results we can deduce necessary and sufficient conditions for $J_{u,v}$ to be $\mathbb{F}_q$-simple as follows.

Corollary 3.3.5. *Assume that* $q \equiv 1 \pmod 4$ *and* $E_{u,v}$ *is ordinary with* $\mathrm{End}^0(E_{u,v}) \not\simeq \mathbb{Q}(i)$. *Then* $J_{u,v}/\mathbb{F}_q$ *splits if and only if* $v \in (\mathbb{F}_q^\times)^4$.

Proof. Suppose that $v \in (\mathbb{F}_q^\times)^4$. By part (a) of Corollary 3.3.4, we know that $J_{u,v}$ splits.

Conversely, suppose that $J_{u,v}$ splits and $v \notin (\mathbb{F}_q^\times)^4$. Suppose first that $v \in (\mathbb{F}_q^\times)^2 \backslash (\mathbb{F}_q^\times)^4$. Since $E_{u,v}$ is ordinary with $\mathrm{End}^0(E_{u,v}) \not\simeq \mathbb{Q}(i)$, it follows from part (b) of Corollary 3.3.4 that $J_{u,v}$ must be simple, which is a contradiction. Thus we suppose that $v \notin (\mathbb{F}_q^\times)^2$. Then the hypotheses of part (b) of Theorem 3.3.3 are fulfilled. Since $v \notin (\mathbb{F}_q^\times)^2$, we have $E_{u,v}/\mathbb{F}_{q^2}$. Observe that

$$\mathrm{End}^0(E_{u,v}) \simeq \mathbb{Q}(\sqrt{tr_{E_{u,v}}^2 - 4q^2}) \simeq \mathbb{Q}(\sqrt{-(4q + 2tr_{E_{u,v}})(4q - 2tr_{E_{u,v}})}) \not\simeq \mathbb{Q}(i)$$

and hence only precisely one of the $4q \pm 2tr_{E_{u,v}}$ is a square in $\mathbb{Z}$. It then follows from part (b) of Theorem 3.3.3 that $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple. This contradicts the assumption that $J_{u,v}$ splits. Therefore, we conclude that $v \in (\mathbb{F}_q^\times)^4$. □

In fact, the above statement can also be deduced by using Theorem 3.2.6 and Theorem 3.3.1, which gives the following alternative proof.

Proof. (Alternative proof of Corollary 3.3.5)
Fix a $\sigma \in \mathbb{F}_{q^4}^\times$ such that $\sigma^4 = v$. Then the map

$$\overline{\tau}(X, Y) = \left(\frac{\sigma^2}{X}, \frac{\sigma^3 Y}{X^3}\right)$$

is an automorphism of $C_{u,v} \otimes \overline{\mathbb{F}_q}$. Indeed, if $(x_0, y_0) \in C_{u,v}(\overline{\mathbb{F}_q})$ and $\overline{\tau}(x_0, y_0) = (x_1, y_1)$,

then

$$\begin{aligned} y_1^2 &= \left(\tfrac{\sigma^3 y_0}{x_0^3}\right)^2 = x_0^{-6}\sigma^6 y_0^2 \\ &= (x_0^{-6}\sigma^6)(x_0^5 + ux_0^3 + vx_0) \\ &= v\left(\tfrac{\sigma^2}{x_0}\right) + u\left(\tfrac{\sigma^2}{x_0}\right)^3 + \left(\tfrac{\sigma^2}{x_0}\right)^5 \\ &= x_1 v + u x_1^3 + x_1^5 \end{aligned}$$

and so we have $(x_1, y_1) \in C_{u,v}(\overline{\mathbb{F}_q})$. Notice that $\overline{\tau} \neq \omega_{C_{u,v}}$. It also has order two, since $\overline{\tau}^2(X,Y) = \overline{\tau}(\frac{\sigma^2}{X}, \frac{\sigma^3 Y}{X^3}) = (X,Y)$. By Theorem 3.3.1, we know that $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E_\chi^2$ and $E_{u,v} \otimes \mathbb{F}_{q^4}$ is a quadratic twist of $E_\chi/\mathbb{F}_{q^4}$. Since $E_{u,v}$ is ordinary, $J_{u,v}$ is also ordinary. Since $q \equiv 1 \pmod 4$, there exists an element $\beta \in \mathbb{F}_q$ such that $\beta^2 = -1$. Define an automorphism $f : C_{u,v} \to C_{u,v}$ by the rule $(X,Y) \mapsto (-X, \beta Y)$. Note that $f^2 = \omega_{C_{u,v}} = (X, -Y)$ and hence f has order 4 in $\mathrm{Aut}(C_{u,v})$. It follows from Theorem 3.2.6 that $J_{u,v}$ splits over $\mathbb{F}_q$ if and only if the automorphism $\overline{\tau} : (X,Y) = (\frac{\sigma^2}{X}, \frac{\sigma^3 Y}{X^3})$ is defined over $\mathbb{F}_q$. Observe that if $\sigma \in \mathbb{F}_q$, then clearly the map $\overline{\tau}$ is defined over $\mathbb{F}_q$. On the other hand, if $\overline{\tau}$ is defined over $\mathbb{F}_q$ then $\sigma^2, \sigma^3 \in \mathbb{F}_q$. This implies that $\sigma = \sigma^3\sigma^{-2} \in \mathbb{F}_q$. It follows that $J_{u,v}$ splits over $\mathbb{F}_q$ if and only if $\sigma \in \mathbb{F}_q$ which is equivalent to $v \in (\mathbb{F}_q)^4$. □

3.4 Bolza-Freeman-Satoh curves

The purpose of this section is to introduce and study the family of Bolza-Freeman-Satoh curves defined over $\mathbb{F}_q$. These curves have the property that their Jacobians split over $\mathbb{F}_{q^6}$. In what follows, we will assume that the characteristic of $\mathbb{F}_q$ is not 2 or 3.

The family of genus two *Bolza-Freeman-Satoh curves* is defined as follow:

$$C_{BFS}/\mathbb{F}_q : \ Y^2 = X^6 + uX^3 + v, \tag{3.4.32}$$

where $v \neq 0$ and $u^2 - 4v \neq 0$. These curves were recently studied and proposed by Freeman and Satoh [13] for the purpose of pairing-based cryptography, and are called Bolza-Freeman-Satoh curves by Dr. Kani for the reason explained below.

Fix a sixth root $\sqrt[6]{v} \in \mathbb{F}_{q^6}$ of $v \in \mathbb{F}_q$, and put

$$a := \frac{u}{(\sqrt[6]{v})^3} \in \mathbb{F}_{q^2}. \tag{3.4.33}$$

Since $v \neq 0$ and $u^2 - 4v \neq 0$, it follows that $a \neq \pm 2$, and hence the following curve will be a genus two curve

$$C_B/\mathbb{F}_{q^2} : \ Y^2 = X^6 + aX^3 + 1. \tag{3.4.34}$$

This is exactly the family of curves studied by Bolza in 1887 [3] and hence the name *Bolza curve* is chosen here. A simple observation pointed out by Dr. Kani, which is implicit in [13], reveals that $C_{BFS} \otimes \mathbb{F}_{q^6} \simeq C_B \otimes \mathbb{F}_{q^6}$ via the following map

$$\begin{array}{rccc} \phi : & C_{BFS} \otimes \mathbb{F}_{q^6} & \to & C_B \otimes \mathbb{F}_{q^6} \\ & (X, Y) & \mapsto & (\sqrt[6]{v}X, \sqrt{v}Y), \end{array} \tag{3.4.35}$$

and hence the name Bolza-Freeman-Satoh curve is chosen here.

The following is a general result on the splitting property of the Jacobians of Bolza curves defined over finite fields. A proof of the similar result for Bolza-Freeman-Satoh curves defined over arbitrary perfect fields can be found on page 8 of [13]. The proof of part (a) of the following result is similar to the one on page 8 of [13], and the proof of part (b) presented below is new. In what follows J_{C_B} is used to denote the Jacobian of the Bolza curve C_B.

Theorem 3.4.1. *(a) Let $a \in \mathbb{F}_q$ be such that $a \neq \pm 2$. Then*

$$E_a : \ Y^2 = (a+1)X^3 - (30-3a)X^2 + (30+3a)X + (2-a) \tag{3.4.36}$$

is an elliptic curve with j-invariant

$$j(E_a) = 2^8 \cdot 3^3 \frac{(5-2a)^3}{(2-a)(2+a)^3}. \tag{3.4.37}$$

Furthermore, $E_a \otimes \mathbb{F}_{q^2} \sim E_{-a} \otimes \mathbb{F}_{q^2}$, where $E_{-a}/\mathbb{F}_q$ is defined as in (3.4.36) with $a \in \mathbb{F}_q$ being replaced by $-a \in \mathbb{F}_q$.

(b) If $C_B/\mathbb{F}_q : Y^2 = X^3 + aX^3 + 1$ is a Bolza curve with $a \neq \pm 2$, then $J_{C_B} \sim E_a \times E_{-a}$.

Proof. (a) Since $a \neq \pm 2$, we can define the following curve

$$E'_a/\mathbb{F}_q : \ Y^2 = X^3 + \frac{(30-3a)}{(a+2)^2}X^2 + \frac{(30+3a)}{(a+2)^3}X + \frac{2-a}{(a+2)^4}.$$

By the formula on page 64 of Silverman [46] and the fact that $a \neq \pm 2$, the discriminant of E'_a can be computed as follows:

$$\Delta(E'_a) = 2^{16} \cdot 3^3 \frac{a-2}{(a+2)^9} \neq 0.$$

Hence, it follows that E'_a is an elliptic curve [46] (page 50). By the formula of [46] (page 64) and by a tedious computation, the j-invariant of E'_a can be computed to obtain

$$j(E'_a) = 2^8 \cdot 3^3 \frac{(5-2a)^3}{(2-a)(2+a)^3}.$$

Observe that E'_a is isomorphic to E_a via the following map:

$$\begin{aligned} E_a \quad &\to \quad E'_a \\ (X,Y) \quad &\mapsto \quad ((a+2)X, (a+2)^2 Y). \end{aligned}$$

Thus E_a is also an elliptic curve and $j(E_a) = j(E'_a)$ ([46] page 50). This proves the first part of part (a). Similary, we know that $E_{-a}/\mathbb{F}_q$ is also an elliptic curve with its j-invariant given as in (3.4.37) with a being replaced by $-a$.

To show that $E_a \otimes \mathbb{F}_{q^2} \sim E_{-a} \otimes \mathbb{F}_{q^2}$, we take the same approach indicated on page 9-10 of [13]. By taking the second derivative of the equation for E_a, Freeman and Satoh found [13] that $(1, \pm 8)$ are rational 3-torsion points. Let $H := \{\infty, (1, \pm 8)\}$ be the cyclic subgroup generated by these points. Freeman and Satoh considered the quotient map $E_a \to (E_a/H)$ of degree 3, and found a model for the curve $(E_a/H)/\mathbb{F}_q$ as follows

$$(E_a/H)/\mathbb{F}_q : Y^2 = X^3 - (3a-30)X^2 + (3a^2 - 924a - 1860)X - (a^3 + 834a^2 + 30972a + 58616),$$

which they showed to be isomorphic to E_{-a} over $\mathbb{F}_{q^2}$ via the map

$$\begin{array}{rcl} (E_a/H) \otimes \mathbb{F}_{q^2} & \to & E_{-a} \otimes \mathbb{F}_{q^2} \\ (X, Y) & \mapsto & \left(\frac{X+2a+40}{3a-6}, -\frac{Y}{(3a-6)\sqrt{-3}} \right). \end{array}$$

It follows that $E_a \otimes \mathbb{F}_{q^2} \sim (E_a/H) \otimes \mathbb{F}_{q^2} \sim E_{-a} \otimes \mathbb{F}_{q^2}$, and hence completes the proof.

(b) Let $E_1 := E_a$ and $E_2 := E_{-a}$. We proceed to show that $J_{C_B} \sim E_a \times E_{-a}$ by first showing that there exist injections $f_i : \mathbb{F}_q(E_i) \hookrightarrow \mathbb{F}_q(C_B)$ where $\mathbb{F}_q(E_i)$ and $\mathbb{F}_q(C_B)$ are the function fields of $E_i/\mathbb{F}_q$ and $C_B/\mathbb{F}_q$ respectively, and $i := 1, 2$. Consider the two functions X and Y in the function field $\mathbb{F}_q(C_B)$ such that they satisfy the curve equation $C_B : Y^2 = X^6 + aX^3 + 1$ and define the following functions in $\mathbb{F}_q(C_B)$.

$$\begin{cases} U_1 := \left(\frac{X+1}{X-1}\right)^2 \\ V_1 := -\frac{8Y}{(X-1)^3} \end{cases} \quad \text{and} \quad \begin{cases} U_2 := \left(\frac{X-1}{X+1}\right)^2 \\ V_2 := -\frac{8Y}{(X+1)^3}. \end{cases}$$

Thus $\mathbb{F}_q(U_i, V_i)$ is a subfield of $\mathbb{F}_q(C_B)$ for $i = 1, 2$. By a tedious computation we can verify that the functions U_i and V_i defined above satisfy the following relations in $\mathbb{F}_q(C_B)$:

$$\begin{aligned} V_1^2 &= (a+1)U_1^3 - (30-3a)U_1^2(30+3a)U_1 + (2-a) \\ V_2^2 &= (-a+1)U_2^3 - (30+3a)U_2^2(30-3a)U_2 + (2+a). \end{aligned}$$

From these relations, it follows that $\mathbb{F}_q(E_i) \simeq \mathbb{F}_q(U_i, V_i)$ and hence gives us the following injection:

$$f_i : \mathbb{F}_q(E_i) \simeq \mathbb{F}(U_i, V_i) \hookrightarrow \mathbb{F}_q(C_B).$$

From Proposition 3.1.1 in Section 3.1 (page 25 of [46]), we know that there exist unique non-constant morphisms

$$\begin{array}{rccc} \varphi_1 : & C_B & \to & E_1 \\ & (X,Y) & \mapsto & \left((\frac{X+1}{X-1})^2, -\frac{8Y}{(X-1)^3}\right), \end{array} \qquad \begin{array}{rccc} \varphi_2 : & C_B & \to & E_2 \\ & (X,Y) & \mapsto & \left((\frac{X-1}{X+1})^2, -\frac{8Y}{(X+1)^3}\right), \end{array}$$

such that $\varphi_i^* = f_i$. Since $U_1 = \left(\frac{X+1}{X-1}\right)^2$ and $U_2 = \left(\frac{X-1}{X+1}\right)^2$, by multiplying $(X-1)^2$ and $(X+1)^2$ to both sides of the equalities respectively and grouping like terms in X we have the following relations

$$(U_1 - 1)X^2 - 2(U_1 + 1)X + (U_1 - 1) = 0, \tag{3.4.38}$$

$$(U_2 - 1)X^2 + 2(U_2 + 1)X + (U_2 - 1) = 0. \tag{3.4.39}$$

From these relations, and by the same argument used in the proof of Theorem 3.3.1, it follows that

$$\deg(\varphi_i) = [\mathbb{F}_q(C_B) : \mathbb{F}_q(E_i)] = [\mathbb{F}_q(X, Y) : \mathbb{F}_q(U_i, V_i)] = 2.$$

Next we proceed to find the involutions that give rise to the subcovers $\varphi_i : C_B \to E_i$. Note that the two roots of the quadratic equation given in (3.4.38) are X and $\frac{1}{X}$, hence the non-trivial automorphism of the extension $\mathbb{F}_q(X)$ over $\mathbb{F}_q(U_1)$ is given by the map $X \mapsto \frac{1}{X}$. Applying this map to the polynomial $X^6 + aX^3 + 1$ on the right hand side of the curve equation, we obtain

$$\frac{1 + aX^3 + X^6}{X^6}.$$

Observe that in $\mathbb{F}_q(C)$ we have $Y^2 = X^6 + aX^3 + 1$, and hence we have

$$\frac{1 + aX^3 + X^6}{X^6} = \left(\frac{Y}{X^3}\right)^2.$$

This leads us to consider the map

$$s_1(X, Y) = \left(\frac{1}{X}, -\frac{Y}{X^3}\right)$$

which turns out to be an automorphism of C_B. Indeed, this follows from the fact that the pair $(\frac{1}{X}, -\frac{Y}{X^3})$ satisfies the curve equation $Y^2 = X^6 + aX^3 + 1$ in the function field $\mathbb{F}_q(C_B)$. Moreover, observe that $s_1^2(X, Y) = s_1(\frac{1}{X}, -\frac{Y}{X^3}) = (X, Y)$, and hence s_1 is an involution. Finally, we verify that the cover $\phi_1 : C_B \to E_1$ is s_1-invariant as follows:

$$s_1(\varphi_1(X)) = s_1\left(\left(\tfrac{X+1}{X-1}\right)^2\right) = \left(\tfrac{\frac{1}{X}+1}{\frac{1}{X}-1}\right)^2 = \left(\tfrac{X+1}{X-1}\right)^2 = \varphi_1(X)$$
$$s_1(\varphi_1(Y)) = s_1\left(\tfrac{-8Y}{(X-1)^3}\right) = \tfrac{-8\frac{-Y}{X^3}}{(\frac{1}{X}-1)^3} = \tfrac{-8Y}{(X-1)^3} = \varphi_1(Y).$$

Thus it follows that the involution s_1 gives rise to the subcover ϕ_1. If we set $s_2 := s_1 \circ \omega_{C_B}$ where ω_{C_B} denotes the hyperelliptic involution of C_B, then clearly

$$s_2(X, Y) = \left(\frac{1}{X}, \frac{Y}{X^3}\right)$$

is an automorphism of C_B and of order 2, since both s_1 and ω_{C_B} are two automorphisms of C_B of order 2 which commute. Furthermore, we verify that the subcover φ_2 is s_2-invariant as follows:

$$s_2(\varphi_2(X)) = s_2\left(\left(\tfrac{X-1}{X+1}\right)^2\right) = \left(\tfrac{\frac{1}{X}-1}{\frac{1}{X}+1}\right)^2 = \left(\tfrac{X-1}{X+1}\right)^2 = \varphi_2(X),$$
$$s_2(\varphi_2(Y)) = s_2\left(\tfrac{-8Y}{(X+1)^3}\right) = \tfrac{-8\frac{Y}{X^3}}{(\frac{1}{X}+1)^3} = \tfrac{-8Y}{(X+1)^3} = \varphi_2(X).$$

Thus it follows that the involution s_2 gives rise to the subcover φ_2. Since the involutions s_i give rise to the two subcovers φ_i with degree two which satisfy the hypotheses of Theorem 3.2.5, it follows from Theorem 3.2.5 that $J_{C_B} \sim E_1 \times E_2$, as claimed. □

Remark 3.4.2. From the theorem above, we observe that if $C_B/\mathbb{F}_q : Y^2 = X^6 + aX^3 + 1$ is a Bolza curve with $a \neq \pm 2$ then $J_{C_B} \otimes \mathbb{F}_{q^2} \sim (E_a \otimes \mathbb{F}_{q^2})^2$.

Some consequences of the theorem will be presented here. In what follows, $J_{C_{BFS}}$ is used to denote the Jacobian of the Bolza-Freeman-Satoh curve C_{BFS} given in (3.4.32).

Corollary 3.4.3. *Let $C_{BFS}/\mathbb{F}_q$ be a Bolza-Freeman-Satoh curve defined in (3.4.32) and let $a \in \mathbb{F}_{q^2}$ be defined as in (3.4.33). Let E_a be the elliptic curve defined in (3.4.36).*

(a) Then, $J_{C_{BFS}} \otimes \mathbb{F}_{q^6} \sim (E_a \otimes \mathbb{F}_{q^6})^2$.

(b) Let $d := 2, 3,$ or 6. If the coefficient v of the curve C_{BFS} satisfies $v \in (\mathbb{F}_q^\times)^d$, then we have

$$\begin{cases} a \in \mathbb{F}_q, & \text{if } d = 2,\ 6, \\ a \in \mathbb{F}_{q^2}, & \text{if } d = 3. \end{cases} \tag{3.4.40}$$

If we define the elliptic curve E_a given in (3.4.36) with the element $a \in \mathbb{F}_{q^2}$ given in (3.4.40), then

$$\begin{cases} J_{C_{BFS}} \otimes \mathbb{F}_{q^3} \sim (E_a \otimes \mathbb{F}_{q^3}) \times (E_{-a} \otimes \mathbb{F}_{q^3}), & \text{if } d = 2, \\ J_{C_{BFS}} \otimes \mathbb{F}_{q^2} \sim E_a^2, & \text{if } d = 3, \\ J_{C_{BFS}} \sim E_a \times E_{-a}, & \text{if } d = 6. \end{cases}$$

(c) If $q \equiv 2 \pmod 3$ or if $\mathrm{End}^0(E_a \otimes \overline{\mathbb{F}_q}) \simeq \mathbb{Q}(\sqrt{-3})$, then $J_{C_{BFS}} \otimes \mathbb{F}_{q^2}$ splits.

Proof. (a) Recall that, by the definition of $C_{BFS}/\mathbb{F}_q$, we have that $a \neq \pm 2$ and that the Bolza curve $C_B/\mathbb{F}_{q^2}$ defined in (3.4.34) is also a genus two curve. Since $C_{BFS} \otimes \mathbb{F}_{q^6} \simeq C_B \otimes \mathbb{F}_{q^6}$ via the map $\phi : (X, Y) \mapsto (\sqrt[6]{v}X, \sqrt{v}Y)$ given in (3.4.35), it follows that $J_{C_{BFS}} \otimes \mathbb{F}_{q^6} \simeq J_{C_B} \otimes \mathbb{F}_{q^6}$ where J_{C_B} denotes the Jacobian of the Bolza curve $C_B/\mathbb{F}_{q^2}$. On the other hand, since $C_B/\mathbb{F}_{q^2}$ is a Bolza curve with $a \neq \pm 2$, it follows from Theorem 3.4.1 (b) that $J_{C_B} \sim E_a \times E_{-a}$ where $E_{\pm a}/\mathbb{F}_{q^2}$ defined in (3.4.36). Since $\sqrt{-3} \in \mathbb{F}_{q^6}$, it follows from Remark 3.4.2 that $J_{C_{BFS}} \otimes \mathbb{F}_{q^6} \simeq J_{C_B} \otimes \mathbb{F}_{q^6} \sim (E_a \otimes \mathbb{F}_{q^6})^2$.

(b) We proceed with distinguishing cases. If $d = 2$, then $v \in (\mathbb{F}_q^\times)^2$ and $\sqrt[6]{v} \in \mathbb{F}_{q^3}$. It

follows that $a = \frac{u}{(\sqrt[6]{v})^3} \in \mathbb{F}_q$. Hence we have $E_{\pm a}/\mathbb{F}_q$ and $C_{BFS} \otimes \mathbb{F}_{q^3} \simeq C_B \otimes \mathbb{F}_{q^3}$ via the map $\phi : (X, Y) \mapsto (\sqrt[6]{v}X, \sqrt{v}Y)$ given in (3.4.35). Together with Theorem 3.4.1 (b), we have $J_{C_{BFS}} \otimes \mathbb{F}_{q^3} \simeq J_{C_B} \otimes \mathbb{F}_{q^3} \sim (E_a \otimes \mathbb{F}_{q^3}) \times (E_{-a} \otimes \mathbb{F}_{q^3})$. Next, if $d = 3$, then $v \in (\mathbb{F}_q^\times)^3$ and $\sqrt[6]{v} \in \mathbb{F}_{q^2}$. It follows that $a = \frac{u}{(\sqrt[6]{v})^3} \in \mathbb{F}_{q^2}$. Hence we have that $E_{\pm a}/\mathbb{F}_{q^2}$ and $C_{BFS} \otimes \mathbb{F}_{q^2} \simeq C_B$ via the map $\phi : (X, Y) \mapsto (\sqrt[6]{v}X, \sqrt{v}Y)$ given in (3.4.35). Together with Theorem 3.4.1 (b) and Remark 3.4.2, we have $J_{C_{BFS}} \otimes \mathbb{F}_{q^2} \simeq J_{C_B} \sim E_a^2$. Finally, if $d = 6$, then $v \in (\mathbb{F}_q^\times)^6$ and $\sqrt[6]{v} \in \mathbb{F}_q$. It follows that $a = \frac{u}{(\sqrt[6]{v})^3} \in \mathbb{F}_q$. Hence we have $E_{\pm a}/\mathbb{F}_q$ and $C_{BFS} \simeq C'_B$ via the map $\phi : (X, Y) \mapsto (\sqrt[6]{v}X, \sqrt{v}Y)$ given in (3.4.35). Together with Theorem 3.4.1 (b), we have $J_{BFC} \simeq J_{C_B} \sim E_a \times E_{-a}$.

