MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

COMPLETE ADDITION LAW FOR TWISTED EDWARDS CURVES

Reza Rezaeian Farashahi[1,2]
Ruhallah Mirzaei Aliarabi[1]
Peyman Shahbazi Dastjerdi[1]

[1]Isfahan University of Technology
[2]Institute for Research in Fundamental Sciences (IPM)

farashahi@iut.ac.ir r.mirzaei@math.iut.ac.ir peyman.shahbazi@math.iut.ac.ir

Abstract. We construct complete addition laws in extended coordinates for twisted Edwards curves $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$, where $a, d \in K^\times$, $a \neq d$, and $\operatorname{char} K \neq 2$. If $t \in K$ makes $(t^2 - a)(t^2 - d)$ a nonzero nonsquare, the construction yields a K-complete formula valid for every pair of K-rational points. The proof describes the exceptional fibres through the difference morphism. Over finite fields of odd cardinality $q > 16$, such a coefficient exists for every nonsingular parameter pair, including the same-square-class cases with full rational two-torsion.

We give full and mixed evaluation schedules. Full addition costs $8M + D_c$ in split elementary models and $10M$ or $12M$, plus fixed-constant costs, in the same-square-class cases. Doubling costs $4M+4S+\min(D_a, D_d)$, independently of coefficient selection. Here M denotes a general field multiplication, S a squaring, and D_c multiplication by a fixed $c \in K$.

1. Introduction

Elliptic-curve computations are carried out through explicit coordinate formulas. Although the group law on an elliptic curve is a morphism, a particular coordinate expression for this morphism may fail on special input pairs. On a short Weierstrass model, for example, the usual chord-and-tangent description separates generic addition, doubling, addition with the neutral element, and addition of inverse points. Such exceptional cases are harmless in the abstract group law, but they matter in computation. Algorithms that perform many group operations—scalar multiplication, elliptic-curve factorization, point-counting subroutines, isogeny computations, and experiments with explicit finite-field arithmetic—benefit from formulas that are uniform, easy to verify, and free of exceptional rational input pairs.

Let E be an elliptic curve over a field K, with identity O. An addition formula is called K-complete if it correctly computes $P + Q$ for every pair

$$(P, Q) \in E(K) \times E(K).$$

Completeness is stronger than unification. A unified formula uses the same expression for addition and doubling, but it may still have exceptional input pairs. A K-complete formula has no exceptional pair on the rational point set. It therefore treats the diagonal $P = Q$, the anti-diagonal $P = -Q$, points involving the neutral

2020 *Mathematics Subject Classification.* Primary 11G20; Secondary 14H52, 94A60.

©XXXX American Mathematical Society

element, and all low-order configurations by the same algebraic expression. This paper is concerned with this field-dependent notion of completeness.

The geometric theory of addition laws explains why complete formulas are subtle. Lange and Ruppert studied addition laws on abelian varieties and on elliptic curves in this language, viewing addition laws as sections attached to projective embeddings and line bundles [LR85, LR87]. In the Weierstrass setting, Bosma and Lenstra gave a concrete and influential form of the theory. They proved that, for an elliptic curve embedded in $\mathbb{P}^2$ in Weierstrass form, no single addition law is geometrically complete; a complete system of two laws is necessary, and a minimal complete system consists of laws of bidegree $(2, 2)$ [BL95]. A key point in their analysis is that the exceptional behaviour of an addition law is controlled by a divisor pulled back through the difference map

$$\delta : E \times E \longrightarrow E, \qquad (P, Q) \longmapsto P - Q.$$

Thus exceptional pairs are not arbitrary pairs of inputs: they are pairs whose difference lies on a specified divisor on the curve.

This difference-divisor viewpoint was later developed further by Kohel and by Arene, Kohel, and Ritzenthaler [Koh11, AKR12]. It also clarifies an important distinction. A system of addition laws may be complete over an algebraic closure, or it may be complete only over the field of computation. A single formula can fail geometrically and still be K-complete if its exceptional divisor has no K-rational point. The present work uses precisely this arithmetic form of completeness. The structural part of the construction is carried out over a general field K with $\operatorname{char} K \neq 2$. Finite fields enter later, when we use quadratic characters and character sums to select the coefficients, count admissible choices, derive operation schedules, and verify the formulas computationally.

Edwards curves changed the computational landscape of complete elliptic-curve arithmetic. Edwards introduced a symmetric normal form for elliptic curves [Edw07], and Bernstein and Lange showed that this symmetry gives very fast addition and doubling formulas [BL07]. Twisted Edwards curves enlarged the family while preserving the Edwards structure and relating it to Montgomery curves [BBJLP08]. Hisil, Wong, Carter, and Dawson then introduced and optimized extended twisted Edwards coordinates, where an auxiliary coordinate records the product xy and enables substantial sharing in the addition formulas [HWCD08]. These extended-coordinate formulas are among the basic reference points for low-cost elliptic-curve arithmetic in odd characteristic.

The twisted Edwards curve is

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

where $a, d \in K^\times$, $a \neq d$, and $\operatorname{char} K \neq 2$. Its extended-coordinate representation will be denoted by

$$\mathcal{E}^e_{a,d} : \qquad aX^2 + Y^2 = Z^2 + dT^2, \qquad XY = ZT.$$

This extended model represents the same twisted Edwards curve, with the auxiliary relation $T/Z = xy$ on the affine chart $Z \neq 0$. In the construction we also use an auxiliary $\mathbb{P}^1 \times \mathbb{P}^1$, or Segre-type, product representation. Thus there are three levels: the curve $E_{a,d}$, its extended-coordinate representation $\mathcal{E}^e_{a,d}$, and the product-coordinate representation used to organize the addition formula.

For Edwards-type formulas, completeness is governed by square classes. The previously known one-formula complete Edwards case corresponds, in twisted parameters, to the opposite-square-class regime

$$ad \notin K^{\times 2}.$$

Equivalently, the parameters a and d lie in opposite square classes. This includes the usual branch in which a is a square and d is a nonsquare, as well as its mirror branch obtained by the standard coefficient swap symmetry; see, for example, the twisted Edwards and extended-coordinate frameworks in [BBJLP08, HWCD08, FH17]. The same-square-class regime

$$ad \in K^{\times 2}$$

is different. It is the regime in which the associated elliptic curve has full rational two-torsion. The known one-formula complete Edwards condition does not by itself give a single complete low-cost formula in these two branches. This same-square-class regime is the main new difficulty addressed in this paper.

The construction begins with two known extended Edwards product laws: the standard product law and its complementary companion. These formulas belong to the extended-coordinate Edwards literature, especially the formulas of Hisil, Wong, Carter, and Dawson and the complete systems studied by Bernstein and Lange [HWCD08, BL11]. We use these known product laws as two generators of a single selected product formula.

At the level of the product representation, the construction is most naturally described by projective selection coefficients

$$\sigma, \tau \in \mathbb{P}^1(K).$$

The standard and complementary Edwards product representatives give two addition-law projections for the x-coordinate of the sum and two for the y-coordinate of the sum. We choose one projective linear combination in each of these two projection spaces. Thus σ selects the x-projection representative and τ selects the y-projection representative. The two selected projections are then recombined by the Segre reconstruction to give one extended-coordinate formula.

In an affine chart one may write

$$\sigma = (s : 1), \qquad \tau = (t : 1).$$

For inputs $P_i = (X_i : Y_i : Z_i : T_i)$, $i = 1, 2$, let x_3, y_3 denote the affine coordinates of $P_1 + P_2$. With the bilinear blocks E, R, H, W, F, G, N, V defined in Subsection 3.1, the selected projections are

$$x_3 = \frac{E + sV}{G + sW}, \qquad y_3 = \frac{H + tN}{F + tR}.$$

The values $s = \infty$ and $t = \infty$ are not field elements; they are projective shorthand for the choices $\sigma = (1 : 0)$ and $\tau = (1 : 0)$. In particular, no multiplication by an infinite element occurs in the formula.

The main criterion is field-uniform. For

$$\sigma = (\sigma_0 : \sigma_1), \qquad \tau = (\tau_0 : \tau_1),$$

define

$$\Delta_y(\sigma) = (\sigma_0^2 - \sigma_1^2)(a\sigma_0^2 - d\sigma_1^2),$$

and

$$\Delta_x(\tau) = (\tau_0^2 - a\tau_1^2)(\tau_0^2 - d\tau_1^2).$$

For every field K with $\operatorname{char} K \neq 2$, if

$$\Delta_y(\sigma), \Delta_x(\tau) \in K^\times \setminus K^{\times 2},$$

then the selected formula is K-complete. Thus the theorem is uniform in the base field, but conditional on the existence of admissible selected coefficients. Over a finite field, let χ be its quadratic character, extended by $\chi(0) = 0$. The admissibility condition becomes

$$\chi(\Delta_y(\sigma)) = \chi(\Delta_x(\tau)) = -1.$$

These are not two independent search requirements. If $a = c^2$, choosing $t = cs$ gives $\Delta_x(t) = a\Delta_y(s)$, so either nonsquare test suffices; with $a = 1$, take $s = t$. If a is a nonsquare, fixing $\sigma = (1 : 0)$ leaves only the t-test. The precise reduction is included in Theorem 3.23.

The difference-divisor principle comes from the general theory of addition laws [LR85, LR87, BL95, Koh11, AKR12]. The standard extended-coordinate Edwards formulas come from the Edwards and twisted Edwards literature [Edw07, BL07, BBJLP08, HWCD08, BL11]. Our contribution is the selected single product formula, the discriminant criteria for its exceptional fibres, the finite-field coefficient-selection and existence results, and the operation schedules that show where the known low-cost Edwards level is preserved and what changes in the remaining branches.

More precisely, the main contributions are the following.

(1) Following Kohel's projection framework, we identify the two standard Edwards product representatives with two bases of bidegree $(1, 1)$ addition-law projection spaces in the product-coordinate representation.
(2) We introduce projective selected coefficients

$$\sigma, \tau \in \mathbb{P}^1(K)$$

and use them to choose one section in each of the two projection spaces. Recombining these two selected projections by the Segre map gives a single extended-coordinate formula.
(3) We compute the exceptional fibres of the selected formula explicitly. The exceptional behaviour is controlled by two fibres of the difference point $P - Q$, one selected by σ and one selected by τ.
(4) We derive the homogeneous discriminants

$$\Delta_y(\sigma) = (\sigma_0^2 - \sigma_1^2)(a\sigma_0^2 - d\sigma_1^2),$$

and

$$\Delta_x(\tau) = (\tau_0^2 - a\tau_1^2)(\tau_0^2 - d\tau_1^2),$$

and prove the field-uniform completeness criterion. Although arbitrary coefficient pairs must satisfy both nonsquare conditions, a complete member can be selected using only one condition and a determined companion coefficient.
(5) Over finite fields, we specialize the criterion to quadratic characters and obtain the four square-class branches. The opposite-square-class branches recover the previously known complete Edwards situation and its mirror form, while the same-square-class branches are handled by selecting the exceptional fibres.

(6) We give finite-field coefficient-selection and existence results. The operation-count consequences and concrete schedules are recorded separately only after the selected coefficients and representations have been fixed.

The result also interacts with recent complete-addition constructions on related coordinate models. Farashahi, Fadavi, and Sabbaghian used extended Montgomery coordinates and maps from extended Edwards coordinates to obtain low-cost complete addition laws in Montgomery-type settings [FFS24]. The present paper does not change those maps. It strengthens the Edwards-side source law: the selected formula supplies complete Edwards-type input laws in square-class regimes that were not covered by the previously known one-formula complete Edwards case.

The paper is organized as follows. Section 2 fixes the notation and distinguishes the twisted Edwards curve, its extended-coordinate representation, and the auxiliary product-coordinate model. It also recalls field-completeness, difference divisors, square classes, and the operation-count conventions used later. Section 3 contains the main construction and proof. It first recalls the classical addition-law results of Lange–Ruppert, Bosma–Lenstra, and Kohel that are used in the proof, and then introduces the selected projections, the homogeneous discriminants, and the field-uniform completeness theorem. The finite-field specialization and coefficient-existence result are also given there. Section 4 records the operation schedules and the doubling specialization. Section 5 explains the computational verification protocol and compares the construction with previous complete-addition frameworks. Section 6 concludes with possible extensions and optimization questions.

2. Preliminaries

This section fixes the notation and the geometric conventions used throughout the paper. We distinguish the twisted Edwards curve itself, its extended-coordinate representation, and the auxiliary product-coordinate representation used later to construct the selected formula. We also recall the field-dependent notion of completeness for addition laws, the difference-divisor mechanism behind exceptional pairs, the square-class branches of the parameters, and the operation-count conventions used in the finite-field part of the paper.

The preliminaries collected in this section are standard. The language of regular functions, line bundles, divisors, and fibre divisors follows the usual conventions of algebraic geometry, as in Hartshorne [Har77]; the basic elliptic-curve terminology follows Silverman [Sil09]. The addition-law framework used later is due to Lange–Ruppert, Bosma–Lenstra, Kohel, and Arene–Kohel–Ritzenthaler [LR85, LR87, BL95, Koh11, AKR12]. For Edwards and twisted Edwards models, extended coordinates, and operation count conventions, we use the standard references [Edw07, BL07, BBJLP08, HWCD08, BL11, FFS24]. Only the notation and the specific consequences needed for the proof are recalled here.

2.1. **Fields and square classes.** Unless explicitly stated otherwise, K denotes a field with $\operatorname{char} K \neq 2$, and $\bar{K}$ is an algebraic closure of K. The structural identities and the geometric statements in Section 3 are proved over such a field K. Finite fields enter in the parts of the paper where we use quadratic characters, count admissible coefficients, give operation schedules, and verify the formulas computationally.

For $u \in K^\times$, we write $u \in K^{\times 2}$ to mean that u is a square in K. If $K = \mathbb{F}_q$ is a finite field of odd cardinality, we use $\chi : \mathbb{F}_q \to \{0, \pm 1\}$ for the quadratic character, extended by $\chi(0) = 0$. Thus $\chi(u) = 1$ if and only if $u \in \mathbb{F}_q^{\times 2}$, and $\chi(u) = -1$ if and only if $u \notin \mathbb{F}_q^{\times 2}$.

For an arbitrary field K, the square-class group $K^\times/K^{\times 2}$ may have more than two elements. Therefore, in the field-uniform part of the paper, square-class conditions will be written directly in terms of membership in $K^{\times 2}$ or in its complement $K^\times \setminus K^{\times 2}$. When $K = \mathbb{F}_q$ is a finite field of odd cardinality, there are exactly two square classes. In the finite-field sections we write S for the square class and N for the nonsquare class. Thus the parameters (a, d) fall into the four branches (S, N), (N, S), (N, N), and (S, S). The opposite-square-class case is characterized by $ad \notin K^{\times 2}$, whereas the same-square-class case is characterized by $ad \in K^{\times 2}$. Over finite fields this gives the usual four-branch table, but the field-uniform statements below do not rely on the finite-field notation S, N.

2.2. **Regular functions, line bundles, divisors, and fibres.** We recall the geometric language used later in the proof. The material in this subsection is standard; our conventions follow the usual terminology for varieties, sheaves, line bundles, and divisors on smooth projective curves [Har77, Chapter II]. The purpose is only to fix notation and to make clear how the projective formulas used in the paper should be interpreted.

Let X be an irreducible variety over K. Its structure sheaf is denoted by $\mathcal{O}_X$. For an open set $U \subset X$, the ring $\mathcal{O}_X(U)$ is the ring of regular functions on U. Equivalently, on an irreducible curve one may regard a regular function on U as a rational function which has no pole at any point of U. Thus regularity is a local condition: a rational function may fail to be regular on the whole curve, but become regular after the points where it has poles are removed.

A line bundle on X, or equivalently an invertible sheaf, is a locally free $\mathcal{O}_X$-module of rank one. Concretely, this means that for every point of X there is an open neighbourhood U on which the line bundle looks like a copy of $\mathcal{O}_U$. After choosing a local basis e on such a set U, every local section s can be written uniquely as $s = fe$, with $f \in \mathcal{O}_X(U)$. The section s is intrinsic, while the representing function f depends on the chosen local basis. We write $\Gamma(X, \mathcal{L}) = H^0(X, \mathcal{L})$ for the vector space of global sections of a line bundle $\mathcal{L}$ on X.

This distinction is important for projective models. If $X \subset \mathbb{P}^r$ is a projective variety, then the homogeneous coordinates of $\mathbb{P}^r$ are not ordinary global functions on X. They are global sections of the line bundle $\mathcal{O}_X(1)$. For example, on projective space the coordinates $X_0, \ldots, X_r$ are defined only up to a common nonzero scalar. Hence X_i alone is not a well-defined function on a projective point. Ratios such as X_i/X_j are genuine regular functions only on the affine chart where $X_j \neq 0$. In the extended Edwards representation used later, the homogeneous coordinates X, Y, Z, T should therefore be viewed as the restrictions of homogeneous coordinate sections of $\mathcal{O}_{\mathcal{E}^e_{a,d}}(1)$, whereas ratios such as X/Z, Y/Z, and T/Z are rational functions, regular on the chart $Z \neq 0$.

We also use the standard language of divisors. If C is a smooth projective curve over K, a divisor on C is a finite formal sum $D = \sum_P n_P[P]$, with $n_P \in \mathbb{Z}$, where P runs over closed points of C. The support of D is $|D| = \{P : n_P \neq 0\}$. When we write $D(K) = \emptyset$, we mean that the support of D contains no K-rational point.

