Complete Addition on Short Weierstrass Curves with Point-Free Lines

Ruhallah Mirzaei Aliarabi[1] Reza Rezaeian Farashahi[1,2]

[1] Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156-83111, Iran

[2] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran

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

Abstract

Let $E_{a,b} : Y^2Z = X^3 + aXZ^2 + bZ^3$ be a nonsingular short-Weierstrass curve over a field K of characteristic different from 2 and 3. A nonvertical line $Y = mX + nZ$ has no K-rational point on the curve if and only if $x^3 - m^2x^2 + (a - 2mn)x + b - n^2$ is rootless in K. We give coordinate changes and formulas for the corresponding K-complete Bosma–Lenstra addition law. An incidence count proves that such a line exists over every finite field in the stated characteristic. The classical five-multiplication cross-product identity reduces the output computation by one multiplication. For normalized horizontal, sloped, and depressed families, the full/full costs are $13M+5D+30A$, $13M+5D+33A$, and $13M+(2 \text{ to } 5)D+60A$, respectively. Horizontal normalization requires a nonzero cube parameter; the depressed family always contains a point-free line over $\mathbb{F}_p$ for $p \geq 47$. The zero-line formula costs $11M + 3D_a + 2D_{3b} + 28A$ and is complete over finite K exactly when $\#E(K)$ is odd. We also give complete doubling formulas, account for changes of coordinates, and apply the five-product identity to published Hessian addition formulas.

1 Introduction

Elliptic-curve scalar multiplication repeatedly adds points whose relations may depend on secrets. Standard short-Weierstrass formulas distinguish generic addition, doubling, inverse pairs, and the identity. Exceptional procedures complicate correctness arguments and have formed an attack surface [9, 15, 19]. A complete law evaluates the sum of every pair of rational points

by one polynomial routine. It still requires constant-time field arithmetic, input validation, and suitable fault protection in an implementation [6, 19].

Completeness here is arithmetic: the exceptional divisor of an individual plane-cubic law may have geometric points but no points over the base field K. We call this K-completeness. A unified formula, which also handles doubling, need not be complete [9, 16, 1].

Background and objective. Lange–Ruppert developed polynomial addition laws; Bosma–Lenstra described the bidegree-$(2,2)$ Weierstrass laws and their exceptional divisors in terms of projective lines [17, 8]. Later work clarified the geometry of completeness and proved existence of a complete biquadratic law on every finite-field Weierstrass curve with $q \geq 5$ [1, Theorem 4.3]. RCB selected the line $Y = 0$ and gave efficient complete schedules for odd-order short-Weierstrass groups [19, Eq. (1), Algorithms 1–2]. Their full/full profile is $12M + 3D_a + 2D_{3b} + 23A$.

The objective here is an explicit selection, transport, and scheduling construction on short Weierstrass curves. The zero line is point-free exactly when nonzero rational 2-torsion is absent, so a general finite-field construction must also admit other lines. For

$$E_{a,b} : Y^2Z = X^3 + aXZ^2 + bZ^3, \qquad \ell_{m,n} : Y = mX + nZ,$$

the intersection test is the rootlessness of

$$f_{m,n}(x) = x^3 - m^2x^2 + (a - 2mn)x + b - n^2. \tag{1}$$

We use the selected line both as a completeness certificate and as a coordinate parameter. Transport to an adapted section $V = 0$ exposes a common six-product output pattern.

The algebraic reduction. The classical five-multiplication cross-product identity [12, 10] evaluates this output pattern. Lemma 3.2 gives a self-contained reconstruction and proof. The lemma includes the explicit five-product form and an equivalent $5M + 8A$ realization used by the exact ledgers. Its proof is a polynomial identity over any commutative ring; it uses no curve equation or completeness assumption. Applied to the zero-line law, it gives $11M + 3D_a + 2D_{3b} + 28A$ in the same projective state and with the same fixed layer as RCB. The reduction exchanges one generic multiplication for five additional additions.

Contributions and scope. We construct the law attached to every non-vertical point-free affine line, with separate horizontal and non-horizontal transports. An exact incidence count gives the number of such lines over a finite field. We prove selection bounds for horizontal, zero-intercept sloped, and depressed families; the depressed family covers every nonsingular model over $\mathbb{F}_p$ for $p \geq 47$. The normalized sloped row costs $13M + 5D + 33A$; depressed rows cost $13M + (2 \text{ to } 5)D + 60A$ under their stated selector conditions. Horizontal cube normalization costs $13M + 5D + 30A$ and requires the nonzero normalization parameter to be a cube.

We also reconstruct the Bosma–Lenstra Section 5 representative and independently verify the two printed-term corrections already recorded by Bernstein–Lange [7, Figure 1.2 and its caption]. We establish explicit contracts for full/full addition, mixed addition, a selected table operand, and complete doubling. The output is a reusable projective point in the stated coordinate representation, with conversion costs counted explicitly.

Short standard- and generalized-Hessian examples illustrate the portability of the five-product lemma. Their underlying formulas remain those of the EFD and Rezaeian Farashahi–Joye [3, 11]; only the output evaluation is refactored. These examples do not change the principal focus on complete short-Weierstrass addition or import a different model's completeness hypotheses into the Weierstrass construction.

Sections 2–3 give the geometry, transport, and algebraic lemma. Section 4 gives the selectors and chainable arithmetic; Section 5 records the Hessian examples. Verification and comparison follow in Sections 6–7, with construction identities and auxiliary proofs in the appendices.

2 Background and conventions

Throughout, K is a field with $\operatorname{char} K \neq 2, 3$, and $E = E_{a,b}$ is nonsingular, so $4a^3 + 27b^2 \neq 0$. The identity is $O = (0 : 1 : 0)$. Standard facts about Weierstrass models and their group law are used as in [21, Ch. III].

2.1 Addition laws and point-free lines

A bidegree-(μ, ν) addition law is a triple of polynomials homogeneous of degree μ in the first projective input and degree ν in the second. Its restriction to $E \times E$ is not identically zero and represents $P + Q$ wherever its coordinates do not vanish simultaneously. A common zero is an *exceptional pair*. A single law is K-complete if it has no exceptional pair in $E(K)^2$; this

differs from a complete *system*, in which several laws cover one another's base loci [17, 8, 1].

A projective line $\ell \subset \mathbb{P}^2_K$ is K-point-free for E if $E(K) \cap \ell(K) = \varnothing$. For example, $Y = 0$ is point-free iff $x^3 + ax + b$ is rootless in K, equivalently iff $E(K)$ has no nonzero rational point of order two [21, Ch. III].

Theorem 2.1 (Bosma–Lenstra line correspondence)**.** *For a Weierstrass cubic E/K, projective lines $\ell : aX + bY + cZ = 0$ correspond, up to nonzero scalar, to nonzero bidegree-$(2, 2)$ addition laws. The exceptional divisor of the law $\mathcal{A}_\ell$ is the inverse image of the scheme $E \cap \ell$ under the difference map $d(P, Q) = P - Q$. Hence $\mathcal{A}_\ell$ is K-complete iff ℓ is K-point-free.*

Proof. This is Theorem 2 and its construction in [8, pp. 234–239]. □

For the difference morphism $s : E \times E \to E$ and $\ell = uX + vY + wZ$, Bosma–Lenstra represent the associated section of the addition-law bundle by multiplying a fixed law by $s^*(uX/Z + vY/Z + w)$ on the affine chart. Clearing denominators gives a bidegree-$(2, 2)$ polynomial triple with exceptional divisor $s^*(E \cap \ell)$, including multiplicities [8, pp. 235–239].

The completeness criterion follows directly. If $E(K) \cap \ell = \varnothing$, then no rational difference $P - Q$ lies on ℓ, so there is no exceptional pair in $E(K)^2$. Conversely, if $R \in E(K) \cap \ell$, then (R, O) is exceptional because $R - O = R$.

2.2 Transport and equality conventions

Over $\overline{K}$, Bézout's theorem gives a length-three intersection $E \cap \ell$, so every individual line law has a geometric exceptional divisor. A complete *system* of formulas covers these exceptional loci [13, Ch. I, Sec. 7].

Lemma 2.2 (Transport)**.** *Let $\phi : E \to E'$ be induced by an invertible projective linear change of coordinates over K, and suppose that $\phi(O) = O'$, where O and O' are the chosen group identities. Transporting an addition law on E' through ϕ transports its exceptional pairs bijectively and preserves K-completeness. If the law of E' corresponds to a line ℓ', the transported law corresponds to $\phi^{-1}(\ell')$.*

Proof. The transported triple evaluates as $\phi^{-1}(\mathcal{A}'(\phi(P), \phi(Q)))$. An isomorphism of elliptic curves preserving the identity preserves the group law [21, Ch. III, Sec. 4]; invertibility also preserves simultaneous vanishing. The line statement follows from Theorem 2.1. □

Polynomial equality is checked in the stated coefficient ring; projective equality is checked by cross products. If F_1, F_2 are the input curve equations, an identity

$$C = Q_1F_1 + Q_2F_2$$

certifies $C = 0$ in the coordinate ring. The accompanying symbolic certificates record the coefficient domain, polynomial generators, reduction order, and quotients Q_1, Q_2.

2.3 Operation counts and input restrictions

M and S denote generic multiplication and squaring, and A denotes a field addition or subtraction. Negation, assignment, and permutation are free; multiplication by a small integer is expanded into an addition chain and included in the stated A-count. The symbol D_c denotes multiplication by a fixed curve or line constant c. Constants are precomputed during setup. Online counts include the stated input preparation, fixed products, and output computation. Coordinate conversions are listed separately when an accumulator uses a different representation.

Operation	Input restriction	Reuse
full/full	arbitrary projective inputs	closed
Z-mixed	$Z_2 = 1$; the table chart excludes O	accumulator
full+selected	zero-line table point with $Y_2 = 1$	accumulator
doubling	one arbitrary full projective input	closed

Here *closed* means that the output can feed the same row, whereas *accumulator* means that only the unrestricted accumulator can be reused. Reuse is a representation property, independent of the polynomial law's K-completeness.

3 The point-free line law

3.1 Intersection criterion and adapted models

Proposition 3.1 (Affine line criterion)**.** *The line $\ell_{m,n} : Y = mX + nZ$ is K-point-free if and only if the cubic*

$$f_{m,n}(x) = x^3 - m^2x^2 + (a - 2mn)x + b - n^2$$

has no root in K. If $m = 0$, this is the rootlessness of $g_n(x) = x^3+ax+b-n^2$.