(c) If $q \equiv 2 \pmod 3$, then every element in $\mathbb{F}_q$ is a cubic root. In particular, $v \in (\mathbb{F}_q)^3$, and so it follows from part (b) that $J_{C_{BFS}} \otimes \mathbb{F}_{q^2} \sim E_a^2$. Now suppose that $\mathrm{End}^0(E_a \otimes \overline{\mathbb{F}_q}) \simeq \mathbb{Q}(\sqrt{-3})$. Then E_a is ordinary and in view of Proposition 2.3.7 the condition $(iv)_3$ does not hold for $E := E_a \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6}$. It then follows from part (b) of Theorem 2.3.5 (i) that $J_{C_{BFS}} \otimes \mathbb{F}_{q^2}$ cannot be simple. Hence the asserted statement is proven. □

Here we present an analogue of Corollary 3.3.5.

Theorem 3.4.4. *Let $C_{BFS}/\mathbb{F}_q$ be the Bolza-Freeman-Satoh curve defined in (3.4.32). Let $a \in \mathbb{F}_{q^2}$ be defined as in (3.4.33), and E_a be the elliptic curve defined in (3.4.36). Assume that $q \equiv 1 \pmod 3$ and that E_a is ordinary with $\mathrm{End}^0(E_a) \not\simeq \mathbb{Q}(\sqrt{-3})$. Then $J_{C_{BFS}}$ is split if and only if $v \in (\mathbb{F}_q^\times)^6$.*

Proof. Fix $\sigma \in \mathbb{F}_{q^6}^\times$ such that $\sigma^6 = v$. Then we claim that the map

$$\overline{\tau}(X, Y) = \left(\frac{\sigma^2}{X}, \frac{\sigma^3 Y}{X^3}\right)$$

is an automorphism of $C_{BFS} \otimes \overline{\mathbb{F}_q}$. Indeed, if $(x_0, y_0) \in C_{BFS}(\overline{F}_q)$ and $\overline{\tau}(x_0, y_0) =$

(x_1, y_1), then

$$\begin{aligned} y_1^2 &= \left(\frac{\sigma^3 y_0}{x_0^3}\right)^2 = x_0^{-6}\sigma^6 y_0^2 \\ &= (x_0^{-6}\sigma^6)(x_0^6 + ux_0^3 + v) \\ &= v + u\left(\frac{\sigma^2}{x_0}\right)^3 + \left(\frac{\sigma^2}{x_0}\right)^6 \\ &= v + ux_1^3 + x_1^6 \end{aligned}$$

and so we have $(x_1, y_1) \in C_{BFS}(\overline{\mathbb{F}_q})$. Notice that $\overline{\tau} \neq \omega_{C_{BFS}}$. It also has order two, since $\overline{\tau}^2(X, Y) = \overline{\tau}(\frac{\sigma^2}{X}, \frac{\sigma^3 Y}{X^3}) = (X, Y)$. By Theorem 3.4.3, we know that

$$J_{C_{BFS}} \otimes \mathbb{F}_{q^6} \sim (E_a \otimes \mathbb{F}_{q^6})^2.$$

Since E_a is ordinary, $J_{C_{BFS}}$ is also ordinary. Since $q \equiv 1 \pmod 3$, there exists a primitive third root of unity $\zeta_3 \in \mathbb{F}_q$. Define an automorphism $f : C_{BFS} \to C_{BFS}$ by the rule $(X, Y) \mapsto (\zeta_3 X, Y)$, and observe that it has order 3 in $\mathrm{Aut}(C_{BFS})$. It follows from Theorem 3.2.6 that $J_{C_{BFS}}$ splits over $\mathbb{F}_q$ if and only if the automorphism $\overline{\tau} : (X, Y) = (\frac{\sigma^2}{X}, \frac{\sigma^3 Y}{X^3})$ is defined over $\mathbb{F}_q$. Observe that if $\sigma \in \mathbb{F}_q$ then clearly the map $\overline{\tau}$ is defined over $\mathbb{F}_q$. On the other hand, if $\overline{\tau}$ is defined over $\mathbb{F}_q$ then $\sigma^2, \sigma^3 \in \mathbb{F}_q$. This will imply that $\sigma = \sigma^3\sigma^{-2} \in \mathbb{F}_q$. It follows that $J_{C_{BFS}}$ splits over $\mathbb{F}_q$ if and only if $\sigma \in \mathbb{F}_q$ which is equivalent to $v \in (\mathbb{F}_q)^6$. □

Remark 3.4.5. In Theorem 4.5 of Freeman and Satoh [13] a sufficient conditioin for $J_{C_{BFS}}$ to be $\mathbb{F}_q$-simple was presented. However, an error in the proof of Theorem 4.5 of Freeman and Satoh [13] occurred when they improperly applied their Proposition 3.1 to conclude that $J_{C_{BFS}}$ is $\mathbb{F}_q$-simple. This is not possible because Proposition 3.1 in [13] in fact requires the abelian varieties under the investigation to be $\mathbb{F}_q$-simple to begin with. The above result gives a necessary and sufficient conditons for $J_{C_{BFS}}$ to be $\mathbb{F}_q$-simple, and fixes the mistake in the Theorem 4.5 of Freeman and Satoh [13].

This section is concluded with the following corollary.

Corollary 3.4.6. *Let $C_{BFS}/\mathbb{F}_q$ be a Bolza-Freeman-Satoh curve defined in (3.4.32), let $a \in \mathbb{F}_{q^2}$ be defined as in (3.4.33), and let E_a be the elliptic curve defined in (3.4.36). Assume that $q \equiv 1 \pmod 3$ and that E_a is ordinary with $\mathrm{End}^0(E_a) \not\simeq \mathbb{Q}(\sqrt{-3})$.*
(a) Let $d := 2, 3$ and $j := \frac{6}{d}$. If the coefficient v of the curve C_{BFS} satisfies $v \in (\mathbb{F}_q^\times)^d \backslash (\mathbb{F}_q^\times)^6$, then $J_{C_{BFS}}$ is $\mathbb{F}_q$- simple but $J_{C_{BFS}} \otimes \mathbb{F}_{q^j} \sim (E_a \otimes \mathbb{F}_{q^j})^2$ and

$$\begin{cases} (tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) &= (\pm tr_{E_a}, tr_{E_a}^2 - q), & \text{if } d = 2, \\ (tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) &= (0, -tr_{E_a}), & \text{if } d = 3. \end{cases}$$

(b) Suppose in addition that q is an odd prime power and that $\frac{q+1}{2} \in \mathbb{Z}$ is odd. Then $J_{C_{BFS}} \otimes \mathbb{F}_{q^m}$ is simple for $m|6$, $m \neq 6$, if and only if $v \notin (\mathbb{F}_q^\times)^2 \cup (\mathbb{F}_q^\times)^3$. If this is the case, then $(tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) = (\pm t, \frac{t^2}{3} + q)$, where $t \in \mathbb{Z}$ such that $3|t$ and $tr_{E_a} = -\frac{t^2}{3} + 2q$.

Proof. (a) Since $q \equiv 1 \pmod 3$ and $v \in (\mathbb{F}_q^\times)^d \backslash (\mathbb{F}_q^\times)^6$, it follows from Theorem 3.4.1 (b), Theorem 3.4.4, and Corollary 3.4.3 (b) that $J_{C_{BFS}}$ is $\mathbb{F}_q$-simple but $J_{C_{BFS}} \otimes \mathbb{F}_{q^j} \sim J_{C_B} \otimes \mathbb{F}_{q^j} \sim (E_a \otimes \mathbb{F}_{q^j})^2$. For $d = 3$, it follows from part (a) of Theorem 2.3.5 and Remark 2.3.6 that $(tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) = (0, -tr_{E_a})$. For $d = 2$, we have $a = \frac{u}{(\sqrt[6]{v})^3} \in \mathbb{F}_q$ and hence $E_a/\mathbb{F}_q$. In view of part (b) of Theorem 2.3.5 (iii), we take $E_0 := E_a^\chi$ and $E := E_a \otimes \mathbb{F}_{q^3}$. Then it follows that

$$E_0 \otimes \mathbb{F}_{q^3} = E_a^\chi \otimes \mathbb{F}_{q^3} \sim (E_a \otimes \mathbb{F}_{q^3})^\chi = E^\chi.$$

Furthermore, since $E_a/\mathbb{F}_q$ is ordinary and $\mathrm{End}^0(E_a) \not\simeq \mathbb{Q}(\sqrt{-3})$, it follows that

$$h_{E_a}(X) = X^2 - tr_{E_a} X + q$$

with $3(4q - tr_{E_a}^2) \notin \mathbb{Z}^2$. We set $t := \pm tr_{E_a}$. By part (b) of Theorem 2.3.5 (iii) (i.e. by the fact that (iii) implies (i)) and also by Remark 2.3.6, there exists an $\mathbb{F}_q$-simple

abelian surface $A/\mathbb{F}_q$ such that $A \otimes \mathbb{F}_{q^3} \sim E^2 \sim (E_a \otimes \mathbb{F}_{q^3})^2$ with $tr_A = t$. On the other hand, since $J_{C_{BFS}} \otimes \mathbb{F}_{q^3} \sim (E_a \otimes \mathbb{F}_{q^3})^2$, it follows from Theorem 2.3.9 that either $J_{C_{BFS}} \sim A$ or that $J_{C_{BFS}} \sim A^\chi$. Hence $(tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) = (\pm tr_{E_a}, tr_{E_a}^2 - q)$.

(b) Applying Theorem 3.4.4 with q replaced by q^m, for $m = 1, 2, 3$, we see that $J_{C_{BFS}} \otimes \mathbb{F}_{q^m}$ is simple if and only if $v \notin (\mathbb{F}_{q^m}^\times)^6$, which is equivalent to

$$v^{\frac{q^m-1}{6}} = \begin{cases} (v^{\frac{q-1}{3}})^{\frac{q+1}{2}} & = \quad -1 \quad \text{if } m = 2 \\ (v^{\frac{q-1}{2}})^{\frac{q^2+q+1}{3}} & = \quad -1 \quad \text{if } m = 3. \end{cases} \tag{3.4.41}$$

(Note that $\frac{q+1}{2} \in \mathbb{Z}$ since q is odd.) Since $q \equiv 1 \pmod 3$ and q is odd, we can write $q = 3w+1$, where $w \in \mathbb{Z}$ is even. It follows that $\frac{q^2+q+1}{3} = 3w^2+3w+1$ is odd. On the other hand, $\frac{q+1}{2}$ is odd. It follows that (3.4.41) holds if and only if $v \notin (\mathbb{F}_q^\times)^2 \cup (\mathbb{F}_q^\times)^3$. Suppose this is the case. Let $A := J_{C_{BFS}}$. Then, by Corollary 3.4.3 (a), it follows that $A \otimes \mathbb{F}_{q^6} \sim E^2$ where $E := E_a \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6}$ and $E_a/\mathbb{F}_{q^2}$. Since $A \otimes \mathbb{F}_{q^m}$ is simple for all $m|6$, $m \neq 6$, it follows from part (b) of Theorem 2.3.5 ((i) implies (iii)) that there exists an elliptic curve $E_0/\mathbb{F}_{q^2}$ with $E_0 \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6} \sim E^\chi$ and an integer $t \in \mathbb{Z}$ such that $tr_{E_0} = \frac{t^2}{3} - 2q$ but $4q - \frac{t^2}{3} \notin \mathbb{Z}^2$. It then follows from Proposition 2.3.9 and Theorem 2.3.4 (a) that $(tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) \in \{(\pm t, \frac{t^2}{3} + q)\}$. It remains to show that $tr_{E_a} = -\frac{t^2}{3} + 2q$. Observe that

$$E_0 \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6} \sim E^\chi \sim (E_a \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6})^\chi \sim E_a^\chi \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6}.$$

Hence it follows that

$$tr_{E_a^\chi \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6}} = tr_{E_a^\chi}^3 - 3q^2 tr_{E_a^\chi} = tr_{E_0}^3 - 3q^2 tr_{E_0} = tr_{E_0 \otimes_{\mathbb{F}_{q^2}} \mathbb{F}_{q^6}}$$

which gives the relation

$$\begin{aligned}
& (tr_{E_a^\chi} - tr_{E_0})[tr_{E_a^\chi}^2 + tr_{E_a^\chi} tr_{E_0} + (tr_{E_0}^2 - 3q^2)] \\
= \; & (tr_{E_a^\chi} - tr_{E_0})[(tr_{E_a^\chi} - tr_{E_0})^2 + 3tr_{E_a^\chi} tr_{E_0} - 3q^2] \\
= \; & (tr_{E_a^\chi} - tr_{E_0})^3 + 3tr_{E_a^\chi} tr_{E_0}(tr_{E_a^\chi} - tr_{E_0}) - 3q^2(tr_{E_a^\chi} - tr_{E_0}) \\
= \; & tr_{E_a^\chi}^3 - tr_{E_0}^3 - 3q^2[tr_{E_a^\chi} - tr_{E_0}] \\
= \; & 0.
\end{aligned}$$

If $tr_{E_a^\chi}^2 + tr_{E_a^\chi} tr_{E_0} + (tr_{E_0}^2 - 3q^2) = 0$, then $-3(tr_{E_0}^2 - 4q^2) \in \mathbb{Z}^2$ since

$$tr_{E_a^\chi} = \frac{-tr_{E_0} \pm \sqrt{-3(tr_{E_0}^2 - 4q^2)}}{2} \in \mathbb{Z}.$$

Since $tr_{E_0} = \frac{t^2}{3} - 2q$, this implies that $-3[tr_{E_0}^2 - 4q^2] = t^2[4q - \frac{t^2}{3}] \in \mathbb{Z}^2$ and hence $4q - \frac{t^2}{3} \in \mathbb{Z}^2$ which is a contradiction. Thus $tr_{E_a^\chi} = tr_{E_0}$ and $tr_{E_a} = -tr_{E_0} = -\frac{t^2}{3} + 2q$. □

Chapter 4

Simple geometrically split abelian surfaces with specified embedding degree

In this chapter the concept of *valid integer tuple* will be presented in Section 4.1. A valid integer tuple is used to describe a set of integer parameters with certain conditions that guarantee the existence of isogeny classes of simple geometrically split ordinary abelian surfaces over finite fields with specified embedding degrees with respect to specified prime numbers. In Section 4.2, it will be shown how a given valid integer tuple can be used to find Legendre-Satoh curves and Bolza-Freeman-Satoh curves over finite fields whose Jacobians are isomorpic to the abelian surfaces over finite fields given by the valid integer tuple.

Both Theorem 4.1.1 and Theorem 4.2.3 presented in this chapter are new.

4.1 Valid integer tuples

In this section, the following result will be presented which gives the necessary and sufficient conditions on a set of integer parameters that guarantee the existence of simple geometrically split ordinary abelian surfaces over finite fields with specified embedding degrees with respect to specified prime numbers.

Theorem 4.1.1. *Let $n = 3, 4, 6$ and $c = \lfloor \frac{n}{2} \rfloor$, and let (k, D, r, q, t) be an integer tuple, where q is a prime power p^m where $p > 5$, $r > 5$ is a prime such that $r \nmid q$, and $k, D \in \mathbb{N}$ such that $r \nmid k$ and $-D$ is a fundamental discriminant with the property that $D \nmid 12$.*

Then the integer tuple (k, D, r, q, t) satisfies the following list of conditions

(i) $4cq = t^2 + x^2 D$ *for some* $x \in \mathbb{Z}$;

(ii) $ord_{\mathbb{F}_r^\times}(q) = k$;

(iii) $t^2 - c(q+1)t + c(q^2 + (c-2)q + 1) \equiv 0 \pmod{r}$;

(iv) $\gcd(t, q) = 1$;

(v) $c \mid t$

if and only if there exists an ordinary abelian surface $A/\mathbb{F}_q$ such that

(vi) $A/\mathbb{F}_q$ *has embedding degree k with respect to the prime r and*

(vii) $tr_A = t$, $A \otimes \mathbb{F}_{q^n} \sim E^2$ *where $A \otimes \mathbb{F}_{q^m}$ is simple for all $m \mid n$, $m \neq n$, and $E/\mathbb{F}_{q^n}$ is an elliptic curve with* $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-D})$.

If this is the case, then the characteristic polynomial of $A/\mathbb{F}_q$ is given as follows:

$$h_A(X) = X^4 - tX^3 + \left(\frac{t^2}{c} + (c-2)q\right)X^2 - tqX + q^2. \tag{4.1.1}$$

Proof. Assume that for each of the $n = 3, 4, 6$ an integer tuple (k, D, r, q, t) which satisfies the listed conditions $(i) - (v)$ is given. By condition (i), it follows that

$$t^2 \leq 4cq. \tag{4.1.2}$$

The following relations will be verified

$$\begin{cases} 4cq \neq t^2 + 3x^2 & \forall x \in \mathbb{Z} \quad \text{if } n = 3, 6, \\ 4cq \neq t^2 + x^2 & \forall x \in \mathbb{Z} \quad \text{if } n = 4. \end{cases} \tag{4.1.3}$$

Suppose for $n = 3, 6$ there exists an $x_1 \in \mathbb{Z}$ such that $4cq = t^2 + 3x_1^2$. From condition (i) it then follows that

$$3x_1^2 = Dx^2, \tag{4.1.4}$$

where $x \in \mathbb{Z}$ is as in condition (i). Since 3 is prime, either $3 \mid D$ or $3 \mid x^2$. If $3 \nmid D$, then $3 \mid x^2$. Hence the exponent of 3 on the left hand side of (4.1.4) will be odd, while the exponent of 3 on the right hand side of (4.1.4) is even, which is clearly a contradiction. Thus it must be the case that $3|D$. Since $3 \mid D$ and $-D$ is a fundamental discriminant, it follows that $D = 3\tilde{D}$ where $\gcd(\tilde{D}, 3) = 1$. Hence equation (4.1.4) becomes $3(x_1^2 - \tilde{D}x^2) = 0$, which gives

$$x_1^2 = \tilde{D}x^2.$$

This equality is possible if $\tilde{D}$ is a square, i.e. if and only if $\tilde{D} = 1$ or 4. This implies that $D = 3$ or 12, which contradicts $D \nmid 12$. Hence no such $x_1 \in \mathbb{Z}$ can exist, and so the relation (4.1.3) holds for $n = 3, 6$. Next suppose that $n = 4$ there exists an

$x_1 \in \mathbb{Z}$ such that $4cq = t^2 + x_1^2$. From condition (i) it then follows that

$$x_1^2 = Dx^2$$

where $x \in \mathbb{Z}$ is as in condition (i). Similarly this equality can happen if and only if $D = 4$, which will contradict $D \nmid 12$. So no such $x_1 \in \mathbb{Z}$ can exist, and hence equation (4.1.3) holds for $n = 4$. From (4.1.2), (4.1.3), condition (iv), and (v), Theorem 2.3.4 (b) is invoked to conclude that there exists a simple, ordinary abelian surface $A/\mathbb{F}_q$ with $tr_A = t$ such that $A \otimes \mathbb{F}_{q^n}$ splits but $A \otimes \mathbb{F}_{q^m}$ remains simple for $m \mid n$, $m \neq n$. Hence the first and the second conditions of condition (vii) are fulfilled. Furthermore, the characteristic polynomial $h_A(X)$ of $A/\mathbb{F}_q$ is given by the second part of Theorem 2.3.4 (b) as

$$h_A(X) = X^4 - tX^3 + \left(\frac{t^2}{c} + (c-2)q\right)X^2 - tqX + q^2,$$

which justifies equation (4.1.1). From condition (iii) and Theorem 2.1.5 (1), it follows that $r \mid \#A(\mathbb{F}_q)$ because

$$\begin{aligned}
\#A(\mathbb{F}_q) &= h_A(1) \\
&= 1 - t + \tfrac{t^2}{c} + (c-2)q - tq + q^2, \\
&= \begin{cases} t^2 - (q+1)t + (q^2 - q + 1), & \text{if } n = 3, \\ \frac{t^2}{2} - (q+1)t + (q^2+1), & \text{if } n = 4, \\ \frac{t^2}{3} - (q+1)t + (q^2+q+1), & \text{if } n = 6, \end{cases} \\
&= \begin{cases} t^2 - (q+1)t + (q^2 - q + 1), & \text{if } n = 3, \\ \frac{1}{2}[t^2 - 2(q+1)t + 2(q^2+1)], & \text{if } n = 4, \\ \frac{1}{3}[t^2 - 3(q+1)t + 3(q^2+q+1)], & \text{if } n = 6, \end{cases} \\
&\equiv 0 \ (\bmod r).
\end{aligned} \tag{4.1.5}$$

Together with condition (ii), this means that $A/\mathbb{F}_q$ has embedding degree k with respect to the prime r. This verifies condition (vi). It remains to show that $\mathrm{End}^0(E) \simeq$

$\mathbb{Q}(\sqrt{-D})$. Since the abelian surface $A/\mathbb{F}_q$ here satisfies (i) of Theorem 2.3.5 (b), it follows from the same theorem that there exists an elliptic curve $E_0/\mathbb{F}_{q^d}$ with $E_0 \otimes \mathbb{F}_{q^n} \sim E^\chi$, $tr_{E_0} = \frac{t^2}{c} - 2(d-1)q$, and

$$(4-c)\left(4q - \frac{t^2}{c}\right) \tag{4.1.6}$$

is not a square, where $t = tr_A$ and $d = \lfloor \frac{n+2}{3} \rfloor$. Note that $E_0/\mathbb{F}_{q^d}$ is ordinary. Since the Frobenius endomorphism π_{E_0} satisfies $h_{E_0}(X) = X^2 - tr_{E_0}X + q^d$, it follows from equation (4.1.6) that

$$\pi_{E_0} = \begin{cases} \frac{tr_{E_0} \pm \sqrt{t^2-4q}}{2} & \text{if } n = 3 \\ \frac{tr_{E_0} \pm \frac{t}{c}\sqrt{t^2-4cq}}{2} & \text{if } n = 4, 6 \end{cases}$$

By condition (i), we know that $t^2 - 4cq = -Dx^2$ and hence $\pi_{E_0} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$, where $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is the ring of integers of $\mathbb{Q}(\sqrt{-D})$. Thus $\mathbb{Z}[\pi_{E_0}] \subseteq \mathrm{End}(E_0) \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$, and $\mathrm{End}^0(E_0) \simeq \mathbb{Q}(\sqrt{-D})$. Since $E_0 \otimes \mathbb{F}_{q^n} \sim E^\chi$ and E^χ is a nontrivial quadratic twist of E, it follows that

$$\mathbb{Q}(\sqrt{-D}) \simeq \mathrm{End}^0(E_0) \simeq \mathrm{End}^0(E_0 \otimes \mathbb{F}_{q^n}) \simeq \mathrm{End}^0(E^\chi) \simeq \mathrm{End}^0(E),$$

which verifies the last condition of (vii).

