SCIS 2010 The 2010 Symposium on Cryptography and Information Security
Takamatsu, Japan, Jan. 19-22, 2010
The Institute of Electronics, Information and Communication Engineers

Fields of definition of torsion points on the Jacobians of genus 2 hyperelliptic curves over finite fields

Tsukasa Ishiguro* Kazuto Matsuo*

Abstract— This paper deals with fields of definition of the l-torsion points on the Jacobians of genus 2 hyperelliptic curves over finite fields in order to speed Gaudry and Schost's point counting algorithm for genus 2 hyperelliptic curves up. A result in this paper shows that the extension degrees of the fields of difinition of the l-torsion points can be in $O(l^3)$ instead of $O(l^4)$. The effects of the result on the point counting algorithm are also discussed in this paper. The discussion concludes that the result in this paper reduces the complexity of the algorithm over $\mathbb{F}_q$ to $O((\log q)^{8.797+o(1)})$ operations in $\mathbb{F}_q$.

Keywords: hyperelliptic curve cryptosystems, genus 2 hyperelliptic curves, Jacobians, l-adic point counting algorithms, torsion points

1 Introduction

For construction of secure hyperelliptic curve cryptosystems [Kob89], square-root algorithms [Elk95, Sut09], CM-field algorithms [Kob97, Wen03, CMT00, CMKT00, MHCT01, Tak02, HKT04], Koblitz's algorithms [Kob89, KNU03], p-adic algorithms [Wan99, Ked01, LW02, Ver02, LL06], and l-adic algorithms are known in common with elliptic curve cryptosystems. Since the l-adic algorithms can be applied to a large class of hyperelliptic curves, an l-adic algorithm that can construct abundantly secure cryptosystems is expected to put hyperelliptic curve cryptosystems to practical use.

The l-adic algorithms are algorithms to count the rational points on the Jacobian of a genus g hyperelliptic curve over a finite field $\mathbb{F}_q$ by seeing the action of the Frobenius map on the l-torsion points for $O(g \log q)$ primes $l \in O(g \log q)$. Schoof [Sch85] originally proposed an l-adic algorithm for elliptic curves, Pila [Pil90] then generalized one for Abelian varieties, including the Jacobians of hyperelliptic curves. Afterwards, many algorithms were proposed for Abelian varieties and the Jacobians of hyperelliptic curves [Kam91, AH96, HI98, GH00, GS04]. Gaudry and Harley [GH00] proposed an l-adic algorithm for the Jacobians of genus 2 hyperelliptic curves. A distinguished point of their algorithm is to obtain *univariate* l-division polynomials for general divisor classes from Cantor's division polynomials [Can94] for the Theta divisors. This leads the algorithm into practical use. Gaudry and Harley [GH00] actually succeeded 128-bit point counting using their algorithm. Moreover [MCT03] also succeeded 160-bit point counting using their algorithm. Gaudry and Schost [GS04] improved Gaudry and Harley's division polynomials in their point counting algorithm (the Gaudry-Schost algorithm). The Gaudry-Schost algorithm can obtain l-division polynomials of degree $\frac{l^4-1}{2}$. We can see that this degree is minimum by analogy with the elliptic curve division polynomial whose degree is $\frac{l^2-1}{2}$. They succeeded 160-bit point counting over a prime field using their algorithm.

However the computations introduced above involved special properties of the definition fields. The result in [MCT03] was obtained for curves over an extension field of degree 4 for which an attack [AMNS06] that is asymptotically faster than the rho method is known. [GS04] used the definition fields whose multiplicative orders were divided by all ls used in the computation so as to reduce the complexity of factoring the division polynomials that dominates the complexity of the Gaudry-Schost algorithm in general as described later. On the other hand, definition fields with fast arithmetic are often used in order to construct efficient (hyper)elliptic curve cryptosystems [BP98, KMKH99, AHK01, GMA+05]. Unfortunately, it is difficult to apply the field selection technique used in [GS04] for the fast arithmetic fields, because the field condition that the Gaudry-Schost algorithm is fast and the condition that the arithmetic is fast are different. Recently, Gaudry and Schost succeeded 254-bit point counting of a family of hyperelliptic curves over a fast arithmetic prime field [GS08]. In their computation, a new fast method that involves almost no factoring was used. However there exist the Jacobians whose orders are difficult to determine by the method. Therefore efficient point counting algorithm is still an issue of general genus 2 hyperelliptic curve cryptosystems.

In order to improve factoring Gaudry and Schost's l-division polynomials of the Jacobians of genus 2 hyperelliptic curves over finite fields, we discuss properties of the factorization of the division polynomials in

* Institute of Information Security, 2-14-1, Tsuruya-cho, Kanagawa-ku, Yokohama 221-0835, Japan.

this paper. Though [GS05] already gave the properties of the factorization of modular polynomials of genus 2 hyperelliptic curves, it did not deal with the l-division polynomials. Using the similar manner of [GS05], this paper shows the extension degrees of the fields of definition of the l-torsion points for each type that is classified by using the factorization modulo l of the characteristic polynomial of the Frobenius map. The extension degrees correspond with the maximum degrees of the irreducible factors of the division polynomials. The result shows that the degrees of the irreducible factors of the l-division polynomials of the Jacobians of genus 2 hyperelliptic curves are bounded by $O(l^3)$. This property can yield an efficient point counting algorithm for genus 2 hyperelliptic curves, so that the effects of this property on the point counting algorithm are also discussed in this paper.

