Fast Formulae for Arithmetic of Degenerate Divisors on Genus *Two* Curves

Zhi Hu[a], Lin Wang[b], Chang-An Zhao[c,d,*]

[a] *School of Mathematics and Statistics in Central South University, Changsha 410083, P.R. China.*
[b] *Science and Technology on Communication Security Laboratory, Chengdu 610041, Sichuan, P. R. China.*
[c] *Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, P.R.China.*
[d] *Guangdong Key Laboratory of Information Security, Guangzhou 510006, China*

Abstract

Scalar multiplications are the main operation in the implementation of hyperelliptic curve cryptosystems, where the basic arithmetic of reduced divisor classes are required. In this paper, we derive the explicit formulae for the arithmetic of reduced divisor classes by exploiting Jacobian coordinates introduced by Hisil and Costello when the degenerate divisor involves. Our results can be regarded as a supplementary study of [1]. An efficiency analysis shows that the degenerate divisor as a base point can be a valid alternative in scalar multiplications as well.

Keywords: Hyperelliptic curves, Scalar multiplication, Degenerate divisor, Efficient arithmetic

1. Introduction

Hyperelliptic curves over finite fields with small genus play a vital role in the construction of cryptographic primitives since the discrete logarithm problem in cyclic groups of prime orders that are embedded in these curves is believed to be

*Corresponding author

Email addresses: huzhi_math@csu.edu.cn (Zhi Hu), linwang@math.pku.edu.cn (Lin Wang), zhaochan3@mail.sysu.edu.cn (Chang-An Zhao)

[1] This work is partially supported by National Key R&D Program of China under Grant No. 2017YFB0802500. The work of Zhi Hu is partially supported by the National Natural Science Foundation of China(NSFC) under Grant No. 61602526. The work of Lin Wang is partially supported by NSFC under Grant No. 61502441. The work of Chang-An Zhao is partially supported by NSFC under Grant No. 61472457.

hard in the presence of the current computational power. On one hand, Diffie-Hellman key exchange can be implemented on a Kummer surface that is related to the Jacobian of a hyperelliptic curve with genus two [2, 3]. On the other hand, hyperelliptic curve cryptosystems(HECC) [4] can be a valid candidate in public key cryptography. We refer to [5, 6] for more details.

Of particular importance are scalar multiplications in the implementation of HECC or other cryptographic protocols [7]. We should point out that generic additions in Jacobians of hyperelliptic curves should be exploited in many practical scenarios. Several efficient implementation techniques to speed up scalar multiplications on hyperelliptic curves have been presented. These include:

- Exploiting properties of the defining fields or models of hyperellitic curves. Generally speaking, the imaginary model should be the popular choice while a few works are devoted to accelerating the arithmetic of Jacobian of hyperelliptic curves in a real model [8, 9, 10]. Note that the equation of hyperelliptic curve depends on the characteristics of base fields. The idea of halving a rational point on elliptic curves [11] was extended to hyperelliptic cases over fields of even characteristic [12, 13, 14].

- Acting efficient endomorphisms on the reduced divisors. This idea was first generated from the case of elliptic curves [15] and then widely used in many applicable scenarios [16, 17].

- Making good use of different interpretations for group laws of Jacobians of hyperelliptic curves. Cantor first presented an efficient algorithm for performing the addition in Jacobian groups of hyperelliptic curves over fields of odd characteristic [18] and Koblitz generalized it to fields of any characteristic [4]. Harley gave a different approach to optimize the arithmetic [19, 20]. Wollinger *et al*. compared these two algorithms explicitly in [21]. The group law of Jacobian are explained from a point of geometric view [22, 7].

- Taking advantages of different projective coordinate systems for avoiding the inversion. Lange speeded up the arithmetic of Jacobian points by using different weighted coordinate systems [23]. Costello and Hisil gave a significant improvement of a mixed-doubling-and-addition by introducing a novel Jacobian coordinate system in [24, 1].

- Using the degenerate divisor as the base point. Tanja Lange gave the explicit formulas according to the degrees of two input divisor classes first [23].

katagi *et al*. investigated scalar multiplications when the degenerate divisor is chosen to be the base point in characteristic *two* [12].

Note that the authors of [1] always assume that all input and output points will be general in the whole scalar multiplication. However, it is possible to meet a degenerate divisor even if the base point is general. In this work, we will address this special case. Our motivations are multi-fold:

(a) By applying the idea of Jacobian coordinates to the case of the degenerate divisor, we give a supplementary study of the arithmetic of the divisor classes which is in accordance with the explicit formulas of [1];

(b) When the base point is chosen to be degenerate in the implementation of scalar multiplications, a mixed-doubling-and-addition or an addition always requires a degenerate divisor as an input;

(c) Our work may be exploited in the implementation of hyperelliptic pairings since input points and scalars are chosen randomly in this scenario. This means that the degenerate divisor could involve in the computation.

On the basis of the above, we revisit the addition of two reduced divisor classes when the degenerate one involves. In particular, we consider the addition of one degenerate divisor and one generate divisor, the tripling of one degenerate divisor, and the addition of two generate divisors (these two divisors could be same) when their sum is degenerate. In essence, these computations can be interpreted by the intersection of a quadratic parabola with the hyperelliptic curve. We find the proposed formula is significantly fast in efficiency. For example, the cost of the addition of one degenerate divisor and one generate divisor only requires $22M+6S+1D+15a$ in Jacobian coordinate systems, where M denotes field multiplications, S denotes squarings, D denotes multiplications by some constants which is related to the curve parameters, and a denotes field additions respectively. We hope that our results lead to more developments on this line of research.

