J. Math. Cryptol. **5** (2011), 1–50
DOI 10.1515/JMC.2011.005 © de Gruyter 2011

An exploration of affine group laws for elliptic curves

Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter and Ed Dawson

Communicated by Alfred Menezes

Abstract. Several forms of elliptic curves are suggested for an efficient implementation of Elliptic Curve Cryptography. However, a complete description of the group law has not appeared in the literature for most popular forms. This paper presents group law in affine coordinates for three forms of elliptic curves. With the existence of the proposed affine group laws, stating the projective group law for each form becomes trivial. This work also describes an automated framework for studying elliptic curve group law, which is applied internally when preparing this work.

Keywords. Elliptic curve, group law, point addition, point doubling, projective coordinates, rational maps, birational equivalence, Riemann–Roch theorem, rational simplification, scalar multiplication, elliptic curve cryptography.

2010 Mathematics Subject Classification. 14H52, 68P25.

1 Introduction

Elliptic curves have been of great interest to algebraists, algebraic geometers, and number theorists for numerous decades. Since the time of Jacobi (more than 150 years ago) and long before the emergence of modern cryptography, it was well known that every elliptic curve is endowed with a unique *group law* which turns the points on an elliptic curve into an abelian group. The binary operation of this group, which is rationally expressed in terms of the coordinates of points of an elliptic curve, is called *the addition law*. The addition law turns out to be efficiently computable for elliptic curves defined over "suitable" fields. After the 1980s, such elliptic curves found several applications in cryptology. Standard references are [30, 31, 34].

In this context, several forms of elliptic curves have been studied for a more efficient computation of elliptic curve point addition. In most studies the most common cases of addition and doubling are covered, and handling of the special cases is omitted. This paper closes this gap by giving a complete description of

the group law in the case of three selected forms of elliptic curves:

(1) Extended Jacobi quartic form, $y^2 = dx^4 + 2ax^2 + 1$ (in variables x and y),

(2) Twisted Edwards form, $ax^2 + y^2 = 1 + dx^2y^2$ (in variables x and y),

(3) Twisted Jacobi intersection form, $bs^2 + c^2 = 1, as^2 + d^2 = 1$ (in variables s, c and d).

The rest of this paper is structured as follows. Section 2 provides formal definitions for background concepts which will be frequently accessed in the subsequent chapters. In particular, *the group law* is defined. Weierstrass forms of selected curves are presented along with birational maps. Section 3 brings together several computational tools which are beneficial in deriving group laws on elliptic curves. Section 4 presents low-degree point addition formulae for fixed forms of elliptic curves and states a complete addition algorithm in affine coordinates for each form by suitably handling all division by zero exceptions and interactions with the point(s) at infinity. Section 4 also contains results from the authors' previous works [24–26]. Section 5 concludes this paper with a summary of the contributions.

2 Elliptic curves

This section provides definitions for background concepts which will be frequently accessed in the subsequent sections.

2.1 Weierstrass form

Throughout this subsection, $\mathbb{K}$ denotes a field of *arbitrary characteristic* and $\mathbb{L}$ an algebraic extension of $\mathbb{K}$.

Definition 2.1. Let $a_1, a_3, a_2, a_4, a_6 \in \mathbb{K}$. A Weierstrass curve defined over $\mathbb{K}$ is a curve

$$E_{\mathbf{W},a_1,a_3,a_2,a_4,a_6} : v^2 + a_1uv + a_3v = u^3 + a_2u^2 + a_4u + a_6.$$

A Weierstrass curve is non-singular if and only if for every $u_1, v_1 \in \overline{\mathbb{K}}$ (closure of $\mathbb{K}$) with $v_1^2 + a_1u_1v_1 + a_3v_1 - (u_1^3 + a_2u_1^2 + a_4u_1 + a_6) = 0$, the partial derivatives $2v_1 + a_1u_1 + a_3$ and $a_1v_1 - 3u_1^2 - 2a_2u_1 - a_4$ do not vanish simultaneously (see the Jacobi criterion in [15, Lemma 4.49]). The singularity check can be done algebraically by computing $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ where $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, and $b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$. A Weierstrass curve is non-singular if and only if $\Delta \neq 0$. The notation $E_{\mathbf{W},a_1,a_3,a_2,a_4,a_6}$ will be abbreviated as $E_{\mathbf{W}}$ when a_1, a_3, a_2, a_4, a_6 are

understood. The projective closure of $E_{\mathbf{W}}$ is given by the equation

$$\overline{E}_{\mathbf{W},a_1,a_3,a_2,a_4,a_6} : V^2W + a_1UVW + a_3VW^2 = U^3 + a_2U^2W + a_4UW^2 + a_6W^3.$$

A point $(U:V:W)$ with $U, V \in \overline{\mathbb{K}}$ and $W \in \overline{\mathbb{K}}\backslash\{0\}$ on $\overline{E}_{\mathbf{W}}$ corresponds to the affine point $(U/W, V/W)$ on $E_{\mathbf{W}}$. The point $(0:1:0)$ on $\overline{E}_{\mathbf{W}}$ is non-singular. This point is called the point at infinity and is denoted by ∞. The point ∞ is $\mathbb{K}$-rational. There are no other points on $\overline{E}_{\mathbf{W}}$ with $W = 0$.

With a slight abuse of notation, $\overline{E}_{\mathbf{W}}(\mathbb{L})$, the set of $\mathbb{L}$-rational points on $\overline{E}_{\mathbf{W}}$ is denoted by

$$E_{\mathbf{W}}(\mathbb{L}) = \{(u, v) \in \mathbb{L}^2 \mid v^2 + a_1uv + a_3v = u^3 + a_2u^2 + a_4u + a_6\} \cup \{\infty\}.$$

An elliptic curve is denoted by its affine part hereafter by assuming that its projective closure is understood.

The following theorem says that every elliptic curve can be expressed as a Weierstrass curve regardless of the characteristic of $\mathbb{K}$ chosen. This can be seen as a reason of why elliptic curves are typically explained with the use of the Weierstrass form.

Theorem 2.2 (Weierstrass form of an elliptic curve). *Let $C/\mathbb{K}$ be a genus 1 curve with a $\mathbb{K}$-rational point. There exist $a_1, a_3, a_2, a_4, a_6 \in \mathbb{K}$ such that*

$$\mathbb{K}(C) \cong \mathbb{K}(E_{\mathbf{W},a_1,a_3,a_2,a_4,a_6}).$$

Thus, C is birationally equivalent over $\mathbb{K}$ to $E_{\mathbf{W}}$.

Proof. The proof follows from an application of the Riemann–Roch theorem, see [39, § III.3.3] and [15, § 4.4.2 and § 13.1]. □

It is natural to ask when are two Weierstrass curves isomorphic over $\mathbb{K}$.

Theorem 2.3. *Let $E_{\mathbf{W},a_1,a_3,a_2,a_4,a_6}$ and $E_{\mathbf{W}',A_1,A_3,A_2,A_4,A_6}$ be two Weierstrass curves defined over $\mathbb{K}$, as in Definition* 2.1. *$E_{\mathbf{W}}$ and $E_{\mathbf{W}'}$ are isomorphic over $\mathbb{K}$ if and only if there exist $c \in \mathbb{K}\backslash\{0\}$ and $r, s, t \in \mathbb{K}$ such that*

$$\begin{aligned}
A_1 &= (a_1 + 2s)/c,\\
A_2 &= (a_2 - sa_1 + 3r - s^2)/c^2,\\
A_3 &= (a_3 + ra_1 + 2t)/c^3,\\
A_4 &= (a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)/c^4,\\
A_6 &= (a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1)/c^6.
\end{aligned}$$

If such c, r, s, t exist then the maps

$$\psi: E_{\mathbf{W}} \to E_{\mathbf{W}'},\ (u, v) \mapsto \left(\frac{u-r}{c^2}, \frac{v-s(u-r)-t}{c^3}\right), \tag{2.1}$$

$$\phi: E_{\mathbf{W}'} \to E_{\mathbf{W}},\ (u', v') \mapsto \left(c^2u' + r, c^3v' + c^2su' + t\right) \tag{2.2}$$

are the desired isomorphisms defined over $\mathbb{K}$.

Proof. See [39, Table 1.2, III.1]. □

The morphism ϕ in Theorem 2.3 is usually called the admissible change of variables.

2.2 Group law

This section presents the group law on elliptic curves. Let $E_{\mathbf{W}}$ be a Weierstrass form elliptic curve with the point at infinity $\infty \in E_{\mathbf{W}}(\mathbb{L})$. The identity element is the point ∞. To specify this choice the identity is denoted by $\mathcal{O}$. Every point in $E_{\mathbf{W}}(\mathbb{L})$ has a unique inverse which can be computed by the unary operation "$-$". A computation of this operation requires case distinctions. In particular, $-\mathcal{O} = \mathcal{O}$. Let $P_1 = (u_1, v_1) \in E_{\mathbf{W}}$. Then $-P_1 = (u_1, -v_1 - a_1u_1 - a_3)$. A computation of the binary operation "$+$" requires somewhat more case distinctions. These cases are summarized in Algorithm 2.5. Using this algorithm, it can be verified that $P_1 + P_2 = P_2 + P_1$ and $(P_0 + P_1) + P_2 = P_0 + (P_1 + P_2)$ for all $P_i \in E_{\mathbf{W}}(\mathbb{K})$. Geometric and algebraic verifications of the group axioms are given in many textbooks, cf. [21, 40].

Definition 2.4. The unary operation $-$ is called the *negation law*. The binary operation $+$ is called the *addition law*. Together with a fixed identity element these two laws become the building blocks of *the group law* which turns $E_{\mathbf{W}}$ into an additively written abelian group.

Both the negation and addition laws require case distinctions. The sets of formulae handling some of these cases will be assigned special names hereafter.

Algorithm 2.5. The addition law for Weierstrass form in affine coordinates

Input : $P_1, P_2, \mathcal{O} \in E_{\mathbf{W},a_1,a_3,a_2,a_4,a_6}(\mathbb{K})$.

Output : $P_3 = P_1 + P_2$.

```
1  if P_1 = O then return P_2.
2  else if P_2 = O then return P_1.
3  else if u_1 = u_2 then
4      if v_1 + a_1 u_1 + a_3 + v_2 = 0 then return O.
5      else
6          λ ← (3u_1^2 + 2a_2 u_1 − a_1 v_1 + a_4)/(2v_1 + a_1 u_1 + a_3).
7          u_3 ← λ^2 + a_1 λ − a_2 − 2u_1.
8          v_3 ← λ(u_1 − u_3) − v_1 − a_1 u_3 − a_3.
9          return (u_3, v_3).
10     end
11 else
12     λ ← (v_1 − v_2)/(u_1 − u_2).
13     u_3 ← λ^2 + a_1 λ − a_2 − u_1 − u_2.
14     v_3 ← λ(u_1 − u_3) − v_1 − a_1 u_3 − a_3.
15     return (u_3, v_3).
16 end
```

Definition 2.6. If a set of formulae can only be used without any case distinction to carry out the operation

- "$-$" for all but finitely many points in $E_{\mathbf{W}}$, then such formulae are called the *point-negation formulae*. The operation carried out is called the *point-negation*.
- "$+$" for all but finitely many pairs of equal points and not for any pair of *distinct* points in $E_{\mathbf{W}} \times E_{\mathbf{W}}$, then such formulae are called the *point-doubling formulae*. For instance, see lines 7, 8, 9 in Algorithm 2.5. The operation carried out is called the *point-doubling*.
- "$+$" for all but finitely many pairs of distinct points in $E_{\mathbf{W}} \times E_{\mathbf{W}}$, then such formulae are called the *dedicated point-addition formulae*. For instance, see lines 13, 14, 15 in Algorithm 2.5. The operation carried out is called the *dedicated point-addition*.
- "$+$" for all but finitely many pairs of not necessarily distinct points in $E_{\mathbf{W}} \times E_{\mathbf{W}}$, then such formulae are called the *unified point-addition formulae*. For instance, see [40, Remark III.3.1]. The operation carried out is called the *unified point-addition*. In some cases, dedicated point-addition formulae can be used to add pairs of equal points after a rotation of coordinates, cf. [29]. Such formulae are called *weakly unified point-addition* and all unified point-

addition formulae which are not weakly unified point-addition are called *strongly unified point-addition* in EFD [7]. The distinction is omitted in this work since all unified point-addition formulae in this work exhibit the strongly unified property.

For economical reasons the "point-" and even the "formulae" part of each term will sometimes be dropped assuming that the meaning is clear from the context.

Theorem 2.7. *Let $E_{\mathbf{W}}/\mathbb{K}$ be an elliptic curve. Then the addition law and the negation law define morphisms*

$$+ : E_{\mathbf{W}} \times E_{\mathbf{W}} \to E_{\mathbf{W}} \qquad \text{and} \qquad - : E_{\mathbf{W}} \to E_{\mathbf{W}}$$
$$(P_1, P_2) \mapsto P_1 + P_2 \qquad\qquad P_1 \mapsto -P_1.$$

Proof. See [39, Theorem III.3.6] for a proof. □

When speaking of one of these terms, say, a unified addition, it may be the case that the denominators vanish and produce division by zero in affine coordinates. Since the addition law is a morphism by Theorem 2.7 it is always possible to switch to another set of formulae to compute the correct output. See also [39, Remark 3.1]. Therefore, when stating the addition law on an elliptic curve all cases should be considered carefully. Section 4 will provide more details on this.

The background in this section covers all elliptic curves. In Section 2.3, the attention will be restricted to cases where $\mathbb{K}$ is of odd characteristic.

2.3 Forms of elliptic curves

This section explicitly describes the birational equivalence between each of the aforementioned elliptic curves in Section 1 and a suitable Weierstrass curve. Some of the birational maps are borrowed from the literature resources while some others are derived by computer algebra tools which use Theorem 2.2 for this purpose. Applied examples on the explicit derivation of the maps will be presented in Section 3.1. Therefore, further discussion is omitted in this section. Note that for each one of the studied forms the identity element and the presented maps comply with the revisited/computed/proposed formulae in Sections 3 and 4.

It is still possible to substantially extend the list of the given forms. Indeed, a recent preprint ([12]) explains a derivation of group laws for many more forms. However, the forms listed at the beginning of this section are still the best when it comes to efficient computations.

Extended Jacobi quartic form

Throughout this subsection, $\mathbb{K}$ denotes a *fixed* field of odd characteristic and $\mathbb{L}$ an algebraic extension of $\mathbb{K}$. Let $d, a \in \mathbb{K}$. Assume that d is a square in $\mathbb{L}$ unless stated otherwise.

Definition 2.8. An extended Jacobi quartic curve defined over $\mathbb{K}$ is the curve

$$E_{\mathbf{Q},d,a} : y^2 = dx^4 + 2ax^2 + 1.$$

This curve is non-singular if and only if $d(a^2 - d) \neq 0$. The j-invariant is given by $64(a^2 + 3d)^3/(d(a^2 - d)^2) \in \mathbb{K}$. The projective closure of $E_{\mathbf{Q}}$ is given by the equation

$$\overline{E}_{\mathbf{Q},d,a} : Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4.$$

A point $(X : Y : Z)$ with $Z \neq 0$ on $\overline{E}_{\mathbf{Q}}$ corresponds to the affine point $(X/Z, Y/Z)$ on $E_{\mathbf{Q}}$. The point $(0 : 1 : 0)$ on $\overline{E}_{\mathbf{Q}}$ is singular. Using the standard "blow-up" techniques (see [21, § 7.3]) the singularity can be resolved. The resolution of singularities produces two points which are labeled as Ω_1 and Ω_2. Note that two "blow-ups" are necessary and sufficient to resolve the singularities. There are no other points on $\overline{E}_{\mathbf{Q}}$ with $Z = 0$.

A way of removing the singularity is by using the projective curve given by the equations

$$\widetilde{E}_{\mathbf{Q},d,a} : Y^2 = dT^2 + 2aX^2 + Z^2, \quad X^2 = TZ.$$

A point $(X : Y : T : Z)$ with $Z \neq 0$ on $\widetilde{E}_{\mathbf{Q}}$ corresponds to the affine point $(X/Z, Y/Z)$ on $E_{\mathbf{Q}}$. Fix $\delta \in \mathbb{K}$ such that $\delta^2 = d$. The points $(0 : \delta : 1 : 0)$ and $(0 : -\delta : 1 : 0)$ correspond to Ω_1 and Ω_2 on the desingularization of $\overline{E}_{\mathbf{Q}}$. There is no other point on $\widetilde{E}_{\mathbf{Q}}$ with $Z = 0$.

Another way of removing the singularity is by using the weighted projective curve

$$\widehat{E}_{\mathbf{Q},d,a} : Y^2 = dX^4 + 2aX^2Z^2 + Z^4.$$

A point $(X : Y : Z)$ with $Z \neq 0$ on $\widehat{E}_{\mathbf{Q}}$ corresponds to the affine point $(X/Z, Y/Z^2)$ on $E_{\mathbf{Q}}$. The points $(1 : \delta : 0)$ and $(1 : -\delta : 0)$ on $\widehat{E}_{\mathbf{Q}}$ correspond to Ω_1 and Ω_2 on the desingularization of $\overline{E}_{\mathbf{Q}}$. There are no other points on $\widehat{E}_{\mathbf{Q}}$ with $Z = 0$.

With a slight abuse of notation, $\overline{E}_{\mathbf{Q}}(\mathbb{L})$, the set of $\mathbb{L}$-rational points on $\overline{E}_{\mathbf{Q}}$ is denoted by

$$E_{\mathbf{Q}}(\mathbb{L}) = \{(x, y) \in \mathbb{L}^2 \mid y^2 = dx^4 + 2ax^2 + 1\} \cup \{\Omega_1, \Omega_2\}$$

where Ω_1, Ω_2 are points at infinity.

Remark 2.9. The points Ω_1, Ω_2 on the desingularization of $\overline{E}_{\mathbf{Q}}$; the points $(1:\delta:0)$, $(1:-\delta:0)$ on $\widehat{E}_{\mathbf{Q}}$; and the points $(0:\delta:1:0)$, $(0:-\delta:1:0)$ on $\widetilde{E}_{\mathbf{Q}}$ are $\mathbb{L}$-rational if and only if d is a square in $\mathbb{L}$.