In this paper, we assume that an operation of univariate polynomials of degree n over $\mathbb{F}_q$ takes $O(n^{1+o(1)})$ operations in $\mathbb{F}_q$.

2 Torsion points and Frobenius map

Let $\mathcal{J}$ be the Jacobian of a genus 2 hyperelliptic curve over a finite field $\mathbb{F}_q$ of odd characteristic and $\chi \in \mathbb{Z}[X]$ the characteristic polynomial of the qth Frobenius map. χ can be written with $s_1,\ s_2 \in \mathbb{Z}$ as

$$\chi = X^4 - s_1X^3 + s_2X^2 - s_1qX + q^2.$$

It is known that the roots of χ satisfy Theorem 1 below [Sti09, Theorem 5.1.15. (e)].

Theorem 1. *Let α_i for $i = 1, \ldots, 4$ be the roots of χ. These α_is can be arranged as*

$$\alpha_1\alpha_3 = \alpha_2\alpha_4 = q$$

holds.

Let l be a prime number relatively prime to q. An element of the l-torsion subgroup

$$\mathcal{J}[l] = \{\mathcal{D} \in \mathcal{J} \mid [l]\mathcal{D} = 0\}$$

is called a l-torsion point on $\mathcal{J}$. The relation

$$\mathcal{J}[l] \cong \mathbb{F}_l^4$$

holds for the l-torsion subgroup [HS00, Theorem A.7.2.7].

The qth Frobenius map of $\mathcal{J}$ acts on $\mathcal{J}[l]$ as an $\mathbb{F}_l$-linear map. We denote the matrix corresponding to the qth Frobenius map by $T \in GL_4(\mathbb{F}_l)$.

Let $\mathbb{F}_{l^n}$ be the minimum extension of $\mathbb{F}_l$ that contains all eigenvalues of T. T can be decomposed as

$$T = PAP^{-1},$$

where $A \in GL_4(\mathbb{F}_{l^n})$ is in Jordan canonical form[1] and $P \in GL_4(\mathbb{F}_{l^n})$.

Let $\tilde{\chi}$ be the reduction of χ modulo l, i.e.

$$\tilde{\chi} = X^4 - \tilde{s}_1X^3 + \tilde{s}_2X^2 - \tilde{s}_1\tilde{q}X + \tilde{q}^2,$$

where $\tilde{q},\ \tilde{s}_1,\ \tilde{s}_2 \in \mathbb{F}_l$ are the residues of $q,\ s_1,\ s_2$ modulo l respectively. $\tilde{\chi}$ is the characteristic polynomial of T and its roots are the eigenvalues of T.

If $l \ll q$, which is usually satisfied in cryptographical use, then $\tilde{s}_1,\ \tilde{s}_2$ can be considered as random elements in $\mathbb{F}_l$.

A classification of the factorization types of $\tilde{\chi}$ over $\mathbb{F}_l$ is given by [GS05]. Column "Char. Poly." in Table 1 shows the classification according to [GS05, Table A.1]. In the column, abbreviation "$[n_1]^{c_1}[n_2]^{c_2}\cdots[n_k]^{c_k}$" denotes the product $f_1^{c_1}f_2^{c_2}\cdots f_k^{c_k}$ for k monic irreducible polynomials $f_i \in \mathbb{F}_l[X]$ of $\deg f_i = n_i$ different from each other with the multiplicities $c_i \in \mathbb{N}$. Note that $\tilde{\chi}$ cannot have a degree 3 irreducible factor over $\mathbb{F}_l$ thanks to [GS05, Lemma 3].

3 Upper bounds of extension degrees

This section discusses the upper bound of the extension degree of the field of definition of $\mathcal{J}[l]$ for each type in Table 1. We assume the orders

$$e = \#\langle\tilde{q}\rangle, \quad e_n = \#\langle-\tilde{q}\rangle, \quad e_r = \#\langle\sqrt{\tilde{q}}\rangle$$

are given.

Note that the discussion below includes for the cases that do not occur in actual in order to simplify the discussion whose aim is just developing upper bounds.