The remainder of this paper is structured as follows. In Section 2, we provide some background and notation on the arithmetic of reduced divisors. In Section 3, we provide an explicit formula of the addition of the divisor classes when the degenerate divisor involves in affine coordinate systems. Also, these formulas are derived mainly by using the interpolation of a quadratic parabola. In Section 4, we convert all the formulae in Jacobian coordinate systems and give the computational cost of them. In Section 5, we discuss the advantage of using the degenerate divisor as the base point when endomorphisms tricks are applicable. In Section 6, efficiency comparisons are given. We show that our formulas have computational advantages in efficiency. Finally, We draw our conclusion in Section 7.

2. Preliminaries

In this section we first recall some basic preliminaries of hyperelliptic curves, and Mumford representation of a reduced divisor. Then we give some facts about degenerate divisors since we will mainly consider the arithmetic of the reduced divisors which involve the degenerate ones.

2.1. Definitions of hyperelliptic curves

Let $\mathbb{F}_p$ be a finite field of order p with characteristic greater than 3, and $\bar{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$. Let C be a genus g hyperelliptic curve given by $C: y^2 = f(x)$, where $f(x) \in \mathbb{F}_p[x]$ and $\deg f = 2g+1$. Let $\mathbb{F}_p(C)/\mathbb{F}_p$ be a function field defined by C.

Let $C(\bar{\mathbb{F}}_p) = \{(a,b) : a,b \in \bar{\mathbb{F}}_p, b^2 = f(a)\} \bigcup \{\infty\}$, where ∞ is the point at infinity. The hyperelliptic involution $^-$ is defined as follows: $\overline{(a,b)} = (a,-b)$ and $\overline{\infty} = \infty$.

A divisor D of $C(\bar{\mathbb{F}}_p)$ is an element of the free abelian group over all points of $C(\bar{\mathbb{F}}_p)$, e.g., $D = \sum_{P \in C(\bar{\mathbb{F}}_p)} n_P P$ where $n_P \in \mathbb{Z}$ and n_P is zero for almost all points P. The degree of D is defined as $\deg(D) = \sum_{P \in C(\bar{\mathbb{F}}_p)} n_P$. A divisor D is called $\mathbb{F}_p$-rational if $\sigma(D) = D$ for all $\sigma \in Gal(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. All $\mathbb{F}_p$-rational divisors of C of degree zero forms a group. Every element $H \in \mathbb{F}_p(C)/\mathbb{F}_p$ can be related to a divisor $div(H) = \sum_{P \in C(\bar{\mathbb{F}}_p)} \nu_P(H) P$ via the valuations at all points of $C(\bar{\mathbb{F}}_p)$. Such a divisor which corresponds to a rational function on C is called a principal divisor. all so-called principal divisors are of degree zero and form a subgroup of the group of degree zero divisors. The divisor class group of degree zero is the quotient of the group of degree zero divisors by the principal divisors. Such a divisor class group is also called the Picard group of C. We can represent a divisor class by a divisor $D = \sum_{i=1}^{k} P_i - k\infty$, where $P_i \neq \infty$, $P_i \neq \overline{P_j}$ for $i \neq j$ and $k \leq g$. Moreover, the divisor class group is isomorphic to the $\mathbb{F}_p$-rational points of the Jacobian of the curve C, a g-dimensional abelian variety. In the following we denote this group by $Jac_C(\mathbb{F}_p)$.

Each nontrivial divisor class in $Jac_C(\mathbb{F}_p)$ has a Mumford representatioin, i.e., it can be represented by a unique pair of polynomials $[u(x), v(x)]$, $u, v \in \mathbb{F}_p[x]$, where u is monic, $\deg v < \deg u \leq g$, and $u | (v^2 - f)$.

More precisely, denote $P_i = (x_i, y_i)$. Then the divisor class of D is represented by $u(x) = \prod_{i=1}^{k}(x - x_i)$. If P_i occurs n_i times, then $(\frac{d}{dx})^j [v(x)^2 - f(x)]|_{x=x_i} = 0$, $0 \le j \le n_i - 1$. Note that $-D = [u(x), -v(x)]$.

In the following we concentrate on $g = 2$. The hyperelliptic curve that we consider is given by the following equation

$$C : y^2 = f(x) = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

where f_i is contained in $\mathbb{F}_p$ for $i = 0,\ 1,\ 2$ and 3. According to the Hasse-Weil Bound, we have $\#Jac_C(\mathbb{F}_p) = O(p^2)$. Moreover, suppose $\#Jac_C(\mathbb{F}_p) = hn$ where n is a large prime and h is called a cofactor.

2.2. Representation of reduced divisors

A reduced divisor $D = [u(x), v(x)] \in Jac_C(\mathbb{F}_p)$ is said to be general if $\deg u(x) = 2$. let D be a general divisor represented in Mumford form as $D = [x^2 + qx + r, sx + t]$. We will sometimes represent a general divisor as $[q, r, s, t]$ for simplicity. Also, the divisor D is said to be degenerate if $\deg u(x) = 1$. More precisely, if $(a, b) \in C(\mathbb{F}_p)$, then $D = [x - a, b]$ is a degenerate divisor in $Jac_C(\mathbb{F}_p)$. Degenerate divisors have been used in the optimization of scalar multiplications [12] and pairing computations on hyperelliptic curves [25].

Suppose $\mathfrak{D}_d = \{D = [u(x), v(x)] \in Jac_C(\mathbb{F}_p) : \deg u(x) = 1\}$, then $\#\mathfrak{D}_d = O(p)$.

A general divisor $D = [u(x), v(x)] \in Jac_C(\mathbb{F}_p)$ is said to be decomposable, if $u(x)$ is reducible in $\mathbb{F}_p[x]$. Given an arbitrary general divisor $D = [u(x), v(x)] = [q, r, s, t]$, we see that it is decomposable if and only if $\Delta(u(x)) = q^2 - 4r$ is a quadratic residue in $\mathbb{F}_p$.