If f is a nonzero rational function on C, then $\operatorname{div}(f)$ records the zeros and poles of f, with multiplicity. At a point P, the integer $\operatorname{ord}_P(f)$ is positive if f has a zero at P, negative if f has a pole at P, and zero if f is regular and nonzero at P. Thus $\operatorname{div}(f) = \sum_P \operatorname{ord}_P(f)[P]$. The line bundle associated to a divisor D is denoted by $\mathcal{O}_C(D)$. We write $D' \sim D$ when $D' - D$ is the divisor of a nonzero rational function, and $D' > D$ when $D' - D$ is a nonzero effective divisor.

Finally, if $\varphi : C \to \mathbb{P}^1$ is a morphism and $Q \in \mathbb{P}^1$, then $\varphi^*(Q)$ is the fibre divisor of φ above Q. In this paper the coordinate functions $x, y : E_{a,d} \to \mathbb{P}^1$ give such fibre divisors. Later, the selected coefficients in the addition formula determine particular horizontal and vertical fibres in the auxiliary $\mathbb{P}^1 \times \mathbb{P}^1$ representation. The completeness proof will reduce to showing that those selected fibres have no K-rational points.

2.3. **Addition laws, exceptional divisors, and arithmetic completeness.** Let E/K be an elliptic curve embedded in projective space $E \subset \mathbb{P}^r$. An addition law on this projective model is an $(r+1)$-tuple $\mathfrak{a} = (A_0, \dots, A_r)$ of bihomogeneous polynomials in the coordinates of two input points such that, on a nonempty open subset of $E \times E$, the projective point $(A_0(P,Q) : \cdots : A_r(P,Q))$ represents the group sum $P + Q$. The common degree in the coordinates of the first input and the common degree in the coordinates of the second input form the bidegree of the law. This is the classical framework for addition laws on abelian varieties and elliptic curves developed by Lange–Ruppert, Bosma–Lenstra, Kohel, and Arene–Kohel–Ritzenthaler [LR85, LR87, BL95, Koh11, AKR12].

The line-bundle interpretation is as follows. Suppose that the projective embedding of E is defined by $\mathcal{L} = \mathcal{O}_E(1)$. Let $\mu : E \times E \to E$ be the addition morphism, and let $\pi_1, \pi_2 : E \times E \to E$ be the two projections. In the standard line-bundle interpretation, addition laws of bidegree (m, n) are represented by global sections of $\mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n$ on $E \times E$. This viewpoint explains why the failure locus of an addition law is naturally controlled by divisors.

The exceptional set of an addition law is $\operatorname{Exc}(\mathfrak{a}) = \{(P,Q) \in E \times E : A_0(P,Q) = \cdots = A_r(P,Q) = 0\}$. At such a pair all output coordinates vanish, so the projective point $(A_0(P,Q) : \cdots : A_r(P,Q))$ is not defined. We call such a pair an exceptional pair.

Definition 2.1. An addition law $\mathfrak{a}$ is called K-complete if $\operatorname{Exc}(\mathfrak{a}) \cap (E(K) \times E(K)) = \emptyset$. Equivalently, the same polynomial expression computes the group sum for every pair of K-rational input points.

This is an arithmetic, field-dependent notion. A formula may be K-complete even if it has exceptional pairs over an extension of K. We use the term geometrically complete only when no exceptional pair remains after base change to an algebraic closure. Thus geometric completeness is stronger than K-completeness. Also, completeness is stronger than unification: a unified formula uses the same expression for addition and doubling, but it may still fail at some exceptional pairs. A K-complete formula works for all K-rational pairs, including $P = Q$, $P = -Q$, $P = O$, and $Q = O$.

The group law gives the difference morphism $\delta : E \times E \to E$, $\delta(P,Q) = P - Q$. In the classical theory, exceptional divisors of addition laws are often described as pullbacks from E through this map. For Weierstrass models, Bosma–Lenstra make this explicit: the exceptional pairs of a bidegree $(2,2)$ law are those whose

difference lies on a divisor cut out by a line in the Weierstrass projective plane [BL95]. Kohel formulates the same mechanism for projectively normal embeddings and for addition-law projections [Koh11].

We shall use the following elementary consequence throughout the paper.

Lemma 2.2 (Difference-divisor completeness criterion)**.** *Let* $\mathfrak{a}$ *be an addition law on* E*. Suppose that there is a divisor* D *on* E *such that* $\mathrm{Exc}(\mathfrak{a}) \subseteq \delta^{-1}(|D|)$*. If* $D(K) = \emptyset$*, then* $\mathfrak{a}$ *is* K*-complete.*

Proof. If $(P, Q) \in E(K) \times E(K)$ were exceptional for $\mathfrak{a}$, then $P - Q \in |D|$. But $P - Q \in E(K)$, since $E(K)$ is a group. This would give a K-rational point in $|D|$, contradicting $D(K) = \emptyset$. Hence no K-rational input pair is exceptional. □

The selected Edwards formula constructed later will be analyzed using this criterion. Its exceptional set will be shown to lie over a union of selected horizontal and vertical fibre divisors under the difference map. The discriminant computations then show when these fibres have no K-rational points, giving arithmetic completeness of a single formula over the chosen field.

2.4. **Twisted Edwards curves and extended coordinates.** Let $a, d \in K^\times$ with $a \neq d$. We start from the affine twisted Edwards model

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

Equivalently, $E_{a,d}$ denotes the smooth projective curve associated with this affine model. Twisted Edwards curves were introduced by Bernstein, Birkner, Joye, Lange, and Peters as a generalization of Edwards curves and as a model closely related to Montgomery curves [BBJLP08]. The original Edwards model and its fast arithmetic were developed in [Edw07, BL07].

Following the extended-coordinate representation of Hisil, Wong, Carter, and Dawson [HWCD08], we introduce an auxiliary coordinate T recording the product xy. In the coordinate order used in this paper, the extended-coordinate representation is

$$\mathcal{E}^e_{a,d}: \qquad aX^2 + Y^2 = Z^2 + dT^2, \qquad XY = ZT.$$

This notation denotes the extended-coordinate representation of $E_{a,d}$; it does not denote a new elliptic curve. On the affine chart $Z \neq 0$, the correspondence is $x = X/Z$, $y = Y/Z$, and $T/Z = xy$. Thus the coordinate T is an auxiliary coordinate introduced to improve the structure and cost of the addition formulas.

The neutral element is represented by $O = (0 : 1 : 1 : 0)$, and the inverse of a point is represented by $-(X : Y : Z : T) = (-X : Y : Z : -T)$. All group-law statements for $\mathcal{E}^e_{a,d}$ are to be understood via the underlying twisted Edwards curve $E_{a,d}$.

Remark 2.3 (Product-coordinate viewpoint). The extended equation $XY = ZT$ is the Segre relation. Thus the extended twisted Edwards representation may be viewed through a product $\mathbb{P}^1 \times \mathbb{P}^1$ chart. The selected coefficients used below choose projective fibres in these two $\mathbb{P}^1$-directions.

Remark 2.4. Some references write extended twisted Edwards coordinates in the order $(X : Y : T : Z)$. We use the order $(X : Y : Z : T)$, because it keeps the two equations in the form $aX^2 + Y^2 = Z^2 + dT^2$ and $XY = ZT$. All formulas in the paper follow this convention.

2.5. **The auxiliary product representation.** The terminology "Segre-type" refers to the classical Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ into $\mathbb{P}^3$. Its image is a smooth quadric cut out by one 2×2 determinantal relation. With the coordinate order used in this paper, this relation is $XY = ZT$. Hence the equation $XY = ZT$ in the extended Edwards representation realizes the ambient quadric as a product-type $\mathbb{P}^1 \times \mathbb{P}^1$ geometry. The second equation $aX^2 + Y^2 = Z^2 + dT^2$ then cuts out the twisted Edwards curve inside this Segre-type quadric. This product viewpoint is the reason why the exceptional divisors later appear as horizontal and vertical fibres. The selected formula constructed later is most naturally organized through an auxiliary product representation. Suppose that two projective pairs $(U_x : Z_x)$ and $(U_y : Z_y)$ represent the affine quantities $x_3 = U_x/Z_x$ and $y_3 = U_y/Z_y$. The corresponding extended coordinates are obtained by the Segre-type reconstruction

$$(U_x : Z_x) \times (U_y : Z_y) \longmapsto (U_xZ_y : Z_xU_y : Z_xZ_y : U_xU_y).$$

Indeed, $(U_xZ_y)(Z_xU_y) = (Z_xZ_y)(U_xU_y)$, so the relation $XY = ZT$ is automatically satisfied.

In the main construction, two candidate projective representatives for the output x-coordinate will be combined by a projective coefficient $\sigma \in \mathbb{P}^1(K)$, and the corresponding representatives for the output y-coordinate will be combined by a projective coefficient $\tau \in \mathbb{P}^1(K)$. In an affine chart these coefficients may be written as $\sigma = (s : 1)$ and $\tau = (t : 1)$, but the projective notation is essential because the choices $\sigma = (1 : 0)$ and $\tau = (1 : 0)$ select the complementary representatives without introducing any infinite field element.

2.6. **Square classes and rational two-torsion.** The square class of ad also controls the rational two-torsion of the elliptic curve represented by $E_{a,d}$. This is useful because the new branches covered in this paper are precisely the same-square-class branches. The twisted Edwards curve $E_{a,d}$ is birationally equivalent, and hence isomorphic as a smooth projective curve, to a Montgomery curve of the form

$$Bv^2 = u^3 + Au^2 + u,$$

with $A = 2(a + d)/(a - d)$ and $B = 4/(a - d)$, up to the standard Montgomery–Edwards parameter correspondence [BBJLP08]. The nontrivial two-torsion points on the Montgomery model have $v = 0$, so their u-coordinates are the roots of $u(u^2 + Au + 1) = 0$. The root $u = 0$ is always rational. The other two roots are rational over K if and only if $A^2 - 4 \in K^{\times 2}$. A direct calculation gives $A^2 - 4 = 16ad/(a-d)^2$. Since 16 and $(a-d)^2$ are squares, this is a square in K if and only if $ad \in K^{\times 2}$. Consequently, in the opposite-square-class regime $ad \notin K^{\times 2}$, the curve has only one nontrivial rational point of order two. In the same-square-class regime $ad \in K^{\times 2}$, it has full rational two-torsion, namely $E_{a,d}(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where $E_{a,d}(K)[2] = \{P \in E_{a,d}(K) : 2P = O\}$. Over a finite field this gives the table

branch	$(\chi(a), \chi(d))$	$\chi(ad)$	$E_{a,d}(\mathbb{F}_q)[2]$
(S, N)	$(+1, -1)$	-1	$\mathbb{Z}/2\mathbb{Z}$
(N, S)	$(-1, +1)$	-1	$\mathbb{Z}/2\mathbb{Z}$
(N, N)	$(-1, -1)$	$+1$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(S, S)	$(+1, +1)$	$+1$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Thus the same-square-class branches are not a minor variant of the usual complete Edwards case. They correspond to a different rational two-torsion structure, and they are the main new cases treated by the selected formula.

2.7. **Operation-count conventions.** The schedules apply over the stated base field; quadratic-character selection tests are specialized to finite fields. We follow the standard notation of the explicit-formula literature for Edwards and Montgomery arithmetic [HWCD08, FFS24]. The symbol M denotes a general multiplication in the base field, and S denotes a squaring. If $c \in K$ is a fixed constant, we write D_c for multiplication by c. In particular, we use D_a, D_d, D_s, and D_t for multiplications by the curve constants and by the selected coefficients. When the constant is left unspecified, D denotes one fixed-constant multiplication.

The selected coefficients in the main construction are projective parameters $\sigma, \tau \in \mathbb{P}^1(K)$. When they lie in the affine chart $\sigma = (s : 1)$ and $\tau = (t : 1)$, we write D_s and D_t for multiplication by the fixed constants s and t. These coefficients are chosen before the online group operation begins, so their selection cost is not included in the online addition cost. If $\sigma = (1 : 0)$ or $\tau = (1 : 0)$, there is no multiplication by an infinite element; the formula simply selects the corresponding complementary projection pair. Thus the operation count must always be read together with the chosen projective chart.

3. Product Laws and the Selected Formula

The goal of this section is to construct the selected product formula and to prove the field-uniform completeness criterion used in the rest of the paper. We begin from two known product representatives in extended twisted Edwards coordinates. These representatives belong to the standard extended-coordinate Edwards framework of Hisil, Wong, Carter, and Dawson and to the complete-system viewpoint for Edwards addition laws [HWCD08, BL11, EFD]. We choose one projective linear combination in each of the two product-coordinate projection spaces and then recombine the selected projections by the Segre reconstruction.

The section proceeds as follows. First we fix the bilinear blocks and recall the standard and complementary product representatives. We then explain the classical addition-law results that justify interpreting these representatives as addition-law projections. Next we introduce projective selection coefficients $\sigma, \tau \in \mathbb{P}^1(K)$ and define the selected formula $\Psi_{\sigma,\tau}$. Finally, we analyze its exceptional locus through the difference-divisor criterion. The resulting homogeneous discriminants give an exact condition for K-completeness, and over finite fields this becomes a quadratic-character condition leading to the branch and coefficient-existence results below.

Throughout this section K is a field with $\operatorname{char} K \neq 2$, and $a, d \in K^\times$ with $a \neq d$. The input points are $P_i = (X_i : Y_i : Z_i : T_i) \in \mathcal{E}^e_{a,d}(K)$, for $i = 1, 2$.

3.1. **Known product representatives.** Define the eight bilinear blocks

$$\begin{aligned} E &= X_1Y_2 + Y_1X_2, & R &= Y_1X_2 - X_1Y_2, \\ H &= Y_1Y_2 - aX_1X_2, & W &= Y_1Y_2 + aX_1X_2, \\ F &= Z_1Z_2 - dT_1T_2, & G &= Z_1Z_2 + dT_1T_2, \\ N &= Z_1T_2 - T_1Z_2, & V &= Z_1T_2 + T_1Z_2. \end{aligned}$$

The pairs (E, R) and (H, W) come from the X, Y-coordinates, while (F, G) and (N, V) come from the Z, T-coordinates.

With this notation, the two known product representatives are

$$\Phi_{\mathrm{std}}(P_1, P_2) = (EF : GH : GF : EH),$$
$$\Phi_{\mathrm{comp}}(P_1, P_2) = (RV : WN : RW : NV).$$

The standard representative corresponds to the product-coordinate projections $(E : G)$ and $(H : F)$, so that, where defined, $x(P_1 + P_2) = E/G$ and $y(P_1 + P_2) = H/F$. The complementary representative corresponds to the projections $(V : W)$ and $(N : R)$, giving the same sum through $x(P_1 + P_2) = V/W$ and $y(P_1 + P_2) = N/R$. The identities $VG = EW$ and $NF = HR$ express the equality of these two x- and y-projections wherever the corresponding pairs are defined.

These four projective projections,

$$(E : G), \qquad (V : W), \qquad (H : F), \qquad (N : R),$$

are the input data for the selected construction. The selected formula below will choose one projective linear combination in the x-projection space and one in the y-projection space, then reconstruct an extended-coordinate output by the Segre product.

3.2. **Classical addition-law results used in the proof.** We recall the classical addition-law results used in the completeness proof. Here k denotes the base field and $\bar{k}$ an algebraic closure of k. Lange–Ruppert give the line-bundle interpretation of addition laws and complete systems. Bosma–Lenstra make the exceptional divisors explicit for Weierstrass models. Kohel then extends the same difference-divisor mechanism to projectively normal embeddings and, crucially for us, to addition-law projections.

The projection spaces and their basis elements in the Edwards product model are due to Kohel; the field-dependent selected projective combinations and the homogeneous discriminants below are the contribution of the present construction.

Theorem 3.1 (Lange–Ruppert: addition laws as sections)**.** *Let A/k be an abelian variety with a projective embedding $\iota : A \to \mathbb{P}^r$ defined by an invertible sheaf $\mathcal{L} = \mathcal{O}_A(1)$. Let $\mu : A \times A \to A$ be the addition morphism, and let $\pi_1, \pi_2 : A \times A \to A$ be the two projections. In the projectively normal setting used below, addition laws of bidegree (m, n) are represented by nonzero global sections of $\mathcal{M}_{m,n} = \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n$. The exceptional set of a nonzero addition law is the support of the corresponding exceptional divisor on $A \times A$.*

The preceding theorem explains why completeness is naturally a question about base loci and divisors. The next result is the classical low-bidegree existence theorem of Lange–Ruppert. We state it in the form used by Kohel; in the original formulation the embedding is induced by a complete linear system associated with a sufficiently high power of an ample line bundle.

Theorem 3.2 (Lange–Ruppert: complete systems in low bidegree)**.** *Let A be embedded projectively normally by $\mathcal{L} = \mathcal{O}_A(1)$. The set of addition laws of bidegrees $(2, 3)$ and $(3, 2)$ is geometrically complete. If $\mathcal{L}$ is symmetric, then the set of addition laws of bidegree $(2, 2)$ is geometrically complete. If $\mathcal{L}$ is not symmetric, then there is no addition law of bidegree $(2, 2)$.*

For elliptic curves in Weierstrass form, Bosma and Lenstra sharpen the general existence statement. They prove that a complete system of minimal size has two

laws and then describe the exceptional pairs of every nonzero bidegree $(2,2)$ law explicitly.

Theorem 3.3 (Bosma–Lenstra: minimal complete systems on Weierstrass models)**.** *Let E/k be an elliptic curve given in Weierstrass form. The smallest cardinality of a complete system of addition laws on E is two. Moreover, if two addition laws form a complete system, then both of them have bidegree $(2,2)$.*

The next theorem is the precise point of contact with the divisor method used later.