3.1 Type I

In this type, $\tilde{\chi}$ has 4 roots $\tilde{\alpha},\ \tilde{\alpha}^l,\ \tilde{\alpha}^{l^2},\ \tilde{\alpha}^{l^3} \in \mathbb{F}_{l^4} \setminus \mathbb{F}_{l^2}$ different from each other. Therefore A can be given over $\mathbb{F}_{l^4}$ as

$$A = \begin{pmatrix} \tilde{\alpha} & 0 & 0 & 0 \\ 0 & \tilde{\alpha}^l & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^{l^2} & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^{l^3} \end{pmatrix}.$$

From Theorem 1 and $\tilde{\alpha} \in \mathbb{F}_{l^2}$ if $\tilde{\alpha}^{l+1} = \tilde{q}$, we can see

$$\tilde{\alpha}^{l^2+1} = \tilde{q} \in \mathbb{F}_l,$$

so that

$$A^{l^2+1} = \begin{pmatrix} \tilde{q} & 0 & 0 & 0 \\ 0 & \tilde{q} & 0 & 0 \\ 0 & 0 & \tilde{q} & 0 \\ 0 & 0 & 0 & \tilde{q} \end{pmatrix}.$$

For $\mathcal{D} \in \mathcal{J}[l]$,

$$\mathcal{D}^{q^{e(l^2+1)}} - \mathcal{D} = 0$$

holds, because

$$\begin{aligned} T^{e(l^2+1)} &= PA^{e(l^2+1)}P^{-1} \\ &= PI_4P^{-1} \\ &= I_4. \end{aligned}$$

Therefore we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e(l^2+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^3-l^2+l-1}}).$$

[1] For the details of the Jordan canonical form, see [Lan87, Chapter 6], [Rom08, Chapter 8] for example.

Table 1: Upper bounds of extension degrees

Type	Char. Poly.	Approx. Prob. ($l \neq 2$)		Case	Max. Ext. Deg.	Max. Ext. Deg.
		$\sqrt{\tilde{q}} \in \mathbb{F}_l$	$\sqrt{\tilde{q}} \notin \mathbb{F}_l$			$(e = e_n = e_r = l-1)$
I	$[4]$	$\frac{1}{4}$			$e(l^2+1)$	$l^3 - l^2 + l - 1$
II	$[2]^2$	$\frac{1}{2l}$		(i)	$e(l+1)$ or $e_n(l+1)$	l^2-1
				(ii), (iii)	$el(l+1)$ or $e_n l(l+1)$	$l^3 - l$
III	$[2][2]$	$\frac{3}{8}$			$(l-1)(l+1)$	l^2-1
IV	$[2][1]^2$	$\frac{1}{2l}$	0	(i)	$e(l+1)$	l^2-1
				(ii)	$el(l+1)$	$l^3 - l$
V	$[2][1][1]$	$\frac{1}{4}$			$\mathrm{lcm}(e(l+1), l-1)$	l^2-1
VI	$[1]^4$	$\frac{2}{l^2}$	0	(i)	e_r	$l-1$
				(ii)	$e_r l$	$l^2 - l$
				(iii)	$e_r l$; $l \neq 2, 3$	$l^2 - l$
					$e_r l^2$; $l = 2, 3$	$l^3 - l^2$
VII	$[1]^2[1]^2$	$\frac{1}{2l}$		(i)	$l-1$	$l-1$
				(ii), (iii)	$l(l-1)$	$l^2 - l$
VIII	$[1]^2[1][1]$	$\frac{1}{l}$	0	(i)	$l-1$	$l-1$
				(ii)	$l(l-1)$	$l^2 - l$
IX	$[1][1][1][1]$	$\frac{1}{8}$			$l-1$	$l-1$

3.2 Type II

In this type, $\tilde{\chi}$ has 2 different double roots $\tilde{\alpha}$, $\tilde{\alpha}^l \in \mathbb{F}_{l^2} \setminus \mathbb{F}_l$. Then A can be given over $\mathbb{F}_{l^2}$ as either

(i) $A = \left(\begin{array}{cc|cc} \tilde{\alpha} & 0 & 0 & 0 \\ 0 & \tilde{\alpha} & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}^l & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^l \end{array}\right)$, (ii) $A = \left(\begin{array}{cc|cc} \tilde{\alpha} & 0 & 0 & 0 \\ 0 & \tilde{\alpha} & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}^l & 1 \\ 0 & 0 & 0 & \tilde{\alpha}^l \end{array}\right)$,

or (iii) $A = \left(\begin{array}{cc|cc} \tilde{\alpha} & 1 & 0 & 0 \\ 0 & \tilde{\alpha} & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}^l & 1 \\ 0 & 0 & 0 & \tilde{\alpha}^l \end{array}\right)$.

Moreover

$$\tilde{\alpha}^{l+1} = \pm\tilde{q} \in \mathbb{F}_l \tag{1}$$

holds[2].

In the following, we discuss the bound for each of cases (i), (ii), and (iii).

(i) In case (i), $A^{e(l+1)} = I_4$ if $\tilde{\alpha}^{l+1} = \tilde{q}$, or $A^{e_n(l+1)} = I_4$ if $\tilde{\alpha}^{l+1} = -\tilde{q}$ from Eq. (1). Therefore we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^2-1}})$$

or

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e_n(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^2-1}}).$$

(ii) In case (ii),

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & 0 & 0 & 0 \\ 0 & \tilde{\alpha}^k & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^{lk} & k\tilde{\alpha}^{l(k-1)} \\ 0 & 0 & 0 & \tilde{\alpha}^{lk} \end{pmatrix}$$

holds for any $k \in \mathbb{N}$, so that $A^{el(l+1)} = I_4$ or $A^{e_n l(l+1)} = I_4$ from Eq. (1). Therefore we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{el(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^3-l}})$$

or

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e_n l(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^3-l}}).$$

[2] If $\tilde{\alpha}^{l+1} = -\tilde{q}$ then $\sqrt{\tilde{q}} \notin \mathbb{F}_l$ for Type II.