Suppose that

$$\mathfrak{D}_r = \{D = [u(x), v(x)] \in Jac_C(\mathbb{F}_p) : \deg u(x) = 2, \text{ and } u(x) \text{ is reducible over } \mathbb{F}_p\},$$

then $\#\mathfrak{D}_r = O(p^2/2)$. If $D = [q, r, s, t] \in \mathfrak{D}_r$, then D can be represented as $D = D_1 + D_2$, where $D_1 = [x - x_1, y_1], D_2 = [x - x_2, y_2] \in \mathfrak{D}_d$. For $x_1 \neq x_2$, We have

$$q = -(x_1 + x_2),\ r = x_1x_2,\ s = \frac{y_1 - y_2}{x_1 - x_2},\ t = \frac{x_1y_2 - x_2y_1}{x_1 - x_2}.$$

That is, $u(x) = (x - x_1)(x - x_2)$.

2.3. Choosing A Base Divisor

Since general divisors take the largest proportion, most literatures choose a general divisor as the desired cryptographic group generator, and thus concentrate on general divisor group operations [23, 26, 1]. Compared with general divisors, degenerate divisors are rare, but they can also be chosen as group generators. We have the following result:

Lemma 1. *Suppose $D \in \mathfrak{D}_r$ and $D = D_1 + D_2$, where $D_1, D_2 \in \mathfrak{D}_d$. If D has prime order n (i.e., $[n]D = P_\infty$), then either D_1 or D_2 also has prime order n (or divided by n).*

The proof of Lemma 1 is obvious and so we omit it here. Also, Lemma 1 says that we can possibly get a degenerate divisor with prime order n by decomposing a generate divisor.

3. Formulae for Arithmetic of Degenerate Divisors

In this section, we consider the addition formulae for two reduced divisors D_1, D_2. We focus mainly on the arithmetic under the following condition: there exists at least one degenerate divisor in $\{D_1, D_2, D_1 + D_2\}$. The interpolation parabola $y = h(x) = ax^2 + bx + c$ through $P_i = (x_i, y_i)$ $(1 \leq i \leq 5)$ with multiplicities intersects the equation of the hyperelliptic curve C as shown in Figure 1. It can be easily seen that

$$P_1 + P_2 + P_3 + P_4 + P_5 - 5\infty \sim \mathrm{div}(y - h(x)) = \mathrm{div}(y - (ax^2 + bx + c)).$$

where the notation $\mathrm{div}(\cdot)$ means a divisor of a function on the curve C. Recall that the involution of P_i is denoted by $\bar{P}_i$. We have $P_i + \bar{P}_i - 2\infty \sim \mathrm{div}(x - x_i)$. We will divide the addition of two reduced divisors into several cases when the degenerate divisor involves in the computation as follows.

3.1. $\deg(u_1) = 1, \deg(u_2) = 2$

Let $P_i = (x_i, y_i) \in C(\mathbb{F}_p)$, $D_1 = P_1 - \infty$, and $D_2 = P_2 + P_3 - 2\infty$. Suppose $D_1 = [x - x_1, y_1]$ and $D_2 = [u_2(x), v_2(x)] = [x^2 + q_2 x + r_2, s_2 x + t_2]$. We assume that P_1 or $-P_1$ does not occur in D_2, that is $u_2(x_1) \neq 0$, then we give an explanation for the arithmetic of degenerate divisors based on the divisor theory. Recall that $P_i + \bar{P}_i - 2\infty \sim \mathrm{div}(x - x_i)$ for $i = 4,\ 5$. It follows that

$$D_1 + D_2 = (P_1 - \infty) + (P_2 + P_3 - 2\infty) = \bar{P}_4 + \bar{P}_5 - 2\infty \sim \mathrm{div}\Big(\frac{y - (ax^2 + bx + c)}{(x - x_4)(x - x_5)}\Big),$$

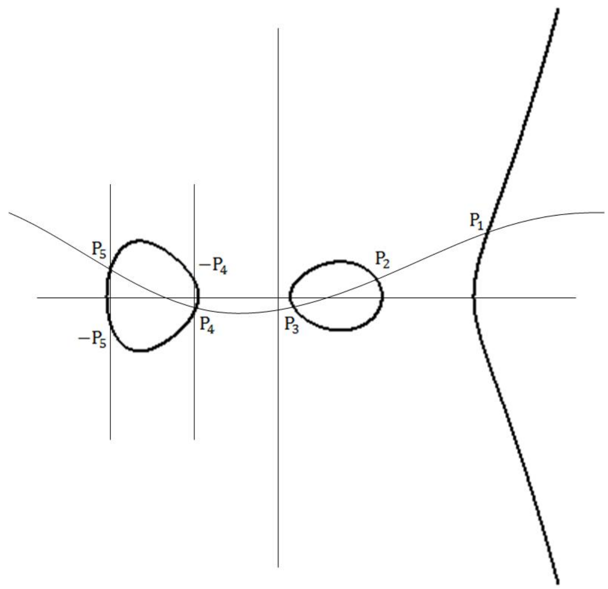

Figure 1: The intersection of a quadratic parabola with the hyperelliptic curve with genus *two*

where a, b and c are the undetermined coefficients.