Theorem 3.4 (Bosma–Lenstra: point parametrization and line criterion)**.** *Let E/k be an elliptic curve in Weierstrass form in $\mathbb{P}^2$. There is a bijection between $\mathbb{P}^2(k)$ and the set of equivalence classes of nonzero addition laws of bidegree $(2,2)$ on E. Let $(a:b:c)\in\mathbb{P}^2(k)$ correspond to such an addition law. For any extension field K/k and any $P_1,P_2\in E(K)$, the pair (P_1,P_2) is exceptional for this law if and only if the difference P_1-P_2 lies in the intersection of $E(K)$ with the line $aX+bY+cZ=0$ in the Weierstrass projective plane $\mathbb{P}^2(K)$.*

Thus Bosma–Lenstra parametrize bidegree $(2,2)$ laws by points of $\mathbb{P}^2(k)$, but the exceptional divisor is the pullback, under the difference morphism, of the intersection of the curve with the corresponding line. Kohel abstracts this mechanism away from the Weierstrass plane model.

Theorem 3.5 (Kohel: bidegree $(2,2)$ laws and the difference morphism)**.** *Let $\iota: E\to\mathbb{P}^r$ be a projectively normal embedding of an elliptic curve with respect to a symmetric sheaf $\mathcal{L}=\mathcal{O}_E(1)\simeq\mathcal{O}_E(D)$. Let $\mathcal{M}=\mu^*\mathcal{L}^{-1}\otimes\pi_1^*\mathcal{L}^2\otimes\pi_2^*\mathcal{L}^2$. Then the difference morphism induces an isomorphism $\Gamma(E,\mathcal{L})\cong\Gamma(E\times E,\mathcal{M})$. Moreover, if the divisor cut out by a section of $\Gamma(E,\mathcal{L})$ is written over $\bar{k}$ as $D'=\sum_i(P_i)$, with $D'\sim D$, then the exceptional divisor of the corresponding bidegree $(2,2)$ addition law on $E\times E$ is $\sum_i\Delta_{P_i}$, where $\Delta_P=\{(Q,R)\in E\times E:\ Q-R=P\}$.*

The previous theorem identifies the components of the exceptional divisor. The following reformulation is the form needed later.

Corollary 3.6 (Kohel: exceptional divisors are pullbacks). Let $\mathfrak{a}$ be a nonzero addition law of bidegree $(2,2)$ on E, and let $\mathrm{ExcDiv}(\mathfrak{a})$ be its exceptional divisor on $E\times E$. Let $D_{\mathfrak{a}}$ be the divisor on E determined by $\mathrm{ExcDiv}(\mathfrak{a})\cap(E\times\{O\})=D_{\mathfrak{a}}\times\{O\}$. Then $\mathrm{ExcDiv}(\mathfrak{a})=\delta^*(D_{\mathfrak{a}})$, where $\delta: E\times E\to E$ is the difference morphism $\delta(P,Q)=P-Q$.

This turns arithmetic completeness into a descent problem: the law may have exceptional pairs over an algebraic closure, but it is complete over the base field if the corresponding exceptional divisor has no rational point over that field.

Corollary 3.7 (Kohel: arithmetic completeness criterion). Under the hypotheses of Theorem 3.5, let $\mathrm{ExcDiv}(\mathfrak{a})=\delta^*D_{\mathfrak{a}}$. Then $\mathfrak{a}$ is k-complete if and only if the support of $D_{\mathfrak{a}}$ has no k-rational point [Koh11, Corollary 12]. Equivalently, no point P_i in its geometric support is k-rational. If that support is separable over k, in particular if k is perfect, this is also equivalent to the absence of a geometrically irreducible k-component of the exceptional divisor.

Lemma 3.8 (Difference-divisor descent criterion)**.** *Let K be a field, let E/K be an elliptic curve, and let $\delta: E\times E\to E$, $\delta(P,Q)=P-Q$, be the difference morphism.*

Let $\mathfrak{a}$ be an addition law on E. Suppose that there is a divisor D on E such that $\mathrm{Exc}(\mathfrak{a}) \subseteq \delta^{-1}(|D|)$. If $|D| \cap E(K) = \emptyset$, then $\mathfrak{a}$ is K-complete.

Proof. If $(P, Q) \in E(K) \times E(K)$ were exceptional for $\mathfrak{a}$, then $P - Q \in |D|$. Since $P - Q \in E(K)$, this would give a K-rational point in $|D|$, contradicting $|D| \cap E(K) = \emptyset$. Hence no K-rational pair is exceptional. □

The preceding results concern full addition laws. For the Edwards product geometry, it is more efficient to first study projections of the sum to $\mathbb{P}^1$-coordinates. Kohel's addition-law projections provide the formalism for doing this.

Definition 3.9 (Kohel: addition-law projection)**.** Let $E \to \mathbb{P}^r$ be projectively normally embedded by $\mathcal{L} = \mathcal{O}_E(1)$, and let $\varphi : E \to C \subset \mathbb{P}^s$ be a morphism with $\mathcal{L}_\varphi = \varphi^* \mathcal{O}_C(1)$. An addition-law projection for $\varphi \circ \mu : E \times E \to C$ of bidegree (m, n) is represented by a nonzero section of

$$\mathcal{M}_{\varphi,m,n} = \mu^* \mathcal{L}_\varphi^{-1} \otimes \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n.$$

The case needed for the product-coordinate Edwards model is the critical bidegree $(1, 1)$.

Theorem 3.10 (Kohel: bidegree $(1,1)$ projection theorem)**.** *Let $\iota : E \to \mathbb{P}^r$ be a projectively normal embedding with respect to a symmetric sheaf $\mathcal{L} = \mathcal{O}_E(1) \simeq \mathcal{O}_E(D)$, and let $\varphi : E \to C \subset \mathbb{P}^s$ be a nonconstant morphism with respect to a symmetric sheaf $\mathcal{L}_\varphi \simeq \mathcal{O}_E(D_\varphi)$. Assume that $D > D_\varphi > 0$ and $\deg D = 2 \deg D_\varphi$. Then the space of bidegree $(1,1)$ addition-law projections is isomorphic to $\Gamma(E, \mathcal{L} \otimes \mathcal{L}_\varphi^{-1})$. If a section of this complementary line bundle cuts out $D' = \sum_i (P_i)$, with $D' \sim D - D_\varphi$, the corresponding exceptional divisor is $\delta^* D' = \sum_i \Delta_{P_i}$* [Koh11, Theorem 26].

The next elementary consequence is the vector-space rule for affine addition-law projections used later. It is the projective version of the linear structure described by Kohel.

Lemma 3.11 (Vector-space rule for affine projections)**.** *Let z be an affine coordinate function on an affine model of E. Suppose that two addition-law projections represent $\mu^*(z)$ in the form f/g and f'/g'. Thus, on their common domain of definition, $f/g = f'/g' = \mu^*(z)$. Then, for any $\alpha, \beta \in k$, the projective pair $(\alpha f + \beta f' : \alpha g + \beta g')$ also represents the same coordinate $\mu^*(z)$, wherever it is not the zero pair.*

Kohel's projection theory gives the following bases for the Edwards product model.

Theorem 3.12 (Kohel: Edwards projection bases)**.** *In Kohel's product-coordinate Edwards setting, the two bidegree $(1,1)$ projection spaces have bases $\{s_0, s_1\}$ and $\{t_0, t_1\}$. For input points $\mathbf{X} = (X_0 : X_1 : X_2 : X_3)$ and $\mathbf{Y} = (Y_0 : Y_1 : Y_2 : Y_3)$ in Kohel's coordinates, one may take*

$$s_0 = (X_0Y_3 + X_3Y_0,\ aX_1Y_1 + X_2Y_2), \quad s_1 = (X_1Y_2 + X_2Y_1,\ dX_0Y_0 + X_3Y_3),$$
$$t_0 = (X_0Y_3 - X_3Y_0,\ X_1Y_2 - Y_1X_2), \quad t_1 = (aX_1Y_1 - X_2Y_2,\ dX_0Y_0 - X_3Y_3).$$

Their exceptional divisors are respectively $\Delta_{T_1} + \Delta_{-T_1}$, $\Delta_{T_2} + \Delta_{-T_2}$, $\Delta_O + \Delta_{2T_1}$, and $\Delta_{T_1+T_2} + \Delta_{T_1-T_2}$. Choosing $\alpha, \beta \in \bar{K}$ with $\alpha^2 = a$ and $\beta^2 = d$, the points $T_1 = (0 : 1 : 0 : \alpha)$ and $T_2 = (1 : 0 : \beta : 0)$ have order four in Kohel's coordinate

order, and $2T_1 = 2T_2 = (0 : 0 : -1 : 1)$ [Koh11, Theorem 39]. *These torsion-point labels are local to this statement.*

Under the Segre embedding, these projection pairs give factored full addition laws.

Corollary 3.13 (Kohel: Segre products of projection bases). Let $\varphi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ be the Segre embedding. The space of bidegree $(2,2)$ addition laws for the corresponding Edwards model in $\mathbb{P}^3$ is spanned by the four factored laws $\varphi(s_i, t_j)$, $0 \le i, j \le 1$.

Kohel also determines when the individual basis projections are already arithmetically complete. This explains why the standard complete Edwards case only covers part of the square-class picture.

Theorem 3.14 (Kohel: arithmetic completeness of the basis projections)**.** *In Kohel's twisted Edwards setting, the projections* s_0, s_1, *and* t_1 *are arithmetically complete if and only if* a, d, *and* ad, *respectively, are nonsquares in the base field. In particular, over a finite field, either zero or two of* s_0, s_1, *and* t_1 *are arithmetically complete.*

We choose projective linear combinations of these basis projections to move the exceptional fibres away from the rational points over the base field.

3.3. **Selected projections and field-uniform completeness.** We keep the notation of Subsection 3.1.

Thus K is a field with $\operatorname{char} K \neq 2$, $a, d \in K^\times$ with $a \neq d$, and $P_i = (X_i : Y_i : Z_i : T_i) \in \mathcal{E}^e_{a,d}(K)$, for $i = 1, 2$.

The first step is to translate Kohel's projection bases into the extended Edwards product blocks used in the selected formula.

Lemma 3.15 (Identification of Kohel bases with extended Edwards blocks)**.** *Under the coordinate identification*

$$(X_0 : X_1 : X_2 : X_3)_{\text{Kohel}} = (T : X : Y : Z),$$

Kohel's two projection bases become, up to common nonzero scalar factors and common signs,

$$s_1 = (E : G), \qquad s_0 = (V : W), \qquad t_1 = (H : F), \qquad t_0 = (N : R).$$

The pairs in each projection space represent the same coordinate of the group sum: $E/G = V/W$ *and* $H/F = N/R$ *on their common domains of definition. Equivalently, the block identities* $VG = EW$ *and* $NF = HR$ *hold on* $\mathcal{E}^e_{a,d} \times \mathcal{E}^e_{a,d}$.

Proof. Kohel's Segre coordinates are $(X_0 : X_1 : X_2 : X_3) = (T : X : Y : Z)$. For the first input point we substitute $(X_0, X_1, X_2, X_3) = (T_1, X_1, Y_1, Z_1)$. For the second input point, to avoid conflict with our Y-coordinate notation, write Kohel's second-input coordinates as $(Y_0^K, Y_1^K, Y_2^K, Y_3^K)$, and substitute

$$(Y_0^K, Y_1^K, Y_2^K, Y_3^K) = (T_2, X_2, Y_2, Z_2).$$

Then Kohel's basis elements give

$$\begin{aligned}
s_0 &= (T_1Z_2 + Z_1T_2,\ aX_1X_2 + Y_1Y_2) = (V : W),\\
s_1 &= (X_1Y_2 + Y_1X_2,\ dT_1T_2 + Z_1Z_2) = (E : G),\\
t_0 &= (T_1Z_2 - Z_1T_2,\ X_1Y_2 - Y_1X_2) = (-N : -R) = (N : R),\\
t_1 &= (aX_1X_2 - Y_1Y_2,\ dT_1T_2 - Z_1Z_2) = (-H : -F) = (H : F).
\end{aligned}$$

The identities $VG = EW$ and $NF = HR$ express the fact that the two representatives in each projection space define the same addition-law projection. □

We now introduce the selected projections. The selected coefficients are projective parameters, not necessarily affine field elements.

Definition 3.16 (Selected projective projections)**.** Let $\sigma = (\sigma_0 : \sigma_1) \in \mathbb{P}^1(K)$ and $\tau = (\tau_0 : \tau_1) \in \mathbb{P}^1(K)$. Define the selected x-projection and y-projection by

$$S_\sigma = \sigma_1 s_1 + \sigma_0 s_0 = (\sigma_1 E + \sigma_0 V : \sigma_1 G + \sigma_0 W),$$

and

$$T_\tau = \tau_1 t_1 + \tau_0 t_0 = (\tau_1 H + \tau_0 N : \tau_1 F + \tau_0 R).$$

Writing $S_\sigma = (A_\sigma : B_\sigma)$ and $T_\tau = (C_\tau : D_\tau)$, define the selected Segre formula by

$$\Psi_{\sigma,\tau}(P_1, P_2) = (A_\sigma D_\tau :\ B_\sigma C_\tau :\ B_\sigma D_\tau :\ A_\sigma C_\tau).$$

Remark 3.17 (Affine notation). If $\sigma_1 \neq 0$, one may write $s = \sigma_0/\sigma_1 \in K$, and then $S_\sigma = (E + sV : G + sW)$. The value $s = \infty$ is shorthand for $\sigma = (1 : 0)$, in which case $S_\sigma = (V : W)$. Similarly, if $\tau_1 \neq 0$, one may write $t = \tau_0/\tau_1 \in K$, and then $T_\tau = (H + tN : F + tR)$, whereas $t = \infty$ means $\tau = (1 : 0)$, giving $T_\tau = (N : R)$. Thus no multiplication by an infinite field element is involved.

Theorem 3.18 (Correctness of the selected Segre product)**.** *If $S_\sigma(P_1, P_2) \neq (0 : 0)$ and $T_\tau(P_1, P_2) \neq (0 : 0)$, then $\Psi_{\sigma,\tau}(P_1, P_2)$ lies on $\mathcal{E}^e_{a,d}$ and represents the group sum $P_1 + P_2$.*

Proof. By Lemma 3.15, the pairs $(E : G)$ and $(V : W)$ represent the same x-projection of $P_1 + P_2$. Therefore every nonzero projective linear combination of them represents the same x-projection. Thus S_σ, when nonzero, represents the x-coordinate of the sum.

Similarly, $(H : F)$ and $(N : R)$ represent the same y-projection of $P_1 + P_2$. Hence T_τ, when nonzero, represents the y-coordinate of the sum.

The Segre reconstruction

$$(A : B) \times (C : D) \longmapsto (AD : BC : BD : AC)$$

is exactly the extended-coordinate reconstruction in the coordinate order $(X : Y : Z : T)$: it gives $X/Z = A/B$, $Y/Z = C/D$, and $T/Z = (A/B)(C/D)$ wherever these affine ratios are defined, and it gives the corresponding projective point in general. Therefore $\Psi_{\sigma,\tau}(P_1, P_2)$ lies on $\mathcal{E}^e_{a,d}$ and represents $P_1 + P_2$. □

We next determine when the selected projection pairs can vanish. This converts the exceptional set of the selected formula into fibre conditions on the difference point. Use auxiliary product coordinates $x = (\mathsf{X}_0 : \mathsf{X}_1)$ and $y = (\mathsf{Y}_0 : \mathsf{Y}_1)$ on $\mathbb{P}^1 \times \mathbb{P}^1$. In these coordinates the product model of $E_{a,d}$ is

$$a\mathsf{X}_0^2\mathsf{Y}_1^2 + \mathsf{X}_1^2\mathsf{Y}_0^2 = \mathsf{X}_1^2\mathsf{Y}_1^2 + d\mathsf{X}_0^2\mathsf{Y}_0^2.$$

For $\sigma = (\sigma_0 : \sigma_1) \in \mathbb{P}^1(K)$, define the selected y-fibre $\mathcal{Y}_\sigma : \sigma_0\mathsf{Y}_0 + \sigma_1\mathsf{Y}_1 = 0$. For $\tau = (\tau_0 : \tau_1) \in \mathbb{P}^1(K)$, define the selected x-fibre $\mathcal{X}_\tau : \tau_0\mathsf{X}_0 - \tau_1\mathsf{X}_1 = 0$. These fibres are understood on the product model of $E_{a,d}$.

Lemma 3.19 (Selected projections and fibres)**.** *With the product-coordinate convention $x = (\mathsf{X}_0 : \mathsf{X}_1)$ and $y = (\mathsf{Y}_0 : \mathsf{Y}_1)$, the selected x-projection $S_\sigma = (\sigma_1 E + \sigma_0 V : \sigma_1 G + \sigma_0 W)$ has exceptional divisor pulled back from the fibre $\mathcal{Y}_\sigma : \sigma_0\mathsf{Y}_0 + \sigma_1\mathsf{Y}_1 = 0$ of the difference point. Similarly, the selected y-projection $T_\tau = (\tau_1 H + \tau_0 N : \tau_1 F + \tau_0 R)$ has exceptional divisor pulled back from the fibre $\mathcal{X}_\tau : \tau_0\mathsf{X}_0 - \tau_1\mathsf{X}_1 = 0$ of the difference point. Consequently,*

$$\mathrm{Exc}(S_\sigma) \subseteq \delta^{-1}(|\mathcal{Y}_\sigma|), \qquad \mathrm{Exc}(T_\tau) \subseteq \delta^{-1}(|\mathcal{X}_\tau|).$$

Proof. Let $\mathcal{L}_x = x^*\mathcal{O}_{\mathbb{P}^1}(1)$ and $\mathcal{L}_y = y^*\mathcal{O}_{\mathbb{P}^1}(1)$. Both have degree two, are symmetric under negation, and satisfy $\mathcal{O}_E(1) \simeq \mathcal{L}_x \otimes \mathcal{L}_y$ by the Segre embedding. Thus the complementary bundles in Theorem 3.10 are $\mathcal{L}_y$ for the x-projection and $\mathcal{L}_x$ for the y-projection. The degree-four embedding is projectively normal.