(iii) In case (iii),

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & k\tilde{\alpha}^{k-1} & 0 & 0 \\ 0 & \tilde{\alpha}^k & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^{lk} & k\tilde{\alpha}^{l(k-1)} \\ 0 & 0 & 0 & \tilde{\alpha}^{lk} \end{pmatrix}$$

holds for any $k \in \mathbb{N}$, so that $A^{el(l+1)} = I_4$ or $A^{e_n l(l+1)} = I_4$ from Eq. (1). Therefore we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{el(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^3-l}})$$

or

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e_n l(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^3-l}}).$$

3.3 Type III

In this type, $\tilde{\chi}$ has 4 roots $\tilde{\alpha}_1$, $\tilde{\alpha}_1^l$, $\tilde{\alpha}_2$, $\tilde{\alpha}_2^l \in \mathbb{F}_{l^2} \setminus \mathbb{F}_l$ different from each other. Therefore A can be given over $\mathbb{F}_{l^2}$ as

$$A = \left(\begin{array}{cc|cc} \tilde{\alpha}_1 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}_1^l & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_2 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}_2^l \end{array}\right).$$

Moreover

$$N_{\mathbb{F}_{l^2}/\mathbb{F}_l}\tilde{\alpha}_i = \tilde{\alpha}_i^{l+1} \in \mathbb{F}_l$$

holds for $i \in \{1, 2\}$. Therfore we have $A^{(l-1)(l+1)} = I_4$ and

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{l^2-1}}).$$

3.4 Type IV

In this type, $\tilde{\chi}$ has 2 roots $\tilde{\alpha}_1$, $\tilde{\alpha}_1^l \in \mathbb{F}_{l^2} \setminus \mathbb{F}_l$ and a double root $\tilde{\alpha}_2 \in \mathbb{F}_l$. Therefore A can be given over $\mathbb{F}_{l^2}$ as either

(i) $A = \left(\begin{array}{cc|cc} \tilde{\alpha}_1 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}_1^l & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_2 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}_2 \end{array}\right)$ or (ii) $A = \left(\begin{array}{cc|cc} \tilde{\alpha}_1 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}_1^l & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_2 & 1 \\ 0 & 0 & 0 & \tilde{\alpha}_2 \end{array}\right)$.

Moreover we see that $\tilde{\alpha}_1^{l+1} = \tilde{q} \in \mathbb{F}_l$ and $\tilde{\alpha}_2 = \sqrt{\tilde{q}}$.

(i) In case (i), $A^{e(l+1)} = I_4$ holds, so that we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^2-1}}).$$

(ii) In case (ii), we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{el(l+1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^3-l}})$$

by the manner similar to (i) with Type II-(ii).

3.5 Type V

In this type, $\tilde{\chi}$ has 4 roots $\tilde{\alpha}_1$, $\tilde{\alpha}_1^l \in \mathbb{F}_{l^2} \setminus \mathbb{F}_l$, $\tilde{\alpha}_2$, $\tilde{\alpha}_3 \in \mathbb{F}_l$ different from each other. Therefore A can be given over $\mathbb{F}_{l^2}$ as

$$A = \left(\begin{array}{c|c|c|c} \tilde{\alpha}_1 & 0 & 0 & 0 \\ \hline 0 & \tilde{\alpha}_1^l & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_2 & 0 \\ \hline 0 & 0 & 0 & \tilde{\alpha}_3 \end{array}\right).$$

From

$$N_{\mathbb{F}_{l^2}/\mathbb{F}_l}\tilde{\alpha}_1 = \tilde{\alpha}_1^{l+1} = \tilde{q} \in \mathbb{F}_l,$$

we have $A^{\mathrm{lcm}(e(l+1),l-1)} = I_4$, so that

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{\mathrm{lcm}(e(l+1),l-1)}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^2-1}}).$$

3.6 Type VI

In this type, $\tilde{\chi}$ has a quadruple root $\tilde{\alpha} = \sqrt{\tilde{q}} \in \mathbb{F}_l$. Then A can be given over $\mathbb{F}_l$ as either

(i) $A = \left(\begin{array}{c|c|c|c} \tilde{\alpha} & 0 & 0 & 0 \\ \hline 0 & \tilde{\alpha} & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha} & 0 \\ \hline 0 & 0 & 0 & \tilde{\alpha} \end{array}\right)$, (ii) $A = \left(\begin{array}{cc|cc} \tilde{\alpha} & 1 & 0 & 0 \\ 0 & \tilde{\alpha} & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha} & 1 \\ 0 & 0 & 0 & \tilde{\alpha} \end{array}\right)$,

or (iii) $A = \begin{pmatrix} \tilde{\alpha} & 1 & 0 & 0 \\ 0 & \tilde{\alpha} & 1 & 0 \\ 0 & 0 & \tilde{\alpha} & 1 \\ 0 & 0 & 0 & \tilde{\alpha} \end{pmatrix}$

from [GS05, Lemma4].

