Binary Edwards Curves

Daniel J. Bernstein[1], Tanja Lange[2], and Reza Rezaeian Farashahi[2,3]

[1] Department of Mathematics, Statistics, and Computer Science (M/C 249)
University of Illinois at Chicago, Chicago, IL 60607–7045, USA
djb@cr.yp.to
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
tanja@hyperelliptic.org, r.rezaeian@tue.nl
[3] Dept. of Mathematical Sciences, Isfahan University of Technology,
P.O. Box 85145 Isfahan, Iran

Abstract. This paper presents a new shape for ordinary elliptic curves over fields of characteristic 2. Using the new shape, this paper presents the first complete addition formulas for binary elliptic curves, i.e., addition formulas that work for all pairs of input points, with no exceptional cases. If $n \geq 3$ then the complete curves cover all isomorphism classes of ordinary elliptic curves over $\mathbf{F}_{2^n}$.

This paper also presents dedicated doubling formulas for these curves using $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$, where $\mathbf{M}$ is the cost of a field multiplication, $\mathbf{S}$ is the cost of a field squaring, and $\mathbf{D}$ is the cost of multiplying by a curve parameter. These doubling formulas are also the first complete doubling formulas in the literature, with no exceptions for the neutral element, points of order 2, etc.

Finally, this paper presents complete formulas for differential addition, i.e., addition of points with known difference. A differential addition and doubling, the basic step in a Montgomery ladder, uses $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ when the known difference is given in affine form.

Keywords: Elliptic curves, Edwards curves, binary fields, complete addition law, Montgomery ladder, countermeasures against side-channel attacks

1 Introduction

The points on a Weierstrass-form elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

* Permanent ID of this document: 592248bfa170d87d90a8d543cb645788. Date of this document: 2008.06.11. This work has been supported in part by the European Commission through the IST Programme under Contract IST–2002–507932 ECRYPT, in part by the National Science Foundation under grant ITR–0716498, and in part by the Ministry of Science, Research and Technology of I. R. Iran under scholarship no. 800.147.

include not only the affine points (x_1, y_1) satisfying the curve equation but also an extra point at infinity serving as the neutral element. The standard formulas to compute a sum $P + Q$ fail if P is at infinity, or if Q is at infinity, or if $P + Q$ is at infinity, or if P is equal to Q. Each of these possibilities needs to be tested for and handled separately; a complete addition *algorithm* is produced by gluing together several incomplete addition *formulas*.

This plethora of cases has caused a seemingly neverending string of problems for implementors of elliptic-curve cryptography, especially in cryptographic hardware subject to side-channel attacks. Consider, for example, computing $nP+mQ$. A typical two-scalar-multiplication algorithm would double P, add P, add Q, etc., where the exact pattern of additions and doublings depends on the values of n and m. What happens if $3P = Q$? Does the implementation take the time to see that $3P = Q$ and to switch from the addition formulas to doubling formulas? Can the attacker detect the switch through timing analysis, power analysis, etc.? If the implementation fails to check for $3P = Q$, what does it end up computing? What about $3P = -Q$? Can an attacker trigger failure cases—and incorrect computations—by choosing inputs cleverly? Can these failures compromise cryptographic security?

Some papers have presented "unified" addition formulas that can be used for doublings. See, e.g., [27], [18], [6], [3], and [5]; for overviews see [17], [25], and [2, Section 5]. "Strongly unified" addition formulas eliminate the need to check for equal inputs. However, they do not eliminate the need to check for inputs and outputs at infinity and for other exceptional cases. The exceptional-points attack presented in [16] targets the exceptional cases in these unified formulas.

Edwards curves. In the recent paper [2], Bernstein and Lange show for fields k with $\mathrm{char}(k) \neq 2$ that if d is not a square in k then the affine points on the "Edwards curve"

$$x^2 + y^2 = 1 + dx^2y^2$$

form a group. The affine addition law introduced by Edwards in [10] is complete for this curve, as are the fast projective formulas introduced in [2].

"Complete" is stronger than "unified": it means that the addition formulas work for *all* pairs of input points. There are no troublesome points at infinity. In particular, the neutral element of the curve is an affine point $(0, 1)$.

If k is finite then approximately $1/4$ of all elliptic curves over k are birationally equivalent to complete Edwards curves, i.e., Edwards curves with non-square d. The formulas in [2] can therefore be used for elliptic-curve computations, and in particular for elliptic-curve cryptography.

Implementors can—although they are not forced to!—gain speed by switching from the addition formulas to dedicated doubling formulas when the inputs are known to be equal. Bernstein and Lange show, for typical scalar-multiplication problems, that their addition formulas and doubling formulas for Edwards curves use fewer multiplications than the best available formulas for previous curve shapes.

Unfortunately, $x^2+y^2 = 1+dx^2y^2$ is not elliptic over fields k with $\mathrm{char}(k) = 2$.

Contributions of this paper. We introduce a new method of carrying out computations on binary elliptic curves, i.e., elliptic curves over fields k with $\mathrm{char}(k) = 2$. In particular, we introduce "complete binary Edwards curves." We present explicit formulas for addition on these curves, an explicit birational equivalence to an elliptic curve in short Weierstrass form, explicit formulas for doubling, and explicit formulas for Montgomery-type differential addition. See Section 2 for the curve shape and birational equivalence; Sections 3 and 5 for the addition law; Section 6 for doubling; and Section 7 for differential addition.

Our curve equation has a surprisingly large number of terms but shares many geometric features with non-binary Edwards curves $x^2 + y^2 = 1 + dx^2y^2$. In particular, we prove that our formulas are complete. We also show that if $n \geq 3$ then every ordinary elliptic curve over $\mathbf{F}_{2^n}$ is birationally equivalent to a complete binary Edwards curve. See Section 4.

Our doubling formulas and differential-addition formulas are extremely fast: for example, $2\mathbf{M} + 5\mathbf{S}$ for projective doubling, and $5\mathbf{M} + 4\mathbf{S}$ for one step of a Montgomery ladder, when curves are chosen to have small parameters. Here $\mathbf{M}$ is a field multiplication and $\mathbf{S}$ is a field squaring. For comparison, state-of-the-art formulas for small-parameter Weierstrass curves—the best formulas in the literature, and some new speedups that we present—use $2\mathbf{M} + 4\mathbf{S}$ for projective doubling and $5\mathbf{M}+4\mathbf{S}$ for one step of a Montgomery ladder. There is one caveat, namely that our general addition formulas use at best $16\mathbf{M}+1\mathbf{S}$ and are therefore not as fast as previous (incomplete) formulas; we can nevertheless recommend binary Edwards curves for a wide variety of applications.

2 Binary Edwards curves

In this section we introduce the new curve shape and show that the affine points are nonsingular. The points at infinity are singular; we give details on the blowup. To prove that the curve describes an elliptic curve we state a birational map to an ordinary elliptic curve in Weierstrass form.

Definition 2.1 (Binary Edwards curve). *Let k be a field with* $\mathrm{char}(k) = 2$. *Let d_1, d_2 be elements of k with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The* binary Edwards curve with coefficients d_1 and d_2 *is the affine curve*

$$\mathrm{E}_{\mathrm{B},d_1,d_2} : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2.$$

This curve is symmetric in x and y and thus has the property that if (x_1, y_1) is a point on the curve then so is (y_1, x_1). We will see in Section 3 that (y_1, x_1) is the negative of (x_1, y_1). The only curve points invariant under this negation law are $(0, 0)$ and $(1, 1)$; $(0, 0)$ will be the neutral element of the addition law while $(1, 1)$ will have order 2. We will also see that $(x_1, y_1) + (1, 1) = (x_1 + 1, y_1 + 1)$.

Theorem 2.2 (Nonsingularity). *Each binary Edwards curve is nonsingular.*

Proof. By definition the curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ has $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The partial derivatives of the curve equation are $d_1 + y + y^2$ and $d_1 + x + x^2$. A singular

point (x_1, y_1) must have $d_1 + y_1 + y_1^2 = 0$ and $d_1 + x_1 + x_1^2 = 0$, and therefore $(x_1 + y_1)^2 = x_1 + y_1$, implying $x_1 = y_1$ or $x_1 = y_1 + 1$.

The case $x_1 = y_1$ implies $0 = x_1^2 + x_1^4$ by the curve equation and therefore $d_1^2 = x_1^2 + x_1^4 = 0$, contradicting the hypothesis that $d_1 \neq 0$.

The case $x_1 = y_1 + 1$ implies $d_1 + d_2 = y_1^2 + y_1^4$ by the curve equation and therefore $d_1^2 = y_1^2 + y_1^4 = d_1 + d_2$, contradicting the hypothesis that $d_2 \neq d_1^2 + d_1$. □

Singularities of the projective closure. The projective closure of the curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ is

$$d_1(X + Y)Z^3 + d_2(X^2 + Y^2)Z^2 = XYZ^2 + XY(X + Y)Z + X^2Y^2.$$

It has the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ at infinity. Both are singular. We present details on the blowup for the first point; by the symmetry of the curve equation all considerations also hold for the second point.

To study the curve around $(1 : 0 : 0)$ we consider the affine curve $d_1(1 + y)z^3 + d_2(1 + y^2)z^2 = yz^2 + y(1 + y)z + y^2$. The partial derivatives $d_1z^3 + z^2 + z$ and $d_1(1 + y)z^2 + y(1 + y)$ both vanish in $(0, 0)$ which shows that the point is singular. We blow up the singularity by putting $y = tz$ and dividing by z^2, obtaining the curve

$$d_1(1 + tz)z + d_2(1 + t^2z^2) = tz + t(1 + tz) + t^2.$$

Substituting $z = 0$ produces the equation $d_2 + t + t^2 = 0$, which has two distinct roots in the algebraic closure of the base field k, corresponding to two distinct points of the blowup. These points are nonsingular since the partial derivative $d_1z^2 + z + 1$ does not vanish for $z = 0$. These blowups are defined over the smallest extension of k in which $d_2 + t + t^2 = 0$ has roots.