The curve $E_{\mathbf{Q}}$ is birationally equivalent over $\mathbb{K}$ to the Weierstrass curve

$$E_{\mathbf{W}}: v^2 = u(u^2 - 4au + 4a^2 - 4d)$$

via the maps

$$\psi: E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x, y) \mapsto \Big(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\Big), \tag{2.3}$$

$$\phi: E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u, v) \mapsto \Big(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\Big). \tag{2.4}$$

It is trivial to check that $\phi \circ \psi = \mathrm{id}_{E_{\mathbf{Q}}}$ and $\psi \circ \phi = \mathrm{id}_{E_{\mathbf{W}}}$ as formal maps. The map ψ is regular at all points on $E_{\mathbf{Q}}$ except $(0, 1)$ which corresponds to ∞ on $\overline{E}_{\mathbf{W}}$. At first glance, it may seem that ψ is not regular at $(0, -1)$. However, it is possible to alter ψ to successfully map all points on $E_{\mathbf{Q}}$ except $(0, 1)$. For instance, the point $(0, -1)$ can be sent to $E_{\mathbf{W}}$ with an alternative map given by

$$\psi': E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x, y) \mapsto \Big(\frac{2dx^2 + 2a(1+y)}{y-1}, \frac{4a(dx^2+2a) - 4d(1-y)}{(1-y)^2}x\Big). \tag{2.5}$$

The map ϕ is regular at all points on $E_{\mathbf{W}}$ except in one case. Before investigating this case observe that the point $(0, 0)$ on $E_{\mathbf{W}}$ can be sent to $E_{\mathbf{Q}}$ with an alternative map given by

$$\phi': E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u, v) \mapsto \Big(\frac{2v}{(u-2a)^2 - 4d}, \frac{u^2 - 4(a^2-d)}{(u-2a)^2 - 4d}\Big). \tag{2.6}$$

The map ϕ is not regular at two points of the form (u, v) with $u \neq 0$ and $v = 0$. These exceptional points correspond to two points at infinity on the desingularization of $\overline{E}_{\mathbf{Q}}$. From Remark 2.9 it follows that ϕ is a morphism if d is a non-square in $\mathbb{K}$.

Every Weierstrass curve $v^2 = u^3 + a_2u^2 + a_4u$ is birationally equivalent over $\mathbb{K}$ to $E_{\mathbf{Q},(a_2^2-4a_4)/16,-a_2/4}$. The shape $v^2 = u^3 + a_2u^2 + a_4u$ covers all elliptic curves (over $\mathbb{K}$) having at least one point of order two. Therefore every elliptic curve of even order can be written in Jacobi quartic form. This extended model covers more isomorphism classes than the Jacobi model $E_{\mathbf{Q},k^2,-(k^2+1)/2}$.

Notes. Jacobi and Abel worked on generalizing the results known for the circle $y^2 = (1 - x^2)$ to the quartic curve $y^2 = (1 - x^2)(1 - k^2x^2)$. This form of elliptic curves is known as the Jacobi model. A Jacobi quartic curve given by $y^2 = x^4 + 2ax^2 + 1$ and its generalized version extended Jacobi quartic curve $y^2 = dx^4 + 2ax^2 + 1$, cf. [43]. In the context of cryptography, extended Jacobi quartic curves are studied in [11] where it is remarked that every elliptic curve of even order can be written in extended Jacobi quartic form.

Twisted Edwards form

Throughout this subsection, $\mathbb{K}$ denotes a *fixed* field of odd characteristic and $\mathbb{L}$ an algebraic extension of $\mathbb{K}$. Let $a, d \in \mathbb{K}$. Assume that both a and d are squares in $\mathbb{L}$ unless stated otherwise.

Definition 2.10. A twisted Edwards curve defined over $\mathbb{K}$ is the curve

$$E_{\mathbf{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

This curve is non-singular if and only if $ad(a - d) \neq 0$. The j-invariant is given by $16(a^2 + 14ad + d^2)^3/(ad(a-d)^4) \in \mathbb{K}$. The projective closure of $E_{\mathbf{E}}$ is given by the equation

$$\overline{E}_{\mathbf{E},a,d} : aX^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2.$$

A point $(X\colon Y\colon Z)$ with $Z \neq 0$ on $\overline{E}_{\mathbf{E}}$ corresponds to the affine point $(X/Z, Y/Z)$ on $E_{\mathbf{E}}$. The points $(0\colon 1\colon 0)$ and $(1\colon 0\colon 0)$ on $\overline{E}_{\mathbf{E}}$ are singular even if $ad(a-d) \neq 0$. Using the standard "blow-up" techniques (see [21, § 7.3]) the singularities can be resolved. The resolution of singularities produces four points (see [3]) which are labeled as Ω_1, Ω_2, Ω_3, and Ω_4. It is convenient to note here that a single "blow-up" for each of the points $(0\colon 1\colon 0)$ and $(1\colon 0\colon 0)$ is necessary and sufficient to resolve the singularities. There are no other points on $\overline{E}_{\mathbf{E}}$ with $Z = 0$.

A way of removing the singularities is by using the projective curve given by the equations

$$\widetilde{E}_{\mathbf{E},a,d} : aX^2 + Y^2 = Z^2 + dT^2, \;\; XY = TZ.$$

A point $(X\colon Y\colon T\colon Z)$ with $Z \neq 0$ on $\widetilde{E}_{\mathbf{E}}$ corresponds to the affine point $(X/Z, Y/Z)$ on $E_{\mathbf{E}}$. Fix $\alpha, \delta \in \mathbb{K}$ such that $\alpha^2 = a$ and $\delta^2 = d$. The points $(\delta\colon 0\colon \alpha\colon 0)$, $(-\delta\colon 0\colon \alpha\colon 0)$, $(0\colon \delta\colon 1\colon 0)$, and $(0\colon -\delta\colon 1\colon 0)$ on $\widetilde{E}_{\mathbf{E}}$ correspond to Ω_1, Ω_2, Ω_3, and Ω_4 on the desingularization of $\overline{E}_{\mathbf{E}}$.

With a slight abuse of notation, $\overline{E}_{\mathbf{E}}(\mathbb{L})$, the set of $\mathbb{L}$-rational points on $\overline{E}_{\mathbf{E}}$ is denoted by

$$E_{\mathbf{E}}(\mathbb{L}) = \{(x, y) \in \mathbb{L}^2 \mid ax^2 + y^2 = 1 + dx^2y^2\} \cup \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$$

where $\Omega_1, \Omega_2, \Omega_3, \Omega_4$ are points at infinity.

Remark 2.11. The points Ω_1 and Ω_2 on the desingularization of $\overline{E}_{\mathbf{E}}$; and the points $(\delta\colon 0\colon \alpha\colon 0)$ and $(-\delta\colon 0\colon \alpha\colon 0)$ on $\widetilde{E}_{\mathbf{E}}$ are $\mathbb{L}$-rational if and only if ad is a square in $\mathbb{K}$. The points Ω_3 and Ω_4 on the desingularization of $\overline{E}_{\mathbf{E}}$; and the points $(0\colon \delta\colon 1\colon 0)$ and $(0\colon -\delta\colon 1\colon 0)$ on $\widetilde{E}_{\mathbf{E}}$ are $\mathbb{L}$-rational if and only if d is a square in $\mathbb{K}$. Therefore, it is necessary to have both a and d squares in $\mathbb{K}$ to make all of these points $\mathbb{L}$-rational simultaneously.

Theorem 2.12 (Bernstein et al., [3]). *Every twisted Edwards curve over $\mathbb{K}$ is birationally equivalent over $\mathbb{K}$ to the Montgomery curve given by $By^2 = x^3 + Ax^2 + x$ for some $A, B \in \mathbb{K}$. Conversely, every Montgomery curve over $\mathbb{K}$ is birationally equivalent over $\mathbb{K}$ to a twisted Edwards curve.*

The explicit maps for Theorem 2.12 are given in [3]. Using those maps, after a formal rescaling of B in Montgomery form, maps for the birational equivalence to the Weierstrass curve

$$E_{\mathbf{W}} : v^2 = u^3 + 2(a + d)u^2 + (a - d)^2u$$

are given as

$$\psi\colon E_{\mathbf{E}} \to E_{\mathbf{W}},\ (x, y) \mapsto \Big((1 + y)^2\frac{1 - dx^2}{x^2}, 2(1 + y)^2\frac{1 - dx^2}{x^3}\Big), \tag{2.7}$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{E}},\ (u, v) \mapsto \Big(2\frac{u}{v}, \frac{u - a + d}{u + a - d}\Big). \tag{2.8}$$

It is trivial to check that $\phi \circ \psi = \mathrm{id}_{E_{\mathbf{E}}}$ and $\psi \circ \phi = \mathrm{id}_{E_{\mathbf{W}}}$ as formal maps. The map ψ is regular at all points on $E_{\mathbf{E}}$ except $(0, 1)$ which corresponds to ∞ on $\overline{E}_W$. At first glance, it may seem that ψ is not regular at $(0, -1)$. However, it is possible to alter ψ to successfully map all points on $E_{\mathbf{E}}$ except $(0, 1)$. For instance, the point $(0, -1)$ can be sent to $E_{\mathbf{W}}$ with an alternative map given by

$$\psi'\colon E_{\mathbf{E}} \to E_{\mathbf{W}},\ (x, y) \mapsto \Big((a - d)\frac{1 + y}{1 - y}, 2(a - d)\frac{a - dy^2}{(1 - y)^2}x\Big). \tag{2.9}$$

The map ϕ is regular at all points on $E_{\mathbf{W}}$ except in two cases. Before investigating these two cases observe that the point $(0,0)$ on $E_{\mathbf{W}}$ can be sent to $E_{\mathbf{E}}$ with an alternative map given by

$$\phi' \colon E_{\mathbf{W}} \to E_{\mathbf{E}},\ (u,v) \mapsto \Big(\frac{2v}{(u-2a)^2-4d}, \frac{u^2-4(a^2-d)}{(u-2a)^2-4d}\Big). \tag{2.10}$$

The map ϕ is not regular at two points of the form (u,v) with $u \neq 0$ and $v = 0$. These exceptional points correspond to two points at infinity on the desingularization of $\overline{E}_{\mathbf{E}}$. The map ϕ is not regular at two points of the form (u,v) with $u = d - a$. These exceptional points correspond to the other two points at infinity on the desingularization of $\overline{E}_{\mathbf{E}}$. From Remark 2.11 it follows that ϕ is a morphism if both d and ad are non-squares in $\mathbb{K}$.

Notes. Building on the historical works of Euler and Gauss, Edwards introduced the normal form $x^2 + y^2 = c^2(1 + x^2y^2)$ of elliptic curves together with an explicit addition law on this curve in [20]. Edwards also showed that every elliptic function field is equivalent to the function field of this curve for some c, over some small finite extension of the $\mathbb{K}$. In [8], Bernstein and Lange introduced Edwards form elliptic curves defined by $x^2 + y^2 = c^2(1 + dx^2y^2)$ where $c, d \in \mathbb{K}$ with $cd(1 - dc^4) \neq 0$, covering more curves than original Edwards curves when $\mathbb{K}$ is finite. Twisted Edwards form was introduced by Bernstein et al. in [3] as a generalization of Edwards curves. The facts about the resolution of singularities or the points at infinity or the coverage of these curves or the group structure have already been studied in different generalities in [3,5,8,20]. Also see [7].

Twisted Jacobi intersection form

Throughout this subsection, $\mathbb{K}$ denotes a *fixed* field of odd characteristic and $\mathbb{L}$ an algebraic extension of $\mathbb{K}$. Let $a, b \in \mathbb{K}$. Assume that both $-a$ and $-b$ are squares in $\mathbb{L}$ unless stated otherwise.

Definition 2.13. A twisted Jacobi intersection curve defined over $\mathbb{K}$ is the curve

$$E_{\mathbf{I},b,a} : bs^2 + c^2 = 1,\ \ as^2 + d^2 = 1.$$

This curve is non-singular if and only if $ab(a - b) \neq 0$. The j-invariant is given by $256(a^2 - ab + b^2)^3/(ab(a - b))^2 \in \mathbb{K}$. The projective closure of $E_{\mathbf{I}}$ is given by the equations

$$\overline{E}_{\mathbf{I},b,a} : bS^2 + C^2 = Z^2,\ \ aS^2 + D^2 = Z^2.$$

A point $(S:C:D:Z)$ with $Z \neq 0$ on $\overline{E}_{\mathbf{I}}$ corresponds to the affine point $(S/Z, C/Z, D/Z)$ on $E_{\mathbf{I}}$. Fix $\alpha, \beta \in \mathbb{K}$ such that $\alpha^2 = -a$ and $\beta^2 = -b$. The points $\Omega_1 = (1:\beta:\alpha:0)$, $\Omega_2 = (1:-\beta:\alpha:0)$, $\Omega_3 = (1:\beta:-\alpha:0)$, and $\Omega_4 = (1:-\beta:-\alpha:0)$ are non-singular. There are no other points on $\overline{E}_{\mathbf{I}}$ with $Z = 0$.

With a slight abuse of notation, $\overline{E}_{\mathbf{I}}(\mathbb{L})$, the set of $\mathbb{L}$-rational points on $\overline{E}_{\mathbf{I}}$ is denoted by

$$E_{\mathbf{I}}(\mathbb{L}) = \{(s, c, d) \in \mathbb{L}^3 \mid bs^2 + c^2 = 1, as^2 + d^2 = 1\} \cup \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$$

where $\Omega_1, \Omega_2, \Omega_3, \Omega_4$ are the points at infinity.

Remark 2.14. The points $\Omega_1, \Omega_2, \Omega_3, \Omega_4$ on $\overline{E}_{\mathbf{I}}$ are $\mathbb{L}$-rational if and only if both $-a$ and $-b$ are squares in $\mathbb{L}$.

The curve $E_{\mathbf{I}}$ is birationally equivalent over $\mathbb{K}$ to the Weierstrass curve

$$E_{\mathbf{W}} : v^2 = u(u - a)(u - b)$$

via the maps

$$\psi: E_{\mathbf{I}} \to E_{\mathbf{W}},\ (s, c, d) \mapsto \Big(\frac{(1 + c)(1 + d)}{s^2}, -\frac{(1 + c)(1 + d)(c + d)}{s^3}\Big), \tag{2.11}$$

$$\phi: E_{\mathbf{W}} \to E_{\mathbf{I}},\ (u, v) \mapsto \Big(\frac{2v}{ab - u^2}, 2u\frac{b - u}{ab - u^2} - 1, 2u\frac{a - u}{ab - u^2} - 1\Big). \tag{2.12}$$

It is trivial to check that $\phi \circ \psi = \mathrm{id}_{E_{\mathbf{I}}}$ and $\psi \circ \phi = \mathrm{id}_{E_{\mathbf{W}}}$ as formal maps. The map ψ is regular at all points on $E_{\mathbf{I}}$ except $(0, 1, 1)$ which corresponds to ∞ on $\overline{E}_W$. At first glance, it may seem that ψ is not regular at some other points with zero s-coordinate: $(0, -1, 1)$, $(0, 1, -1)$, and $(0, -1, -1)$. However, it is possible to alter ψ to successfully map all points except $(0, 1, 1)$. For instance, the points $(0, -1, 1)$, $(0, 1, -1)$, $(0, -1, -1)$ can be sent to $E_{\mathbf{W}}$ with an alternative map given by

$$\psi': E_{\mathbf{I}} \to E_{\mathbf{W}},\ (s, c, d) \mapsto \Big(b\frac{1 + d}{1 - c}, b\frac{a(1 - c) - b(1 + d)}{(1 - c)^2}s\Big), \tag{2.13}$$

$$\psi'': E_{\mathbf{I}} \to E_{\mathbf{W}},\ (s, c, d) \mapsto \Big(a\frac{1 + c}{1 - d}, a\frac{b(1 - d) - a(1 + c)}{(1 - d)^2}s\Big). \tag{2.14}$$

The map ϕ is regular at all points on $E_{\mathbf{W}}$ except the points of the form (u, v) with $u^2 = ab$. These exceptional points correspond to the four points at infinity on $\overline{E}_{\mathbf{I}}$ if ab is a square in $\mathbb{K}$. From Remark 2.14 it follows that ϕ is a morphism if ab is a non-square in $\mathbb{K}$.

Notes. An elliptic curve can be represented generically as the intersection of two quadrics [42, § 2.5.4]. See [11, 13, 32] for cryptographic applications of Jacobi intersection form. Every elliptic curve having three points of order 2 is birational to a twisted Jacobi intersection curve.

3 A toolbox for group laws

This section brings together several computational tools which are beneficial in deriving the group law on an elliptic curve. The approach will be algebraic rather than geometric, and the emphasis lies on the development of computer algebra routines to derive the desired group laws. In this direction, Section 3.1 outlines an automated method to derive the group laws on elliptic curves and provides case studies. Section 3.2 revisits rational simplification techniques by Monagan and Pearce ([36]) in the context of efficient automated group law derivation to detect useful formulae. Section 3.3 shows how to validate worked formulae in Maple ([35]) system based on a similar strategy from [7]. Section 3.4 provides a method to derive alternative formulae for point doubling and addition on elliptic curves.

3.1 Automated derivations

This section outlines how to derive the group law on an elliptic curve embedded in a suitable affine space. The method simply uses Riemann–Roch computations. In a rough sense, this can be viewed as a "conversion" of the well known group law for Weierstrass curves to the corresponding group law on a birationally equivalent curve using rational mappings.

The following theorem shows how to find the affine part of the addition law on an arbitrary elliptic curve.

Theorem 3.1. *Let $W/\mathbb{K}$ and $M/\mathbb{K}$ be affine curves. Assume that $\overline{W}$ and $\overline{M}$, each with a fixed $\mathbb{K}$-rational point, are elliptic curves. Assume that W and M are birationally equivalent over $\mathbb{K}$. Let $\phi : W \to M$ and $\psi : M \to W$ be maps such that $\phi \circ \psi$ and $\psi \circ \phi$ are equal to the identity maps id_M and id_W, respectively. Let $+_W : W \times W \to W$ be the affine part of the unique addition law on $\overline{W}$. The affine part of the unique addition law on $\overline{M}$ is given by the compositions*

$$+_M = \phi \circ +_W \circ (\psi \times \psi). \tag{3.1}$$

Before giving the proof, the following lemma will be useful.

