

Arithmetic of Genus 2 Real Hyperelliptic Curves

$$y^2 + (h_3 x^3 + h_2 x^2 + h_1 x + h_0) \cdot y = f_6 x^6 + f_5 x^5 + f_4 x^4 + f_3 x^3 + f_2 x^2 + f_1 x + f_0$$

If the characteristic of k is not 2, then $h(x) = 0$. If the characteristic of k is not 3, then $f_5 = 0$.

If the characteristic of k is 2 and $f_6 = 1$ (which is possible if and only the number of elements in k is an even power of 2), then $h_3 = 1$ and $h_2 = f_5 = f_4 = f_3 = 0$.

$$\begin{aligned} \tilde{v} &\equiv h + 2v \pmod{u} & i &= r(\tilde{v})^{-1} \pmod{u} \\ k &= \frac{f+hv-v^2}{u} & k' &\equiv k \pmod{u} \\ s' &\equiv k' \cdot i' & s &= \frac{1}{r} \cdot s' \\ \tilde{u} &= s^2 + \frac{(h+2v) \cdot s - k}{u} & u' &= \tilde{u} \text{ made monic} \\ v' &\equiv -h - s \cdot u - v \pmod{u'} \end{aligned}$$

Doubling, Reduced Basis, deg $u = 2$		
Input	$[u, v], u = x^2 + u_1 x + u_0, v = x^3 + v_1 x + v_0$	
Output	$[u', v'] = 2[u, v] := [u, v] \oplus [u, v]$	
Step	Expression	# of Ops
1	$\tilde{v} = \tilde{v}_1 x + \tilde{v}_0 \quad w_1 = u_1^2$ <i>Odd:</i> $\tilde{v}_1 = 2(v_1 + w_1 - u_0), \tilde{v}_0 = 2(v_0 + u_0 \cdot u_1)$ <i>Even:</i> $\tilde{v}_1 = h_1 + w_1 + u_0, \tilde{v}_0 = h_0 + u_0 \cdot u_1$	1M, 1S (1M, 1S)
2	resultant $r = \text{res}(\tilde{v}, u)$, almost inverse $i = i_1 x + i_0$ $w_2 = u_0 \cdot \tilde{v}_1, w_3 = u_1 \cdot \tilde{v}_1, i_1 = \tilde{v}_1, i_0 = w_3 - \tilde{v}_0, r = \tilde{v}_0 \cdot i_0 - w_2 \cdot \tilde{v}_1$	4M
3	$k' \equiv (f - hv - v^2)/u \pmod{u} = k'_1 x + k'_0$: <i>Odd:</i> $k'_2 = f_4 - 2v_1, k'_1 = f_3 - 2v_0 - 2k'_2 \cdot u_1, k'_0 = f_2 - v_1^2 - k'_1 \cdot u_1 - (w_1 + 2u_0) \cdot k'_2$ <i>Even:</i> $k'_1 = h_0 + v_0, k'_0 = f_2 + (h_1 + v_1) \cdot (v_1 + w_1) + k'_1 \cdot u_1 + w_1^2 + u_0^2$	3M, 1S (2M, 2S)
4	$s' = s'_1 x + s'_0$ $s'_1 = i_1 \cdot k'_0 - \tilde{v}_0 \cdot k'_1, s'_0 = i_0 \cdot k'_0 - w_2 \cdot k'_1$	4M
5	Inversion, $\tilde{u}_2^{-1}, r^{-1}, s_0, s_1$ <i>Odd:</i> $u'_2 = (s'_1 + r)^2 - r^2$ <i>Even:</i> $u'_2 = s'_1 \cdot (s'_1 + r) + r^2$ $I = 1/(r \cdot u'_2), \tilde{r} = u'_2 \cdot I, \tilde{u}_2 = r \cdot r^2 \cdot I, s_1 = \tilde{r} \cdot s'_1, s_0 = \tilde{r} \cdot s'_0$;	I, 6M, 2S (I, 7M, 1S)
6	$u' = x^2 + u'_1 x + u'_0$ <i>Odd:</i> $u'_1 = 2[(s_0 + u_1) \cdot s_1 - s_0] \cdot \tilde{u}_2,$ $u'_0 = [f_4 - 2v_1 + (s_0 + 2u_1) \cdot s_0 + 2(u_0 - w_1 - v_0) \cdot s_1] \cdot \tilde{u}_2$ <i>Even:</i> $u'_1 = (s_0 + u_1 \cdot s_1) \cdot \tilde{u}_2, u'_0 = [v_1 + h_1 + \tilde{v}_1 \cdot s_1 + (u_1 + s_0) \cdot s_0] \cdot \tilde{u}_2$	5M (5M)
7	$v' = x^3 + v'_1 x + v'_0$ $z_0 = u'_0 - u_0, z_1 = u'_1 - u_1, w_0 = z_0 \cdot s_0, w_1 = z_1 \cdot s_1$ <i>Odd:</i> $v'_1 = 2(u'_0 - u_1^2) - v_1 + (z_0 + z_1) \cdot (s_0 + s_1) - w_0 - (u'_1 + 1) \cdot w_1,$ $v'_0 = w_0 - v_0 - u'_0 \cdot (2u'_1 + w_1)$ <i>Even:</i> $v'_1 = h_1 + v_1 + u'_0 + u_1^2 + (z_0 + z_1) \cdot (s_0 + s_1) + w_0 + (u'_1 + 1) \cdot w_1$ $v'_0 = h_0 + v_0 + w_0 + (u'_1 + w_1) \cdot u'_0$	5M, 1S (5M, 1S)
Total		1I, 28M, 5S (1I, 28M, 5S)