(i) In case (i), we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e_r}}) \subset \mathcal{J}(\mathbb{F}_{q^{l-1}})$$

from $A^{\#\langle\tilde{\alpha}\rangle} = A^{e_r} = I_4$.

(ii) In case (ii), we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e_r l}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^2-l}})$$

by the manner similar to (i) with Type II-(iii).

(iii) In case (iii),

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & k\tilde{\alpha}^{k-1} & \frac{k(k-1)}{2}\tilde{\alpha}^{k-2} & \frac{k(k-1)(k-2)}{6}\tilde{\alpha}^{k-3} \\ 0 & \tilde{\alpha}^k & k\tilde{\alpha}^{k-1} & \frac{k(k-1)}{2}\tilde{\alpha}^{k-2} \\ 0 & 0 & \tilde{\alpha}^k & k\tilde{\alpha}^{k-1} \\ 0 & 0 & 0 & \tilde{\alpha}^k \end{pmatrix}$$

holds for any $k \in \mathbb{N}$. Therefore we have, for $l \notin \{2, 3\}$,

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e_r l}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^2-l}})$$

from $A^{e_r l} = I_4$, and for $l \in \{2, 3\}$,

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{e_r l^2}}) \subset \mathcal{J}(\mathbb{F}_{q^{l^3-l^2}})$$

from $A^{e_r l^2} = I_4$.

3.7 Type VII

In this type, $\tilde{\chi}$ has 2 double roots $\tilde{\alpha}_1$, $\tilde{\alpha}_2 \in \mathbb{F}_l$. Therefore A can be given over $\mathbb{F}_l$ as either

(i) $A = \left(\begin{array}{c|c|c|c} \tilde{\alpha}_1 & 0 & 0 & 0 \\ \hline 0 & \tilde{\alpha}_1 & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_2 & 0 \\ \hline 0 & 0 & 0 & \tilde{\alpha}_2 \end{array}\right)$, (ii) $A = \left(\begin{array}{c|c|cc} \tilde{\alpha}_1 & 0 & 0 & 0 \\ \hline 0 & \tilde{\alpha}_1 & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_2 & 1 \\ 0 & 0 & 0 & \tilde{\alpha}_2 \end{array}\right)$,

or (iii) $A = \left(\begin{array}{cc|cc} \tilde{\alpha}_1 & 1 & 0 & 0 \\ 0 & \tilde{\alpha}_1 & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_2 & 1 \\ 0 & 0 & 0 & \tilde{\alpha}_2 \end{array}\right)$.

(i) In case (i), from $A^{l-1} = I_4$, we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{l-1}}).$$

(ii), (iii) In these cases, from $A^{l(l-1)} = I_4$, we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{l^2-l}}).$$

3.8 Type VIII

In this type, $\tilde{\chi}$ has 2 single roots $\tilde{\alpha}_1$, $\tilde{\alpha}_2 \in \mathbb{F}_l$, and a double root $\tilde{\alpha}_3 = \sqrt{\tilde{q}} \in \mathbb{F}_l$ different from each other. Therefore A can be given over $\mathbb{F}_l$ as either

(i) $A = \left(\begin{array}{c|c|c|c} \tilde{\alpha}_1 & 0 & 0 & 0 \\ \hline 0 & \tilde{\alpha}_2 & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_3 & 0 \\ \hline 0 & 0 & 0 & \tilde{\alpha}_3 \end{array}\right)$ or (ii) $A = \left(\begin{array}{c|c|cc} \tilde{\alpha}_1 & 0 & 0 & 0 \\ \hline 0 & \tilde{\alpha}_2 & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_3 & 1 \\ 0 & 0 & 0 & \tilde{\alpha}_3 \end{array}\right)$.

(i) In case (i), from $A^{l-1} = I_4$, we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{l-1}}).$$

(ii) In case (ii), from $A^{l(l-1)} = I_4$, we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{l^2-l}}).$$

3.9 Type IX

In this type, $\tilde{\chi}$ has 4 roots $\tilde{\alpha}_1$, $\tilde{\alpha}_2$, $\tilde{\alpha}_3$, $\tilde{\alpha}_4 \in \mathbb{F}_l$ different from each other, so that A can be give over $\mathbb{F}_l$ as

$$A = \left(\begin{array}{c|c|c|c} \tilde{\alpha}_1 & 0 & 0 & 0 \\ \hline 0 & \tilde{\alpha}_2 & 0 & 0 \\ \hline 0 & 0 & \tilde{\alpha}_3 & 0 \\ \hline 0 & 0 & 0 & \tilde{\alpha}_4 \end{array}\right).$$