Lemma 3.2. *If two irreducible algebraic curves M and W are birationally equivalent then $\mathbb{K}(W) \cong \mathbb{K}(M)$ and $\mathbb{K}(W \times W) \cong \mathbb{K}(M \times M)$.*

Proof. For the isomorphism $\mathbb{K}(M) \cong \mathbb{K}(W)$ see the proof of Theorem 10 in [17, § 5.5]. The isomorphism $\psi^* : \mathbb{K}(W) \to \mathbb{K}(M)$ is constructed via the pull-back map $\psi^*(f) = f \circ \psi$ where $f \in \mathbb{K}(W)$. In the same fashion, the map $\psi^* \times \psi^* : \mathbb{K}(W \times W) \to \mathbb{K}(M \times M)$ given by $(\psi^* \times \psi^*)(g) = g \circ (\psi \times \psi)$ where $g \in \mathbb{K}(W \times W)$, is an isomorphism by the universal property of products, cf. [37, Theorem 28.5]. □

Proof of Theorem 3.1. Let P_1 and P_2 be points on M. By the definition of ϕ, ψ, and $+_W$, the following equalities hold:

$$\begin{aligned} P_1 +_M P_2 &= (\mathrm{id}_M)(P_1 +_M P_2) = (\phi \circ \psi)(P_1 +_M P_2) = \phi(\psi(P_1 +_M P_2)) \\ &= \phi(\psi(P_1) +_W \psi(P_2)) \\ &= (\phi \circ +_W \circ (\psi \times \psi))(P_1, P_2) \text{ if defined.} \end{aligned} \tag{3.2}$$

The construction (3.2) works for all but finitely many pairs of points. The rest of the claim (regarding the formal maps) follows from Lemma 3.2 and from the unicity of the addition law. □

Note that the negation law can be computed accordingly.

For simplicity assume that W is in Weierstrass form

$$E_{\mathbf{W},a_1,a_3,a_2,a_4,a_6} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

which is a nonsingular model for W. Assume also that the rational mapping $+_W$ defined by

$$+_W : W \times W \to W,\ (P_1, P_2) \mapsto P_1 + P_2,$$

is the group law. By Theorem 2.7, $+_W$ is a morphism, i.e., the group law is defined for all of $W \times W$. Noting that $+_W$ is already known explicitly for W, determining $+_M$ depends only on the definition of W, ϕ and ψ. Therefore, these definitions are crucial to have the automated derivation work. In the general case, Riemann–Roch computations always guarantee a transformation to a non-singular almost-Weierstrass form given by $c_0y^2 + a_1xy + a_3y = c_2x^3 + a_2x^2 + a_4x + a_6$ with $c_0, c_2, a_i \in \mathbb{K}$, cf. [39, Theorem 3.1]. After this step, Nagell reduction can be applied (partially) to rescale c_0 and c_2 to 1, cf. [14, Algorithm 7.4.10]. A partially open source implementation is available in MAGMA, see in particular the `CrvEll` package. An alternative method based on integral basis computations is given in [41]. An open source implementation by Hoeij is available in Maple, see in particular the `algcurves` package. The latter implementation requires M to be a plane curve. Also see [19] for more applications on SINGULAR ([22]).

Next, examples will be presented to show how to automate the group law derivation. This section is limited to examples on Maple. On the other hand, it should be possible to write similar scripts in other computer algebra systems.

Example 3.3. Consider the derivation of the group law for the twisted Jacobi intersection curve $E_{I,b,a}$. This curve is obtained by the intersection of two quadratic affine surfaces in 3-space. The coordinate functions $s_1, c_1, d_1, s_2, c_2, d_2$ for $E_{I,b,a} \times E_{I,b,a}$ are labeled as `s1`, `c1`, `d1`, `s2`, `c2`, `d2`. The coordinate functions u_1, v_1, u_2, v_2 for $E_{W,0,0,-a-b,ab,0} \times E_{W,0,0,-a-b,ab,0}$ are labeled as `u1`, `v1`, `u2`, `v2`. The following Maple script defines `W`, `C`, `phi`, `psi`, `psipsi` to represent $W = E_{W,0,0,-a-b,ab,0}$, $M = E_{I,b,a}$, ϕ, ψ, and (ψ, ψ), respectively.

```
> a1:=0: a3:=0: a2:=-a-b: a4:=a*b: a6:=0:
> W:=(u,v)->(v^2+a1*u*v+a3*v-(u^3+a2*u^2+a4*u+a6)):
> C:=(s,c,d)->(b*s^2+c^2-1,a*s^2+d^2-1):
> phi:=(u,v)->(-2*v/(u^2-a*b),(u^2-2*b*u+a*b)/(u^2-a*b),(u^2-2*a*u+a*b)/(u^2-a*b)):
> psi:=(s,c,d)->(a*(1+c)/(1-d),-a^2*s*(1+c)*(c+d)/((1-d)^2*(1+d))):
> psipsi:=(s1,c1,d1,s2,c2,d2)->(psi(s1,c1,d1),psi(s2,c2,d2)):
```

In this example, W, ϕ, and ψ are copied from "Twisted Jacobi intersection form" of Section 2 to match a standard choice of the identity element.

Addition. The following Maple script derives the corresponding addition formulae. The first line defines the addition formulae for W and the second line applies 3.1.

```
> addW:=(u1,v1,u2,v2)->(((v2-v1)/(u2-u1))^2+a1*(v2-v1)/(u2-u1)-a2-u1-u2,(v2-v1)/ \
    (u2-u1)*(u1-(((v2-v1)/(u2-u1))^2+a1*(v2-v1)/(u2-u1)-a2-u1-u2))-v1-a1*u3-a3):
> addM:=phi(addW(psipsi(s1,c1,d1,s2,c2,d2))):
```

The addition formulae stored in `addM` are given by $(s_1, c_1, d_1) + (s_2, c_2, d_2) = (s_3, c_3, d_3)$ where

$$
\begin{aligned}
s_3 = {} & -2((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+ \\
& d_1)/((1-d_1)^2(1+d_1)))(2a(1+c_1)/(1-d_1) - (-a^2 s_2(1+c_2)(c_2+ \\
& d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+ \\
& d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1))^2 + a(1+c_2)/(1-d_2) - \\
& a-b)/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1)) + a^2 s_1(1+c_1)(c_1+ \\
& d_1)/((1-d_1)^2(1+d_1)))/(((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + \\
& a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+ \\
& c_1)/(1-d_1))^2 - a(1+c_1)/(1-d_1) - a(1+c_2)/(1-d_2) + a + b)^2 - ab),
\end{aligned}
$$

$$c_3 = (((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1))^2 - a(1+c_1)/(1-d_1) - a(1+c_2)/(1-d_2) + a + b)^2 - 2b((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1))^2 - a(1+c_1)/(1-d_1) - a(1+c_2)/(1-d_2) + a + b) + ab)/(((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1))^2 - a(1+c_1)/(1-d_1) - a(1+c_2)/(1-d_2) + a + b)^2 - ab),$$

$$d_3 = (((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1))^2 - a(1+c_1)/(1-d_1) - a(1+c_2)/(1-d_2) + a + b)^2 - 2a((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1))^2 - a(1+c_1)/(1-d_1) - a(1+c_2)/(1-d_2) + a + b) + ab)/(((-a^2 s_2(1+c_2)(c_2+d_2)/((1-d_2)^2(1+d_2)) + a^2 s_1(1+c_1)(c_1+d_1)/((1-d_1)^2(1+d_1)))^2/(a(1+c_2)/(1-d_2) - a(1+c_1)/(1-d_1))^2 - a(1+c_1)/(1-d_1) - a(1+c_2)/(1-d_2) + a + b)^2 - ab).$$

Specialized negation and doubling formulae can be computed following the same framework.

The computer-derived formulae are overly involved with many terms which makes them inefficient in computations. For instance, both addition and doubling formulae have total degree of the fractions over 50. The next section is a continuation of Example 3.3 for finding more "suitable" representatives for s_3, c_3, and d_3 among each of the residue classes $[s_3]$, $[c_3]$, and $[d_3]$, respectively.

3.2 Minimal total degree

Let V be a variety over $\mathbb{K}$ and $\mathbb{K}(V)$ the function field of V. Note that the elements of $\mathbb{K}(V)$ are represented by rational functions on V.

Since the chief objects of study are group laws on elliptic curves, V can be fixed to an elliptic curve E or to the product $E \times E$. Let $P \in V$ and $f \in \mathbb{K}(V)$ such that f is regular at P. Suppose that the aim is to evaluate $f = h/g$ at P *efficiently* with $g \neq 0$. It is then reasonable to find a suitable $\hat{f} = \hat{h}/\hat{g}$ such that $\hat{h}g - h\hat{g} \equiv 0 \bmod I(V)$ where $I(V)$ is the ideal generated by the defining equation(s) of V. Then, $f(P) = \hat{f}(P)$ assuming that $\hat{g}(P) \neq 0$.

The computational effort for finding the suitable $\hat{f}$ can be neglected here since $\hat{f}$ can be fixed for many evaluations. Roughly speaking, the smaller the number

of field operations used for an evaluation of $\hat{f}$ at P, the more *efficient* the evaluation is. The term efficiency here is usually understood as the *running time* or the space consumption of an algorithm. Note that other interpretations are possible such as the required transmission size of some data or consumed energy along the execution. The emphasis here is on the running time aspect. See also [16].

A common experience for an efficient evaluation of a rational function on a variety at a randomly chosen non-singular point is that the evaluation takes less time if the numerator and denominator have lower total degrees, and preferably having no "common factor", cf. [13]. The numerator and denominator of a rational function in $\mathbb{K}(V)$ can be viewed as polynomial functions in $\mathbb{K}[V]$. These polynomial functions, for the purpose of this work, are the multivariate polynomial expressions arising in the group law of an elliptic curve. Therefore, the main emphasis of this section is on finding suitable fractions of polynomials with low/lowest total degree in making a description of the group law. Note that the arithmetic of elliptic curves is known to be very efficient and it has attracted a lot of attention over the past few decades. Standard references are [15, 23]. More updated reviews can be found in [7]. In this sense, the present work is an attempt to improve previous upper bounds for efficient computations.

Concerning the numerator and denominator of s_3 (or c_3 or d_3) in Example 3.3, it is intuitive to ask whether the denominator is a unit in the corresponding coordinate ring. If this is the case, the fraction reduces to a polynomial which allows working in affine coordinates without inverting elements of $\mathbb{K}$. In large characteristic fields, this turns out to be possible for negation formulae most of the time. However, for doubling and addition this is not possible in any of the three forms that are studied in this work.

It is also intuitive to ask whether there exists representatives having minimal total degrees for both the numerators and denominators. The two may not be possible simultaneously, i.e. among all possible fractions, a fraction with minimal total degree numerator may not have a minimal total degree denominator (and vice versa). However, there always exist representatives with minimal total degree. This section collects necessary tools from literature to find such representatives. Computer algebra examples are also provided. Efficiency of the simplification process is not a major issue as long as the simplification can be done in a reasonable time.

Two algorithms for simplifying rational expressions, proposed by Monagan and Pearce in 2006 in [36], are adapted in this section since their algorithms perfectly fit the aforementioned goal of finding formulae with low/lowest total degree of fractions in the corresponding coordinate ring (i.e. $\mathbb{K}[M]$ for negation and doubling; and $\mathbb{K}[M \times M]$ for addition). Monagan and Pearce's first algorithm computes a reduced canonical form (RCF) of a fraction f/g modulo a proper prime ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ where $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. The coordinates $x_1, \ldots, x_n$

can be suitably renamed to $s_1, c_1, d_1, s_2, c_2, d_2$ in the case of Example 3.3. Using a prime ideal ensures that $\mathbb{K}[x_1, \ldots, x_n]/I$ is an integral domain and thus contains no zero divisors. Note that this is always the case for coordinate rings of elliptic curves (or their products). Now, let m/h be an RCF for a/b such that $ah - bm \equiv 0 \mod I$ where $a, b, m, h \in \mathbb{K}[x_1, \ldots, x_n]$ with $b, h \notin I$. The algorithm is built on three observations:

1. The colon ideal $J = (\langle g \rangle + I) : \langle f \rangle$ contains an h having no common components with g. Let $\{h_1, \ldots, h_t\}$ be a reduced Gröbner basis with respect to a graded monomial ordering. Each h_i is a candidate for h since $h \in \langle h_1, \ldots, h_t \rangle$.
2. By the definition of a colon ideal, b must divide $h_i a$. Thus, $m_i = h_i a/b$ can be computed using an exact division. Now selecting $m/h = m_i/h_i$ with $\min(\deg(h_i))$ gives a representation which guarantees a minimal total degree for the denominator of m/h and a removal of all common components. Note that for all curve models considered in this work, this computation yields formulae having minimal total degree of fractions, which will be used in Section 4. However, to this end there is no guarantee that a minimal $\deg(m) + \deg(h)$ will be obtained.
3. Sometimes adding a common component to the numerator or denominator leads to a lower total degree sum. This idea is pursued by Monagan and Pearce by a computation of the reduced Gröbner basis of the module $\{[m, h] : fh - gm \equiv 0 \mod I\}$ with respect to a term-over-position order. Refer to the original paper [36] for details and to [1] for definitions of modules and term-over-position order.

   This last modification finds a "good" balance between numerator and denominator. However, there is still no guarantee that a minimal $\deg(m) + \deg(h)$ will be obtained.

An implementation of this algorithm comes with Maple v.11+. An open source Maple implementation is given in Pearce's thesis [38].

Example 3.4. The following Maple script simplifies the automated formulae from Example 3.3 using Monagan/Pearce reduced canonical form algorithm:

```
> addM:=simplify([addM],[M(s1,c1,d1),M(s2,c2,d2)],tdeg(c1,c2,d1,d2));
```

Addition. The simplified addition formulae are given by

$$(s_1, c_1, d_1) + (s_2, c_2, d_2) = \Big(\frac{s_1c_2d_2 + c_1d_1s_2}{1 - abs_1^2s_2^2}, \frac{c_1c_2 - bs_1d_1s_2d_2}{1 - abs_1^2s_2^2}, \frac{d_1d_2 - as_1c_1s_2c_2}{1 - abs_1^2s_2^2}\Big).$$

In all of these outputs, the total degrees of the denominators are minimized with respect to the fixed monomial ordering. Without a justification for now, it can be stated that the addition formulae are not of minimal total degree sum.

Monagan and Pearce's second algorithm always finds a fraction with minimal total degree sum of the numerator and denominator. Their algorithm makes a search among all possible m/n starting from lowest degree 0 assuming that the fraction can be simplified to a constant in $\mathbb{K}$. If the solution of the resulting system does not give the hypothesized numerator and denominator, the hypothesized degree is increased by one for both the numerator and denominator. The procedure is repeated until a solution is found. Then the remaining cases are explored in a recursive manner. For details see [38, § 4]. An implementation of this algorithm comes with Maple v.11+. An open source Maple implementation is given in Pearce's thesis [38].

Example 3.5. The following Maple script[1] simplifies the automated addition formulae using Monagan/Pearce minimal total degree algorithm:

```
> addM:=simplify(addM,[M(s1,c1,d1),M(s2,c2,d2)],mindeg);
```

Addition. The simplified addition formulae are given by

$$(s_1, c_1, d_1) + (s_2, c_2, d_2) = \Big(\frac{s_1^2 - s_2^2}{s_1c_2d_2 - c_1d_1s_2}, \frac{s_1c_1d_2 - d_1s_2c_2}{s_1c_2d_2 - c_1d_1s_2}, \frac{s_1d_1c_2 - c_1s_2d_2}{s_1c_2d_2 - c_1d_1s_2}\Big).$$

It is experimentally observed that the rational simplification for finding minimal total degree addition formulae takes less than a second on a Core 2 processor running at 2.66 GHz once the algorithm is fed with initial formulae in canonical form. Using the same algorithm, it can be checked that the addition formulae

[1] *Warning:* Maple v.11 and v.12 have internal bugs which are triggered by this example. The problem is that the minimal total degree implementation uses local variables which clash with the coordinate functions `c1`, `d1`, `c2`, and `d2` resulting in wrong outputs. To surpass these bugs, simply rename `c1` to `cc1`; `d1` to `dd1`; `c2` to `cc2`; and `d2` to `dd2` in all relevant scripts in this section.

computed above are really of minimal total degree. This also justifies the claims of Example 3.4.

For other forms of elliptic curves (including the projective representations), it is easy to modify/parametrize the scripts of Section 3.1 and of this section, in order to detect "reduced" formulae for negation, doubling, and addition.

Let $\mathbb{L}$ be an algebraic extension of $\mathbb{K}$. The computer derived addition formulae will be used in Section 4 to make a complete description of the morphism $+_{M/\mathbb{L}}$ for desingularized curves of genus 1 in several different forms.

3.3 Automated validations

It is useful to have a validation tool to decide whether two rational functions on a variety are equivalent. The key tool is described in the following lemma.

Lemma 3.6 (Ideal membership). *Let G be a Gröbner basis for an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Let f be a polynomial in $\mathbb{K}[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the normal form of f by G is zero.*

Proof. The proof follows from basic properties of Gröbner basis. See [17, § 2.6]. □

Let V be a variety and $I(V)$ the ideal of V. Let $f, \hat{f}, g, \hat{g} \in \mathbb{K}[V]$ such that $g, \hat{g} \notin I(V)$. Recall from Section 2 that the quotients f/g and $\hat{f}/\hat{g}$ with $g, \hat{g} \neq 0$ define the same function on V if and only if $\hat{f}g - f\hat{g} \in I(V)$. Now, applying Lemma 3.6 answers whether f/g and $\hat{f}/\hat{g}$ are equivalent functions on V.

Example 3.7. It can be validated that the addition formulae in Examples 3.4 and 3.5 are coordinate-wise equivalent rational functions on $V = M \times M$. The following Maple script implements this validation. Note that the last line defines the quotient relations.

```
> simplify([
>   (s1*c2*d2+c1*d1*s2)*(s1*c2*d2-c1*d1*s2)-(s1^2-s2^2)*(1-a*b*s1^2*s2^2),
>   (c1*c2-b*s1*d1*s2*d2)*(s1*c2*d2-c1*d1*s2)-(s1*c1*d2-d1*s2*c2)*(1-a*b*s1^2*s2^2),
>   (d1*d2-a*s1*c1*s2*c2)*(s1*c2*d2-c1*d1*s2)-(s1*d1*c2-c1*s2*d2)*(1-a*b*s1^2*s2^2)
> ],[b*s1^2+c1^2-1,a*s1^2+d1^2-1,b*s2^2+c2^2-1,a*s2^2+d2^2-1]);
```

More implementations have already been developed in [7] and several examples are given in that database.

