An Explicit Theorem of the Square for Hyperelliptic Jacobians

JANE ARLEDGE & DAVID GRANT

Introduction

Let $A$ be an abelian variety over a field $k$, $D$ a symmetric divisor on $A$, $s$ and $d$ the sum and difference maps from $A \times A$ into $A$, and $p_1$ and $p_2$ the projections onto the first and second factors. The theorem of the square and the seesaw principle [M1, Secs. 5, 6] guarantee that there exists a function $f(u, v)$ on $A \times A$ (determined up to constant multiples) with divisor $s^*D + d^*D - 2p_1^*D - 2p_2^*D$. Since this function encodes all the information about the group morphism on $A$, it is useful to know $f(u, v)$ explicitly. Indeed, if $a, b, c \in A$ and if $D_c$ is the image of $D$ under the translation-by-$c$ map, then the divisor of $f(u - \frac{a+b}{2}, -\frac{a+b}{2})/f(u - \frac{a+b}{2}, -\frac{a+b}{2})$ is $D_{a+b} + D - D_a - D_b$, which is the theorem of the square for $D$. If $k$ is the complex numbers, then the construction of $f$ is classical. One merely takes a theta function $\theta$ with divisor $D$ (see e.g. [La]); then

$$f(u, v) = \theta(u + v)\theta(u - v)/\theta(u)^2\theta(v)^2,$$

for $u, v$ in the universal cover of $A$, has the desired property.

When $A$ is the Jacobian $J$ of a curve $C$, it is useful to determine $f$ in terms of symmetric functions on $C$. If $k$ is the complex numbers and $D$ is a theta divisor of $J$, then Riemann’s theta identities (see [Mu, p. 212]) express $\theta(u + v)\theta(u - v)$ in terms of sums of products of theta functions with characteristics evaluated at $u$ and $v$. When $C$ is hyperelliptic, Baker [Ba2] described how the resulting functions of $u$ and $v$ can be expressed as explicit symmetric functions in the coordinates of the points in the support of the divisors corresponding to $u$ and $v$; he found a way to express $f(u, v)$ as a polynomial in the second logarithmic derivatives of a theta function evaluated at $u$ and $v$. In genus 1, Baker’s formula was well known and is a cornerstone of the analytic theory of elliptic curves. In genus 2, this formula was recently used to understand the group law on $J$ [G1], the derivatives of theta functions [G3], and the arithmetic of certain points on intersections of divisors [G2]. In genus 3, some of these same applications were carried out in [O]; in [A], a version of this formula was needed that worked over any field $k$ in order to understand the arithmetic of certain torsion points.

In this paper we prove a version of Baker’s formula for hyperelliptic curves of any genus $g$ over any field $k$, generalizing the argument in [A]. Our formula takes a different shape than Baker’s, but it must agree with his when $k$ is the complex
numbers. We do not know whether our formula was known to Baker or his contemporaries in the complex case, but related formulas appear for \( g = 2 \) in [Bal, Sec. 218].

We hope the explicit nature of the result will be of use not only to number theorists and geometers but also—with the introduction of hyperelliptic curves into coding and cryptology [BHHW; K]—to computer scientists.

We would like to thank the referee for several useful suggestions.

Preliminaries

Let \( k \) be a field and \( \bar{k} \) an algebraic closure of \( k \). Unless stated otherwise, all algebraic geometric objects will be assumed to be defined over \( \bar{k} \): Take \( g_1 = 1 \): Let \( p, q \in k[x] \) be such that \( p \) is monic of degree 2, \( g \) is of degree at most \( g \), and the affine curve

\[
y^2 + q(x)y = p(x)
\]

is nonsingular (for the conditions this puts on \( p \) and \( q \), see [L]). Let \( C \) be the projective nonsingular curve over \( k \) associated to the affine curve, and let \( \hat{1} \) denote the lone point at infinity on \( C \) with respect to the affine model, which is \( k \)-rational. Then \( C \) is a hyperelliptic curve of genus \( g \); and every hyperelliptic curve of genus \( g \) over \( k \) with a \( k \)-rational Weierstrass point arises in this fashion. The hyperelliptic involution on \( C \) is given by \( \hat{p} = (x, -y - q(x)) \) for a point \( P = (x, y) \), with \( \hat{\infty} = \infty \). We let \( \hat{y} = -y - q(x) \). The Weierstrass points of \( C \) are the fixed points of the involution. Note that \( x \) and \( y \) have poles of order 2 and 2 (respectively) at \( \infty \).