We can determine the coefficients of the parabola ax^2+bx+c by using Lagrange interpolation since we are given the point P_1 and the divisor D_2. This is similar to Section 3 of [22]. Finally, the general formula for $D_3 = D_1 + D_2 = [q_3, r_3, s_3, t_3]$ can be stated as

$$\begin{aligned} a =& \frac{y_1 - (s_2x_1 + t_2)}{x_1^2 + q_2x_1 + r_2}, b = s_2 + q_2 \cdot a, c = t_2 + r_2 \cdot a, \\ q_3 =& x_1 - q_2 - a^2,\ r_3 = f_3 + q_2^2 - r_2 - a(b + s_2) + x_1 \cdot q_3, \\ s_3 =& a \cdot q_3 - b,\ t_3 = a \cdot r_3 - c. \end{aligned}$$

3.2. $3D_1$ *with* $\deg(u_1) = 1$

We are particularly interested in the arithmetic of $3D_1$ where D_1 is degenerate and has not order *three* in this subsection. Let $P_1 = (x_1, y_1) \in C(\mathbb{F}_p)$ and $D_1 = P_1 - \infty = [x - x_1, y_1]$. We can compute $3D_1$ through the procedure $D_1 \to 2D_1 \to 4D_1 \to 3D_1 = 4D_1 - D_1$. However, we introduce an alternative way to compute $D_3 = 3D_1$ as follows: Define $h(x) = ax^2 + bx + c$. The two curves $y = h(x)$ and $y^2 = f(x)$ are tangent at P_1 with multiplicity three. We can assume $P_1 = P_2 = P_3$ in this special case as shown in Figure 1. Then we have $3D_1 = \bar{P}_4 + \bar{P}_5 - 2(\infty) \sim \mathrm{div}(\frac{y-(ax^2+bx+c)}{(x-x_4)(x-x_5)})$.

Note that

$$\begin{aligned} f'(x_1) &= 5x_1^4+3f_3x_1^2+2f_2x_1+f_1, f''(x_1)=20x_1^3+6f_3x_1+2f_2, \\ y' &= 2ax_1+b=\frac{f'(x_1)}{2y_1}, y''=2a=\frac{f''(x_1)-2(y')^2}{2y_1}, \end{aligned}$$

thus

$$a=\frac{2y_1^2f''(x_1)-f'(x_1)^2}{8y_1^3}, b=\frac{f'(x_1)}{2y_1}-2ax_1, c=y_1-ax_1^2-bx_1.$$

Hence we obtain $3D_1=[q_3,r_3,s_3,t_3]$, where

$$q_3=3x_1-a^2, r_3=f_3-2a\cdot b+3x_1\cdot(q_3-x_1), s_3=a\cdot q_3-b, t_3=a\cdot r_3-c.$$

3.3. D_1+D_2 or $2D_1$ is degenerate

In this subsection, we consider the case that the sum of two generate divisors D_1 and D_2 is degenerate. We still use Figure 1 as an illustration. Let $D_1=P_1+P_2-2\infty$ and $D_2=P_3+P_4-2\infty$. The output of D_1+D_2 equals $D_3=\bar{P}_5-(\infty)$. We can still consider the intersection of the parabola $y=ax^2+bx+c$ (the coefficient $a\neq 0$) and the hyperelliptic curve C.

Suppose that the two general divisors are $D_1=[q_1,r_1,s_1,t_1]$ and $D_2=[q_2,r_2,s_2,t_2]$. The following intermediate variables are borrowed from [1]. Define

$$\begin{aligned} A &= (t_1-t_2)\cdot(q_2\cdot(q_1-q_2)-r_1+r_2)-r_2\cdot(q_1-q_2)\cdot(s_1-s_2); \\ B &= (r_1-r_2)\cdot(q_2\cdot(q_1-q_2)-r_1+r_2)-r_2\cdot(q_1-q_2)^2; \\ C &= (q_1-q_2)\cdot(t_1-t_2)-(r_1-r_2)\cdot(s_1-s_2); \end{aligned}$$

if $D_1\neq D_2$. Otherwise, we define

$$\begin{aligned} A &= ((q_1^2+f_3-4r_1)\cdot q_1-f_2+s_1^2)\cdot(q_1\cdot s_1-t_1)+(3q_1^2+f_3-2r_1)\cdot r_1\cdot s_1; \\ B &= (2(q_1\cdot s_1-t_1))\cdot t_1-2r_1\cdot s_1^2; \\ C &= ((q_1^2+f_3-4r_1)\cdot q_1-f_2+s_1^2)\cdot s_1+(3q_1^2+f_3-2r_1)\cdot t_1; \end{aligned}$$

Note that the condition $C = 0$ induces that the sum $D_3 = D_1 + D_2$ would be a degenerate divisor. Suppose $D_5 = D_1 + D_2 = [x - x_5, y_5]$. Then

$$
\begin{aligned}
x_5 &= (q_1 + q_2) + \frac{A^2}{B^2}, \\
y_5 &= x_3(\frac{A}{B}(q_1 - x_3) - s_1) + (\frac{A}{B}r_1 - t_1).
\end{aligned}
$$

In fact, the above computation can be viewed as the intersection of a degenerate parabola $y = dx^3 + ax^2 + bx + c$ ($d = 0$) and the hyperelliptic curve C. Note that

$$
\begin{aligned}
d &= -C/B, \\
a &= -(A + q_1 \cdot C)/B, \\
b &= -(q_1 \cdot A - s_1 \cdot B + r_1 \cdot C)/B, \\
c &= -(r_1 \cdot A - t_1 \cdot B)/B.
\end{aligned}
$$

This implies that $d = 0$ if and only if $C = 0$. And thus we have

$$
\begin{aligned}
x_5 &= (q_1 + q_2) + a^2, \\
y_5 &= -(a \cdot x_3^2 + b \cdot x_3 + c).
\end{aligned}
$$

3.4. $\deg(u_1) = \deg(u_2) = 1$

Suppose $D_1 = [x - x_1, y_1]$ and $D_2 = [x - x_2, y_2]$. If $x_1 = x_2$ and $y_1 = -y_2$, then $D_1 + D_2 = D_\infty = [1, 0]$. If $D_1 = D_2$, then

$$
2D_1 = [(x - x_1)^2, \frac{f'(x_1)(x - x_1)}{2y_1} + y_1].
$$

Otherwise

$$
D_1 + D_2 = [(x - x_1)(x - x_2), (\frac{y_1 - y_2}{x_1 - x_2})x + \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}].
$$

4. Degenerate Divisors in Jacobian Coordinates

Jacobian coordinates have been extensively studied to work projectively on elliptic and hyperelliptic curves. In hyperelliptic case, let D be a general divisor represented in Mumford form as $D = [x^2 + qx + r, sx + t]$. Recall that this representation is denoted by $[q, r, s, t]$ throughout this paper. Jacobian coordinates can be stated as $[Q : R : S : T : Z : W]$ [24], which have the following correspondence $[q, r, s, t] = [\frac{Q}{Z^2}, \frac{R}{Z^4}, \frac{S}{Z^3 W}, \frac{T}{Z^5 W}]$.