3.4 Finding more formulae

In Section 3.2, it was noted how a computation of colon ideals was used for removing common components of the numerator and denominator of a rational expression modulo a polynomial ideal. For the purpose of this work, these rational expressions are rational functions on an elliptic curve M or rational functions on the product $M \times M$. By using a graded monomial order and by skipping the module construction phase in the Monagan/Pearce method, it is possible to minimize the total degree of either the numerator or denominator. More formulae can then be derived from the other low degree denominators that appear in the reduced Gröbner basis.

Example 3.8. It is convenient to continue with the investigation on twisted Jacobi intersection form. Consider the polynomials $f = s_1^2 - s_2^2$ and $g = s_1c_2d_2 - c_1d_1s_2$ in $\mathbb{K}[c_1, c_2, d_1, d_2, s_1, s_2]$ where $\mathbb{K} = \mathbb{Q}(a, b)$. Since $\mathrm{GCD}(f, g) = 1$, the fraction f/g does not simplify in $\mathbb{K}(c_1, c_2, d_1, d_2, s_1, s_2)$. Now assume that f/g is a function on $E_{I,b,a} : bs^2 + c^2 - 1, as^2 + d^2 - 1$ where $a, b \in \mathbb{K}$ with $ab(a - b) \neq 0$. Let K be the ideal generated by the relations $bs_1^2 + c_1^2 - 1$, $as_1^2 + d_1^2 - 1$, $bs_2^2 + c_2^2 - 1$, $as_2^2 + d_2^2 - 1$. The reduced Gröbner basis of the colon ideal $J = (\langle f \rangle + K) : \langle g \rangle$ with respect to any graded monomial order must contain a minimal total degree denominator, see Section 3.2. In addition, it *often* contains other low degree denominators because of the graded order which dominates in reducing the total degree of the generators. Indeed the generators of the reduced Gröbner basis of J with respect to graded reverse lexicographical order with $c > d > s$ are given by the sequence

$$
\begin{aligned}
G = \; & [c_2d_1s_1^2s_2 - c_1d_2s_1s_2^2 + (1/b)c_1d_2s_1 - (1/b)c_2d_1s_2, c_1d_2s_1^2s_2 - \\
& c_2d_1s_1s_2^2 + (1/a)c_2d_1s_1 - (1/a)c_1d_2s_2, c_2s_1^3s_2 - (1/(ab))c_1d_1d_2 - \\
& (1/b)c_2s_1s_2, d_2s_1^3s_2 - (1/(ab))c_1c_2d_1 - (1/a)d_2s_1s_2, c_1s_1s_2^3 - \\
& (1/(ab))c_2d_1d_2 - (1/b)c_1s_1s_2, d_1s_1s_2^3 - (1/(ab))c_1c_2d_2 - \\
& (1/a)d_1s_1s_2, c_1c_2d_1d_2 - abs_1^3s_2 - abs_1s_2^3 + (a + b)s_1s_2, c_1c_2d_1s_2 + \\
& bd_2s_1s_2^2 - d_2s_1, c_1d_1d_2s_2 + ac_2s_1s_2^2 - c_2s_1, c_1c_2s_1s_2 + \\
& (1/a)d_1d_2, d_1d_2s_1s_2 + (1/b)c_1c_2, s_1^2s_2^2 - (1/(ab)), c_2d_2s_1 - \\
& c_1d_1s_2, c_1^2 + bs_1^2 - 1, c_2^2 + bs_2^2 - 1, d_1^2 + as_1^2 - 1, d_2^2 + as_2^2 - 1].
\end{aligned}
$$

By the definition of colon ideal, J trivially contains K. Therefore, the generators of G can be discarded if they are in K. This can be efficiently detected using Lemma 3.6. Observe that the initial denominator $s_1c_2d_2 - c_1d_1s_2$ is in G. On the other hand, there are several more low total degree entries which are other candidates for the denominator of equivalent fractions. For instance, select the entry $c_1c_2s_1s_2 + (1/a)d_1d_2$. Using a multivariate exact division algorithm the new

numerator is computed as $(c_1c_2s_1s_2 + (1/a)d_1d_2)f/g = (c_1s_2d_2 + s_1d_1c_2)/a$. So the alternative formula is given by $(c_1s_2d_2 + s_1d_1c_2)/(d_1d_2 + ac_1c_2s_1s_2)$. For an exact division algorithm see Pearce's thesis [38]. Each one of the other entries gives rise to another fraction. Even more fractions can be obtained by changing order of the variables in the lexicographical ordering.

4 Group law in affine coordinates

The goal of this section is two-fold. The first part of the goal is to find low-degree point addition formulae for fixed representations of elliptic curves. Some of the formulae are obtained from literature resources whereas some others are derived with the tools from Section 3. In this context, each of the sections mainly concentrates on two denominators which naturally arise when searching for low degree group laws for each elliptic curve form. As the second part of the goal, the exceptional cases of the selected denominators are explicitly determined and practical ways of preventing division-by-zero exceptions are studied including pointers to the literature when possible. This work focuses on three aforementioned forms of elliptic curves in Section 2 which are the most commonly used ones in practical applications.

A complete addition algorithm is presented for each of the forms to handle all possible inputs including the point(s) at infinity. The complete description of addition law for all curves given in a particular form can be extracted from the relevant birational maps in Section 2.3 and the discussions on the exceptional points of the birational equivalence. In this context, exceptions can be handled by first sending the summands on a curve given in a particular form to the birationally equivalent Weierstrass curve, then carrying out the addition on the Weierstrass curve where a complete addition algorithm is present in the literature, and finally sending the sum on the Weierstrass curve to the desired sum on the original curve. Indeed, this approach *implicitly* describes a complete addition algorithm on all curves of a particular form. However, the arithmetic is now dependent on the arithmetic of Weierstrass curves. It is motivating to make a self-contained complete addition algorithm for each of these forms. The lemmas presented in Sections 4.1–4.3 investigate exceptional inputs and make the statement of a complete addition algorithm easier. These lemmas also provide useful information for an exception-free implementation. Since the same goals are set for each curve model, it is not surprising to have analogous results in each section. Therefore, some repetitions are unavoidable. However, it is still motivating to observe how similar ideas work for almost all studied forms.

4.1 Extended Jacobi quartic form

This section presents the group law on $E_{\mathbf{Q},d,a}$ in affine coordinates. It also investigates the exceptional summands for each formula and provides a complete addition algorithm for all extended Jacobi quartic curves by properly handling an entire set of division-by-zero exceptions. In addition, practical ways of preventing these exceptions are explained.

Throughout this section, let $\mathbb{K}$ be a field of odd characteristic. Recall from Section 2 that an extended Jacobi quartic curve is defined by

$$E_{\mathbf{Q},d,a} : y^2 = dx^4 + 2ax^2 + 1$$

where $a, d \in \mathbb{K}$ with $d(a^2 - d) \neq 0$. Recall from Section 2 that the set of $\mathbb{K}$-rational points on the desingularization of $E_{\mathbf{Q},d,a}$ is defined by

$$E_{\mathbf{Q},d,a}(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid y^2 = dx^4 + 2ax^2 + 1\} \cup \{\Omega_1, \Omega_2\}$$

where Ω_1, Ω_2 are points at infinity.

Identity element and negation. The identity element is $(0, 1)$. Let (x_1, y_1) be a point on $E_{\mathbf{Q},d,a}$. The negative of (x_1, y_1) is $(-x_1, y_1)$.

Doubling. The doubling formulae on $E_{\mathbf{Q},d,a}$ are given by $[2](x_1, y_1) = (x_3, y_3)$ where

$$x_3 = 2x_1y_1/\big(2 - y_1^2 + 2ax_1^2\big), \tag{4.1}$$

$$y_3 = \Big(2y_1^2\big(y_1^2 - 2ax_1^2\big)/\big(2 - y_1^2 + 2ax_1^2\big)^2\Big) - 1 \tag{4.2}$$

assuming that $2 - y_1^2 + 2ax_1^2 \neq 0$. These formulae do not depend on the curve constant d and are of minimal total degree. By the curve equation the denominator $2 - y_1^2 + 2ax_1^2$ is equivalent to $1 - dx_1^4$. This denominator can also be used if the total degree is not of concern.

Affine points of order 2 can be determined by solving $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ and $(x_3, y_3) = (0, 1)$ for x_1 and y_1 where x_3 and y_3 are given by (4.1) and (4.2). The point $(0, -1)$ is of order 2. There are no other affine points of order 2. There are three points of order 2 in total (over a sufficiently large finite extension of $\mathbb{K}$). Therefore, both points at infinity Ω_1 and Ω_2 have to be of order 2.

The four points of the form $(x, 0)$ are of order 4 which can be determined by solving $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ and $(x_3, y_3) = (0, -1)$ for x_1 and y_1 where x_3 and y_3 are given by (4.1) and (4.2). There are twelve points of order 4 in total (over

a sufficiently large finite extension of $\mathbb{K}$). Doubling each of the remaining eight points must give Ω_1 or Ω_2. These eight affine points can be explicitly determined by solving $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ and $2 - y_1^2 + 2ax_1^2 = 0$ for x_1 and y_1. These points are the only exceptions of (4.1) and (4.2). The following remark is immediate.

Remark 4.1. $[2](x_1, y_1)$ is a point at infinity if and only if $2 - y_1^2 + 2ax_1^2 = 0$.

Remark 4.1 does not extend to the case of generic additions. However, it is still useful in proving some lemmas regarding the generic addition formulae which will be presented next.

Dedicated addition. Further let (x_2, y_2) be a point on $E_{\mathbf{Q},d,a}$. The addition formulae on $E_{\mathbf{Q},d,a}$ are given by $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ where

$$x_3 = (x_1^2 - x_2^2)/(x_1y_2 - y_1x_2), \tag{4.3}$$

$$y_3 = (x_1^2 + x_2^2)(y_1y_2 - 2ax_1x_2)/(x_1y_2 - y_1x_2)^2 - 2x_1x_2(1 + dx_1^2x_2^2)/(x_1y_2 - y_1x_2)^2 \tag{4.4}$$

assuming that $x_1y_2 - y_1x_2 \neq 0$. These formulae are of minimal total degree. These formulae do not work for identical summands hence the name *dedicated*.

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then $x_1y_2 - y_1x_2 = 0$. Otherwise, $(x_1, y_1) + (x_2, y_2)$ would be an affine point since it can be shown using the relations $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ and $y_2^2 = dx_2^4 + 2ax_2^2 + 1$ that the algebraic expressions for (x_3, y_3) satisfy $y_3^2 = dx_3^4 + 2ax_3^2 + 1$. The converse, however, does not necessarily apply. This means that if $x_1y_2 - y_1x_2 = 0$ then $(x_1, y_1) + (x_2, y_2)$ may not be a point at infinity. Therefore it is worth investigating the exceptional cases. The denominators of (4.3) and (4.4) vanish for some summands which are described in the following lemma explicitly.

Lemma 4.2. *Let $a, d \in \mathbb{K}$ with $d(a^2 - d) \neq 0$. Fix $\delta \in \mathbb{K}$ so that $\delta^2 = d$. Fix $x_1, x_2 \in \mathbb{K}\backslash\{0\}$ and $y_1, y_2 \in \mathbb{K}$ such that $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ and $y_2^2 = dx_2^4 + 2ax_2^2 + 1$. Then $x_1y_2 - y_1x_2 = 0$ if and only if $(x_2, y_2) \in S$ where*

$$S = \left[(x_1, y_1), (-x_1, -y_1), \left(\frac{1}{\delta x_1}, \frac{y_1}{\delta x_1^2}\right), \left(\frac{-1}{\delta x_1}, \frac{-y_1}{\delta x_1^2}\right)\right].$$

Proof. $\Rightarrow$: Assume that $x_1y_2 - y_1x_2 = 0$. Solving the system of equations $x_1y_2 - y_1x_2 = 0$, $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ for x_2 and y_2 gives S. All entries in S are defined since $x_1 \neq 0$.

$\Leftarrow$: The claim follows trivially by substitution. □

The following lemma shows that if one of the summands is of odd order then in the presence of an exception, the other summand is always of even order.

Lemma 4.3. *Let a, d, x_1, y_1, x_2, y_2 be defined as in Lemma 4.2. Assume that $P_1 = (x_1, y_1)$ is a fixed point of odd order. Assume that $P_2 \in S\backslash\{P_1\}$. Then P_2 is of even order.*

Proof. First note that points at infinity are of order 2. Assume that $P_1 = (x_1, y_1)$ is a fixed point of odd order hence not a point at infinity. Suppose that P_2 is of odd order hence not a point at infinity. It follows that $P_1 \pm P_2$, $M = 2P_1$, and $N = 2P_2$ are all of odd order hence not points at infinity.

Assume that $P_2 \in S\backslash\{P_1\}$. So, $P_2 \neq P_1$. In addition, $x_1y_2 - y_1x_2 = 0$ by Lemma 4.2. It follows that $P_1 \neq -P_2$, for otherwise, $x_1y_2 - y_1x_2 = 2x_1y_1 = 0$ which means that x_1 or y_1 is zero. But then P_1 would be of even order since $x_1 \neq 0$.

Note that $y_2 = y_1x_2/x_1$ is defined since $x_1 \neq 0$, by the definition. Using this relation together with (4.1), (4.2), and the curve equation gives

$$\begin{aligned}
x(N)^2 &= \frac{(2x_2y_2)^2}{(2 - y_2^2 + 2ax_2^2)^2} \\
&= \frac{(2x_2y_2)^2}{(2 - y_2^2 + 2ax_2^2)^2 + 4(y_2^2 - (dx_2^4 + 2ax_2^2 + 1))} \\
&= \frac{(2x_2y_2)^2}{(y_2^2 - 2ax_2^2)^2 - 4dx_2^4} = \frac{(2x_2\frac{y_1x_2}{x_1})^2}{((\frac{y_1x_2}{x_1})^2 - 2ax_2^2)^2 - 4dx_2^4} \\
&= \frac{(2x_1y_1)^2}{(2 - y_1^2 + 2ax_1^2)^2} = x(M)^2, \\
y(N) &= \frac{2y_2^2(y_2^2 - 2ax_2^2)}{(2 - y_2^2 + 2ax_2^2)^2} - 1 = \frac{2y_2^2(y_2^2 - 2ax_2^2)}{(y_2^2 - 2ax_2^2)^2 - 4dx_2^4} - 1 \\
&= \frac{2(\frac{y_1x_2}{x_1})^2((\frac{y_1x_2}{x_1})^2 - 2ax_2^2)}{((\frac{y_1x_2}{x_1})^2 - 2ax_2^2)^2 - 4dx_2^4} - 1 = \frac{2y_1^2(y_1^2 - 2ax_1^2)}{(2 - y_1^2 + 2ax_1^2)^2} - 1 \\
&= y(M),
\end{aligned}$$

where $x(N)$ means the x-coordinate of the point N and similarly for $x(M)$, $y(N)$, and $y(M)$.

Hence, $M = \pm N$. But then $M \mp N = 2P_1 \mp 2P_2 = 2(P_1 \mp P_2) = (0, 1)$. Since $P_1 \neq \pm P_2$, it follows that $P_1 \mp P_2$ is a point of order 2, a contradiction. In conclusion, $P_2 \in S\backslash\{P_1\}$ is of even order because P_1 is of odd order. □

A practical solution is now provided to prevent the exceptional cases of (4.3) and (4.4).

Lemma 4.4. *Let $\mathbb{K}$ be a field of odd characteristic. Let $E_{\mathbf{Q},d,a}$ be an extended Jacobi quartic curve defined over $\mathbb{K}$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E_{\mathbf{Q},d,a}$. Assume that P_1 and P_2 are of odd order with $P_1 \neq P_2$. It follows that $x_1y_2 - y_1x_2 \neq 0$.*

Proof. Assume that P_1 and P_2 are of odd order with $P_1 \neq P_2$. Suppose that $x_1 = 0$ and $x_2 = 0$. Then, $P_1 = P_2 = (0, 1)$, a contradiction. So, either $x_1 \neq 0$ or $x_2 \neq 0$. Suppose that $x_1 \neq 0$ and $x_2 = 0$ or $x_1 = 0$ and $x_2 \neq 0$ then the claim follows trivially. Now, $x_1x_2 \neq 0$. The claim then follows from Lemma 4.2 and Lemma 4.3 (by swapping P_1 and P_2 when necessary). □

Unified addition. Alternative addition formulae on $E_{\mathbf{Q},d,a}$ are given by $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ where

$$x_3 = (x_1y_2 + y_1x_2)/(1 - dx_1^2x_2^2), \tag{4.5}$$

$$y_3 = (y_1y_2 + 2ax_1x_2)(1 + dx_1^2x_2^2)/(1 - dx_1^2x_2^2)^2 + 2dx_1x_2(x_1^2 + x_2^2)/(1 - dx_1^2x_2^2)^2 \tag{4.6}$$

assuming that $1 - dx_1^2x_2^2 \neq 0$. These formulae work for identical summands in most of the cases hence the name *unified*.

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then $1 - dx_1^2x_2^2 = 0$. Otherwise, $(x_1, y_1) + (x_2, y_2)$ would be an affine point since it can be shown using the relations $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ and $y_2^2 = dx_2^4 + 2ax_2^2 + 1$ that the algebraic expressions for (x_3, y_3) satisfy $y_3^2 = dx_3^4 + 2ax_3^2 + 1$. The converse, however, does not necessarily apply. This means that if $1 - dx_1^2x_2^2 = 0$ then $(x_1, y_1) + (x_2, y_2)$ may not be a point at infinity. Therefore it is worth investigating the exceptional cases. The denominators of (4.5) and (4.6) vanish for some summands which are described in the following lemma explicitly.

Lemma 4.5. *Let $a, d \in \mathbb{K}$ with $d(a^2 - d) \neq 0$. Fix $\delta \in \mathbb{K}$ so that $\delta^2 = d$. Fix $x_1, x_2 \in \mathbb{K}\backslash\{0\}$ and $y_1, y_2 \in \mathbb{K}$ such that $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ and $y_2^2 = dx_2^4 + 2ax_2^2 + 1$. Then $1 - dx_1^2x_2^2 = 0$ if and only if $(x_2, y_2) \in S'$ where*

$$S' = \Big[\Big(\frac{1}{\delta x_1}, \frac{-y_1}{\delta x_1^2}\Big), \Big(\frac{-1}{\delta x_1}, \frac{y_1}{\delta x_1^2}\Big), \Big(\frac{1}{\delta x_1}, \frac{y_1}{\delta x_1^2}\Big), \Big(\frac{-1}{\delta x_1}, \frac{-y_1}{\delta x_1^2}\Big)\Big].$$

Proof. $\Rightarrow$: Assume that $1 - dx_1^2x_2^2 = 0$. Solving the system of equations $1 - dx_1^2x_2^2 = 0$, $y_1^2 = dx_1^4 + 2ax_1^2 + 1$ for x_2 and y_2 gives S'. All entries in S' are defined since $x_1 \neq 0$.