Let \( J \) be the Jacobian of \( C \) over \( k \), so that the points of \( J \) parameterize the group \( \text{Pic}^0(C) \) of divisors of degree 0 on \( C \) modulo linear equivalence. We will identify points of \( J \) with the corresponding divisor classes in \( \text{Pic}^0(C) \). We write \( D_1 \sim D_2 \) to denote that two divisors are linearly equivalent, and we let \( \text{cl}(D) \) be the class of the divisor \( D \) modulo linear equivalence. For any \( P \in C \), considering the divisor of \( x - x(P) \) shows that \( P + \hat{P} \sim 2\infty \).

Let \( \psi : C \to J \) be the Albanese embedding that uses \( \infty \) as base point. Then we have morphisms over \( k \),

\[
C^g \xrightarrow{\pi} C^{(g)} \xrightarrow{\psi} J,
\]

from the product \( C^g \) into the symmetric product \( C^{(g)} \) into \( J \), where \( \pi \) is the natural projection and \( \psi \) is induced from \( \hat{\psi} \). It follows from the Riemann–Roch theorem that \( \overline{\varphi} \) is a surjective birational map, and via \( \psi \) we will often identify symmetric functions on \( C^g \) with functions on \( J \).

Let \( M_i \) be the divisor \( C \times \cdots \times C \times C \times \cdots \times C \) in \( C^g \) (the \( \infty \) occurring in the \( i \)th slot), let \( M \) be the image under \( \pi \) of any \( M_i \), and let \( \Theta \) be the image under \( \varphi \) of \( M \). Let \( N_{ij} \) be the divisor in \( C^g \) consisting of points whose \( j \)th component is the hyperelliptic involution of the \( i \)th component; let \( N \) be the image under \( \pi \) of any \( N_{ij} \).

If \( P_1 + \cdots + P_g \sim Q_1 + \cdots + Q_g \), then \( P_1 + \cdots + P_g + \hat{Q}_1 + \cdots + \hat{Q}_g - 2g \infty \) is the divisor of a function, which must be a polynomial in \( x \). Thus, if the \( Q_i \) are not a permutation of the \( P_i \), then \( P_i = \hat{P}_j \) for some \( i \neq j \).

It follows that every divisor class \( D \in \text{Pic}^0(C) \) can be uniquely represented by a divisor of the form \( P_1 + \cdots + P_r - r \infty \) for some \( r \leq g \), where \( P_i \neq \infty \).
and, for $i \neq j$, $P_i \neq \tilde{P}_j$. In particular, $\Theta$ consists of divisor classes of the form $\text{cl}(P_1 + \cdots + P_r - r\infty)$ for $r \leq g - 1$ and $J - \Theta$ consists of divisor classes of the form $\text{cl}(P_1 + \cdots + P_g - g\infty)$, where $P_i \neq \infty$ and $P_i \neq \tilde{P}_i$ for $i \neq j$. Hence $\varphi(N) \subset \Theta$ and $\varphi$ is an isomorphism from $C(\overline{x}) - N - M$ onto $J - \Theta$ [M2, Sec. 5].

**Lemma 1.** Let $f \in \tilde{k}(J)$, and take $F = \pi^*\varphi^*f$ in $\tilde{k}(C^{g-1})(C)$ by considering functions in $\tilde{k}(C^{g-1})$ as functions of the first factor $C$ with coefficients in the function field of the product of the other factors. Then

$$\text{ord}_{\varphi}(f) = \text{ord}_{\infty}(F).$$

**Proof.** From the foregoing we have $\varphi^*\Theta = mM + nN$ for some positive $m$ and $n$. Since $\varphi$ is a birational morphism of nonsingular projective varieties and since $\varphi(N)$ is not dense in $\Theta$, [I, Thm. 2.28] implies that $m = 1$. Hence

$$\text{ord}_{\varphi}(f) = \text{ord}_{M} \varphi^*(f).$$

By construction, $\pi^*(M) = I(M_1 + M_2 + \cdots + M_g)$ for some positive $I$. Since $\pi$ is a surjective finite morphism of nonsingular varieties, [I, Lemma 2.26] gives us

$$\sum_{i=1}^{g} l[\tilde{k}(M_i) : \tilde{k}(M)] = \deg(\pi).$$

But $\deg(\pi) = [\tilde{k}(C^{g}) : \tilde{k}(C^{g-1})] = g!$ and $[\tilde{k}(M_i) : \tilde{k}(M)] = (g - l)!$, so $l = 1$. Hence $\pi^*(M) = M_1 + \cdots + M_g$ and

$$\text{ord}_{\varphi}(f) = \text{ord}_{M_1} \pi^* \varphi^*(f).$$

Finally, we note that $\text{ord}_{M_1}(F)$ is just the order at $\infty$ of $F$ considered as a function of the first factor $C$ with coefficients in the function field of the product of the other factors.