To identify the sections, restrict to $E \times \{O\}$, where δ is the identity, and write

$$P = (\mathsf{X}_0\mathsf{Y}_1 : \mathsf{X}_1\mathsf{Y}_0 : \mathsf{X}_1\mathsf{Y}_1 : \mathsf{X}_0\mathsf{Y}_0).$$

Substitution of $O = (0 : 1 : 1 : 0)$ in the bilinear blocks gives

$$S_\sigma(P, O) = (\sigma_1\mathsf{Y}_1 + \sigma_0\mathsf{Y}_0)(\mathsf{X}_0, \mathsf{X}_1),$$
$$T_\tau(P, O) = (\tau_1\mathsf{X}_1 - \tau_0\mathsf{X}_0)(\mathsf{Y}_0, \mathsf{Y}_1).$$

The two projective coordinate pairs are nonzero everywhere. Consequently their common-zero divisors, including multiplicities and projective boundary points, are precisely $\mathcal{Y}_\sigma$ and $\mathcal{X}_\tau$. The selected sections are nonzero because the generators are bases. The cited projection theorem therefore gives

$$\mathrm{ExcDiv}(S_\sigma) = \delta^*\mathcal{Y}_\sigma, \qquad \mathrm{ExcDiv}(T_\tau) = \delta^*\mathcal{X}_\tau,$$

which proves the stated containments as well. □

Theorem 3.20 (Exceptional fibre containment)**.** *Let $\delta : E_{a,d} \times E_{a,d} \to E_{a,d}$ be the difference morphism $\delta(P_1, P_2) = P_1 - P_2$. For the selected formula $\Psi_{\sigma,\tau}$, one has*

$$\mathrm{Exc}(\Psi_{\sigma,\tau}) \subseteq \delta^{-1}\big(|\mathcal{Y}_\sigma| \cup |\mathcal{X}_\tau|\big).$$

Proof. The selected Segre formula is undefined only if at least one of the selected projection pairs vanishes, namely if $S_\sigma(P_1, P_2) = (0 : 0)$ or $T_\tau(P_1, P_2) = (0 : 0)$. By Lemma 3.19, the first condition implies $P_1 - P_2 \in |\mathcal{Y}_\sigma|$, and the second implies $P_1 - P_2 \in |\mathcal{X}_\tau|$. Therefore every exceptional pair lies in $\delta^{-1}\big(|\mathcal{Y}_\sigma| \cup |\mathcal{X}_\tau|\big)$. □

The next theorem converts the fibre condition into explicit square-class conditions.

Theorem 3.21 (Homogeneous discriminants of selected fibres)**.** *Let $\sigma = (\sigma_0 : \sigma_1) \in \mathbb{P}^1(K)$ and $\tau = (\tau_0 : \tau_1) \in \mathbb{P}^1(K)$. Define*

$$\Delta_y(\sigma) = (\sigma_0^2 - \sigma_1^2)(a\sigma_0^2 - d\sigma_1^2), \qquad \Delta_x(\tau) = (\tau_0^2 - a\tau_1^2)(\tau_0^2 - d\tau_1^2).$$

Then the selected fibre $\mathcal{Y}_\sigma$ has no K-rational point on the product model if and only if $\Delta_y(\sigma) \in K^\times \setminus K^{\times 2}$, and $\mathcal{X}_\tau$ has no K-rational point on the product model if and only if $\Delta_x(\tau) \in K^\times \setminus K^{\times 2}$. Moreover, the square classes of $\Delta_y(\sigma)$ and $\Delta_x(\tau)$ are independent of the chosen homogeneous representatives of σ and τ.

Proof. The fibre $\mathcal{Y}_\sigma$ is defined by $\sigma_0\mathsf{Y}_0 + \sigma_1\mathsf{Y}_1 = 0$, so we may write $(\mathsf{Y}_0 : \mathsf{Y}_1) = (-\sigma_1 : \sigma_0)$. Substituting this into the product equation gives

$$(a\sigma_0^2 - d\sigma_1^2)\mathsf{X}_0^2 = (\sigma_0^2 - \sigma_1^2)\mathsf{X}_1^2.$$

We use the elementary criterion that a binary projective equation $AU^2 = BV^2$ has no K-rational point in $\mathbb{P}^1(K)$ if and only if $AB \in K^\times \setminus K^{\times 2}$. Indeed, if $A = 0$ or $B = 0$, then the equation has the rational solution $(1 : 0)$ or $(0 : 1)$, respectively. If $A, B \neq 0$, then a solution exists if and only if $B/A \in K^{\times 2}$, which is equivalent to $AB \in K^{\times 2}$. This proves the criterion for $\mathcal{Y}_\sigma$.

Similarly, the fibre $\mathcal{X}_\tau$ is defined by $\tau_0\mathsf{X}_0 - \tau_1\mathsf{X}_1 = 0$, so $(\mathsf{X}_0 : \mathsf{X}_1) = (\tau_1 : \tau_0)$. Substitution gives

$$(\tau_0^2 - d\tau_1^2)\mathsf{Y}_0^2 = (\tau_0^2 - a\tau_1^2)\mathsf{Y}_1^2,$$

and the same binary-projective criterion gives the statement for $\mathcal{X}_\tau$.

Finally, replacing σ by $\lambda\sigma$ multiplies $\Delta_y(\sigma)$ by λ^4, and replacing τ by $\mu\tau$ multiplies $\Delta_x(\tau)$ by μ^4. Since fourth powers are squares, the square classes are independent of the chosen representatives. □

Definition 3.22 (Admissible selected coefficients)**.** We say that $(\sigma, \tau) \in \mathbb{P}^1(K) \times \mathbb{P}^1(K)$ is K-admissible for $\mathcal{E}^e_{a,d}$ if

$$\Delta_y(\sigma) \in K^\times \setminus K^{\times 2}, \qquad \Delta_x(\tau) \in K^\times \setminus K^{\times 2}.$$

Theorem 3.23 (Field-uniform completeness criterion)**.** *Let K be any field with $\operatorname{char} K \neq 2$, and let $a, d \in K^\times$, $a \neq d$. The selected formula $\Psi_{\sigma,\tau}$ is K-complete on $\mathcal{E}^e_{a,d}$ if and only if σ, τ are K-admissible. Equivalently, it is defined and gives the group sum for every rational input pair if and only if both homogeneous discriminants are nonzero nonsquares in K. Moreover, a complete member exists if and only if there is a finite $t \in K$ such that $(t^2 - a)(t^2 - d)$ is a nonzero nonsquare. Given such a t, take $s = t/c$ if $a = c^2$, and $\sigma = (1 : 0)$ if a is a nonsquare.*

Proof. By Theorem 3.18, the selected formula represents the correct group sum whenever both selected projection pairs are nonzero. By Theorem 3.20,

$$\operatorname{Exc}(\Psi_{\sigma,\tau}) \subseteq \delta^{-1}\big(|\mathcal{Y}_\sigma| \cup |\mathcal{X}_\tau|\big).$$

Since (σ, τ) is K-admissible, Theorem 3.21 gives $\mathcal{Y}_\sigma(K) = \emptyset$ and $\mathcal{X}_\tau(K) = \emptyset$. If $P_1, P_2 \in E_{a,d}(K)$, then $P_1 - P_2 \in E_{a,d}(K)$. Hence $P_1 - P_2$ cannot lie on either selected exceptional fibre. Therefore no pair of K-rational input points is exceptional, and the formula is defined and correct on all K-rational pairs. Conversely, if either discriminant is zero or a square, its fibre has a K-rational point P by Theorem 3.21. The calculation at (P, O) in Lemma 3.19 shows that the corresponding selected pair vanishes. All four Segre output coordinates then vanish, so the law is not K-complete.

For the selection assertion, $\Delta_x(1 : 0) = 1$, so an admissible τ is finite. If $a = c^2$, direct substitution gives $\Delta_x(t) = a\Delta_y(t/c)$; since a is a square, the two discriminants have the same square class. If a is a nonsquare, $\Delta_y(1 : 0) = a$ already supplies the other condition. □

Remark 3.24 (Field dependence of completeness). The preceding theorem is uniform in the base field K, but it is conditional on the existence of K-admissible selected coefficients. This dependence is unavoidable. If K is quadratically closed,

then $K^\times = K^{\times 2}$, so no nonzero discriminant can lie in $K^\times \setminus K^{\times 2}$. Thus the theorem is an arithmetic completeness theorem over a given base field, not a claim of geometric completeness over an algebraic closure.

Proposition 3.25 (Elementary admissible choices over an arbitrary field). Let K be a field with $\operatorname{char} K \neq 2$, and let $a, d \in K^\times$, $a \neq d$. Then the following hold.

(1) The choice $\sigma = (0:1)$, $\tau = (0:1)$ is K-admissible if and only if $d \in K^\times \setminus K^{\times 2}$ and $ad \in K^\times \setminus K^{\times 2}$.
(2) The choice $\sigma = (1:0)$, $\tau = (0:1)$ is K-admissible if and only if $a \in K^\times \setminus K^{\times 2}$ and $ad \in K^\times \setminus K^{\times 2}$.
(3) More generally, for any $\sigma, \tau \in \mathbb{P}^1(K)$, the selected formula is K-complete whenever $\Delta_y(\sigma), \Delta_x(\tau) \in K^\times \setminus K^{\times 2}$.

Proof. The identities

$$\Delta_y(0:1) = d, \qquad \Delta_y(1:0) = a, \qquad \Delta_x(0:1) = ad$$

give the first two assertions. The final assertion is Theorem 3.23. □

3.4. **Finite-field specialization.** We now specialize the field-uniform criterion to finite fields. This is not needed for the proof of the general K-completeness theorem; it turns admissibility into a quadratic-character test and gives existence results for selected coefficients.

Let $K = \mathbb{F}_q$, with q odd, and let χ be the quadratic character, extended by $\chi(0) = 0$.

Corollary 3.26 (Finite-field character criterion). If $\chi(\Delta_y(\sigma)) = -1$ and $\chi(\Delta_x(\tau)) = -1$, then $\Psi_{\sigma,\tau}$ is $\mathbb{F}_q$-complete.

Proof. The conditions $\chi(\Delta_y(\sigma)) = -1$ and $\chi(\Delta_x(\tau)) = -1$ are equivalent to $\Delta_y(\sigma), \Delta_x(\tau) \in K^\times \setminus K^{\times 2}$. The result follows from Theorem 3.23. □

Proposition 3.27 (Finite-field branch consequences). Let $K = \mathbb{F}_q$, with q odd. Then the following hold.

(1) If $(\chi(a), \chi(d)) = (+1, -1)$, then $\sigma = (0:1)$, $\tau = (0:1)$ gives an $\mathbb{F}_q$-complete selected formula.
(2) If $(\chi(a), \chi(d)) = (-1, +1)$, then $\sigma = (1:0)$, $\tau = (0:1)$ gives an $\mathbb{F}_q$-complete selected formula.
(3) If $(\chi(a), \chi(d)) = (-1, -1)$, then $\sigma = (0:1)$ is admissible, and it remains to choose $\tau \in \mathbb{P}^1(K)$ such that $\chi(\Delta_x(\tau)) = -1$.
(4) If $(\chi(a), \chi(d)) = (+1, +1)$, choose $c^2 = a$. It is enough to find t with $\chi((t^2 - a)(t^2 - d)) = -1$ and set $s = t/c$. Equivalently, find an admissible s and set $t = cs$; in the model $a = 1$, take $s = t$.

Proof. In a finite field of odd cardinality, $K^\times / K^{\times 2}$ has exactly two classes, and $\chi(ad) = \chi(a)\chi(d)$. The identities

$$\Delta_y(0:1) = d, \qquad \Delta_y(1:0) = a, \qquad \Delta_x(0:1) = ad$$

give the first two cases and the admissibility of $\sigma = (0:1)$ in the third case. The last case uses the one-condition selection rule in Theorem 3.23. □

Proposition 3.28 (Existence over finite fields). Let $K = \mathbb{F}_q$, with q odd, and let $a, d \in K^\times$, $a \neq d$. If $q > 16$, then there exist finite choices $\sigma = (s:1)$ and $\tau = (t:1)$ such that $\chi(\Delta_y(\sigma)) = -1$ and $\chi(\Delta_x(\tau)) = -1$. Consequently, for

$q > 16$, the selected formula can be made $\mathbb{F}_q$-complete for every nonsingular twisted Edwards parameter pair (a, d).

Proof. For $\tau = (t : 1)$, one has $\Delta_x(\tau) = f_x(t)$, where $f_x(T) = (T^2 - a)(T^2 - d)$. Since $a, d \neq 0$, $a \neq d$, and $\operatorname{char} K \neq 2$, this polynomial is squarefree of degree four and is not a square in $K[T]$. The Weil bound for quadratic character sums gives

$$\left| \sum_{T \in K} \chi(f_x(T)) \right| \leq 3\sqrt{q}$$

[LN97]. The polynomial f_x has at most four zeros. Hence the number of $t \in K$ with $\chi(f_x(t)) = -1$ is at least

$$\frac{q - 4 - 3\sqrt{q}}{2},$$

which is positive for $q > 16$.

This single t-search already selects a complete member by Theorem 3.23. If finite coefficients in both projections are required, the same bound also applies to $f_y(S) = (S^2 - 1)(aS^2 - d)$, since $\Delta_y(s : 1) = f_y(s)$. Therefore there exists $s \in K$ such that $\chi(f_y(s)) = -1$. Taking $\sigma = (s : 1)$ and $\tau = (t : 1)$ gives the claim. □

Remark 3.29. The existence statement is a finite-field consequence of the character-sum estimate. It is not part of the field-uniform completeness theorem. Over a general field K, the main theorem remains conditional on the existence of K-admissible selected coefficients.

4. Operation Counts and Optimization of the Selected Formula

The preceding section proved a field-uniform completeness criterion for the selected formula. We now study the arithmetic cost of the same construction. The discussion has two layers. First, we record schedules and optimizations which are valid over an arbitrary field K of characteristic different from 2, provided the required constants and coordinate normalizations exist over K. Second, we specialize these schedules to finite fields, where quadratic characters and square-class branches give more explicit coefficient choices.

The costs below are upper bounds obtained from explicit evaluation schedules in the selected product-coordinate framework. We therefore keep separate the general field multiplications, the squarings, and the multiplications by fixed curve or selection constants. This distinction is important because fixed constants may be cheap, may be absorbed by a global change of representation, or may be moved into a precomputation table.

4.1. Cost conventions and the separated baseline.

We count a general multiplication in K as M, a squaring as S, and a multiplication by a fixed constant $c \in K$ as D_c. Additions and subtractions are not included in the main cost expressions. We write D_a, D_d for multiplications by the curve constants, and D_s, D_t for multiplications by finite selected coefficients s, t.

A fixed-constant multiplication is counted only when it is performed online. If a constant is absorbed into the coordinate representation by a global change of variables, the corresponding D_c-term is removed and the required field condition is stated explicitly. If a constant depending only on a precomputed point is moved into a table, the cost is moved to table construction rather than deleted. Thus raw

mixed additions and table-precomputed mixed additions are recorded separately in the summary table.

The selected coefficients are projective:

$$\sigma = (\sigma_0 : \sigma_1), \qquad \tau = (\tau_0 : \tau_1) \in \mathbb{P}^1(K).$$

The selected projection pairs are

$$S_\sigma = (\sigma_1 E + \sigma_0 V : \sigma_1 G + \sigma_0 W), \qquad T_\tau = (\tau_1 H + \tau_0 N : \tau_1 F + \tau_0 R).$$

In the affine chart $\sigma = (s : 1)$, $\tau = (t : 1)$, these become

$$S_\sigma = (E + sV : G + sW), \qquad T_\tau = (H + tN : F + tR),$$

and the schedule may contain two multiplications by s and two by t. If $\sigma = (1 : 0)$, then $S_\sigma = (V : W)$; if $\tau = (1 : 0)$, then $T_\tau = (N : R)$. Thus the informal notation $s = \infty$ or $t = \infty$ only means that the complementary projective representative has been selected.

Proposition 4.1 (Normalization of projective selection coefficients). The selected formula $\Psi_{\sigma,\tau}$ depends only on the projective classes of $\sigma, \tau \in \mathbb{P}^1(K)$, not on the chosen homogeneous representatives. More precisely, if

$$\sigma' = (\lambda\sigma_0 : \lambda\sigma_1), \qquad \tau' = (\mu\tau_0 : \mu\tau_1), \qquad \lambda, \mu \in K^\times,$$

then $\Psi_{\sigma',\tau'} = \Psi_{\sigma,\tau}$ as a projective extended-coordinate output. Consequently, whenever $\sigma_1\tau_1 \neq 0$, we may use the affine representatives

$$\sigma = (s : 1), \qquad \tau = (t : 1), \qquad s = \sigma_0/\sigma_1, \quad t = \tau_0/\tau_1.$$

In this chart the online schedule involves multiplications by s and t, not separate multiplications by the four homogeneous coordinates $\sigma_0, \sigma_1, \tau_0, \tau_1$.