Proof. The line does not contain O. In the affine chart, substituting $y = mx + n$ into $y^2 = x^3 + ax + b$ gives $f_{m,n}(x) = 0$, with a bijection between its K-roots and $E(K) \cap \ell_{m,n}$. □

For $m \neq 0$, set

$$X = m^2X', \quad Y = m^3Y', \quad A = a/m^4, \quad B = b/m^6, \quad \eta = n/m^3.$$

This scaling carries the original curve $E = E_{a,b}$ to the normalized short-Weierstrass curve

$$E'_{A,B} : Y'^2Z = X'^3 + AX'Z^2 + BZ^3,$$

and carries $\ell_{m,n}$ to $Y' = X' + \eta Z$. The further change

$$T = X' + \eta Z, \qquad V = Y' - X' - \eta Z = Y' - T, \qquad Z = Z$$

gives the adapted long model

$$V^2Z + 2TVZ = T^3 + A_2T^2Z + A_4TZ^2 + A_6Z^3, \tag{2}$$

where

$$A_2 = -(3\eta + 1), \qquad A_4 = A + 3\eta^2, \qquad A_6 = B - A\eta - \eta^3.$$

The selected line is $V = 0$. Moreover, its intersection cubic $h_\eta(t) = t^3 + A_2t^2 + A_4t + A_6$ satisfies $h_\eta(x/m^2 + \eta) = m^{-6}f_{m,n}(x)$, so rootlessness is preserved. Indeed $X' = T - \eta Z$, $Y' = V + T$ sends the line equation to $V = 0$; substitution in the short equation and collection gives (2); and direct expansion gives the displayed cubic identity. Appendix B.1 gives the corresponding polynomial identities.

The horizontal branch uses no slope division. With $V = Y - nZ$, the curve is

$$V^2Z + 2nVZ^2 = X^3 + aXZ^2 + (b - n^2)Z^3, \tag{3}$$

again with selected line $V = 0$. The split is necessary because the non-horizontal normalization uses m^{-1} and is undefined at $m = 0$. The two models have $a_1 = 2, a_3 = 0$ and $a_1 = a_2 = 0, a_3 = 2n$, respectively.

3.2 The non-horizontal master schedule

Let $P_i = (T_i : V_i : Z_i)$ on (2) and put

$$W_i = V_i + 2T_i, \quad \Pi = T_1T_2, \quad R = Z_1Z_2, \quad U = T_1Z_2 + T_2Z_1,$$
$$\alpha = T_1W_2, \quad \beta = V_1T_2, \quad Q = V_1V_2, \quad \gamma = W_1Z_2, \quad \delta = Z_1V_2, \quad S = \gamma + \delta,$$
$$L = \alpha + \beta - \eta S, \quad C_L = A_4 + \eta A_2, \quad D_L = \eta A_4 + 3A_6,$$
$$E_L = -A_4^2 - 9\eta A_6,$$
$$H_1 = C_L(\Pi + U), \quad H_2 = D_L(U + R), \quad H_3 = (C_L - D_L)U.$$

The remaining blocks and output are

$$\begin{aligned} X_c &= Q + 2\beta - A_2\Pi - A_4U - 3A_6R, \\ M &= -\eta(Q + 2\beta) + H_1 - H_3 + E_LR, \\ N &= Q - \Pi + H_2 + H_3 + 2\eta\gamma, \\ G &= 3\Pi + A_2U + A_4R + 2\gamma, \\ (T_3, V_3, Z_3) &= (X_cL - SM,\ X_cN + GM,\ GL + SN). \end{aligned} \tag{4}$$

The output map is a cross product: for $u = (X_c, S, -G)$ and $v = (M, L, N)$, one has $u \times v = (Z_3, -V_3, T_3)$. Its evaluation in five multiplications is classical [12]; the author's 2015 revised preface traces it to Fiduccia's 1973 thesis. We record two self-contained realizations for use in the curve schedules.

Lemma 3.2 (Five-product reconstruction)**.** *Let X_c, G, L, M, N, and S be elements of a commutative ring. The three outputs in* (4) *admit the following five-product reconstruction. Set*

$$r_0 = S(M - N), \quad r_T = X_c(L - N), \quad r_Z = G(L - M),$$
$$r_V = (S + G)M, \qquad r_N = (X_c - S)N,$$

and recover

$$T_3 = r_T + r_N - r_0, \qquad V_3 = r_N + r_V - r_0, \qquad Z_3 = r_Z + r_V - r_0.$$

Ericson's cross-product formula [10, Sec. 3.3.5] gives the following equivalent realization under the substitution u, v above:

$$s_1 = X_c - S, \quad s_2 = L + N, \quad s_3 = s_1 + G, \quad s_4 = M - s_2,$$
$$m_1 = -GM, \quad m_2 = X_cN, \quad m_3 = s_1s_2,$$
$$m_4 = Ls_3, \quad m_5 = Ss_4, \quad h = m_3 - m_2,$$
$$T_3 = h - m_5, \qquad V_3 = m_2 - m_1, \qquad Z_3 = m_4 - h.$$

This latter realization costs exactly $5M + 8A$, with no squaring, division, or multiplication by a curve constant.

Proof. Expansion gives $r_T + r_N - r_0 = X_c L - SM$, $r_N + r_V - r_0 = X_c N + GM$, and $r_Z + r_V - r_0 = GL + SN$.

For the second realization, expansion gives the same three expressions. Its four input additions, one addition forming h, and three output additions give $8A$. The first realization also uses five products; sharing $r_V - r_0$ gives a $5M + 10A$ implementation of that form. □

Compared with direct evaluation, the $5M + 8A$ realization saves one multiplication and uses five additional additions. Its runtime therefore depends on the field implementation. Section 5 gives applications to Hessian addition.

Reusing the output reduction. The six direct products

$$X_c L, \quad SM, \quad X_c N, \quad GM, \quad GL, \quad SN$$

form the three coordinates in Lemma 3.2. The five-product realization evaluates the same polynomials over any commutative ring, without a curve equation or completeness hypothesis. It therefore applies whenever an addition formula supplies the six input blocks. Its full cost includes the computation of those blocks, fixed multipliers, and any input or output coordinate changes.

3.3 Specialization of the Bosma–Lenstra law

We use the two corrections to the printed Bosma–Lenstra law recorded by Bernstein–Lange [7, Fig. 1.2 and its caption]. The following derivation independently recovers their specializations from the construction preceding the printed expansion. Let $\mathcal{B}^{(1)}$ be the first explicit Bosma–Lenstra law and normalize $\mathcal{B}^{(2)}_{\mathrm{der}} = s^*(Y/Z)\mathcal{B}^{(1)}$ by its unchanged third coordinate. The displayed functions on pp. 235–237 of [8] are denominator-cleared in Appendix A, which also states the reconstructible quotient identity for each residual.

Proposition 3.3 (Specializations of the known Bosma–Lenstra corrections)**.** *For $(a_1, a_2, a_3, a_4, a_6) = (2, A_2, 0, A_4, A_6)$, put $D = T_1 Z_2$, $E = T_2 Z_1$, and $B_0 = 3A_2A_6 - A_4^2$. Then*

$$T_{\mathrm{der}} = T_{\mathrm{print}}, \qquad Z_{\mathrm{der}} = Z_{\mathrm{print}}, \qquad V_{\mathrm{der}} = V_{\mathrm{print}} + B_0 D(D + 2E).$$

For $(0,0,\lambda,a,c)$, writing $xz = X_1Z_2$, $zx = X_2Z_1$,

$$X_{\mathrm{der}} = X_{\mathrm{print}} - \lambda a\, zx(3xz - zx),$$
$$V_{\mathrm{der}} = V_{\mathrm{print}} - a^2 xz(xz + 2zx), \qquad Z_{\mathrm{der}} = Z_{\mathrm{print}}.$$

Thus the coefficient of $D(D+2E)$ in the first specialization is $12A_6 + 2B_0$, rather than the printed $12A_6 + B_0$.

Proof. In the affine chart, put $d = x_1 - x_2$. With the common sign fixed as in Appendix A, the construction gives $Z_{\mathrm{der}} = -s^*(Y/Z)d^3$, $X_{\mathrm{der}} = fZ_{\mathrm{der}}$, and $V_{\mathrm{der}} = gZ_{\mathrm{der}}$. Substitution of the source formulas, clearing d^3, and reduction by the two input curve equations gives the two displayed residual identities above.

Appendix A gives the coefficient calculation; the six quotient decompositions certify these identities modulo the input curve equations. □

Let $\widetilde{E}_\eta$ denote the curve (2).

Theorem 3.4 (Adapted addition law)**.** *The triple* (4) *is the corrected Bosma–Lenstra bidegree-$(2,2)$ law for $V = 0$ on* (2)*. Its exceptional divisor is*

$$d^{-1}\big(\widetilde{E}_\eta \cap \{V = 0\}\big),$$

and it is K-complete whenever h_η is rootless.

Proof. Theorem 2.1 and its Section 5 construction make $\mathcal{B}^{(2)}_{\mathrm{der}}$ a valid law. Proposition 3.3 identifies its corrected coordinates. Exact collection then gives

$$GL + SN - Z_{\mathrm{der}} = -(A_2 + 3\eta + 1)\Pi S,$$
$$X_cL - SM - T_{\mathrm{der}} = 4A_6RS(A_2 + 3\eta + 1),$$
$$X_cN + GM - V_{\mathrm{der}} = (A_2 + 3\eta + 1)C_V,$$

where

$$C_V = A_2\Pi^2 + A_4\Pi U - \Pi Q - 2\Pi\beta - 9A_6\Pi R - 4A_2A_6UR - 4A_4A_6R^2 - 8A_6\gamma R.$$

All three vanish because $A_2 + 3\eta + 1 = 0$, proving coordinate-wise schedule equality. The exceptional divisor now follows from Theorem 2.1, and rootlessness eliminates its K-points. □

3.4 Horizontal addition law

For $P_i = (X_i : Y_i : Z_i)$ on the original short model, put

$$\begin{gathered} P = X_1X_2, \quad Q = Y_1Y_2, \quad R = Z_1Z_2, \\ T = X_1Y_2 + Y_1X_2, \quad U = X_1Z_2 + Z_1X_2, \quad \Sigma = Y_1Z_2 + Z_1Y_2, \\ h = X_1Z_2 - Z_1X_2, \quad u = X_1Y_2 - Y_1X_2, \quad k = Z_1Y_2 - Y_1Z_2. \end{gathered}$$

With $C = 3b$, define

$$\begin{gathered} Z_c = aU + CR, \quad X_c = Q - Z_c, \quad Z_s = Q + Z_c, \\ G = 3P + aR, \quad H_c = a(P - aR) + CU, \\ L = T - nh, \qquad M = H_c + nu, \qquad N = Z_s - nk. \end{gathered}$$

The transported horizontal law is

$$\mathcal{H}_n(P_1, P_2) = (X_cL - \Sigma M,\ X_cN + GM,\ \Sigma N + GL), \tag{5}$$

with the same five-product output core.