An alternate curve shape. The curve

$$d_1(1 + x + y) + d_2(1 + x^2 + y^2) = xy + xy(x + y) + x^2y^2$$

is isomorphic to $\mathrm{E}_{\mathrm{B},d_1,d_2}$ via the map $(x, y) \mapsto (x, y + 1)$, and is another suitable generalization of Edwards curves to the binary case. Since the addition and doubling formulas look slightly simpler on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ we picked that one but would like to point out here that all considerations also apply to this shifted curve.

Birational equivalence. Traditionally elliptic curves are given in Weierstrass form; see, e.g., [9]. An ordinary elliptic curve over k can be expressed in short Weierstrass form

$$v^2 + uv = u^3 + a_2u^2 + a_6$$

with $a_6 \neq 0$. The neutral element of the addition law is the point at infinity and negation is defined as $-(u_1, v_1) = (u_1, v_1 + u_1)$.

The map $(x, y) \mapsto (u, v)$ defined by

$$u = d_1(d_1^2 + d_1 + d_2)(x + y)/(xy + d_1(x + y)),$$
$$v = d_1(d_1^2 + d_1 + d_2)(x/(xy + d_1(x + y)) + d_1 + 1)$$

is a birational equivalence from $\mathrm{E}_{\mathrm{B},d_1,d_2}$ to the elliptic curve

$$v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + d_1^4(d_1^4 + d_1^2 + d_2^2)$$

with j-invariant $1/(d_1^4(d_1^4 + d_1^2 + d_2^2))$. An inverse map is given as follows:

$$x = d_1(u + d_1^2 + d_1 + d_2)/(u + v + (d_1^2 + d_1)(d_1^2 + d_1 + d_2)),$$
$$y = d_1(u + d_1^2 + d_1 + d_2)/(v + (d_1^2 + d_1)(d_1^2 + d_1 + d_2)).$$

We define a function φ on all affine points of $\mathrm{E}_{\mathrm{B},d_1,d_2}$ by extending the rational map $(x, y) \mapsto (u, v)$ given above. Specifically, the rational map is undefined at $(0, 0)$; we define $\varphi(0, 0) = P_\infty$. There are no other exceptional cases: if $xy + d_1(x + y) = 0$ then $d_2(x^2 + y^2) = xy(x + y) + x^2y^2 = d_1(x + y)^2 + d_1^2(x + y)^2$ so $(d_2 + d_1^2 + d_1)(x^2 + y^2) = 0$ so $x^2 + y^2 = 0$ so $x = y$. Use $xy + d_1(x + y) = 0$ again to see that $xy = 0$ so $x^2 = 0$ so $x = 0$ so $(x, y) = (0, 0)$.

3 The addition law

This section presents an addition law for the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ and proves that the addition law corresponds to the usual addition law on an elliptic curve in Weierstrass form. One consequence of the proof is that the addition law on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ is strongly unified: it can be used with two identical inputs, i.e., to double.

Here is the addition law. The sum of two points $(x_1, y_1), (x_2, y_2)$ on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ is the point (x_3, y_3) defined as follows:

$$x_3 = \frac{d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)},$$
$$y_3 = \frac{d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + (y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1x_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)}.$$

If the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero then the sum (x_3, y_3) is a point on $\mathrm{E}_{\mathrm{B},d_1,d_2}$: i.e., $d_1(x_3 + y_3) + d_2(x_3^2 + y_3^2) = x_3y_3 + x_3y_3(x_3 + y_3) + x_3^2y_3^2$. We present a script in the Sage computer-algebra system [34] that verifies this:

```
R.<d1,d2,x1,y1,x2,y2>=GF(2)[]
S=R.quotient([
  d1*(x1+y1)+d2*(x1^2+y1^2)+x1*y1+x1*y1*(x1+y1)+x1^2*y1^2,
  d1*(x2+y2)+d2*(x2^2+y2^2)+x2*y2+x2*y2*(x2+y2)+x2^2*y2^2
])
x3 = (
  d1*(x1+x2)+d2*(x1+y1)*(x2+y2)+(x1+x1^2)*(x2*(y1+y2+1)+y1*y2)
) / (d1+(x1+x1^2)*(x2+y2))
y3 = (
  d1*(y1+y2)+d2*(x1+y1)*(x2+y2)+(y1+y1^2)*(y2*(x1+x2+1)+x1*x2)
```

```
) / (d1+(y1+y1^2)*(x2+y2))
verif = d1*(x3+y3)+d2*(x3^2+y3^2)+x3*y3+x3*y3*(x3+y3)+x3^2*y3^2
0 == S(numerator(verif))
```

Inserting $(x_1, y_1) = (0, 0)$ or $(x_2, y_2) = (0, 0)$ into the addition law shows that $(0, 0)$ is the neutral element. Similarly $(x_1, y_1) + (1, 1) = (x_1 + 1, y_1 + 1)$; in particular $(1, 1) + (1, 1) = (0, 0)$. Furthermore $(x_1, y_1) + (y_1, x_1) = (0, 0)$, so $-(x_1, y_1) = (y_1, x_1)$. We emphasize that the addition law works without change for all of these inputs.

The following lemma will be useful in Section 7 and later in this section.

Lemma 3.1. *Let k be a field with $\mathrm{char}(k) = 2$. Let d_1, d_2 be elements of k with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_3, y_3), (x_2, y_2) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(k)$. Assume that $(x_3, y_3)+(x_2, y_2)$ is defined. Then $(x_3, y_3)+(y_2, x_2)$ is also defined. Furthermore define $(x_5, y_5) = (x_3, y_3) + (x_2, y_2)$ and $(x_1, y_1) = (x_3, y_3) + (y_2, x_2)$. Then $d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3) \neq 0$ and*

$$w_5 = \frac{d_1(d_1(w_2+w_3) + x_2x_3(x_2+x_3+1) + y_2y_3(y_2+y_3+1) + (x_2x_3+y_2y_3)^2)}{d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3)},$$
$$w_1w_5 = \frac{d_1^2(w_2 + w_3)^2}{d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3)},$$

where $w_i = x_i + y_i$.

Proof. The denominators of the coordinates of $(x_3, y_3) + (x_2, y_2)$ are $d_1 + (x_3 + x_3^2)(x_2 + y_2)$ and $d_1 + (y_3 + y_3^2)(x_2 + y_2)$; these formulas are symmetric in x_2, y_2, so they are the same as the denominators of $(x_3, y_3) + (y_2, x_2)$. Furthermore, their product is

$$\begin{aligned}
&(d_1 + (x_3 + x_3^2)(x_2 + y_2))(d_1 + (y_3 + y_3^2)(x_2 + y_2)) \\
&\quad = d_1^2 + d_1(x_3 + x_3^2 + y_3 + y_3^2)(x_2 + y_2) + (x_3 + x_3^2)(y_3 + y_3^2)(x_2 + y_2)^2 \\
&\quad = d_1^2 + d_1(w_3 + w_3^2)w_2 + (d_1w_3 + d_2w_3^2)w_2^2 \\
&\quad = d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3),
\end{aligned}$$

so $d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3)$ is nonzero. Note that we used the curve equation in the second-to-last equality.

Cross-multiplying and using the curve equation again gives the stated numerator of w_5; we omit the details. Similarly we obtain the numerator of w_1. Multiplying, using the curve equation again, and cancelling $d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3)$ produces the stated formula for w_1w_5. □

The rest of this section is devoted to the proof that this addition law corresponds to the addition law on the elliptic curve $v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + d_1^4(d_1^4 + d_1^2 + d_2^2)$ under the function φ defined in the previous section: i.e., that $\varphi(x_3, y_3) = \varphi(x_1, y_1) + \varphi(x_2, y_2)$.

Lemma 3.2. *Let k be a field with* $\mathrm{char}(k) = 2$. *Let d_1, d_2 be elements of k with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_2, y_2), (x_3, y_3) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(k)$. If $(x_3, y_3) + (x_2, y_2) = (0, 0)$ then $(x_3, y_3) = (y_2, x_2)$.*

Proof. Define w_i as in Lemma 3.1. Then $w_5 = 0$ so

$$d_1^2(w_2 + w_3)^2 = w_1 w_5(d_1^2 + w_2 w_3(d_1(1 + w_2 + w_3) + d_2 w_2 w_3)) = 0$$

so $w_2 + w_3 = 0$; i.e., $x_2 + y_2 + x_3 + y_3 = 0$. Similarly

$$d_1(d_1(w_2 + w_3) + x_2 x_3(x_2 + x_3 + 1) + y_2 y_3(y_2 + y_3 + 1) + (x_2 x_3 + y_2 y_3)^2) = 0$$

so $x_2 x_3(x_2 + x_3 + 1) + y_2 y_3(y_2 + y_3 + 1) + (x_2 x_3 + y_2 y_3)^2 = 0$. Substitute $y_3 = x_2 + y_2 + x_3$ to see that $x_2 x_3(x_2 + x_3 + 1) + y_2(x_2 + y_2 + x_3)(y_2 + (x_2 + y_2 + x_3) + 1) + (x_2 x_3 + y_2(x_2 + y_2 + x_3))^2 = 0$, and simplify to see that $(x_2 + y_2)(x_2 + y_2 + 1)(x_3 + y_2)(x_3 + y_2 + 1) = 0$. We now separately consider the four factors.