4.1. $\deg(u_1) = 1, \deg(u_2) = 2$

Let D_1 be a degenerate divisor generated by point $P = (x_1, y_1) \in C(\bar{\mathbb{F}}_p)$, and $D_2 = [Q_2 : R_2 : S_2 : T_2 : Z_2 : W_2]$ be a general divisor in $Jac_C(\mathbb{F}_p)$ with Jacobian coordinates. Consider $D_3 = D_1 + D_2 = [Q_3 : R_3 : S_3 : T_3 : Z_3 : W_3]$. Then

$$\begin{aligned}
A &= y_1 \cdot Z_2^5 \cdot W_2 - x_1 \cdot Z_2^2 \cdot S_2 - T_2,\ B = x_1 \cdot Z_2^2 \cdot (x_1 \cdot Z_2^2 + Q_2) + R_2, \\
Z_3 &= Z_2 \cdot (W_2 \cdot B),\ W_3 = 1, \\
Q_3 &= x_1 \cdot Z_3^2 - Q_2 \cdot (W_2 B)^2 - A^2, \\
R_3 &= f_3 \cdot Z_3^4 + (Q_2^2 - R_2) \cdot (W_2 B)^4 - A \cdot (W_2 B)^2 \cdot (A \cdot Q_2 + 2B \cdot S_2) + x_1 \cdot Z_3^2 \cdot Q_3, \\
S_3 &= A \cdot Q_3 - (W_2 B)^2 \cdot (A \cdot Q_2 + B \cdot S_2), \\
T_3 &= A \cdot R_3 - (W_2 B)^4 \cdot (A \cdot R_2 + B \cdot T_2).
\end{aligned}$$

The explicit formulas for such a mixed addition is given in the Appendix in Magma language. The cost of above operation is $22M + 6S + 1D + 15a$ (If $W_2 = 1$, then $2M$ would be saved). If we extend the Jacobian coordinates as $[Q : R : S : T : Z : W : Z^2]$, then one square can be further reduced. Moreover, note that $W_3 = 1$ in the output of the above function, thus in the iteration of scalar multiplication we can usually save $3M$ when doubling D_3 as [1].

4.2. $3D_1$ *with* $\deg(u_1) = 1$

Let $D_1 = [x - x_1, y_1]$. We can compute $D_3 = 3D_1 = [Q_3, R_3, S_3, T_3, Z_3, W_3]$ as

$$\begin{aligned}
Z_3 &= 8y_1^3, \\
A &= 2y_1^2 f''(x_1) - f'(x_1)^2, B = f'(x_1) \cdot 4y_1^2 - 2 \cdot A \cdot x_1, C = y_1 \cdot Z_3 - A \cdot x_1^2 - B \cdot x_1, \\
Q_3 &= 3x_1 \cdot Z_3^2 - A^2, R_3 = [f_3 \cdot Z_3^2 - 2AB + 3x_1(Q_3 - x_1 \cdot Z_3^2)] \cdot Z_3^2, \\
S_3 &= A \cdot Q_3 - B \cdot Z_3^2, T_3 = A \cdot R_3 - C \cdot (Z_3^2)^2, W_3 = 1.
\end{aligned}$$

The above cost is $17M + 5S + 2D$. Compared with the procedure $D_1 \to 2D_1 \to 4D_1 \to 3D_1 = 4D_1 - D_1$ which roughly costs $45M + 14S + 3D$, we save almost $28M + 9S$.

4.3. $D_1 + D_2$ or $2D_1$ is degenerate

In Jacobian coordinates, if $D_1 = [Q_1 : R_1 : S_1 : T_1 : Z_1 : W_1]$ and $D_2 = [Q_2 : R_2 : S_2 : T_2 : Z_1 : W_1]$, define

$$\begin{aligned}
A &= (T_1 - T_2) \cdot (Q_2 \cdot (Q_1 - Q_2) - (R_1 - R_2)) - R_2 \cdot (Q_1 - Q_2) \cdot (S_1 - S_2);\\
B &= (R_1 - R_2) \cdot (Q_2 \cdot (Q_1 - Q_2) - (R_1 - R_2)) - R_2 \cdot (Q_1 - Q_2)^2;\\
C &= (Q_1 - Q_2)(T_1 - T_2) - (R_1 - R_2)(S_1 - S_2);
\end{aligned}$$

if $D_1 = D_2$, then define

$$\begin{aligned}
A &= (Q_1 \cdot (Q_1^2 - 4R_1) + (f_3 Q_1 - f_2 Z_1^2) \cdot Z_1^4 \cdot W_1^2 + S_1^2) \cdot (Q_1 \cdot S_1 - T_1)\\
&+ (3Q_1^2 - 2R_1 + f_3 Z_1^4) \cdot W_1^2 \cdot R_1 \cdot S_1;\\
B &= 2(Q_1 \cdot S_1 - T_1) \cdot T_1 - 2R_1 S_1^2;\\
C &= (Q_1 \cdot (Q_1^2 - 4R_1) + (f_3 Q_1 - f_2 Z_1^2) \cdot Z_1^4 \cdot W_1^2 + S_1^2) \cdot S_1\\
&+ (3Q_1^2 - 2R_1 + f_3 Z_1^4) \cdot W_1^2 \cdot T_1.
\end{aligned}$$