Theorem 3.5 (Horizontal line law)**.** *The triple* (5) *is the corrected Bosma–Lenstra law for $Y = nZ$. It is K-complete iff $g_n(x) = x^3 + ax + b - n^2$ is rootless.*

Proof. Use Proposition 3.3 with $\lambda = 2n$ and $c = b - n^2$. Direct collection identifies its corrected triple with (5); Theorem 2.1 gives the exceptional line, and Proposition 3.1 gives the rootless criterion. The horizontal transport $Y = V + nZ$ is invertible. □

At $n = 0$, the first-coordinate correction vanishes and the second coordinate has coefficient $-2a^2$, consistent with RCB equation (1). Appendix A.4 verifies both laws by comparison with the chord formula and by their restrictions to $Q = O$.

3.5 Transport to the original line

Theorem 3.6 (Master point-free affine-line law)**.** *Let $\ell_{m,n} : Y = mX + nZ$ be nonvertical. If $f_{m,n}$ in* (1) *is rootless, then:*

1. *if $m = 0$,* (5) *is a K-complete law attached to $\ell_{0,n}$;*

2. *if* $m \neq 0$, *transport of* (4) *through*

$$(T : V : Z) = \big(X/m^2 + \eta Z : Y/m^3 - X/m^2 - \eta Z : Z\big),$$
$$(X : Y : Z) = \big(m^2(T - \eta Z) : m^3(V + T) : Z\big)$$

is a K*-complete law attached to* $\ell_{m,n}$.

Proof. Proposition 3.1 identifies point-freeness. Theorems 3.4 and 3.5 prove the adapted laws, and Lemma 2.2 preserves their exceptional sets. □

3.6 Exact finite-field count

Let $E/\mathbb{F}_q$, $N = \#E(\mathbb{F}_q)$, $N_{\text{aff}} = N - 1$, and $F = \#E(\mathbb{F}_q)[3] - 1$. Thus $F \in \{0, 2, 8\}$ counts affine rational flexes. Their tangents are nonvertical: an affine point with vertical tangent has order two [21, Ch. III, Secs. 2–3].

Theorem 3.7 (Counting point-free nonvertical affine lines)**.** *The number* N_{empty} *of point-free lines* $Y = mX + nZ$ *over* $\mathbb{F}_q$ *is*

$$N_{\text{empty}} = q^2 - qN_{\text{aff}} + \frac{N_{\text{aff}}(N_{\text{aff}} - 1) - F}{3}. \tag{6}$$

Writing $N = q + 1 - \tau$*, this is*

$$N_{\text{empty}} = \frac{q^2 + q\tau + \tau^2 - q + \tau - F}{3}.$$

Proof. Let e, h, t, s count, respectively, nonvertical affine lines with no rational intersection, one rational point plus an irreducible quadratic, a nonflex divisor $2P + Q$, and three distinct rational intersections. Together with the F flex lines these exhaust the factorization patterns. Counting point–line incidences gives

$$h + 2t + 3s + F = qN_{\text{aff}}.$$

Ordered affine triples (P, Q, R) with $P + Q + R = O$ number $N_{\text{aff}}(N_{\text{aff}} - 1)$: for each P, exclude $Q = -P$. A secant contributes six orderings, a nonflex tangent three, and a flex one, so

$$6s + 3t + F = N_{\text{aff}}(N_{\text{aff}} - 1).$$

Since $q^2 = e + h + t + s + F$, eliminating h, t, s gives (6). Substitution $N_{\text{aff}} = q - \tau$ gives the second form. □

Corollary 3.8 (Finite-field existence)**.** *Every nonsingular short-Weierstrass curve over a finite field of characteristic different from* $2, 3$ *has a point-free nonvertical affine line, and hence a* K*-complete law from Theorem 3.6.*

Proof. Completing the square in $3N_{\text{empty}}$ gives

$$3N_{\text{empty}} = \left(\tau + \frac{q+1}{2}\right)^2 + \frac{3q^2 - 6q - 1}{4} - F.$$

Here $q \geq 5$ and $F \leq 8$, so the right side is positive. This argument does not need the Hasse bound. □

Remark 3.9 (Base-field limitations)**.** *Over an algebraically closed field every line meets E; over a real closed field every cubic $f_{m,n}$ has a root. Thus no point-free projective line exists in either case. Over a Hilbertian field of characteristic zero, Hilbert irreducibility applied to $x^3+ax+b-T^2$ yields infinitely many point-free horizontal lines. The generic cubic is irreducible over $K(T)$: a rational root would give a nonconstant rational map $\mathbb{P}^1 \dashrightarrow E$, impossible by genus, while a constant root cannot satisfy the equation. Hilbert irreducibility then gives infinitely many irreducible specializations [13, Ch. IV, Sec. 2]; see also [20, Ch. 3] for Hilbert irreducibility.*

4 Point-free line families and chainable arithmetic

The master law applies to every nonvertical point-free line. We consider four families: $Y = 0$, horizontal levels $Y = nZ$, zero-intercept slopes $Y = mX$, and depressed slopes. Each family below records its root test, schedule, and full/full cost. Parameters are chosen once in setup; online counts exclude this search.

The zero and horizontal branches use the usual short-Weierstrass state $(X : Y : Z)$. The sloped and depressed branches use the invertible line-adapted coordinates $(T : V : Z)$.

All operation counts below use the $5M + 8A$ realization of Lemma 3.2.

4.1 Common five-product output core

Each family below supplies the six blocks of Lemma 3.2 and evaluates their common output with $5M + 8A$. Six source products give an $11M$ formula; eight source products give a $13M$ formula. The family-specific linear computations and fixed multipliers are counted separately in the displayed costs. The completeness condition is the rootlessness of the intersection cubic for the selected line.

4.2 The zero line

For $P_i = (X_i : Y_i : Z_i)$, compute

$$P = X_1X_2, \quad Q = Y_1Y_2, \quad R = Z_1Z_2,$$
$$T = (X_1 + Y_1)(X_2 + Y_2) - P - Q,$$
$$U = (X_1 + Z_1)(X_2 + Z_2) - P - R, \quad \Sigma = (Y_1 + Z_1)(Y_2 + Z_2) - Q - R.$$

With $C = 3b$, set

$$Z_c = aU + CR, \quad X_c = Q - Z_c, \quad Z_s = Q + Z_c,$$
$$G = 3P + aR, \qquad H_c = a(P - aR) + CU,$$

and return

$$(X_3, Y_3, Z_3) = (X_cT - \Sigma H_c,\ X_cZ_s + GH_c,\ GT + \Sigma Z_s). \tag{7}$$

Theorem 4.1 (Zero-line branch)**.** *The following are equivalent:*

$$x^3 + ax + b \text{ is rootless}, \qquad E(K)[2] = \{O\}, \qquad Y = 0 \text{ is point-free}.$$

Under these conditions (7) *is K-complete and costs $11M + 3D_a + 2D_C + 28A$ full/full.*

Proof. The equivalences follow from $y = 0$ and inversion $(x, y) \mapsto (x, -y)$. Completeness follows from Theorem 3.6. The schedule has six source products, five core products, and the displayed fixed layer. □

This is the Bosma–Lenstra zero-line specialization used by RCB [8, 19, 4], evaluated with the five-product core above.

4.3 Horizontal levels

Let $n \neq 0$, put $Y_i^{\pm} = Y_i \pm nZ_i$, and compute

$$p = X_1X_2, \quad r = Z_1Z_2, \quad w = (X_1 + Z_1)(X_2 + Z_2),$$
$$\alpha = X_1Y_2^-, \quad \beta = X_2Y_1^+, \quad q = Y_1Y_2, \quad \gamma = Y_1Y_2^+, \quad \delta = Y_2Y_1^-.$$

With $C = 3b$, define

$$U = w - p - r, \quad L = \alpha + \beta, \quad \Sigma = (\gamma - \delta)/n, \quad A_r = ar,$$
$$Z_c = aU + Cr, \quad X_c = q - Z_c, \quad G = 3p + A_r,$$
$$M = a(p - A_r) + n(\alpha - \beta) + (C + n^2)U,$$
$$N = \gamma + \delta - q + Z_c.$$

The output is

$$(X_3, Y_3, Z_3) = (X_c L - \Sigma M,\ X_c N + GM,\ \Sigma N + GL).$$

Multiplying Σ, X_c, G by n clears the displayed division and scales all output coordinates by n.

By Theorem 3.5, this schedule is K-complete exactly when $x^3+ax+b-n^2$ is rootless. If $n = c^3 \neq 0$, the scaling $X = c^2X'$, $Y = c^3Y'$ sends the line to $Y' = Z$. On the normalized short model put

$$A' = a/c^4, \qquad B' = b/c^6, \qquad C' = 3B'.$$

At $n = 1$, the two fixed products involving the curve's constant term are $C'r$ and $(C'+1)U$. The resulting schedule costs $13M+3D_{A'}+D_{C'}+D_{C'+1}+30A$, hence five fixed products. Direct and division-free original-model counts are given in Appendix B.4.