$\Leftarrow$: The claim follows trivially by substitution. □

This lemma and Lemma 4.2 exclude $x_1 = 0$. For $x_1 = 0$ the denominators in (4.5) and (4.6) are defined and equal to 1.

The following lemma shows that if one of the summands is of odd order then in the presence of a vanished denominator, the other summand is always of even order.

Lemma 4.6. *Let a, d, x_1, y_1, x_2, y_2 be defined as in Lemma* 4.5. *Assume that $P_1 = (x_1, y_1)$ is a fixed point of odd order. Assume that $P_2 = (x_2, y_2) \in S'$. Then P_2 is of even order.*

Proof. First note that points at infinity are of order 2. Assume that $P_1 = (x_1, y_1)$ is a fixed point of odd order hence not a point at infinity. Suppose that P_2 is of odd order hence not a point at infinity. It follows that $P_1 \pm P_2$, $M = 2P_1$, and $N = 2P_2$ are all of odd order hence not points at infinity.

Assume that $P_2 \in S'$. Then, $1 - dx_1^2x_2^2 = 0$ by Lemma 4.5 and it follows that $P_1 \neq \pm P_2$, for otherwise, $1 - dx_1^4 = 2 - y_1^2 + 2ax_1^2 = 0$ and P_1 would be of even order by Remark 4.1.

Note that $x_1 \neq 0$ since $1 - dx_1^2x_2^2 = 0$ (also true by definition). So, $x_2^2 = 1/(dx_1^2)$ is defined. Using this relation together with (4.5), (4.6), and the curve equation gives

$$
\begin{aligned}
x(N)^2 &= \frac{(2x_2y_2)^2}{(1-dx_2^4)^2} = \frac{4x_2^2(dx_2^4 + 2ax_2^2 + 1)}{(1-dx_2^4)^2} \\
&= \frac{4\frac{1}{dx_1^2}(d(\frac{1}{dx_1^2})^2 + 2a\frac{1}{dx_1^2} + 1)}{(1-d(\frac{1}{dx_1^2})^2)^2} \\
&= \frac{4x_1^2(dx_1^4 + 2ax_1^2 + 1)}{(1-dx_1^4)^2} = \frac{(2x_1y_1)^2}{(1-dx_1^4)^2} = x(M)^2, \\
y(N) &= \frac{(y_2^2 + 2ax_2^2)(1+dx_2^4) + 4dx_2^4}{(1-dx_2^4)^2} \\
&= \frac{((dx_2^4 + 2ax_2^2 + 1) + 2ax_2^2)(1+dx_2^4) + 4dx_2^4}{(1-dx_2^4)^2}
\end{aligned}
$$

$$= \frac{((d(\frac{1}{dx_1^2})^2 + 2a\frac{1}{dx_1^2} + 1) + 2a\frac{1}{dx_1^2})(1 + d(\frac{1}{dx_1^2})^2) + 4d(\frac{1}{dx_1^2})^2}{(1 - d(\frac{1}{dx_1^2})^2)^2}$$

$$= \frac{((dx_1^4 + 2ax_1^2 + 1) + 2ax_1^2)(1 + dx_1^4) + 4dx_1^4}{(1 - dx_1^4)^2}$$

$$= \frac{(y_1^2 + 2ax_1^2)(1 + dx_1^4) + 4dx_1^4}{(1 - dx_1^4)^2} = y(M). \tag{4.7}$$

Hence, $M = \pm N$. But then $M \mp N = 2P_1 \mp 2P_2 = 2(P_1 \mp P_2) = (0, 1)$. Since $P_1 \neq \pm P_2$, it follows that $P_1 \mp P_2$ is a point of order 2, contradiction. In conclusion, $P_2 \in S'$ is of even order because P_1 is of odd order. □

The points at infinity on the desingularized projective closure of $E_{\mathbf{Q},d,a}$ are not defined over $\mathbb{K}$ if d is not a square in $\mathbb{K}$. Having noted this, the following lemma implies that these addition formulae are complete (i.e. these formulae define the addition law) provided that d is not a square in $\mathbb{K}$.

Lemma 4.7. *Let $d, x_1, x_2 \in \mathbb{K}$. Assume that d is non-square. Then*

$$1 - dx_1^2x_2^2 \neq 0.$$

Proof. Suppose that $1 - dx_1^2x_2^2 = 0$. So $d, x_1, x_2 \neq 0$. But then we have $d = (1/(x_1x_2))^2$, a contradiction. □

In the following lemma, with reasonable assumptions, it is shown that exceptions can be prevented regardless of any assumption on the curve constants.

Lemma 4.8. *Let $\mathbb{K}$ be a field of odd characteristic. Let $E_{\mathbf{Q},d,a}$ be an extended Jacobi quartic curve defined over $\mathbb{K}$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E_{\mathbf{Q},d,a}$. Assume that P_1 and P_2 are of odd order. It follows that $1 - dx_1^2x_2^2 \neq 0$.*

Proof. Assume that P_1 and P_2 are of odd order. Assume that $x_1x_2 = 0$ then $1-dx_1^2x_2^2 \neq 0$ as desired. From now on assume that $x_1x_2 \neq 0$. The claim follows from Lemma 4.5 and Lemma 4.6 (by swapping P_1 and P_2 when necessary). □

Exception handling in the general case. Algorithm 4.9 provides a complete addition on all extended Jacobi quartic curves.

Algorithm 4.9. Addition law in affine coordinates for extended Jacobi quartic form

Input : $P_1, P_2, \Omega_1, \Omega_2 \in E_{\mathbf{Q},d,a}(\mathbb{K})$ and fixed $\delta \in \mathbb{K}$ such that $\delta^2 = d$.

Output : $P_1 + P_2$.

1 **if** $P_1 \in \{\Omega_1, \Omega_2\}$ **then** $P_t \leftarrow P_1$, $P_1 \leftarrow P_2$, $P_2 \leftarrow P_t$.
2 **if** $P_2 = \Omega_1$ **then**
3 | **if** $P_1 = \Omega_1$ **then return** $(0, 1)$. **else if** $P_1 = \Omega_2$ **then return** $(0, -1)$.
4 | **else if** $P_1 = (0, 1)$ **then return** Ω_1. **else if** $P_1 = (0, -1)$ **then return** Ω_2.
5 | **else return** $(-1/(\delta x_1), y_1/(\delta x_1^2))$.
6 **else if** $P_2 = \Omega_2$ **then**
7 | **if** $P_1 = \Omega_1$ **then return** $(0, -1)$. **else if** $P_1 = \Omega_2$ **then return** $(0, 1)$.
8 | **else if** $P_1 = (0, -1)$ **then return** Ω_1. **else if** $P_1 = (0, 1)$ **then return** Ω_2.
9 | **else return** $(1/(\delta x_1), -y_1/(\delta x_1^2))$.
10 **else if** $x_1 y_2 - y_1 x_2 \neq 0$ **then**
11 | $x_3 \leftarrow (x_1^2 - x_2^2)/(x_1 y_2 - y_1 x_2)$.
12 | $y_3 \leftarrow ((x_1^2 + x_2^2)(y_1 y_2 - 2a x_1 x_2) - 2x_1 x_2(1 + d x_1^2 x_2^2))/(x_1 y_2 - y_1 x_2)^2$.
13 | **return** (x_3, y_3).
14 **else if** $1 - d x_1^2 x_2^2 \neq 0$ **then**
15 | $x_3 \leftarrow (x_1 y_2 + y_1 x_2)/(1 - d x_1^2 x_2^2)$.
16 | $y_3 \leftarrow ((y_1 y_2 + 2a x_1 x_2)(1 + d x_1^2 x_2^2) + 2d x_1 x_2 (x_1^2 + x_2^2))/(1 - d x_1^2 x_2^2)^2$.
17 | **return** (x_3, y_3).
18 **else**
19 | **if** $P_2 = (1/(\delta x_1), y_1/(\delta x_1^2))$ **then return** Ω_1.
20 | **else return** Ω_2.
21 **end**

The correctness of the algorithm follows from two observations. Firstly, when a point at infinity is involved as the sum or as one of the summands along the lines 2 to 21, it is tedious but straightforward to check that the output of the algorithm is correct using the *implicit* technique mentioned at the start of the section. Line 1 conditionally swaps the inputs to eliminate half of the input-wise symmetric branches. The second observation is that *glueing* together the unified addition and the dedicated addition formulae is enough to handle all exceptions when both of the summands and the sum are affine points. This fact follows from Lemma 4.5 and Lemma 4.2 by observing that $\#(S' \cap S) = 2$. This means that if $(x_2, y_2) \in S' \cap S$ then the output must be a point at infinity (lines 19 and 20) since there are exactly two points at infinity. The remaining exceptional cases which occur at $(x_2, y_2) \in S' \backslash (S' \cap S)$ are handled by the dedicated addition formulae (lines 11 and 12). Similarly the exceptions at $(x_2, y_2) \in S \backslash (S' \cap S)$ are handled by the unified addition formulae (lines 15 and 16).

Algorithm 4.9 complies with the completeness criterion since only the lines 15 to 17 are necessary in this case. Note that the assumption on the curve constant d limits the number of curves in extended Jacobi quartic form for which the unified addition formulae are complete.

Algorithm 4.9 also complies with Lemma 4.8. If P_1 and P_2 are points of odd order then only the lines 15 to 17 are necessary. This technique applies to all extended Jacobi quartic curves.

Algorithm 4.9 also complies with Lemma 4.4. If P_1 and P_2 are distinct points of odd order then only the lines 11 to 13 are necessary. This technique applies to all extended Jacobi quartic curves. The doubling formulae (4.1) and (4.2) are enough to handle the special case $P_1 = P_2$.

The negation formulae were previously noted as $-(x_1, y_1) = (-x_1, y_1)$ for an affine point (x_1, y_1). To complete the negation law, it is sufficient to note that $-\Omega_1 = \Omega_1$ and $-\Omega_2 = \Omega_2$.

Literature notes. Other results related to the affine formulae for extended Jacobi quartic form can be found in the literature. Some pointers are [28, 33, 43, 44]. The dedicated addition formulae presented in this section are essentially the same formulae used by Chudnovsky and Chudnovsky in [13, 4.10i, p. 418] with the minor detail that the formulae in this section are given in affine coordinates, the curve equation is $y^2 = dx^4 + 2ax^2 + 1$ rather than $y^2 = x^4 + a'x^2 + b'$, and the identity is the point $(0, 1)$ rather than a point at infinity. The choice of the identity element in this work matches with [11].

4.2 Twisted Edwards form

This section presents the group law on $E_{\mathbf{E},a,d}$ in affine coordinates. It also investigates the exceptional summands for each set of formulae and provides a complete addition algorithm for all twisted Edwards curves by properly handling an entire set of division-by-zero exceptions. In addition, practical ways of preventing these exceptions are explained.

Throughout this section, let $\mathbb{K}$ be a field of odd characteristic. Recall from Section 2 that a twisted Edwards curve is defined by

$$E_{\mathbf{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2$$

where $a, d \in \mathbb{K}$ with $ad(a - d) \neq 0$. Recall from Section 2 that the set of $\mathbb{K}$-rational points on the desingularization of $E_{\mathbf{E},a,d}$ is defined by

$$E_{\mathbf{E},a,d}(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid ax^2 + y^2 = 1 + dx^2y^2\} \cup \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$$

where $\Omega_1, \Omega_2, \Omega_3, \Omega_4$ are points at infinity.

Identity element and negation. The identity element is $(0, 1)$. Let (x_1, y_1) be a point on $E_{\mathbf{E},a,d}$. The negative of (x_1, y_1) is $(-x_1, y_1)$.

Doubling. The doubling formulae on $E_{\mathbf{E},a,d}$ are given by $[2](x_1, y_1) = (x_3, y_3)$ where

$$x_3 = 2x_1y_1/\big(y_1^2 + ax_1^2\big), \tag{4.8}$$

$$y_3 = \big(y_1^2 - ax_1^2\big)/\big(2 - y_1^2 - ax_1^2\big) \tag{4.9}$$

assuming that $(2 - y_1^2 - ax_1^2)(y_1^2 + ax_1^2) \neq 0$, see [3] (also see [4, 5, 8]). These formulae do not depend on the curve constant d and are of minimal total degree. By the curve equation the denominator $y_1^2 + ax_1^2$ is equivalent to $1 + dx_1^2y_1^2$. Similarly, the denominator $2 - y_1^2 - ax_1^2$ is equivalent to $1 - dx_1^2y_1^2$. These denominators can also be used if the total degree is not of concern.

The point $(0, -1)$ is of order 2 which can be determined by solving $ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $(x_3, y_3) = (0, 1)$ for x_1 and y_1 where x_3 and y_3 are given by (4.8) and (4.9). There are three points of order 2 in total (over a sufficiently large finite extension of $\mathbb{K}$). Therefore, two of the points at infinity have to be of order 2. See also [3]. Ω_1 and Ω_2 are taken to be of order 2 hereafter.

The two points of the form $(x, 0)$ are of order 4 which can be determined by solving $ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $(x_3, y_3) = (0, -1)$ for x_1 and y_1 where x_3 and y_3 are given by (4.8) and (4.9). There are twelve points of order 4 in total (over a sufficiently large finite extension of $\mathbb{K}$). Eight of these points can be explicitly determined to be affine points by solving $ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $(2 - y_1^2 - ax_1^2)(y_1^2 + ax_1^2) = 0$ for x_1 and y_1. Therefore, the remaining two points of order 4 have to be the points at infinity Ω_3 and Ω_4. See also [3]. The doubles of the eight points are either Ω_1 or Ω_2. The doubles of Ω_3 and Ω_4 are $(0, -1)$. These points are the only exceptions of (4.8) and (4.9). The following remark is immediate.

Remark 4.10. $[2](x_1, y_1)$ is a point at infinity if and only if

$$(2 - y_1^2 - ax_1^2)(y_1^2 + ax_1^2) = 0.$$

Remark 4.10 does not extend to the case of generic additions. However, it is still useful in proving some lemmas regarding the generic addition formulae which will be presented next.

Dedicated addition. Further let (x_2, y_2) be a point on $E_{\mathbf{E},a,d}$. The addition formulae on $E_{\mathbf{E},a,d}$ are given by $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ where

$$x_3 = \big(x_1y_1 + x_2y_2\big)\big/\big(y_1y_2 + ax_1x_2\big), \tag{4.10}$$

$$y_3 = \big(x_1y_1 - x_2y_2\big)\big/\big(x_1y_2 - y_1x_2\big) \tag{4.11}$$

assuming that $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) \neq 0$. These formulae are of minimal total degree. These formulae do not work for identical summands hence the name *dedicated*.

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 0$. Otherwise, $(x_1, y_1) + (x_2, y_2)$ would be an affine point since it can be shown using the relations $ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$ that the algebraic expressions for (x_3, y_3) satisfy $ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$. The converse, however, does not necessarily apply. This means that if $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 0$ then $(x_1, y_1) + (x_2, y_2)$ may not be a point at infinity. Therefore it is worth investigating the exceptional cases. The denominators of (4.10) and (4.11) vanish for some summands which are described in the following lemma explicitly.

Lemma 4.11. *Let $a, d \in \mathbb{K}$ with $ad(a - d) \neq 0$. Fix $\alpha, \delta \in \mathbb{K}$ so that $\alpha^2 = a$ and $\delta^2 = d$. Fix $x_1, y_1, x_2, y_2 \in \mathbb{K}\backslash\{0\}$ such that $ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$. Now, $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 0$ if and only if $(x_2, y_2) \in S$ where*

$$S = \Big[(x_1, y_1), (-x_1, -y_1), \Big(\frac{y_1}{\alpha}, -x_1\alpha\Big), \Big(\frac{-y_1}{\alpha}, x_1\alpha\Big), \\ \Big(\frac{1}{\delta y_1}, \frac{1}{\delta x_1}\Big), \Big(\frac{-1}{\delta y_1}, \frac{-1}{\delta x_1}\Big), \Big(\frac{1}{\alpha\delta x_1}, \frac{-\alpha}{\delta y_1}\Big), \Big(\frac{-1}{\alpha\delta x_1}, \frac{\alpha}{\delta y_1}\Big)\Big].$$

Proof. $\Rightarrow$: Assume that $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 0$. Solving the equations $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 0$ and $ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$ simultaneously for x_2 and y_2 gives S. All entries in S are defined since $x_1y_1 \neq 0$.

$\Leftarrow$: The claims follow trivially by substitution. □

The following lemma shows that if one of the summands is of odd order then in the presence of an exception, the other summand is always of even order.

Lemma 4.12. *Let a, d, x_1, y_1, x_2, y_2 be defined as in Lemma* 4.11. *Assume that $P_1 = (x_1, y_1)$ is a fixed point of odd order. Assume that $P_2 \in S\backslash\{P_1\}$. Then P_2 is of even order.*

Proof. In [8] (where $a = 1$) and later in [3], it is proven that the points at infinity (over the extension of $\mathbb{K}$ where they exist) are of even order. Assume that $P_1 = (x_1, y_1)$ is a fixed point of odd order hence not a point at infinity. Suppose that P_2 is of odd order hence not a point at infinity. It follows that $P_1 \pm P_2$, $M = 2P_1$, and $N = 2P_2$ are all of odd order hence not points at infinity.

Assume that $P_2 \in S\backslash\{P_1\}$. So, $P_1 \neq P_2$. Plus, $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 0$ by Lemma 4.11. It follows that $P_1 \neq -P_2$, for otherwise we have $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 2x_1y_1(y_1^2 - ax_1^2) = 0$ which means that $y_1^2 - ax_1^2 = 0$ since $x_1, y_1 \neq 0$. Using this relation, the doubling formulae simplify to $(x_3, y_3) = (x_1/y_1, 0/(2 - 2y_1^2))$. The output x_3 is defined since $x_1y_1 \neq 0$. Whenever $0/(2 - 2y_1^2)$ is defined, it produces a point of order 4. But then P_1 would be of even order (in particular of order 8). If $y_1 = \pm 1$ then $0/(2 - 2y_1^2)$ is not defined. However these cases can be omitted since $x_1 \neq 0$ and the only points with $y_1 = \pm 1$ require x_1 to be zero.