Proof. Scaling σ by λ scales both coordinates of S_σ by λ, and scaling τ by μ scales both coordinates of T_τ by μ. The Segre reconstruction

$$(A : B) \times (C : D) \longmapsto (AD : BC : BD : AC)$$

therefore scales all four output coordinates by the common factor $\lambda\mu$. The projective output is unchanged. The affine formulas follow by dividing by σ_1 and τ_1, when these entries are nonzero. □

Transport under curve normalization. Projective rescaling of σ, τ must be distinguished from a change of curve model. For $c \in K^\times$, the identity-preserving isomorphism

$$\nu_c(X : Y : Z : T) = (cX : Y : Z : cT)$$

has target parameters and finite selected coefficients

$$a' = a/c^2, \qquad d' = d/c^2, \qquad s' = s, \qquad t' = t/c. \tag{4.1}$$

Primes denote blocks evaluated on $\nu_c(P_i)$ with parameters a', d'. Thus

$$(E', R', N', V') = c(E, R, N, V),$$
$$(H', W', F', G') = (H, W, F, G).$$

Writing $A = E + sV$, $B = G + sW$, $C = H + tN$, and $D = F + tR$, the selected pairs become $(cA : B)$ and $(C : D)$, so their output is $(cAD : BC : BD : cAC) = \nu_c(AD : BC : BD : AC)$. For homogeneous selectors the rule is $\sigma' = \sigma$, $\tau' = (\tau_0 : c\tau_1)$, up to common scalars. This also proves

$$\Delta'_y(s) = c^{-2}\Delta_y(s), \qquad \Delta'_x(t/c) = c^{-4}\Delta_x(t),$$

so admissibility is preserved. The online cost of a chosen constant need not be preserved. Every normalization below uses these transported coefficients, or chooses fresh coefficients in the fixed target model.

For example, in $\mathbb{F}_{17}$, $(a, d, s, t) = (2, 4, 2, 1)$ is admissible. With $c = 6$, the transported data are $(1, 2, 2, 3)$. Retaining $t' = 1$ would instead give a zero discriminant and zero output on $((1 : 0 : 1 : 0), O)$.

Remark 4.2 (Normalized coefficient search). The normalized representatives describe all available charts, but two independent coefficient searches are unnecessary. In the finite charts one has

$$\Delta_y(s) = (s^2 - 1)(as^2 - d), \qquad \Delta_x(t) = (t^2 - a)(t^2 - d),$$

while

$$\Delta_y(\infty) = a, \qquad \Delta_x(\infty) = 1.$$

Thus $\tau = \infty$ is never admissible by the nonsquare criterion, whereas $\sigma = \infty$ is admissible exactly when a is a nonsquare in K. The single-condition rule in Theorem 3.23 therefore searches only t: set $s = t/c$ when $c^2 = a$, or fix $\sigma = (1 : 0)$ when a is a nonsquare. With $a = 1$, set $s = t$. The selection is performed offline and is not included in an individual addition.

We now give the separated baseline schedule. Let $P_i = (X_i : Y_i : Z_i : T_i)$, $i = 1, 2$, be two input points. The eight bilinear blocks are

$$\begin{aligned} E &= X_1Y_2 + Y_1X_2, & R &= Y_1X_2 - X_1Y_2, \\ H &= Y_1Y_2 - aX_1X_2, & W &= Y_1Y_2 + aX_1X_2, \\ F &= Z_1Z_2 - dT_1T_2, & G &= Z_1Z_2 + dT_1T_2, \\ N &= Z_1T_2 - T_1Z_2, & V &= Z_1T_2 + T_1Z_2. \end{aligned}$$

They are obtained from the eight products

$$X_1Y_2, \quad Y_1X_2, \quad Y_1Y_2, \quad X_1X_2, \quad Z_1Z_2, \quad T_1T_2, \quad Z_1T_2, \quad T_1Z_2,$$

together with one multiplication by a and one by d. Thus the block layer costs $8M + D_a + D_d$.

For finite selected coefficients $\sigma = (s : 1)$, $\tau = (t : 1)$, write

$$(A_\sigma : B_\sigma) = (E + sV : G + sW), \qquad (C_\tau : D_\tau) = (H + tN : F + tR).$$

The selection layer costs $2D_s + 2D_t$, with the corresponding term omitted when $s = 0$ or $t = 0$. The selected output is the Segre product

$$\Psi_{\sigma,\tau}(P_1, P_2) = (A_\sigma D_\tau : \ B_\sigma C_\tau : \ B_\sigma D_\tau : \ A_\sigma C_\tau),$$

whose final layer costs $4M$.

Proposition 4.3 (Separated cost of the selected formula). Assume that $\sigma = (s : 1)$ and $\tau = (t : 1)$ are finite selected coefficients. A separated evaluation of $\Psi_{\sigma,\tau}$ has cost

$$12M + D_a + D_d + 2D_s + 2D_t.$$

If $s = 0$, the term $2D_s$ is absent; if $t = 0$, the term $2D_t$ is absent.

Proof. The block layer costs $8M+D_a+D_d$, the finite selection layer costs $2D_s+2D_t$, and the Segre reconstruction costs $4M$. Hence the total is

$$8M + D_a + D_d + 2D_s + 2D_t + 4M = 12M + D_a + D_d + 2D_s + 2D_t.$$

The terms involving s or t disappear when the corresponding selected coefficient is zero. □

For projective points at infinity, the same cost principle is read using the normalized representatives from Proposition 4.1. If $\sigma = (1 : 0)$, then $S_\sigma = (V : W)$ and no D_s-term occurs; if $\tau = (1 : 0)$, then $T_\tau = (N : R)$ and no D_t-term occurs.

Corollary 4.4 (Separated cost in normalized projective charts). Let $\sigma, \tau \in \mathbb{P}^1(K)$ be normalized as above. The separated evaluation cost of $\Psi_{\sigma,\tau}$ is $12M + D_a + D_d$, plus the constant multiplications required by the finite nonzero selected coefficients. Thus the finite nonzero chart has cost

$$12M + D_a + D_d + 2D_s + 2D_t,$$

with $2D_s$ or $2D_t$ omitted when the corresponding coefficient is 0 or $\infty = (1 : 0)$.

Remark 4.5 (Separated baseline versus later optimizations). The separated cost is the baseline schedule. Later optimizations reduce it in two ways: by choosing elementary charts such as $\sigma = 0$, $\sigma = \infty$, or $\tau = 0$, which remove part of the selection layer, and by changing the representation so that fixed constants are normalized, absorbed, or moved to precomputation. These reductions are representation-dependent and will always be stated with their field conditions.

4.2. **Elementary charts and split-pair optimizations.** The separated schedule of Proposition 4.3 applies to arbitrary selected coefficients. Two projective choices are especially useful because they remove the selected-constant layer completely:

$$(\sigma, \tau) = ((0 : 1), (0 : 1)), \qquad (\sigma, \tau) = ((1 : 0), (0 : 1)).$$

They give the standard and mirror elementary product representatives. Their arithmetic schedules are field-uniform; their completeness is still governed by the admissibility criterion of Theorem 3.23.
The standard chart. For $\sigma = (0 : 1)$, $\tau = (0 : 1)$, we have

$$S_\sigma = (E : G), \qquad T_\tau = (H : F),$$

and hence

$$\Psi_{0,0}(P_1, P_2) = (EF : GH : GF : EH).$$

By Proposition 3.25, this chart is K-admissible if and only if

$$d, ad \in K^\times \setminus K^{\times 2}.$$

Over a finite field this includes the branch $(\chi(a), \chi(d)) = (+1, -1)$.

The schedule avoids the unused blocks R, W, N, V. Compute

$$A = X_1X_2, \quad B = Y_1Y_2, \quad C = T_1T_2, \quad D = Z_1Z_2, \quad P = (X_1 + Y_1)(X_2 + Y_2).$$

Then

$$E = P - A - B, \qquad H = B - aA, \qquad F = D - dC, \qquad G = D + dC,$$

and finally

$$(X_3 : Y_3 : Z_3 : T_3) = (EF : GH : GF : EH).$$

Proposition 4.6 (Cost of the standard chart). The chart $(\sigma, \tau) = ((0 : 1), (0 : 1))$ has separated cost

$$9M + D_a + D_d.$$

If a or d is normalized to 1, -1, or is otherwise treated as a cheap fixed constant in the representation, the corresponding D-term is omitted or replaced by the appropriate cheap-constant cost.

Proof. The five products A, B, C, D, P cost $5M$, the fixed multiplications aA and dC cost $D_a + D_d$, and the four output products cost $4M$. Hence the total is $9M + D_a + D_d$. □

The mirror chart. For $\sigma = (1 : 0)$, $\tau = (0 : 1)$, we have

$$S_\sigma = (V : W), \qquad T_\tau = (H : F),$$

and hence

$$\Psi_{\infty,0}(P_1, P_2) = (VF : WH : WF : VH).$$

This chart is K-admissible if and only if

$$a, ad \in K^\times \setminus K^{\times 2}.$$

Over a finite field this includes the branch $(\chi(a), \chi(d)) = (-1, +1)$.

Again we avoid the unused blocks. Compute

$$A = X_1X_2, \quad B = Y_1Y_2, \quad C = T_1T_2, \quad D = Z_1Z_2, \quad Q = (Z_1 + T_1)(Z_2 + T_2).$$

Then

$$V = Q - D - C, \qquad H = B - aA, \qquad W = B + aA, \qquad F = D - dC,$$

and finally

$$(X_3 : Y_3 : Z_3 : T_3) = (VF : WH : WF : VH).$$

Proposition 4.7 (Cost of the mirror chart). The chart $(\sigma, \tau) = ((1 : 0), (0 : 1))$ has separated cost

$$9M + D_a + D_d.$$

As in Proposition 4.6, any global normalization or cheap representation of a or d removes or reduces the corresponding fixed-constant cost.

Proof. The five products A, B, C, D, Q cost $5M$, the fixed multiplications aA and dC cost $D_a + D_d$, and the four output products cost $4M$. Hence the total is $9M + D_a + D_d$. □

The two elementary charts are the low-cost starting point for the optimized branch schedules. They already remove the selected layer $2D_s + 2D_t$. One can sometimes reduce the remaining cost further by splitting one bilinear pair.

In the standard chart, the relevant X, Y-pair is

$$E = X_1Y_2 + Y_1X_2, \qquad H = Y_1Y_2 - aX_1X_2.$$

If $-a = \alpha^2$ with $\alpha \in K^\times$, then

$$H + \alpha E = (Y_1 + \alpha X_1)(Y_2 + \alpha X_2), \qquad H - \alpha E = (Y_1 - \alpha X_1)(Y_2 - \alpha X_2).$$

Thus the pair (E, H), up to fixed scalings, is obtained from two multiplications. Similarly, in the mirror chart the relevant Z, T-pair is

$$V = Z_1T_2 + T_1Z_2, \qquad F = Z_1Z_2 - dT_1T_2.$$

If $-d = \beta^2$ with $\beta \in K^\times$, then

$$F + \beta V = (Z_1 + \beta T_1)(Z_2 + \beta T_2), \qquad F - \beta V = (Z_1 - \beta T_1)(Z_2 - \beta T_2).$$

Thus the pair (V, F), again up to fixed scalings, is obtained from two multiplications.

Proposition 4.8 (Split-pair schedules). Let $\operatorname{char} K \neq 2$.

(1) If $c^2 = -a$, the model with $(a', d') = (-1, d/c^2)$ admits the standard-chart schedule $8M + D_{d'}$.
(2) If $c^2 = -d$, the model with $(a', d') = (a/c^2, -1)$ admits the mirror-chart schedule $8M + D_{a'}$.

The selected coefficients are transported by (4.1). Output stays in the chosen normalized extended model, so successive operations require no repeated conversion.

Proof. In the standard normalized model, suppress primes on coordinates and compute

$$\begin{aligned} A &= (Y_1 - X_1)(Y_2 - X_2), & B &= (Y_1 + X_1)(Y_2 + X_2), \\ C &= 2d'T_1T_2, & D &= 2Z_1Z_2, \\ e &= B - A, & h &= B + A, \quad f = D - C, \quad g = D + C. \end{aligned}$$

Here $(e, h, f, g) = 2(E, H, F, G)$. The output $(ef : gh : gf : eh)$ is the standard tuple multiplied by the common nonzero scalar 4. The first layer costs $4M + D_{d'}$ and the four output products cost $4M$.

For the mirror normalized model compute

$$\begin{aligned} A &= (Z_1 - T_1)(Z_2 - T_2), & B &= (Z_1 + T_1)(Z_2 + T_2), \\ C &= 2a'X_1X_2, & D &= 2Y_1Y_2, \\ v &= B - A, & f &= B + A, \quad h = D - C, \quad w = D + C. \end{aligned}$$

Now $(v, f, h, w) = 2(V, F, H, W)$, and $(vf : wh : wf : vh)$ is four times the mirror tuple. The cost is $4M + D_{a'} + 4M = 8M + D_{a'}$. Both outputs use the same standard extended coordinates as their inputs. □

Remark 4.9 (Representation dependence of the split cost). The split costs refer to the fixed normalized models in Proposition 4.8. Conversion into that model is performed once; conversion back after every operation would have to be counted separately. No uncomputed output scaling is hidden in the stated online schedules, since the factor 4 is common to all four coordinates.

4.3. **Schedules in the same-square-class cases.** We now record the schedules used when the curve constants lie in the same square class. The formulas and operation counts in this subsection are valid over any field K of characteristic different from 2, once the required selected coefficients exist. Over a finite field, these are the two branches in which a and d are both nonsquares or both squares. The nontrivial same-square-class case. Assume first that a and d have the same nontrivial square class:

$$aK^{\times 2} = dK^{\times 2} \neq K^{\times 2}.$$

Then a and d are nonsquares, while ad is a square. Hence $\sigma = (0 : 1)$ and $\sigma = (1 : 0)$ are admissible on the y-side, since $\Delta_y(0) = d$ and $\Delta_y(\infty) = a$, but $\tau = (0 : 1)$ is not admissible because $\Delta_x(0) = ad$. We therefore choose $\tau = (t : 1)$ with

$$(t^2 - a)(t^2 - d) \in K^\times \setminus K^{\times 2}.$$

The two useful formulas are

$$\Psi_{0,t} = \big(E(F + tR) : G(H + tN) : G(F + tR) : E(H + tN)\big),$$

and

$$\Psi_{\infty,t} = \big(V(F + tR) : W(H + tN) : W(F + tR) : V(H + tN)\big).$$

Proposition 4.10 (Schedules in the nontrivial same-square-class case). Let K be a field with $\operatorname{char} K \neq 2$, and assume

$$aK^{\times 2} = dK^{\times 2} \neq K^{\times 2}.$$

If $t \in K$ satisfies

$$(t^2 - a)(t^2 - d) \in K^{\times} \setminus K^{\times 2},$$

then both $\Psi_{0,t}$ and $\Psi_{\infty,t}$ are K-complete. Moreover,

$$\Psi_{0,t}: \quad 10M + 2D_a + D_d + 2D_t,$$

and

$$\Psi_{\infty,t}: \quad 10M + D_a + 2D_d + 2D_t.$$

If t is a cheap fixed constant, the term $2D_t$ is replaced by the corresponding cheap constant cost; in particular, for $t = 1$ the term $2D_t$ is absent.

Proof. Completeness follows from the discriminant criterion. The assumptions imply that a and d are nonsquares, so $\sigma = (0 : 1)$ and $\sigma = (1 : 0)$ are admissible. The displayed condition on t gives admissibility of $\tau = (t : 1)$.

For $\Psi_{0,t}$, compute

$$M_1 = X_1Y_2, \qquad M_2 = Y_1X_2, \qquad D_1 = aX_1, \qquad M_3 = (Y_1 - D_1)(X_2 + Y_2).$$

Then

$$E = M_1 + M_2, \qquad R = M_2 - M_1, \qquad H = M_3 - M_2 + aM_1.$$

This gives the required X, Y-block (E, R, H) in cost

$$3M + 2D_a.$$

Next compute

$$M_4 = Z_1Z_2, \qquad M_5 = T_1T_2, \qquad M_6 = (Z_1 - T_1)(Z_2 + T_2), \qquad D_3 = dM_5.$$

Then

$$F = M_4 - D_3, \qquad G = M_4 + D_3, \qquad N = M_6 - M_4 + M_5.$$

This gives the required Z, T-block (F, G, N) in cost

$$3M + D_d.$$

Finally form $H + tN$ and $F + tR$, costing $2D_t$, and compute the four Segre products. Hence

$$(3M + 2D_a) + (3M + D_d) + 2D_t + 4M = 10M + 2D_a + D_d + 2D_t.$$

For $t = 1$ in the operational model, $2D_t$ is absent. If the input data are instead transported to $a' = -1$ with $c^2 = -a$, the cost is $10M + D_{d'} + 2D_{t'}$, where $t' = t/c$. For the mirror schedule, compute

$$u_1 = X_1X_2, \quad u_2 = Y_1Y_2, \quad u_3 = (Y_1 - X_1)(Y_2 + X_2),$$
$$H = u_2 - au_1, \quad W = u_2 + au_1, \quad R = u_3 - u_2 + u_1$$

in $3M + D_a$. Next compute

$$u_4 = Z_1T_2, \quad u_5 = T_1Z_2, \quad b = dT_1, \quad u_6 = (Z_1 - b)(Z_2 + T_2),$$
$$V = u_4 + u_5, \quad N = u_4 - u_5, \quad F = u_6 - u_4 + du_5$$

in $3M + 2D_d$. Form $C = H + tN, D = F + tR$, then output $(VD : WC : WD : VC)$. The selection and output layers cost $2D_t + 4M$, proving the second count as well. □

Remark 4.11 (Normalized costs in the nontrivial same-square-class case). If $-a \in K^{\times 2}$, choose $c^2 = -a$. In the target model the first cost is $10M + D_{d'} + 2D_{t'}$, with $t' = t/c$. It becomes $10M + D_{d'}$ if a fresh admissible coefficient $t' = 1$ is chosen in that target model. An original choice $t = 1$ does not in general have this property. Similarly, normalizing $d' = -1$ with $c^2 = -d$ gives $10M + D_{a'} + 2D_{t'}$ for the mirror schedule.