The case $C = 0$ induces that the sum $D_3 = D_1 + D_2$ would be a degenerate divisor. Suppose $D_3 = (X_3, Y_3, Z_3)$. Then

$$\begin{aligned}
X_3 &= (Q_1 + Q_2) \cdot B^2 W^2 + A^2,\\
Y_3 &= X_3((A \cdot Q_1 - S_1 \cdot B) \cdot B^2 W^2 - A \cdot X_3) + (A \cdot R_1 - B \cdot T_1) \cdot (B^2 W^2)^2,\\
Z_3 &= B \cdot W \cdot Z;
\end{aligned}$$

4.4. $\deg(u_1) = \deg(u_2) = 1$

Let D_1 and D_2 be two degenerate divisors generated respectively by points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on $C(\bar{\mathbb{F}}_p)$. Consider $D_3 = D_1 + D_2 = [Q_3 : R_3 : S_3 : T_3 : Z_3 : W_3]$.

$$\begin{gathered}
Q_3 = -(x_1 + x_2),\ R_3 = x_1 \cdot x_2,\ S_3 = y_1 - y_2,\\
T_3 = x_1 \cdot y_2 - x_2 \cdot y_1,\ Z_3 = 1,\ W_3 = x_1 - x_2.
\end{gathered}$$

The cost of the above operation will be $3M + 4a$.

If $D_1 = D_2 = [x - x_1, y_1]$. By using the representation of Jacobian coordinates in [1], we compute $D_3 = [2]D = [Q_2 : R_2 : S_2 : T_2 : Z_2 : W_2]$ as

$$\begin{aligned}
Q_2 &= -2x_1,\ \ R_2 = x_1^2,\ \ T = y_1^2,\\
S_2 &= (5R_2 + 3f_3) \cdot R_2 - f_2 \cdot Q_2 + f_1,\\
T_2 &= 2T - S_2 \cdot x_1,\ \ Z_2 = 1,\ \ W_2 = 2y_1.
\end{aligned}$$

The cost of the above operation will be $2M+2S+1D+5a$. We neglect the cost of the multiplication by a "small" constant that is no more than 5.

5. Endomorphisms on Degenerate Divisors

Endomorphisms on elliptic or hyperelliptic curves have been used to accelerate scalar multiplications, which is the main operation in ECC or HECC. Such a technique is usually known as GLV method [15]. Compared with endomorphisms on general divisors, an endomorphism on degenerate divisors has much more simple expressions. For the efficient endomorphism ϕ defined on Buhler-Koblitz [27] (BK) or Furukawa-Kawazoe-Takahashi [28] (FKT) curves, if D is a degenerate divisor on the desired curve, then $\phi(D)$ is still a degenerate divisor.

We firstly take the BK Curve as an example. Suppose the hyperelliptic curve $C/\mathbb{F}_p$ is defined by the equation $y^2 = x^5 + b$, and take any $1 \neq \xi_5 \in \mathbb{F}_p$ such that $\zeta_5^5 = 1$. There is an efficient computable endomorphism ϕ on $Jac_C(\mathbb{F}_p)$ with minimal polynomial $T^4+T^3+T^2+T+1=0$. If $(x,y) \in C(\mathbb{F}_p)$, then $\phi(x,y) = (\xi_5 x, y)$, which means it acts on a degenerate divisor with only 1 multiplication in $\mathbb{F}_p$. ϕ acts on a general divisor $[q,r,s,t]$ as $\phi([q,r,s,t]) = [\xi_5 q, \xi_5^2 r, \xi_5^4 s, t]$, which costs 3 multiplications in $\mathbb{F}_p$.

For FKT curves, suppose hyperelliptic curve $C/\mathbb{F}_p$ is defined by the equation $y^2 = x^5 + ax$, and take any $\pm 1 \neq \xi_8 \in \mathbb{F}_p$ such that $\xi_8^8 = 1$. There is an efficient computable endomorphism ϕ on $Jac_C(\mathbb{F}_p)$ with minimal polynomial $T^4+1=0$. If $(x,y) \in C(\mathbb{F}_p)$, then $\phi(x,y) = (\xi_8^2 x, \xi_8 y)$, which means it acts on a degenerate divisor with only 2 multiplication in $\mathbb{F}_p$. ϕ acts on a general divisor $[q,r,s,t]$ as $\phi([q,r,s,t]) = [\xi_8^2 q, \xi_8^4 r, \xi_8^7 s, \xi_8 t]$, which costs 4 multiplications in $\mathbb{F}_p$.

If we apply the (2 dimensional) GLV method to accelerate the scalar multiplication on desired curves, we usually need to evaluate the operation $k_1 D_1 + k_2 D_2$, where D_1, D_2 are degenerate divisors, and k_1, k_2 have the same bitlength. Here we adopt the novel technique called Joint Regular Form (JRF) [29].

`JRF`: Let $< k_{n-1}, \ldots, k_0 >$ and $l_{n-1}, \ldots, l_0$ be signed binary representations of k and l, respectively, satisfying $k+l \equiv 1 \bmod 2$. $< k_{n-1}, \ldots, k_0 >$ and $< l_{n-1}, \ldots, l_0 >$ is called Joint Regular Form (JRF) of (k,l), if k_i and l_i satisfy $k_i + l_i = \pm 1$, that is, $(k_i, l_i) = (0, \pm 1)$ or $(\pm 1, 0)$ for any i.

We summarize such a procedure as the following algorithm.

Algorithm 1 Simultaneous scalar multiplication

Input: JRF of (k,l) as $< k_{n-1},...,k_0 >$ and $< l_{n-1},...,l_0 >$, two degenerate divisors D_1, D_2.
Output: $kD_1 + lD_2$.
1. $R \leftarrow 0$;
2. for i from $n-1$ downto 0 do
2.1 $R \leftarrow 2R$;
2.2 $R \leftarrow R + k_i D_1 + l_i D_2$;
3. return R.