Case 1: $x_2 + y_2 = 0$. Then (x_2, y_2) is either $(0, 0)$ or $(1, 1)$. Furthermore $x_3 + y_3 = 0$ so (x_3, y_3) is either $(0, 0)$ or $(1, 1)$. We must have $(x_3, y_3) = (x_2, y_2)$ since $(0, 0) + (1, 1) \neq (0, 0)$. Thus also $(x_3, y_3) = (y_2, x_2)$.

Case 2: $x_2 + y_2 = 1$. Then $x_2^4 + x_2^2 = d_1 + d_2$ from the curve equation. Furthermore $x_3 + y_3 = 1$ so $x_3^4 + x_3^2 = d_1 + d_2$ so $x_3 = x_2$ or $x_3 = x_2 + 1$. If $x_3 = x_2$ then $(x_3, y_3) + (x_2, y_2) = (1, 1) \neq (0, 0)$. Thus $x_3 = x_2 + 1$ so $(x_3, y_3) = (x_2 + 1, x_2) = (y_2, x_2)$.

Case 3: $x_3 + y_2 = 0$. Then $x_2 + y_3 = 0$. Hence $(x_3, y_3) = (y_2, x_2)$.

Case 4: $x_3 + y_2 = 1$. Then $x_2 + y_3 = 1$. Hence $(x_3, y_3) + (x_2, y_2) = (y_2 + 1, x_2 + 1) + (x_2, y_2) = (1, 1)$, contradiction. □

Lemma 3.3. *Let k be a field with* $\mathrm{char}(k) = 2$. *Let d_1, d_2 be elements of k with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_1, y_1), (x_2, y_2) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(k)$. If $\varphi(x_1, y_1) = \varphi(x_2, y_2)$ then $(x_1, y_1) = (x_2, y_2)$.*

Proof. If $(x_1, y_1) = (0, 0)$ then $\varphi(x_1, y_1) = P_\infty$ so $\varphi(x_2, y_2) = P_\infty$ so $(x_2, y_2) = (0, 0) = (x_1, y_1)$ as claimed. Similar comments apply if $(x_2, y_2) = (0, 0)$. Assume from now on that $(x_1, y_1) \neq (0, 0)$ and $(x_2, y_2) \neq (0, 0)$.

By definition of φ we have

$$y_1(x_2 y_2 + d_1(x_2 + y_2)) = y_2(x_1 y_1 + d_1(x_1 + y_1)),$$
$$x_1(x_2 y_2 + d_1(x_2 + y_2)) = x_2(x_1 y_1 + d_1(x_1 + y_1)).$$

Note for future reference that this system of equations is symmetric between 1 and 2, and between x and y. Multiply the first equation by x_1 and the second by y_1 and add to obtain $(x_1 y_2 + x_2 y_1)(x_1 y_1 + d_1(x_1 + y_1)) = 0$. Recall that $x_1 y_1 + d_1(x_1 + y_1) \neq 0$ so $x_1 y_2 + x_2 y_1 = 0$. Now replace $x_1 y_2$ with $x_2 y_1$ in the second equation and simplify to obtain $x_2(x_1 + x_2) y_1 = 0$.

If $y_1 = 0$ then $x_1 \neq 0$. The curve equation now says $d_1 x_1 + d_2 x_1^2 = 0$ so $x_1 = d_1/d_2$. Furthermore $y_2 = x_2 y_1 / x_1 = 0$ so also $x_2 = d_1/d_2$ so $(x_1, y_1) = (x_2, y_2)$.

Assume from now on that $y_1 \neq 0$. Apply symmetry between 1 and 2, and between x and y, to obtain also $x_2 \neq 0$. Then $x_1 + x_2 = 0$. Apply symmetry between x and y to see that $y_1 + y_2 = 0$. Thus $(x_1, y_1) = (x_2, y_2)$. □

Lemma 3.4. *Let k be a field with* $\mathrm{char}(k) = 2$. *Let d_1, d_2 be elements of k with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_1, y_1) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(k)$. Then $\varphi(y_1, x_1) = -\varphi(x_1, y_1)$.*

Proof. If $(x_1, y_1) = (0, 0)$ then $\varphi(y_1, x_1) = P_\infty = \varphi(x_1, y_1)$. Assume from now on that $(x_1, y_1) \neq (0, 0)$. Write $(u_1, v_1) = \varphi(x_1, y_1)$ and $(u_2, v_2) = \varphi(y_1, x_1)$. Then $u_1 = u_2$ and $v_1 + v_2 = u_1$ from the definition of φ. Hence $(u_2, v_2) = (u_1, v_1 + u_1) = -(u_1, v_1)$. □

Theorem 3.5. *Let k be a field with* $\mathrm{char}(k) = 2$. *Let d_1, d_2 be elements of k with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(k)$. Assume that $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$. Then $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_3, y_3)$.*

Proof. Write $a_2 = d_1^2 + d_2$ and $a_6 = d_1^4(d_1^4 + d_1^2 + d_2^2)$. There are two cases in the definition of φ and several cases in the definition of addition on the Weierstrass curve $v^2 + uv = u^3 + a_2u^2 + a_6$; the proof splits into several cases correspondingly.

If $(x_1, y_1) = (0, 0)$ then $(x_2, y_2) = (x_3, y_3)$. Now $\varphi(x_2, y_2) = \varphi(x_3, y_3)$ and $\varphi(x_1, y_1) = P_\infty$, so $\varphi(x_1, y_1) + \varphi(x_2, y_2) = P_\infty + \varphi(x_2, y_2) = \varphi(x_2, y_2) = \varphi(x_3, y_3)$. Similar comments apply if $(x_2, y_2) = (0, 0)$.

If $(x_3, y_3) = (0, 0)$ then $(x_2, y_2) = (y_1, x_1)$ by Lemma 3.2. Now $\varphi(x_3, y_3) = \varphi(0, 0) = P_\infty$ and $\varphi(x_2, y_2) = \varphi(y_1, x_1) = -\varphi(x_1, y_1)$ by Lemma 3.4. Thus $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_1, y_1) - \varphi(x_1, y_1) = P_\infty = \varphi(x_3, y_3)$.

Assume from now on that $(x_1, y_1) \neq (0, 0)$, $(x_2, y_2) \neq (0, 0)$, and $(x_3, y_3) \neq (0, 0)$. Write $(u_i, v_i) = \varphi(x_i, y_i)$.

Case 1: $(u_1, v_1) = (u_2, v_2)$. Then $(x_1, y_1) = (x_2, y_2)$ by Lemma 3.3. If $u_1 = 0$ then $x_1 = y_1$ from the definition of φ so either $(x_1, y_1) = (0, 0)$ or $(x_1, y_1) = (1, 1)$; in either case $(x_1, y_1) + (x_2, y_2) = (x_1, y_1) + (x_1, y_1) = (0, 0)$, already handled above. Assume from now on that $u_1 \neq 0$. The usual doubling formulas for Weierstrass coordinates say that $2(u_1, v_1) = (u_4, v_4)$ where $u_4 = \lambda^2 + \lambda + d_1^2 + d_2$, $v_4 = v_1 + \lambda(u_1 + u_4) + u_4$, and $\lambda = (u_1^2 + v_1)/u_1$. A lengthy but straightforward calculation then shows that $(u_3, v_3) = (u_4, v_4)$; here is the corresponding Sage script:

```
R.<d1,d2,x1,y1>=GF(2)[]
S=R.quotient([
  d1*(x1+y1)+d2*(x1^2+y1^2)+x1*y1+x1*y1*(x1+y1)+x1^2*y1^2
])
x2 = x1
y2 = y1
x3 = (
  d1*(x1+x2)+d2*(x1+y1)*(x2+y2)+(x1+x1^2)*(x2*(y1+y2+1)+y1*y2)
) / (d1+(x1+x1^2)*(x2+y2))
y3 = (
  d1*(y1+y2)+d2*(x1+y1)*(x2+y2)+(y1+y1^2)*(y2*(x1+x2+1)+x1*x2)
) / (d1+(y1+y1^2)*(x2+y2))
u1 = d1*(d1^2+d1+d2)*(x1+y1)/(x1*y1+d1*(x1+y1))
v1 = d1*(d1^2+d1+d2)*(x1/(x1*y1+d1*(x1+y1))+d1+1)
u3 = d1*(d1^2+d1+d2)*(x3+y3)/(x3*y3+d1*(x3+y3))
```

```
v3 = d1*(d1^2+d1+d2)*(x3/(x3*y3+d1*(x3+y3))+d1+1)
lam = (u1^2+v1)/u1
u4 = lam^2+lam+d1^2+d2
v4 = v1+lam*(u1+u4)+u4
0 == S(numerator(u3-u4))
0 == S(numerator(v3-v4))
```

Hence $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_3, y_3)$.