Therefore, from $A^{l-1} = I_4$, we have

$$\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^{l-1}}).$$

3.10 Summary

Table 1 summarizes the result in this section. In the table, column "Max. Ext. Deg." shows the maximum extension degree of fields of definition of the l-torsion points on $\mathcal{J}$ in each type. The maximum extension degree for the case that e, e_n, and e_r take their maxima (i.e. $e = e_n = e_r = l - 1$) is also shown. Note that the minimum extension degrees of the fields of definition always divide the corresponding degree in "Max. Ext. Deg.." In column "Approx. Prob.," an approximate probability for $l \neq 2$ of $\tilde{\chi}$ to be in each type is also shown under the assumption that $(\tilde{s}_1, \tilde{s}_2)$ is distributed uniformly in $\mathbb{F}_q^2$ for reference. Column "$\sqrt{\tilde{q}} \in \mathbb{F}_l$" shows the probability in the case of q being a quadratic residue modulo l and column "$\sqrt{\tilde{q}} \notin \mathbb{F}_l$" the probability in the case of q being a quadratic non-residue modulo l.

Theorem 2 below can be immediately obtained from Table 1.

Table 2: Complexity of DDF of l-division polynomial

Algorithm	$s \in O(l^4)$	$s \in O(l^3)$
Cantor-Zassenhaus	$O(l^{9+o(1)})$	$O(l^{8+o(1)})$
Gathen-Shoup	$O(l^{8+o(1)})$	$O(l^{8+o(1)})$
Shoup	$O(l^{10})$	$O(l^{9.5})$
Kaltofen-Shoup with the classical matrix multiplication ($\omega = 3$)	$O(l^{8.5+o(1)})$	$O(l^{8+o(1)})$
Kaltofen-Shoup with Strassen's multiplication ($\omega = \log_2 7$)	$O(l^{8.272+o(1)})$	$O(l^{7.797+o(1)})$
Kaltofen-Shoup under the result of [CW90] ($\omega = 2.375477$)	$O(l^{7.667+o(1)})$	$O(l^{7.260+o(1)})$

Theorem 2. *There exists a positive integer $d \leq l^3 - l$ such that $\mathcal{J}[l] \subset \mathcal{J}(\mathbb{F}_{q^d})$ holds.*

Therefore the degrees of the irreducible factors of Gaudry and Schost's l-division polynomials are bounded by $O(l^3)$. Unlike the division polynomials for elliptic curves, the l-division polynomials for genus 2 hyperelliptic curves are thus always reducible over $\mathbb{F}_q$.

Remark 1. *Gaudry and Schost's l-division polynomials regard 2 points that map to each other by the hyperelliptic involution as the same point. Therefore the maximum degrees of the irreducible factors are not $l^3 - l$ but $\frac{l^3-l}{2}$.*

4 Application to point counting

A l-division polynomial $f \in \mathbb{F}_q[X]$ of degree $\frac{l^4-1}{2}$ in the Gaudry-Schost algorithm can be factored by a general factoring algorithm for univariate polynomials over $\mathbb{F}_q$. The factoring algorithms can be classified into 2 classes, i.e. algorithms in the Cantor-Zassenhaus [CZ81] fashion, and in the Barlekamp [Ber70] fashion. Because the l-adic algorithms do not always use all irreducible factors of f, an algorithm in the Cantor-Zassenhaus fashion is usually invoked by the l-adic algorithms.

If there were an irreducible factor $\in \Theta(l^4)$ of f, the complexities of factoring f for $l \in \Theta(\log q)$ by algorithms[3] in the Cantor-Zassenhaus fashion would be $O(l^{9+o(1)})$ operations in $\mathbb{F}_q$ by the Cantor-Zassenhaus algorithm [CZ81], $O(l^{8+o(1)})$ by the Gathen-Shoup algorithm [GS92], $O(l^{10})$ by Shoup's practical algorithm[4] [Sho95, Section 2], and $O(l^{(13\omega-5)/(\omega+1)+o(1)})$, where $2 < \omega \leq 3$ and m^ω denotes the cost of an $m \times m$ matrix multiplication, by the Kaltofen-Shoup algorithm [KS97]. On the other hand, the other part of the Gaudry-Schost algorithm takes only $O(l^{6+o(1)})$ operations in $\mathbb{F}_q$ [GG03, Corollary 11.18], so that an efficient method to factorize f yields faster point counting for general genus 2 hyperelliptic curves.

The factoring algorithms in Cantor-Zassenhaus fashion consist of a squarefree decomposition (SFD), a distinct-degree factorization (DDF), and an equal-degree factorization (EDF). Since DDF dominates the complexity of a factoring algorithm in Cantor-Zassenhaus fashion and f is usually the input of DDF, i.e. f is usually squarefree, we treat DDF of f hereafter.

[3] Recently, Kedlaya and Umans [KU08, KU09] proposed an asymptotically faster algorithm. The algorithm is however known not to take effect in our interesting case [BZ09].

[4] Shoup's practical algorithm is implemented in his `C++` library NTL [Sho90].