The above method can also be generalized into higher dimensional cases. When implementing the GLV method, we usually adopt the multiple-base multiplication algorithm, and thus require a lookup table with divisors $\sum k_{ij} D_i$, where $k_{ij} \in \{0,1\}$. A $2m$ dimensional multiple-base multiplication algorithm usually requires to store 2^{2m} divisors, while accomplished with JRF it only needs to store 2^m divisors.

6. Efficiency Analysis

Let $\mathscr{G}$ denote a general divisor, and $\mathscr{D}$ denote a degenerate divisor. We summarize the above algorithms and previously related work in the following, and list the basic cost of divisor operations as Table 1.

Table 1: Divisor Arithmetic Cost

Doubling		**Addition**	
Operation	Costs	Operation	Costs
$2\mathscr{G} = \mathscr{G}$[1]	26M+8S+2D+25a	$\mathscr{G} + \mathscr{G} = \mathscr{G}$[1]	41M+ 7S + 22a
$2\mathscr{D} = \mathscr{G}$	2M+2S+1D+2a	$\mathscr{G} + \mathscr{D} = \mathscr{G}$	22M+6S+1D+15a
$3\mathscr{D} = \mathscr{G}$	17M+5S+2D	$\mathscr{D} + \mathscr{D} = \mathscr{G}$	3M+4a

We also consider the scalar multiplication based on a general/degenerate divisor. Previous work [23, 26, 1] concentrated on the general generator case. In this work, we find that scalar multiplication based on degenerate divisor could be performed efficiently as well. Note that in the iteration of scalar multiplication, it basically requires two operations: the DBL and the mDBLADD (DBL-and-ADD mode like [23, 26] or ADD-and-ADD mode like [1]). If the base divisor is chosen to be degenerate, the first doubling operation and the double-and-add operation would involve degenerate divisors. We conclude the cost of these operations and previous work in table 1, where we only count the costs of "plain" formulae.

Table 2: Operation count

Work	DBL	mADD	mDBLADD
Lange [23]	32M+7S+2D	36M+5S	68M+12S+2D
Costello and Lauter [26]	30M+9S+2D	36M+5S	66M+14S+2D
Costello and Hisil [1]	26M+8S+2D	32M+5S	57M+8S
This work(Degenerate case)	26M+8S+2D	22M+6S+1D	45M+13S+3D

We should mention that katagi *et al*. in [12] also presented formulae for degenerate divisors, which were given in affine coordinates and tackle the cases in characteristic *two*. Thus we do not list their results to the above tables, since we mainly consider the arithmetic of the reduced divisors over finite fields with odd characteristics here.

Let $|k|_2 = n$, $|k_1|_2 = |k_2|_2 = n/2$. Let D be a general divisor, and D_1, D_2 be two degenerate divisors. We consider the scalar multiplication for three kinds of base divisors, the general base, the degenerate base and the double degenerate bases. For general base scalar multiplications, we follow the method of Costello and Hisil [1], and adopt the non-adjacent form (NAF) to represent the scalar such that the average density of nonzero digits is approximately $\frac{1}{3}$. For degenerate base scalar multiplications, we use the same DBL function as [1], while the mDBLADD function is described in the above section. We should point out that the mDBLADD operation in this work involves the degenerate divisor. We can not say that our formulae are faster than the previous results since they are used in different scenarios.

The GLV technique [15] or the verification of an ECDSA signature requires one to perform a double-base scalar multiplication. Suppose the two base divisors D_1, D_2 are degenerate, we consider how to efficiently perform $k_1D_1 + k_2D_2$. If we use the JRF of scalar (k_1, k_2) and apply the simultaneous algorithm (a.k.a Shamir trick), the addition operation in mDBLADD only involves two cases: $+D_1$ or $+D_2$, and thus the iteration routine is regular.

Table 3: Random base Scalar multiplication

Operation	Scalar rep.	Regular	Cost
kD[1]	NAF	No	$\frac{n}{3}(109M+24S+4D)$
kD_1(this work)	NAF	No	$\frac{n}{3}(97M+29S+7D)$
$k_1D_1+k_2D_2$(this work)	JRF	Yes	$\frac{n}{2}(45M+13S+3D)$

7. Conclusion

In this work, we showed that the addition formulae involved with the degenerate divisor can be speeded up efficiently by using Jacobian coordinates. Also, these formulae may be applied into the computations of pairings on hyperelliptic curves. We hope that these results can encourage more significant efforts on this line.

Appendix

We now give the explicit formulae for the addition of one degenerate divisor and one generate divisor in Magma language as follows .

$Mix\_Add := function(x1, y1, Q2, R2, S2, T2, Z2, W2, f3)$

$Z22 := Z2^2; Z24 := Z22^2; x1Z22 := x1 * Z22; Z25 := Z24 * Z2; M1 := y1 * Z24;$

$M2 := Z2 * W2; M3 := M1 * M2; M4 := x1Z22 * S2; A := M3 - M4 - T2;$

$W2B := W2 * B; B := x1Z22 * (x1Z22 + Q2) + R2; Z3 := Z2 * W2B; W3 := 1;$

$W2B2 := W2B^2; A2 := A^2; Q3 := (x1Z22 - Q2) * W2B2 - A2; Q22 := Q2^2;$

$M5 := f3 * Z24; M6 := (M5 + Q22 - R2) * W2B2; AQ2 := A * Q2;$

$BS2 := B * S2; M7 := A * (AQ2 + 2 * BS2); M8 := x1Z22 * Q3;$

$R3 := (M6 - M7 + M8) * W2B2; AQ3 := A * Q3; S3 := AQ3 - W2B2 * (AQ2 + BS2);$

$AR3 := A * R3; AR2 := A * R2; BT2 := B * T2; W2B22 := W2B2^2;$

$T3 := AR3 - W2B22 * (AR2 + BT2);$

$return\ \ [Q3, R3, S3, T3, Z3, W3];$

$end\ function;$

References

[1] H. Hisil, C. Costello, Jacobian coordinates on genus 2 curves, Journal of Cryptology 30 (2017) 572–600.