Now,

- in the case $y_1y_2 + ax_1x_2 = 0$, the expression $x_2 = -y_1y_2/(ax_1)$ is defined since $x_1 \neq 0$ by definition. Using this relation together with (4.8) and the curve equation gives

$$x(N) = \frac{2x_2y_2}{y_1^2 + ax_1^2} = \frac{2\frac{-y_1y_2}{ax_1}y_2}{y_2^2 + a(\frac{-y_1y_2}{ax_1})^2} = -\frac{2x_1y_1}{y_1^2 + ax_1^2} = -x(M);$$

- in the case $x_1y_2 - y_1x_2 = 0$, the expression $y_2 = y_1x_2/x_1$ is defined since $x_1 \neq 0$ by definition. Using this relation together with (4.8) and the curve equation gives

$$x(N) = \frac{2x_2y_2}{y_2^2 + ax_2^2} = \frac{2x_2\frac{y_1x_2}{x_1}}{(\frac{y_1x_2}{x_1})^2 + ax_2^2} = \frac{2x_1y_1}{y_1^2 + ax_1^2} = x(M).$$

By the curve definition, $y(M) = \pm y(N)$ since $|x(M)| = |x(N)|$. Now,

- $x(M) = x(N)$ and $y(M) = y(N)$:
  $M - N = (0, 1)$. So, $M - N = 2P_1 - 2P_2 = 2(P_1 - P_2) = (0, 1)$.
- $x(M) = x(N)$ and $y(M) = -y(N)$:
  $M + N = (0, -1)$. So, $2(M + N) = 2(2P_1 + 2P_2) = 4(P_1 + P_2) = (0, 1)$.
- $x(M) = -x(N)$ and $y(M) = y(N)$:
  $M + N = (0, 1)$. So, $M + N = 2P_1 + 2P_2 = 2(P_1 + P_2) = (0, 1)$.
- $x(M) = -x(N)$ and $y(M) = -y(N)$:
  $M - N = (0, -1)$. So, $2(M - N) = 2(2P_1 - 2P_2) = 4(P_1 - P_2) = (0, 1)$.

Since $P_1 \neq \pm P_2$, in all cases $P_1 \pm P_2$ is of even order, contradiction. In conclusion, $P_2 \in S \backslash \{P_1\}$ is of even order because P_1 is of odd order. □

A practical solution is now provided to prevent the exceptional cases of (4.10) and (4.11).

Lemma 4.13. *Let $\mathbb{K}$ be a field of odd characteristic. Let $E_{\mathbf{E},a,d}$ be a twisted Edwards curve defined over $\mathbb{K}$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E_{\mathbf{E},a,d}$. Assume that P_1 and P_2 are of odd order with $P_1 \neq P_2$. It follows that $y_1y_2 + ax_1x_2 \neq 0$ and $x_1y_2 - y_1x_2 \neq 0$.*

Proof. Assume that P_1 and P_2 are of odd order with $P_1 \neq P_2$. Suppose that $x_1 = 0$ and $x_2 = 0$. Then, either $P_1 = P_2 = (0, 1)$ or $P_1 = (0, -1)$ or $P_2 = (0, -1)$, both are contradictions. So, either $x_1 \neq 0$ or $x_2 \neq 0$. Suppose that $y_1y_2 = 0$. Then, either P_1 or P_2 is of even order, contradiction. So, $y_1y_2 \neq 0$. Therefore, either $x_1y_1 \neq 0$ or $x_2y_2 \neq 0$. The claim then follows from Lemma 4.11 and Lemma 4.12 (by swapping P_1 and P_2 when necessary). □

Unified addition. Alternative addition formulae on $E_{\mathbf{E},a,d}$ are given by $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ where

$$x_3 = \big(x_1y_2 + y_1x_2\big)\big/\big(1 + dx_1y_1x_2y_2\big), \tag{4.12}$$

$$y_3 = \big(y_1y_2 - ax_1x_2\big)\big/\big(1 - dx_1y_1x_2y_2\big) \tag{4.13}$$

assuming $(1 - dx_1y_1x_2y_2)(1 + dx_1y_1x_2y_2) \neq 0$, see [3]. These formulae work for identical summands in most of the cases hence the name *unified*.

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then we have

$$(1 - dx_1y_1x_2y_2)(1 + dx_1y_1x_2y_2) = 0.$$

Otherwise, $(x_1, y_1)+(x_2, y_2)$ would be an affine point by [8, Theorem 3.1] and by the remark in [3, § 6] stating that $E_{\mathbf{E},a,d}$ is isomorphic to $E_{\mathbf{E},1,d/a}$. The converse, however, does not necessarily apply. This means that if $(1 - dx_1y_1x_2y_2)(1 + dx_1y_1x_2y_2) = 0$ then $(x_1, y_1)+(x_2, y_2)$ may not be a point at infinity. Therefore it is worth investigating the exceptional cases. The denominators of (4.12) and (4.13) vanish for some summands which are described in the following lemma explicitly.

Lemma 4.14. *Let $a, d \in \mathbb{K}$ with $ad(a - d) \neq 0$. Fix $\alpha, \delta \in \mathbb{K}$ so that $\alpha^2 = a$ and $\delta^2 = d$. Fix $x_1, y_1, x_2, y_2 \in \mathbb{K}\backslash\{0\}$ such that $ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and*

$ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$. *It follows that* $dx_1y_1x_2y_2 \in \{1, -1\}$ *if and only if* $(x_2, y_2) \in S'$ *where*

$$S' = \Big[\Big(\frac{1}{\delta y_1}, \frac{-1}{\delta x_1}\Big), \Big(\frac{-1}{\delta y_1}, \frac{1}{\delta x_1}\Big), \Big(\frac{1}{\alpha\delta x_1}, \frac{\alpha}{\delta y_1}\Big), \Big(\frac{-1}{\alpha\delta x_1}, \frac{-\alpha}{\delta y_1}\Big),$$
$$\Big(\frac{1}{\delta y_1}, \frac{1}{\delta x_1}\Big), \Big(\frac{-1}{\delta y_1}, \frac{-1}{\delta x_1}\Big), \Big(\frac{1}{\alpha\delta x_1}, \frac{-\alpha}{\delta y_1}\Big), \Big(\frac{-1}{\alpha\delta x_1}, \frac{\alpha}{\delta y_1}\Big)\Big].$$

Proof. $\Rightarrow$: Assume that $(1 - dx_1y_1x_2y_2)(1 + dx_1y_1x_2y_2) = 0$. Solving the equations $(1 - dx_1y_1x_2y_2)(1 + dx_1y_1x_2y_2) = 0$ and $ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$ simultaneously for x_2 and y_2 gives S'. All entries in S' are defined since $x_1y_1 \neq 0$.

$\Leftarrow$: The claims follow trivially by substitution. □

This lemma and Lemma 4.11 exclude $x_1y_1 = 0$. For $x_1y_1 = 0$ the denominators in (4.12) and (4.13) are defined and equal to 1.

The following lemma shows that if one of the summands is of odd order then in the presence of a vanished denominator, the other summand is always of even order.

Lemma 4.15. *Let* a, d, x_1, y_1, x_2, y_2 *be defined as in Lemma* 4.14. *Assume that* $P_1 = (x_1, y_1)$ *is a fixed point of odd order. Assume that* $P_2 = (x_2, y_2) \in S'$. *Then,* P_2 *is of even order.*

Proof. In [8] (where $a = 1$) and later in [3], it is proven that the points at infinity (over the extension of $\mathbb{K}$ where they exist) are of even order. Assume that $P_1 = (x_1, y_1)$ is a fixed point of odd order hence not a point at infinity. Suppose that P_2 is of odd order hence not a point at infinity. It follows that $P_1 \pm P_2$, $M = 2P_1$, and $N = 2P_2$ are all of odd order hence not points at infinity.

Assume that $P_2 \in S'$. Then, $dx_1y_1x_2y_2 \in \{1, -1\}$ by Lemma 4.14 and it follows that $P_1 \neq \pm P_2$, for otherwise, $dx_1^2y_1^2 \in \{1, -1\}$ and P_1 would be of even order, see Remark 4.10.

Note that $x_1, y_1 \neq 0$ since $dx_1y_1x_2y_2 \in \{1, -1\}$ (also true by definition). So, $x_2y_2 = \pm 1/(dx_1y_1)$ are defined taking the signs independently. Using this relation together with (4.12) gives

$$x(N) = \frac{2x_2y_2}{1 + dx_2^2y_2^2} = \frac{2\frac{\pm 1}{dx_1y_1}}{1 + d(\frac{\pm 1}{dx_1y_1})^2} = \pm\frac{2x_1y_1}{1 + dx_1^2y_1^2} = \pm x(M).$$

By the curve definition, $y(M) = \pm y(N)$ since $|x(M)| = |x(N)|$. Now,

- $x(M) = x(N)$ and $y(M) = y(N)$:
  $M - N = (0, 1)$. So, $M - N = 2P_1 - 2P_2 = 2(P_1 - P_2) = (0, 1)$.

- $x(M) = x(N)$ and $y(M) = -y(N)$:
  $M + N = (0, -1)$. So, $2(M + N) = 2(2P_1 + 2P_2) = 4(P_1 + P_2) = (0, 1)$.
- $x(M) = -x(N)$ and $y(M) = y(N)$:
  $M + N = (0, 1)$. So, $M + N = 2P_1 + 2P_2 = 2(P_1 + P_2) = (0, 1)$.
- $x(M) = -x(N)$ and $y(M) = -y(N)$:
  $M - N = (0, -1)$. So, $2(M - N) = 2(2P_1 - 2P_2) = 4(P_1 - P_2) = (0, 1)$.

Since $P_1 \neq \pm P_2$, in all cases $P_1 \pm P_2$ is of even order, contradiction. In conclusion, $P_2 \in S'$ is of even order because P_1 is of odd order. □

The points at infinity on the desingularized projective closure of $E_{\mathbf{E},a,d}$ are not defined over $\mathbb{K}$ if d is not a square in $\mathbb{K}$ and a is a square in $\mathbb{K}$, see [3]. Having noted this, it was proven in [8] (where $a = 1$) and later in [3] that the unified addition formulae (4.12) and (4.13) are complete provided that d is not a square in $\mathbb{K}$ and a is a square in $\mathbb{K}$.

In the following lemma, with reasonable assumptions, it is shown that exceptions can be prevented regardless of any assumption on the curve constants.

Lemma 4.16. *Let $\mathbb{K}$ be a field of odd characteristic. Let $E_{\mathbf{E},a,d}$ be a twisted Edwards curve defined over $\mathbb{K}$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E_{\mathbf{E},a,d}$. Assume that P_1 and P_2 are points on $E_{\mathbf{E},a,d}$ of odd order. It follows that $1 \pm dx_1x_2y_1y_2 \neq 0$.*

Proof. Assume that P_1 and P_2 are points of odd order. If $x_1y_1x_2y_2 = 0$ then $1 \pm dx_1y_1x_2y_2 \neq 0$ as desired. If $x_1y_1x_2y_2 \neq 0$ then the claim follows from Lemma 4.14 and Lemma 4.15 (by swapping P_1 and P_2 when necessary). □

Exception handling in the general case. Algorithm 4.17 provides a complete addition on all twisted Edwards curves.

The correctness of the algorithm follows from two observations. Firstly, when a point at infinity is involved as the sum or as one of the summands along the lines 2 to 39, it is tedious but straightforward to check that the output of the algorithm is correct using the *implicit* technique mentioned at the start of the section. Line 1 conditionally swaps the inputs to eliminate half of the input-wise symmetric branches. The second observation is that *glueing* together the unified addition and the dedicated addition formulae is enough to handle all exceptions when both of the summands and the sum are affine points. This fact follows from Lemma 4.14 and Lemma 4.11 by observing that $\#(S' \cap S) = 4$. This means that if $(x_2, y_2) \in S' \cap S$ then the output must be a point at infinity (lines 35 to 38) since there are exactly four points at infinity. The remaining exceptional cases which

Algorithm 4.17. Addition law in affine coordinates for twisted Edwards form

Input : $P_1, P_2, \Omega_1, \Omega_2, \Omega_3, \Omega_4 \in E_{\mathbf{E},a,d}(\mathbb{K})$ and fixed $\alpha, \delta \in \mathbb{K}$ such that $\alpha^2 = a$ and $\delta^2 = d$.

Output : $P_1 + P_2$.

if $P_1 \in \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$ **then** $P_t \leftarrow P_1$, $P_1 \leftarrow P_2$, $P_2 \leftarrow P_t$.
if $P_2 = \Omega_1$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,-1)$.
  else if $P_1 = \Omega_3$ **then return** $(-1/\alpha, 0)$. **else if** $P_1 = \Omega_4$ **then return** $(1/\alpha, 0)$.
  else if $P_1 = (0,1)$ **then return** Ω_1. **else if** $P_1 = (0,-1)$ **then return** Ω_2.
  else if $P_1 = (-1/\alpha, 0)$ **then return** Ω_3. **else if** $P_1 = (1/\alpha, 0)$ **then return** Ω_4.
  else return $(-1/(\alpha\delta x_1), -\alpha/(\delta y_1))$.
else if $P_2 = \Omega_2$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,-1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,1)$.
  else if $P_1 = \Omega_3$ **then return** $(1/\alpha, 0)$. **else if** $P_1 = \Omega_4$ **then return** $(-1/\alpha, 0)$.
  else if $P_1 = (0,-1)$ **then return** Ω_1. **else if** $P_1 = (0,1)$ **then return** Ω_2.
  else if $P_1 = (1/\alpha, 0)$ **then return** Ω_3. **else if** $P_1 = (-1/\alpha, 0)$ **then return** Ω_4.
  else return $(1/(\alpha\delta x_1), \alpha/(\delta y_1))$.
else if $P_2 = \Omega_3$ **then**
  if $P_1 = \Omega_1$ **then return** $(-1/\alpha, 0)$. **else if** $P_1 = \Omega_2$ **then return** $(1/\alpha, 0)$.
  else if $P_1 = \Omega_3$ **then return** $(0,-1)$. **else if** $P_1 = \Omega_4$ **then return** $(0,1)$.
  else if $P_1 = (1/\alpha, 0)$ **then return** Ω_1. **else if** $P_1 = (-1/\alpha, 0)$ **then return** Ω_2.
  else if $P_1 = (0,1)$ **then return** Ω_3. **else if** $P_1 = (0,-1)$ **then return** Ω_4.
  else return $(1/(\delta y_1), -1/(\delta x_1))$.
else if $P_2 = \Omega_4$ **then**
  if $P_1 = \Omega_1$ **then return** $(1/\alpha, 0)$. **else if** $P_1 = \Omega_2$ **then return** $(-1/\alpha, 0)$.
  else if $P_1 = \Omega_3$ **then return** $(0,1)$. **else if** $P_1 = \Omega_4$ **then return** $(0,-1)$.
  else if $P_1 = (-1/\alpha, 0)$ **then return** Ω_1. **else if** $P_1 = (1/\alpha, 0)$ **then return** Ω_2.
  else if $P_1 = (0,-1)$ **then return** Ω_3. **else if** $P_1 = (0,1)$ **then return** Ω_4.
  else return $(-1/(\delta y_1), 1/(\delta x_1))$.
else if $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) \neq 0$ **then**
  $x_3 \leftarrow (x_1y_1 + x_2y_2)/(y_1y_2 + ax_1x_2)$.
  $y_3 \leftarrow (x_1y_1 - x_2y_2)/(x_1y_2 - y_1x_2)$.
  return (x_3, y_3).
else if $(1 - dx_1x_2y_1y_2)(1 + dx_1x_2y_1y_2) \neq 0$ **then**
  $x_3 \leftarrow (x_1y_2 + y_1x_2)/(1 + dx_1x_2y_1y_2)$.
  $y_3 \leftarrow (y_1y_2 - ax_1x_2)/(1 - dx_1x_2y_1y_2)$.
  return (x_3, y_3).
else
  if $P_2 = (1/(\alpha\delta x_1), -\alpha/(\delta y_1))$ **then return** Ω_1.
  else if $P_2 = (-1/(\alpha\delta x_1), \alpha/(\delta y_1))$ **then return** Ω_2.
  else if $P_2 = (1/(\delta y_1), 1/(\delta x_1))$ **then return** Ω_3.
  else return Ω_4.
end

occur at $(x_2, y_2) \in S' \backslash (S' \cap S)$ are handled by the dedicated addition formulae (lines 27 and 28). Similarly the exceptions at $(x_2, y_2) \in S - (S' \cap S)$ are handled by the unified addition formulae (lines 31 and 32).

Algorithm 4.17 complies with the completeness criterion since only the lines 31 to 33 are necessary in this case. Note that the assumptions on the curve constants a and d limit the number of curves in twisted Edwards form for which the unified addition formulae are complete. In [3] such curves are named *complete Edwards curves*.

Algorithm 4.17 also complies with Lemma 4.16. If P_1 and P_2 are points of odd order only the lines 31 to 33 are necessary. This technique applies to all twisted Edwards curves.

Algorithm 4.17 also complies with Lemma 4.13. If P_1 and P_2 are distinct points of odd order then only the lines 27 to 29 are necessary. This technique applies to all twisted Edwards curves. The doubling formulae (4.8) and (4.9) are enough to handle the special case $P_1 = P_2$.

The negation formulae were previously noted as $-(x_1, y_1) = (-x_1, y_1)$ for an affine point (x_1, y_1). To complete the negation law, it is sufficient to note that $-\Omega_1 = \Omega_1, -\Omega_2 = \Omega_2, -\Omega_3 = \Omega_4$, and $-\Omega_4 = \Omega_3$.

Literature notes. Other results related to the affine formulae for twisted Edwards curves can be found in the literature. Bernstein et al. used Edwards curves (i.e. $a = 1$) in the ECM method of integer factorization in [5]. Bernstein et al. introduced the shape $d_1(x + y) + d_2(x^2 + y^2) = (x + x^2)(y + y^2)$ and presented results on the arithmetic of these curves when $\mathrm{char}(\mathbb{K}) = 2$ in [10]. These curve are named binary Edwards curves. In chronological order, Das and Sarkar ([18]), Ionica and Joux ([27]), and Arène et al. ([2]) introduced successively faster formulae for pairing computations. The results in [18, 27] are based on the unified addition formulae and the doubling formulae with $a = 1$. The results in [2] are based on the dedicated addition formulae and the doubling formulae. The same reference also provided a geometric interpretation of the group law on twisted Edwards curves. Bernstein and Lange introduced in [9] a complete addition law on an arbitrary twisted Edwards curve by embedding the curve into $\mathbb{P}^1 \times \mathbb{P}^1$. Their method achieve exactly the same goal of this section but using only two set of incomplete formulae. The trade-off between the proposals is the number of the coordinates used. Their method uses four coordinates where the proposed one requires only two resulting in more branches to handle special cases. Algorithm 4.17 agrees with the addition law in [9]. Point additions involving points at infinity can also be checked from [9] which also includes a self-contained proof.