The square–square case. Now assume

$$a, d \in K^{\times 2}.$$

Here the coefficients may be coupled: if $c^2 = a$, take $t = cs$ and test only $(s^2 - 1)(as^2 - d)$. The more general schedules also allow independently chosen admissible coefficients. Take $\sigma = (s : 1)$ and $\tau = (t : 1)$, with

$$(s^2 - 1)(as^2 - d) \in K^\times \setminus K^{\times 2}, \qquad (t^2 - a)(t^2 - d) \in K^\times \setminus K^{\times 2}.$$

The selected formula is

$$\begin{aligned}\Psi_{s,t} = \big((E + sV)(F + tR) : (G + sW)(H + tN) : \\ (G + sW)(F + tR) : (E + sV)(H + tN)\big).\end{aligned}$$

Proposition 4.12 (Schedule in the square–square case). Let K be a field with $\operatorname{char} K \neq 2$, and assume $a, d \in K^{\times 2}$. If $s, t \in K$ satisfy

$$(s^2 - 1)(as^2 - d) \in K^\times \setminus K^{\times 2}, \qquad (t^2 - a)(t^2 - d) \in K^\times \setminus K^{\times 2},$$

then $\Psi_{s,t}$ is K-complete. If $c^2 = a$, its transported law has $a' = 1, d' = d/a, s' = s, t' = t/c$ and online cost

$$12M + D_{d'} + 2D_s + 2D_{t'}.$$

The coupled choice $t = cs$ has $s' = t' = s$, so only one nonsquare test is needed and the cost is $12M + D_{d'} + 4D_s$. Cheapness is tested in this target model.

Proof. Completeness follows from the discriminant criterion and is preserved by (4.1). With $a' = 1$, the block and output layers cost $12M + D_{d'}$; the transported selection layer costs $2D_s + 2D_{t'}$. This proves the stated count. □

Remark 4.13 (Unnormalized square–square cost). Without the normalization $a' = 1$, the same separated selected schedule has cost

$$12M + D_a + D_d + 2D_s + 2D_t.$$

The normalization $a' = 1$ is available in the square–square case because $a \in K^{\times 2}$.

Remark 4.14 (Relation with absorption). In the nontrivial same-square-class case, after fixing $\sigma = (0 : 1)$ or $\sigma = (1 : 0)$, only the selected layer $2D_t$ remains. In the square–square case, the selected layer is $2D_s + 2D_t$. The next subsection studies when these selected constant terms can be absorbed into the representation and removed from the online cost.

4.4. **Absorbed selected coefficients.** For general selected coefficients the separated schedule contains $2D_s + 2D_t$. We call a coefficient absorbed only when an explicit fixed representation makes its online multiplications unnecessary and the output stays in that representation. This must be distinguished from admissibility of the selected fibres.

Proposition 4.15 (Cost effect of absorbed selected coefficients). Let $t \in K^\times$ and $\sigma \in \mathbb{P}^1(K)$. The identity-preserving change

$$\nu_t(X : Y : Z : T) = (tX : Y : Z : tT)$$

transports the selected law to

$$a_t = a/t^2, \qquad d_t = d/t^2, \qquad \sigma_t = \sigma, \quad \tau_t = (1 : 1).$$

For finite $\sigma = (s : 1)$, it therefore has full separated cost

$$12M + D_{a_t} + D_{d_t} + 2D_s.$$

For $\sigma = (0 : 1)$ and $\sigma = (1 : 0)$, the refined full costs are, respectively,

$$10M + 2D_{a_t} + D_{d_t}, \qquad 10M + D_{a_t} + 2D_{d_t}.$$

These are online costs in the fixed target model, including its new curve constants. They require no fourth-power condition. The relations $s^4 = d/a,\ t^4 = ad$ alone do not justify deletion of the remaining $2D_s$.

Proof. Take $c = t$ in (4.1). The selected t-coefficient becomes 1 and the output of each addition remains in $\mathcal{E}^e_{a_t,d_t}$. The costs follow from the separated and refined schedules applied in that model. Initial conversion, or conversion back after each operation, is a separate cost; doubling uses the same target constants.

To see the limitation of a diagonal scaling argument for s, suppose (X, Y, Z, T) are rescaled to (uX, vY, wZ, rT) and the Segre relation is preserved. Necessarily $uv = wr$. The two numerator blocks then have weights $E' = uvE$ and $V' = wrV = uvV$. Thus unequal weights of E and V cannot eliminate s from $E + sV$. Rescaling a basis generator merely moves the same constant to its evaluation. Consequently the fourth-power identity, without a separate explicit evaluation schedule, is not an absorption proof for s. The stated schedules count its multiplications. □

Remark 4.16 (Absorption versus completeness). Absorption is only a cost optimization. Completeness still requires the selected discriminants to be nonsquares:

$$\Delta_y(\sigma), \Delta_x(\tau) \in K^\times \setminus K^{\times 2}.$$

For the dependent choices of Theorem 3.23, only one nonsquare test remains. Over finite fields it is a quadratic-character test.

The absorption identities are useful because, in a natural subfamily, they also force the two discriminants to have the same square class.

Proposition 4.17 (Fourth-power coefficients with automatic admissibility). Let K be a field with $\operatorname{char} K \neq 2$, and let $a, d \in K^\times$, $a \neq d$. Suppose that $s, t \in K^\times$ satisfy

$$s^4 = \frac{d}{a}, \qquad t^4 = ad.$$

Then

$$\Delta_y(s) = -a\, s^2(s^2 - 1)^2, \qquad \Delta_x(t) = -t^2 a^{-1}(t^2 - a)^2.$$

In particular, if $-a \in K^\times \setminus K^{\times 2}$, then both $\Delta_y(s)$ and $\Delta_x(t)$ are nonsquares. Thus the same fourth-power choice of s, t also gives admissibility whenever $-a$ is a nonsquare.

Proof. From $s^4 = d/a$, we have $d = as^4$, and hence

$$\Delta_y(s) = (s^2-1)(as^2-d) = (s^2-1)(as^2-as^4) = -a\,s^2(s^2-1)^2.$$

This is nonzero, since $s^2 = 1$ would imply $d = a$. Similarly, from $t^4 = ad$, we have $d = t^4/a$, so

$$\Delta_x(t) = (t^2-a)\left(t^2 - \frac{t^4}{a}\right) = -t^2a^{-1}(t^2-a)^2.$$

This is nonzero as well, since $t^2 = a$ would imply $d = a$. All factors except $-a$ are squares in $K^\times$, because a^{-1} has the same square class as a. Hence both discriminants have the square class of $-a$. □

Corollary 4.18 (Fourth-power coefficients in the square–square finite-field case). Let $K = \mathbb{F}_q$, $q \equiv 3 \pmod 4$, and $(\chi(a), \chi(d)) = (+1, +1)$. There exist $s, t \in K^\times$ with $s^4 = d/a$, $t^4 = ad$, and these coefficients are admissible. The t-normalized representation of Proposition 4.15 has

$$a_t = a/t^2, \quad d_t = d/t^2, \quad (s_t, t_t) = (s, 1)$$

and full separated cost $12M + D_{a_t} + D_{d_t} + 2D_s$. Alternatively the $a' = 1$ representation has $12M + D_{d'} + 2D_s + 2D_{t'}$, with $t' = t/c$, $c^2 = a$. The two cost expressions refer to different fixed models.

Proof. Since $q \equiv 3 \pmod 4$, the subgroup of squares in $\mathbb{F}_q^\times$ has odd order; hence every square is a fourth power. Because a and d are squares, both d/a and ad are fourth powers. Thus the required s, t exist. Moreover $\chi(-a) = \chi(-1)\chi(a) = -1$, so admissibility follows from Proposition 4.17. □

Corollary 4.19 (Absorbed t-coefficient in the nonsquare–nonsquare finite-field case). Let $K = \mathbb{F}_q$, $q \equiv 1 \pmod 4$, and $(\chi(a), \chi(d)) = (-1, -1)$. Suppose $ad \in (K^\times)^4$ and choose t with $t^4 = ad$. Then t is admissible on the second side. In the fixed t-normalized model $a_t = a/t^2, d_t = d/t^2$, the selected coefficient is 1; the two full costs are

$$10M + 2D_{a_t} + D_{d_t}, \qquad 10M + D_{a_t} + 2D_{d_t}.$$

Here $a_t d_t = 1$. Since $-a_t$ is a nonsquare, normalization to $a' = -1$ over K is unavailable in this case.

Proof. The fourth-power identity gives $\Delta_x(t) = -t^2a^{-1}(t^2-a)^2$, whose square class is that of $-a$. Since $\chi(-1) = 1$ and $\chi(a) = -1$, it is a nonsquare. Proposition 4.15 transports the law to $t_t = 1$, preserving admissibility. Applying both schedules of Proposition 4.10 to this model proves the costs. The same character calculation gives $\chi(-a_t) = -1$. □

Remark 4.20 (Normalized fourth-power case). With $a = 1$ and $\rho \in K^\times$, the choice $s = t = \rho$ satisfies both fourth-power identities exactly when $d = \rho^4$. Its cost in this model is $12M + D_d + 4D_\rho$. In the t-normalized model it instead has parameters $(a_t, d_t) = (\rho^{-2}, \rho^2)$, selectors $(\rho, 1)$, and cost $12M + D_{\rho^{-2}} + D_{\rho^2} + 2D_\rho$. These explicit alternatives permit a comparison of actual constant costs; neither deletes $2D_s$ merely from the fourth-power identity.

4.5. **Doubling.** Although the selected formula is designed for addition, its restriction to the diagonal is independent of the selected coefficients. Let $P = (X : Y : Z : T) \in \mathcal{E}^e_{a,d}$. For $P_1 = P_2 = P$, the alternating blocks vanish and the two symmetric blocks coincide:

$$R = N = 0, \qquad V = E, \qquad W = G.$$

Indeed, $E = 2XY = 2ZT = V$ follows from $XY = ZT$, and $W = Y^2 + aX^2 = Z^2 + dT^2 = G$ follows from the curve equation.

Hence, on the diagonal,

$$S_\sigma = (\sigma_0 + \sigma_1)(E : G), \qquad T_\tau = \tau_1(H : F).$$

For admissible selected coefficients the scalars $\sigma_0+\sigma_1$ and τ_1 are nonzero; otherwise the selected exceptional fibre would contain the neutral difference point. Therefore the selected formula restricts to the standard doubling product

$$[2]P = (EF : GH : GF : EH).$$

Proposition 4.21 (Doubling formula and cost). For any admissible selected coefficients (σ, τ), the doubling specialization of $\Psi_{\sigma,\tau}$ is independent of σ and τ. It is represented by

$$[2]P = (EF : GH : GF : EH),$$

where, on the diagonal,

$$E = 2XY, \qquad H = Y^2 - aX^2, \qquad G = Y^2 + aX^2, \qquad F = Z^2 - dT^2.$$

It can be evaluated with cost

$$4M + 4S + \min(D_a, D_d).$$

If the cheaper of a and d is normalized to ± 1, or its multiplication is absorbed in the representation, the cost becomes

$$4M + 4S.$$

Proof. The identities $R = N = 0$, $V = E$, and $W = G$ show that the selected projection pairs are nonzero scalar multiples of $(E : G)$ and $(H : F)$. Since the Segre reconstruction is projective, these scalars do not change the output point.

For the cost, there are two symmetric schedules. The a-side schedule computes $A = X^2$, $B = Y^2$, $C = Z^2$, and $E = (X + Y)^2 - A - B$, then forms

$$aA, \qquad G = B + aA, \qquad H = B - aA, \qquad F = 2C - G.$$

It costs $4M + 4S + D_a$. The d-side schedule computes $B = Y^2$, $C = Z^2$, $D = T^2$, and $E = (Z + T)^2 - C - D$, then forms

$$dD, \qquad G = C + dD, \qquad F = C - dD, \qquad H = 2B - G.$$

It costs $4M+4S+D_d$. Taking the cheaper of the two gives $4M+4S+\min(D_a, D_d)$. □

Remark 4.22 (Comparison with addition). The disappearance of σ and τ in doubling is structural. It is not a finite-field phenomenon and does not depend on the square-class case. The square-class analysis affects which selected coefficients give complete addition, but the diagonal specialization is the same for all admissible choices.

4.6. **Mixed additions and precomputation conventions.** We distinguish two mixed-addition conventions. A raw mixed addition assumes that one input, usually the second point, is normalized in the chosen representation, but no point-dependent auxiliary quantities have been stored. Thus products involving the fixed input are still counted online; only products made trivial by the normalization, such as multiplication by a coordinate equal to 1, are removed.

A table-precomputed mixed addition assumes that the second input is a table entry and that expressions depending only on that entry may be stored with the table. For instance, quantities such as dT_2, X_2+Y_2, Z_2+T_2, or selected-coordinate expressions depending only on the table entry may be moved to table construction. Such terms are not counted in the online mixed-addition line, but they have not disappeared from the overall precomputation cost.

Definition 4.23 (Raw and table-precomputed mixed additions)**.** A raw mixed addition is an addition in which one input point is normalized, but no point-dependent auxiliary expressions are assumed to have been stored in advance.

A table-precomputed mixed addition is an addition in which one input point is a precomputed table entry and the table may store fixed expressions depending only on that entry. Costs moved to the table-building step are not counted in the online mixed-addition cost, but they should not be interpreted as algebraic cancellations in the addition law.

This distinction is especially relevant for selected formulas. If $\sigma = (s : 1)$ and $\tau = (t : 1)$ are fixed, the online selected pairs involve

$$E + sV, \qquad G + sW, \qquad H + tN, \qquad F + tR.$$

When one input is a table entry, some terms involving s, t and that entry may be precomputed, depending on the schedule. This reduces the online cost of repeated mixed additions, but it does not change the full-addition cost.

Remark 4.24 (How mixed costs are reported)*.* The summary table reports mixed costs in two forms: raw mixed addition and mixed addition with table precomputation. The first is the cost of a single addition with a normalized input. The second is the online cost when the fixed input is a precomputed table entry. Whenever a D_c-term is removed only because it has been moved to the table, this is a precomputation convention, not a new algebraic cancellation.

Remark 4.25 (Independence from completeness)*.* Mixed-addition schedules are cost refinements of the same selected formula. They do not change the exceptional set and do not alter the admissibility conditions

$$\Delta_y(\sigma), \Delta_x(\tau) \in K^\times \setminus K^{\times 2}.$$

Thus completeness remains the one proved by Theorem 3.23.

4.7. **Low-cost coefficient selection over finite fields.** Every candidate test in this subsection uses the fixed operational parameters a, d. A quoted normalized cost assumes that the candidates are chosen in that normalized model; otherwise (4.1) must be applied first. Let $K = \mathbb{F}_q$, q odd, and let χ denote the quadratic character of K. The existence theorem guarantees admissible finite coefficients for $q > 16$, but the arithmetic cost depends on how expensive it is to multiply by the selected constants. This issue appears only in the same-square-class cases: in the nonsquare–nonsquare case, after fixing $\sigma = (0 : 1)$ or $\sigma = (1 : 0)$, one still has to

choose t, and the selected layer is $2D_t$. In the square–square case one may choose $c^2 = a$ and set $t = cs$, using only one nonsquare test. In the fixed model $a = 1$, take $s = t$; the selected layer is then $4D_s$. Independent cheap menus remain an option, with layer $2D_s + 2D_t$.

The discriminant tests are explicit. A fixed value $t = c$ is admissible on the x-side exactly when

$$\chi((c^2 - a)(c^2 - d)) = -1,$$

and a fixed value $s = c$ is admissible on the y-side exactly when

$$\chi((c^2 - 1)(ac^2 - d)) = -1.$$

Thus any small set of cheap constants gives a deterministic finite menu: each candidate is tested by one quadratic-character computation. A successful t-candidate, with its companion from Theorem 3.23, gives a complete chart; the derived companion need not belong to the same cheap menu.

Remark 4.26 (Cost of powers of two). For an integer $i \geq 0$ and $c = 2^i$, multiplication by c uses repeated doublings:

$$2^i x = \underbrace{2(2(\cdots 2x))}_{i \text{ doublings}}.$$

Thus D_{2^i} is implemented by i doublings. For small i, this is substantially cheaper than an M-multiplication, and in cost tables it should be kept separate from a general fixed-constant multiplication.

Proposition 4.27 (Cheap selected-coefficient tests). Let $K = \mathbb{F}_q$, q odd.

(1) If $c \in K$ satisfies

$$\chi((c^2 - a)(c^2 - d)) = -1,$$

then $\tau = (c : 1)$ is admissible on the x-side. In any schedule containing the selected layer $2D_t$, choosing $t = c$ replaces this layer by $2D_c$. In particular, if $c = 2^i$, then $2D_c$ is implemented by $2i$ doublings.

(2) If $c \in K$ satisfies

$$\chi((c^2 - 1)(ac^2 - d)) = -1,$$

then $\sigma = (c : 1)$ is admissible on the y-side. In any schedule containing the selected layer $2D_s$, choosing $s = c$ replaces this layer by $2D_c$. The values $c = \pm 1$ are excluded automatically, since then the y-side discriminant is zero.