Case 2: $(u_1, v_1) \neq (u_2, v_2)$. If $u_1 = u_2$ then $(u_1, v_1) = -(u_2, v_2)$ so $\varphi(x_1, y_1) = -\varphi(x_2, y_2) = \varphi(y_2, x_2)$ by Lemma 3.4 so $(x_1, y_1) = (y_2, x_2)$ by Lemma 3.3 so $(x_1, y_1)+(x_2, y_2) = (0, 0)$, already handled above. Assume from now on that $u_1 \neq u_2$. The usual addition formulas for Weierstrass coordinates say that $(u_1, v_1) + (u_2, v_2) = (u_4, v_4)$ where $u_4 = \lambda^2+\lambda+u_1+u_2+d_1^2+d_2$, $v_4 = v_1+\lambda(u_1+u_4)+u_4$, and $\lambda = (v_1 + v_2)/(u_1 + u_2)$. Another lengthy but straightforward calculation then shows that $(u_3, v_3) = (u_4, v_4)$; here is the corresponding Sage script:

```
R.<d1,d2,x1,y1,x2,y2>=GF(2)[]
S=R.quotient([
  d1*(x1+y1)+d2*(x1^2+y1^2)+x1*y1+x1*y1*(x1+y1)+x1^2*y1^2,
  d1*(x2+y2)+d2*(x2^2+y2^2)+x2*y2+x2*y2*(x2+y2)+x2^2*y2^2
])
x3 = (
  d1*(x1+x2)+d2*(x1+y1)*(x2+y2)+(x1+x1^2)*(x2*(y1+y2+1)+y1*y2)
) / (d1+(x1+x1^2)*(x2+y2))
y3 = (
  d1*(y1+y2)+d2*(x1+y1)*(x2+y2)+(y1+y1^2)*(y2*(x1+x2+1)+x1*x2)
) / (d1+(y1+y1^2)*(x2+y2))
u1 = d1*(d1^2+d1+d2)*(x1+y1)/(x1*y1+d1*(x1+y1))
v1 = d1*(d1^2+d1+d2)*(x1/(x1*y1+d1*(x1+y1))+d1+1)
u2 = d1*(d1^2+d1+d2)*(x2+y2)/(x2*y2+d1*(x2+y2))
v2 = d1*(d1^2+d1+d2)*(x2/(x2*y2+d1*(x2+y2))+d1+1)
u3 = d1*(d1^2+d1+d2)*(x3+y3)/(x3*y3+d1*(x3+y3))
v3 = d1*(d1^2+d1+d2)*(x3/(x3*y3+d1*(x3+y3))+d1+1)
lam = (v2+v1)/(u2+u1)
u4 = lam^2+lam+u1+u2+d1^2+d2
v4 = v1+lam*(u1+u4)+u4
0 == S(numerator(u3-u4))
0 == S(numerator(v3-v4))
```

Hence $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_3, y_3)$. □

4 Complete binary Edwards curves

If d_2 does not have the form $t^2 + t$ then the addition law on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ has the very nice feature of *completeness*. This means that there are *no* exceptions to the addition law: the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$

and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ never vanish. The addition law *always* produces a point on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ corresponding to the usual sum of points on elliptic curves in Weierstrass form.

In this section we prove completeness for these d_2's. We also prove that over finite fields $\mathbf{F}_{2^n}$ with $n \geq 3$ all ordinary curves are birationally equivalent to complete binary Edwards curves.

Theorem 4.1 (Completeness of the addition law). *Let k be a field with $\mathrm{char}(k) = 2$. Let d_1, d_2 be elements of k with $d_1 \neq 0$. Assume that no element $t \in k$ satisfies $t^2 + t + d_2 = 0$. Then the addition law on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}(k)$ is complete.*

Proof. We show for all $(x_1, y_1), (x_2, y_2) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(k)$ that the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero.

If $x_2 + y_2 = 0$ then the denominators are d_1, which is nonzero by hypothesis. Assume from now on that $x_2 + y_2 \neq 0$, and suppose that $d_1/(x_2 + y_2) = x_1 + x_1^2$. Use the curve equation to see that

$$\begin{aligned}\frac{d_1}{x_2 + y_2} &= \frac{d_1(x_2 + y_2)}{x_2^2 + y_2^2} = \frac{d_2(x_2^2 + y_2^2) + x_2y_2 + x_2y_2(x_2 + y_2) + x_2^2y_2^2}{x_2^2 + y_2^2} \\ &= d_2 + \frac{x_2y_2 + x_2y_2(x_2 + y_2) + y_2^2}{x_2^2 + y_2^2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2} \\ &= d_2 + \frac{y_2 + x_2y_2}{x_2 + y_2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2}\end{aligned}$$

and hence that $t^2 + t + d_2 = 0$ where $t = x_1 + (y_2 + x_2y_2)/(x_2 + y_2) \in k$. Contradiction. Hence $d_1 + (x_1 + x_1^2)(x_2 + y_2) \neq 0$. Similarly $d_1 + (y_1 + y_1^2)(x_2 + y_2) \neq 0$. □

Definition 4.2 (Complete binary Edwards curve). *Let k be a field with $\mathrm{char}(k) = 2$. Let d_1, d_2 be elements of k with $d_1 \neq 0$. Assume that no element $t \in k$ satisfies $t^2 + t + d_2 = 0$. The* complete binary Edwards curve with coefficients d_1 and d_2 *is the affine curve*

$$\mathrm{E}_{\mathrm{B},d_1,d_2} : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2.$$

There is no conflict in notation or terminology here: the complete binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ is the same as the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$. The complete case has the extra requirement that $t^2 + t + d_2 \neq 0$ for *all* $t \in k$, not just for $t = d_1$. If k is a finite field $\mathbf{F}_{2^n}$ then an equivalent requirement is that $\mathrm{Tr}(d_2) = 1$, where Tr is the absolute trace of $\mathbf{F}_{2^n}$ over $\mathbf{F}_2$.

Generality of $\mathbf{E_{B,d_1,d_2}}$. We now study which isomorphism classes of elliptic curves over a finite field $\mathbf{F}_{2^n}$ are birationally equivalent to complete binary Edwards curves $\mathrm{E}_{\mathrm{B},d_1,d_2}$.

Theorem 4.3. *Let n be an integer with $n \geq 3$. Each ordinary elliptic curve over $\mathbf{F}_{2^n}$ is birationally equivalent over $\mathbf{F}_{2^n}$ to a complete binary Edwards curve.*

Proof. Each ordinary elliptic curve over $\mathbf{F}_{2^n}$ is isomorphic to $v^2 + uv = u^3 + a_2u^2 + a_6$ for some $a_2 \in \mathbf{F}_{2^n}$ and $a_6 \in \mathbf{F}_{2^n}^*$. Note that if $\mathrm{Tr}(a_2) = \mathrm{Tr}(a_2')$ then the two curves $v^2 + uv = u^3 + a_2u^2 + a_6$ and $v^2 + uv = u^3 + a_2'u^2 + a_6$ are isomorphic: there exists b such that $a_2' = a_2 + b + b^2$, and the map $v \mapsto v + bu$ is an isomorphism from $v^2+uv = u^3+a_2u^2+a_6$ to $v^2+uv = u^3+(a_2+b+b^2)u^2+a_6$.

Fix a_2, a_6 for the rest of the proof. For each $\delta, \epsilon \in \mathbf{F}_2$ define

$$D_{\delta,\epsilon} = \left\{d_1 \in \mathbf{F}_{2^n}^* : \mathrm{Tr}(d_1) = \delta,\ \mathrm{Tr}(\sqrt{a_6}/d_1^2) = \epsilon\right\}.$$

If $d_1 \in D_{\mathrm{Tr}(a_2)+1,1}$ then the pair (d_1, d_2) with $d_2 = d_1^2 + d_1 + \sqrt{a_6}/d_1^2$ has $\mathrm{Tr}(d_2) = \mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$ and therefore defines a complete binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$. This curve is birationally equivalent to $v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + a_6$, since $d_1^4(d_1^4 + d_1^2 + d_2^2) = a_6$, and therefore birationally equivalent to $v^2 + uv = u^3 + a_2u^2 + a_6$, since $\mathrm{Tr}(d_1^2 + d_2) = \mathrm{Tr}(d_1) + \mathrm{Tr}(d_2) = \mathrm{Tr}(a_2)$.

Our goal is to show that $D_{\mathrm{Tr}(a_2)+1,1}$ is nonempty. We will do this by counting the number of elements in both D_{01} and D_{11}.

Observe first that $\#D_{00} + \#D_{01} = 2^{n-1} - 1$. Indeed, $\#D_{00} + \#D_{01}$ is the number of $d_1 \in \mathbf{F}_{2^n}^*$ with $\mathrm{Tr}(d_1) = 0$.

Observe next that $\#D_{01}+\#D_{11} = 2^{n-1}$. Indeed, $\#D_{01}+\#D_{11}$ is the number of $d_1 \in \mathbf{F}_{2^n}^*$ with $\mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$. As d_1 runs through $\mathbf{F}_{2^n}^*$, the quotient $\sqrt{a_6}/d_1^2$ also runs through $\mathbf{F}_{2^n}^*$, so it has trace 1 exactly 2^{n-1} times.

The heart of the proof is a bound on $\#D_{00} + \#D_{11}$, the number of $d_1 \in \mathbf{F}_{2^n}^*$ with $\mathrm{Tr}(d_1 + \sqrt{a_6}/d_1^2) = 0$. For each such d_1 there are exactly two choices of $s \in \mathbf{F}_{2^n}$ such that $s^2+s = d_1+\sqrt{a_6}/d_1^2$, producing two choices of point $(U_1, V_1) = (d_1, d_1s)$ on the elliptic curve $V^2 + UV = U^3 + \sqrt{a_6}$. All points on this elliptic curve appear uniquely in this way, except that the point at infinity and the point $(0, 0)$ do not appear. By Hasse's theorem, this curve has $2^n + 1 + t$ points for some integer t in the interval $[-2\sqrt{2^n}, 2\sqrt{2^n}]$. Therefore $\#D_{00} + \#D_{11} = 2^{n-1} + (t - 1)/2$.

Now $2\#D_{01} = (\#D_{00} + \#D_{01}) + (\#D_{01} + \#D_{11}) - (\#D_{00} + \#D_{11}) = 2^{n-1} - 1 + 2^{n-1} - 2^{n-1} - (t - 1)/2 = 2^{n-1} - (t + 1)/2$ and $2\#D_{11} = 2^n - 2\#D_{01} = 2^{n-1} + (t+1)/2$. The crude bound $(\sqrt{2^n} - 1)^2 \geq (\sqrt{8} - 1)^2 > 2$ implies $2^n > 2\sqrt{2^n} + 1 \geq |t| + 1$, so both D_{01} and D_{11} are nonempty. □

Given a_2, a_6 defining a Weierstrass curve, one can choose a random d_1 with $\mathrm{Tr}(d_1) = \mathrm{Tr}(a_2) + 1$, check whether $\mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$, and if so compute $d_2 = d_1^2+d_1+\sqrt{a_6}/d_1^2$, obtaining a complete binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ birationally equivalent to the original curve. The theorem says that this procedure succeeds for *at least one* d_1, but the proof actually shows more: the procedure succeeds for approximately 50% of all d_1 with $\mathrm{Tr}(d_1) = \mathrm{Tr}(a_2)+1$. Computer experiments show that it suffices to search a few *small* field elements d_1, where "small" means "allowing very fast multiplications."