**Notation.** We let $O$ denote the identity of $J$; for a function $f$, we let $(f)$ denote its divisor. For $P \in J$, we let $\Theta_P$ denote the translate of $\Theta$ under the translation-by-$P$ map.

**The Function**

Let $P_1, \ldots, P_{2g}$ be independent generic points on $C$, so $u = \text{cl}(P_1 + \cdots + P_g - g\infty)$ and $v = \text{cl}(P_{g+1} + \cdots + P_{2g} - g\infty)$ are independent generic points on $J$. We write $P_i = (x_i, y_i)$. Let $a = \left[\frac{g-2}{2}\right]$ and $b = \left[\frac{3g-1}{2}\right]$, where the square brackets denote the greatest integer function.

Define the matrices

$$W = \begin{pmatrix}
y_1 x_1^a & \cdots & y_1 x_1^2 & y_1 x_1 & x_1^b & \cdots & x_1^2 & x_1 & 1 \\
y_2 x_2^a & \cdots & y_2 x_2^2 & y_2 x_2 & x_2^b & \cdots & x_2^2 & x_2 & 1 \\
y_{g+1} x_{g+1}^a & \cdots & y_{g+1} x_{g+1}^2 & y_{g+1} x_{g+1} & x_{g+1}^b & \cdots & x_{g+1}^2 & x_{g+1} & 1 \\
y_{2g} x_{2g}^a & \cdots & y_{2g} x_{2g}^2 & y_{2g} x_{2g} & x_{2g}^b & \cdots & x_{2g}^2 & x_{2g} & 1
\end{pmatrix}.$$
Theorem 2. \[ f \text{ of the form } 1 \] and we let \[ D \] let \[ P \] and we similarly consider as a function in \( P \) and evaluate the divisor of \( H(u, v) \) regular for \( u, v \in J - \Theta \).

Our main result is as follows.

**Theorem 2.** The divisor of \( H(u, v) \) is

\[
s^*\Theta + d^*\Theta - 2p_1^*\Theta - 2p_2^*\Theta.
\]

In order to prove the theorem, we will specialize \( v \) and evaluate the divisor of \( H_v(u) = \eta_v(u)/\delta_v(u) \in \tilde{k}(J), \) where \( \eta_v(u) = \eta(u, v) \in \tilde{k}(J) \) and \( \delta_v(u) = \delta(u, v) \in \tilde{k}(J). \)

Let \( E \subset J \) be the irreducible divisor on \( J \) representing divisor classes in \( \text{Pic}^0(C) \) of the form \( \{\text{cl}(2Q_1 + Q_2 + \cdots + Q_{g-1} - g\infty) | Q_i \in C\} \). If \( g = 1 \), we take \( E \) to be the zero divisor.

**Proposition 3.** Let \( u = \text{cl}(P_1 + \cdots + P_g - g\infty) \) and \( v = \text{cl}(P_{g+1} + \cdots + P_{2g} - g\infty) \) be points in \( J - \Theta - E \), and suppose that \( P_i \neq P_j \) and \( P_i \neq \hat{P}_j \) for any \( 1 \leq i \leq g \) and \( g + 1 \leq j \leq 2g \). Then \( u + v \in \Theta \) if and only if \( D = 0 \), and \( u - v \in \Theta \) if and only if \( D = 0 \).