Proof. Both statements are direct substitutions in the finite-field discriminant criterion. The cost statement follows from the fact that t occurs only in $H + tN$ and $F + tR$, while s occurs only in $E + sV$ and $G + sW$. □

There are two useful ways to choose the menu. The first is to test small integers, such as

$$c \in \{1, 2, 3, 4, \ldots\}.$$

For the t-coefficient, the first tests are

$$c = 1 : \ \chi((a - 1)(d - 1)) = -1, \qquad c = 2 : \ \chi((4 - a)(4 - d)) = -1,$$

and

$$c = 3 : \ \chi((9 - a)(9 - d)) = -1.$$

For the s-coefficient, the first admissible small values start at $c = 2$:

$$c = 2 : \ \chi(3(4a - d)) = -1, \qquad c = 3 : \ \chi(8(9a - d)) = -1.$$

The second, more structured, menu consists of powers of two:

$$C_B = \{2^0, 2^1, \dots, 2^B\}, \qquad B \in \mathbb{Z}_{\geq 0}.$$

For $t = 2^i$, the test is

$$\chi((4^i - a)(4^i - d)) = -1.$$

For $s = 2^j$, with $j \geq 1$, the test is

$$\chi((4^j - 1)(a4^j - d)) = -1.$$

This menu is especially attractive because every multiplication by a selected coefficient is implemented by a short sequence of doublings.

Proposition 4.28 (Power-of-two menu). Let $K = \mathbb{F}_q$, q odd, and put

$$C_B = \{2^i : 0 \leq i \leq B\}.$$

(1) If a schedule only requires a t-coefficient and there exists $0 \leq i \leq B$ such that

$$\chi((4^i - a)(4^i - d)) = -1,$$

then $t = 2^i$ gives an admissible selected coefficient. In the $\Psi_{0,t}$-schedule of Proposition 4.10, the cost becomes

$$10M + 2D_a + D_d + 2D_{2^i},$$

and when the fixed operational model already has $a = -1$, it becomes

$$10M + D_d + 2D_{2^i}.$$

(2) If independent powers of two are desired for s, t and there exist i, j with $0 \leq i \leq B$, $1 \leq j \leq B$, such that

$$\chi((4^j - 1)(a4^j - d)) = -1, \qquad \chi((4^i - a)(4^i - d)) = -1,$$

then $s = 2^j, t = 2^i$ give an admissible selected chart. The separated cost is

$$12M + D_a + D_d + 2D_{2^j} + 2D_{2^i}.$$

If this operational model has $a = 1$, one may simply take $i = j$ and check only $\chi((4^i-1)(4^i-d)) = -1$, with $i \geq 1$. The cost is then $12M+D_d+4D_{2^i}$.

Proof. The two assertions are exactly the two tests of Proposition 4.27 applied to powers of two, together with the corresponding operation counts from Propositions 4.10 and 4.12. □

Remark 4.29 (Approximate coverage of a fixed menu). Here the parameter space is the unnormalized set of ordered pairs (a, d) in fixed nonzero square classes, with $a \neq d$. Fix an integer $r \geq 1$, and let $u_1, \dots, u_r$ be distinct nonzero squares in $K = \mathbb{F}_q$. For the t-tests with candidate squares u_i, the density of pairs on which every test fails is

$$2^{-r} + O_r(q^{-1/2}).$$

Zeros of the tested polynomials change the density by only $O_r(q^{-1})$. In particular the limiting covered density is $1 - 2^{-r}$.

For either prescribed character value $\alpha \in \{\pm 1\}$ and each sign vector $\epsilon \in \{\pm 1\}^r$, the number of z with $\chi(z) = \alpha$ and $\chi(u_i - z) = \epsilon_i$ is $q/2^{r+1} + O_r(\sqrt{q})$. Expand

the indicator as a product of $r+1$ quadratic-character indicators. Every nonconstant term involves a squarefree product of a subset of the distinct linear factors $z, u_1 - z, \dots, u_r - z$; the character-sum bound gives the stated error [LN97]. For a prescribed vector of product signs $\chi((u_i - a)(u_i - d))$, sum over the 2^r possible sign vectors for a; the vector for d is then determined. This gives $q^2/2^{r+2} + O_r(q^{3/2})$ pairs. Removing $a = d$, zero factors and singular cases changes only $O_r(q)$ pairs. Dividing by the branch size $q^2/4 + O(q)$ proves the density.

The same one-variable argument gives $1 - 2^{-r_s} + O_{r_s}(q^{-1/2})$ coverage for an s-menu with r_s distinct nonzero candidate squares different from 1, using d/a as the variable. These are marginal coverage statements. For a normalized model such as $a = 1$, the test $t = 1$ always fails and the $s = t$ tests coincide; the present parameter-space density must not be applied there as an independence assumption.

For the t-menu $C_B = \{2^i : 0 \le i \le B\}$, assume that $4^0, \dots, 4^B$ are distinct. Then $r = B + 1$. Over the unnormalized parameter branch described above, the limiting uncovered and covered densities are as follows, with error $O_B(q^{-1/2})$:

B	C_B	uncovered density	covered density
0	$\{1\}$	$\approx 1/2$	$\approx 1/2$
1	$\{1, 2\}$	$\approx 1/4$	$\approx 3/4$
2	$\{1, 2, 4\}$	$\approx 1/8$	$\approx 7/8$
3	$\{1, 2, 4, 8\}$	$\approx 1/16$	$\approx 15/16$
4	$\{1, 2, 4, 8, 16\}$	$\approx 1/32$	$\approx 31/32$
5	$\{1, 2, 4, 8, 16, 32\}$	$\approx 1/64$	$\approx 63/64$

Thus $C_4 = \{1, 2, 4, 8, 16\}$ has asymptotic t-coverage $31/32$ in this unnormalized parameter space, with the stated error and distinctness condition. This does not assert the same density after fixing $a = 1$, nor that the companion coefficient lies in a prescribed second cheap menu. One successful t-test nevertheless suffices for completeness using the companion rule of Theorem 3.23.

Proposition 4.30 (The $t = 1$ and $(s, t) = (2, 1)$ subcases). Let $K = \mathbb{F}_q$, q odd.

(1) In the nonsquare–nonsquare branch, if

$$\chi((a-1)(d-1)) = -1,$$

then $\sigma = (0 : 1)$, $\tau = (1 : 1)$ is admissible. The formula

$$\Psi_{0,1} = \big(E(F+R) : G(H+N) : G(F+R) : E(H+N)\big)$$

is complete and has cost

$$10M + 2D_a + D_d.$$

If this operational model already has $a = -1$, the cost is

$$10M + D_d.$$

(2) In the square–square branch, if

$$\chi(3(4a-d)) = -1, \qquad \chi((a-1)(d-1)) = -1,$$

then $\sigma = (2 : 1), \tau = (1 : 1)$ is admissible and the cost in this model is $12M + D_a + D_d + 2D_2$. If $c^2 = a$, the transported model $a' = 1$ instead uses $(s', t') = (2, 1/c)$, with cost

$$12M + D_{d'} + 2D_2 + 2D_{1/c}.$$

Multiplication by 2 is implemented by a field doubling.

Proof. The first statement is the $t = 1$ case of the t-test. The second statement uses

$$\Delta_y(2) = 3(4a - d), \qquad \Delta_x(1) = (1 - a)(1 - d).$$

The stated costs follow from Propositions 4.10 and 4.12. □

A normalized square–square alternative. If the fixed model has $a = 1$, the two discriminants coincide for $s = t = c$. Thus $\chi((c^2 - 1)(c^2 - d)) = -1$ gives a complete choice, at cost $12M + D_d + 4D_c$. In particular $s = t = 2$ is valid precisely when $\chi(3(4-d)) = -1$, at cost $12M + D_d + 4D_2$. Here $t = 1$ is inadmissible because $a = 1$ gives $\Delta_x(1) = 0$.

Remark 4.31 (Designing parameters with a prescribed cheap t). The same criterion can be used in the reverse direction. Suppose one wants a prescribed cheap value $t = c$. Choose a fixed nonsquare $\nu \in K^\times \setminus K^{\times 2}$, choose $a \in K^\times$ with $c^2 \neq a$, and set

$$d = c^2 - \frac{\nu}{c^2 - a}.$$

Then $(c^2 - a)(c^2 - d) = \nu$, so $\tau = (c : 1)$ is admissible by construction. The usual curve conditions $d \in K^\times$, $d \neq a$ must still be checked. The y-side can then be supplied by $s = c/r$ if $r^2 = a$, or by $\sigma = (1 : 0)$ if a is a nonsquare. A separately prescribed cheap s still requires its own test. This gives a simple parameter-design principle for families in which a prescribed cheap selected coefficient works by design.

Remark 4.32 (Menus versus existence). The small menus do not replace the existence theorem. They provide a deterministic list of very cheap candidates together with exact character tests. If the menu succeeds, the selected constant layer is cheap or absent. If it fails, one may continue the search over K; the existence theorem guarantees that admissible coefficients exist for $q > 16$.

4.8. **Summary of costs.** We summarize the online costs obtained in this section. The table below is the main cost table: it records the optimized finite-field schedules in the relevant square-class cases, including full addition, raw mixed addition, table-based mixed addition, and affine–affine input.

The general separated selected formula has cost $12M + D_a + D_d + 2D_s + 2D_t$. The elementary charts $(0, 0)$ and $(\infty, 0)$, shorthand for $((0 : 1), (0 : 1))$ and $((1 : 0), (0 : 1))$, remove the selected layer and have cost $9M + D_a + D_d$. When the corresponding split representation is available, these become $8M + D_d$ in the standard case and $8M + D_a$ in the mirror case. Doubling is independent of the selected coefficients and has cost $4M + 4S + \min(D_a, D_d)$.

All costs in the table are online costs in the indicated chart and representation. The table does not replace the completeness criterion: a selected formula is complete only when the corresponding discriminants are nonsquares,

$$\Delta_y(\sigma), \Delta_x(\tau) \in K^\times \setminus K^{\times 2},$$

or, over a finite field, when the equivalent quadratic-character conditions hold.

Remark 4.33 (Source of the mixed and affine savings in the square–square row). In the normalized square–square representation $a' = 1$, the full selected schedule costs $12M + D_{d'} + 2D_s + 2D_t$. The raw mixed reduction uses the normalization

$Y_2 = 1$: the X, Y-block (E, R, H, W) then needs only the two products Y_1X_2 and X_1X_2, instead of four products. This saves two general multiplications and gives

$$10M + D_{d'} + 2D_s + 2D_t.$$

If the second input is a table entry, the table may store $d'T_2$, so the online $D_{d'}$-term is moved to table construction and the online cost becomes

$$10M + 2D_s + 2D_t.$$

For affine–affine input, $Y_1 = Y_2 = 1$, and the same X, Y-block needs only the product X_1X_2. This saves one more multiplication and gives

$$9M + D_{d'} + 2D_s + 2D_t.$$

In this table C and L denote the curve-constant and selection-constant costs specified separately in each row.

case	chart / normalization	C	L
SN	$a' = -1,\ (0, 0)$ $-a \in K^{\times 2}$	$D_{d'}$	0
NS	$d' = -1,\ (\infty, 0)$ $-d \in K^{\times 2}$	$D_{a'}$	0
NN	$a' = -1,\ (0, t)$ $-a \in K^{\times 2}$	$D_{d'}$	$2D_t$
NN_1	$a' = -1,\ (0, 1)$ $-a \in K^{\times 2}$	$D_{d'}$	0
SS	$a' = 1,\ (s, t)$ $a \in K^{\times 2}$	$D_{d'}$	$2D_s + 2D_t$
SS_t	$(a_t, d_t) = (a/t^2, d/t^2)$ $(s, 1)$, admissible	$D_{a_t} + D_{d_t}$	$2D_s$

case	full	mixed raw	mixed table	aff.–aff.
SN	$8M + C$	$7M + C$	$7M$	$6M + S + C$
NS	$8M + C$	$7M + C$	$7M$	$6M + S + C$
NN	$10M + C + L$	$9M + C + L$	$9M + C + L$	$8M + C + L$
NN_1	$10M + C$	$9M + C$	$9M + C$	$8M + C$
SS	$12M + C + L$	$10M + C + L$	$10M + L$	$9M + C + L$
SS_t	$12M + C + L$	$10M + C + L$	$10M + L$	$9M + C + L$

SN, NS, NN, SS denote respectively (S, N), (N, S), (N, N), (S, S); NN_1 is its $t = 1$ subcase and SS_t is the t-normalized square–square case.

TABLE 1. Optimized finite-field online costs in normalized selected charts.

All selection coefficients in the table refer to the stated operational model. In the final row the table stores a_tX_2, d_tT_2, so both curve-constant costs move to precomputation. In this row, as in the square–square row, mixed and affine–affine mean $Y_2 = 1$ and $Y_1 = Y_2 = 1$, respectively. Points outside these charts use full addition.

Remark 4.34 (Normalizations in the mixed and affine columns). The mixed normalization is branch-dependent. In the (S,N) row, mixed means $Z_2 = 1$, and affine–affine means $Z_1 = Z_2 = 1$. In the (N,S) row, mixed means $Y_2 = 1$, and affine–affine means $Y_1 = Y_2 = 1$. In the (N,N) row, either $Y_2 = 1$ or $Z_2 = 1$ gives the displayed mixed count. In the (S,S) row, mixed means $Y_2 = 1$, and affine–affine means $Y_1 = Y_2 = 1$.

Remark 4.35 (Split normalizations). The rows containing $a' = -1$ or $d' = -1$ assume the corresponding split normalization. Thus $a' = -1$ requires $-a \in K^{\times 2}$, and $d' = -1$ requires $-d \in K^{\times 2}$. These are representation conditions, not additional completeness criteria.

Remark 4.36 (The squaring in the affine–affine split rows). The S-term in the first two affine–affine rows comes from a difference-of-squares identity. In the standard split row, $Z_1 = Z_2 = 1$ gives $F = 1-c$, $G = 1+c$, with $c = d'T_1T_2$, so $GF = 1-c^2$. In the mirror split row, $Y_1 = Y_2 = 1$ gives $H = 1-u$, $W = 1+u$, with $u = a'X_1X_2$, so $WH = 1-u^2$. Thus one output multiplication is replaced by one squaring.

Remark 4.37 (Selected and absorbed coefficients). In the nonsquare–nonsquare case only t is needed after fixing $(0,t)$. A choice $t = 1$ in the operational model has no D_t-term. For a nonzero original t, absorption by ν_t changes the model to a_t, d_t, and the costs must use those constants. In the square–square case $2D_s$ remains in the t-normalized schedule. The fourth-power identities guarantee admissibility under the stated hypotheses, not deletion of this remaining term.

Remark 4.38 (Co-Z variants). Co-Z inputs share the coordinate $Z_1 = Z_2$. This evaluation regime is not included in Table 1. In the (N,N) row with chart $(0,t)$, the co-Z cost is

$$9M + S + D_{d'} + 2D_t.$$

In the (S,S) row, the corresponding co-Z cost is

$$11M + S + D_{d'} + 2D_s + 2D_t.$$

In a t-normalized model the corresponding general co-Z costs are $9M + S + 2D_{a_t} + D_{d_t}$ for $(0,1)$, and $11M + S + D_{a_t} + D_{d_t} + 2D_s$ for finite $(s,1)$. These follow by replacing the single product Z_1Z_2 by one squaring; the other layers remain unchanged.

Remark 4.39 (Lazy materialization of T_3). The table counts a fully materialized extended-coordinate output. If the two selected projective pairs are $(A : B)$ and $(C : D)$, the Segre reconstruction is $(AD : BC : BD : AC)$, which costs $4M$. In a controlled chain where the next operation is a doubling, or where the factors A and C are retained, the last product $T_3 = AC$ may be delayed. This saves one online multiplication in that step, but it is not counted in the full-addition costs above. If T_3 has not been formed, a following doubling must use the a-side schedule, which uses only X_3, Y_3, Z_3. The d-side schedule requires T_3. Retaining its factors delays the multiplication but does not remove its cost when a later operation actually needs the materialized coordinate.

Remark 4.40 (Completeness is unchanged by cost refinements). Mixed additions, table precomputation, affine–affine inputs, co-Z evaluation, and lazy materialization are evaluation strategies for the same selected formula. They do not change the exceptional set or the admissibility conditions. All completeness statements still

come from the discriminant criterion. The full law remains complete; a mixed or affine–affine evaluation has the stated chart as its input domain. No normalization is assumed possible for points whose required coordinate is zero.

5. Computational Verification and Comparison

The computational checks cover the explicit formulas, coordinate conventions, selected coefficients, and operation schedules. They test output nonvanishing, curve membership, and agreement with an independent group-law computation.

5.1. **Verification protocol.** The verification was carried out over finite fields of odd characteristic. For each tested field $K = \mathbb{F}_q$ and each nonsingular parameter pair $a, d \in K^\times$, $a \neq d$, we enumerated the K-rational projective points of

$$\mathcal{E}^e_{a,d}: \qquad aX^2 + Y^2 = Z^2 + dT^2, \qquad XY = ZT.$$

The enumeration uses the product parametrization of the quadric $XY = ZT$, so projective points are tested modulo projective scaling.

For every ordered pair $P_1, P_2 \in \mathcal{E}^e_{a,d}(K)$, the selected formula $\Psi_{\sigma,\tau}(P_1, P_2)$ was evaluated. Three checks were then performed. First, the output must be nonzero. Second, it must satisfy the two defining equations of $\mathcal{E}^e_{a,d}$. Third, it must agree projectively with the two-law oracle

$$\mathcal{L}_0 = (EF : GH : GF : EH), \qquad \mathcal{L}_1 = (RV : WN : RW : NV).$$

The oracle uses $\mathcal{L}_0$ when this tuple is nonzero, and uses $\mathcal{L}_1$ exactly when $\mathcal{L}_0$ vanishes. These two laws form the complete system of Bernstein–Lange [BL11] and are independent of the selected coefficients.