5 Explicit addition formulas

This section presents explicit formulas for affine addition, projective addition, and mixed addition on binary Edwards curves. The formulas are not as fast as

known formulas for Weierstrass curves but have the advantage of being strongly unified and, for suitable d_2, the advantage of completeness. We are continuing to investigate addition speed; we have already found several speedups and incorporated those speedups into the formulas here.

See Section 6 for much faster doubling formulas, and Section 7 for much faster differential-addition formulas. We have integrated all of our formulas into the Explicit-Formulas Database, `http://hyperelliptic.org/EFD`.

Affine addition. The following formulas, given (x_1, y_1) and (x_2, y_2) on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, compute the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ if it is defined:

$$\begin{aligned}
&w_1 = x_1 + y_1,\ w_2 = x_2 + y_2,\ A = x_1^2 + x_1,\ B = y_1^2 + y_1,\ C = d_2 w_1 \cdot w_2,\\
&D = x_2 \cdot y_2,\ x_3 = y_1 + (C + d_1(w_1 + x_2) + A \cdot (D + x_2))/(d_1 + A \cdot w_2),\\
&y_3 = x_1 + (C + d_1(w_1 + y_2) + B \cdot (D + y_2))/(d_1 + B \cdot w_2).
\end{aligned}$$

These formulas use $2\mathbf{I} + 8\mathbf{M} + 2\mathbf{S} + 3\mathbf{D}$, where $\mathbf{I}$ is the cost of a field inversion, $\mathbf{M}$ is the cost of a field multiplication, $\mathbf{S}$ is the cost of a field squaring, and $\mathbf{D}$ is the cost of a multiplication by a curve parameter. The $3\mathbf{D}$ here are two multiplications by d_1 and one multiplication by d_2. One can replace $2\mathbf{I}$ with $1\mathbf{I} + 3\mathbf{M}$ using Montgomery's inversion trick.

For complete binary Edwards curves the denominators $d_1 + A \cdot w_2 = d_1 + (x_1^2 + x_1)(x_2 + y_2)$ and $d_1 + B \cdot w_2 = d_1 + (y_1^2 + y_1)(x_2 + y_2)$ cannot be zero. See Theorem 4.1.

Mixed addition. The following formulas, given $(X_1 : Y_1 : Z_1)$ and (x_2, y_2) on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, compute the sum $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (x_2, y_2)$ if it is defined:

$$\begin{aligned}
&W_1 = X_1 + Y_1,\ w_2 = x_2 + y_2,\ A = x_2^2 + x_2,\ B = y_2^2 + y_2,\\
&D = W_1 \cdot Z_1,\ E = d_1 Z_1^2,\ H = (E + d_2 D) \cdot w_2,\\
&I = d_1 Z_1,\ U = E + A \cdot D,\ V = E + B \cdot D,\ Z_3 = U \cdot V,\\
&X_3 = Z_3 \cdot y_2 + (H + X_1 \cdot (I + A \cdot (Y_1 + Z_1))) \cdot V,\\
&Y_3 = Z_3 \cdot x_2 + (H + Y_1 \cdot (I + B \cdot (X_1 + Z_1))) \cdot U.
\end{aligned}$$

These formulas use $13\mathbf{M} + 3\mathbf{S} + 3\mathbf{D}$. As above the $3\mathbf{D}$ are two multiplications by d_1 and one multiplication by d_2. For complete binary Edwards curves the product $Z_3 = Z_1^4(d_1 + (x_2^2 + x_2)(x_1 + y_1))(d_1 + (y_2^2 + y_2)(x_1 + y_1))$ cannot be zero.

Projective addition. The following formulas, given $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, compute the sum $(X_3 : Y_3 :$

$Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ if it is defined:

$$W_1 = X_1 + Y_1,\ W_2 = X_2 + Y_2,\ A = X_1 \cdot (X_1 + Z_1),\ B = Y_1 \cdot (Y_1 + Z_1),$$
$$C = Z_1 \cdot Z_2,\ D = W_2 \cdot Z_2,\ E = d_1 C^2,\ H = (d_1 Z_2 + d_2 W_2) \cdot W_1 \cdot C,$$
$$I = d_1 C \cdot Z_1,\ U = E + A \cdot D,\ V = E + B \cdot D,\ S = U \cdot V,$$
$$X_3 = S \cdot Y_1 + (H + X_2 \cdot (I + A \cdot (Y_2 + Z_2))) \cdot V \cdot Z_1,$$
$$Y_3 = S \cdot X_1 + (H + Y_2 \cdot (I + B \cdot (X_2 + Z_2))) \cdot U \cdot Z_1,\ Z_3 = S \cdot Z_1.$$

These formulas use $21\mathbf{M} + 1\mathbf{S} + 4\mathbf{D}$. The $4\mathbf{D}$ are three multiplications by d_1 and one multiplication by d_2. For complete binary Edwards curves the product $Z_3 = Z_1^5 Z_2^4 (d_1 + (x_2^2 + x_2)(x_1 + y_1))(d_1 + (y_2^2 + y_2)(x_1 + y_1))$ cannot be zero.

The following formulas are considerably better than the previous formulas when d_1 and d_2 are small:

$$A = X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2,\ D = d_1 C,\ E = C^2,\ F = d_1^2 E,$$
$$G = (X_1 + Z_1) \cdot (X_2 + Z_2),\ H = (Y_1 + Z_1) \cdot (Y_2 + Z_2),$$
$$I = A + G,\ J = B + H,\ K = (X_1 + Y_1) \cdot (X_2 + Y_2),$$
$$U = C \cdot (F + d_1 K \cdot (K + I + J + C)),$$
$$V = U + D \cdot F + K \cdot (d_2 (d_1 E + G \cdot H + A \cdot B) + (d_2 + d_1) I \cdot J),$$
$$X_3 = V + D \cdot (A + D) \cdot (G + D),\ Y_3 = V + D \cdot (B + D) \cdot (H + D),$$
$$Z_3 = U + (d_2 + d_1) C \cdot K^2.$$

These formulas use $18\mathbf{M} + 2\mathbf{S} + 7\mathbf{D}$. The $7\mathbf{D}$ are three multiplications by d_1, two multiplications by $d_2 + d_1$, one multiplication by d_1^2, and one multiplication by d_2. One can alternatively compute F as D^2, replacing $1\mathbf{D}$ with $1\mathbf{S}$. For complete binary Edwards curves the denominator Z_3 cannot be zero.

These formulas become simpler in the case $d_1 = d_2$:

$$A = X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2,\ D = d_1 C,\ E = C^2,\ F = d_1^2 E,$$
$$G = (X_1 + Z_1) \cdot (X_2 + Z_2),\ H = (Y_1 + Z_1) \cdot (Y_2 + Z_2),$$
$$I = A + G,\ J = B + H,\ K = (X_1 + Y_1) \cdot (X_2 + Y_2),\ L = d_1 K,$$
$$U = C \cdot (F + L \cdot (K + I + J + C)),$$
$$V = U + D \cdot F + L \cdot (d_1 E + G \cdot H + A \cdot B),$$
$$X_3 = V + D \cdot (A + D) \cdot (G + D),\ Y_3 = V + D \cdot (B + D) \cdot (H + D),$$
$$Z_3 = U.$$

These formulas use $16\mathbf{M} + 1\mathbf{S} + 4\mathbf{D}$. The $4\mathbf{D}$ are three multiplications by d_1 and one multiplication by d_1^2. As above one can replace $1\mathbf{D}$ with $1\mathbf{S}$. For complete binary Edwards curves the denominator Z_3 cannot be zero.

6 Doubling

This section presents extremely fast doubling formulas on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, first in affine coordinates and then in inversion-free projective coordinates. The formulas are complete if the curve is complete.

Since the addition formulas on the curve are strongly unified, they can be used to double. This is an interesting option when doublings occur "by accident" or when side-channel uniformity is an issue. This section shows the relation of the doubling formulas to the general addition formulas.

This section also reviews the literature on doubling formulas for binary elliptic curves, presents two improvements to the best previous formulas for Weierstrass form, and compares the doubling speeds of binary Edwards curves and Weierstrass curves.