**Proof.** Suppose the sum \( u + v \in \Theta \). Then we can write \( u + v = \text{cl}(\hat{P}_{2g+1} + \cdots + \hat{P}_{3g-1} - (g - 1)\infty) \) for some \( P_{2g+1}, \ldots, P_{3g-1} \in C \). Then we have \( R = \text{cl}(P_1 + \cdots + P_{3g-1} - (3g - 1)\infty) \sim O \), which implies that there exists a function \( F \in \mathcal{L}(3g - 1) \) with divisor \( R \). By the Riemann–Roch theorem, \( \mathcal{L}(3g - 1) \) has a basis consisting of the \( 2g \) functions

\[
\{1, x, x^2, \ldots, x^b, y, xy, yx^2, \ldots, xy^a\}.
\]

Hence we can put
We now turn our attention to the divisor of \( v.u/ \): \( fP.u/ \) Then \( C^{2ˆ} \) has poles precisely along \( .x \)

Proposition 5. J: sider as a function on \( k \) This is clear from the definitions and Proposition 3 if the characteristic of \( 2 \) least to order \( i \) for \( \alpha_i \) Consider the dependence relation between the columns of \( W \), \( \gamma_0 + \gamma_1 x_i + \gamma_2 x_i^2 + \cdots + \gamma_b x_i^b + \alpha_0 y_i + \alpha_1 y_i x_i + \alpha_2 y_i x_i^2 + \cdots + \alpha_n y_i x_i^n = 0 \) for \( i = 1, \ldots, 2g \). Since \( u, v \neq O \), we do not have \( \alpha_j, \gamma_j \) all zero. Thus the determinant \( D = 0 \).

Conversely, suppose \( D = 0 \). Then there exists a dependence relationship between the columns of \( W \); say, 

\[ \gamma_0 + \gamma_1 x_i + \gamma_2 x_i^2 + \cdots + \gamma_b x_i^b + \alpha_0 y_i + \alpha_1 y_i x_i + \alpha_2 y_i x_i^2 + \cdots + \alpha_n y_i x_i^n = 0 \]

for \( i = 1, \ldots, 2g \) and some \( \alpha_j, \gamma_j \in \tilde{k} \), not all 0. Then

\[ F = \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \cdots + \gamma_b x^b + \alpha_0 y + \alpha_1 y x + \alpha_2 y x^2 + \cdots + \alpha_n y x^n \]

is in \( L(3g - 1)\infty \). Because the \( P_i \) \( (1 \leq i \leq 2g) \) are distinct points in the support of the divisor of zeros of \( F \), it follows that there exist points \( P_{2g+1}, \ldots, P_{3g-1} \in C \) such that

\[ (F) = P_1 + \cdots + P_{3g-1} - (3g - 1)\infty \]

and hence \( u + v = \text{cl}(\tilde{P}_{2g+1} + \cdots + \tilde{P}_{3g-1} - (g - 1)\infty) \in \Theta \).

Now \( -v = \text{cl}(\tilde{P}_{g+1} + \cdots + \tilde{P}_g - g\infty) \). Since \( P_i \neq \tilde{P}_j \) for \( 1 \leq i \leq g \) and \( g + 1 \leq j \leq 2g \), we can substitute \(-v\) for \( v \) in the proof just described to get \( u - v \in \Theta \) if and only if \( \tilde{D} = 0 \).

Corollary 4. Let \( v \in J - \Theta - E = \text{cl}(P_{g+1} + \cdots + P_g - g\infty) \). Then \( \eta_v(u) \) has poles precisely along \( \Theta \) and zeros precisely along \( \Theta - v, \Theta - v, E, \Theta - \phi(P), \) and \( \Theta - \phi(P) \) for \( g + 1 \leq i \leq 2g \). If the characteristic of \( k \) is 2, then \( \eta_v(u) \) vanishes at least to order 2 at \( E \).

Proof. This is clear from the definitions and Proposition 3 if the characteristic of \( k \) is not 2, so suppose it is. Then, since \(-1 = 1 \), it follows that \( D \) and \( \tilde{D} \) are both functions on \( C^* \) that are invariant under the symmetric group and so can be considered as functions on \( J \); each of them vanishes on \( E \).

We now turn our attention to the divisor of \( \delta_e(u) \). It has poles only along \( \Theta \), and we need to determine its divisor of zeros.

Let \( P = (r, s) \in C - \infty \), let \( P_i = (x_i, y_i), 1 \leq i \leq g \), be independent generic points on \( C \), and let \( u = \text{cl}(P_1 + P_2 + \cdots + P_g - g\infty) \in J \). Define \( f_P(u) = (x_1 - r)(x_2 - r) \cdots (x_g - r) \), which is a symmetric function on \( C^* \) that we consider as a function on \( J \).

Proposition 5. The divisor of \( f_P(u) \) is given by

\[ (f_P(u)) = \Theta_{\phi(P)} + \Theta_{\phi(P)} - 2\Theta. \]

Proof. Note that \( f_P \) is regular off \( \Theta \) and, by Lemma 1, has a pole at \( \Theta \) of order 2.