4.4 Zero-intercept slopes

Let $m \neq 0$. The scaling $X = m^2X'$, $Y = m^3Y'$ gives

$$E'_{A,B} : Y'^2Z = X'^3 + AX'Z^2 + BZ^3, \qquad A = a/m^4, \quad B = b/m^6,$$

and sends the line to $Y' = X'$. With $T = X'$, $V = Y'-X'$, put $W_i = V_i+2T_i$ and compute

$$\Pi = T_1T_2, \quad R = Z_1Z_2, \quad U = (T_1 + Z_1)(T_2 + Z_2) - \Pi - R,$$
$$\alpha = T_1W_2, \quad \beta = V_1T_2, \quad Q = V_1V_2, \quad \gamma = W_1Z_2, \quad \delta = Z_1V_2.$$

For $C = 3B$, the family schedule is

$$S = \gamma + \delta, \quad L = \alpha + \beta, \quad Z_c = AU + CR,$$
$$X_c = Q + 2\beta + \Pi - Z_c, \quad N = Q - \Pi + Z_c,$$
$$G = 3\Pi - U + AR + 2\gamma, \qquad M = A(\Pi - AR) + CU,$$

followed by

$$(T_3, V_3, Z_3) = (X_c L - SM,\ X_c N + GM,\ GL + SN).$$

This is the $\eta = 0$ specialization of Theorem 3.4. It is K-complete exactly when $x^3 - m^2x^2 + ax + b$ is rootless and has full/full adapted cost $13M + 3D_A + 2D_C + 33A$.

4.5 Depressed slopes and the squared parameter

For

$$\ell_m : Y = mX - \frac{m^3}{3}Z, \qquad m \neq 0,$$

set $s = m^2 \in K^{\square,\times}$. The two choices $m = \pm\sqrt{s}$ give two lines, but the intersection cubic and adapted constants depend only on s. After $x = z + s/3$, the root test is

$$\Phi_s(z) = z^3 + \frac{\mathcal{R}(s)}{3}z + \frac{\mathcal{J}(s)}{27}, \quad \mathcal{R}(s) = s^2 + 3a, \quad \mathcal{J}(s) = s^3 + 9as + 27b. \tag{8}$$

Thus ℓ_m is point-free exactly when Φ_s is rootless.

In normalized coordinates, $A = a/s^2$, $C = 3b/s^3$, and

$$\rho = A + \tfrac{1}{3}, \quad \Lambda = C + \tfrac{2A}{3}, \quad \kappa = \rho - \Lambda, \quad \Theta = C + \tfrac{A}{3} - A^2.$$

Use the same eight source products as in the sloped schedule and set

$$H_1 = \rho(\Pi + U), \quad H_2 = \Lambda(U + R), \quad H_3 = \kappa U, \quad H_\rho = \rho R, \quad H_\Theta = \Theta R.$$

A denominator-free assignment layer is

$$\begin{aligned} \bar{S} &= 3(\gamma + \delta), \qquad \bar{L} = 3(\alpha + \beta) + \gamma + \delta, \\ \bar{X}_c &= 3(Q + 2\beta) - 3H_2 - 3H_3 - H_\rho, \\ \bar{G} &= 9\Pi + 3H_\rho + 6\gamma, \\ \bar{M} &= Q + 2\beta + 3H_1 - 3H_3 + 3H_\Theta, \\ \bar{N} &= 3(Q - \Pi + H_2 + H_3) - 2\gamma. \end{aligned}$$

Applying Lemma 3.2 with every middle-layer register replaced by its barred counterpart scales the projective result uniformly by 9. The generic cost is $13M + 2D_\rho + D_\Lambda + D_\kappa + D_\Theta + 60A$.

For selection define

$$\begin{aligned} \mathcal{R}(s) &= s^2 + 3a, & \mathcal{L}(s) &= 2as + 9b, \\ \mathcal{K}(s) &= s^3 + as - 9b, & \mathcal{T}(s) &= as^2 + 9bs - 3a^2. \end{aligned}$$

Then

$$\rho = \frac{\mathcal{R}(s)}{3s^2}, \quad \Lambda = \frac{\mathcal{L}(s)}{3s^3}, \quad \kappa = \frac{\mathcal{K}(s)}{3s^3}, \quad \Theta = \frac{\mathcal{T}(s)}{3s^4}.$$

These are setup identities; they add no online products. In the table, rD means r applications of precomputed constants after all displayed identifications. Earlier rows take precedence.

Condition on a point-free $s \in K^{\square,\times}$	Full/full cost
$\mathcal{R}(s) = 0$	$13M + 2D + 60A$
$(\mathcal{L}(s) = 0$ or $\mathcal{K}(s) = 0)$ and $\mathcal{T}(s) \in \{0, \pm s^2\mathcal{R}(s)\}$	$13M + 3D + 60A$
$\mathcal{L}(s)\mathcal{K}(s)\mathcal{T}(s) = 0$	$13M + 4D + 60A$
otherwise	$13M + 5D + 60A$

For example, $\mathcal{R}(s) = 0$ gives $\rho = 0$, $\kappa = -\Lambda$, and $\Theta = \Lambda$; the fixed layer reduces to $\Lambda(U + R)$ and $-\Lambda U$. A selector scans nonzero squares s, tests (8), ranks successful candidates by the table, and then chooses either square root m. The listed $60A$ bound uses the same linear circuit in every case; individual specializations may reduce this count.

Full/full operation counts. The four full/full branches are summarized below. The parenthetical count is the number of fixed-constant products.

Family	Normalization	Online profile
$Y = 0$	none	$11M + 3D_a + 2D_{3b} + 28A$ $(5D)$
$Y = nZ$	$n = c^3 \neq 0$	$13M + 3D_{A'} + D_{C'} + D_{C'+1} +$ $30A$ $(5D)$
$Y = mX$	$m \neq 0$	$13M + 3D_A + 2D_C + 33A$ $(5D)$
depressed	$s = m^2 \neq 0$	$13M + 2D_\rho + D_\Lambda + D_\kappa + D_\Theta +$ $60A$ $(2D$–$5D)$

4.6 Existence and prime-field coverage

The rootlessness conditions for the four families are:

Family	Point-free condition
$Y = 0$	$x^3 + ax + b$ is rootless
$Y = nZ$	$x^3 + ax + b - n^2$ is rootless
$Y = mX$	$x^3 - m^2x^2 + ax + b$ is rootless
depressed	$s \in K^{\square,\times}$ and Φ_s in (8) is rootless

Write $K^\square = \{u^2 : u \in K\}$. The horizontal pencil contains a point-free line iff

$$K^\square \not\subseteq \{x^3 + ax + b : x \in K\}.$$

If $b \neq 0$, put $\phi_{a,b}(x) = x + a/x + b/x^2$ on $K^\times$. The nonzero sloped pencil contains a point-free line iff

$$K^{\square,\times} \not\subseteq \phi_{a,b}(K^\times).$$

These follow by solving the intersection equation for n^2 and m^2. When $b = 0$, the point $(0, 0)$ lies on every sloped line. The proofs below use the standard cubic-discriminant criterion, quadratic-character bounds, and Hasse–Weil estimates [20, Chs. 1 and 3], [18, Ch. 3], and [22, Ch. 5].

Proposition 4.2 (Zero-line prevalence)**.** *For $p > 3$, the zero line is point-free for exactly $(p^2-1)/3$ of the p^2-p nonsingular short-Weierstrass models over $\mathbb{F}_p$, a proportion*

$$\frac{p+1}{3p}.$$

Proof. Irreducible cubics $x^3 + ax + b$ correspond to degree-three elements of trace zero in $\mathbb{F}_{p^3}$, modulo Frobenius orbits. The trace kernel has p^2 elements and meets $\mathbb{F}_p$ only in zero, so the count is $(p^2 - 1)/3$. Exactly p coefficient pairs are singular. □

Theorem 4.3 (Prime-field selector coverage)**.** *Let $E_{a,b}/\mathbb{F}_p$ be nonsingular.*

1. *If $p \geq 17$, a nonzero point-free horizontal line exists iff it is not the case that $a = 0$ and $p \equiv 2 \pmod 3$.*
2. *If $p \geq 37$, a nonzero point-free sloped line exists iff $b \neq 0$.*
3. *If $p \geq 47$, the depressed pencil contains a point-free line for every (a, b).*

Proof. Let χ be the quadratic character of $\mathbb{F}_p$, with $\chi(0) = 0$. For the horizontal claim, $a = 0$ and $p \equiv 2 \pmod 3$ make $x \mapsto x^3 + b$ a permutation, so every horizontal line meets E. Otherwise, assume for contradiction that every nonzero horizontal level meets E. For $a \neq 0$, the quartic

$$\Delta(y) = -4a^3 - 27(b - y^2)^2$$

is squarefree by nonsingularity. Let B_h count the nonzero $y \in \mathbb{F}_p$ for which $\Delta(y)$ is a nonzero square. The genus-one character bound, with at most four zeros and the parameter $y = 0$ removed, gives

$$B_h \geq \frac{p - 7 - 2\sqrt{p}}{2}.$$

A separable reducible cubic with square discriminant splits completely. Our assumption therefore gives at least $(p-1)+2B_h$ affine points on E. Hasse's bound gives at most $p+2\sqrt{p}$, so $B_h \leq \sqrt{p}+1/2$. Combining the inequalities yields $p - 8 \leq 4\sqrt{p}$, which fails for $p \geq 31$. The primes $17, 19, 23, 29$ are

checked by enumeration. If $a = 0$ and $p \equiv 1 \pmod 3$, every nonzero value in the image of the cube map has three preimages. At most two nonzero levels have $y^2 = b$; hence the failure assumption gives at least $3p - 7$ affine points, contradicting Hasse's bound for $p \geq 17$.

For slopes, $b = 0$ forces the common point $(0, 0)$. If $b \neq 0$, use

$$\Delta(m) = 4bm^6 + a^2m^4 - 18abm^2 - 4a^3 - 27b^2.$$

Let B_s count nonzero slopes with nonzero square discriminant, and suppose that every nonzero slope meets E. Since $b \neq 0$, no intersection has $x = 0$; distinct slopes give distinct affine points. As above, $B_s \leq \sqrt{p} + 1/2$. If Δ is squarefree, the genus-two character bound gives

$$B_s \geq \frac{p - 9 - 4\sqrt{p}}{2}.$$

Thus $p - 10 \leq 6\sqrt{p}$, which fails for $p \geq 59$. The only repeated-factor case is $a^3 = 27b^2$. Here $u = 3b/a \in \mathbb{F}_p^\times$ satisfies $a = 3u^2, b = u^3$, and

$$\Delta(m) = u^3(m^2 + 3u)^2(4m^2 - 15u).$$

The quadratic character sum for $u^3(4m^2 - 15u)$ is $-\chi(u)$. Removing $m = 0$ and the at most two roots of $m^2 + 3u$ gives a sum at least -4, while Δ has at most four nonzero roots. Hence $B_s \geq (p - 9)/2$, already incompatible with the upper bound for $p \geq 37$. Enumeration covers $37, 41, 43, 47, 53$ in the squarefree case.