In DDF, the computation of X^{q^i} modulo f for $i = 1, \ldots, \deg f$ is usually invoked and dominates the complexity of DDF in general. If we know the (possible) maximum degree $s \leq \deg f$ of the irreducible factors of f then it suffice to compute them for $i = 1, \ldots, s$.

The Cantor-Zassenhaus algorithm computes X^{q^i}s by a sequential manner, i.e. X^{q^i} is computed from $X^{q^{i-1}}$ by the repeated squaring. Therefore Theorem 2 reduces the complexity of factoring f by the Cantor-Zassenhaus algorithm. Note that the maximum degree originally takes effect on the Cantor-Zassenhaus algorithm, so that any modification to adapt the algorithm to Theorem 2 is not required.

The Gathen-Shoup algorithm computes X^{q^i}s by a binary strategy called the "iterated Frobenius" [GS92, Algorithm 3.1]. It computes $\{X^{q^i} \mid 1 \leq i \leq 2^j\}$ for $j \in \mathbb{N}$ from $\{X^{q^i} \mid 1 \leq i \leq 2^{j-1}\}$, so that Theorem 2 takes effect on the algorithm as a constant.

Both Shoup's practical algorithm and the Kaltofen-Shoup algorithm use a slightly different manner for the computation treated here. They only involve X^{q^i} for $1 \leq i \leq r_b$ and $X^{q^{r_b j}}$ for $1 \leq j \leq r_g$, where $r_b \approx s^\beta$ and $r_g \approx s^{1-\beta}$ with $0 \leq \beta \leq 1$. The parameter β is usually chosen so as to minimize the complexity when $s = \deg f$, so that the proper βs under Theorem 2, i.e. $s \in O(l^3)$, reduces the complexities of factoring f by the algorithms.

Column "$s \in O(l^3)$" in Table 2 shows the complexity of DDF of the l-division polynomial f by each algorithm with the modification according to Theorem 2. Since the algorithm invokes matrix multiplications, each complexity with the classical multiplication, Strassen's multiplication [Str69], and the result of [CW90] as the matrix multiplications is shown for the Kaltofen-Shoup algorithm. The complexity for a general univariate polynomial of degree $O(l^4)$ over $\mathbb{F}_q$ is also shown in column "$s \in O(l^4)$" for reference.

Since DDF dominates the complexities of the factoring algorithms, the complexities shown in Table 2 are also of factoring the l-division polynomial f. That is the univariate l-division polynomial f over $\mathbb{F}_q$ can be factorized within $O(l^{7.797+o(1)})$ operations in $\mathbb{F}_q$ by the Kaltofen-Shoup algorithm with Strassen's multiplication. Moreover, as the Gaudry-Schost algorithm invokes $O(\log q)$ factoring for the l-division polynomial in $\mathbb{F}_q[X]$ for $l \in O(\log q)$, we see that the complexity of the algorithm is $O((\log q)^{8.797+o(1)})$ operations in $\mathbb{F}_q$ by using the Kaltofen-Shoup algorithm with Strassen's multiplication.

References

[AH96] L. M. Adleman and M. D. Huang, *Counting rational points on curves and Abelian varieties over finite fields*, ANTS-II, LNCS 1122, Springer, 1996, 1–16.

[AHK01] K. Aoki, F. Hoshino, and T. Kobayashi, *A cyclic window algorithm for ECC defined over extension fields*, ICICS 2001, LNCS 2229, Springer, 2001, 62–73.

[AMNS06] S. Arita, K. Matsuo, K. Nagao, and M. Shimura, *A Weil descent attack against elliptic curve cryptosystems over quartic extension fields*, IEICE Trans. **E89-A** (2006), no. 5, 1246–1254.

[Ber70] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp **24** (1970), 713–735.

[BP98] D. V. Bailey and C. Paar, *Optimal extension fields for fast arithmetic in public-key algorithms*, CRYPTO '98, LNCS 1462, Springer, 1998, 472–485.

[BSS99] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, LMS 265, Cambridge U. P., 1999.

[BZ09] R. P. Brent and P. Zimmermann, *Factoring and testing irreducibility of sparse polynomials over small finite fields*, Talk at Queen Mary, U. London, `http://wwwmaths.anu.edu.au/~brent/pd/QMt4.pdf`, 2009.

[Can94] D. G. Cantor, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. **447** (1994), 91–145.

[CMKT00] J. Chao, K. Matsuo, H. Kawashiro, and S. Tsujii, *Construction of hyperelliptic curves with CM and its application to cryptosystems*, ASIACRYPT 2000, LNCS 1976, Springer, 2000, 259–273.

[CMT00] J. Chao, K. Matsuo, and S. Tsujii, *Fast construction of secure discrete logarithm problems over Jacobian varieties*, SEC 2000, Kluwer, 2000, 241–250.

[CW90] D. Coppersmith and S. Winograd, *Matrix multiplication via arithmetic progressions*, J.Symbolic Comp. **9** (1990), no. 3, 23–52.

[CZ81] D. G. Cantor and H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981), 587–592.

[Elk95] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory, AMS, 1995, 21–76.

[GG03] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 2nd ed., Cambridge U. P., 2003.