Suppose \( u \in J - \Theta \) and \( u = \text{cl}(P_1 + P_2 + \cdots + P_g - g\infty) \) with \( P_i = (x_i, y_i) \). Then \( f_P(u) = 0 \) exactly when \( x_i = r \) for some \( i \), which happens exactly when
We need the following well-known lemma, whose proof we include owing to a lack of suitable reference.

**Lemma 6.** Let \( s_1, \ldots, s_n \) be the elementary symmetric polynomials in the independent variables \( x_1, \ldots, x_n \), \( n \geq 2 \). Then, if \( k \) is any field, the discriminant polynomial \( \Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \) is an irreducible element in the ring of power series \( k[[s_1, \ldots, s_n]] \) if the characteristic of \( k \) is not 2, and \( \Delta \) is the square of an irreducible element if the characteristic of \( k \) is 2.

**Proof.** Since \( k[[s_1, \ldots, s_n]] \) is a unique factorization domain, if \( \Delta = fg \) for \( f, g \in k[[s_1, \ldots, s_n]] \) then, for some \( i < j \), we have that \( x_i - x_j \) divides \( f \) if \( f \) is not a unit. Since the symmetric group \( S_n \) is doubly transitive, \( e = \prod_{1 \leq i < j \leq n} (x_i - x_j) \) divides \( f \). Likewise, if \( g \) also is not a unit then \( e \) divides \( g \), so \( f \) and \( g \) are units multiplied by \( e \). But if the characteristic of \( k \) is not 2 then \( e \) is not invariant under \( S_n \), so \( \Delta \) is irreducible. If the characteristic of \( k \) is 2, the argument shows that \( e \) is irreducible.

**Proposition 7.** The divisor of \( d(u) = nE - 4(g-1)\Theta \), where \( n = 2 \) if the characteristic of \( k \) is 2 and \( n = 1 \) otherwise.

**Proof.** This is trivial if \( g = 1 \), so take \( g > 1 \). Note that \( d \) is regular off \( \Theta \) and (by Lemma 1) has a pole at \( \Theta \) of order \( 4(g-1) \). Note then that \( d(u) \) vanishes for \( u \in E - \Theta \) precisely when \( u \in E \) and so, since \( E \) is irreducible, the divisor of zeros of \( d(u) \) is \( nE \) for some positive integer \( n \). We can compute \( n \) by considering a local equation for \( E \) in any local ring at a point along \( E \).

Let \( P \in C \) be a non-Weierstrass point. Then \( Q = \text{cl}(g(P - \infty)) \in J - \Theta \), \( Q \in E \), so we consider the local ring \( \mathcal{O}_{J, Q} \). This is isomorphic to \( \mathcal{O}_{C^{(e)}_R} \), where \( R = \mathcal{O}_{C^{(e)}_R} \). Let \( f \) be a local equation for \( \phi^*E \) in \( \mathcal{O}_{C^{(e)}_R} \), so \( d = f^n g \) for \( g \in \mathcal{O}_{C^{(e)}_R} \) and \( g \) not a multiple of \( f \). Since \( x - r \) is a uniformizer at \( P \), we know from [M2, Prop. 3.2] that we can identify the completed local ring \( \hat{\mathcal{O}}_{C^{(e)}_R} \) with the power series ring over \( \hat{k} \) generated by the elementary symmetric polynomials \( s_1, \ldots, s_g \) of \( x_i - r \). Considering the equation \( d = f^n g \) after embedding \( d, f, \) and \( g \) into \( \hat{k}[[s_1, \ldots, s_n]] \), we see that \( f \) is not a unit. Hence, if the characteristic of \( k \) is not 2 then (by Lemma 6) \( n = 1 \) and \( d \) is a local equation for \( E \). Likewise, if the characteristic of \( k \) is 2, then \( d \) is the square of an irreducible element in \( \hat{k}[[s_1, \ldots, s_n]] \) that must vanish at \( E \), so \( n = 2 \).

Putting the last two propositions together, we have the following corollary.
We are finally in a position to prove our main result.