For the depressed pencil, the auxiliary cubic

$$T^3 + 9T^2U + 27U^3 + 9aTW^2 + 27aUW^2 + 27bW^3 = 0$$

is geometrically integral with normalization of genus at most one. Adjoining $m^2 = T/W$ gives genus at most four. If every parameter failed, the Hasse–Weil and character bounds would give $p - 18 \leq 19\sqrt{p}$, false for $p \geq 397$. Exhaustive enumeration covers every prime $47 \leq p < 397$. The geometric-integrality, ramification, exceptional factorization, and singularity calculations are proved in Appendix B.2. □

There are $p^2 - p$ nonsingular coefficient pairs. Of these, $p - 1$ have $b = 0$, so the sloped family covers the exact proportion $1 - 1/p$. The coverage and operation counts for $p \geq 47$ are:

Family	Coverage of nonsingular models	Consequence
$Y = 0$	$\frac{p+1}{3p}$	$11M + 5D + 28A$
$Y = nZ$	all except $a = 0$ when $p \equiv 2 \pmod 3$	existence as stated; $13M+5D+30A$ requires a successful cube n
$Y = mX$	$1 - \frac{1}{p}$	$13M + 5D + 33A$; precisely $b = 0$ fails
depressed	100%	$13M + 5D + 60A$ always; $2D$–$4D$ under the selector conditions above

The horizontal existence result does not require n to be a cube; this additional condition is needed only for the normalized cost in the table. Section 6 describes the finite enumerations.

4.7 Selector algorithm

For a fixed curve and platform, setup selects once and the online loop uses the chosen schedule:

1. Test $Y = 0$; if rootless, use the $11M$ row.
2. Scan horizontal levels and then nonzero slopes.
3. Scan the depressed pencil; over $\mathbb{F}_p$, $p \geq 47$, it is guaranteed.
4. Choose an addition variant compatible with the table coordinates, and a doubling formula returning the same accumulator state.

Over other finite fields, if these families supply no point-free line, enumerate all q^2 pairs (m, n). Corollary 3.8 guarantees success. All completeness statements assume that both inputs belong to the stated curve.

4.8 Mixed addition and a selected table operand

The following mixed formulas leave the first operand as an unrestricted projective accumulator. In the zero-line branch, setting $Z_2 = 1$ replaces R, U, Σ by $Z_1, X_1 + X_2 Z_1, Y_1 + Y_2 Z_1$. The source layer then uses

$$X_1 X_2, \quad Y_1 Y_2, \quad (X_1 + Y_1)(X_2 + Y_2), \quad X_2 Z_1, \quad Y_2 Z_1,$$

so Lemma 3.2 gives the accumulator-chainable profile $10M + 3D_a + 2D_C + 22A$. The corresponding $Z_2 = 1$ source layer has six products in the normalized sloped and depressed states, giving $11M + 3D_A + 2D_C + 30A$ and $11M + 2D_\rho + D_\Lambda + D_\kappa + D_\Theta + 57A$, respectively.

When $Y = 0$ is point-free, every rational table point has a representative $Q = (x : 1 : z)$. For a full accumulator $P = (X : Y : Z)$, the five products

$$Xx, \quad Zz, \quad Yx, \quad Yz, \quad (X + Z)(x + z)$$

recover the six symmetric source forms, after which the common five-product core returns a full projective accumulator. Hence full-plus-selected addition costs exactly

$$\boxed{10M + 3D_a + 2D_C + 22A} \tag{9}$$

without squaring or online normalization. The table operand satisfies $Y_2 = 1$; the output is an unrestricted projective point and can be used as the next accumulator.

4.9 Complete and chainable doubling

The addition loop also needs a doubling operation that accepts every projective representative, including O and points of order two, and returns a full projective point. Write the short model as

$$E_{A,C} : \qquad Y^2Z = X^3 + AXZ^2 + \frac{C}{3}Z^3. \tag{10}$$

For $P = (X : Y : Z)$, form

$$p = X^2, \quad q = Y^2, \quad r = Z^2, \quad \ell = (X + Y)^2 - p - q,$$
$$u = (X + Z)^2 - p - r, \qquad \sigma = (Y + Z)^2 - q - r,$$

and then

$$d_0 = Ar, \quad d_1 = Cu, \quad d_2 = (A + C)(r + u),$$
$$d_3 = A(p - d_0), \qquad Z_c = d_2 - d_0 - d_1,$$
$$\Xi = q - Z_c, \quad N = q + Z_c, \quad G = 3p + d_0, \quad H = d_3 + d_1.$$

The alternative $d_2 = (A - C)(u - r)$, $Z_c = d_2 + d_0 + d_1$ permits the cheaper of $A + C$ and $A - C$. Finally apply the low-addition core of Lemma 3.2:

$$s_1 = \Xi - \sigma, \quad s_2 = \ell + N, \quad s_3 = s_1 + G, \quad s_4 = H - s_2,$$
$$m_1 = -GH, \quad m_2 = \Xi N, \quad m_3 = s_1 s_2,$$
$$m_4 = \ell s_3, \quad m_5 = \sigma s_4, \quad h = m_3 - m_2,$$

and return

$$(X_2, Y_2, Z_2) = (h - m_5,\ m_2 - m_1,\ m_4 - h). \tag{11}$$

Proposition 4.4 (Complete full-projective doubling)**.** *Equations* (10)–(11) *define the doubling morphism on every nonsingular $E_{A,C}$, have no geometric common zero, and cost*

$$5M + 6S + 2D_A + D_C + \min\{D_{A+C}, D_{A-C}\} + 27A.$$

Thus the uniform fixed-multiplier count is $5M+6S+4D+27A$ in the short-Weierstrass state $(X : Y : Z)$. The output is a full projective state and can feed the same doubling row or short-state full/full addition. Adapted-state doubling includes the boundary costs below. If $A = -1/3$, respectively $A = 0$, the complete specializations in Appendix B.3 reduce this to $5M + 6S + D_\Lambda + 67A$, respectively $3M + 5S + D_C + 15A$. The first count uses the straightforward addition chains displayed in Appendix B.3.

For a normalized sloped accumulator the addition-only boundary maps are

$$(X' : Y' : Z) = (T : V + T : Z), \qquad (T_2 : V_2 : Z_2) = (X_2' : Y_2' - X_2' : Z_2),$$

whereas for the depressed state they may be written without division as

$$\begin{aligned} (X' : Y' : Z) &= (3T + Z : 3V + 3T : 3Z), \\ (T_2 : V_2 : Z_2) &= (3X_2' - Z_2 : 3Y_2' - 3X_2' + Z_2 : 3Z_2). \end{aligned} \tag{12}$$

The zero and horizontal branches apply the same schedule directly in their short-model coordinates. The sloped maps cost $1A$ in each direction. For the depressed maps, computing $3T, 3V, 3Z$ and the two incoming sums costs $8A$; sharing T_2 in $V_2 = 3Y_2' - T_2$ gives another $8A$ on return. Thus a complete generic doubling call, including return to the adapted accumulator state, costs

accumulator state	generic doubling cost
short Weierstrass	$5M + 6S + 4D + 27A$
normalized sloped	$5M + 6S + 4D + 29A$
depressed	$5M + 6S + 4D + 43A.$

The same $2A$ or $16A$ overhead applies to either coefficient specialization when it is used through these maps. These maps require no field multiplication. Converting to or from the original scaled model has its separate fixed-product cost at the external boundary.

Addition and doubling costs.

Operation and input restriction	Online cost and reuse
zero ADD ($Z_2 = 1$)	$10M + 3D_a + 2D_C + 22A$; accumulator
slope ADD ($Z_2 = 1$)	$11M + 3D_A + 2D_C + 30A$; accumulator
depressed ADD ($Z_2 = 1$)	$11M + 2D_\rho + D_\Lambda + D_\kappa + D_\Theta + 57A$; accumulator
full+selected ADD ($Y_2 = 1$)	$10M + 3D_a + 2D_C + 22A$; accumulator
generic DBL, short state	$5M + 6S + 4D + 27A$; closed
generic DBL, sloped state	$5M + 6S + 4D + 29A$; closed
generic DBL, depressed state	$5M + 6S + 4D + 43A$; closed
DBL, $A = -1/3$, short state	$5M + 6S + D_\Lambda + 67A$; closed
DBL, $A = 0$, short state	$3M + 5S + D_C + 15A$; closed

5 Applications to Hessian addition

This section records two applications of the algebraic identity in Lemma 3.2. They are evaluations of already published triples, with the same coordinates, input restrictions, and exceptional pairs. No change of elliptic-curve model is used to obtain the savings.

5.1 Standard projective Hessian addition

For the standard Hessian model

$$X^3 + Y^3 + Z^3 = 3dXYZ, \qquad d^3 \neq 1,$$

use the identity $O_H = (1 : -1 : 0)$. Take the EFD `add2` schedule [3]. Write its six input products as

$$\begin{aligned} A &= X_1Y_2, \quad B = X_1Z_2, \quad C = Y_1Z_2, \\ D &= Y_1X_2, \quad E = Z_1X_2, \quad F = Z_1Y_2. \end{aligned}$$

The output is

$$(X_3, Y_3, Z_3) = (DC - FA,\ BA - DE,\ FE - BC). \tag{13}$$

Substitute

$$(X_c, G, L, M, N, S) = (D, B, C, A, -E, F)$$

in Lemma 3.2. It returns $(X_3, Y_3, -Z_3)$; negating its third coordinate recovers (13) exactly. Thus the $5M + 8A$ output realization replaces the original $6M + 3A$ block.

For full inputs the source layer uses six products. If $Z_2 = 1$, then $B = X_1$ and $C = Y_1$ are free, leaving four source products. If also $Z_1 = 1$, then $E = X_2$ and $F = Y_2$ are free, leaving two. The corresponding EFD mixed and doubly affine triples are precisely these specializations. The total online costs of these schedules are

input contract	published evaluation	five-product evaluation
full/full	$12M + 3A$	$11M + 8A$
$Z_2 = 1$	$10M + 3A$	$9M + 8A$
$Z_1 = Z_2 = 1$	$8M + 3A$	$7M + 8A$.

The output remains a full projective triple. In particular, the doubly affine input contract is not preserved by general addition. The refactoring preserves every exceptional input of the source formula and does not make an incomplete Hessian law complete. In particular, the standard cycle vanishes identically when $P_1 = P_2$, so it does not provide a doubling formula.