Conversely, assume that there exists an ordinary abelian surface $A/\mathbb{F}_q$ which satisfies conditions $(vi)-(vii)$, for a given number $n = 3, 4$ or 6. From condition (vii), Theorem 2.3.5 is invoked to conclude that $\gcd(t, q) = 1$ and $c|t$, which fulfills conditions (iv) and (v). Furthermore, the last part of Theorem 2.3.5 shows that the characteristic polynomial $h_A(X)$ of $A/\mathbb{F}_q$ is given by (4.1.1). From condition (vi), we know that $ord_{\mathbb{F}_r^*}(q) = k$, which is condition (ii), and that $\#A(\mathbb{F}_q) = h_A(1) \equiv 0 \pmod{r}$. By using (4.1.5), we thus obtain condition (iii). It remains to show condition (i) holds. Since $A/\mathbb{F}_q$ is simple and ordinary and has the property that $A \otimes \mathbb{F}_{q^n} \sim E^2$, we

know by Theorem 2.3.3 (b) that $K = \mathbb{Q}[X]/(h_A(X))$ is biquadratic extension of $\mathbb{Q}$. Let $\alpha_1, \alpha_2 \in \mathbb{C}$ be two distinct roots of $h_A(X)$. If $\sigma \in Gal(K/\mathbb{Q})$ is chosen such that $\sigma(\alpha_1) = \alpha_2$, then from the last part of condition (vii) and the fact that $\mathrm{End}^0(E) \simeq \mathbb{Q}(\alpha_1^n)$ (i.e. $K_E = \mathbb{Q}(\pi_A^n)$ from (2.3.9)) we have

$$\mathrm{End}^0(\mathrm{E}) \simeq \mathbb{Q}(\alpha_1^{\mathrm{n}}) \simeq \mathrm{K}^\sigma \simeq \mathbb{Q}(\sqrt{-\mathrm{D}}).$$

Let $b := \alpha_1 + \alpha_2$, and observe that $\sigma(b) = b$. Hence, we have $b \in \mathbb{Q}(\sqrt{-D})$. Let $\eta \in Gal(K/\mathbb{Q})$ denotes the automorphism induced by complex conjugation. Recall the relation $\alpha_1 = \zeta_n \alpha_2$ from (2.3.11). Then we see that b and $\sigma(b)$ are roots of

$$X^2 - tX + cq, \tag{4.1.7}$$

because $b + \eta(b) = t$, $\zeta_n + \eta(\zeta_n) = c - 2$, and $b\eta(b) = cq$. This implies that $b \in \mathcal{O}_{\mathbb{Q}(\sqrt{-\mathcal{D}})}$. Note that the discriminant of b is $Disc(b) = t^2 - 4cq$ and so it follows that $t^2 - 4cq = (-D)x^2$ where $x = [\mathcal{O}_{\mathbb{Q}(\sqrt{-\mathcal{D}})} \colon \mathbb{Z}[b]]$. This verifies condition (i). □

The following important definition is motivated by the theorem above.

Definition 4.1.2. Let $c = \lfloor \frac{n}{2} \rfloor$ be as stated in Theorem 4.1.1 where $n = 3, 4, 6$. The conditions $(i) - (v)$ in Theorem 4.1.1 are referred to as the the list of desired conditions for a given n. An integer tuple (k, D, r, p, t) satisfying the list of desired conditions is said to be a *valid integer tuple for a given n*.

From Theorem 4.1.1, it is clear that once a valid integer tuple (k, D, r, q, t) for a given n is specified, then the characteristic polynomial $h_A(X)$ of an isogeny class of abelian surfaces $A/\mathbb{F}_q$ which satisfying conditions (vi) and (vii) of Theorem 4.1.1 is also determined. Hence with a valid integer tuple (k, D, r, q, t) for a given n it will be really interesting to see if there is a genus two curve $C/\mathbb{F}_q$ whose characteristic polynomial $h_{J_C}(X)$ of its Jacobian J_C matches the characteristic polynomial $h_A(X)$

of the isogeny class of abelian surfaces $A/\mathbb{F}_q$ determined by the valid integer tuple. The following section will be devoted to this investigation.

4.2 Curves given by valid integer tuples

In Section 4.1, it was shown that for a given $n = 3, 4, 6$ there is a one-to-one correspondence between the set of valid integer tuples (k, D, r, q, t) for the given n and the set of isogeny classes of $\mathbb{F}_q$-simple ordinary abelian surfaces $A/\mathbb{F}_q$ such that $A/\mathbb{F}_q$ satisfies the conditions (vi) and (vii). In this section, a result will be presented which specifies the conditions needed for a given valid integer tuple of a given $n = 3, 4, 6$ that leads to the construction of a Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_q$ or a non-trivial quadratic twist C^{χ}_{BFS} of it, and the construction of a Legendre-Satoh curve $C_{u,v}/\mathbb{F}_q$ such that the Jacobian is isogenous to the $\mathbb{F}_q$-simple ordinary abelian surface $A/\mathbb{F}_q$ induced by the given valid integer tuple respectively. The construction of these curves will be outlined in the proof of Theorem 4.2.3. Before we present the proof of Theorem 4.2.3, we need the following definition and a few notations.

Definition 4.2.1. Let $C_{u,v}/\mathbb{F}_q$ and $C_{BFC}/\mathbb{F}_q$ be Legendre-Satoh curve and Bolza-Freeman-Satoh curve defined in (3.3.25) and (3.4.32), respectively. Let $b \in (\mathbb{F}_q^{\times})\backslash(\mathbb{F}_q^{\times})^2$. Then the quadratic twists $C^{\chi}_{u,v}/\mathbb{F}_q$ and $C^{\chi}_{BFS}/\mathbb{F}_q$ of $C_{u,v}/\mathbb{F}_q$ and $C_{BFS}/\mathbb{F}_q$ by b are given by

$$\begin{aligned} C^{\chi}_{u,v}/\mathbb{F}_q: \quad Y^2 &= b^{-1}(X^5 + uX^3 + vX), \\ C^{\chi}_{BFS}/\mathbb{F}_q: \quad Y^2 &= b^{-1}(X^6 + uX^3 + v), \end{aligned}$$

respectively.

Remark 4.2.2. It is easy to see that the quadratic twists $J^{\chi}_{u,v}$ and $J^{\chi}_{C_{BFS}}$ of the Jacobians $J_{u,v}$ and $J_{C_{BFS}}$ are isogenous to the Jacobians of the quadratic twists $C^{\chi}_{u,v}/\mathbb{F}_q$ and $C^{\chi}_{BFS}/\mathbb{F}_q$ of $C_{u,v}/\mathbb{F}_q$ and $C_{BFS}/\mathbb{F}_q$, respectively. This follows from the general facts about a hyperelliptic curve $C/\mathbb{F}_q$ and its quadratic twist $C^{\chi}/\mathbb{F}_q$; namely the fact that, $tr_{J_C} = 1 + q - |C(\mathbb{F}_q)|$ and the fact that $|C(\mathbb{F}_q)| + C^{\chi}(\mathbb{F}_q) = 2q + 2$ (See p. 187 and p. 205 of [18]).

For what follows, we put $h_{-d}(X) := h_{\mathcal{O}_{-d}}(X)$ where $h_{\mathcal{O}_{-d}}(X)$ is the class polynomial associated with the order $\mathcal{O}_{-d} \subset \mathbb{Q}(\sqrt{-D})$ of discriminant $-d$ where $d > 0$. If $\mathrm{Pic}(\mathcal{O}_{-d}) = \{\mathfrak{a}_1, \cdots, \mathfrak{a}_h\}$, then it follows from Theorem 13.2 on page 286 of [9] that

$$h_{-d}(X) = \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)) \in \mathbb{Z}[X]$$

where $j(\mathfrak{a}_i)$ is the j-function on the ideal representative $\mathfrak{a}_i$ of $\mathcal{O}_{-d}$. Furthermore, if $p \in \mathbb{Z}^+$, then we define

$$h_{-d,p}(X) := h_{-d}(X) \pmod{p}.$$

Here we present the statement and the proof of Theorem 4.2.3.

Theorem 4.2.3. *Let (k, D, r, q, t) be a valid integer tuple for $n = 3, 4, 6$, respectively, where q is some power of an odd prime p. Let $A/\mathbb{F}_q$ be an ordinary abelian surface satisfying (vi) and (vii) of Theorem 4.1.1 which corresponds to the given valid integer tuple. Let $j \in \overline{\mathbb{F}_q}$ denote a root of $h_{-D,p}(X)$, and let the polynomial $g(X) \in \overline{\mathbb{F}_q}[X]$ be defined as follows.*

$$g(X) := \begin{cases} 2^8 3^3 (2X - 5)^3 - j(X - 2)(X + 2)^3, & \text{if } n = 3, 6, \\ 256(X + 1)^3 - j(X + 2), & \text{if } n = 4. \end{cases} \tag{4.2.8}$$

Suppose q and a root $a \in \overline{\mathbb{F}_q}$ of $g(X)$ satisfy the conditions outlined in the table below.

n	q	a
3	$q \equiv 1$ *(mod 3)*	$a \in (\mathbb{F}_q^{\times})\backslash\{\pm 2\}$
4	$q \equiv 1$ *(mod 4)*	$a \in \mathbb{F}_{q^4}\backslash\mathbb{F}_q$ *and* $\theta := \frac{2-a}{2a+12}$ *with* $\theta^2 \in \mathbb{F}_q$ *and* $\theta^{\frac{1}{4}} \notin \mathbb{F}_{q^4}$
6	$q \equiv 1$ *(mod 3),* $\frac{q+1}{2}$ *is odd*	$a \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ *with* $a^{\frac{1}{3}} \notin \mathbb{F}_{q^2}$ *and* $a^2 \in \mathbb{F}_q$

(4.2.9)

Then for $n = 3, 6$ there exists either a Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_q$ or a nontrivial quadratic twist $C_{BFS}^{\chi}/\mathbb{F}_q$ of it such that its Jacobian is isogenous to A. On the other hand, for $n = 4$ there exists a Legendre-Satoh curve $C_{u,v}/\mathbb{F}_q$ such that $J_{u,v} \sim A$.

Proof. We will present the proof in three steps.

Step 1: Show that there exists a root $j_o \in \mathbb{F}_{q^d}$ of $h_{-D,p}(X)$ where $d := \lfloor \frac{n+2}{3} \rfloor$.

By hypothesis, $A/\mathbb{F}_q$ is an ordinary abelian surface such that $A/\mathbb{F}_q$ has embedding degree k with respect to the prime r, and $A \otimes \mathbb{F}_{q^m}$ is simple for all $m|n$, $m \neq n$, and with the property that $A \otimes \mathbb{F}_{q^n} \sim E^2$ where $E/\mathbb{F}_{q^n}$ is an elliptic curve such that $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-D})$ and $D \nmid 12$. Furthermore, by Theorem 4.1.1 we also know that

$$(tr_A, s_A) = \left(t, \frac{t^2}{c} + (c-2)q\right). \tag{4.2.10}$$

It follows from $(iv)_n$ of Proposition 2.3.7 that there exists an elliptic curve $E_i/\mathbb{F}_{q^d}$ such that

$$\begin{cases} E_1 \otimes \mathbb{F}_{q^n} \sim E & \text{if } n = 3, 6 \\ E_0 \otimes \mathbb{F}_{q^n} \sim E^{\chi} & \text{if } n = 4 \end{cases}$$

where $i = 0, 1$ and $d = \lfloor \frac{n+2}{3} \rfloor$. Furthermore, by Remark 2.3.8 we know that

$$\begin{cases} tr_{E_1} = -\frac{t^d}{c} + 2(d-1) & \text{if } n = 3, 6 \\ tr_{E_0} = \frac{t^2}{2} - 2q & \text{if } n = 4 \end{cases}$$

where $c = \lfloor \frac{n}{2} \rfloor$. Since $A/\mathbb{F}_q$ is ordinary, so are $E/\mathbb{F}_{q^n}$, $E^\chi/\mathbb{F}_q$, and $E_i/\mathbb{F}_{q^d}$, and it follows that

$$\begin{cases} \mathrm{End}^0(E_1) \simeq \mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-D}) & \text{if } n = 3, 6 \\ \mathrm{End}^0(E_0) \simeq \mathrm{End}^0(E^\chi) \simeq \mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-D}) & \text{if } n = 4 \end{cases}$$

It follows from Corollary 18 of Kani [28] that there exists an elliptic curve

$$E_i'/\mathbb{F}_{q^d} \tag{4.2.11}$$

such that $E_i' \sim E_i$ with $\mathrm{End}(E_i') \simeq \mathcal{O}_{-D}$ where $\mathcal{O}_{-D}$ is the maximal order of $\mathbb{Q}(\sqrt{-D})$ where $i = 0, 1$ respectively. Note that $j(E_i') \neq 0$ or 1728. Indeed, since $E_i'/\mathbb{F}_{q^d}$ is also ordinary, and if $j(E_i') = 0$ or 1728, then we have $\mathrm{End}(E_i') \simeq \mathcal{O}_{-3}$ or $\mathcal{O}_{-4}$, respectively. This contradicts the hypothesis that $D \nmid 12$.

By the Deuring Lifting Theorem (Theorem 14 of [33]), there exists a number field $L/\mathbb{Q}$, a prime ideal $\mathcal{P}|p$ of L and an elliptic curve $\widetilde{E_i}'/L$ with good reduction at $\mathcal{P}$ such that $\widetilde{E_i}' \otimes \mathcal{O}_{-D}/\mathcal{P} \simeq E_i'$ and

$$\mathrm{End}(\widetilde{E_i}') \simeq \mathrm{End}(E_i') \simeq \mathcal{O}_{-D}. \tag{4.2.12}$$

Then by Theorem 12 of [33] we know that p splits completely in $\mathbb{Q}(\sqrt{-D})$ and hence

$$\left(\frac{-D}{p}\right) = 1.$$

It follows from page 339 of Silverman [46] that (4.2.12) is equivalent to

$$\widetilde{E_i}' \simeq \mathbb{C}/\mathfrak{a}$$

where $\mathfrak{a} \subset \mathcal{O}_{-D}$ is some invertible ideal. It then follows from Proposition 13.2 of [9] that $h_{-D}(j(\widetilde{E_i}')) = 0$. By taking $j_0 := j(\widetilde{E_i}') \pmod{\mathcal{P}}$, it follows from the fact that $j(\widetilde{E_i}') \equiv j(E_i') \pmod{\mathcal{P}}$ we have

$$h_{-D,p}(j_0) \equiv h_{-D,p}(j(E_i')) \equiv h_{-D}(j(\widetilde{E_i}')) \equiv 0 \pmod{\mathcal{P}}.$$

Step 2: Show that we can take $j_0 = j$ where $j_0 \in \mathbb{F}_{q^d}$ from Step 1 and $j \in \overline{\mathbb{F}_q}$ is as in the statement of theorem.

Given the ordinary elliptic curve $E_i'/\mathbb{F}_{q^d}$ from (4.2.11) of Step 1, it is well known (cf. equation (55) in Remark 22 of Kani [28]) that there exists precisely $h = \#\mathrm{Pic}(\mathcal{O}_{-D})$ many isomorphism classes of elliptic curves $E_{i,l}'/\mathbb{F}_{q^d}$ with $E_{i,l}' \sim E_i'$ and $\mathrm{End}(E_{i,l}') \simeq \mathcal{O}_{-D}$ where $1 \leq l \leq h$.

Similar to the second part of the proof in Step 1, by the Deuring Lifting Theorem (Theorem 14 of [33]), for every isomorphism class of elliptic curve $E_{i,l}'/\mathbb{F}_{q^d}$ mentioned above there exists a number field $L_{i,l}/\mathbb{Q}$, a prime ideal $\mathcal{P}_{i,l}|p$ of $L_{i,l}$ and an elliptic curve $\widetilde{E_{i,l}}'/L_{i,l}$ with good reduction at $\mathcal{P}_{i,l}$ such that $\widetilde{E_{i,l}}' \otimes \mathcal{O}_{-D}/\mathcal{P}_{i,l} \simeq E_{i,l}'$ and

$$\mathrm{End}(\widetilde{E_{i,l}}') \simeq \mathrm{End}(E_{i,l}') \simeq \mathcal{O}_{-D}. \tag{4.2.13}$$

Then by Theorem 12 of [33] we know that p splits completely in $\mathbb{Q}(\sqrt{-D})$ and

$$\left(\frac{-D}{p}\right) = 1.$$

It follows from page 339 of Silverman [46] that (4.2.13) is equivalent to

$$\widetilde{E_{i,l}}' \simeq \mathbb{C}/\mathfrak{a}_{i,l}$$

where $\mathfrak{a}_{i,l} \subset \mathcal{O}_{-D}$ is some invertible ideal. It then follows from Proposition 13.2 of [9] that $h_{-D}(j(\widetilde{E_{i,l}}')) = 0$ where $1 \leq l \leq h$. By the fact that $j(\widetilde{E_{i,l}}') \equiv j(E_{i,l}') \pmod{\mathcal{P}_{i,l}}$ and $j(E_{i,l}') \in \mathbb{F}_{q^d}$ we have

$$h_{-D,p}(X) = \prod_{l=1}^{h}(X - j(E_{i,l}'))$$

splits completely over $\mathbb{F}_{q^d}$ and so $j = j(E_{i,l}') = j_0$ for a suitable l. Note that by construction $E_{i,l}' \sim E_i'$.

Step 3: We show how to choose a Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_q$ or the twist of it for $n = 3, 6$ and a Legendre-Satoh curve $C_{u,v}/\mathbb{F}_q$ for $n = 4$ such that its

Jacobian is isogenous to A.

By the hypothesis that $a \in \overline{\mathbb{F}_q}$ is a root of $g(X)$ and the result of Step 2 that $j \in \mathbb{F}_{q^d}$ is a root of $h_{-D,p}(X)$, we obtain the relation

$$j = \begin{cases} 2^8 3^3 \frac{(5-2a)^3}{(2-a)(2+a)^3} & \text{if } n = 3, 6 \\ 256 \frac{(a+1)^3}{(a+2)} & \text{if } n = 4 \end{cases} \tag{4.2.14}$$

Next we define the coefficients u and v for a Legendre-Satoh curve $C_{u,v}$ and for a Bolza-Freeman-Satoh curve C_{BFS} according to the following rules.

n	u	v
3	$u \in \mathbb{F}_q^\times$	$(\frac{u}{a})^2$ where $(\frac{u}{a})^{\frac{1}{3}} \notin \mathbb{F}_q$
4	$u \in \mathbb{F}_q^\times$	$(u\theta)^2$
6	$u \in \mathbb{F}_q^\times$ such that $u^{\frac{1}{3}} \in \mathbb{F}_q^\times$	$(\frac{u}{a})^2$

(4.2.15)

By the conditions on $a, \theta \in \overline{\mathbb{F}_q}$ given in Table 4.2.9, we know that $u, v \in \mathbb{F}_q^\times$.

For $n = 3, 6$, it follows from the construction of $u, v \in \mathbb{F}_q^\times$ above and $a \neq \pm 2$ that $u^2 - 4v = u^2(1 - \frac{4}{a^2}) \neq 0$. Hence the Bolza-Freeman-Satoh curve C_{BFS} defined by the coefficients $u, v \in \mathbb{F}_q^\times$ outlined above is indeed a genus two curve by the definition (3.4.32). It follows from Corollary 3.4.3 (a) that $J_{C_{BFS}} \otimes \mathbb{F}_{q^6} \sim (E_a \otimes \mathbb{F}_{q^6})^2$ where $E_a/\mathbb{F}_{q^d}$ is the elliptic curve defined in (3.4.36) with j-invariant

$$j(E_a) = 2^8 3^3 \frac{(5-2a)^3}{(2-a)(2+a)^3}. \tag{4.2.16}$$

Hence, from (4.2.14), (4.2.16), Step 1, and Step 2 we know that

$$j = j(E_1') = j(E_a) \notin \{0, 1728\}.$$

It then follows from Lemma VIII.3 of Black, Seroussi, Smart [2] (page 153) that $E_1'/\mathbb{F}_{q^d}$ and $E_a/\mathbb{F}_{q^d}$ are either isomorphic or they are quadratic twists of each other.

Thus, by the proof of Step 1 we have

$$tr_{E_a} = \pm tr_{E_1'} = \pm tr_{E_1} = \pm\left(-\frac{t^d}{c} + 2(d-1)q\right)$$

where $c = \lfloor \frac{n}{2} \rfloor$, and $E_a/\mathbb{F}_{q^d}$ is also ordinary. By the proof of Step 1, we then have

$$\mathrm{End}^0(E_a) \simeq \mathrm{End}^0(E_1') \simeq \mathrm{End}^0(E_1) \simeq \mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-D}),$$

where $D \neq 3$ since $D \nmid 12$.

In the particular case that $n = 3$, we note that $v \in (\mathbb{F}_q^\times)^2 \backslash (\mathbb{F}_q^\times)^6$ by construction. Since $q \equiv 1 \pmod 3$, $E_a/\mathbb{F}_q$ is ordinary with $\mathrm{End}^0(E_a) \not\simeq \mathbb{Q}(\sqrt{-3})$, and $v \in (\mathbb{F}_q^\times)^2 \backslash (\mathbb{F}_q^\times)^6$, it follows from Corollary 3.4.6 (a) that $J_{C_{BFS}}$ is $\mathbb{F}_q$-simple and

$$(tr_{J_{C_{BFS}}}, S_{J_{C_{BFS}}}) = (\pm tr_{E_a}, tr_{E_a}^2 - q) = (\pm t, t^2 - q) = (\pm tr_A, s_A),$$

where the last equality comes from (4.2.10). If $(tr_{J_{C_{BFS}}}, S_{J_{C_{BFS}}}) = (t, t^2 - q)$, then the Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_q$ defined with coefficients $u, v \in \mathbb{F}_q$ specified by Table 4.2.15 will be the desired curve. Otherwise, by Remark 4.2.2 the nontrivial quadratic twist C_{BFS}^χ of C_{BFS} will be the desired curve.

In the particular case of $n = 6$, we observe that $v \notin (\mathbb{F}_q^\times)^2$ since $u \in \mathbb{F}_q^\times$ and $a \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. On the other hand, we have $v \notin (\mathbb{F}_q^\times)^3$. Indeed, if $v \in (\mathbb{F}_q^\times)^3$, then by the construction of v it follows that $v = \frac{u^2}{a^2} \in (\mathbb{F}_q^\times)^3$. Since $u^2 \in (\mathbb{F}_q^\times)^3$, it follows that $a^2 \in (\mathbb{F}_q^\times)^3$ and that hence $a \in (\mathbb{F}_{q^2}^\times)^3$, contradiction.Thus $v \notin (\mathbb{F}_q^\times)^2 \cup (\mathbb{F}_q^\times)^3$. Since q is an odd prime power such that $q \equiv 1 \pmod 3$ and $\frac{q+1}{2}$ is odd, and $E_a/\mathbb{F}_{q^2}$ is ordinary with $\mathrm{End}^0(E_a) \not\simeq \mathbb{Q}(\sqrt{-3})$, it follows from Corollary 3.4.6 (b) that $J_{C_{BFS}} \otimes \mathbb{F}_{q^m}$ is simple for all $m|6$ but $m \neq 6$ and

$$(tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) = (\pm t, \frac{t^3}{3} + q) = (\pm tr_A, s_A)$$

where the last equality comes from (4.2.10). Similarly, if $(tr_{J_{C_{BFS}}}, s_{J_{C_{BFS}}}) = (t, \frac{t^3}{3} + q)$, then the Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_q$ defined with coefficients $u, v \in \mathbb{F}_q$

specified by Table 4.2.15 will be the desired curve. Otherwise, by Remark 4.2.2 the nontrivial quadratic twist C_{BFS}^{χ} of C_{BFS} will be the desired curve.

For $n = 4$, we first observe that $\theta \neq \pm 2^{-1} \in \mathbb{F}_q$. If $\theta = 2^{-1}$ or -2^{-1} in $\mathbb{F}_q$, then by the construction of θ in (4.2.9) we will have $a = -2$ or 2, respectively. This is clearly a contradiction since $a \in \mathbb{F}_{q^4} \backslash \mathbb{F}_q$. Hence it follows from the construction of $u, v \in \mathbb{F}_q^{\times}$ stated in Table 4.2.15 that $v \neq 0$ and $u^2 - 4v = u^2(1 - 4\theta^2) \neq 0$. We then know that the Legendre-Satoh curve $C_{u,v}$ defined by $u, v \in \mathbb{F}_q^{\times}$ outlined above is indeed a genus two curve by the definition (3.3.25).

Since $\theta = \frac{2-a}{2a+12}$ with $\theta^2 \in \mathbb{F}_q$, it follows that $(4\theta^2-1)a^2-(48\theta^2-4)a+(144\theta^2-4) = 0$ and hence $a \in \mathbb{F}_{q^2}$. We also observe that

$$\gamma := 2\frac{u - 6(u\theta)}{u + 2(u\theta)} = 2\frac{1 - 6\theta}{1 + 2\theta} = 2\frac{1 - 6\left(\frac{2-a}{2a+12}\right)}{1 + 2\left(\frac{2-a}{2a+12}\right)} = a,$$

and hence we can define an elliptic curve $E_{u,v}/\mathbb{F}_{q^2}$ as in (3.3.28) with j-invairant

$$j(E_{u,v}) = 256\frac{(a+1)^3}{a+2}. \tag{4.2.17}$$

Hence, from (4.2.14), (4.2.17), Step 1, and Step 2 we know that

$$j = j(E_0') = j(E_{u,v}) \notin \{0, 1728\}.$$

It then follows from Lemma VIII.3 of Black, Seroussi, Smart [2] (page 153) that $E_0'/\mathbb{F}_{q^2}$ and $E_{u,v}/\mathbb{F}_{q^2}$ are either isomorphic or they are quadratic twists of each other. Thus, by the proof of Step 1 we have

$$tr_{E_{u,v}} = \pm tr_{E_0'} = \pm tr_{E_0} = \pm\left(\frac{t^2}{2} - 2q\right), \tag{4.2.18}$$

and $E_{u,v}/\mathbb{F}_{q^2}$ is also ordinary. On the other hand, by the proof of part (a) we then have

$$\mathrm{End}^0(E_{u,v}) \simeq \mathrm{End}^0(E_0') \simeq \mathrm{End}^0(E_0) \simeq \mathrm{End}^0(E^{\chi}) \simeq \mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-D})$$

where $D \neq 1$ since $D \nmid 12$.