Affine doubling. Let (x_1, y_1) be a point on $\mathrm{E}_{\mathrm{B},d_1,d_2}$, and assume that the sum $(x_1, y_1) + (x_1, y_1)$ is defined. Computing $(x_3, y_3) = (x_1, y_1) + (x_1, y_1)$ we obtain

$$\begin{aligned} x_3 &= \frac{d_2(x_1+y_1)^2 + (x_1+x_1^2)(x_1+y_1^2)}{d_1 + (x_1+y_1)(x_1+x_1^2)} \\ &= \frac{d_1(x_1+y_1) + x_1y_1 + x_1^2(1+x_1+y_1)}{d_1 + x_1y_1 + x_1^2(1+x_1+y_1)} \\ &= 1 + \frac{d_1(1+x_1+y_1)}{d_1 + x_1y_1 + x_1^2(1+x_1+y_1)}, \end{aligned}$$

where the second line uses that $d_2(x_1+y_1)^2 + x_1^2y_1^2 + x_1y_1^2 = d_1(x_1+y_1) + x_1y_1 + x_1^2y_1$ for all points on $\mathrm{E}_{\mathrm{B},d_1,d_2}$. Likewise we have

$$y_3 = 1 + \frac{d_1(1+x_1+y_1)}{d_1 + x_1y_1 + y_1^2(1+x_1+y_1)}.$$

To compute the affine formulas with one inversion we note that the product of the denominators of x_3 and y_3 is

$$\begin{aligned} &(d_1 + x_1y_1 + x_1^2(1+x_1+y_1))(d_1 + x_1y_1 + y_1^2(1+x_1+y_1)) \\ &= d_1^2 + (x_1^2+y_1^2)(d_1(1+x_1+y_1) + x_1y_1(1+x_1+y_1) + x_1^2y_1^2) \\ &= d_1^2 + (x_1^2+y_1^2)(d_1 + d_2(x_1^2+y_1^2)) = d_1(d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4+y_1^4)), \end{aligned}$$

where we used the curve equation again. This leads to the doubling formulas

$$\begin{aligned} x_3 &= 1 + \frac{d_1 + d_2(x_1^2+y_1^2) + y_1^2 + y_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4+y_1^4)}, \\ y_3 &= 1 + \frac{d_1 + d_2(x_1^2+y_1^2) + x_1^2 + x_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4+y_1^4)} \end{aligned}$$

needing $1\mathbf{I} + 2\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$. The $2\mathbf{D}$ are one multiplication by d_2 and one multiplication by d_2/d_1. For complete binary Edwards curves all denominators here are nonzero.

If $d_1 = d_2$ some multiplications can be grouped as follows:

$$\begin{aligned} &A = x_1^2,\ B = A^2,\ C = y_1^2,\ D = C^2,\ E = A + C, \\ &F = 1/(d_1 + E + B + D),\ x_3 = (d_1E + A + B) \cdot F,\ y_3 = x_3 + 1 + d_1F. \end{aligned}$$

These formulas use only $1\mathbf{I}+1\mathbf{M}+4\mathbf{S}+2\mathbf{D}$. The $2\mathbf{D}$ are two multiplications by d_1.

Projective doubling. Here are explicit formulas to compute $2(X_1 : Y_1 : Z_1) = (X_3 : Y_3 : Z_3)$ if it is defined:

$$A = X_1^2,\ B = A^2,\ C = Y_1^2,\ D = C^2,\ E = Z_1^2,\ F = d_1E^2,$$
$$G = (d_2/d_1)(B + D),\ H = A \cdot E,\ I = C \cdot E,\ J = H + I,\ K = G + d_2J,$$
$$Z_3 = F + J + G,\ X_3 = K + H + D,\ Y_3 = K + I + B.$$

These formulas use $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$. The $3\mathbf{D}$ are multiplications by d_1, d_2/d_1, and d_2. For complete binary Edwards curves the denominator Z_3 is nonzero.

If $d_1 = d_2$ then a squaring can be saved as follows:

$$W_1 = X_1 + Y_1,\ E = (W_1(W_1 + Z_1))^2,$$
$$X_3 = ((\sqrt{d_1}W_1 + X_1)Z_1 + X_1^2)^2,\ Y_3 = X_3 + E,\ Z_3 = E + d_1(Z_1^2)^2.$$

These formulas use $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$. The $2\mathbf{D}$ are multiplications by d_1 and $\sqrt{d_1}$; an alternative, rewriting $d_1(Z_1^2)^2$ as $(\sqrt{d_1}Z_1^2)^2$, uses two multiplications by $\sqrt{d_1}$. For complete binary Edwards curves the denominator Z_3 is nonzero.

Comparison with previous work. All of the doubling formulas for binary elliptic curves presented in the literature have exceptional cases, such as doubling a point of order 2. Our doubling formulas for complete Edwards curves are the first complete doubling formulas in the literature. The following comparison shows that our doubling formulas also provide quite attractive speeds.

The fastest inversion-free doubling formulas mentioned in [9, Table 13.4] are in López-Dahab coordinates and take $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$; these formulas were introduced by Lange in [26]. The $1\mathbf{D}$ is a multiplication by a_2 and is eliminated by typical curve choices. Formulas in [9, page 294], introduced by López and Dahab in [28], take $3\mathbf{M}+5\mathbf{S}+1\mathbf{D}$ when $a_2 \in \{0, 1\}$; here the $1\mathbf{D}$ is a multiplication by the curve parameter $\sqrt{a_6}$.

For random curves, experiments show that we can always choose d_1 to be small, so our new $2\mathbf{M}+6\mathbf{S}+3\mathbf{D}$ becomes at worst $4\mathbf{M}+6\mathbf{S}$, slightly slower than $4\mathbf{M} + 4\mathbf{S}$. By choosing curves with small $d_1 = d_2$ we achieve $2\mathbf{M} + 5\mathbf{S}$, which is significantly faster than $3\mathbf{M} + 5\mathbf{S}$ and $4\mathbf{M} + 4\mathbf{S}$.

In [21] Kim and Kim present doubling formulas for curves of the form $v^2 + uv = u^3 + u^2 + a_6$ needing $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$, where the $2\mathbf{D}$ are both by a_6. Our $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ formulas are the same speed. Our $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ formulas are slightly slower but have the advantages of extra generality and completeness.

Our improvements of previous work. We present here two improvements to doubling formulas in López-Dahab coordinates for binary curves in Weierstrass form. Of course, this makes the speed competition more challenging for Edwards curves! ;–)

The first improvement is an easy speedup of the Kim–Kim formulas. Kim and Kim represent an affine point (u_1, v_1) as $(U_1 : V_1 : W_1 : T_1)$, where $u_1 = U_1/W_1$,

$v_1 = V_1/W_1^2$, and $T_1 = W_1^2$. Our improved formulas compute $2(U_1 : V_1 : W_1 : T_1) = (U_3 : V_3 : W_3 : T_3)$ as

$$A = U_1^2,\ B = V_1^2,\ W_3 = T_1 \cdot A,\ T_3 = W_3^2,$$
$$U_3 = (A + \sqrt{a_6}\, T_1)^2,\ V_3 = B \cdot (B + U_3 + W_3) + a_6 T_3 + T_3.$$

These improved formulas use only $2\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$, where the $2\mathbf{D}$ are one multiplication by a_6 and one multiplication by $\sqrt{a_6}$.

The second improvement achieves $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for curves of the shape $v^2 + uv = u^3 + a_6$. We represent a point by $(U_1 : V_1 : W_1 : T_1 : S_1)$, where additionally $S_1 = U_1 W_1$. The idea used by Kim and Kim does not carry over to these curves but we have developed the following formulas to compute $2(U_1 : V_1 : W_1 : T_1 : S_1) = (U_3 : V_3 : W_3 : T_3 : S_3)$:

$$A = U_1^2,\ B = V_1^2,\ W_3 = S_1^2,\ U_3 = (A + \sqrt{a_6}\, T_1)^2,$$
$$T_3 = W_3^2,\ S_3 = U_3 \cdot W_3,\ V_3 = B \cdot (B + U_3 + W_3) + a_6 T_3 + S_3.$$

We caution the reader that these Weierstrass formulas are not complete.

7 Differential addition

This section presents fast explicit formulas for w-coordinate differential addition on binary Edwards curves. Here $w = x + y$. Note that $w(-P) = w(P)$, since $-(x, y) = (y, x)$.

"Differential addition" means computing $Q + P$ given $Q, P, Q - P$: e.g., computing $(2m+1)P$ given $(m+1)P, mP, P$, or computing $2mP$ given $mP, mP, 0P$. In particular, "w-coordinate differential addition" means computing $w(Q + P)$ given $w(Q), w(P), w(Q - P)$. This section also discusses "w-coordinate differential addition and doubling": computing both $w(2P)$ and $w(Q + P)$, again given $w(Q), w(P), w(Q - P)$.

More concretely, write $(x_1, y_1) = Q - P$, $(x_2, y_2) = P$, $(x_3, y_3) = Q$, $(x_4, y_4) = 2P$, and $(x_5, y_5) = Q + P$. This section presents fast explicit formulas to compute $x_5 + y_5$ given $x_1 + y_1$, $x_2 + y_2$, and $x_3 + y_3$. This section also presents fast explicit formulas to compute $x_4 + y_4$ and $x_5 + y_5$ given $x_1 + y_1$, $x_2 + y_2$, and $x_3 + y_3$. As in previous sections, the formulas are complete if the curve is complete.

We analyze the costs of our formulas in several situations. The simplest situation is that inputs $x_1 + y_1, x_2 + y_2, x_3 + y_3$ and outputs $x_4 + y_4, x_5 + y_5$ are represented in affine form, i.e., as field elements. If inversions are expensive—as they usually are—and storage is available then it is better for each input and output to be represented in projective form, i.e., as a ratio of two field elements. Some applications use mixed differential additions, where $x_1 + y_1$ is given in

affine form while everything else is projective. We achieve the following speeds:

	general case	$d_2 = d_1$
affine diff addition	$1\mathbf{I} + 3\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$	$1\mathbf{I} + 1\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$
affine diff addition+doubling	$2\mathbf{I} + 4\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$	$2\mathbf{I} + 1\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$
mixed diff addition	$6\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$	$5\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$
mixed diff addition+doubling	$6\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$
projective diff addition	$8\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$	$7\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$
projective diff addition+doubling	$8\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$	$7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$

Why differential addition is interesting. Montgomery in [30] presented fast formulas for u-coordinate differential addition on non-binary elliptic curves $v^2 = u^3 + a_2u^2 + u$. As an application, Montgomery suggested what is now called the "Montgomery ladder" to compute $u(mP), u((m+1)P)$ given $u(P)$. The idea is to recursively compute $u(\lfloor m/2 \rfloor P), u((\lfloor m/2 \rfloor + 1)P)$, and then to compute $u(mP), u((m+1)P)$ with a differential addition and doubling.