5.2 The generalized-Hessian unified triple

For the split generalized-Hessian curve

$$H_{c,d} : X^3 + Y^3 + cZ^3 = dXYZ, \qquad c(d^3 - 27c) \neq 0,$$

with identity $O_H = (1 : -1 : 0)$, Rezaeian Farashahi–Joye give the blocks [11, Eq. (11)]

$$A = X_1X_2, \quad B = Y_1Y_2, \quad C = cZ_1Z_2,$$
$$D = X_1Z_2, \quad E = Y_1X_2, \quad F = Z_1Y_2,$$

and the unified output

$$(X_3, Y_3, Z_3) = (CF - AE,\ BE - CD,\ AD - BF). \tag{14}$$

The substitution

$$(X_c, G, L, M, N, S) = (C, B, F, E, -D, A)$$

again yields $(X_3, Y_3, -Z_3)$, so a free final negation gives the exact published triple. The source layer costs $6M + D_c$, or $4M + D_c$ when $Z_2 = 1$. Consequently

input contract	published evaluation	five-product evaluation
full/full	$12M + D_c + 3A$	$11M + D_c + 8A$
$Z_2 = 1$	$10M + D_c + 3A$	$9M + D_c + 8A$.

Here D_c is the fixed multiplication by the source parameter c. The source completeness criterion is retained exactly: the unified law is K-complete when c is not a cube in K [11, Theorem 3]. Equality of the output polynomials, rather than a new completeness argument, is what transfers that property.

In both examples the reduction is one generic multiplication at the cost of five additions. The source layer and any conversion, normalization, or table preparation must still be charged under their actual storage contract. These examples establish portability of the lemma, not a cross-model timing comparison.

These examples refactor the specified source programs. Hisil's earlier twisted-Hessian formulas already achieve $11M + D_a$ full addition and $9M + D_a$ mixed addition in characteristic different from two [14, 2]. Swapping X and Z identifies the generalized-Hessian coefficient c with the twisted-Hessian coefficient a, without field arithmetic. The EFD records $16A$ and one doubling for that output program, or $17A$ under our convention, compared with $8A$ for the core here [5]. The multiplication counts agree with Hisil's; the linear computations differ.

6 Computational verification

The accompanying programs check the transport identities, reconstruct the Bosma–Lenstra laws from their affine generators, and compare the resulting formulas with the chord-and-tangent group law. Polynomial certificates express residuals as combinations of the input curve equations. Each computation has the scope of its stated polynomial ring or finite range.

6.1 Identities and verification programs

Run `python verification/run_verification.py` from the project root to execute all eight programs. The README records dependency versions and individual commands.

Identity or computation	Program in `verification/`
Transport, model, and intersection cubic	`transport_certificates_v3.py`
Independent derivation of known Bosma–Lenstra corrections	`bl_construction_certificates_v3.py`
Dense-open law, bidegrees, and identity restrictions	`independent_group_law_certificates.py`
Complete doubling and coefficient specializations	`doubling_certificates_v5.py`
Both five-product forms and Hessian substitutions	`five_product_and_hessian_v9.py`
Finite horizontal, sloped, and depressed selector ranges	`finite_selectors_v9.py`
Executed operation counts and schedule identities	`operation_ledgers_v9.py`
Independent affine group-law oracle over five fields	`independent_finite_field_audit_v9.py`

The first three programs retain quotient certificates with coefficient domains, ordered generators, input equations, residuals, and quotients. The independent chord calculation uses no printed Bosma–Lenstra coordinate as its target. The identity restrictions recover the selected line scheme-theoretically as explained in Appendix A.4. The five-product identity and both Hessian substitutions are checked over $\mathbb{Z}$.

6.2 Finite ranges and operation counts

The selector program examines every nonsingular coefficient pair for horizontal primes $17 \le p \le 31$, sloped primes $37 \le p \le 53$, and depressed primes $47 \le p < 397$. It records the obstruction sets, field ranges, model counts, and source hash. The first two families have the obstructions stated in Theorem 4.3; the depressed range has none. The character-sum arguments in Section 4 and Appendix B.2 prove the remaining prime ranges.

Operation counters execute 16 arithmetic programs: normalized horizontal addition; zero-line full, mixed, and selected addition; sloped and depressed full and mixed addition; generic doubling in short, sloped, and depressed coordinates; two coefficient-specialized doubling formulas; both original-coordinate horizontal formulas; and the explicit original-coordinate sloped transport. They distinguish multiplication, squaring, fixed products, and addition. Small-integer products use the stated addition chains. Polynomial identities check the schedules, including the common factor 9

in the depressed output and the curve multiples in specialized doubling. Appendix B.4 gives the assignments and conversion costs.

An independent program implements ordinary affine chord-and-tangent addition over $\mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}, \mathbb{F}_{25}, \mathbb{F}_{49}$, without importing the other verification modules. It checks the line-count formula on all 3,124 nonsingular coefficient pairs, classifying 6,038,020 lines, and tests generic and applicable specialized doubling at every point. Addition uses all point pairs on a listed set of models and deterministic boundary pairs elsewhere, for 304,707 scaled input pairs in total. The tests include the identity, inverse pairs, points of order two, projective rescaling, chained output reuse, and deliberately exceptional pairs.

The Hessian examples are checked through an invertible linear map to short Weierstrass form. Its determinant and curve identity are verified symbolically. The finite tests include 33 model/formula cases on 21 distinct Hessian models, including the standard cycle's expected diagonal zeros and the generalized model's noncube complete cases.

6.3 Attribution and scope

Bosma–Lenstra supply the line-law space, construction, and exceptional divisor correspondence [8]. The two printed-term corrections are already recorded by Bernstein–Lange [7, Figure 1.2 and its caption]; the construction here verifies them independently. The five-product output identity is classical [12, 10]. RCB supply the zero-line factoring and its published full and mixed schedules [19]. The Hessian laws retain the hypotheses of their sources [3, 11] and are compared with Hisil's earlier multiplication counts in Section 5.

Completeness concerns validated points on the stated curve over the stated field. Constant-time field arithmetic, subgroup validation, fault resistance, and implementation timing require separate analysis.

7 Comparison and further work

The principal comparison uses the same short-Weierstrass state and input contract. The zero-line law is the complete RCB specialization, but the five-product lemma replaces its final $6M + 3A$ block by $5M + 8A$. Thus full/full addition costs $11M+3D_a+2D_C+28A$, compared with the published $12M + 3D_a + 2D_C + 23A$, where $C = 3b$ [19, Table 1 and Algorithm 1]. The mixed and selected-table rows return a reusable full accumulator, with their table restrictions stated explicitly.

Table 1: Comparison under explicit input contracts.

Contract	Published evaluation	Evaluation here
RCB full/full	$12M + 3D_a + 2D_C + 23A$	$11M + 3D_a + 2D_C + 28A$
RCB $Z_2 = 1$	$11M + 3D_a + 2D_C + 17A$	$10M + 3D_a + 2D_C + 22A$
Hessian full/full	$12M + 3A$	$11M + 8A$
Hessian $Z_2 = 1$	$10M + 3A$	$9M + 8A$
Hessian $Z_1 = Z_2 = 1$	$8M + 3A$	$7M + 8A$
Generalized Hessian full/full	$12M + D_c + 3A$	$11M + D_c + 8A$
Generalized Hessian $Z_2 = 1$	$10M + D_c + 3A$	$9M + D_c + 8A$
Hisil full/full, after coordinate swap	$11M + D_c + 17A$	$11M + D_c + 8A$
Hisil $Z_2 = 1$, after coordinate swap	$9M + D_c + 17A$	$9M + D_c + 8A$

The first two baselines are RCB [19, 4]; the remaining baselines and their exact output substitutions are given in Section 5 [3, 11]. The first seven rows save one generic multiplication and add five field additions. The final two rows compare with Hisil [14, 5]: the multiplication counts agree, and the linear cost decreases by nine additions. Swapping X and Z identifies his coefficient a with c, without field arithmetic. A doubly affine output is not assumed, and no change in source completeness hypotheses is claimed.

The main construction has broader reach than the zero line. Nonzero rational 2-torsion prevents $Y = 0$ from being point-free, but the exact incidence count guarantees another nonvertical affine point-free line over every finite field in the stated characteristic. The explicit transport and family schedules turn that certificate into arithmetic. For $p \geq 47$, the depressed family is a guaranteed one-parameter selector, with $13M$ and at most five fixed products; its special fixed layers may reduce the latter count to two.

This develops an explicit construction and scheduling result within the known existence theory for complete finite-field Weierstrass laws [1]. The independent verification of known printed-term corrections, rootlessness tests, explicit input restrictions, and geometrically complete doubling formulas establish the validity and reuse conditions. The short Hessian examples illustrate reuse of the algebraic lemma while the Weierstrass point-free-line construction remains the subject of the paper.

7.1 Future work

The next step is to extend this point-free construction to Hessian and twisted-Hessian curves. The existing complete formulas [11, 2, 14, 5] provide the starting points.

The questions are how to choose an exceptional section without rational points and how to use it in a reusable projective representation. A complete construction will require proofs for identity, doubling, and inverse pairs, together with full/full and mixed formulas whose costs include coordinate conversions and any cached quantities. Polynomial identities and finite-field computations will check the resulting formulas.

For the short-Weierstrass formulas, further work concerns line-search algorithms, shared linear computations, and constant-time implementation. Benchmarks will include fixed multipliers, register pressure, memory traffic, and representation conversion.

A Verification of the known Bosma–Lenstra corrections

The two corrections used here are recorded in the caption of Figure 1.2 of Bernstein–Lange [7], which credits Nicole L. Pitcher. This appendix independently recovers their specializations from the construction in [8, pp. 235–238] and supplies exact quotient certificates.