We also note that $v \notin (\mathbb{F}_q^\times)^2$. Indeed, if $v \in (\mathbb{F}_q^\times)^2$, then by construction $\theta \in \mathbb{F}_q^\times$. Hence it follows that $\theta^{\frac{1}{4}} \in \mathbb{F}_{q^4}^\times$, which is a contradition. Since $v \notin (\mathbb{F}_q^\times)^2$, we have $v \notin (\mathbb{F}_q^\times)^4$. Since $q \equiv 1 \pmod 4$, $v \notin (\mathbb{F}_q^\times)^4$, and $E_{u,v}/\mathbb{F}_{q^2}$ is ordinary with $\mathrm{End}^0(E_{u,v}) \not\simeq \mathbb{Q}(i)$, it follows from Corollary 3.3.5 that $J_{u,v}/\mathbb{F}_q$ is simple. Furthermore, we observe that

$$4q \pm 2tr_{E_{u,v}} = 4q \pm tr_{E_0'} = \begin{cases} t^2 \\ \\ 8q - t^2 = x^2 D \end{cases}$$

and exactly one of the above is a square. It follows from (4.2.10) and Theorem 3.3.3 (b) that $J_{u,v} \otimes \mathbb{F}_{q^2}$ is also simple and with

$$(tr_{J_{u,v}}, s_{J_{u,v}}) = \left(\pm t, \frac{t^2}{2}\right) = (\pm tr_A, s_A).$$

Similarly, if $(tr_{J_{u,v}}, S_{J_{u,v}}) = (t, \frac{t^2}{2})$, then the Legendre-Satoh curve $C_{u,v}/\mathbb{F}_q$ defined with coefficients $u, v \in \mathbb{F}_q$ specified by Table 4.2.15 will be the desired curve. Otherwise, by Remark 4.2.2 the nontrivial quadratic twist $C_{u,v}^\chi$ of $C_{u,v}$ will be the desired curve. Note that by [7], Remark 34 (a), this twist is again an Legendre-Satoh curve, and so the assertion follows. □

Remark 4.2.4. The proof of Steps 1 and 2 of the above theorem shows that if (k, D, r, q, t) is a valid integer tuple for n and q is a power of p, then $h_{-D,p}(X)$ splits completely over $\mathbb{F}_{q^d}$, where $d = [\frac{n+2}{3}]$.

If a given valid integer tuple (k, D, r, q, t) for $n = 3, 4, 6$ satisfies the hypotheses stated in the above theorem, then as was shown in the proof of the above theorem we can construct a Legendre-Satoh curve $C_{u,v}/\mathbb{F}_q$, and a Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_q$ or a nontrivial quadratic twist $C_{BFS}^\chi/\mathbb{F}_q$ of it such that $J_{u,v} \sim A$, and $J_{C_{BFS}} \sim A$ or $J_{C_{BFS}^\chi} \sim A$ respectively, where $A/\mathbb{F}_q$ is the abelian surface induced by

the given valid integer tuple. Hence the Jacobian $J_{u,v}$ and $J_{C_{BFS}}$ (or $J_{C^{\chi}_{BFS}}$) will have the desired specified embedding degrees k with respect to the specified primes r, and will have the desired minimal splitting property as the associated $A/\mathbb{F}_q$. It will be the interest of the next chapters to search for valid integer tuples (k, D, r, q, t) for a given $n \in \{3, 4, 6\}$, and in particular, to search for those tuples that satisfy the additional hypotheses of Theorem 4.2.3.

Chapter 5

Method I

Given $n \in \{3, 4, 6\}$, put $c := \lfloor \frac{n}{2} \rfloor$ as in Theorem 4.1.1. Let $k, D \in \mathbb{N}$ where $D \nmid 12$ and $-D$ is a fundamental discriminant. The main focus of this chapter is to present a method on searching for an integer t, a prime r, and a prime power q such that (k, D, r, q, t) is a valid integer tuple for the given n and such that it satisfies the hypotheses of Theorem 4.2.3. Furthermore, the method presented in this chapter will lead to the constructions of Legendre-Satoh curves and Bolza-Freeman-Satoh curves whose Jacobians are isogenous to the abelian surfaces induced by the valid integer tuple (k, D, r, q, t). The main ideas of this method will be presented in Section 5.1, while the implementation of this method will be presented in Section 5.2.

5.1 Main ideas

The following conjecture is due to Bouniakowsky [5] and Schinzel [44].

Conjecture 5.1.1. *If $f(X) \in \mathbb{Z}[X]$ is a non-constant polynomial such that $f(X)$ has a positive leading coefficient, $f(X)$ is irreducible over $\mathbb{Z}$, and* $\gcd(\{f(x_1) : x_1 \in$

$\mathbb{Z}^+\}) = 1$, *then* $f(z)$ *will take infinitely many prime values for all* $z \in \mathbb{Z}^+$.

If a non-constant polynomial $f(X) \in \mathbb{Z}[X]$ satisfies the conditions specified in the above conjecture, then the polynomial $f(X)$ is said to *represent primes*. An example of a non-constant polynomial that represents primes is the kth cyclotomic polynomial $\Phi_k(X) \in \mathbb{Z}[X]$ when $k > 1$. Indeed, it is monic and irreducible over $\mathbb{Z}$, as is well-known. Furthermore, by the fact that $\Phi_k(1) = p$ if $k = p^m$ and otherwise $\Phi_k(1) = 1$, where p is a prime and $m \in \mathbb{N}$ (See Theorem 1.4 of [50]), it follows that $\gcd(\{\Phi_k(x_1) : x_1 \in \mathbb{Z}^+\}) = 1$.

Recall from Proposition 2.2.2 that if $r \in \mathbb{N}$ is a prime and $k \in \mathbb{N}$ such that $r \nmid k$, then $\Phi_k(a) \equiv 0 \pmod{r}$ if and only if $ord_{\mathbb{F}_r^\times}(a) = k$ for some $a \in \mathbb{Z}$. This implies that if $\Phi_k(a) \equiv 0 \pmod{r}$ for some $a \in \mathbb{Z}$ then $\Phi_i(a) \not\equiv 0 \pmod{r}$ for integer $0 < i < k$. This observation is important to a theorem later and hence is formulated as a lemma below.

Lemma 5.1.2. *Let* r *be a prime,* $k \in \mathbb{N}$ *such that* $r \nmid k$ *and* $a \in \mathbb{Z}$. *If* $\Phi_k(a) \equiv 0$ *(mod* r*) then* $\Phi_i(a) \not\equiv 0$ *(mod* r*) for all* $0 < i < k$.

If a valid integer tuple (k, D, r, q, t) for some $n \in \{3, 4, 6\}$ is given, then the following proposition shows that a certain congruence equation mod D is solvable.

Proposition 5.1.3. *Let* $n = 3, 4,$ *or* 6 *and put* $c := \lfloor \frac{n}{2} \rfloor$. *If* (k, D, r, q, t) *is a valid integer tuple for* n, *then the following congruence equation is solvable in* $\mathbb{Z}/D\mathbb{Z}$

$$AX \equiv (C - B) \pmod{D}, \tag{5.1.1}$$

where

$$A := 4cnr, \quad B := 4c\overline{q}, \quad \text{and} \quad C := t^2 \tag{5.1.2}$$

with $\overline{q} \equiv q \pmod{nr}$.

Proof. Since (k, D, r, q, t) is a valid integer tuple, it follows from the definition that

$$4cq = t^2 + x^2 D \tag{5.1.3}$$

for some $x \in \mathbb{Z}$. Next we express the integer parameter q as follows

$$q = m(nr) + \overline{q} \tag{5.1.4}$$

via the division algorithm where $m \in \mathbb{Z}$ and $0 \leq \overline{q} < nr$. By a substitution of the expression of q from (5.1.4) into equation (5.1.3), it follows that

$$Am = C - B + Dx^2$$

which gives $Am \equiv (C - B)$ (mod D). Hence equation (5.1.1) is solvable in $\mathbb{Z}/D\mathbb{Z}$ for $X \equiv m \pmod{D}$. □

The proposition above suggests that, during the process of searching for valid integer tuples, we will only be interested in candidate integer tuples (k, D, r, q, t) for $n \in \{3, 4, 6\}$ such that the congruence equation (5.1.1) is solvable in $\mathbb{Z}/D\mathbb{Z}$. The following theorem, which makes use of the primes represented by cyclotomic polynomials and which exploits special cases of the solvability of congruence equation (5.1.1), will play an important role later in the search of valid integer tuples that lead to desired Legendre-Satoh curves and Bolza-Freeman-Satoh curves.

Theorem 5.1.4. *Let $n = 3, 4, 6$ and put $c := \lfloor \frac{n}{2} \rfloor$. Let $k, D \in \mathbb{N}$ be such that $D \nmid 12$ and $-D$ is a fundamental discriminant. Suppose that $r > 13$ is a prime represented by the kth cyclotomic polynomial $\Phi_k(X)$; that is, $r := \Phi_k(l) > 13$ is a prime for some $l \in \mathbb{Z}^+$. Furthermore, suppose that $r \nmid k$ and that $r \equiv 1$ (mod $lcm(k, n)$).*

(a) There exists an integer $t \in \mathbb{Z}^+$ *with*

$$t \equiv \begin{cases} 2 \ (mod\ 3) & \text{if } n = 3 \\ 0 \ (mod\ 2) & \text{if } n = 4 \\ 0 \ (mod\ 6) & \text{if } n = 6 \end{cases} \tag{5.1.5}$$

and an integer $0 \leq \overline{q} < nr$ *with*

$$\begin{cases} \overline{q} \equiv l \ (mod\, r), \\ \overline{q} \equiv 1 \ (mod\, n), \end{cases} \tag{5.1.6}$$

such that the integers $t, \overline{q} \in \mathbb{Z}$ *satisfy the relation*

$$t^2 - c(\overline{q}+1)t + c(\overline{q}^2 + (c-2)\overline{q} + 1) \equiv 0 \ (mod\ r). \tag{5.1.7}$$

(b) Let the integers $t, \overline{q} \in \mathbb{Z}$ *be as in part (a). We set*

$$A := 4cnr, \quad B := 4c\overline{q}, \quad \text{and} \quad C := t^2. \tag{5.1.8}$$

If $\gcd(A, D) = 1$*, then the integers* $m_0, z_0 \in \mathbb{Z}$ *are defined by*

$$m_0 := (C - B)A^{-1} \ (mod\ D), \quad z_0 := \frac{Am_0 + B - C}{D}.$$

If $\gcd(A, D) \neq 1$ *and* $D|(B - C)$*, then the integers* $m_0, z_0 \in \mathbb{Z}$ *are defined by*

$$m_0 := 0, \quad z_0 := \frac{B - C}{D}.$$

Furthermore, the integer q_0 *is defined by*

$$q_0 := nm_0r + \overline{q},$$

and for each $i \in \mathbb{N}$ *the integers* $m_i, z_i, q_i \in \mathbb{Z}$ *are defined by*

$$m_i := m_0 + iD, \quad z_i := z_0 + iA, \quad \text{and} \quad q_i := nm_ir + \overline{q}. \tag{5.1.9}$$

If, for some $i \in \mathbb{N}$*, the integers* z_i *and* q_i *defined above satisfy the following constraints*

(i) $z_i = x^2$ *for some* $x \in \mathbb{Z}$*.*

(ii) q_i *is a prime power with* $\gcd(q_i, t) = 1$*,*

then the integer tuple (k, D, r, q_i, t) *is a valid integer tuple.*

Proof. (a) We note that $\gcd(r, n) = 1$ since $r = \Phi_k(l) > 13$ is a prime. By the Chinese Reminder Theorem, there exists an integer $0 \leq \overline{q} < nr$ such that

$$\begin{cases} \overline{q} \equiv l \pmod{r}, \\ \overline{q} \equiv 1 \pmod{n}, \end{cases} \tag{5.1.10}$$

which fulfills condition (5.1.6). For $n = 3, 4, 6$ we consider the following polynomials modulo r

$$g_n(T) := \begin{cases} 9T^2 - (9 + 3l)T + (l^2 + 3), & \text{if } n = 3, \\ 4T^2 - 4(l + 1)T + 2(l^2 + 1), & \text{if } n = 4, \\ 36T^2 - 18(l + 1)T + 3(l^2 + l + 1) & \text{if } n = 6, \end{cases} \tag{5.1.11}$$

and observe that for $n = 3, 4, 6$ the discriminants of $g_n(T)$ are $-3^3(l+1)^2$, $-2^4(l-1)^2$, and $-2^2 3^3 (l-1)^2$ respectively. Since $r \equiv 1 \pmod{n}$, it follows that the discriminants of $g_n(T)$ are all squares in $\mathbb{F}_r$ and hence $g_n(T)$ splits over $\mathbb{F}_r$. To choose the appropriate integer $t \neq 0$, we proceed by distinguishing different cases. For $n = 3$, let $\alpha \in \mathbb{Z}$ be such that $-\frac{r}{2} \leq \alpha \leq \frac{r}{2}$ is a root of $g_3(T) \in \mathbb{F}_r[T]$ and put

$$t := 3\alpha - 1.$$

It follows that $t \neq 0$ since $\alpha \in \mathbb{Z}$. For $n = 4, 6$, we observe that $g_n(T)$ has a zero root in $\mathbb{F}_r$ if and only if

$$\Phi_4(l) = l^2 + 1 \equiv 0 \pmod{r} \text{ if } n = 4 \text{ and } \Phi_3(l) = l^2 + l + 1 \equiv 0 \pmod{r} \text{ if } n = 6. \tag{5.1.12}$$

If this is the case, then the other root of $g_n(T)$ in $\mathbb{F}_r$ must be

$$(l + 1)4^{-1} \text{ if } n = 4, \text{ and } (l + 1)2^{-1} \text{ if } n = 6,$$

respectively. Hence the other root of $g_n(T)$ for $n = 4, 6$ in $\mathbb{F}_r$ is also zero if and only

if

$$\Phi_2(l) = l + 1 \equiv 0 \pmod{r}. \tag{5.1.13}$$

From the hypothesis that $\Phi_k(l) \equiv 0 \pmod{r}$ and Lemma 5.1.2, it follows from (5.1.12) and (5.1.13) that there must exist a nonzero root of $g_n(T)$ in $\mathbb{F}_r$. Let an integer $\alpha \neq 0$ be such that $-\frac{r}{2} \leq \alpha \leq \frac{r}{2}$ and $g_n(\alpha) \equiv 0 \pmod{r}$. We then define the following nonzero values of t

$$t := 2\alpha, \quad \text{if } n = 4, \ \ \textit{and} \ \ t := 6\alpha, \quad \text{if } n = 6.$$

Note that the choices of t defined above for $n = 3, 4, 6$ have fulfilled the condition (5.1.5). Finally, it follows from the construction of $\overline{q}, t \in \mathbb{Z}$ that

$$\begin{aligned}
& t^2 - c(\overline{q}+1)t + c(\overline{q}^2 + (c-2)\overline{q} + 1) \\
\equiv & \begin{cases} 9\alpha^2 - 3(l+3)\alpha + (l^2+3) & (\text{mod } r) \quad \text{if } n = 3 \\ 4\alpha^2 - 4(l+1)\alpha + 2(l^2+1) & (\text{mod } r) \quad \text{if } n = 4 \\ 36\alpha^2 - 18(l+1)\alpha + 3(l^2+l+1) & (\text{mod } r) \quad \text{if } n = 6 \end{cases} \\
\equiv & \ g_n(\alpha) \qquad\qquad\qquad\qquad\qquad\qquad (\text{mod } r) \\
\equiv & \ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{mod } r)
\end{aligned}$$

Hence by the construction the integers $t, \overline{q} \in \mathbb{Z}$ satisfy the listed conditions.

(b) Let $t, \overline{q} \in \mathbb{Z}$ be the integers given in part (a). We put integer parameters A, B, C, z_i, m_i, and q_i accordingly. Suppose that for some $i \in \mathbb{N}$ the integer z_i and q_i satisfy listed constraints (i) and (ii). By the properties of $t \in \mathbb{Z}$ from part (a) and the definition and hypothesis of q_i, it follows that $c|t$ and that $q_i \equiv \overline{q} \pmod{r}$; thus,

$$\begin{aligned}
& t^2 - c(q_i+1)t + c(q_i^2 + (c-2)q_i + 1) \\
\equiv & \ t^2 - c(\overline{q}+1)t + c(\overline{q}^2 + (c-2)\overline{q} + 1) \qquad (\text{mod } r) \\
\equiv & \ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{mod } r),
\end{aligned}$$

and also q_i and t fulfill the desired conditions (iii) and (v) of Theorem 4.1.1. Since

$q_i \equiv \bar{q} \pmod{r}$, it also follows that

$$\begin{aligned} \Phi_k(q_i) &\equiv \Phi_k(\bar{q}) \pmod{r} \\ &\equiv \Phi_k(l) \pmod{r} \\ &\equiv 0 \pmod{r}. \end{aligned}$$

Since $r \nmid k$, we know that $ord_{\mathbb{F}_q^\times}(q_i) = k$ from Proposition 2.2.2, which fulfills the desired condition (ii) of Theorem 4.1.1. By the construction of the parameters A, B, C, and D, m_0, and z_0, these integer parameters satisfy the relation

$$Am_0 + B - C = z_0 D.$$

It follows from the construction of $m_i, z_i \in \mathbb{Z}$ and the hypothesis on z_i that

$$\begin{aligned} Am_i + B - C &= Am_0 + iAD + B - C \\ &= z_0 D + iAD \\ &= z_i D = x^2 D \end{aligned}$$

where $x \in \mathbb{Z}$. On the other hand, these integer parameters satisfy

$$\begin{aligned} Am_i + B - C &= 4cnrm_i + 4c\bar{q} - t^2 \\ &= 4c(nrm_i + \bar{q}) - t^2 \\ &= 4cq_i - t^2 \end{aligned}$$

by (5.1.8) and (5.1.9). We thus have that $4cq_i = t^2 + x^2 D$ fulfills the desired condition (i) of Theorem 4.1.1. Since $\gcd(t, q_i) = 1$ it then follows that (k, D, r, q_i, t) is a valid integer tuple. □

Remark 5.1.5. (a) Note that (5.1.9) and (5.1.10) show that the prime power q_i of the valid integer tuple (k, D, r, q_i, t) for $n = 3, 4, 6$, which is constructed by Theorem 5.1.4, has the property that $q_i \equiv 1 \pmod{\text{n}}$.

(b) If we are only interested in the case that q_i is a prime in place of a prime power, then we can replace condition (ii) by the stronger condition

(ii)' q_i is a prime with $q_i > 4c$.

To see that this implies (ii), note that since $4cq_i = t^2 + x^2D$, it follows from (ii)' that $t^2 \leq 4cq_i < q_i^2$, and so $|t| < q_i$. But since q_i is prime and $t \neq 0$ by part (a) we see that $\gcd(t, q_i) = 1$, and so (ii) holds.

In fact, Theorem 5.1.4 together with Remark 5.1.5 (b) gives rise to a method of searching for valid integer tuples (k, D, r, p, t) that satisfy the hypotheses of Theorem 4.2.3 where p is a prime. This method will be described in the following section.

5.2 Method I

Fix $n = 3, 4, 6$, and $k, D \in \mathbb{N}$. The purpose of this section is to present a method for searching for an integer t, a prime r, and a prime p, such that (k, D, r, p, t) is a valid integer tuple for the given n. Furthermore, once such a valid integer tuple is found, it will also satisfy the hypotheses of Theorem 4.2.3 which in turn gives Legendre-Satoh curves and Bolza-Freeman-Satoh curves whose Jacobians are isogenous to the ordinary abelian sufaces associated to the valid integer tuple. This method consists of several procedures which are based on Theorem 5.1.4 and Theorem 4.2.3 and will be presented in the form of pseudo codes.

The following procedure called **NumerateRightR** initializes appropriate parameters based on Theorem 5.1.4 and plays an important part in Method I. The basic idea is to specify an upper bound $m \in \mathbb{N}$ and search for some suitable prime $r := \Phi_k(l)$ where $1 \leq l \leq m$.

NumerateRightR:

Input: $n, k, m, D \in \mathbb{N}$ where $n = 3, 4, 6$ and $D \nmid 12$ with $-D$ a fundamental discriminant.

Output: A table of integer tuples $(l, r, \overline{p}, t, m_0, z_0, A, B, C) \in \mathbb{Z}^9$ where

(1) $r := \Phi_k(l) > 13$ is a prime with $1 \leq l \leq m$ and $r \equiv 1 \pmod{\text{lcm}(n, k)}$

(2) $\overline{p} \in \mathbb{Z}$ where $0 \leq \overline{p} \leq nr$ such that $\overline{p}$, l and r it satisfies the congruence relation (5.1.6)

(3) $t \in \mathbb{Z}$ satisfies the congruence relation (5.1.5) and together with $\overline{p}$ and r it satisfies

the congruence relation stated in (5.1.7)

(4) $A = 4cnr$, $B = 4c\overline{p}$, and $C = t^2$, where $c = \lfloor \frac{n}{2} \rfloor$

(5) $z_0, m_0 \in \mathbb{Z}$ such that $Am_0 + B - C = z_0 D$.

Let R be an empty table.

For what follows, we will loop over $l \in \mathbb{Z}$ such that $1 \leq l \leq m$.

Step 1: We set $r := \Phi_k(l)$.

If $r > 13$ is prime and $r \equiv 1 \pmod{\text{lcm}(k, n)}$, then go to Step 2. Otherwise, go to the next l.

Step2: Compute $\overline{p} \in \mathbb{Z}$ where $0 \leq \overline{p} \leq nr$ such that it satisfies the congruence relation (5.1.6) via the Chinese Remainder Theorem. Compute two integers α_i where

$i = 1, 2$ such that $-\frac{r}{2} < \alpha_i < \frac{r}{2}$ and $g_n(\alpha_i) \equiv 0 \pmod{r}$, where $g_n(T)$ is defined in

(5.1.11). For each of the two integers α_i, $i = 1, 2$, set the following quantities

$$A := 4cnr,\ B := 4c\overline{p},\ \text{ and }\ C_i := t_i^2$$

where

$$t_i := \begin{cases} 3\alpha_i - 1 & \text{if } n = 3 \\ 2\alpha_i & \text{if } n = 4 \\ 6\alpha_i & \text{if } n = 6. \end{cases}$$

Step 3: For both tuples (A, B, C_i) from Step 2, we do the following.

If $\gcd(A, D) = 1$, then

compute $m_{0,i} := (C_i - B)A^{-1} \pmod{D}$ and $z_{0,i} := \frac{Am_{0,i}+B-C_i}{D} \in \mathbb{Z}$.

Go to Step 4.

If $\gcd(A, D) \neq 1$ and $D|(B - C_i)$ then

set $m_{0,i} := 0$ and $z_{0,i} := \frac{B-C_i}{D} \in \mathbb{Z}$.

Go to Step 4.

If both tuples (A, B, C_i) from Step 2 are such that

$$\gcd(A, D) \neq 1 \text{ and } (\gcd(A, D) = 1 \text{ or } D \nmid (B - C_i))$$

then

go to the next l.

Step 4: If $z_{0,i} \in (\mathbb{Z}/4cn\mathbb{Z})^2$ and if the Legendre symbol $(\frac{z_{0,i}}{r}) = 1$, then

set $m_0 := m_{0,i}$, $z_0 := z_{0,i}$, and $C := C_i$, and add $(l, r, \overline{p}, t, m_0, z_0, A, B, C)$ to R.

else go to the next l.

Step 5: Return R.

The following procedure called **CurveConstruct** is a probabilistic algorithm that searches for Legendre-Satoh curves and Bolza-Freeman-Satoh curves based on Theorem 4.2.3. The input class polynomial $h_{-D}(X)$ of **CurveConstruct** can be precomputed via the command HilbertClassPolynomial in Magma.