The Montgomery ladder is one of the most popular scalar-multiplication methods. It has several attractive features: it is fast; it fits into extremely small hardware; and its uniform double-and-add structure adds a natural layer of protection against simple side-channel attacks. See [29], [6], [15], [11], and [19]. The input $u(P)$ is normally given in affine form, creating affine differential additions if inversions are inexpensive and mixed differential additions otherwise.

Montgomery also suggested a more complicated "PRAC" chain of differential additions to compute $u(mP)$ from $u(P)$. This chain uses more memory than the Montgomery ladder and does not have the same simple structure, but it is faster in some situations. This chain rarely reuses the input $u(P)$; it relies mainly on projective differential additions if inversions are expensive.

Differential-addition formulas for binary elliptic curves. Several authors have given formulas for u-coordinate differential additions on binary elliptic curves $v^2 + a_1uv = u^3 + a_2u^2 + a_6$. The resulting Montgomery ladders for binary elliptic-curve scalar-multiplication fit into even smaller hardware than the ladders for the non-binary case, and they have similar resistance to simple side-channel attacks.

Specifically, u-coordinate differential-addition formulas for the case $a_1 = 1$ were presented by Agnew, Mullin, and Vanstone in [1, page 808]; by Lopez and Dahab in [29, Lemma 2 and Section 4.2]; by Vanstone, Mullin, Antipa, and Gallant, according to [33]; by Stam in [33, Section 3.1], and by Gaudry in [13, page 33]. Lopez and Dahab say that their formulas use $6\mathbf{M} + 5\mathbf{S}$ for a mixed differential addition and doubling; see [29, Lemma 5]. Stam, after pointing out various speedups, says that projective differential addition takes $6\mathbf{M} + 1\mathbf{S}$; that mixed differential addition takes $4\mathbf{M} + 1\mathbf{S}$; and that a doubling takes $1\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$. Stam also presents differential-addition formulas for the case $a_6 = 1/a_1^2$, using only $5\mathbf{M}$ and an unspecified number of $\mathbf{S}$ for projective differential addition. Gaudry states a cost of $5\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for mixed differential addition and doubling; Gaudry and Lubicz state the same cost in [14, page 16].

All of the formulas in [1], [29], [33], and [13] fail if the neutral element on the curve appears. Our new formulas have no trouble with the neutral element, and have the advantage of completeness for suitable d_2. Our formulas are also competitive in speed with previous formulas—slightly slower in some situations but slightly faster in others.

The new formulas. Let (x_2, y_2) be a point on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$. Assume that the sum $(x_2, y_2) + (x_2, y_2)$ is defined (as it always is on complete binary Edwards curves). Write $(x_4, y_4) = (x_2, y_2) + (x_2, y_2)$, and write $w_i = x_i + y_i$. Then $d_1^2 + d_1 w_2^2 + d_2 w_2^4 \neq 0$ and

$$w_4 = \frac{d_1 w_2^2 + d_1 w_2^4}{d_1^2 + d_1 w_2^2 + d_2 w_2^4} = \frac{w_2^2 + w_2^4}{d_1 + w_2^2 + (d_2/d_1) w_2^4}$$

by Lemma 3.1. In particular, if $d_2 = d_1$, then $d_1 + w_2^2 + w_2^4 \neq 0$ and

$$w_4 = 1 + \frac{d_1}{d_1 + w_2^2 + w_2^4}.$$

More generally, assume that $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_5, y_5)$ are points on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ satisfying $(x_1, y_1) = (x_3, y_3) - (x_2, y_2)$ and $(x_5, y_5) = (x_2, y_2) + (x_3, y_3)$, and write $w_i = x_i + y_i$ as before. Then, by Lemma 3.1,

$$d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3) \neq 0$$

and

$$w_1 + w_5 = \frac{d_1 w_2 w_3 (1 + w_2)(1 + w_3)}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)},$$
$$w_1 w_5 = \frac{d_1^2 (w_2 + w_3)^2}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)}.$$

In particular, if $d_2 = d_1$, then $d_1 + w_2 w_3 (1 + w_2)(1 + w_3) \neq 0$ and

$$w_1 + w_5 = 1 + \frac{d_1}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)},$$
$$w_1 w_5 = \frac{d_1 (w_2 + w_3)^2}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)}.$$

Cost of affine w-coordinate differential addition and doubling. The explicit formulas

$$R = w_2 \cdot w_3,\ S = R^2,\ T = R \cdot (1 + w_2 + w_3) + S,$$
$$w_5 = T \cdot \frac{1}{d_1 + T + (d_2/d_1 + 1) S} + w_1$$

use $1\mathbf{I} + 3\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$, where the $1\mathbf{D}$ is a multiplication by the curve parameter $d_2/d_1 + 1$. For complete binary Edwards curves the denominator is never zero.

If $d_2 = d_1$ then the explicit formulas

$$A = w_2^2,\ B = A + w_2,\ C = w_3^2,\ D = C + w_3,\ w_5 = 1 + d_1 \frac{1}{d_1 + B \cdot D} + w_1$$

use just $1\mathbf{I}+1\mathbf{M}+2\mathbf{S}+1\mathbf{D}$. For complete binary Edwards curves the denominator is never zero.

Doubling: The explicit formulas

$$A = w_2^2,\ J = A^2,\ K = A + J,\ w_4 = K \cdot \frac{1}{d_1 + K + (d_2/d_1 + 1)J}$$

use $1\mathbf{I}+1\mathbf{M}+2\mathbf{S}+1\mathbf{D}$, where the $1\mathbf{D}$ is a multiplication by the curve parameter $d_2/d_1 + 1$. For complete binary Edwards curves the denominator is never zero. The total cost of a differential addition and doubling is $2\mathbf{I} + 4\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$, or $1\mathbf{I} + 7\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$ with Montgomery's inversion trick.

If $d_2 = d_1$ then the explicit formulas

$$A = w_2^2,\ B = A + w_2,\ w_4 = 1 + d_1 \frac{1}{d_1 + B^2}$$

use just $1\mathbf{I} + 2\mathbf{S} + 1\mathbf{D}$. For complete binary Edwards curves the denominator is never zero. These formulas can share the computations of A and B with differential addition, reducing the total cost of a differential addition and doubling to $2\mathbf{I} + 1\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$, or $1\mathbf{I} + 4\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$ with Montgomery's inversion trick.

Cost of mixed w-coordinate differential addition and doubling. Assume that w_1 is given as a field element, that w_2, w_3 are given as fractions $W_2/Z_2, W_3/Z_3$, and that w_4, w_5 are to be output as fractions $W_4/Z_4, W_5/Z_5$.

The explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ D = W_3 \cdot (Z_3 + W_3),\ E = Z_2 \cdot Z_3,\ F = W_2 \cdot W_3,$$
$$V = C \cdot D,\ U = V + (\sqrt{d_1}\, E + \sqrt{d_2/d_1 + 1}\, F)^2,\ W_5 = V + w_1 \cdot U,\ Z_5 = U$$

use $6\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$, where the $2\mathbf{D}$ are multiplications by the curve parameters $\sqrt{d_1}$ and $\sqrt{d_2/d_1 + 1}$. For complete binary Edwards curves Z_5 cannot be zero.

If $d_2 = d_1$ then the explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ D = W_3 \cdot (Z_3 + W_3),\ E = Z_2 \cdot Z_3,$$
$$V = C \cdot D,\ U = V + d_1 E^2,\ W_5 = V + w_1 \cdot U,\ Z_5 = U$$

use only $5\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

Doubling: The explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ W_4 = C^2,\ Z_4 = W_4 + ((\sqrt[4]{d_1}\, Z_2 + \sqrt[4]{d_2/d_1 + 1}\, W_2)^2)^2$$

use $1\mathbf{M}+3\mathbf{S}+2\mathbf{D}$, where the $2\mathbf{D}$ are multiplications by the curve parameters $\sqrt[4]{d_1}$ and $\sqrt[4]{d_2/d_1 + 1}$. For complete binary Edwards curves Z_4 cannot be zero. These

formulas can share the computation of C with differential addition, reducing the total cost of differential addition and doubling to $6\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$.

If $d_2 = d_1$ then the explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ W_4 = C^2,\ Z_4 = d_1(Z_2^2)^2 + W_4$$

use $1\mathbf{M}+3\mathbf{S}+1\mathbf{D}$ and can share the computation of C with differential addition, reducing the total cost of differential addition and doubling to $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$.

Cost of projective w-coordinate differential addition and doubling. Assume that w_1, w_2, w_3 are given as fractions $W_1/Z_1, W_2/Z_2, W_3/Z_3$, and that w_4, w_5 are to be output as fractions $W_4/Z_4, W_5/Z_5$.

Replacing "$W_5 = V + w_1 \cdot U,\ Z_5 = U$" in any of the mixed formulas with "$W_5 = V \cdot Z_1 + U \cdot W_1,\ Z_5 = U \cdot Z_1$" produces projective formulas costing $2\mathbf{M}$ extra. For example, starting from the $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ formulas for mixed differential addition and doubling with $d_2 = d_1$, one obtains $7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ formulas for projective differential addition and doubling with $d_2 = d_1$.

Our w_1w_5 formulas offer an interesting alternative. For example, the explicit formulas

$$A = W_2 \cdot W_3,\ B = Z_2 \cdot Z_3,\ C = (W_2 + Z_2) \cdot (W_3 + Z_3),$$
$$W_5 = Z_1 \cdot (d_1(C + A + B)^2),\ Z_5 = W_1 \cdot (A \cdot C + (\sqrt{d_1}\, B + \sqrt{d_2/d_1 + 1}\, A)^2)$$

use only $6\mathbf{M} + 2\mathbf{S} + 3\mathbf{D}$ for differential addition. These formulas assume that w_1 is known, or checked, to be nonzero—if $w_1 = 0$ then one must resort to the previous formulas for w_5—but they still have the virtue of handling arbitrary w_2, w_3, w_4, w_5. Note that w_1 is fixed throughout the Montgomery ladder, and is 0 only if the starting point is $(0, 0)$ or $(1, 1)$.