[2] P. Gaudry, Fast genus 2 arithmetic based on theta functions, Journal of Mathematical Cryptology JMC 1 (2007) 243–265.

[3] D. J. Bernstein, C. Chuengsatiansup, T. Lange, P. Schwabe, Kummer Strikes Back: New DH Speed Records, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 317–337. URL: `https://doi.org/10.1007/978-3-662-45611-8_17`. doi:`10.1007/978-3-662-45611-8_17`.

[4] N. Koblitz, Hyperelliptic cryptosystems, Journal of Cryptology 1 (1989) 139–150.

[5] H. Cohen, G. Frey (Eds.), Handbook of elliptic and hyperelliptic curve cryptography, CRC Press, 2005.

[6] S. D. Galbraith, Mathematics of public key cryptography, Cambridge University Press, 2012.

[7] C. Costello, K. Lauter, Group Law Computations on Jacobians of Hyperelliptic Curves, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 92–117. URL: `https://doi.org/10.1007/978-3-642-28496-0_6`. doi:`10.1007/978-3-642-28496-0_6`.

[8] S. Erickson, M. J. Jacobson, N. Shang, S. Shen, A. Stein, Explicit Formulas for Real Hyperelliptic Curves of Genus 2 in Affine Representation, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, pp. 202–218. URL: `https://doi.org/10.1007/978-3-540-73074-3_16`. doi:`10.1007/978-3-540-73074-3_16`.

[9] S. Galbraith, M. Harrison, D. Mireles Morales, Efficient hyperelliptic arithmetic using balanced representation for divisors, Algorithmic number theory (2008) 342–356.

[10] S. Erickson, T. Ho, S. Zemedkun, Explicit projective formulas for real hyperelliptic curves of genus 2, Adv. Math. Commun. (2014). To appear.

[11] E. W. Knudsen, Elliptic scalar multiplication using point halving, in: Asiacrypt, volume 99, Springer, 1999, pp. 135–149.

[12] I. Kitamura, M. Katagi, T. Takagi, A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 146–157. URL: https://doi.org/10.1007/11506157_13. doi:10.1007/11506157_13.

[13] P. Birkner, Efficient divisor class halving on genus two curves, in: Selected Areas in Cryptography, volume 4356, Springer, 2006, pp. 317–326.

[14] P. Birkner, N. Thériault, Efficient halving for genus 3 curves over binary fields., Adv. in Math. of Comm. 4 (2010) 23–47.

[15] R. Gallant, R. Lambert, S. Vanstone, Faster point multiplication on elliptic curves with efficient endomorphisms, in: Advances in Cryptology – CRYPTO 2001, Springer, 2001, pp. 190–200.

[16] Y.-H. Park, S. Jeong, J. Lim, Speeding up point multiplication on hyperelliptic curves with efficiently-computable endomorphisms, in: EUROCRYPT, volume 2332, Springer, 2002, pp. 197–208.

[17] J. W. Bos, C. Costello, H. Hisil, K. Lauter, Fast Cryptography in Genus 2, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 194–210. URL: https://doi.org/10.1007/978-3-642-38348-9_12. doi:10.1007/978-3-642-38348-9_12.

[18] D. G. Cantor, Computing in the jacobian of a hyperelliptic curve, Mathematics of computation 48 (1987) 95–101.

[19] P. Gaudry, R. Harley, Counting points on hyperelliptic curves over finite fields, in: ANTS, volume 1838, Springer, 2000, pp. 313–332.

[20] R. Harley, Fast arithmetic on genus 2 curves, 2000. See http://cristal.inria.fr/harley/hyper for C source code and further explanations.

[21] T. Wollinger, J. Pelzl, C. Paar, Cantor versus harley: optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems, IEEE Transactions on Computers 54 (2005) 861–872.

[22] F. Leitenberger, et al., About the group law for the jacobi variety of a hyperelliptic curve, Contributions to Algebra and Geometry 46 (2005) 125–130.

[23] T. Lange, Formulae for arithmetic on genus 2 hyperelliptic curves, Applicable Algebra in Engineering, Communication and Computing 15 (2005) 295–328.

[24] H. Hisil, C. Costello, Jacobian coordinates on genus 2 curves, in: P. Sarkar, T. Iwata (Eds.), Advances in Cryptology – ASIACRYPT 2014, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 338–357.

[25] G. Frey, T. Lange, Fast bilinear maps from the tate-lichtenbaum pairing on hyperelliptic curves, in: ANTS, Springer, 2006, pp. 466–479.

[26] C. Costello, K. Lauter, Group law computations on jacobians of hyperelliptic curves, in: International Workshop on Selected Areas in Cryptography, Springer, 2011, pp. 92–117.

[27] B. Joe, K. Neal, Lattice basis reduction, jacobi sums and hyperelliptic cryptosystems, Bulletin of the Australian Mathematical Society 58 (1998) 147–154.

[28] E. Furukawa, M. Kawazoe, T. Takahashi, Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields, in: International Workshop on Selected Areas in Cryptography, 2003, pp. 26–41.

[29] T. Akishita, M. Katagi, I. Kitamura, Spa-resistant scalar multiplication on hyperelliptic curve cryptosystems combining divisor decomposition technique and joint regular form, in: International Workshop on Cryptographic Hardware and Embedded Systems, 2006, pp. 148–159.