CurveConstruct:

Input: A tuple $(k, D, r, p, t, h_{-D}(X))$ where (k, D, r, p, t) is a valid integer tuple for a fixed $n = 3, 4, 6$ and $h_{-D}(X) \in \mathbb{Z}[X]$ is the class polynomial associated to a fundamental discriminant $-D$.

Output: A table of Legendre-Satoh curves $C_{u,v}/\mathbb{F}_p$ if $n = 4$, or a table of Bolza-Freeman-Satoh curves $C_{BFS}/\mathbb{F}_p$ if $n = 3, 6$ which have the property that their Jacobians are isogenous to the ordinary abelian surfaces associated to the input valid integer tuple. Or, 'Fail' if

(1) The prime p satisfies the conditions

$$\begin{cases} p \equiv 2 \pmod 3 & \text{if } n = 3 \\ p \equiv 3 \pmod 4 & \text{if } n = 4 \\ p \equiv 2 \pmod 3 \text{ or } p \equiv 3 \pmod 4 & \text{if } n = 6, \end{cases}$$

(2) A random point P on the Jacobian of the curve constructed has the property that $\gcd(h, h^\chi)P = 0$, where $h = 1 - t + (\frac{t^2}{c} + (c-2)p) - tp + p^2$ and $h^\chi = 1 + t + (\frac{t^2}{c} + (c-2)p) + tp + p^2$ (Such curves are cryptographically uninteresting; cf. Remark 5.2.1).

Let S be the empty table.

Step 1: If $n = 3$ and $p \equiv 2 \pmod 3$, then return Fail

elif $n = 4$ and $p \equiv 3 \pmod 4$ then return Fail

elif $n = 6$ and ($p \equiv 2 \pmod 3$ or $p \equiv 3 \pmod 4$) then return Fail

else go to Step 2.

Step 2: Compute the set $J := \{j \in \mathbb{F}_{p^n} |\ h_{-D}(j) \equiv 0 \pmod p\}$.

In what follows, we will loop over $j \in J$.

Step 3: Define $g_j(X) \in \mathbb{F}_{p^n}[X]$ as indicated in (4.2.8). Compute the set

$G_j := \{a \in \mathbb{F}_{p^n} \mid g_j(a) = 0\}$. If $G_j = \emptyset$, then go to the next $j \in J$, else go to Step 4.

For what follows, we will loop over $a \in G_j$.

Step 4: If $n = 3$ and ($a \in G_j$ such that $a \neq \pm 2$) then

Define a Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_p$ with coefficients

$u, v \in \mathbb{F}_p$ such that $u \in \mathbb{F}_p^\times$ is chosen at random with the property that

$(\frac{u}{a}) \notin (\mathbb{F}_p^\times)^3$ and put $v := (\frac{u}{a})^2$. Go to Step 5.

elif $n = 4$ and ($a \in G_j$ such that $a \notin \mathbb{F}_p$, $2a + 12 \neq 0$) then

Define $\theta := \frac{2-a}{2a+12}$.

If $\theta^2 \in \mathbb{F}_p$ and $\theta^{\frac{1}{4}} \notin \mathbb{F}_{p^4}$ then

Define a Legendre-Satoh curve $C_{u,v}/\mathbb{F}_p$ where $u \in \mathbb{F}_p^\times$ is chosen

at random and put $v := (u\theta)^2$. Go to Step 5.

else

go to the next $a \in G_j$.

elif $n = 6$ and ($a \in G_j$ such that $a \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ with $a \notin (\mathbb{F}_{p^2})^3$ and $a^2 \in \mathbb{F}_p$) then

Define a Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_p$ with coefficients

$u, v \in \mathbb{F}_p$ such that $u \in \mathbb{F}_p^\times$ is chosen at random with the property that

$u \in (\mathbb{F}_p^\times)^3$ and $v := (\frac{u}{a})^2$. Go to Step 5.

else

go to the next $a \in G_j$.

Step 5: If $n = 4$, then set $C := C_{u,v}$ and $J_C := J_{u,v}$, else set $C := C_{BFS}$ and $J_C := J_{C_{BFS}}$.

Put $h := 1 - t + (\frac{t^2}{c} + (c-2)p) - tp + p^2$ and $h^\chi := 1 + t + (\frac{t^2}{c} + (c-2)p) + tp + p^2$.

Pick a random point $P \in J_C(\mathbb{F}_p)$ and test that $\gcd(h, h^\chi)P = O_{J_C}$.

If this is the case, then return Fail.

If not, then check that $hP = O_{J_C}$.

If so, then add $C/\mathbb{F}_p$ to S,

else add the quadratic twist $C^\chi/\mathbb{F}_p$ of $C/\mathbb{F}_p$ to S.

Step 6: Return S.

Remark 5.2.1. (1) The only time this procedure fails is when the prime p does not satisfy the conditions specified, or when all the $j \in J$ have been exhausted, and no curves were found, then an empty table will be returned.

(2) By Remark 4.2.4, we know that $J \neq \emptyset$ in Step 2.

(3) We point out that in Step 5 we abandon the curves $C/\mathbb{F}_p$ with points $P \in J_C(\mathbb{F}_p)$ such that $\gcd(h, h^\chi)P = O_{J_C}$. These curves are considered to be cryptographically uninteresting, since they do not seem to have a point of large enough order. To see this, we recall the bound $|h-1-p^2| \leq cp^{\frac{3}{2}}$ due to Weil where c is some contant which can be taken to be 8 for $p > 4$. Similarly, we have $|h^\chi - 1 - p^2| \leq cp^{\frac{3}{2}}$. It follows that $|h - h^\chi| \leq 2cp^{\frac{3}{2}}$. Since $\gcd(h, h^\chi)|(h - h^\chi)$, it follows that $\gcd(h, h^\chi) \leq 2cp^{\frac{3}{2}}$.

(4) The random point $P \in J_C(\mathbb{F}_q)$ in Step 5 can be easily picked via command like *Random($J_C(\mathbb{F}_q)$)* in Magma.

By providing $n = 3, 4, 6$, and $k, D \in \mathbb{N}$ such that $-D$ is a fundamental discriminant with $D \nmid 12$, and the class polynomial $h_{-D}(X) \in \mathbb{Z}[X]$ associated with $-D$, the following procedure, **Method I**, gives an approach for searching for valid integer tuples (k, D, r, p, t) satisfying the hypotheses of Theorem 4.2.3. In addition, it may output Legendre-Satoh curves or Bolza-Freeman-Satoh curves whose Jacobians are isogenous to the ordinary abelian surfaces induced by the valid integer tuples found. See Remark 5.2.2 for the explanation of the input parameters m and e in the following

procedure.

Method I:

Input: $n, k, m, D, e \in \mathbb{N}$ and $h_{-D}(X) \in \mathbb{Z}[X]$, where $n = 3, 4, 6$ and $h_{-D}(X)$ is the class polynomial associated with the fundamental discriminant $-D$ with $D \nmid 12$.

Output: A table of of entries $((k, D, r, p, t), C)$ where (k, D, r, p, t) is a valid integer tuple and $C/\mathbb{F}_p$ is a Legendre-Satoh curve if $n = 4$, or a Bolza-Freeman-Satoh curve if $n = 3, 6$ whose Jacobian is isogenous to the ordinary abelian surface induced by the input valid integer tuple (k, D, r, p, t). Or, 'Fail', if no valid integer tuples are found in the given range or if the valid integer tuples found do not lead to Legendre-Satoh curves/Bolza-Freeman-Satoh curves.

Let T be an empty table.

Step 1: Let $R :=$ NumerateRightR(n, k, m, D).

If $(R = \emptyset)$, then return Fail.

In what follows, we loop over each entry $(l, r, \overline{p}, t, m_0, z_0, A, B, C) \in R$.

Step 2: Compute $\tau :=$ Squareroot$(z_0 \pmod r)$

For what follows, we loop over $w \in \mathbb{Z}$ where $1 \leq w \leq e$.

Set $x := wr + \tau$ and $c := \lfloor \frac{n}{2} \rfloor$.

If $x^2 - z_0 \not\equiv 0 \pmod{4nc}$, then go to the next w.

Set $i := \frac{x^2 - z_0}{A} \in \mathbb{Z}$, $m_i := m_0 + iD$, and $p_i := nm_i r + \overline{p}$.

If $p_i > 4c$ is not prime, then go to the next w

else

Set $S :=$ CurveConstruct$(k, D, r, p_i, t, h_{-D}(X))$.

If $S =$ Fail, then go to the next entry $(l, r, \overline{p}, t, m_0, z_0, A, B, C) \in R$.

If $S = \emptyset$, then go to the next w.

If $S \neq \emptyset$, then

add $((k, D, r, p_i, t), C)$ to T where $C \in S$.

break on w and go to the next entry $(l, r, \overline{p}, t, m_0, z_0, A, B, C) \in R$.

Step 3: If $T = \emptyset$, then return Fail. Otherwise, return T.

Remark 5.2.2. (1) The parameter m serves as an upper bound for our search of $r := \Phi_k(l)$ where $1 \leq l \leq m$, which takes place in the procedure **NumerateRightR** in Step 1.

(2) The parameter e is an upper bound for our search of the smallest x in Step 2. Since the smallest suitable x found in Step 2 implies a smaller size of the prime p_i, we break the loop on w as soon as the valid integer tuple (k, D, r, p, t) in Step 3 leads to some Legendre-Satoh curves/Bolza-Freeman-Satoh curves.

The computational results of Method I described above will be summarized in the next section.

5.3 Computational Results

The pseudo codes of **Method I** outlined in Section 5.2 were implemented in Magma V2.11 on a Gateway personal laptop with Intel Pentium processor T4300 and 4GB memory. Many examples of valid integer tuples for $n \in \{3, 4, 6\}$ and examples of Legendre-Satoh cruves and Bolza-Freeman-Satoh curves induced by these valid tuples were found.

Recall that the input parameters for **Method I** is a tuple $(n, k, m, D, e, h_{-D}(X))$ where $m, e \in \mathbb{N}$ are explained in Remark 5.2.2, $n \in \{3, 4, 6\}$, $D \nmid 12$ such that $-D$ is a fundamental discriminant, and $h_{-D}(X) \in \mathbb{Z}[X]$ is the class polynomial

associated with fundamental discriminant $-D$. In our search of valid integer tuples, Bolza-Freeman-Satoh curves and Legendre-Satoh curves, we fixed $m = 1000$ and $e = 10000$. We restricted the input parameter $k \in \{8, 16, 24, 32, 40, 48, 56\}$ and the fundamental discriminant $-D$ to those whose associated class number h_{-D} satisfies $1 \leq h_{-D} \leq 4$. Furthermore, the fundamental discriminants used were taken from the tables provided on page 229 of Cohen [8] and on pages 514-515 of Cox [9]. The input class polynomial $h_{-D}(X) \in \mathbb{Z}[X]$ associated to each fundamental discriminant $-D$ used was precomputed via the command HilberClassPolynomial(-D) in Magma.

In Step 1 of the procedure **Method I**, we collected all those successful output tuples $(l, r, \overline{p}, t, m_0, z_0, A, B) \in \mathbb{Z}^8$ generated by **NumerateRightR**. For each of the output tuple $(l, r, \overline{p}, t, m_0, z_0, A, B) \in \mathbb{Z}^8$ gathered from Step 1, we proceeded to compute the lift of $\overline{p}$ to prime $p_i > 4c$ as indicated in Step 2 of **Method I**, so that the tuple (k, D, r, p_i, t) is a valid integer tuple. In Step 3, we output all the Legendre-Satoh curves or Bolza-Freeman-Satoh curves derived from the first successful valid integer tuple (k, D, r, p_i, t) obtained from Step 2 such that the procedure **CurveConstruct**$(k, D, r, p_i, t, h_{-D}(X))$ does not return fail, nor an empty table. Then, we start over again with the next successful output tuple $(l, r, \overline{p}, t, m_0, z_0, A, B) \in \mathbb{Z}^8$ generated by **NumerateRightR** until all the output tuples of **NumerateRightR** in Step 1 have been exhausted.

In what follows, we will summarize the computational results of each step in **Method I**, and we will proceed by distinguishing cases of $n = 3, 4$, and 6. We will use D_i to indicate the fundamental discriminant whose associated class number $h_{D_i} = i$ where $1 \leq i \leq 4$.

The computational results for $n = 3$ case are summarized in Table A.1, A.2, A.3,

and A.4 of Appendix A. It took two weeks to generate these data. The computational results for $n = 4$ case are summaried in Table A.5, A.6, A.7, and A.8 of Appendix A. It took one week to generate these table entries. For each pair of the specified integer k and D_i in these tables, the number of $(l, r, \overline{p}, t, m_0, z_0, A, B) \in \mathbb{Z}^8$ from the nonempty output table generated by **NumerateRightR** in the Step 1 of **Method I** is recorded under the column NRR. If the output table of the procedure **NumerateRightR** in the Step 1 of **Method I** is empty, then the procedure **Method I** terminates in Step 1, and a symbol $*$ is indicated in the corresponding entries in the column NRR. If this is the case, then the subsequent entries in that row under different columns will be $*$ as well. For each of the tuple $(l, r, \overline{p}, t, m_0, z_0, A, B) \in \mathbb{Z}^8$ from the nonempty output table generated by **NumerateRightR** in the Step 1 of **Method I**, we proceed to compute various lifts of $\overline{p}$ to primes $p_i > 4c$ as indicated in the Step 2 of **Method I**. If none of the tuples from Step 1 gives rise to any valid integer tuple, then the procedure **Method I** returns an empty table in Step 3, and a symbol # is indicated in the corresponding entries in the column of VIT. If this is the case, then the subsequent entries in that row under different columns will be # as well. Otherwise, the entries in the columns of VIT indicate the number of valid integer tuples being checked in order to obtain the number of the first Legendre-Satoh curves or Bolza-Freeman-Satoh curves found in Step 2, which is recorded under the columns of L-S curves or B-F-S curves. If the valid integer tuples found in Step 2 do not lead to any curve, then the symbol # is recorded in the corresponding entries of the columns of L-S curves or B-F-S curves. Finally, the averages and the smallest ρ-values obtained from these curves are recorded in the last two columns.

For $n = 3$ case, the entries in the columns NRR of Table A.1, A.2, A.3, and

A.4 suggest that the procedure **NumerateRightR** in Step 1 generates at most 234 many outputs. These all occurred in the row of $k = 24$ and with $D_1 = 19$, $D_2 = 115$, $D_3 = 23$, and $D_4 = 715$. The entries in the columns of NRR in Table A.2 and Table A.4 suggest that we may want to avoid using D_2 and D_4 due to the high failure rate in Step 1 of **Method I**. Overall the average ρ-values obtained are around 4.5.

We point out two general patterns in each of the Tables A.1, A.2, A.3, and A.4 here. First of all, the average ρ-values obtained in general tend to decrease as the prescribed embedding degrees k increase. Second of all, if the prescribed embedding degree k is fixed then the average ρ-value obtained in general tend to increase as we increase the class number of the fundamental discriminants. The following is an example of Bolza-Freeman-Satoh curve found in our computation for $n = 3$ which has the smallest ρ-value.

Example 5.3.1. The input parameters for the **Method I** are $n = 3$, $k = 40$, $m = 1000$, $D_1 = 8$, and $h_{-D_1}(X) = X - 8000$. In Step 1, the outputs of **NumerateRightR** are

$$
\begin{aligned}
l &= 169 \quad , \quad r = \Phi_{40}(l) = 44277926323403992859535928774463904 1, \\
\overline{p} &= 169 \quad , \quad t = 91644833561244647255587238352278651 0, \\
m_0 &= 0 \quad , \quad z_0 = -1049846939808529156844994453062511509938048582 6 \\
&\qquad\qquad\qquad\qquad 0086161937651549379747428, \\
B &= 676 \quad , \quad A = 53133511588084791431443114529356684 92, \\
&\qquad\qquad\qquad C = 83987755184682332547599556245000920795043886608 \\
&\qquad\qquad\qquad\qquad 0689295501212395037980100.
\end{aligned}
$$

In Step 2, we found $w = 1$ and also the following parameters

$$\begin{aligned}
\tau &= 420896506376081760776061158896004453,\\
x &= 863675769610121689371420446640643494,\\
i &= 160147617494061533471006372991993942,\\
m_i &= 128118093995249226776805098393595153 6,\\
p_i &= 170184105798497783111925858657940993705\\
&\quad 387986953102079897700645675685510 97,
\end{aligned}$$

The Bolza-Freeman-Satoh curve found in Step 3 by **Method I** is the following

$$\begin{aligned}
C_{BFS}/\mathbb{F}_{p_i}: \quad & Y^2 = 884723633216141029309772903963494607\\
& 031006583277546109615172754839862929X^6\\
& +6325297879012934429615451854751937 06\\
& 28739325989599838093932194546296990 5X^3\\
& +2476412138433659706773999593585331 03690\\
& 52209723421910388636326831576183 0,
\end{aligned}$$

which has

$$\begin{aligned}
\#J_{C_{BFS}}(\mathbb{F}_{p_i}) &= 289626298664342867643731430913106688062422644390544\\
&\quad 068417632619984390779530159562762272507080342644964 9\\
&\quad 327992267677166177219741255409627089244433.
\end{aligned}$$

The ρ-vaule of this curve is 4.056.

For $n = 4$, the columns of NRR in Table A.5, A.6, A.7, A.8 of Appendix indicate that the procedure **NumerateRightR** in Step 1 does not generate many outputs. We observe that in Table A.5 the only pair of k and D_1 together with $n = 4$, $m = 1000$ such that **NumerateRightR**(n, k, D_1, m) in Step 1 of **Method I** gives successful outputs are $k = 16, 24, 32, 40, 48, 56$, and $D_1 = 8$. Of all the valid integer tuples being processed in Step 2, none of them give rise to Legendre-Satoh curves. We also observe that most of the Legendre-Satoh curves found in Table A.6 are those

with parameter $D_2 = 24$. We point out that the success rate of Step 1 is zero when D_3 is used (See Table A.7). Finally, we observe that in Table A.8 when the input fundamental discriminant $D_4 = 120$ is used then **Method I** is more likley to find Legendre-Satoh curves. The following is an example of a Legendre-Satoh curve found in our computation for $n = 4$ which has the smallest ρ-value.

Example 5.3.2. The input parameters for the **Method I** are $n = 4$, $k = 56$, $m = 1000$, $D_4 = 520$, and

$$\begin{aligned} h_{-D_4}(X) &= X^4 - 1295888944240605829642234473600 0X^3 \\ &\quad +4665000313914630792242188817484545322397593600 0X^2 \\ &\quad -7800653452887194984590836097657958620600147968000000 0X \\ &\quad +1715174758910223724285055191855485592223464976547840000 00. \end{aligned}$$

In Step 1, the outputs of **NumerateRightR** are

$$\begin{aligned} l &= 614\ , \\ r &= \Phi_{56}(l) = 824215746492029735619385969618273451499, \\ &\qquad 119949087986595411530702232 1, \\ \overline{p} &= 247264723947608920685815790885482035449735984726 39 \\ &\quad 597862345921067577, \\ t &= 824215746492029735619386035964720468048416059191009860292 \\ &\quad 5616851544, \\ m_0 &= 0, \\ z_0 &= \text{-}130640691685656505276446793869802450032398391677492872 23 \\ &\quad 887761738081553499978267068069512563278011511210302966776 \\ &\quad 7926261422038397391, \end{aligned}$$

$$A = 263749038877449515398203510277847504479718383708155710531689824714272,$$

$$B = 1978117791580871365486526327083856283597887877811167828987673685406160,$$

$$C = 1978117791580871365486526327083856283597887877811167828987673685406160,$$

In Step 2, we found $w = 24$ and also the following parameters.

$$\tau = 32308579394305164391053910871408783997164662100770743414520995544150,$$

$$x = 20104263709751765298775802379552650675950525399119385724021946809011900,$$

$$i = 15324519377906108559491175064645191671302611313063654568187639959561600,$$

$$m_i = 79687500765111764509354110336154996690773578827931003754575727789720320,$$

$$p_i = 26271877171680313476832472277462346836913239237944640616110243521083469701626800394774156353054492008523664901406391886400753860762701184570,$$

The Legendre-Satoh curve found by **Method I** is the following

$$C_{u,v}/\mathbb{F}_{p_i}: \quad Y^2 = 1176087552106653795219176012305741382108252586357883993852470635253637029971616194239117058885172191179553514100377091587689022804872432721X^5+191552122435651132652645459791691831621808517931739128399695676776623870389817904695994941821909287525968076709884293467798723397345209545 7X^3+2506157902000124450675779835634728795842799777352572295201922149074136184756013949239128579473105306644455353044003438292770037789523402X$$

which has

$$\#J_{u,v}(\mathbb{F}_{p_i}) = 690211530123857187443700158062266702147771081450257929898535170705159127240442173327645010783386253229396117901896733758354934052794530874970691458983603267599083832456886536975080194036829745489341178964053482772319182629356987745041554923277744066268162756875057 8576599453666.$$

The ρ-vaule of this curve is 4.1371.

For $n = 6$, the computational results are summarized in Table A.9, A.10, A.11, and A.12 of Appendix A. It took four days to generate these table entries. We point out that no examples are found with parameters D_1, D_2, and D_3. Of all the examples found in Table A.12, it seems that the computation with the input parameter $D_4 = 39$ leads to most of the Bolza-Freeman-Satoh curves found. The following is the example Bolza-Freeman-Satoh curve found in our computation that has the smallest ρ-value.

Example 5.3.3. The input parameters for the **Method I** are $n = 6$, $k = 56$,

$m = 1000$, $D_4 = 39$, and

$$\begin{aligned} h_{-D_4}(X) &= X^4 - 331531596X^3 + 429878960946X^2 - 109873509788637459X \\ &\quad +20919104368024767633. \end{aligned}$$

In Step 1, the outputs of **NumerateRightR** are

$$\begin{aligned} l &= 830\ , \\ r &= \Phi_{56}(l) = 11425473754346960309867960922324797923550716, \\ &\qquad 44656800162305242951679000 1, \\ \overline{p} &= 57127368771734801549339804611623989617753582232840008115 \\ &\quad 262147583950835, \\ t &= 29026168220003975816462838147399521960351680557425323875 \\ &\quad 617542611010200, \\ m_0 &= 0, \\ z_0 &= \text{-}21603036962460737790639086838390254002880564162701397 39 \\ &\quad 93455916373131229593101992399458675294194394484128594039 \\ &\quad 062132475222028729357306828 20, \\ A &= 82263411031298114231049318640738545049565158415289611685 \\ &\quad 9774925208880072, \\ B &= 68552842526081761859207765533948787541304298679408009738 \\ &\quad 3145771007410020, \\ C &= 84251844153596877383492438669721990611234200234535449857 \\ &\quad 44780738552124809415230311755074257250134779759769297953 \\ &\quad 29110733463295190264504040000, \end{aligned}$$

In Step 2, we found $w = 438$ and also the following parameters.

$$\begin{aligned}
\tau &= 2924825729037335936616300883055489817209596211578746085999937973133004,\\
x &= 5007282330133005951658783184861316980332423399808363456982964066327153442,\\
i &= 3047879685801005675164349983014531880869055041745113770949168745590213569 7,\\
m_i &= 1188673077462392213314096493375667433538931466280594370670175810780183292183,\\
p_i &= 8148691829427236120737339897292813922397912568309888320790629257561874239490547818446247531900319287063450181581845815003293620472484327419912393 3,
\end{aligned}$$

The Bolza-Legendre-Satoh curve found by **Method I** is the following

$$\begin{aligned}
C_{u,v}/\mathbb{F}_{p_i}: \quad Y^2 = X^6 &+ 8036503870185816908204140560533234\\
&2619920760841388331279895704181767143008926792\\
&1962115070541239060960987809561476407845973981 5\\
&189991838446520809 7X^3 + 677633829526011165526\\
&9858909164597339368370914349189795753248632377 4\\
&3247054209992542826048408700588742608137779024 4\\
&1066623548737622773994462996047
\end{aligned}$$

which has

$$\begin{aligned}\#J_{u,v}(\mathbb{F}_{p_i}) &= 6640117853097419621339456885539399493394745123640069050647399187475665750792389945\\ &\quad 57239034134997986102800249976399270438374252668468557663517000199195411259050185057714604284000479546089214968821104282440101322461166184307795726813623255590217889554678520817186574049274401933833187098906\\ &\quad 5623\end{aligned}$$

The ρ-value of this curve is 4.1654.