Recovering $2P$ from $Q - P, w(P), w(Q)$. If $w_1^2 + w_1 \neq 0$ then

$$x_2^2+x_2 = \frac{w_3\left(d_1+w_1w_2(1+w_1+w_2)+\frac{d_2}{d_1}w_1^2w_2^2\right)+d_1(w_1+w_2)+(y_1^2+y_1)(w_2^2+w_2)}{w_1^2+w_1}.$$

One can use this formula to compute $2(x_2, y_2)$ given x_1, y_1, w_2, w_3; i.e., to recover $2P$ given $Q-P, w(P), w(Q)$. The formula produces $x_2^2+x_2$; a "half-trace" computation reveals either x_2 or x_2+1, and therefore either (x_2, y_2) or $(x_2, y_2)+(1, 1)$. The failure case $w_1^2 + w_1 = 0$ occurs only if $4(Q - P) = (0, 0)$.

In particular, one can recover $2mP$ given $P, w(mP), w((m + 1)P)$, except in the easily recognizable case $4P = (0, 0)$. The Montgomery ladder can therefore be used not just to compute $w(mP)$ given $w(P)$, but also to compute $2mP$ given P. If P has odd order ℓ, as it does in typical cryptographic applications, then one can replace m by $(m/2) \bmod \ell$, obtaining $mP = 2((m/2) \bmod \ell)P$ from P via $w(((m/2) \bmod \ell)P)$.

References

1. Agnew, G.B., Mullin, R.C., Vanstone, S.A., An implementation of elliptic curve cryptosystems over $F_{2^{155}}$, IEEE Journal on Selected Areas in Communications 11 (1993), 804–813. Citations in this document: §7, §7.
2. Bernstein, D.J., Lange, T., Faster addition and doubling on elliptic curves, in Asiacrypt 2007 [24] (2007), 29–50. Citations in this document: §1, §1, §1, §1.
3. Billet, O., Joye, M., The Jacobi model of an elliptic curve and side-channel analysis, in AAECC 2003 [12] (2003), 34–42. MR 2005c:94045. URL: `http://eprint.iacr.org/2002/125`. Citations in this document: §1.
4. Blake, I.F., Seroussi, G., Smart, N.P. (eds.), Advances in elliptic curve cryptography, London Mathematical Society Lecture Note Series, 317, Cambridge University Press, 2005. ISBN 0–521–60415–X. MR 2007g:94001. See [17].
5. Brier, É, Déchène, I., Joye, M., Unified point addition formulae for elliptic curve cryptosystems, in [32] (2004), 247–256. Citations in this document: §1.
6. Brier, É, Joye, M., Weierstrass elliptic curves and side-channel attacks, in PKC 2002 [31] (2002), 335–345. URL: `www.geocities.com/MarcJoye/publications.html`. Citations in this document: §1, §7.
7. Cohen, H., Frey, G. (eds.), Handbook of elliptic and hyperelliptic curve cryptography, CRC Press, 2005. ISBN 1–58488–518–1. MR 2007f:14020. See [9], [25].
8. Desmedt, Y.G. (ed.), Public key cryptography—PKC 2003, 6th international workshop on practice and theory in public key cryptography, Miami, FL, USA, January 6–8, 2003, proceedings, Lecture Notes in Computer Science, 2567, Springer, Berlin, 2002. ISBN 3–540–00324–X. See [16], [33].
9. Doche, C., Lange, T., Arithmetic of elliptic curves, in [7] (2005), 267–302. MR 2162729. Citations in this document: §2, §6, §6.
10. Edwards, H.M., A normal form for elliptic curves, Bulletin of the American Mathematical Society 44 (2007), 393–422. URL: `http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html`. Citations in this document: §1.
11. Fischer, W., Giraud, C., Knudsen, E.W., Seifert, J.-P., Parallel scalar multiplication on general elliptic curves over $\mathbb{F}_p$ hedged against non-differential side-channel attacks (2002). URL: `http://eprint.iacr.org/2002/007`. Citations in this document: §7.
12. Fossorier, M., Høholdt, T., Poli, A. (eds.), Applied algebra, algebraic algorithms and error-correcting codes, 15th international symposium, AAECC-15, Toulouse, France, May 12–16, 2003, proceedings, Lecture Notes in Computer Science, 2643, Springer, 2003. ISBN 3–540–40111–3. MR 2004j:94001. See [3].
13. Gaudry, P., Variants of the Montgomery form based on Theta functions (2006). URL: `http://www.loria.fr/~gaudry/publis/toronto.pdf`. Citations in this document: §7, §7.
14. Gaudry, P., Lubicz, D., The arithmetic of characteristic 2 Kummer surfaces (2008). URL: `http://eprint.iacr.org/2008/133`. Citations in this document: §7.
15. Izu, T., Takagi, T., A fast parallel elliptic curve multiplication resistant against side channel attacks, in PKC 2002 [31] (2002), 280-296. Citations in this document: §7.
16. Izu, T., Takagi, T., Exceptional procedure attack on elliptic curve cryptosystems, in PKC 2003 [8] (2002), 224–239. Citations in this document: §1.
17. Joye, M., Defences against side-channel analysis, in [4] (2005), 87–100. Citations in this document: §1.
18. Joye, M., Quisquater, J.-J., Hessian elliptic curves and side-channel attacks, in CHES 2001 [22] (2001), 402–410. MR 2003k:94032. URL: `www.geocities.com/MarcJoye/publications.html`. Citations in this document: §1.

19. Joye, M., Yen, S.-M., The Montgomery powering ladder, in CHES 2002 [20] (2003), 291–302. URL: http://www.gemplus.com/smart/rd/publications/pdf/JY03mont.pdf. Citations in this document: §7.
20. Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.), Cryptographic hardware and embedded systems—CHES 2002, 4th international workshop, Redwood Shores, CA, USA, August 13–15, 2002, revised papers, Lecture Notes in Computer Science, 2523, Springer, 2003. ISBN 3–540–00409–2. See [19].
21. Kim, K.H., Kim, S.I., A new method for speeding up arithmetic on elliptic curves over binary fields (2007). URL: http://eprint.iacr.org/2007/181. Citations in this document: §6.
22. Koç, Ç.K., Naccache, D., Paar, C. (eds.), Cryptographic hardware and embedded systems — CHES 2001, third international workshop, Paris, France, May 14–16, 2001, proceedings, Lecture Notes in Computer Science, 2162, Springer, 2001. ISBN 3–540–42521–7. MR 2003g:94002. See [18], [27].
23. Koç, Ç.K., Paar, C. (eds.), Cryptographic hardware and embedded systems, first international workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, proceedings, Lecture Notes in Computer Science, 1717, Springer, 1999. ISBN 3-540-66646-X. See [29].
24. Kurosawa, K. (ed.), Advances in cryptology — ASIACRYPT 2007, 13th international conference on the theory and application of cryptology and information security, Kuching, Malaysia, December 2–6, 2007, proceedings, Lecture Notes in Computer Science, 4833, Springer, 2007. ISBN 978–3–540–76899–9. See [2].
25. Lange, T., Mathematical countermeasures against side-channel attacks, in [7] (2005), 687–714. MR 2163785. Citations in this document: §1.
26. Lange, T., A note on López-Dahab coordinates, Tatra Mountains Mathematical Publications 33 (2006), 75–81. MR 2007f:11139. URL: http://eprint.iacr.org/2004/323. Citations in this document: §6.
27. Liardet, P.-Y., Smart, N.P., Preventing SPA/DPA in ECC systems using the Jacobi form, in CHES 2001 [22] (2001), 391–401. MR 2003k:94033. Citations in this document: §1.
28. López, J., Dahab, R., Improved algorithms for elliptic curve arithmetic in GF(2^n), in SAC 1998 [35] (1999), 201–212. MR 1715809. Citations in this document: §6.
29. López, J., Dahab, R., Fast multiplication on elliptic curves over GF(2^m) without precomputation, in CHES 1999 [23] (1999), 316–327. Citations in this document: §7, §7, §7, §7.
30. Montgomery, P.L., Speeding the Pollard and elliptic curve methods of factorization, Mathematics of Computation 48 (1987), 243–264. ISSN 0025–5718. MR 88e:11130. URL: http://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3. Citations in this document: §7.
31. Naccache, D., Paillier, P. (eds.), Public key cryptography, 5th international workshop on practice and theory in public key cryptosystems, PKC 2002, Paris, France, February 12–14, 2002, proceedings, Lecture Notes in Computer Science, 2274, Springer, 2002. ISBN 3–540–43168–3. MR 2005b:94044. See [6], [15].
32. Nedjah, N., Mourelle, L.M. (eds.), Embedded cryptographic hardware: methodologies & architectures, Nova Science Publishers, 2004. ISBN 1–59454–012–8. See [5].
33. Stam, M., On Montgomery-like representations for elliptic curves over GF(2^k), in PKC 2003 [8] (2002), 240–254. Citations in this document: §7, §7, §7.
34. Stein, W. (ed.), Sage Mathematics Software (Version 2.8.13), The Sage Group, 2008. URL: http://www.sagemath.org. Citations in this document: §3.

35. Tavares, S., Meijer, H. (eds.), Selected areas in cryptography, 5th annual international workshop, SAC'98, Kingston, Ontario, Canada, August 17–18, 1998, proceedings, Lecture Notes in Computer Science, 1556, Springer, Berlin, 1999. ISBN 3-540-65894-7. MR 1715799. See [28].