[GH00] P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, ANTS-IV, LNCS 1838, Springer, 2000, 313–332.

[GMA+05] M. Gonda, K. Matsuo, K. Aoki, J. Chao, and S. Tsujii, *Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementation*, IEICE Trans. **E88-A** (2005), no. 1, 89-96.

[GS92] J. von zur Gathen and V. Shoup, *Computing Frobenius maps and factoring polynomials*, STOC '92, ACM, 1992, 97–105.

[GS04] P. Gaudry and É. Schost, *Construction of secure random curves of genus 2 over prime fields*, EUROCRYPT 2004, LNCS 3027, Springer, 2004, 239–256.

[GS05] ———, *Modular equations for hyperelliptic curves*, Math. Comp. **74** (2005), 429–454.

[GS08] ———, *Hyperelliptic curve point counting record: 254 bit Jacobian*, `http://www.loria.fr/~gaudry/record127/`, 2008.

[HI98] M. D. Huang and D. Ierardi, *Counting rational point on curves over finite fields*, J. Symbolic Computation **25** (1998), 1–21.

[HKT04] M. Haneda, M. Kawazoe, and T. Takahashi, *Formulae of the order of Jacobians for certain hyperelliptic curves*, SCIS 2004, 2004, 885–890.

[HS00] M. Hindy and J. H. Silverman, *Diophantine geometry : an introduction*, GTM 201, Springer, 2000.

[Kam91] W. Kampkötter, *Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven*, Ph.D. thesis, GH Essen, 1991.

[Ked01] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washinitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338.

[KMKH99] T. Kobayashi, H. Morita, K. Kobayashi, and F. Hoshino, *Fast elliptic curve algorithm combining Frobenius map and table reference to adapt to higher characteristic*, EUROCRYPT '99, LNCS 1592, Springer, 1999, 176–189.

[KNU03] N. Kanayama, K. Nagao, and S. Uchiyama, *Generating secure genus two hyperelliptic curves using Elkies' point counting algorithm*, IEICE Trans. **E86-A** (2003), no. 4, 908–918.

[Kob89] N. Koblitz, *Hyperelliptic curve cryptosystems*, J. Cryptology **1** (1989), no. 3, 139–150.

[Kob97] ———, *A very easy way to generate curves over prime field for hyperelliptic cryptosystems*, Rump talk at CRYPTO '97, 1997.

[KS97] E. Kaltofen and V. Shoup, *Fast polynomial factorization over high algebraic extensions of finite fields*, ISSAC '97, ACM, 1997, 184–188.

[KU08] K. S. Kedlaya and C. Umans, *Fast modular composition in any characteristics*, FOCS 2008, 2008, 481–490.

[KU09] ———, *Fast polynomial factorization and modular composition*, preprint, Available from `http://www.cs.caltech.edu/~umans/paper/KU08-final.pdf`, 2009.

[Lan87] S. Lang, *Linear algebra*, 3rd ed., Springer, 1987.

[LL06] R. Lercier and D. Lubicz, *A quasi quadratic time algorithm for hyperelliptic curve point counting*, The Ramanujan J. **12** (2006), no. 3, 399–423.

[LW02] A. Lauder and D. Wan, *Computing zeta functions of Artin-Schreier curves over finite fields*, LMS J. Comput. Math. **5** (2002), 33–55.

[MCT03] K. Matsuo, J. Chao, and S. Tsujii, *Baby step giant step algorithms in point counting of hyperelliptic curves*, IEICE Trans. **E86-A** (2003), no. 5, 1127–1134.

[MHCT01] K. Matsuo, T. Haga, J. Chao, and S. Tsujii, *On construction of secure hyperelliptic curve cryptosystems using Igusa invariants*, IEICE Trans. **J84-A** (2001), no. 8, 1045–1053, in Japanese.

[Pil90] J. Pila, *Frobenius maps of Abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), 745–763.

[Rom08] S. Roman, *Advanced linear algebra*, 3rd ed., GTM 135, Springer, 2008.

[Sch85] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494.

[Sho90] V. Shoup, *NTL: A library for doing number theory*, `http://www.shoup.net/ntl/`.

[Sho95] ———, *A new polynomial factorization algorithm and its implementation*, J. Symbolic Computation **20** (1995), 363–397.

[Sti09] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., GTM 254, Springer, 2009.

[Str69] V. Strassen, *Gaussian elimination is not optimal*, Numerishe Mathematik **13** (1969), 354–356.

[Sut09] A. V. Sutherland, *A generic approach to searching for Jacobians*, Math. Comp. **78** (2009), 485–507.

[Tak02] K. Takashima, *Improvements in the CM-method of genus 2 hyperelliptic curve cryptosystems*, Trans. of JSIAM **12** (2002), 269–279, in Japanese.

[Ver02] F. Vercauteren, *Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2*, CRYPTO 2002, LNCS 2442, Springer, 2002, 369–384.

[Wan99] D. Wan, *Computing zeta functions over finite fields*, Contemporary Mathematics **245** (1999), 131–141.

[Wen03] A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458.