Remark 5.3.4. (a) Both Bolza-Freeman-Satoh curves $C_{BFS}/\mathbb{F}_p$ found and summarized in Example 5.3.1 and 5.3.3 are such that $J_{C_{BFS}} \otimes \mathbb{F}_{p^m}$ are simple for $m \mid n$, $m \neq n$, where $n = 3, 6$, respectively. In particular, Example 5.3.3 is the first pairing-friendly Bolza-Freeman-Satoh curve whose Jacobian is simple and not split over a quadratic extension nor over a cubic extension of the ground field.

(b) The Legendre-Satoh curve $C_{u,v}/\mathbb{F}_p$ found and summarized in Example 5.3.2 is the first example of a pairing-friendly Legendre-Satoh curve such that $J_{u,v} \otimes \mathbb{F}_{q^m}$ is simple for $m \mid 4$, $n \neq 4$. Satoh [43] and Freeman and Satoh [13] were unable to check in their construction if the Jacobians of their Legendre-Satoh curves constructed split over a quadratic extension of the ground fields or not, because they did not have the precise splitting condition given in [7], Theorem 31.

Chapter 6

Future Work

6.1 An extension of Method I

In this section, we sketch a method of searching for a valid integer tuple for $n = 3$ which has led to the discovery of a cryptographic example of Bolza-Freeman-Satoh curve whose Jacobian is simple and has the smallest ρ-value ever recorded.

Recall from Section 5.1 that a non-constant integer polynomial $f(X) \in \mathbb{Z}[X]$ is said to represent primes if it is irreducible over $\mathbb{Z}$, has positive leading coefficient, and $\gcd(\{f(x_1) : x_1 \in \mathbb{Z}^+\}) = 1$. Now if $f(X) \in \mathbb{Q}(X)$ is a rational polynomial such that $f(x_0) \in \mathbb{Z}$ for some integer x_0, then it is an easy exercise to show that $f(X \cdot d + x_0) \in \mathbb{Z}[X]$, where d denotes the denominator of f, i.e., $d = \mathrm{lcm}(\{b_i\})$, if $f(X) = \sum \frac{a_i}{b_i} X^i$, where $\gcd(a_i, b_i) = 1$. Furthermore, if the given $f(X) \in \mathbb{Q}[x]$ is non-constant, and also satisfies the three conditions imposed by the conjecture of Bouniakowsky and Schinzel, then we know that $f(X \cdot d + x_0) \in \mathbb{Z}[X]$ will represent primes. This motivates to extend the previous definition to the following which is due to Freeman and Teske[14] (page 11).

Definition 6.1.1. Let $f(X) \in \mathbb{Q}[X]$. We say that f *represents primes* if the following conditions are satisfied:

(1) $f(X)$ is non-constant;

(2) $f(X)$ has positive leading coefficient;

(3) $f(X)$ is irreducible;

(4) $f(x_0) \in \mathbb{Z}$ for some $x_0 \in \mathbb{Z}$;

(5) $\gcd(\{f(x_1) : x_1, f(x_1) \in \mathbb{Z}\}) = 1$.

Let $n = 3, 4, 6$ and put $c = \lfloor \frac{n}{2} \rfloor$. Let $k, D \in \mathbb{N}$ where $-D$ is a fundamental discriminant such that $D \nmid 12$. Then the task of searching for valid integer tuples (k, D, r, p, t) for the given n can be split into two tasks:
Task 1: Search for the polynomial tuples $r(X), p(X), t(X) \in \mathbb{Q}[X]$ such that the following conditions hold:

$$\begin{cases} r(X), p(X) \in \mathbb{Q}[X] \text{ represent primes;} \\ \Phi_k(p(X)) \equiv 0 \pmod{r(X)}; \\ t(X)^2 - c(p(X)+1)t(X) + c(p(X)^2 + (c-2)p(X) + 1) \equiv 0 \pmod{r(X)} \text{ simultaneously;} \\ 4cp(X) = t(X)^2 + y(X)^2 D \text{ for some } y(X) \in \mathbb{Q}[X]. \end{cases} \tag{6.1.1}$$

Task 2: Search for $x_1 \in \mathbb{Z}$ such that $r(x_1), p(x_1), t(x_1), y(x_1) \in \mathbb{Z}$ where both $p(x_1)$ and $r(x_1)$ take on prime values greater than 5, $r(x_1) \nmid k$, and $t(x_1) \in \mathbb{Z}$ with $\gcd(t(x_1), p(x_1)) = 1$ and $t(x_1) \equiv 0 \pmod{c}$. Then the integer tuple $(k, D, r(x_1), p(x_1), t(x_1))$ will automatically be a valid integer tuple for the chosen n.

Hence it follows from Theorem 4.1.1 that there exists an ordinary abelian surface

$A/\mathbb{F}_{p(x_i)}$ such that it has embedding degree k with respect to the prime $r(x_1)$. Moreover, we have that $tr_A = t(x_1)$, $A \otimes \mathbb{F}_{p(x_1)^n} \sim E^2$ where $A \otimes \mathbb{F}_{p(x_1)^m}$ is simple for all $m \mid n$, $n \neq m$, and that $E/\mathbb{F}_{p(x_1)^n}$ is an elliptic curve with $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-D})$. This suggests the following definition.

Definition 6.1.2. Let $n = 3, 4, 6$ and put $c = \lfloor \frac{n}{2} \rfloor$. Let $k, D \in \mathbb{N}$ be such that $-D$ is a fundamental discriminant and $D \nmid 12$. If $r(X), p(X), t(X) \in \mathbb{Q}[X]$ satisfy the conditions stated in (6.1.1), then the polynomial tuple $(k, D, r(X), p(X), t(X))$ is said to be a *valid polynomial tuple for a given n*. Thus, such a tuple represents a family of simple geometrically split abelian surfaces with specified embedding degree k.

The following technical proposition is proven in Chou [6] (page 9) which leads to a method in searching for valid polynomial tuples $(k, D, r(X), p(X), t(X))$ for $n = 3$.

Proposition 6.1.3. *Given $k, D \in \mathbb{N}$ such that $-D$ is a fundamental discriminant. Set $l_3 := lcm(k, 3, D)$ and $l_4 := lcm(k, 4, D)$.*
(a) The smallest cyclotomic field containing $\mathbb{Q}(\zeta_k, \sqrt{-3}, \sqrt{-D})$ is $\mathbb{Q}(\zeta_{l_3})$. The smallest cyclotomic field containing $\mathbb{Q}(\zeta_k, \sqrt{-1}, \sqrt{-D})$ is $\mathbb{Q}(\zeta_{l_4})$. Furthermore, $\sqrt{-D} \in \mathbb{Z}[\zeta_{l_3}]$ (resp. $\in \mathbb{Z}[\zeta_{l_4}]$) and if $\sqrt{-D} = \sum_{i=1}^{\phi(l_3)-1} a_i \zeta_{l_3}^i$ (resp. $\sqrt{-D} = \sum_{i=1}^{\phi(l_4)-1} a_i \zeta_{l_4}^i$), then

$$\frac{1}{\sqrt{-D}} = \sum_{i=1}^{\phi(l_3)-1} \frac{a_i}{-D} \zeta_{l_3}^i \text{ (resp. } \frac{1}{\sqrt{-D}} = \sum_{i=1}^{\phi(l_4)-1} \frac{a_i}{-D} \zeta_{l_4}^i)$$

where $a_i \in \mathbb{Z}$.

(b) For any $\alpha \in \mathbb{Q}(\zeta_{l_3})$ and $\beta \in \mathbb{Q}(\zeta_{l_4})$, we set

$$f_{(3)}(X) := \quad X^2 - (\alpha+1)X + (\alpha^2 - \alpha + 1), \tag{6.1.2}$$

$$f_{(6)}(X) := \quad X^2 - 3(\alpha+1)X + 3(\alpha^2 + \alpha + 1), \tag{6.1.3}$$

$$f_{(4)}(X) := \quad X^2 - 2(\beta+1)X + 2(\beta^2 + 1). \tag{6.1.4}$$

Then the kth cyclotomic polynomial $\Phi_k(X)$ and both $f_{(3)}(X)$ and $f_{(6)}(X)$ split over $\mathbb{Q}(\zeta_{l_3})$, and both $\Phi_k(X)$ and $f_{(4)}(X)$ split over $\mathbb{Q}(\zeta_{l_4})$. Let $t_{(3)}$, $t_{(4)}$, and $t_{(6)}$ denote the roots of $f_{(3)}(X)$, $f_{(4)}(X)$, and $f_{(6)}(X)$ respectively. If $\alpha \in \mathbb{Z}[\zeta_{l_3}]$ and $\beta \in \mathbb{Z}[\zeta_{l_4}]$, then $t_{(3)}, t_{(6)} \in \mathbb{Z}[\zeta_{l_3}]$ and $t_{(4)} \in \mathbb{Z}[\zeta_{l_4}]$. Furthermore if $\sqrt{-D} = \sum_{i=1}^{\phi(l_3)-1} a_i \zeta_{l_3}^i \in \mathbb{Z}[\zeta_{l_3}]$ then we have

$$\frac{t_{(3)}^2 - 4\alpha}{-D} = \left(\sum_{i=1}^{\phi(l_3)-1} \frac{a_i(\zeta_3^2\alpha + \zeta_3)}{-D} \zeta_{l_3}^i \right)^2. \tag{6.1.5}$$

The main idea is to set $r(X) := \Phi_{l_3}(X)$ and to search for suitable polynomials $t_{(3)}(X) \in \mathbb{Z}[X]$ and $p(X) \in \mathbb{Q}[X]$ such that $p(X)$ represents primes, $\Phi_k(p(X)) \equiv 0 \pmod{r(X)}$, and $f_{(3)}(X) = t_{(3)}(X)^2 - (p(X)+1)t_{(3)}(X) + (p(X)^2 - p(X) + 1) \equiv 0 \pmod{r(X)}$. This approach all boils down to testing if

$$p(X) := \frac{1}{4}(t_{(3)}(X)^2 + Dy(X)^2) \in \mathbb{Q}[X] \tag{6.1.6}$$

represents primes or not, where $y(X) \in \mathbb{Z}[X]$ is such that $y(X)^2 \equiv \frac{t_{(3)}(X)^2 - 4p(X)}{-D} \pmod{r(X)}$. Note that the integral coefficients of $t_{(3)}(X)$ and $y(X)$ are given by Proposition 6.1.3. Once the polynomial $p(X)$ defined above is shown to represent primes, then the polynomial tuple $(k, D, r(X), p(X), t_{(3)}(X))$ will be a valid polynomial tuple. It can then be used to search for some $x_1 \in \mathbb{Z}$ such that $(k, D, r(x_1), p(x_1), t_{(3)}(x_1))$ is a valid integer tuple which satisfies the conditions of Theorem 4.2.3 and gives rise to the desire Bolza-Freeman-Satoh curve.

The following example is the result of a preliminary implementation of this method

in Magma V2.11 on a Gateway peronal laptop with Intel Pentium processor T4300 and 4GB memory.

Example 6.1.4. We fix $n = 3$, $k = 6$ and $D = 7$. Then the valid polynomial parameters found are

$$\begin{aligned} r(X) &= X^{12} + X^{11} - X^9 - X^8 + X^6 - X^4 - X^3 + X + 1 \\ p(X) &= \tfrac{1}{7}X^{18} - \tfrac{1}{7}X^{16} + \tfrac{2}{7}X^{14} + \tfrac{2}{7}X^{13} - \tfrac{3}{7}X^{11} - \tfrac{2}{7}X^{10} + \tfrac{1}{7}X^9 \\ &\quad + \tfrac{2}{7}X^8 - X^7 - \tfrac{2}{7}X^6 - \tfrac{2}{7}X^5 + \tfrac{1}{7}X^4 + \tfrac{2}{7}X^3 + \tfrac{1}{7}X^2 + 1 \\ t_{(3)}(X) &= -X^7 + 2 \end{aligned}$$

These valid polynomial parameters lead to the following valid integer parameters

$$\begin{aligned} x_1 &= 45402 \\ r(x_1) &= 767201384057771295678477563092190991034576067708374548 19 \\ p(x_1) &= 95995677513033996783604844042263420933974858579859836360 \\ &\quad 685376324246956983032264221 \\ t_{(3)}(x_1) &= -39767188735119669060124495985932 6, \end{aligned}$$

which lead to the following Bolza-Freeman-Satoh curve $C_{BFS}/\mathbb{F}_{p(x_1)}$

$$\begin{aligned} Y^2 = {} & 256934801867210627579496865625123701148467170463840872306 9 \\ & 247649561305313327075672 0\, X^6 + 158000965777013008971514120862 91 \\ & 858540262848139669770361269014446632707644344713791\, X^3 + 846322 \\ & 653522066407027683156679176225752993796567222515355870199406390 \\ & 65535950269943 \end{aligned}$$

whose Jacobian $J_{C_{BFS}}$ is $\mathbb{F}_{p(x_1)}$-simple and has embedding degree 6 with respect to the prime $r(x_1)$. Moreover, $J_{C_{BFS}}(\mathbb{F}_{p(x_1)}) \otimes \mathbb{F}_{p(x_1)^3}$ splits as a product of elliptic curves. The ρ-value obtained is 2.969.

Remark 6.1.5. Since $\log_2(r(x_1)) = 186$, $\log_2(p(x_1)) = 276$, and by the same reason stated in the part (a) of Remark 5.3.4, the Bolza-Freeman-Satoh curve presented above is the first cryptographic example of pairing-friendly Bolza-Freeman-Satoh curve whose Jacobian is simple over the ground field and with the lowest ρ-value ever recorded.

One future line of research is to carry out a more detailed and systematic implementation of the method described above with various prescribed embedding degrees k and fundamental discriminants $-D$. It would be interesting to investigate whether in general this method can lead to other cryptographic examples of pairing-friendly Bolza-Freeman-Satoh curves whose Jacobians have lower ρ-value than those found in Chapter 5.

Another future line of research is to extend the method described here to the cases of $n = 4$ and $n = 6$ by investigating if the quantities $\frac{t_{(4)}^2 - 4\alpha}{-D}$ and $\frac{t_{(6)}^2 - 4\alpha}{-D}$ are also squares in $\mathbb{Q}(\zeta_{l_4})$ and $\mathbb{Q}(\zeta_{l_3})$ respectively, where l_3, l_4, $t_{(4)}$, $t_{(6)}$ are as stated in Proposition 6.1.3. If this is indeed the case, then we can search for the polynomials $p(X)$ representing primes in the same way as in (6.1.6), which may give rise to valid polynomials tuples for the $n = 4$ and $n = 6$ cases. Then we can use these valid polynomial tuples to find the desired Legendre-Staoh curves and Bolza-Freeman-Satoh curves in a similar way, and investigate the ρ-value associated with their Jacobians.

Bibliography

[1] R. Avanzi, C. Doche, H. Cohen, G. Frey, T. Lange, and K. Nguyen, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[2] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[3] O. Bolza. On Binary Sextics with Linear Transformations into Themselves. *Amer. J. Math.*, 10(1):47–70, 1887.

[4] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4):297–319, 2004.

[5] V. Bouniakowsky. Sur les diviseurs numériques invariables des fonctions rationnelles entières. *Mémoires. Sc. Math et phys. T.*, VI:307–329, 1854-1855.

[6] K.J. Chou. Method III: Ideas based on the Brezing and Weng 2005 paper. Unpublished manuscript, June 15, 2010.

[7] K.J. Chou and E. Kani. Simple geometrically split abelian surfaces over finite fields. *Preprint*, 2010.

[8] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[9] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[10] P. Deligne. Variétés abéliennes ordinaries sur un coprs fini. *Invent. Math.*, 8:238–243, 1969.

[11] D. Freeman. Constructing pairing-friendly genus 2 curves with ordinary Jacobians. In *Pairing 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, pages 152–176. Springer, Berlin, 2007.

[12] D. Freeman. A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties. In *Pairing-Based Cryptography*, volume 5209/2008 of *Lecture Notes in Comput. Sci.*, pages 146–163. Springer, Berlin, 2007.

[13] D. Freeman and T. Satoh. Constructing pairing-friendly hyperelliptic curves using Weil restriction. *Preprint, http://theory.stanford.edu/ dfreeman/papers/weil.pdf*, 2009.

[14] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2):224–280, 2010.

[15] David Freeman, Peter Stevenhagen, and Marco Streng. Abelian varieties with prescribed embedding degree. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 60–73. Springer, Berlin, 2008.

[16] G. Frey and H.G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.

[17] S. Galbraith. Supersingular curves in cryptography. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 495–513. Springer, Berlin, 2001.

[18] S. Galbraith. *Mathematics of Public Key Cryptography.* To be published by Cambridge University Press in 2011, Online First Preprint, Available at: http://www.math.auckland.ac.nz/ sgal018/crypto-book/crypto-book.html, June 21, motivation.

[19] S. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. In *Pairing-Based Cryptography V Pairing 2007*, volume 4575/2007 of *Lecture Notes in Comput. Sci.*, pages 108–131. Springer, Berlin, 2007.

[20] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 19–34. Springer, Berlin, 2000.

[21] P. Gaudry and E. Thomé. A double large prime variation for small genus hyperelliptic index calculus. *Cryptology ePrint Archive, Report 2004/153*, 2004.

[22] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[23] Laura Hitt. Families of genus 2 curves with small embedding degree. *J. Math. Cryptol.*, 3(1):19–36, 2009.

[24] T. Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[25] E. W. Howe and H. J. Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *J. Number Theory*, 92(1):139–163, 2002.

[26] E.W. Howe. Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.*, 347(7):2361–2401, 1995.

[27] A. Joux. A one round protocol for tripartite Diffie-Hellman. *J. Cryptology*, 17(4):263–276, 2004.

[28] E. Kani. Products of CM elliptic curves. *Collect. Math.*, 62:297–339, 2011.

[29] E. Kani. A splitting criterion for J_C. Unpublished manuscript, August 20, 2010.

[30] E. Kani. Subcovers and involutions. Unpublished manuscript, September 3, 2010.

[31] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[32] M. Kawazoe and T. Takahashi. Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$. In *Pairing-Based Cryptography*, volume

5209/2008 of *Lecture Notes in Comput. Sci.*, pages 164–177. Springer, Berlin, 2008.

[33] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[34] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

[35] D. Maisner and E. Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[36] A. J. Menezes, P. van Oorschot, and S.A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[37] A.J. Menezes, O. Tatsuaki, and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[38] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[39] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[40] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[41] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[42] K. Nagao. Improvement of Theriault algorithm of index calculus for Jacobian of hyperelliptic curves of small genus. *Cryptology ePrint Archive, Report 2004/161*, 2004.

[43] T. Satoh. Generating genus two hyperelliptic curves over large characteristic finite fields. In *Advances in cryptology—EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Comput. Sci.*, pages 536–553. Springer, Berlin, 2009.

[44] A. Schinzel and W. Sierpinski. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.*, 4:185–208, 1958.

[45] J. Scholten and F. Vercauteren. An introduction to elliptic and hyperelliptic curve cryptography and the NTRU cryptosystem. *Preprint available at: http : //homes.esat.kuleuven.be/ fvercaut/papers/cc*03.*pdf*.

[46] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[47] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In *Advances in cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, pages 75–92. Springer, Berlin, 2003.

[48] W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New*

York, Stony Brook, N.Y., 1969), pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[49] André Weil. Sur les fonctions algébriques à corps de constantes fini. *C. R. Acad. Sci. Paris*, 210:592–594, 1940.

[50] G. Yes. Cyclotomic polynomials and prime numbers. *Preprint*, 2010.

Appendix A

Tables

The tables presented in this Appendix contain data generated by the implementation of the procedure **Method I** described in Section 5.2. The following is the legend for these tables.

Notation	Notes
k	Embedding degree $k \in \{8, 16, 24, 32, 40, 48, 56\}$.
D_i	Fundamental discriminants with class number $h_{D_i} = i$ where $1 \leq i \leq 4$.
NRR	Number of outputs of **NumerateRightR**$(n, k, 1000, D_i)$ in Step 1 of **Method I**.
VIT	Number of valid integer tuples found and processed in Step 2 of **Method I** to obtain Legendre-Satoh curves or Bolza-Freeman-Satoh curves.
Suitable VIT ($n = 6$)	Number of valid integer tuples found and processed in Step 2 of **Method I** which the prime p satisfies the conditions in table (4.2.9) of Theorem 4.2.3 for $n = 6$ and obtain Bolza-Freeman-Satoh curves.

Notation	Notes
L-S curves \ B-F-S curves	Number of Legendre-Satoh curves \ Bolza-Freeman-Satoh curves found in Step 3 of **Method I**.
average \ smallest ρ-value	The average\ smallest ρ-value of the Legendre-Satoh curves or Bolza-Freeman-Satoh curves found.
$*$	If the output table of the procedure **NumerateRightR** in the Step 1 of **Method I** is empty, then the procedure **Method I** terminates in Step 1, and a symbol $*$ is indicated in the corresponding entries in the column NRR. If this is the case, then the subsequent entries in that row under different columns will be $*$ as well.
#	If none of the tuples from Step 1 gives rise to any valid integer tuple, then the procedure **Method I** returns an empty table in Step 3, and a symbol # is indicated in the corresponding entries in the column of VIT. If this is the case, then the subsequent entries in that row under different columns will be # as well.

$n = 3$						
k	D_1	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
8	7, 8, 11, 19, 43, 67, 163.	34, 8, 26, 36, 34 , 34, 24.	15, 8, 21, 36, 33, 33, 24.	15, 8, 21, 36, 33, 33, 24.	4.9719, 4.7656, 4.8430, 5.0086, 5.0363, 5.1275, 5.0774.	4.2349, 4.4778, 4.3452, 4.3860, 4.5163, 4.4930, 4.5019.
16	7, 8, 11, 19, 43, 67, 163.	16, 6, 14, 6, 12, 18, 12.	6, 6 ,13 , 6, 12, 18, 12.	6, 6, 13, 6, 12, 18, 12.	4.3891, 4.4364, 4.5077, 4.4388, 4.4910, 4.5461, 4.4635.	4.2578, 4.2243, 4.3712, 4.3765, 4.2821, 4.3157, 4.2265.
24	7, 8, 11, 19, 43, 67, 163.	136, 80, 104, 218, 154, 182, 166.	59, 57, 91, 192, 146, 179, 166.	59, 57, 91, 192, 146, 179, 166.	4.4659, 4.4280, 4.4708, 4.5935, 4.6123, 4.6367, 4.5605.	4.0517, 4.1368, 4.1667, 4.1361, 4.2415, 4.2351, 4.2183.
32	7, 8, 11, 19, 43,67, 163,	12, 9, 16, 18, 28, 14, 14.	10, 9, 14, 18, 27, 14, 14.	10, 9, 14, 18, 27, 14, 14.	4.2496, 4.2189, 4.2718, 4.2961, 4.3116, 4.2961, 4.2721.	4.1572, 4.1349, 4.1607, 4.1147, 4.2345, 4.1841, 4.2000.
40	7,8,11, 19,43,67, 163.	128, 11, 78, 82, 66, 82, 48.	49, 7, 75, 74, 64, 82, 48.	49, 7, 75, 74, 64, 82, 48.	4.3247, 4.2328, 4.30149, 4.3289, 4.3179, 4.3159, 4.2942.	4.1237, 4.0526, 4.0986, 4.1377, 4.1432, 4.1013, 4.1362.
48	7,8,11, 19,43,67, 163.	64, 38, 34, 102, 74, 82, 66.	31, 27, 28, 94, 73, 78, 66.	31, 27, 28, 94, 73, 78, 66.	4.2833, 4.2320, 4.2820, 4.3352, 4.3263, 4.3349, 4.3285.	4.1079, 4.0657, 4.1308, 4.1221, 4.1087, 4.0544, 4.1580.
56	7,8,11, 19,43,67, 163.	114, 12, 38, 74, 56, 56, 32.	49, 10, 34, 71, 54, 56, 32.	49, 10, 34, 71, 54, 56, 32.	4.1962, 4.1734, 4.200, 4.2201, 4.2130, 4.2687, 4.3021.	4.1013, 4.1127, 4.0708, 4.1167, 4.0864, 4.0564, 4.1485.