A.1 The construction before expansion

On the affine chart $Z_1 = Z_2 = 1$, write the long Weierstrass equation as

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

and put $d = x_1 - x_2$. The first law has $Z_0 = d^3$, $X^{(1)} = fZ_0$, and $Y^{(1)} = gZ_0$. In the notation of the source,

$$\begin{aligned} d^2f &= (y_1 - y_2)^2 + a_1(y_1 - y_2)d - (x_1 + x_2 + a_2)d^2, \\ d^3g &= -\{(y_1 - y_2 + a_1d)d^2f - (y_1x_2 - y_2x_1)d^2 + a_3d^3\}. \end{aligned}$$

For subtraction set

$$K = y_1 + y_2 + a_1x_2 + a_3, \qquad M = y_1x_2 + y_2x_1 + a_1x_1x_2 + a_3x_1.$$

The displayed κ and μ on p. 236 are $\kappa = K/d$ and $\mu = -M/d$. Hence, with

$$S_X = K^2 + a_1Kd - (x_1 + x_2 + a_2)d^2,$$

denominator clearing gives

$$d^3 s^*(Y/Z) = -(K + a_1 d)S_X + Md^2 - a_3 d^3. \tag{15}$$

The law for $(0 : 1 : 0)$ is constructed before its printed expansion by

$$Z_{\mathrm{raw}} = s^*(Y/Z)Z_0, \qquad X_{\mathrm{raw}} = fZ_{\mathrm{raw}}, \qquad Y_{\mathrm{raw}} = gZ_{\mathrm{raw}}.$$

The collected coordinates on pp. 237–238 use the opposite common unit from the raw affine Z_0 convention. We therefore define $(X_{\mathrm{der}}, Y_{\mathrm{der}}, Z_{\mathrm{der}}) = -(X_{\mathrm{raw}}, Y_{\mathrm{raw}}, Z_{\mathrm{raw}})$; this normalization is fixed by $Z_{\mathrm{der}} = Z_{\mathrm{print}}$.

For a candidate polynomial triple (X, Y, Z), equality with the construction is certified by the three polynomial targets

$$Z_{\mathrm{der}} - Z, \qquad (d^2 f)Z_{\mathrm{der}} - d^2 X, \qquad (d^3 g)Z_{\mathrm{der}} - d^3 Y.$$

Each target is divided by the ordered input equations $F(x_1, y_1), F(x_2, y_2)$. The saved quotient pairs reconstruct the target over $\mathbb{Z}$ and leave zero remainder. Since all coordinates are bihomogeneous of bidegree $(2, 2)$, equality on this dense chart determines the projective representative [13, Ch. I, Sec. 3].

A.2 Non-horizontal residual

Specialize $(a_1, a_2, a_3, a_4, a_6) = (2, A_2, 0, A_4, A_6)$, and let $D = T_1 Z_2$, $E = T_2 Z_1$, $B_0 = 3A_2 A_6 - A_4^2$. Direct specialization of the two sensitive terms on p. 238 gives

$$(12A_6 + B_0)D(D + 2E) - B_0(D + E)(D - E).$$

In contrast, substituting (15) into (A.1), then reducing by the two input equations, gives

$$(12A_6 + 2B_0)D(D + 2E) - B_0(D + E)(D - E).$$

The first two targets in (A.1) vanish with $X = X_{\mathrm{print}}$, $Z = Z_{\mathrm{print}}$; the second-coordinate target vanishes precisely for

$$Y = Y_{\mathrm{print}} + B_0 D(D + 2E).$$

Thus the construction gives the residual directly. The printed coefficient is missing one copy of B_0.

A.3 Horizontal residual

Now specialize $(a_1, a_2, a_3, a_4, a_6) = (0, 0, \lambda, a, c)$, with $xz = X_1Z_2$ and $zx = X_2Z_1$. Running the same three targets gives

$$\begin{aligned} X_{\mathrm{der}} - X_{\mathrm{print}} &= -\lambda a\, zx(3xz - zx), \\ Y_{\mathrm{der}} - Y_{\mathrm{print}} &= -a^2 xz(xz + 2zx), \\ Z_{\mathrm{der}} - Z_{\mathrm{print}} &= 0. \end{aligned}$$

After $\lambda = 2n$ and $c = b - n^2$, it supplies the corrected horizontal representative used in Theorem 3.5.

A.4 Comparison with the chord formula

On the dense chord chart, the three cross products between each scheduled output and the generic long-Weierstrass sum reduce to zero modulo the two input equations. Let $\mathcal{A}_{\mathrm{nh}}$ and $\mathcal{A}_{\mathrm{h}}$ denote the laws in long-model coordinates $(T : V : Z)$ and $(X : V : Z)$, respectively. Their identity restrictions are

$$\mathcal{A}_{\mathrm{nh}}(P, O) = (V_1T_1, V_1^2, V_1Z_1), \qquad \mathcal{A}_{\mathrm{h}}(P, O) = (V_1X_1, V_1^2, V_1Z_1).$$

Thus each triple is nonzero generically and restricts to V_1P. On $E \times \{O\}$, its base ideal is $(V_1T_1, V_1^2, V_1Z_1) = V_1(T_1, V_1, Z_1)$, with T_1 replaced by X_1 in the horizontal model. In the original short coordinates, $\mathcal{H}_n(P, O) = (Y_1 - nZ_1)P$. The projective irrelevant ideal sheafifies to the unit ideal, so the base section is scheme-theoretically $E \cap \{V = 0\}$, including multiplicities. The restriction identifies the associated line as $V = 0$; Theorem 2.1 gives its exceptional divisor on $E \times E$.

B Auxiliary proofs and operation counts

B.1 Transport identities

For the normalized short model $Y'^2Z = X'^3 + AX'Z^2 + BZ^3$, substitute $X' = T - \eta Z$, $Y' = V + T$. Direct expansion gives

$$\begin{aligned} &(V + T)^2Z - (T - \eta Z)^3 - A(T - \eta Z)Z^2 - BZ^3 \\ &\quad = V^2Z + 2TVZ - T^3 + (3\eta + 1)T^2Z \\ &\qquad - (A + 3\eta^2)TZ^2 - (B - A\eta - \eta^3)Z^3. \end{aligned}$$

This is exactly (2). The selected-line identity is

$$Y' - X' - \eta Z = (V + T) - (T - \eta Z) - \eta Z = V.$$

Finally, with $A = a/m^4$, $B = b/m^6$, and $\eta = n/m^3$, direct collection yields

$$m^6 h_\eta(x/m^2 + \eta) = x^3 - m^2x^2 + (a - 2mn)x + b - n^2 = f_{m,n}(x).$$

Thus the inverse maps are

$$\begin{aligned} T &= X/m^2 + \eta Z, \quad V = Y/m^3 - X/m^2 - \eta Z, \\ X &= m^2(T - \eta Z), \quad Y = m^3(V + T). \end{aligned}$$

These identities determine the coordinate changes independently of the addition formulas.

B.2 The large-prime step for the depressed pencil

Put

$$D_{a,b} : T^3 + 9T^2U + 27U^3 + 9aTW^2 + 27aUW^2 + 27bW^3 = 0.$$

On $W = 1$, this is the incidence curve for a root z of the depressed intersection cubic with parameter $t = m^2$.

Lemma B.1. *For nonsingular $E_{a,b}/\mathbb{F}_p$ with $p \geq 397$, $D_{a,b}$ is geometrically integral, its normalization has genus at most one, and $t = T/W$ is not a square in its geometric function field. The function t has at most three zeros and three poles.*

Proof. A reducible plane cubic has a linear factor. Substitution of $T + uU + vW$ and coefficient comparison gives

$$\begin{aligned} -u^3 + 9u^2 + 27 = 0, &\qquad uv(6 - u) = 0, \\ (u - 3)(3a + v^2) = 0, &\quad v^3 + 9av - 27b = 0. \end{aligned}$$

The first relation excludes $u = 0, 6$, hence $v = 0$; the remaining relations force either the contradiction $u = 3$ in the first equation or $a = b = 0$. A factor with zero T-coefficient is proportional to $U + vW$ or W, but restriction retains respectively a nonzero T^3 term or $T^3 + 9T^2U + 27U^3$. Hence no linear factor exists.

An integral plane cubic has arithmetic genus one [13, Ch. I, Sec. 7]. The divisors cut by $T = 0$ and $W = 0$ each have degree three. At $T = 0$ the restriction is $U^3 + aUW^2 + bW^3$, whose roots are simple by nonsingularity of $E_{a,b}$. Thus t has a simple zero, its divisor is not even, and it is not a square. □

Assume now that every nonzero m makes the depressed cubic reducible. Adjoining m with $m^2 = t$ gives a geometrically integral double cover of the normalization. Ramification can occur only at zeros and poles of t, at most six points. Riemann–Hurwitz therefore gives genus at most four [22, Ch. 3]. Singularities in the affine (t, z)-model satisfy

$$9z^2 + 3a + t^2 = 0, \qquad 6tz + 3a + t^2 = 0,$$

so $3z(3z - 2t) = 0$. The first case contradicts nonsingularity; the second forces $z = 2t/3$, $a = -5t^2/3$, $b = 10t^3/9$, and hence at most two choices of m. Hasse–Weil therefore bounds the number of affine pairs (m, z), $m \neq 0$, by $p + 3 + 8\sqrt{p}$ [22, Ch. 5].

The cubic discriminant is

$$-\frac{5m^{12} + 54am^8 + 54bm^6 + 189a^2m^4 + 486abm^2 + 108a^3 + 729b^2}{27}.$$

Writing it as $\delta(m^2)$, the discriminant of δ is a nonzero constant times $(4a^3 + 15b^2)(4a^3 + 27b^2)^4$. In the only extra case $4a^3 + 15b^2 = 0$, write over the algebraic closure $a = -15u^2$, $b = \epsilon 30u^3$; then

$$\delta(t) = -\frac{5}{27}(t - 3\epsilon u)^2(t^4 + 6\epsilon u t^3 - 135u^2t^2 - 540\epsilon u^3 t + 6480u^4),$$

and the quartic factor has discriminant $2^{11}3^{16}5^2u^{12} \neq 0$. Thus the squarefree part is nonconstant of degree at most twelve. The quadratic-character bound gives at least $(p - 14 - 11\sqrt{p})/2$ nonzero parameters with nonzero square discriminant [18, Ch. 5]. A reducible cubic with square discriminant has three roots, so the failure assumption gives at least $2p - 15 - 11\sqrt{p}$ affine pairs. Comparison yields $p - 18 \leq 19\sqrt{p}$, false for $p \geq 397$. This proves the large-prime part of Theorem 4.3; the finite range is exhausted as described in Section 4.