The Magma implementation records zero-output failures, membership failures, oracle failures, and projective mismatches. These tests are intended to catch errors in signs, coordinate order, selected-coefficient conventions, normalizations, and branch-dependent schedules. For larger fields, representative curves were also tested in each of the four square-class cases. The selected coefficients were found by the same discriminant tests used in the proof, starting from the low-cost menus of small integers and powers of two.

5.2. **Test families and coefficient selection.** Throughout this subsection $K = \mathbb{F}_q$, q is odd, and χ denotes the quadratic character. The verification tests the four square-class cases separately. The selected coefficients are chosen by the same discriminant criteria used in the proofs.

case	selected chart	criterion	formula
(S, N)	$(0, 0)$	$\chi(d) = -1$	$\Psi_{0,0}$
(N, S)	$(\infty, 0)$	$\chi(a) = -1$	$\Psi_{\infty,0}$
(N, N)	$(0, t)$	$\chi((t^2 - a)(t^2 - d)) = -1$	$\Psi_{0,t}$
(S, S)	(s, t)	$\chi(\Delta_y(s)) = \chi(\Delta_x(t)) = -1$	$\Psi_{s,t}$

Here $(0, 0)$ denotes $((0 : 1), (0 : 1))$, and $(\infty, 0)$ denotes $((1 : 0), (0 : 1))$.

In the (S, N) and (N, S) cases, no finite selected coefficient is needed. The verification therefore tests the elementary standard and mirror charts directly. In the (N, N) case, the script fixes $\sigma = (0 : 1)$ and searches for t. It first tries the cheap menu $t \in \{1, 2, 4, 8, 16, 32\}$, and if the menu fails it continues with a full search in K. In the (S, S) case, the Magma tests use independently selected s, t.

The supplementary Python tests also cover the one-condition choice $t = cs$, with $c^2 = a$.

The tests also include the normalized schedules used in the cost table. Thus, when $-a \in K^{\times 2}$, the $a' = -1$ schedule is checked; when $-d \in K^{\times 2}$, the $d' = -1$ schedule is checked; and in the square–square case the $a' = 1$ normalization is checked. The t-normalized schedules use a_t, d_t and selectors $(s, 1)$. Fourth-power subfamilies are tested for admissibility; their arithmetic costs retain the remaining D_s-terms.

For larger fields, the verification also searches for ordinary and supersingular examples in each square-class case. When both types exist in a given branch, one representative of each type is tested exhaustively on all ordered pairs of projective points. If one type is not found for a particular field and branch, the computation records this fact and continues with the available examples.

5.3. **Exhaustive small-field results.** The first verification run uses the prime fields $\mathbb{F}_p$ listed below and is exhaustive in two senses: all admissible parameters $a, d \in \mathbb{F}_p^\times$, $a \neq d$, are tested, and for each parameter pair all ordered pairs of projective points of $\mathcal{E}^e_{a,d}(\mathbb{F}_p)$ are tested. The following table summarizes this all-parameter projective verification.

p	#parameter pairs	$\sum \#\mathcal{E}^e_{a,d}(\mathbb{F}_p)$	#ordered pairs tested	failures
17	240	4320	81792	0
19	306	6120	128160	0
23	462	11088	276672	0
29	756	22680	702240	0
31	870	27840	917760	0
37	1260	47880	1865952	0
total	3894	119928	3972576	0

In addition, representative projective tests were run over the larger prime fields

$$p = 103, 127, 151, 167, 211, 307, 431, 1009.$$

For these larger fields, the implementation selected curves in the four square-class cases, chose the corresponding admissible coefficients, and tested all ordered projective pairs whenever feasible. For the largest field $p = 1009$, both exhaustive selected-curve tests and sampled tests with 10^6 random ordered projective pairs were used. Across all reported runs, the Magma implementation reported checking 14,744,000 ordered projective input pairs.

All failure counters were zero. In every reported test, the selected formula had nonzero output, the output lay on $\mathcal{E}^e_{a,d}$, and the output agreed projectively with the two-law oracle.

Independent reproducible checks. An accompanying Python 3/NumPy implementation checks the formulas and schedules using an independent Montgomery group law. It is run by

`python verify_selected_edwards.py`.

It reproduces every count in the small-field table, using one admissible finite selection pair per curve and all ordered projective input pairs. Its reference operation is chord-and-tangent arithmetic on $Bv^2 = u^3 + Au^2 + u$, with $A = 2(a + d)/(a - d)$,

$B = 4/(a-d)$. The ordinary map is $u = (1+y)/(1-y), v = u/x$; the identity and $(0,-1)$ are handled separately, and the boundary maps are

$$(0 : Y : 0 : T) \mapsto (-1, -Y/T), \qquad (X : 0 : 0 : T) \mapsto ((X+T)/(X-T), 0).$$

All 3 972 576 comparisons pass. The accompanying implementation also checks the full and mixed schedules in Section 4, operation counts, both doubling schedules, and the normalization rule with $c = 2, 3$ on 7 945 152 ordered pairs. The t-normalized representations are checked separately, with their new curve constants included. Projection vanishing at (P, O) is tested for all projective selection coefficients over $\mathbb{F}_{17}$.

Further checks cover all admissible cases over the prime fields $3, 5, 7, 11, 13$, and one curve in each of the four square-class branches over each of $\mathbb{F}_9, \mathbb{F}_{25}, \mathbb{F}_{49}$. The two parameter pairs $(a, d) = (1, 4), (4, 1)$ over $\mathbb{F}_5$ have no admissible projective selector pair and are recorded as such. They do not contradict the existence theorem for $q > 16$. The larger-field Magma aggregate is reported separately from these Python counts; the accompanying JSON output specifies the fields, cases, and counts. Additional checks of one-condition selection cover every finite t, both square roots when a is a square, and $s = \infty$ otherwise, over $\mathbb{F}_p$ for $p = 3, 5, 7, 11, 13, 17, 19$. On 812 curves, all 19 314 coefficient choices and 6 545 520 ordered-pair evaluations satisfy the completeness criterion and agree with the Montgomery sum wherever the formula is defined.

5.4. **Relation to existing complete-addition frameworks.** The geometric language used in this paper is the classical language of addition laws, exceptional sets, complete systems, and difference divisors. In that sense the construction fits into the framework developed by Lange–Ruppert, Bosma–Lenstra, Kohel, and Arene–Kohel–Ritzenthaler [LR85, LR87, BL95, Koh11, AKR12]. The present paper uses this viewpoint in the product-coordinate geometry associated with extended twisted Edwards coordinates.

The arithmetic formulas themselves are also rooted in known Edwards and extended Edwards arithmetic. The Edwards, twisted Edwards, and extended coordinate formulas of Edwards, Bernstein–Lange, Bernstein–Birkner–Joye–Lange–Peters, and Hisil–Wong–Carter–Dawson provide the basic product laws used here [Edw07, BL07, BBJLP08, HWCD08]. We apply the selection mechanism to these known product laws: a single product formula is chosen by projective coefficients, and the discriminant criterion gives completeness over the rational point set.

This differs from complete systems of addition laws. For example, Bernstein–Lange complete systems show how several laws can cover all input pairs even when one standard Edwards law is incomplete [BL11]. Here, after the coefficients s, t have been fixed, the arithmetic uses one selected polynomial formula. Completeness is obtained by choosing the exceptional fibres so that they have no rational points over the base field.

Complete formulas on short Weierstrass curves, such as the formulas of Renes–Costello–Batina, give a different and complementary approach to complete addition [RCB16]. They apply to Weierstrass models and broad curve classes. The present work remains in the Edwards-type setting and exploits the product structure and extended-coordinate sharing available there.

Finally, transfer results between Edwards-type and Montgomery-type representations show that complete source laws can be transported to other coordinate

Framework	Main mechanism	Role in this paper
Lange–Ruppert; Bosma–Lenstra	Addition laws, complete systems, and difference divisors	Geometric framework for exceptional sets and completeness
Bernstein–Lange complete systems	Several Edwards laws cover all input pairs	Background complete system and comparison point
Extended Edwards formulas	Known product laws in extended coordinates	Source arithmetic used in the selected formula
Scaled extended Edwards schedules	Low-cost formulas after parameter scaling	Baseline for the $8M+D$ elementary branches
Renes–Costello–Batina	Complete formulas on short Weierstrass curves	Complementary complete-addition framework in another model
Extended Montgomery transfer work	Transport of complete Edwards-side laws to Montgomery-type coordinates	Motivation for strengthening the Edwards-side source law
This paper	Finite-field selection of one product formula	Single selected formula after coefficient selection

TABLE 2. Relation with existing complete-addition frameworks.

systems [FFS24]. The selected formula supplies a complete Edwards-side law for these transfers in the square-class cases covered by the discriminant criterion.

The scaling techniques used in the known extended Edwards schedules are also part of the baseline. In the elementary split branches, the costs (8M+D) come from the already known scaled extended-coordinate schedules. The discriminant criterion determines when the selected product formula is complete over the base field.

The comparison is summarized in Table 2.

The construction selects a single product formula whose exceptional fibres avoid the rational difference set, with explicit coefficient criteria and evaluation schedules.

6. Conclusion

We proved completeness for a single selected product formula on the extended-coordinate representation $\mathcal{E}^e_{a,d}$ of twisted Edwards curves over finite fields of odd characteristic. The formula is obtained from the classical extended Edwards product laws by fixing two projective selected coefficients. The central criterion is that the two exceptional fibres selected by these coefficients have no rational points. For finite fields this condition is expressed by the nonsquareness of the two discriminants

$$\Delta_y(\sigma), \Delta_x(\tau).$$

Selecting a complete member needs only one condition: if $a = c^2$, set $t = cs$, so the two discriminants have the same square class; otherwise fix $s = \infty$ and test only t. In the normalized model $a = 1$, the choice $s = t$ makes the two tests identical.

The square-class analysis gives a uniform way to choose the selected chart. In the opposite-square-class cases, the elementary charts $(0, 0)$ and $(\infty, 0)$ recover the

known complete Edwards-type situations and their mirror form. In the same-square-class cases, where the elementary charts no longer suffice, the selected coefficients s, t move the exceptional fibres away from the rational difference set. The existence argument gives admissible coefficients for $q > 16$, and the finite-field coefficient menus provide a simple deterministic way to find low-cost choices in practice.

We also recorded explicit operation schedules for the selected formula. In the split elementary branches, the online cost remains $8M + D$, while the same-square-class branches require the additional selected-constant layer $2D_t$ or $2D_s + 2D_t$. Small coefficients and powers of two reduce these costs. A nonzero t can be absorbed by the explicit model change ν_t, with the new curve constants counted; the fourth-power conditions give admissible subfamilies but do not alone remove $2D_s$. The doubling specialization is independent of the selected coefficients. The Magma verification was carried out at the projective level: the selected formula was checked against a complete two-law oracle, and the reported tests produced no zero-output, membership, oracle, or projective-mismatch failures.

Further work includes reducing the multiplication count in the same-square-class schedules, extending selected-fibre constructions to other $\mathbb{P}^1 \times \mathbb{P}^1$-type models, and studying how the present completeness criteria affect transfers to Montgomery-type representations.

A related direction is to apply the same selected-fibre method to the standard law and companion product laws in the other elliptic-curve models.

References

AKR12. C. Arene, D. Kohel, and C. Ritzenthaler, Complete addition laws on abelian varieties, LMS Journal of Computation and Mathematics 15, 308–316, 2012. DOI: https://doi.org/10.1112/S1461157012001027.

BBJLP08. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, Twisted Edwards curves, Progress in Cryptology – AFRICACRYPT 2008, Lecture Notes in Computer Science 5023, 389–405, Springer, 2008. DOI: https://doi.org/10.1007/978-3-540-68164-9_26. Available at: https://eprint.iacr.org/2008/013.

BL07. D. J. Bernstein and T. Lange, Faster addition and doubling on elliptic curves, Advances in Cryptology – ASIACRYPT 2007, Lecture Notes in Computer Science 4833, 29–50, Springer, 2007. DOI: https://doi.org/10.1007/978-3-540-76900-2_3. Available at: https://eprint.iacr.org/2007/286.

BL11. D. J. Bernstein and T. Lange, A complete set of addition laws for incomplete Edwards curves, Journal of Number Theory 131(5), 858–872, 2011. DOI: https://doi.org/10.1016/j.jnt.2010.06.015. Available at: https://cr.yp.to/newelliptic/completed-20101006.pdf.

BL95. W. Bosma and H. W. Lenstra Jr., Complete systems of two addition laws for elliptic curves, Journal of Number Theory 53(2), 229–240, 1995. DOI: https://doi.org/10.1006/jnth.1995.1088. Available at: https://www.math.ru.nl/~bosma/pubs/JNT1995.pdf.

BJ02. É. Brier and M. Joye, Weierstraß elliptic curves and side-channel attacks, Public Key Cryptography – PKC 2002, Lecture Notes in Computer Science 2274, 335–345, Springer, 2002. DOI: https://doi.org/10.1007/3-540-45664-3_24.

BJ03. O. Billet and M. Joye, The Jacobi model of an elliptic curve and side-channel analysis, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes – AAECC 2003, Lecture Notes in Computer Science 2643, 34–42, Springer, 2003. DOI: https://doi.org/10.1007/3-540-44828-4_4.

CS18. C. Costello and B. Smith, Montgomery curves and their arithmetic, Journal of Cryptographic Engineering 8(3), 227–240, 2018. DOI: https://doi.org/10.1007/s13389-017-0157-6. Available at: https://arxiv.org/abs/1703.01863.

Edw07. H. M. Edwards, A normal form for elliptic curves, Bulletin of the American Mathematical Society 44(3), 393–422, 2007. DOI: https://doi.org/10.1090/S0273-0979-07-01153-6.

EFD. D. J. Bernstein and T. Lange, Explicit-Formulas Database: extended coordinates for twisted Edwards curves, Available at: https://www.hyperelliptic.org/EFD/g1p/auto-twisted-extended.html. Accessed: 14 June 2026.

FFS24. R. R. Farashahi, M. Fadavi, and S. Sabbaghian, Faster complete addition laws for Montgomery curves, IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(4), 737–762, 2024. DOI: https://doi.org/10.46586/tches.v2024.i4.737-762.

FH17. R. R. Farashahi and S. G. Hosseini, Differential addition on twisted Edwards curves, Information Security and Privacy – ACISP 2017, Lecture Notes in Computer Science 10343, 366–378, Springer, 2017. DOI: https://doi.org/10.1007/978-3-319-59870-3_21.

FJ10. R. R. Farashahi and M. Joye, Efficient arithmetic on Hessian curves, Public Key Cryptography – PKC 2010, Lecture Notes in Computer Science 6056, 243–260, Springer, 2010. DOI: https://doi.org/10.1007/978-3-642-13013-7_15. Available at: https://marcjoye.github.io/papers/FJ10ghess.pdf.

His09. H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson, Jacobi quartic curves revisited, Information Security and Privacy – ACISP 2009, Lecture Notes in Computer Science 5594, 452–468, Springer, 2009. DOI: https://doi.org/10.1007/978-3-642-02620-1_31.

HWCD08. H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson, Twisted Edwards curves revisited, Advances in Cryptology – ASIACRYPT 2008, Lecture Notes in Computer Science 5350, 326–343, Springer, 2008. DOI: https://doi.org/10.1007/978-3-540-89255-7_20. Available at: https://eprint.iacr.org/2008/522.

JQ01. M. Joye and J.-J. Quisquater, Hessian elliptic curves and side-channel attacks, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Computer Science 2162, 402–410, Springer, 2001. DOI: https://doi.org/10.1007/3-540-44709-1_33.

Koh11. D. Kohel, Addition law structure of elliptic curves, Journal of Number Theory 131(5), 894–919, 2011. DOI: https://doi.org/10.1016/j.jnt.2010.12.001. Available at: https://arxiv.org/abs/1005.3623.

KPKK19. J. Kim, J. H. Park, D.-C. Kim, and W.-H. Kim, Complete addition law for Montgomery curves, Information Security and Cryptology – ICISC 2019, Lecture Notes in Computer Science 11975, 260–277, Springer, 2020. DOI: https://doi.org/10.1007/978-3-030-40921-0_16.

RCB16. J. Renes, C. Costello, and L. Batina, Complete addition formulas for prime order elliptic curves, Advances in Cryptology – EUROCRYPT 2016, Lecture Notes in Computer Science 9665, 403–428, Springer, 2016. DOI: https://doi.org/10.1007/978-3-662-49890-3_16. Available at: https://eprint.iacr.org/2015/1060.

SC. D. J. Bernstein and T. Lange, SafeCurves: completeness, Available at: https://safecurves.cr.yp.to/complete.html. Accessed: 14 June 2026.

LR85. H. Lange and W. Ruppert, Complete systems of addition laws on Abelian varieties, Inventiones Mathematicae 79 (1985), 603–610.

LR87. H. Lange and W. Ruppert, Addition laws on elliptic curves in arbitrary characteristics, Journal of Algebra 107 (1987), 106–116.

Har77. R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics 52, Springer, New York, 1977.

Sil09. J. H. Silverman, The Arithmetic of Elliptic Curves, 2nd ed., Graduate Texts in Mathematics 106, Springer, Dordrecht, 2009.

LN97. R. Lidl and H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997.

Mon87. P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, Mathematics of Computation 48 (1987), no. 177, 243–264.