Table A.1: $n = 3$, Class number 1

$n = 3$						
k	D_2	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
8	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	5, 2, 8, 42, 4, 1, *, *, 34 , 38, *, *, 34, *, 48, *, 34, 48.	4, 2, 8, 27, 4, 1, *, *, 29, 30, *, *, 24, *, 38, *, 30, 45.	14, 16, 52, 216, 32, 8, *, *, 232, 240, *, *, 192, *, 304, *, 240, 360.	4.7806, 4.9571, 4.9505, 4.9304, 4.8119, 5.2669, *, *, 5.1046, 5.0348, *, *, 5.0640, *, 5.0673, *, 5.0626, 5.1817.	4.4883, 4.8851, 4.4449, 4.6202, 4.4978, 5.2669, *, *, 4.4577, 4.4486, *, *, 4.4941,*, 4.5830, *, 4.4336, 4.5760.
16	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	2, 2, 1, 8, *, 1, *,*, 10, 10, *, *, 14, *, 14, *, 12, 8.	2, 2, 1, 7, *, 1, *, *, 6, 7, *, *, 13, *, 10, *, 10, 8.	4, 16, 2, 56, *, 2, *, *, 48, 56, *, *, 104, *, 80, *, 80, 64.	4.4320, 4.4996, 4.4701, 4.4568, *, 4.4462, *, *, 4.6057, 4.5302, *, *, 4.5803, *, 4.5681, *, 4.5959, 4.6033.	4.4176, 4.4826, 4.4701, 4.3247, *, 4.4462, *, *, 4.5175, 4.3591, *, *, 4.3988, *, 4.4367, *, 4.4436, 4.5175.
24	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	61, 38, 65, 136, 24, 30, 17, 15, 176, 234, 13, 3, 124, 2, 172, 3, 186, 170.	32, 6, 52, 109, 4, 28, 9, 10, 141, 204, 12, 1, 100, 0, 156, 2, 169, 143.	154, 48, 314, 872, 32, 182, 72, 80, 1128, 1632, 66, 8, 800, 0, 1248, 16, 1352, 1144.	4.5107, 4.4292, 4.4976, 4.5346, 4.5279, 4.5652, 4.4936, 4.5280, 4.6606, 4.6724, 4.4855, 4.7068, 4.6642, # , 4.6907, 4.6380, 4.6749, 4.6245.	4.0778, 4.2444, 4.1861, 4.1499, 4.4440, 4.2378, 4.3388, 4.3589, 4.1851, 4.2338, 4.1377, 4.7068, 4.2548, # , 4.2053, 4.5186, 4.3007, 4.1944.
32	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, 5, 22, *, 2, 2, *, 10, 12, *, *, 16, *, 18, 1, 24, 18.	*, *, 5, 10, *, 2, 2, *, 8, 9, *, *, 11, *, 13, 1, 21, 16.	*, *, 22, 80, *, 10, 16, *, 64, 72, *, , 88, *, 104, 2, 168, 128.	*, *, 4.2931, 4.2713, *, 4.2706, 4.2344, *, 4.3140, 4.3019, *, *, 4.3323, *, 4.2890, 4.2484, 4.3028, 4.3158.	*, *, 4.2395, 4.1891, *, 4.2419, 4,1645, *, 4.2258, 4.1740, *, *, 4.2808, *, 4.2158, 4.2484, 4.2118, 4.2053.

$n = 3$ (continued)						
k	D_2	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
40	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	26, 7, 10, 128, *, 3, 2, *, 128, 48, 1, 1, 64, 1, 32, *, 70, 88,	7, 2, 6, 84, *, 3, 2, *, 103, 36, 1, #, 57, 1, 25, *, 63, 75,	38, 16, 24, 672, *, 6, 16, *, 824, 288, 2, #, 456, 8, 200, *, 504, 600,	4.4836, 4.2316, 4.2828, 4.3020, *, 4.6482, 4.2959, *, 4.3738, 4.3705, 4.2491, #, 4.3103, 4.2862, 4.3864, *, 4.3471, 4.3644,	4.2155, 4.2258, 4.2158, 4.0920, *, 4.2717, 4.2927, *, 4.1562, 4.1519, 4.2491, #, 4.1362, 4.2862, 4.1872, *, 4.1243, 4.1380.
48	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	22, 16, 25, 64, 13, 6, 4, 4, 90, 82, 3, 4, 78, 4, 74, 2, 90, 80.	11, 3, 17, 50, 4, 6, #, #, 75, 73, 3, #, 70, 3, 62, 2, 78, 70.	58, 24, 100, 400, 32, 36, #, #, 600, 584, 24, #, 560, 24, 496, 10, 624, 560.	4.2570, 4.2504, 4.3097, 4.3099, 4.2506, 4.3461, #, # , 4.3459, 4.3452, 4.3467, #, 4.3581, 4.3065, 4.3460, 4.2422, 4.3363, 4.3399.	4.1877, 4.1858, , 4.1238, 4.1885, 4.2375, #, #, 4.1630, 4.1351, 4.3149, #, 4.1910, 4.2863, 4.2037, 4.1701, 4.1758, 4.1808.
56	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	11, 8, 15, 114, 1, 3, 4, 2, 114, 82, 2, *, 52, *, 22, *, 68, 54.	8, 2, 11, 75, 1, 3, 1, 1, 85, 60, 2, *, 45, *, 19, *, 61, 43.	34, 16, 46, 600, 8, 18, 8, 8, 680, 480, 10, *, 360, *, 152, *, 488, 344.	4.1815, 4.1881, 4.1932, 4.2445, 4.2267, 4.2159, 4.2102, 4.2373, 4.2785, 4.2534, 4.2189, *, 4.2775, *, 4.2586, *, 4.2535, 4.2434.	4.1327, 4.1352, 4.1012, 4.0985, 4.2267, 4.1881, 4.2102, 4.2373, 4.1103, 4.1195, 4.2094, *, 4.0835, *, 4.0934, *, 4.1408, 4.1628.

Table A.2: $n = 3$, Class number 2

$n = 3$						
k	D_3	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
8	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907.	34, 38, 32, 34, 40, 34, 38, 34, 38, 36, 34, 46, 42, 38, 36, 34.	16, 25, 32, 33, 39, 33, 38, 34, 38, 36, 34, 46, 42, 38, 36, 34.	192, 300, 384, 396, 469, 369, 456, 408, 456, 432, 408, 552, 504, 456, 432, 408.	5.0117, 5.0198, 5.0036, 5.1259, 5.1630, 5.3382, 5.1292, 5.3493, 5.2714, 5.2158, 5.1541, 5.2563, 5.1358, 5.2352, 5.4068, 5.1869.	4.4873, 4.6353, 4.3639, 4.6249, 4.4024, 4.5428, 4.5263, 4.4458, 4.6462, 4.4582, 4.6522, 4.5579, 4.4585, 4.8293, 4.7691, 4.5826.
16	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907.	18, 10, 10, 18, 16, 16, 12, 16, 12, 12, 12, 14, 16, 14, 14, 10.	12, 6, 10, 18, 16, 15, 12, 16, 12, 12, 12, 14, 16, 14, 14, 10.	144, 72, 120, 216, 192, 180, 144, 192, 144, 144, 144, 168, 192, 168, 168, 120.	4.4103, 4.5279, 4.5106, 4.5168, 4.5757, 4.5983, 4.6637, 4.6170, 4.6186, 4.6277, 4.5980, 4.6062, 4.6082, 4.6556, 4.6332, 4.5743.	4.1982, 4.3373, 4.3983, 4.2550, 4.3806, 4.3421, 4.5231, 4.3588, 4.4189, 4.3742, 4.4678, 4.3760, 4.4379, 4.3509, 4.5069, 4.3117.
24	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907.	234, 142, 152, 176, 192, 186, 198, 178, 152, 160, 158, 196, 176, 174, 148, 166.	127, 75, 150, 174, 190, 183, 196, 178, 152, 159, 157, 196, 175, 174, 148, 165.	1524, 900, 1800, 2088, 2280, 2196, 2352, 2136, 1824, 1908, 1884, 2352, 2100, 2088, 1776, 1980.	4.5866, 4.5984, 4.6942, 4.6838, 4.6689, 4.6963, 4.7791, 4.6921, 4.6865, 4.7569, 4.7157, 4.6962, 4.6872, 4.7188, 4.7649, 4.6986.	4.1359, 4.3021, 4.2682, 4.1726, 4.1546, 4.3233, 4.3233, 4.2817, 4.3171, 4.2672, 4.3268, 4.2679, 4.3166, 4.2645, 4.2182, 4.2657.
32	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907.	22, 30, 18, 22, 20, 16, 10, 20, 18, 20, 20, 18, 14, 22, 14, 12.	12, 18, 17, 22, 19, 16, 10, 20, 18, 20, 20, 18, 14, 22, 14, 12.	144, 216, 204, 264, 228, 192, 120, 240, 216, 240, 240, 216, 168, 264, 168, 144.	4.2744, 4.3054, 4.3058, 4.2895, 4.3022, 4.3383, 4.3169, 4.3220, 4.3235, 4.2921, 4.3314, 4.3182, 4.3156, 4.3323, 4.3313, 4.3034.	4.1644, 4.1545, 4.1623, 4.1253, 4.1874, 4.2102, 4.1077, 4.1435, 4.1494, 4.1006, 4.2108, 4.1510, 4.2194, 4.1716, 4.2191, 4.1318.

$n = 3$ (continued)						
k	D_3	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
40	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907.	48, 70, 96, 76, 52, 50, 68, 54, 64, 62, 62, 62, 52, 74, 72, 60.	20, 26, 94, 73, 50, 50, 68, 54, 64, 62, 62, 62, 52, 74, 72, 60.	240, 312, 1128, 876, 600, 600, 816, 648, 768, 744, 744, 744, 624, 888, 864, 720.	4.3383, 4.3580, 4.3794, 4.3937, 4.3842, 4.3267, 4.4001, 4.3523, 4.4179, 4.4115, 4.3421, 4.3441, 4.3868, 4.4209, 4.3987, 4.4078.	4.1812, 4.2096, 4.0651, 4.1650, 4.1237, 4.1084, 4.1799, 4.1868, 4.2116, 4.1991, 4.2033, 4.2056, 4.2089, 4.2158, 4.1818, 4.1766.
48	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907.	82, 64, 78, 82, 80, 96, 104, 74, 74, 74, 80, 72, 72, 80, 74, 96.	47, 30, 78, 81, 78, 95, 103, 74, 73, 73, 80, 72, 72, 80, 74, 95.	564, 360, 936, 972, 936, 1140, 1236, 888, 876, 876, 960, 864, 864, 960, 888, 1140.	4.3033, 4.3320, 4.3478, 4.3344, 4.3529, 4.3909, 4.3833, 4.3659, 4.3882, 4.3896, 4.3911, 4.3946, 4.3895, 4.3585, 4.3838, 4.4096.	4.10173, 4.1846, 4.1392, 4.1137, 4.1328, 4.1849, 4.1562, 4.1542, 4.1594, 4.1622, 4.1336, 4.2219, 4.1690, 4.1788, 4.1758, 4.1712.
56	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907.	82, 68, 54, 62, 52, 62, 62, 48, 52, 48, 54, 66, 50, 52, 62, 54.	37, 33, 53, 60, 51, 61, 61, 48, 52, 48, 54, 66, 50, 51, 62, 54.	444, 396, 636, 720, 612, 732, 732, 576, 624, 576, 648, 792, 600, 612, 744, 648.	4.20667, 4.2561, 4.2306, 4.2428, 4.3004, 4.2513, 4.2933, 4.2554, 4.3028, 4.3391, 4.2750, 4.3199, 4.2612, 4.2612, 4.3054, 4.3251.	4.0667, 4.0811, 4.1212, 4.1140, 4.1160, 4.0718, 4.1420, 4.1264, 4.1208, 4.1192, 4.0933, 4.1106, 4.1248, 4.1183, 4.1724, 4.1687.

Table A.3: $n = 3$, Class number 3

$n = 3$						
k	D_4	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
8	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	6, 46, *, , *, 1, *, , *, *, 42, , , 1, *, , 1, *, 1, 38, *, 3, 54, 1, *, , *, *, 40, , , *, 30, *, *, 1, , , *, 2, *, *, 1, , , *, 1, 34, *, 38, *, 38, *, , *, 42, *, , , 46, 36, *, 40, *, , 40, 34, 42, 36, 32, 40.	3, 15, *, , *, 1, *, , *, *, 34, , , *, 1, 1, *, 1, 33, *, 3, 47, 1, *, , *, *, 35, , , *, 22, *, *, 1, , , *, 1, *, *, 2, , , *, 1, *, *, 1, , , *, 36, 23, *, 36, *, 22, *, , *, 36, *, , , 40, 32, *, 37, *, , 37, 31, 36, 25, 30, 33.	12, 240, *, , *, 16, *, , *, *, 544, , , 4, *, 4, 528, *, 24, 752, 16, *, , *, *, 560, , , *, 352, *, *, 16, , , *, 32, *, *, 16, , , *, 576, 368, *, 576, *, 352, *, , *, 576, *, , *, 640, 512, , , 592, *, , 592, 496, 576, 400, 480, 528.	5.0121, 5.0872, *, , *, 5.1400, *, , *, *, 5.0519, , , 4.7505, *, 4.8068, 5.0762, *, 4.6827, 5.2073, 5.0455, *, , *, *, 5.0727, , , *, 5.1888, *, *, 5.0559, , , *, 4.8844, , , *, 4.8110, 5.0833, *, 5.1357, *, 5.1734, *, , *, 5.2064, *, , *, 5.2571, 5.2675, *, 5.1651, *, , 5.2900, 5.1963, 5.2647, 5.2662, 5.1910, 5.2956.	4.6594, 4.4896, *, , *, 5.1400, *, , *, *, 4.3733, , , 4.7505, *, 4.8068, 4.5043, *, 4.3903, 4.7839, 5.0455, *, , *, *, 4.7925, , , *, 4.6565, *, *, 5.0559, , , *, 4.7876, *, *, 4.8110, , , *, 4.7046, 4.5048, *, 4.6322, *, , *, 4.6802, *, , *, 4.5896, 4.4889, *, 4.4855, *, , 4.5585, 4.7330, 4.6914, 4.6832, 4.5767, 4.6538.

$n = 3$ (continued)

k	D_4	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
16	39, 55, 56,	*, 10, *,	*, 5, *,	*, 80, *,	*, 4.5219, *,	*, 4.4064, *,
	68, 84, 120,	2, *, *,	2, *, *,	32, *, *,	4.5791, *, *,	4.5264, *, *,
	132, 136, 155,	*, 1, 18,	*, 1, 15,	*, 16, 240,	*, 4.7168, 4.5416,	*, 4.7168, 4.2821,
	168, 184, 195,	*, *, 1,	*, *, #,	*, *, #,	*, *, #,	*, *, #,
	203, 219, 228,	12, *, *,	11, *, *,	176, *, *,	4.5426, *, *,	4.3273, *, *,
	259, 280, 291,	8, *, *,	7, *, *,	112, *, *,	4.6813, *, *,	4.5799, *, *,
	292, 312, 323,	*, *, 6,	*, *, 6,	*, *, 96,	*, *, 4.6086,	*, *, 4.5067,
	328, 340, 355,	*, 1, 8,	*, 1, 4,	*, 16, 64,	*, 4.5352, 4.6087,	*, 4.5352, 4.5078,
	372, 388, 408,	*, *, 1,	*, *, 1,	*, *, 4,	*, *, 4.5752,	*, *, 4.5752,
	435, 483, 520,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	532, 555, 568,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	595, 627, 667,	8, *, 10,	7, *, 8,	112, *, 128,	4.5039, *, 4.6875,	4.29998, *, 4.5675,
	708, 715, 723,	*, 8, *,	*, 4, *,	*, 64, *,	*, 4.5377, *,	*, 4.4157, *,
	760, 763, 772,	*, 18, *,	*, 15, *,	*, 240, *,	*, 4.6584, *,	*, 4.5339, *,
	795, 955, 1003,	*, 14, 10,	*, 10, 10,	*, 160, 160,	*, 4.6520, 4.6155,	*, 4.4509, 4.4639,
	1012, 1027, 1227,	*, 10, *,	*, 9, *,	*, 144, *,	*, 4.6746, *,	*, 4.4635, *,
	1243, 1387, 1411,	12, 12, 18,	10, 11, 18,	160, 176, 288,	4.6471, 4.6344, 4.4061,	4.4903, 4.4257, 4.4167,
	1435, 1507, 1555.	10, 12, 14.	4, 11, 9.	64, 176, 144.	4.6289, 4.6839, 4.6338.	4.5234, 4.5666, 4.3983.

$n = 3$ (continued)						
k	D_4	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
24	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	22, 104, 23, 19, 16, 18, 15, 11, 142, 12, 8, 3, 190, 10, 10, 176, 7, 7, 2, 8, 194, 2, 7, 138, 11, 3, 7, 2, 3, 4, 5, 2, 2, 156, 2, 160, 3, 200, *, 4, 160, 2, 3, 186, 180, 2, 180, *, 180, 182, 172, 154, 192, 180.	10, 42, 14, 12, 7, 4, 10, 7, 120, 9, 5, 2, 154, 10, 1, 148, 1, 7, 2, 5, 157, #, #, 126, 2, #, 5, #, 2, #, #, 2, #, 115, 2, 148, 1, 151, *, #, 136, #, 2, 169, 160, 1, 168, *, 156, 166, 156, 118, 171, 162.	100, 672, 224, 192, 88, 64, 124, 112, 1920, 96, 80, 20, 2464, 136, 16, 2368, 16, 76, 32, 56, 2512, #, #, 2016, 20, #, 56, #, 8, #, #, 20, #, 1840, 32, 2368, 16, 2416, *, #, 2176, #, 32, 2704, 2560, 16, 2688, *, 2496, 2656, 2496, 1888, 2736, 2592.	4.5271, 4.5642, 4.4972, 4.5241, 4.5223, 4.5651, 4.5145, 4.5892, 4.6265, 4.5401, 4.5928, 4.6009, 4.6573, 4.5679, 4.6309, 4.75502, 4.6097, 4.5664, 4.5195, 4.4976, 4.6458, #, #, 4.7190, 4.5115, #, 4.5525, #, 4.5854, #, #, 4.5615, #, 4.6740, 4.7249, 4.7063, 4.6449, 4.7060, *, #, 4.7907, #, 4.5928, 4.7653, 4.7124, 4.6330, 4.7324, *, 4.7473, 4.7679, 4.7441, 4.6726, 4.7702, 4.7090.	4.3421, 4.2565, 4.2358, 4.3465, 4.3278, 4.2974, 4.3102, 4.4422, 4.2368, 4.4392, 4.4240, 4.5925, 4.1818, 4.3535, 4.6309, 4.2690, 4.6097, 4.2990, 4.4707, 4.2934, 4.2525, #, #, 4.2684, 4.4494, #, 4.3070, #, 4.5453, #, #, 4.5148, #, 4.2608, 4.6404, 4.3141, 4.6449, 4.2871, *, #, 4.3642, #, 4.5786, 4.2407, 4.2309, 4.6330, 4.2987, *, 4.3293, 4.3375, 4.3431, 4.3220, 4.2777, 4.3150.

$n = 3$ (continued)

k	D_4	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
32	39, 55, 56,	5, 22, *,	3, 8, *,	36, 128, *,	4.3159, 4.2958, *,	4.2533, 4.1923, *,
	68, 84, 120,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	132, 136, 155,	*, *, 8,	*, *, 6,	*, *, 96,	*, *, 4.2921,	*, *,4.2200
	168, 184, 195,	*, 1, *,	*, 1, *,	*, 16, *,	*, 4.3117, *,	*, 4.3117, *,
	203, 219, 228,	20, *, *,	16, *, *,	256, *, *,	4.3178, *, *,	4.2160, *, *,
	259, 280, 291,	22, *, *,	17, *, *,	272, *, *,	4.3541, *, *,	4.2193, *, *,
	292, 312, 323,	*, *, 18,	*, *, 16,	*, *, 256,	*, *, 4.2953,	*, *, 4.1377,
	328, 340, 355,	*, *, 14,	*, *, 10,	*, *, 160,	*, *, 4.3247,	*, *, 4.2678,
	372, 388, 408,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	435, 483, 520,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	532, 555, 568,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	595, 627, 667,	22, *, 10,	9, *, 10,	144, *, 160,	4.3152, *, 4.3498,	4.1397, *, 4.2392,
	708, 715, 723,	*, 16, *,	*, 11, *,	*, 176, *,	*, 4.3467, *,	*, 4.2800, *,
	760, 763, 772,	*, 16, *,	*, 15, *,	*, 240, *,	*, 4.3382, *,	*, 4.2923, *,
	795, 955, 1003,	*, 22, 18,	*, 17, 16,	*, 272, 256,	*, 4.3302, 4.3418,	*, 4.1477, 4.2602,
	1012, 1027, 1227,	*, 22, 1,	*, 21, 1,	*, 336, 16,	*, 4.3294, 4.3358,	*, 4.2126, 4.3358,
	1243, 1387, 1411,	20, 20, 22,	18, 19, 20,	288, 304, 320,	4.3167, 4.3247, 4.3213,	4.2430, 4.1486, 4.1145,
	1435, 1507, 1555.	16, 20, 20.	8, 19, 12.	128, 304, 192.	4.3183, 4.3316, 4.3122.	4.2783, 4.1936, 4.2111.

$n = 3$ (continued)

k	D_4	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
40	39, 55, 56,	9, 78, 3,	3, 21, 2,	12, 336, 32,	4.2422, 4.3907, 4.3171,	4.1792, 4.2368, 4.2963,
	68, 84, 120,	1, 3, 1,	#, 1, 1,	#, 4, 4,	#, 4.2598, 4.3786,	#, 4.2598, 4.3786,
	132, 136, 155,	*, 1, 70,	*, #, 51,	*, #, 816,	*, #, 4.3307,	*, #, 4.1084,
	168, 184, 195,	1, *, 3,	#, *, 3,	#, *, 36,	#, *, 4.2999,	#, *, 4.2205,
	203, 219, 228,	60, 2, *,	51, 2, *,	816, 20, *,	4.3292, 4.2518, *,	4.1613, 4.1812, *,
	259, 280, 291,	72, *, 1,	59, *, 1,	944, *, 16,	4.3608, *, 5.3044,	4.1107, *, 5.3044,
	292, 312, 323,	*, 1, 72,	*, 1, 58,	*, 4, 928,	*, 4.1438, 4.3236,	*, 4.1438, 4.1019,
	328, 340, 355,	*, *, 48,	*, *, 38,	*, *, 608,	*, *, 4.4010,	*, *, 4.1028,
	372, 388, 408,	*, 1, *,	*, #, *,	*, #, *,	*, #, *,	*, #, *,
	435, 483, 520,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	532, 555, 568,	*, *, *,	*, *, *,	*, *, *,	*, *, *,	*, *, *,
	595, 627, 667,	102, *, 56,	59, *, 53,	944, *, 848,	4.3748, *, 4.4397,	4.2022, *, 4.1208,
	708, 715, 723,	1, 78, *,	#, 54, *,	#, 864, *,	#, 4.3794, *,	#, 4.1917, *,
	760, 763, 772,	*, 46, *,	*, 42, *,	*, 672, *,	*, 4.4141, *,	*, 4.2272, *,
	795, 955, 1003,	*, 64, 90,	*, 50, 79,	*, 800, 1264,	*, 4.3971, 4.3810,	*, 4.1874, 4.1776,
	1012, 1027, 1227,	*, 32, *,	*, 28, *,	*, 448, *,	*, 4.4217, *,	*, 4.2089, *,
	1243, 1387, 1411,	58, 58, 62,	56, 50, 56,	896, 800, 896,	4.3841, 4.4684, 4.4055,	4.1838, 4.1807, 4.2307,
	1435, 1507, 1555.	46, 48, 44.	29, 46, 33.	464, 736, 528.	4.3470, 4.3563, 4.3722.	4.1757, 4.2075, 4.2075.