B.3 Proof and coefficient specializations for doubling

Expanding the reconstruction in (11) gives

$$X_2 = \Xi\ell - \sigma H, \qquad Y_2 = \Xi N + GH, \qquad Z_2 = G\ell + \sigma N,$$

which is the diagonal specialization of the corrected line-law representative. If $D = E \cap \ell$ and $d(P, Q) = P - Q$, its exceptional divisor is $d^{-1}(D)$. On the diagonal $d(P, P) = O$, while every line used here is affine and excludes O; hence the diagonal has no geometric base point. In particular, the schedule

sends O to O and returns a nonzero representative of $2P = O$ at every point of order two. The source layer uses six squares, the output layer five products, and the fixed layer $2D_A + D_C + \min\{D_{A+C}, D_{A-C}\}$, proving Proposition 4.4.

Two full-projective coefficient specializations reduce the fixed layer further. First suppose $A = -1/3$, put $\Lambda = C - 2/9$, and use the six quadratic registers p, q, r, ℓ, u, σ from Section 4.9. With the single fixed product $h = \Lambda r$, form

$$\begin{aligned} m_1 &= \ell(3q - 9h - 2r), & m_2 &= \sigma(9p + r), \\ m_3 &= \big(9(q-p) + 27h - r + 3u\big) \\ &\qquad \cdot \big(9(q+p) + 27h + r - 3u\big), \\ m_4 &= h(3u - 2r - 27h), & m_5 &= q\sigma, \end{aligned}$$

and return

$$(X_2, Y_2, Z_2) = (27m_1 + 9m_2,\ m_3 + 36m_4,\ 324m_5). \tag{16}$$

For

$$\mathcal{F}_\Lambda = (9\Lambda + 2)Z^3 + 27X^3 - 9XZ^2 - 27Y^2Z,$$

let $(\mathcal{X} : \mathcal{Y} : \mathcal{Z})$ be the generic output at $A = -1/3$, $C = \Lambda + 2/9$. Direct polynomial expansion gives

$$X_2 - 81\mathcal{X} = 0, \quad Y_2 - 81\mathcal{Y} = -18\Lambda Z\mathcal{F}_\Lambda, \quad Z_2 - 81\mathcal{Z} = -18Y\mathcal{F}_\Lambda.$$

Thus (16) agrees with the complete generic output on the curve. Reusing $3q, 9q, 9p, 9h, 27h, 2r, 3u$ costs $30A$ before the five products. The output scalings use $27 = 3^3$, $9 = 3^2$, $36 = 4 \cdot 9$, and $324 = 4 \cdot 81$, giving $28A$ including the two output sums. Together with $9A$ for the quadratic source forms, the cost is $5M + 6S + D_\Lambda + 67A$.

If $A = 0$, nonsingularity gives $C \neq 0$. Compute

$$q = Y^2, \quad r = Z^2, \quad \sigma = (Y + Z)^2 - q - r, \quad e = XY, \quad k = Cr,$$

and return

$$(X_2, Y_2, Z_2) = \big(2e(q - 3k),\ (q + 3k)^2 - 12k^2,\ 4q\sigma\big). \tag{17}$$

Writing $\mathcal{F}_0 = CZ^3 + 3X^3 - 3Y^2Z$, the difference from the generic output is coordinate-wise

$$0, \qquad -2CZ\mathcal{F}_0, \qquad -2Y\mathcal{F}_0.$$

Consequently (17) is also geometrically complete and closed in the short state, with cost $3M + 5S + D_C + 15A$. The boundary maps (12) preserve nonvanishing and require no field product. A call returning to the sloped or depressed state adds $2A$ or $16A$, respectively, to either specialized short-state row.

B.4 Addition and doubling costs

All online counts use the conventions of Section 2. Specialization may identify constants, but no term is dropped merely because it is cheap on a particular platform.

Full/full branch	Online cost
zero line	$11M + 3D_a + 2D_C + 28A$
horizontal, direct	$13M + 3D_a + D_C + D_{C+n^2} + 3D_n + D_{n^{-1}} + 30A$
horizontal, division-free	$13M + 3D_a + D_C + D_{C+n^2} + 5D_n + 30A$
horizontal, cube-normalized	$13M + 3D_{A'} + D_{C'} + D_{C'+1} + 30A$
sloped, normalized	$13M + 3D_A + 2D_C + 33A$
sloped, original coordinates	$13M + 11D + 34A$
depressed	$13M + 2D_\rho + D_\Lambda + D_\kappa + D_\Theta + 60A$

For the sloped row in original coordinates, precompute $A = a/m^4$, $C = 3b/m^6$, m^{-2}, m^{-3}, m^2, m^3. For each input set

$$T_i = m^{-2}X_i, \qquad Y_i' = m^{-3}Y_i, \qquad V_i = Y_i' - T_i, \qquad W_i = Y_i' + T_i.$$

These assignments use four fixed products and four additions for the two inputs; the four additions replace the computation of $W_i = V_i + 2T_i$ in the normalized formula. Evaluate the normalized sloped formula and return

$$(X_3 : Y_3 : Z_3) = \big(m^2 T_3 : m^3(V_3 + T_3) : Z_3\big).$$

The return map adds two fixed products and one addition. The full cost is

$$13M + 3D_A + 2D_C + 2D_{m^{-2}} + 2D_{m^{-3}} + D_{m^2} + D_{m^3} + 34A.$$

Operation	Multiplications and squares	State and closure
zero full/full	$6M$ input + $5M + 8A$ core	full projective; closed
zero $Z_2 = 1$	$5M$ input + $5M + 8A$ core	normalized table; accumulator
sloped/depressed full/full	$8M$ input + $5M + 8A$ core	adapted full; closed
sloped/depressed $Z_2 = 1$	$6M$ input + $5M + 8A$ core	normalized table; accumulator
full plus selected	$5M$ input + $5M + 8A$ core	full accumulator; accumulator
generic doubling, short	$5M + 6S$	$2D_A + D_C + D_{A\pm C}$; closed
doubling, $A = -1/3$, short	$5M + 6S$	D_Λ; closed
doubling, $A = 0$, short	$3M + 5S$	D_C; closed

The additions can be counted by stage. The zero-line full/full formula uses $12A$ for the symmetric input forms, $8A$ for the fixed layer, and $8A$ for Lemma 3.2, giving $28A$. Horizontal normalization uses $22A$ before the common core, hence $30A$, with distinct fixed coefficients $C' = 3B'$ and $C' + 1$; the normalized sloped row uses $8A$ in its source preparation and $17A$ in its middle layer, hence $33A$. Sharing $\gamma + \delta$, $Q + 2\beta$, 2γ, and $3H_i$ in the depressed formula gives $8A + 44A + 8A = 60A$. Setting $Z_2 = 1$ reduces the source layers by $6A$, $3A$, and $3A$ in the zero, sloped, and depressed rows, respectively. The displayed doubling rows use short-state counts; adding the sloped or depressed maps gives $29A$ or $43A$ for the generic closed call. The accompanying operation counters check the displayed addition and doubling programs and their polynomial identities. The expanded direct-coordinate formulas are listed separately from the normalized formulas used in the accumulator.

The fixed layer for every zero-line row is $3D_a + 2D_C$. In particular, for a full accumulator $(X : Y : Z)$ and a selected table point $(x : 1 : z)$, the five products

$$Xx, \quad Zz, \quad Yx, \quad Yz, \quad (X + Z)(x + z)$$

recover all six symmetric input forms; the five-product output core then gives $10M + 3D_a + 2D_C + 22A$, without squaring or online normalization. When an operation changes the accumulator representation, its coordinate conversion must be counted as in Section 4.9.

References

[1] C. Arène, D. Kohel, and C. Ritzenthaler. Complete addition laws on abelian varieties. *LMS Journal of Computation and Mathematics*,

15:308–316, 2012.

[2] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange. Twisted hessian curves. In *Progress in Cryptology – LATINCRYPT 2015*, volume 9230 of *Lecture Notes in Computer Science*, pages 269–294. Springer, 2015.

[3] D. J. Bernstein and T. Lange. Explicit-Formulas Database: Projective Coordinates for Hessian Curves. `https://www.hyperelliptic.org/EFD/g1p/auto-hessian-standard.html`. Accessed 2026-10-31.

[4] D. J. Bernstein and T. Lange. Explicit-Formulas Database: Projective Coordinates for Short Weierstrass Curves. `https://www.hyperelliptic.org/EFD/g1p/auto-shortw-projective.html`. Accessed 2026-10-31.

[5] D. J. Bernstein and T. Lange. Explicit-Formulas Database: Projective Coordinates for Twisted Hessian Curves. `https://www.hyperelliptic.org/EFD/g1p/auto-twistedhessian-projective.html`. Accessed 2026-10-31.

[6] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, 2007.

[7] 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.

[8] 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.

[9] E. Brier and M. Joye. Weierstraß elliptic curves and side-channel attacks. In *Public Key Cryptography – PKC 2002*, volume 2274 of *Lecture Notes in Computer Science*, pages 335–345. Springer, 2002.

[10] C. Ericson. *Real-Time Collision Detection*. Morgan Kaufmann, 2005.

[11] R. R. Farashahi and M. Joye. Efficient arithmetic on hessian curves. In *Public Key Cryptography – PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 243–260. Springer, 2010.

[12] J. L. Gustafson and S. Aluru. Massively parallel searching for better algorithms or how to do a cross product with five multiplications. *Scientific Programming*, 5(3):203–217, 1996. The author's 2015 revised preface credits the five-multiplication cross product to C. M. Fiduccia's 1973 doctoral thesis.

[13] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[14] H. Hisil. *Elliptic Curves, Group Law, and Efficient Computation*. PhD thesis, Queensland University of Technology, 2010.

[15] T. Izu and T. Takagi. Exceptional procedure attack on elliptic curve cryptosystems. In *Public Key Cryptography – PKC 2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 224–239. Springer, 2003.

[16] D. Kohel. Addition law structure of elliptic curves. *Journal of Number Theory*, 131(5):894–919, 2011.

[17] H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Inventiones Mathematicae*, 79:603–610, 1985.

[18] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2 edition, 1997.

[19] J. Renes, C. Costello, and L. Batina. Complete addition formulas for prime order elliptic curves. In *Advances in Cryptology – EUROCRYPT 2016, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 403–428. Springer, 2016.

[20] J.-P. Serre. *Topics in Galois Theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, 2 edition, 2008.

[21] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, 2 edition, 2009.

[22] H. Stichtenoth. *Algebraic Function Fields and Codes*, volume 254 of *Graduate Texts in Mathematics*. Springer, 2 edition, 2009.