Proposition 9. Let \( v \in J - \Theta - E \). Then the divisor of \( H_v(u) \) is given by

\[
(H_v(u)) = \Theta_v + \Theta_{-v} - 2\Theta.
\]

Proof. From the two corollaries, we have immediately that \( H_v(u) \) has poles only along \( \Theta \) and zeros at \( \Theta_v \) and \( \Theta_{-v} \). Considering \( D \) and \( \tilde{D} \) as functions of \( P_1 = (x_1, y_1) \), they have poles at \( \infty \) of order at most \( 3g - 1 \) whether \( g \) is even or odd and so (by Lemma 1) \( D\tilde{D} \) has a pole at \( \Theta \) of order at most \( 6g - 2 \). Hence, by Corollary 8, \( H_v(u) \) has a pole at \( \Theta \) of order at most 2. Since \( v + (-v) = O \), by the theorem of the square there exists a function \( g \in k(J) \) with \( (g) = \Theta_v + \Theta_{-v} - 2\Theta \). Then \( H_v(u)/g(u) \) has no poles and is therefore constant. Since \( H_v(u) \) is not identically 0, for \( v \in J - \Theta - E \) we have

\[
(H_v(u)) = \Theta_v + \Theta_{-v} - 2\Theta. \quad \square
\]

We are finally in a position to prove our main result.

Proof of Theorem 2. Since \( \Theta \) is symmetric, we have noted that the divisor \( s^*\Theta + d^*\Theta - 2p_1^*\Theta - 2p_2^*\Theta \) is principal. Now let \( F \) be a function on \( J \times J \) with this divisor. Again, since \( \Theta \) is a symmetric divisor, the divisor of \( F(v, u) \) is the same as that of \( F(u, v) \), so they differ by a constant. Let \( F_v(u) \in k(J) \) be \( F(u, v) \) with \( v \) fixed in \( J - \Theta \), so that \( (F_v) = \Theta_v + \Theta_{-v} - 2\Theta \). Then, by restricting \( v \) to \( J - \Theta - E \), we have that \( H_v(u) = F_v(u) \cdot g(v) \) for some \( g \) depending only on \( v \).

We now claim that \( \eta(v, u) = \pm \eta(u, v) \). Indeed, reversing the roles of \( u \) and \( v \) in \( W \) amounts to switching \( P_i \) and \( P_{i+g} \) for \( 1 \leq i \leq g \), which induces \( g \) transpositions of the rows \( W \) and changes \( D \) by at most a sign. Reversing the roles of \( u \) and \( v \) in \( \tilde{W} \) amounts to switching \( P_i \) and \( P_{i+g} \) for \( 1 \leq i \leq g \) (which again induces \( g \) transpositions of the rows of \( \tilde{W} \)) and applying the hyperelliptic involution to the entries of the first \( a + 1 \) columns of \( W \). Since \( a + g \leq b \), the application of the hyperelliptic involution to each of these columns changes merely the sign of \( D \). As a consequence, \( H(v, u) = \pm H(u, v) \).

Therefore, by a symmetric argument and restricting \( u \) to \( J - \Theta - E \), we see that \( H(u, v)/F(u, v) \) depends only on \( u \). Thus \( H(u, v)/F(u, v) \) is constant on an open dense subset of \( J \times J \) and hence is constant on all of \( J \times J \). Since \( H(u, v) \) is not identically 0, it follows that \( H(u, v) \) has the same divisor as \( F(u, v) \). \( \square \)

Examples. 1. When \( g = 1 \), we obtain the familiar \( H(u, v) = x_1 - x_2 \).
2. When \( g = 2 \), \( q(x) = 0 \), and \( p(x) = x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5 \), expanding the determinants for \( D \) and \( \tilde{D} \) and using \( y^2 = p(x) \) yields
\[ H(u, v) = \varphi_{11}(u) - \varphi_{11}(v) + \varphi_{12}(u)\varphi_{22}(v) - \varphi_{12}(v)\varphi_{22}(u), \]

where, for the divisor class \( z = \text{cl}((x, y) + (x', y') - 2\infty) \), we have \( \varphi_{22}(z) = x + x' \), \( \varphi_{12}(z) = -xx' \), and

\[
\varphi_{11}(z) = \frac{(x + x')(xx')^2 + 2b_1(xx')^2 + b_2(xx')xx'}{(x - x')^2} + 2b_3xx' + b_4(x + x') + 2b_5 - 2yy',
\]

which (up to a change in notation, since Baker did not take \( p \) to be monic) agrees over the complex numbers with the formula given by Baker in [Ba2, p. 381] and [Ba1, Sec. 218]. See also [G1].

References