$n = 3$ (continued)

k	D_4	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
48	39, 55, 56,	8, 34, 5,	4, 15, 2,	40, 240, 32,	4.3369, 4.3179, 4.3531,	4.2065, 4.1381, 4.3496,
	68, 84, 120,	5, 6, 6,	2, 3, 2,	32, 48, 32,	4.2363, 4.3045, 4.3102,	4.1390, 4.2928, 4.2688,
	132, 136, 155,	8, 5, 64,	4, 4, 54,	40, 64, 864,	4.2916, 4.3262, 4.3285,	4.1049, 4.2739, 4.1223,
	168, 184, 195,	6, 3, 3,	3, 2, 2,	48, 32, 20,	4.2841, 4.3642, 4.2924,	4.2556, 4.3433, 4.2458,
	203, 219, 228,	76, 2, 4,	63, 2, 2,	1008, 20, 32,	4.3624, 4.3536, 4.2507,	4.1410, 4.3074, 4.2441,
	259, 280, 291,	92, 2, 4,	82, #, 4,	1312, #, 52,	4.40136, #, 4.2903,	4.1490, #, 4.2059,
	292, 312, 323,	1, 2, 70,	1, #, 68,	16, #, 1088,	4.2365, #, 4.3498,	4.2365, #, 4.1283,
	328, 340, 355,	1, 1, 72,	#, #, 64,	#, #, 1024,	#, #, 4.4050,	#, #, 4.2060,
	372, 388, 408,	2, 2, 1,	#, #, 1,	#, #, 4,	#, #, 4.2955,	#, #, 4.2955,
	435, 483, 520,	*, *, 4,	*, *, #,	*, *, #,	*, *, #,	*, *, #,
	532, 555, 568,	', ', 4,	', ', #,	', ', #,	', ', #,	', ', #,
	595, 627, 667,	2, 1, *,	#, #, *,	#, #, *,	#, #, *,	#, #, *,
	708, 715, 723,	72, 2, 70.	57, 1, 68.	912, 4, 1088.	4.3745, 4.4840, 4.4083.	4.1921, 4.4840, 4.1993.
	760, 763, 772,	1, 100, *,	1, 80, *,	16, 1280, *,	4.2315, 4.3448, *,	4.2315, 4.1372, *,
	795, 955, 1003,	1, 76, *,	#, 70, *,	#, 1120, *,	#, 4.3733, *,	#, 4.1183, *,
	1012, 1027, 1227,	1, 86, 86,	#, 76, 83,	#, 1216, 1328,	#, 4.3899, 4.3955,	#, 4.1511, 4.2116,
	1243, 1387, 1411,	1, 86, *,	#, 78, *,	#, 1248, *,	#, 4.4065, *,	#, 4.1616, *,
	1435, 1507, 1555.	78, 70, 86,	69, 68, 83,	1104, 1088, 1328,	4.4086, 4.4058, 4.3875,	4.1939, 4.2008, 4.2121,
		64, 86, 80.	50, 75, 77.	800, 1200, 1232.	4.3759, 4.3785, 4.3977.	4.1561, 4.1739, 4.1613.

$n = 3$ (continued)						
k	D_4	NRR	VIT	B-F-S curves	average ρ-value	smallest ρ-value
56	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	6, 38, 3, 2, 6, 2, 1, 1, 68, 3, *, 2, 90, 1, 1, 70, *, 1, *, *, 64, *, *, 48, 1, *, 1, *, *, *, 1, *, *, 84, *, 70, *, 38, *, *, 42, *, 1, 60, 72, *, 78, *, 58, 54, 60, 64, 60, 40.	2, 13, 2, 2, 3, 2, 1, 1, 55, 2, *, 1, 74, 1, #, 54, *, 1, *, *, 57, *, *, 42, 1, *, 1, *, *, *, #, *, *, 51, *, 65, *, 22, *, *, 37, *, 1, 45, 70, *, 69, *, 55, 49, 56, 44, 51, 31.	8, 208, 32, 32, 24, 20, 16, 16, 880, 20, *, 4, 1184, 16, #, 864, *, 4, *, *, 912, *, *, 672, 16, *, 4, *, *, *, #, *, *, 816, *, 1040, *, 352, *, *, 592, *, 16, 720, 1120, *, 1104, , 880, 784, 896, 704, 816, 496.	4.1830, 4.2469, 4.1786, 4.2092, 4.1972, 4.2293, 4.2286, 4.2285, 4.2530, 4.2038, *, 4.1956, 4.2684, 4.5579, #, 4.3231, *, 4.24499, *, *, 4.2472, *, *, 4.2499, 4.2031, *, 4.1626, *, *, *, #, *, *, 4.2749, *, 4.2730, *, 4.2779, *, *, 4.3057, *, 4.2573, 4.3184, 4.2969, *, 4.2987, *, 4.3004, 4.3279, 4.2327, 4.3394, 4.2527, 4.3453.	4.1765, 4.1476, 4.1704, 4.1928, 4.1872, 4.2022, 4.2286, 4.2285, 4.0746, 4.1850, *, 4.1956, 4.1362, 4.5579, #, 4.1634, *, 4.2450, *, *, 4.1471, *, *, 4.1834, 4.2031, *, 4.1626, *, *, *, #, *, *, 4.0915, *, 4.1121, *, 4.1834, *, *, 4.0861, *, 4.2573, 4.0900, 4.1132, *, 4.1394, *, 4.1186, 4.1711, 4.0978, 4.1629, 4.1453, 4.1740.

Table A.4: $n = 3$, Class number 4

$n = 4$						
k	D_1	NRR	VIT	L-S curves	average ρ-value	smallest ρ-value
8	7, 8, 11, 19, 43, 67, 163,	*, *, *, *, *, *, *.	*, *, *, *, *, *, *.	*, *, *, *, *, *, *.	*, *, *, *, *, *, *.	*, *, *, *, *, *, *.
16	7, 8, 11, 19, 43, 67, 163,	*, 14, *, *, *, *, *.	*, 28, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.
24	7, 8, 11, 19, 43, 67, 163,	*, 52, *, *, *, *, *.	*, 149, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.
32	7, 8, 11, 19, 43, 67, 163,	*, 28, *, *, *, *, *.	*, 30, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.
40	7, 8, 11, 19, 43, 67, 163,	*, 10, *, *, *, *, *.	*, 14, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.
48	7, 8, 11, 19, 43, 67, 163,	*, 20, *, *, *, *, *.	*, 32, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.
56	7, 8, 11, 19, 43, 67, 163,	*, 12, *, *, *, *, *.	*, 9, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.	*, #, *, *, *, *, *.

Table A.5: $n = 4$, Class number 1

,

$n = 4$						
k	D_2	NRR	VIT	L-S curves	average ρ-value	smallest ρ-value
8	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, 12, *, *, *, *, *, *, *, *, 1, *, *, *, *.	*, *, *, *, 12, *, *, *, *, *, *, *, *, 1, *, *, *, *.	*, *, *, *, 24, *, *, *, *, *, *, *, *, 2, *, *, *, *.	*, *, *, *, 4.8453, *, *, *, *, *, *, *, *, 4.6397, *, *, *, *.	*, *, *, *, 4.2596, *, *, *, *, *, *, *, *, 4.6397, *, *, *, *.
16	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
24	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, 25, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 16, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 32, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 4.8160, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 4.3946, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
32	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
40	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, 10, *, *, *, *, 2, *, *, *, *, *, *, *, *, *, *.	*, *, 6, *, *, *, *, 2, *, *, *, *, *, *, *, *, *, *.	*, *, 12, *, *, *, *, 4, *, *, *, *, *, *, *, *, *, *.	*, *, 4.5693, *, *, *, *, 4.2710, *, *, *, *, *, *, *, *, *, *.	*, *, 4.2467, *, *, *, *, 4.2710, *, *, *, *, *, *, *, *, *, *.
48	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, 9, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 4, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 8, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 4.3540, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 4.2542, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
56	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, 6, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 3, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 6, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 4.7902, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, 4.1781, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.

Table A.6: $n = 4$, Class number 2

$n = 4$						
k	D_3	NRR	VIT	L-S curves	average ρ-value	smallest ρ-value
8	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *.	*, *.	*, *.	*, *.	*, *.
16	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *.	*, *.	*, *.	*, *.	*, *.
24	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *.	*, *.	*, *.	*, *.	*, *.
32	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *.	*, *.	*, *.	*, *.	*, *.
40	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *.	*, *.	*, *.	*, *.	*, *.
48	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *.	*, *.	*, *.	*, *.	*, *.
56	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *.	*, *.	*, *.	*, *.	*, *.

Table A.7: $n = 4$, Class number 3

$n = 4$						
k	D_4	NRR	VIT	L-S curves	average ρ-value	smallest ρ-value
8	39, 55, 56, 68,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	84, 120, 132, 136,	*, 1, *, *,	*, 1, *, *,	*, 4, *, *,	*, 5.1106, *, *,	*, 5.1106, *, *,
	155, 168, 184, 195,	*, 3, *, *,	*, 2, *, *,	*, 8, *, *,	*, 7.4205, *, *,	*, 4.9601, *, *,
	203, 219, 228, 259,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	280, 291, 292, 312,	*, *, 2, *,	*, *, 2, *,	*, *, 8, *,	*, *, 5.6523, *,	*, *, 5.2046, *,
	323, 328, 340, 355,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	372, 388, 408, 435,	*, 1, *, *,	*, 1, *, *,	*, 4, *, *,	*, 5.2743, *, *,	*, 5.2743, *, *,
	483, 520, 532, 555,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	568, 595, 627, 667,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	708, 715, 723, 760,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	763, 772, 795, 955,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1003,1012, 1027, 1227,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1243, 1387, 1411, 1435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1507, 1555.	*, *.	*, *.	*, *.	*, *.	*, *.
16	39, 55, 56, 68,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	84, 120, 132, 136,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	155, 168, 184, 195,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	203, 219, 228, 259,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	280, 291, 292, 312,	*, *, 1, *,	*, *, 1, *,	*, *, 4, *,	*, *, 4.5880, *,	*, *, 4.5880, *,
	323, 328, 340, 355,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	372, 388, 408, 435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	483, 520, 532, 555,	*, 2, *, *,	*, 2, *, *,	*, 8, *, *,	*, 4.5374, *, *,	*, 4.4888, *, *,
	568, 595, 627, 667,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	708, 715, 723, 760,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	763, 772, 795, 955,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1003,1012, 1027, 1227,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1243, 1387, 1411, 1435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1507, 1555.	*, *.	*, *.	*, *.	*, *.	*, *.

$n = 4$ (continued)						
k	D_4	NRR	VIT	L-S curves	average ρ-value	smallest ρ-value
24	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003,1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	*, *, 5, 3, *, 4, *, 4, *, *, *, *, *, *, *, *, *, *, *, 2, *, 1, *, *, *, *, 3, *.	*, *, 1, 3, *, 2, *, 3, *, *, *, *, *, *, *, *, *, *, *, 2, *, 1, *, *, *, *, 2, *.	*, *, 4, 12, *, 8, *, 12, *, *, *, *, *, *, *, *, *, *, *, 8, *, 4, *, *, *, *, 8, *.	*, *, 4.4954, 4.5240, *, 4.5738, *, 4.6967, *, *, *, *, *, *, *, *, *, *, *, 4.6271, *, 4.6461, *, *, *, *, 4.6536, *.	*, *, 4.4954, 4.4490, *, 4.5550, *, 4.5268, *, *, *, *, *, *, *, *, *, *, *, 4.5609, *, 4.6461, *, *, *, *, 4.6120, *.
32	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003,1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	*, *, *, *, *, *, *, 2, *, *, *, *, *, *, *, *, 1, *, 2, *, *, *, *, *, *, 1, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 1, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, 2, *, *, *, *, *, *, *, *, #, *, 2, *, *, *, *, *, *, 1, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 1, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, 8, *, *, *, *, *, *, *, *, #, *, 8, *, *, *, *, *, *, 4, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 4, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, 4.2463, *, *, *, *, *, *, *, *, #, *, 4.3142, *, *, *, *, *, *, 4.3048, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 4.2368, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, 4.2425, *, *, *, *, *, *, *, *, #, *, 4.3007, *, *, *, *, *, *, 4.3048, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 4.2368, *, *, *, *, *, *, *, *, *, *, *, *.

$n = 4$ (continued)						
k	D_4	NRR	VIT	L-S curves	average ρ-value	smallest ρ-value
40	39, 55, 56, 68,	*, *, 7, *,	*, *, 1, *,	*, *, 4, *,	*, *, 4.4051, *,	*, *, 4.4051, *,
	84, 120, 132, 136,	*, 4, *, *,	*, 1, *, *,	*, 4, *, *,	*, 4.2500, *, *,	*, 4.2500, *, *,
	155, 168, 184, 195,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	203, 219, 228, 259,	*, *, 1, *,	*, *, 1, *,	*, *, 4, *,	*, *, 4.2821, *,	*, *, 4.2821, *,
	280, 291, 292, 312,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	323, 328, 340, 355,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	372, 388, 408, 435,	*, *, 1, *,	*, *, 1, *,	*, *, 4, *,	*, *, 4.3155, *,	*, *, 4.3155, *,
	483, 520, 532, 555,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	568, 595, 627, 667,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	708, 715, 723, 760,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	763, 772, 795, 955,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1003,1012, 1027, 1227,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1243, 1387, 1411, 1435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1507, 1555.	*, *.	*, *.	*, *.	*, *.	*, *.
48	39, 55, 56, 68,	*, *, 4, 2,	*, *, 2, #,	*, *, 8, #,	*, *, 4.6408, #,	*, *, 4.2990, #,
	84, 120, 132, 136,	*, 4, *, 1,	*, 1, *, #,	*, 4, *, #,	*, 4.4617, *, #,	*, 4.4617, *, #,
	155, 168, 184, 195,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	203, 219, 228, 259,	*, *, 1, *,	*, *, 1, *,	*, *, 4, *,	*, *, 4.2420, *,	*, *, 4.2420, *,
	280, 291, 292, 312,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	323, 328, 340, 355,	*, 1, *, *,	*, #, *, *,	*, #, *, *,	*, #, *, *,	*, #, *, *,
	372, 388, 408, 435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	483, 520, 532, 555,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	568, 595, 627, 667,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	708, 715, 723, 760,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	763, 772, 795, 955,	*, 1, *, *,	*, 1, *, *,	*, 4, *, *,	*, 4.2714, *, *,	*, 4.2714, *, *,
	1003,1012, 1027, 1227,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1243, 1387, 1411, 1435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1507, 1555.	*, *.	*, *.	*, *.	*, *.	*, *.

$n = 4$						
k	D_4	NRR	VIT	L-S curves	average ρ-value	smallest ρ-value
56	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003,1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	*, *, *, *, 5, *, 2, *, 1, *, *, 1, *, *, *, *, *, 2, *, *, 1, *, *, *, *, *, *, *, *, *, 1, *, *, *, *, *, *, 1, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, #, *, 1, *, 1, *, *, #, *, *, *, *, *, #, *, *, *, #, *, *, *, *, *, *, *, *, *, 1, *, *, *, *, *, *, #, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, #, *, 4, *, 4, *, *, #, *, *, *, *, *, #, *, *, *, #, *, *, *, *, *, *, *, *, *, 4, *, *, *, *, *, *, #, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, #, *, 4.1625, *, 4.1990, *, *, #, *, *, *, *, *, #, *, *, *, #, *, *, *, *, *, *, *, *, *, 4.1371, *, *, *, *, *, *, #, *, *, *, *, *, *, *, *, *, *, *, *, *.

Table A.8: $n = 4$, Class number 4

$n = 6$							
k	D_1	NRR	VIT	suitable VIT	B-F-S curves	average ρ-value	smallest ρ-value
8	7, 8, 11, 19, 43, 67, 163.	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .
16	7, 8, 11, 19, 43, 67, 163.	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .
24	7, 8, 11, 19, 43, 67, 163.	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .
32	7, 8, 11, 19, 43, 67, 163.	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .
40	7, 8, 11, 19, 43, 67, 163.	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .
48	7, 8, 11, 19, 43, 67, 163.	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .
56	7, 8, 11, 19, 43, 67, 163.	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .	* * * * * * , , , , , , * , * .

Table A.9: $n = 6$, Class number 1

$n = 6$							
k	D_2	NRR	VIT	suitable VIT	B-F-S currves	average ρ-value	smallest ρ-value
8	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
16	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
24	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
32	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.

$n = 6$ (continued)							
k	D_2	NRR	VIT	suitable VIT	B-F-S currves	average ρ-value	smallest ρ-value
40	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
48	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.
56	15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.	*, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *, *.

Table A.10: $n = 6$, Class number 2

$n = 6$

k	D_3	NRR	VIT	suitable VIT	B-F-S curves	average ρ-value	smallest ρ-value
8	23, 31, 59, 83,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	40, 51, 52, 88,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	107, 139, 211, 283,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	307, 331, 379, 499,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	547, 643, 883, 907.	* , * .	* , * .	* , * .	* , * .	* , * .	* , * .
16	23, 31, 59, 83,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	40, 51, 52, 88,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	107, 139, 211, 283,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	307, 331, 379, 499,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	547, 643, 883, 907.	* , * .	* , * .	* , * .	* , * .	* , * .	* , * .
24	23, 31, 59, 83,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	40, 51, 52, 88,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	107, 139, 211, 283,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	307, 331, 379, 499,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	547, 643, 883, 907.	* , * .	* , * .	* , * .	* , * .	* , * .	* , * .
32	23, 31, 59, 83,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	40, 51, 52, 88,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	107, 139, 211, 283,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	307, 331, 379, 499,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,	* , * , * , * ,
	547, 643, 883, 907.	* , * .	* , * .	* , * .	* , * .	* , * .	* , * .

$n = 6$ (continued)

k	D_3	NRR	VIT	suitable VIT	B-F-S currves	average ρ-value	smallest ρ-value
40	23, 31, 59, 83,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	40, 51, 52, 88,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	107, 139, 211, 283,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	307, 331, 379, 499,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	547, 643, 883, 907.	* *.	* *.	* *.	* *.	* *.	* *.
48	23, 31, 59, 83,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	40, 51, 52, 88,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	107, 139, 211, 283,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	307, 331, 379, 499,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	547, 643, 883, 907.	* *.	* *.	* *.	* *.	* *.	* *.
56	23, 31, 59, 83,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	40, 51, 52, 88,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	107, 139, 211, 283,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	307, 331, 379, 499,	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *
	547, 643, 883, 907.	* *.	* *.	* *.	* *.	* *.	* *.

Table A.11: $n = 6$, Class number 3

$n = 6$							
k	D_4	NRR	VIT	suitable VIT	B-F-S currves	average ρ-value	smallest ρ-value
8	39, 55, 56, 68,	5, *, *, *,	84, *, *, *,	5, *, *, *,	10, *, *, *,	5.0129, *, *, *,	4.9222, *, *, *,
	84, 120, 132, 136,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	155, 168, 184, 195,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	203, 219, 228, 259,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	280, 291, 292, 312,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	323, 328, 340, 355,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	372, 388, 408, 435,	1, *, *, 1,	65, *, *, 37,	#, *, *, #,	#, *, *, #,	#, *, *, #,	#, *, *, #,
	483, 520, 532, 555,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	568, 595, 627, 667,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	708, 715, 723, 760,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	763, 772, 795, 955,	*, *, 1, *,	*, *, 1, *,	*, *, 1, *,	*, *, 4, *,	*, *, 4.9215, *,	*, *, 4.9215, *,
	1003, 1012, 1027, 1227,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1243, 1387, 1411, 1435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1507, 1555.	*, *.	*, *.	*, *.	*, *.	*, *.	*, *.
16	39, 55, 56, 68,	2, *, *, *,	37, *, *, *,	#, *, *, *,	#, *, *, *,	#, *, *, *,	#, *, *, *,
	84, 120, 132, 136,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	155, 168, 184, 195,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	203, 219, 228, 259,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	280, 291, 292, 312,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	323, 328, 340, 355,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	372, 388, 408, 435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	483, 520, 532, 555,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	568, 595, 627, 667,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	708, 715, 723, 760,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	763, 772, 795, 955,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1003, 1012, 1027, 1227,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1243, 1387, 1411, 1435,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,	*, *, *, *,
	1507, 1555.	*, *.	*, *.	*, *.	*, *.	*, *.	*, *.

$n = 6$ (continued)							
k	D_4	NRR	VIT	suitable VIT	B-F-S currves	average ρ-value	smallest ρ-value
24	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	12, *, *, *, 5, 8, *, *, *, *, *, *, *, 4, 9, *, *, 1, *, *, *, *, *, *, 1, *, 3, 2, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 2, *, *, *, *, *, *, *, *, *, *, *.	115, *, *, *, 63, 87, *, *, *, *, *, *, *, 17, 197, *, *, 8, *, *, *, *, *, *, 20, *, 47, 38, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 2, *, *, *, *, *, *, *, *, *, *, *.	16, *, *, *, #, 3, *, *, *, *, *, *, *, 3, #, *, *, #, *, *, *, *, *, *, #, *, 1, #, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 2, *, *, *, *, *, *, *, *, *, *, *.	26, *, *, *, #, 6, *, *, *, *, *, *, *, 8, #, *, *, #, *, *, *, *, *, *, #, *, 2, #, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 6, *, *, *, *, *, *, *, *, *, *, *.	4.6390, *, *, *, #, 4.8233, *, *, *, *, *, *, *, 5.0658, #, *, *, #, *, *, *, *, *, *, *, *, 4.5958, #, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 4.6388, *, *, *, *, *, *, *, *, *, *, *.	4.5071, *, *, *, #, 4.5878, *, *, *, *, *, *, *, 4.6578, #, *, *, #, *, *, *, *, *, *, *, *, 4.5958, #, *, *, *, *, *, *, *, *, *, *, *, *, *, *, 4.5766, *, *, *, *, *, *, *, *, *, *, *.
32	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	3, *, *, *, 2, *, 1, *.	3, *, *, *, 9, *, 8, *.	3, *, *, *, #, *, #, *.	10, *, *, *, #, *, #, *.	4.2373, *, *, *, #, *, #, *.	4.1897, *, *, *, #, *, #, *.

$n = 6$ (continued)							
k	D_4	NRR	VIT	suitable VIT	B-F-S currves	average ρ-value	smallest ρ-value
40	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	12, *, *, *, *, 2, *, *, *, *, *, *, *, *, 5, *, *, 1, *, 1, *, *, *, *, *, *.	68, *, *, *, *, 12, *, *, *, *, *, *, *, *, 62, *, *, 1, *, 1, *, *, *, *, *, *.	7, *, *, *, *, 1, *, *, *, *, *, *, *, *, #, *, *, 1, *, 1, *, *, *, *, *, *.	18, *, *, *, *, 4, *, *, *, *, *, *, *, *, #, *, *, 4, *, 2, *, *, *, *, *, *.	4.3018, *, *, *, *, 4.2770, *, *, *, *, *, *, *, *, #, *, *, 4.3715, *, 4.5592, *, *, *, *, *, *.	4.2269, *, *, *, *, 4.2770, *, *, *, *, *, *, *, *, #, *, *, 4.3715, *, 4.5592, *, *, *, *, *, *.
48	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	5, *, *, *, 1, 6, *, *, *, *, *, *, *, 1, 1, *, *, *, *, *, *, *, *, *, 1, *, *, 3, *.	27, *, *, *, 12, 36, *, *, *, *, *, *, *, 1, 12, *, *, *, *, *, *, *, *, *, 14, *, *, 3, *.	3, *, *, *, #, 2, *, *, *, *, *, *, *, 1, #, *, *, *, *, *, *, *, *, *, #, *, *, 3, *.	8, *, *, *, #, 4, *, *, *, *, *, *, *, 2, #, *, *, *, *, *, *, *, *, *, #, *, *, 6, *.	4.3545, *, *, *, #, 4.3393, *, *, *, *, *, *, *, 4.3225, #, *, *, *, *, *, *, *, *, *, #, *, *, 4.3557, *.	4.2810, *, *, *, #, 4.3393, *, *, *, *, *, *, *, 4.3225, #, *, *, *, *, *, *, *, *, *, #, *, *, 4.3512, *.

$n = 6$ (continued)							
k	D_4	NRR	VIT	suitable VIT	B-F-S currves	average ρ-value	smallest ρ-value
56	39, 55, 56, 68, 84, 120, 132, 136, 155, 168, 184, 195, 203, 219, 228, 259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532, 555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.	13, *, *, *, 8, 6, *, *, *, *, *, *, *, *, 2, *, *, *, *, *, *, *, *, *, 3, *, 2, 1, *.	35, *, *, *, 38, 22, *, *, *, *, *, *, *, *, 13, *, *, *, *, *, *, *, *, *, 35, *, 11, 8, *.	8, *, *, *, #, 1, *, *, *, *, *, *, *, *, #, *, *, *, *, *, *, *, *, *, #, *, #, #, *.	28, *, *, *, #, 2, *, *, *, *, *, *, *, *, #, *, *, *, *, *, *, *, *, *, #, *, #, #, *.	4.2062, *, *, *, #, 4.1822, *, *, *, *, *, *, *, *, #, *, *, *, *, *, *, *, *, *, #, *, #, #, *.	4.1654, *, *, *, #, 4.1822, *, *, *, *, *, *, *, *, #, *, *, *, *, *, *, *, *, *, #, *, #, #, *.

Table A.12: $n = 6$, Class number 4