4.3 Twisted Jacobi intersection form

This section presents the group law on $E_{\mathbf{I},b,a}$ in affine coordinates. It also investigates the exceptional summands for each set of formulae and provides a complete addition algorithm for all twisted Jacobi intersection curves by properly handling an entire set of division-by-zero exceptions. In addition, practical ways of preventing these exceptions are explained.

Throughout this section, let $\mathbb{K}$ be a field of odd characteristic. Recall from Section 2 that a twisted Jacobi intersection curve is defined by

$$E_{\mathbf{I},b,a} : bs^2 + c^2 = 1, \;\; as^2 + d^2 = 1$$

where $a, b \in \mathbb{K}$ with $ab(a-b) \neq 0$. Recall from Section 2 that the set of $\mathbb{K}$-rational points on $E_{\mathbf{I},b,a}$ is defined by

$$E_{\mathbf{I},b,a}(\mathbb{K}) = \{(s,c,d) \in \mathbb{K}^3 \mid bs^2 + c^2 = 1, as^2 + d^2 = 1\} \cup \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$$

where $\Omega_1, \Omega_2, \Omega_3, \Omega_4$ are points at infinity.

Identity element and negation. The identity element is $(0,1,1)$. Let (s_1, c_1, d_1) be a point on $E_{\mathbf{I},b,a}$. The negative of (s_1, c_1, d_1) is $(-s_1, c_1, d_1)$.

Doubling. The doubling formulae on $E_{\mathbf{I},b,a}$ is given by $[2](s_1, c_1, d_1) = (s_3, c_3, d_3)$ where

$$s_3 = 2s_1c_1d_1/\big(c_1^2 + bs_1^2d_1^2\big), \tag{4.14}$$

$$c_3 = \big(c_1^2 - bs_1^2d_1^2\big)/\big(c_1^2 + bs_1^2d_1^2\big), \tag{4.15}$$

$$d_3 = \big(2d_1^2 - c_1^2 - bs_1^2d_1^2\big)/\big(c_1^2 + bs_1^2d_1^2\big). \tag{4.16}$$

assuming that $c_1^2 + bs_1^2d_1^2 \neq 0$. These formulae are of minimal total degree and do not depend on the curve constants a and b. By the curve equation the denominator $c_1^2 + bs_1^2d_1^2$ is equivalent to $1 - abs_1^4$ or $c_1^2 + d_1^2 - c_1^2d_1^2$ or $d_1^2 + as_1^2c_1^2$. These denominators can also be used.

The points $(0,-1,1)$, $(0,1,-1)$, and $(0,-1,-1)$ are of order 2. This can be determined by solving $bs_1^2 + c_1^2 = 1, as_1^2 + d_1^2 = 1$ and $(s_3, c_3, d_3) = (0,1,1)$ for s_1, c_1, and d_1 where s_3, c_3, and d_3 are given by (4.14), (4.15), and (4.16).

The four points of the form having the c-coordinates equal to zero are of order 4. This can be determined by solving $bs_1^2 + c_1^2 = 1, as_1^2 + d_1^2 = 1$ and $(s_3, c_3, d_3) = (0,-1,1)$ for s_1, c_1, and d_1. Another set of four points having the d-coordinates equal to zero are also of order 4. This can be determined by solving $bs_1^2 + c_1^2 = 1$,

$as_1^2 + d_1^2 = 1$ and $(s_3, c_3, d_3) = (0, 1, -1)$ for s_1, c_1, and d_1. There are twelve points of order 4 in total (over a sufficiently large finite extension of $\mathbb{K}$). Therefore the remaining four points of order 4 have to be the points at infinity Ω_1, Ω_2, Ω_3, and Ω_4. These points are the only exceptions of (4.14), (4.15), and (4.16). The following remark is immediate.

Remark 4.18. [2](s_1, c_1, d_1) is a point at infinity if and only if $c_1^2 + bs_1^2 d_1^2 = 0$.

Remark 4.18 does not extend to the case of generic additions. However, it is still useful in proving some lemmas regarding the generic addition formulae which will be presented next.

Dedicated addition. Further let (s_2, c_2, d_2) be a point on $E_{\mathbf{I},b,a}$. The addition formulae on $E_{\mathbf{I},b,a}$ are given by $(s_1, c_1, d_1) + (s_2, c_2, d_2) = (s_3, c_3, d_3)$ where

$$s_3 = \big(s_1^2 - s_2^2\big)\big/\big(s_1c_2d_2 - c_1d_1s_2\big), \tag{4.17}$$

$$c_3 = \big(s_1c_1d_2 - d_1s_2c_2\big)\big/\big(s_1c_2d_2 - c_1d_1s_2\big), \tag{4.18}$$

$$d_3 = \big(s_1d_1c_2 - c_1s_2d_2\big)\big/\big(s_1c_2d_2 - c_1d_1s_2\big) \tag{4.19}$$

assuming that $s_1c_2d_2 - c_1d_1s_2 \neq 0$. These formulae are of minimal total degree and do not depend on the curve constants a and b. These formulae do not work for identical summands hence the name *dedicated*.

If $(s_1, c_1, d_1) + (s_2, c_2, d_2)$ is a point at infinity then $s_1c_2d_2 - c_1d_1s_2 = 0$. Otherwise, $(s_1, c_1, d_1) + (s_2, c_2, d_2)$ would be an affine point since it can be shown using the relations $bs_1^2 + c_1^2 = 1, as_1^2 + d_1^2 = 1$ and $bs_2^2 + c_2^2 = 1, as_2^2 + d_2^2 = 1$ that the algebraic expressions for (s_3, c_3, d_3) satisfy $bs_3^2 + c_3^2 = 1, as_3^2 + d_3^2 = 1$. The converse, however, does not necessarily apply. This means that if $s_1c_2d_2 - c_1d_1s_2 = 0$ then $(s_1, c_1, d_1) + (s_2, c_2, d_2)$ may not be a point at infinity. Therefore it is worth investigating the exceptional cases. The denominators of (4.17), (4.18), and (4.19) vanish for some summands which are described in the following lemma explicitly.

Lemma 4.19. *Let $a, b \in \mathbb{K}$ with $ab(a - b) \neq 0$. Fix $\alpha, \beta \in \mathbb{K}$ so that $\alpha^2 = -a$ and $\beta^2 = -b$. Fix $s_1, s_2 \in \mathbb{K}\backslash\{0\}$ and $c_1, d_1, c_2, d_2 \in \mathbb{K}$ such that $bs_1^2 + c_1^2 = 1$, $as_1^2 + d_1^2 = 1$, $bs_2^2 + c_2^2 = 1$, and $as_2^2 + d_2^2 = 1$. Now, $s_1c_2d_2 - c_1d_1s_2 = 0$ if and only if $(s_2, c_2, d_2) \in S$ where*

$$S = \Big[(s_1, c_1, d_1), (s_1, -c_1, -d_1), (-s_1, -c_1, d_1), (-s_1, c_1, -d_1),$$

$$\Big(\frac{1}{\alpha\beta s_1}, \frac{d_1}{\alpha s_1}, \frac{c_1}{\beta s_1}\Big), \Big(\frac{1}{\alpha\beta s_1}, \frac{-d_1}{\alpha s_1}, \frac{-c_1}{\beta s_1}\Big), \Big(\frac{-1}{\alpha\beta s_1}, \frac{-d_1}{\alpha s_1}, \frac{c_1}{\beta s_1}\Big), \Big(\frac{-1}{\alpha\beta s_1}, \frac{d_1}{\alpha s_1}, \frac{-c_1}{\beta s_1}\Big)\Big].$$

Proof. $\Rightarrow$: Assume that $s_1c_2d_2 - c_1d_1s_2 = 0$. Solving the equations $s_1c_2d_2 - c_1d_1s_2 = 0$, $bs_2^2 + c_2^2 = 1$ and $as_2^2 + d_2^2 = 1$ simultaneously for s_2, c_2, and d_2 gives S. All entries in S are defined since $s_1 \neq 0$.

$\Leftarrow$: The claims follow trivially by substitution. □

The following lemma shows that if one of the summands is of odd order then in the presence of an exception, the other summand is always of even order.

Lemma 4.20. *Let $a, b, s_1, c_1, d_1, s_2, c_2, d_2$ be defined as in Lemma* 4.19. *Assume that $P_1 = (s_1, c_1, d_1)$ is a fixed point of odd order. Assume that $P_2 \in S\backslash\{P_1\}$. Then P_2 is of even order.*

Proof. Note that points at infinity (over the extension of $\mathbb{K}$ where they exist) are of even order. Assume that $P_1 = (s_1, c_1, d_1)$ is a fixed point of odd order hence not a point at infinity. Suppose that P_2 is of odd order hence not a point at infinity. It follows that $P_1 \pm P_2$, $M = 2P_1$, and $N = 2P_2$ are all of odd order hence not points at infinity.

Assume that $P_2 \in S\backslash\{P_1\}$. So, $P_1 \neq P_2$. Plus, $s_1c_2d_2 - c_1d_1s_2 = 0$ by Lemma 4.19. It follows that $P_1 \neq -P_2$, for otherwise, $s_1c_2d_2 - c_1d_1s_2 = 2s_1c_1d_1 = 0$ which means that $c_1d_1 = 0$ since $s_1 \neq 0$. But then P_1 would be of even order.

It is possible to continue in a similar way used in the previous sections however this time computer algebra will be used. The following Maple script verifies that $s(M)^2 = s(N)^2$, $c(M)^2 = c(N)^2$, and $d(M)^2 = d(N)^2$.

```
> Q:=(s,c,d)->(b*s^2+c^2-1,a*s^2+d^2-1):
> sM:=2*s1*c1*d1/(c1^2+b*s1^2*d1^2): cM:=(c1^2-b*s1^2*d1^2)/(c1^2+b*s1^2*d1^2):
> dM:=(2*d1^2-c1^2-b*s1^2*d1^2)/(c1^2+b*s1^2*d1^2):
> sN:=2*s2*c2*d2/(c2^2+b*s2^2*d2^2): cN:=(c2^2-b*s2^2*d2^2)/(c2^2+b*s2^2*d2^2):
> dN:=(2*d2^2-c2^2-b*s2^2*d2^2)/(c2^2+b*s2^2*d2^2): simplify([sM^2-sN^2,cM^2-cN^2,
> dM^2-dN^2],[s1*c2*d2-c1*d1*s2=0,Q(s1,c1,d1),Q(s2,c2,d2)]);
[0,0,0]
```

Therefore, $s(M) = \pm s(N)$, $c(M) = \pm c(N)$, and $d(M) = \pm d(N)$. Now,

- $s(M) = \pm s(N)$, $c(M) = c(N)$, $d(M) = d(N)$:
  $M \mp N = (0, 1, 1)$. So, $M \mp N = 2P_1 \mp 2P_2 = 2(P_1 \mp P_2) = (0, 1, 1)$;
- $s(M) = \pm s(N)$, $c(M) = -c(N)$, $d(M) = d(N)$:
  $M \pm N = (0, -1, 1)$. So, $2(M \pm N) = 2(2P_1 \pm 2P_2) = 4(P_1 \pm P_2) = (0, 1, 1)$;
- $s(M) = \pm s(N)$, $c(M) = c(N)$, $d(M) = -d(N)$:
  $M \pm N = (0, 1, -1)$. So, $2(M \pm N) = 2(2P_1 \pm 2P_2) = 4(P_1 \pm P_2) = (0, 1, 1)$;

- $s(M) = \pm s(N), c(M) = -c(N), d(M) = -d(N)$:
  $M \mp N = (0, -1, -1)$. So, $2(M \mp N) = 2(2P_1 \mp 2P_2) = 4(P_1 \mp P_2) = (0, 1, 1)$.

Since $P_1 \neq \pm P_2$, in all cases $P_1 \pm P_2$ is of even order, contradiction. In conclusion, $P_2 \in S \backslash \{P_1\}$ is of even order because P_1 is of odd order. □

A practical solution is now provided to prevent the exceptional cases of (4.17), (4.18), and (4.19).

Lemma 4.21. *Let $\mathbb{K}$ be a field of odd characteristic. Let $E_{\mathbf{I},b,a}$ be a twisted Jacobi intersection curve defined over $\mathbb{K}$. Let $P_1 = (s_1, c_1, d_1)$ and $P_2 = (s_2, c_2, d_2)$ be points on $E_{\mathbf{I},b,a}$. Assume that P_1 and P_2 are of odd order with $P_1 \neq P_2$. It follows that $s_1c_2d_2 - c_1d_1s_2 \neq 0$.*

Proof. Assume that P_1 and P_2 are of odd order with $P_1 \neq P_2$. Suppose that $s_1 = 0$ and $s_2 = 0$. Then, $P_1 = P_2 = (0, 1, 1)$, contradiction. So, either $s_1 \neq 0$ or $s_2 \neq 0$. Suppose that $s_1 \neq 0$ and $s_2 = 0$ or $s_1 = 0$ and $s_2 \neq 0$ then the claim follows trivially. Now, $s_1s_2 \neq 0$. The claim then follows from Lemma 4.19 and Lemma 4.20 (by swapping P_1 and P_2 when necessary). □

Unified addition. Alternative addition formulae on $E_{\mathbf{I},b,a}$ are given by $(s_1, c_1, d_1) + (s_2, c_2, d_2) = (s_3, c_3, d_3)$ where

$$s_3 = \big(s_1c_2d_2 + c_1d_1s_2\big)\big/\big(1 - abs_1^2s_2^2\big), \tag{4.20}$$

$$c_3 = \big(c_1c_2 - bs_1d_1s_2d_2\big)\big/\big(1 - abs_1^2s_2^2\big), \tag{4.21}$$

$$d_3 = \big(d_1d_2 - as_1c_1s_2c_2\big)\big/\big(1 - abs_1^2s_2^2\big) \tag{4.22}$$

assuming that $1 - abs_1^2s_2^2 \neq 0$. These formulae work for identical summands in most of the cases hence the name *unified*.

If $(s_1, c_1, d_1)+(s_2, c_2, d_2)$ is a point at infinity then $1-abs_1^2s_2^2 = 0$. Otherwise, $(s_1, c_1, d_1) + (s_2, c_2, d_2)$ would be an affine point since it can be shown using the relations $bs_1^2 + c_1^2 = 1, as_1^2 + d_1^2 = 1$ and $bs_2^2 + c_2^2 = 1, as_2^2 + d_2^2 = 1$ that the algebraic expressions for (s_3, c_3, d_3) satisfy $bs_3^2 + c_3^2 = 1, as_3^2 + d_3^2 = 1$. The converse, however, does not necessarily apply. This means that if $1 - abs_1^2s_2^2 = 0$ then $(s_1, c_1, d_1) + (s_2, c_2, d_2)$ may not be a point at infinity. Therefore it is worth investigating the exceptional cases. The denominators of (4.20), (4.21), and (4.22) vanish for some summands which are described in the following lemma explicitly.

Lemma 4.22. *Let $a, b, s_1, c_1, d_1, s_2, c_2, d_2$ be defined as in Lemma* 4.19*. It follows that $1 - abs_1^2 s_2^2 \neq 0$ if and only if $(s_2, c_2, d_2) \in S'$ where*

$$S' = \Big[\Big(\frac{1}{\alpha\beta s_1}, \frac{-d_1}{\alpha s_1}, \frac{c_1}{\beta s_1}\Big), \Big(\frac{1}{\alpha\beta s_1}, \frac{d_1}{\alpha s_1}, \frac{-c_1}{\beta s_1}\Big), \Big(\frac{-1}{\alpha\beta s_1}, \frac{d_1}{\alpha s_1}, \frac{c_1}{\beta s_1}\Big),$$
$$\Big(\frac{-1}{\alpha\beta s_1}, \frac{-d_1}{\alpha s_1}, \frac{-c_1}{\beta s_1}\Big), \Big(\frac{1}{\alpha\beta s_1}, \frac{d_1}{\alpha s_1}, \frac{c_1}{\beta s_1}\Big), \Big(\frac{1}{\alpha\beta s_1}, \frac{-d_1}{\alpha s_1}, \frac{-c_1}{\beta s_1}\Big),$$
$$\Big(\frac{-1}{\alpha\beta s_1}, \frac{-d_1}{\alpha s_1}, \frac{c_1}{\beta s_1}\Big), \Big(\frac{-1}{\alpha\beta s_1}, \frac{d_1}{\alpha s_1}, \frac{-c_1}{\beta s_1}\Big)\Big].$$

Proof. $\Rightarrow$: Assume that $1 - abs_1^2 s_2^2 = 0$. Solving the equations $1 - abs_1^2 s_2^2 = 0$, $bs_2^2 + c_2^2 = 1$, and $as_2^2 + d_2^2 = 1$ simultaneously for s_2, c_2, and d_2 gives S'. All entries in S' are defined since $s_1 \neq 0$.

$\Leftarrow$: The claims follow trivially by substitution. □

This lemma and Lemma 4.19 exclude $s_1 = 0$. For $s_1 = 0$ the denominators in (4.20), (4.21) and (4.22) are defined and equal to 1.

The following lemma shows that if one of the summands is of odd order then in the presence of a vanished denominator, the other summand is always of even order.

Lemma 4.23. *Let $a, b, s_1, c_1, d_1, s_2, c_2, d_2$ be defined as in Lemma* 4.22*. Assume that $P_1 = (s_1, c_1, d_1)$ is a fixed point of odd order and that $P_2 = (s_2, c_2, d_2) \in S'$. Then, P_2 is of even order.*

Proof. The proof is similar to the proof of Lemma 4.20. The only difference is that the expression `s1*c2*d2-c1*d1*s2=0` should be changed to `1-a*b*s1*s1*s2*s2=0` in the Maple script and the claim follows. □

The points at infinity on the projective closure of $E_{\mathbf{I},b,a}$ are not defined over $\mathbb{K}$ if a is not a square in $\mathbb{K}$. Having noted this, the following lemma implies that these addition formulae are complete if a is not a square in $\mathbb{K}$.

Lemma 4.24. *Let $a, b, s_1, s_2 \in \mathbb{K}$. Assume that ab is non-square. Then*

$$1 - abs_1^2 s_2^2 \neq 0.$$

Proof. See the proof of Lemma 4.7 in Section 4.1. □

In the following lemma, with reasonable assumptions, it is shown that exceptions can be prevented regardless of any assumption on the curve constants.

Lemma 4.25. *Let $\mathbb{K}$ be a field of odd characteristic. Let $E_{\mathbf{I},b,a}$ be a twisted Jacobi intersection curve defined over $\mathbb{K}$. Let $P_1 = (s_1, c_1, d_1)$ and $P_2 = (s_2, c_2, d_2)$ be points on $E_{\mathbf{I},b,a}$. Assume that P_1 and P_2 are of odd order. It follows that $1 - abs_1^2 s_2^2 \neq 0$.*

Proof. Assume that P_1 and P_2 are of odd order. If $s_1 s_2 = 0$ then $1 - abs_1^2 s_2^2 \neq 0$ as desired. If $s_1 s_2 \neq 0$ then the claim follows from Lemma 4.22 and Lemma 4.23 (by swapping P_1 and P_2 when necessary). □

Exception handling in the general case. Algorithm 4.26 provides a complete addition on all twisted Jacobi intersection curves.

The correctness of the algorithm follows from two observations. Firstly, when a point at infinity is involved as the sum or as one of the summands along lines 2 to 41, it is tedious but straightforward to check that the output of the algorithm is correct using the *implicit* technique mentioned at the start of the section. Line 1 conditionally swaps the inputs to eliminate half of the input-wise symmetric branches. The second observation is that *glueing* together the unified addition and the dedicated addition formulae is enough to handle all exceptions when both of the summands and the sum are affine points. This fact follows from Lemma 4.22 and Lemma 4.19 by observing that $\#(S' \cap S) = 4$. This means that if $(s_2, c_2, d_2) \in S' \cap S$ then the output must be a point at infinity (lines 37 to 40) since there are exactly four points at infinity. The remaining exceptional cases which occur at $(s_2, c_2, d_2) \in S' \backslash (S' \cap S)$ are handled by the dedicated addition formulae (lines 27 to 30). Similarly the exceptions at $(s_2, c_2, d_2) \in S \backslash (S' \cap S)$ are handled by the unified addition formulae (lines 32 to 34).

Algorithm 4.26 complies with the completeness criterion since only the lines 32 to 35 are necessary in this case. Note that the assumption on the curve constants a and b limits the number of curves in twisted Jacobi intersection form for which the unified addition formulae are complete.

Algorithm 4.26 also complies with Lemma 4.25. If P_1 and P_2 are points of odd order then all branches are eliminated and the lines 32 to 35 suffice. This technique applies to all twisted Jacobi intersection curves.

Algorithm 4.26 also complies with Lemma 4.21. If P_1 and P_2 are distinct points of odd order then all branches are eliminated and the lines 27 to 30 suffice. This technique applies to all twisted Jacobi intersection curves. The doubling formulae (4.14), (4.15) and (4.16) are enough to handle the special case $P_1 = P_2$.

The negation formulae were previously noted as $-(s_1, c_1, d_1) = (-s_1, c_1, d_1)$ for an affine point (s_1, c_1, d_1). To complete the negation law, it is sufficient to note that $-\Omega_1 = \Omega_4$, $-\Omega_4 = \Omega_1$, $-\Omega_2 = \Omega_3$, and $-\Omega_3 = \Omega_2$.

Algorithm 4.26. Addition law in affine coordinates for twisted Jacobi intersection form

Input : $P_1, P_2, \Omega_1, \Omega_2, \Omega_3, \Omega_4 \in E_{\mathbf{I},b,a}(\mathbb{K})$ and fixed $\alpha, \beta \in \mathbb{K}$ such that $\alpha^2 = -a$ and $\beta^2 = -b$.

Output : $P_1 + P_2$.

if $P_1 \in \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$ **then** $P_t \leftarrow P_1$, $P_1 \leftarrow P_2$, $P_2 \leftarrow P_t$.
if $P_2 = \Omega_1$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,-1,-1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,-1,1)$.
  else if $P_1 = \Omega_3$ **then return** $(0,1,-1)$. **else if** $P_1 = \Omega_4$ **then return** $(0,1,1)$.
  else if $P_1 = (0,1,1)$ **then return** Ω_1. **else if** $P_1 = (0,1,-1)$ **then return** Ω_2.
  else if $P_1 = (0,-1,1)$ **then return** Ω_3. **else if** $P_1 = (0,-1,-1)$ **then return** Ω_4.
  else return $(-1/(\alpha\beta s_1), d_1/(\alpha s_1), c_1/(\beta s_1))$.
else if $P_2 = \Omega_2$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,-1,1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,-1,-1)$.
  else if $P_1 = \Omega_3$ **then return** $(0,1,1)$. **else if** $P_1 = \Omega_4$ **then return** $(0,1,-1)$.
  else if $P_1 = (0,1,-1)$ **then return** Ω_1. **else if** $P_1 = (0,1,1)$ **then return** Ω_2.
  else if $P_1 = (0,-1,-1)$ **then return** Ω_3. **else if** $P_1 = (0,-1,1)$ **then return** Ω_4.
  else return $(1/(\alpha\beta s_1), d_1/(\alpha s_1), -c_1/(\beta s_1))$.
else if $P_2 = \Omega_3$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,1,-1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,1,1)$.
  else if $P_1 = \Omega_3$ **then return** $(0,-1,-1)$. **else if** $P_1 = \Omega_4$ **then return** $(0,-1,1)$.
  else if $P_1 = (0,-1,1)$ **then return** Ω_1. **else if** $P_1 = (0,-1,-1)$ **then return** Ω_2.
  else if $P_1 = (0,1,1)$ **then return** Ω_3. **else if** $P_1 = (0,1,-1)$ **then return** Ω_4.
  else return $(1/(\alpha\beta s_1), -d_1/(\alpha s_1), c_1/(\beta s_1))$.
else if $P_2 = \Omega_4$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,1,1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,1,-1)$.
  else if $P_1 = \Omega_3$ **then return** $(0,-1,1)$. **else if** $P_1 = \Omega_4$ **then return** $(0,-1,-1)$.
  else if $P_1 = (0,-1,-1)$ **then return** Ω_1. **else if** $P_1 = (0,-1,1)$ **then return** Ω_2.
  else if $P_1 = (0,1,-1)$ **then return** Ω_3. **else if** $P_1 = (0,1,1)$ **then return** Ω_4.
  else return $(-1/(\alpha\beta s_1), -d_1/(\alpha s_1), -c_1/(\beta s_1))$.
else if $s_1c_2d_2 - c_1d_1s_2 \neq 0$ **then**
  $s_3 \leftarrow (s_1^2 - s_2^2)/(s_1c_2d_2 - c_1d_1s_2)$.
  $c_3 \leftarrow (s_1c_1d_2 - d_1s_2c_2)/(s_1c_2d_2 - c_1d_1s_2)$.
  $d_3 \leftarrow (s_1d_1c_2 - c_1s_2d_2)/(s_1c_2d_2 - c_1d_1s_2)$.
  return (s_3, c_3, d_3).
else if $1 - abs_1^2s_2^2 \neq 0$ **then**
  $s_3 \leftarrow (s_1c_2d_2 + c_1d_1s_2)/(1 - abs_1^2s_2^2)$.
  $c_3 \leftarrow (c_1c_2 - bs_1d_1s_2d_2)/(1 - abs_1^2s_2^2)$.
  $d_3 \leftarrow (d_1d_2 - as_1c_1s_2c_2)/(1 - abs_1^2s_2^2)$.
  return (s_3, c_3, d_3).
else
  if $P_2 = (1/(\alpha\beta s_1), -d_1/(\alpha s_1), -c_1/(\beta s_1))$ **then return** Ω_1.
  else if $P_2 = (-1/(\alpha\beta s_1), -d_1/(\alpha s_1), c_1/(\beta s_1))$ **then return** Ω_2.
  else if $P_2 = (-1/(\alpha\beta s_1), d_1/(\alpha s_1), -c_1/(\beta s_1))$ **then return** Ω_3.
  else return Ω_4.
end

Literature notes. Other results related to the affine formulae for twisted Jacobi intersection form can be found in the literature. The group law on Jacobi intersection curves are typically derived directly from Jacobi elliptic functions, cf. [11, 13, 28, 43].

5 Conclusion

This paper has focused on the group law on elliptic curves. In this context, an automated method of finding cryptographically interesting point addition formulae is described. Three forms of elliptic curves are revisited and many missed low-degree formulae are detected. With these new formulae a complete description of the group law is made in affine coordinates.

Section 2 reviewed the elliptic curve group law on Weierstrass curves together with definitions of frequently used technical terms. Birational equivalences between selected curves and suitable Weierstrass curves were demonstrated using literature results and computer algebra. Section 2 also compared the estimated coverage of each studied form of elliptic curves.

Section 3 brought together several computational tools using fundamental results in algebraic geometry: the Riemann–Roch theorem and products of curves, and in arithmetic of function fields: Gröbner basis computations and rational simplifications. The final product is a toolbox for optimizing the group law arising from elliptic curves given in some particular form. The first tool is capable of finding group laws on elliptic curves using computer algebra. This is a high-level tool which produces massive and inefficient formulae. This tool uses birational maps between curves and symbolically deduces the group law for some form of an elliptic curve. The second tool is responsible for rational simplification for finding lowest-degree point addition/doubling formulae. The notion of finding the lowest-degree rational expression modulo a prime ideal was developed in [36]. To the best of the authors' knowledge, combining these two stages and systematically finding the *lowest-degree* group laws is an outcome of this paper and of the authors' previous works in [24–26].

Section 4 presented low-degree point addition formulae, some of which are outcomes of this paper. The new formulae include dedicated addition formulae for extended Jacobi quartic ((4.3), (4.4)), twisted Edwards ((4.10), (4.11)), and twisted Jacobi intersection forms ((4.17), (4.18), (4.19)) and a set of minimal-degree doubling formulae for extended Jacobi quartic form ((4.1), (4.2)). Each of these new formulae have a lower total degree than original formulae presented in the literature. A complete statement of the group law in affine coordinates was presented for each of the studied forms. These complete descriptions in affine coordinates

cannot be found in the literature. The algorithms contributed are Algorithm 4.9 in Section 4.1, Algorithm 4.17 in Section 4.2, and Algorithm 4.26 in Section 4.3. In order to justify these algorithms each section contains a series of lemmas to systematically investigate exceptional situations that might appear in the computation. All of the proposed algorithms contain several conditional branches. In an optimized implementation these branches are best eliminated. This is achieved with two methods. The first method was initiated by Bernstein and Lange in [8] for Edwards curves and was extended to suitable classes of elliptic curves in twisted Edwards form in [3] and to twisted Hessian form in [6]. This technique forces the point(s) at infinity to be defined over a proper extension of $\mathbb{K}$ but not defined over $\mathbb{K}$. Therefore, all points on the selected curve are affine points. The rest of the method is composed of finding a single set of addition formulae with a denominator which cannot vanish for any pair of summands. This section has extended the same idea for suitable classes of elliptic curves in extended Jacobi quartic and twisted Jacobi intersection forms, see Section 4.1 and 4.3 respectively. The second method selects a suitable subgroup of points which does not contain any points at infinity. The rest of the method is again composed of finding a single set of addition formulae with denominators which cannot vanish for any pair of summands. Using this method, it was shown how to prevent all exceptions of dedicated addition formulae for distinct inputs. This latter contribution is perfectly suited to the context of fast scalar multiplications, since dedicated additions are more efficient than unified additions in almost all cases.

Acknowledgments. The authors wish to thank the referees for corrections and helpful suggestions.

Bibliography

[1] W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, 1996.

[2] C. Arène, T. Lange, M. Naehrig and C. Ritzenthaler, *Faster pairing computation*, Cryptology ePrint Archive, 2009, `http://eprint.iacr.org/2009/155`. To appear in Journal of Number Theory.

[3] D. J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, *Twisted Edwards Curves*, AFRICACRYPT 2008, LNCS 5023, pp. 389–405, Springer, 2008.

[4] D. J. Bernstein, P. Birkner, T. Lange and C. Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, INDOCRYPT 2007, LNCS 4859, pp. 167–182, Springer, 2007.

[5] D. J. Bernstein, P. Birkner, T. Lange and C. Peters, *ECM using Edwards curves*, Cryptology ePrint Archive, Report 2008/016, 2008, `http://eprint.iacr.org/`.

[6] D. J. Bernstein, D. Kohel and T. Lange, *Twisted Hessian curves*, Explicit-Formulas Database, 2009, `www.hyperelliptic.org/EFD/g1p/auto-twistedhessian.html`.

[7] D. J. Bernstein and T. Lange, *Explicit-formulas database*, 2007, `www.hyperelliptic.org/EFD`.

[8] D. J. Bernstein and T. Lange, *Faster addition and doubling on elliptic curves*, ASIACRYPT 2007, LNCS 4833, pp. 29–50. Springer, 2007.

[9] D. J. Bernstein and T. Lange, *A complete set of addition lawsfor incomplete Edwards curves*, Cryptology ePrint Archive, 2009, `http://eprint.iacr.org/2009/580`. To appear in Journal of Number Theory.

[10] D. J. Bernstein, T. Lange and R. Rezaeian Farashahi, *Binary Edwards Curves*, CHES 2008, LNCS 5154, pp. 244–265, Springer, 2008.

[11] O. Billet and M. Joye, *The Jacobi Model of an Elliptic Curve and Side-Channel Analysis*, AAECC-15, LNCS 2643, pp. 34–42, Springer, 2003.

[12] W. Castryck and F. Vercauteren, *Toric forms of elliptic curves and their arithmetic*, preprint, 2009.

[13] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Mathematics 7 (1986), pp. 385–434.

[14] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer, New York, 1993.

[15] H. Cohen and G. Frey (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, 2005.

[16] H. Cohen, A. Miyaji and T. Ono, *Efficient Elliptic Curve Exponentiation Using Mixed Coordinates*, ASIACRYPT'98, LNCS 1514, pp. 51–65, Springer, 1998.

[17] D. A. Cox, J. B. Little and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, 3rd ed., Springer, 2007.

[18] M. P. Das and P. Sarkar, *Pairing computation on twisted Edwards form elliptic curves*, Pairing'08, Lecture Notes in Mathematics 5209, pp. 192–210, Springer, 2008.

[19] W. Decker and C. Lossen, *Computing in Algebraic Geometry, A Quick Start using SINGULAR*, Algorithms and Computation in Mathematics 16, Springer, Berlin, Heidelberg, 2006.

[20] H. M. Edwards, *A Normal Form for Elliptic Curves*, Bulletin of the AMS 44 (2007), pp. 393–422.

[21] W. Fulton, *An introduction to algebraic geometry*, A. W. Benjamin Publishing Company, New York, 1969.

[22] G. M. Greuel, G. Pfister and H. Schönemann, SINGULAR *3-1-0 – A computer algebra system for polynomial computations*, 2009, `www.singular.uni-kl.de`.

[23] D. Hankerson, A. J. Menezes and S. A. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, New York, 2003.

[24] H. Hisil, K. K. Wong, G. Carter and E. Dawson, *Twisted Edwards Curves Revisited*. ASIACRYPT 2008, LNCS 5350, pp. 326–343, Springer, 2008.

[25] H. Hisil, K. K. Wong, G. Carter and E. Dawson, *Faster Group Operations on Elliptic Curves*, Australasian Information Security Conference (AISC 2009), Wellington, New Zealand, January 2009, 98, pp. 7–19. Conferences in Research and Practice in Information Technology (CRPIT), 2009.

[26] H. Hisil, K. K. Wong, G. Carter and E. Dawson, *Jacobi quartic curves revisited*, ACISP 2009, LNCS 5594, pp. 452–468, Springer, 2009.

[27] S. Ionica and A. Joux, *Another approach to pairing computation in Edwards coordinates*, Cryptology ePrint Archive, 2008, `http://eprint.iacr.org/2008/292`.

[28] C. G. J. Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, Sumtibus Fratrum Borntræger, 1829.

[29] M. Joye and J. J. Quisquater, *Hessian Elliptic Curves and Side-Channel Attacks*, CHES 2001 2162, LNCS Generators, pp. 402–410, Springer, 2001.

[30] N. Koblitz, *Elliptic Curve Cryptosystems*, Mathematics of Computation 48 (1987), pp. 203–209.

[31] H. W. Lenstra, *Factoring Integers with Elliptic Curves*, The Annals of Mathematics 126 (1987), pp. 649–673.

[32] P. Y. Liardet and N. P. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form*, CHES 2001, LNCS 2162, pp. 391–401, Springer, 2001.

[33] H. McKean and V. Moll, *Elliptic Curves: Function Theory, Geometry, Arithmetic*, Cambridge University Press, 1999.

[34] V. S. Miller, *Use of elliptic curves in cryptography*, CRYPTO'85, LNCS 218, pp. 417–426, Springer, 1986.

[35] *Maple 12*, Waterloo Maple Inc., 2008, `www.maplesoft.com/`.

[36] M. Monagan and R. Pearce, *Rational simplification modulo a polynomial ideal*, ISSAC'06, pp. 239–245, ACM, 2006.

[37] C. Musili, *Algebraic Geometry for Beginners*, Texts and Readings in Mathematics 20, Hindustan Book Agency, 2001.

[38] R. Pearce, *Rational expression simplification with side relations*, Master Thesis, Simon Fraser University, 2005.

[39] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer, 1st ed. 1986, corr. 3rd printing 1994.

[40] J. H. Silverman and J. Suzuki, *Elliptic Curve Discrete Logarithms and the Index Calculus*, ASIACRYPT'98, LNCS, Springer, 1998.

[41] M. van Hoeij, *An algorithm for computing the Weierstrass normal form*, ISSAC '95: International symposium on symbolic and algebraic computation, pp. 90–95, ACM, 2003.

[42] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, 2003.

[43] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge University Press, 1927.

[44] N. Yui, *Jacobi quartics, Legendre polynomials and formal groups*, Elliptic Curves and Modular Forms in Algebraic Topology, Lecture Notes in Mathematics 1326, pp. 182–215, Springer, 1988.

Received September 4, 2010; revised March 3, 2011.

Author information

Huseyin Hisil, Information Security Institute, Australia.
E-mail: h.hisil@qut.edu.au

Kenneth Koon-Ho Wong, Information Security Institute, Australia.
E-mail: kk.wong@qut.edu.au

Gary Carter, Information Security Institute, Australia.
E-mail: g.carter@qut.edu.au

Ed Dawson, Information Security Institute, Australia.
E-mail: e.dawson@qut.edu.au