Cantor's Algorithm for Real Case

Let $(u, v) = (x^2 + u_1x + u_0, x^3 + v_1x + v_0)$ be a degree two reduced basis Mumford representation with both points of the divisor are not equal to their opposites. Then Cantor's Algorithm for doubling the divisor (u, v) must result in (U_1, V_1) such that

$$\begin{aligned} U_0 &= u^2 \\ V_0 &\equiv v \pmod{u} \\ (V_0 &= v + su \text{ for some } s) \\ V_1 &= h - V_0 + \left\lfloor \frac{V_0+d}{U_0} \right\rfloor U_0 \\ U_1 &= \frac{f+hV_1-V_1^2}{U_0} \end{aligned}$$

Here, s is chosen such that U_0 divides $V_0^2 - hV_0 - f$. Again, $\left\lfloor \frac{V_0+d}{U_0} \right\rfloor$ is zero since U_0 has degree 4 and $V_0 + d$ has degree 3. Hence, $V_1 = h - V_0 = h - v - su$ and

$$\begin{aligned} U_1 &= \frac{f+h(h-v-su)-(h-v-su)^2}{u^2} \\ &= \frac{f+hv-v^2+(h-2v)su-s^2u^2}{u^2} \\ &= \frac{1}{u} \left(\frac{f+hv-v^2}{u} + (h-2v)s \right) - s^2 \\ &= \frac{1}{u} (k + (h-2v)s) - s^2 \end{aligned}$$

where the division in $k = \frac{f+hv-v^2}{u}$ is exact. By choosing $s \equiv -k \cdot (h-2v)^{-1} \pmod{u}$, we have

$$k + (h-2v)s \equiv k - (h-2v) \cdot k \cdot (h-2v)^{-1} \equiv 0 \pmod{u}$$

so that the division of $k + (h-2v)s$ by u is exact. Finally, U_1 will be made monic, so we factor out a negative (noting that $h = 0$ in odd characteristic or $h = -h$ in even characteristic) to arrive at

$$\begin{aligned} u' &= s^2 + \frac{(h+2v)s-k}{u} \text{ made monic} \\ v' &\equiv V_1 = h - v - su \pmod{u'} \end{aligned}$$

Composition, Reduced Basis

$$\tilde{v} = \tilde{v}_1x + \tilde{v}_0 \equiv h + 2v \pmod{u}, \mathbf{1M}, \mathbf{1S}$$

$$\begin{aligned} \tilde{v} &= (h_3 + 2)x^3 + h_2x^2 + (h_1 + 2v_1)x + (h_0 + 2v_0) \\ &\equiv (h_2 - (h_3 + 2)u_1)x^2 + (h_1 + 2v_1 - (h_3 + 2)u_0)x + (h_0 + 2v_0) \\ &\equiv (h_1 + 2v_1 - (h_3 + 2)u_0 - (h_2 - (h_3 + 2)u_1)u_1)x \\ &\quad + (h_0 + 2v_0 - (h_2 - (h_3 + 2)u_1)u_0) \pmod{u} \\ \tilde{v}_1 &= h_1 + 2v_1 - (h_3 + 2)u_0 - (h_2 - (h_3 + 2)u_1)u_1 \\ \tilde{v}_0 &= h_0 + 2v_0 - (h_2 - (h_3 + 2)u_1)u_0 \end{aligned}$$

In odd characteristic,

$$\begin{aligned}\tilde{v}_1 &= 2v_1 - 2u_0 + 2u_1^2 = 2(v_1 - u_0 + u_1^2) \\ \tilde{v}_0 &= 2(v_0 + u_0 \cdot u_1)\end{aligned}$$

In even characteristic,

$$\begin{aligned}\tilde{v}_1 &= h_1 + h_2u_1 + h_3(u_0 + u_1^2) = h_1 + u_0 + u_1^2 \\ \tilde{v}_0 &= h_0 + h_2u_0 + h_3u_0u_1 = h_0 + u_0 \cdot u_1\end{aligned}$$

under the assumption that $h_3 = 1$ and $h_2 = 0$.

$$\underline{i = i_1x + i_0 \equiv r(\tilde{v})^{-1} \pmod{u}, \mathbf{4M}}$$

Using the division algorithm for $u = i \cdot \tilde{v} + r$, we have

$$\begin{aligned}x^2 + u_1x + u_0 &= \left(\frac{1}{\tilde{v}_1}x + \left(\frac{u_1}{\tilde{v}_1} - \frac{\tilde{v}_0}{\tilde{v}_1^2}\right)\right)(\tilde{v}_1x + \tilde{v}_0) + \left(u_0 - \frac{u_1\tilde{v}_0}{\tilde{v}_1} + \frac{\tilde{v}_0^2}{\tilde{v}_1^2}\right) \equiv 0 \pmod{u} \\ &\left(\frac{\tilde{v}_1}{\tilde{v}_1^2}x + \left(\frac{u_1\tilde{v}_1 - \tilde{v}_0}{\tilde{v}_1^2}\right)\right)(\tilde{v}_1x + \tilde{v}_0) \equiv \frac{-u_0\tilde{v}_1^2 + u_1\tilde{v}_0\tilde{v}_1 - \tilde{v}_0^2}{\tilde{v}_1^2} \pmod{u} \\ &(\tilde{v}_1x + (u_1\tilde{v}_1 - \tilde{v}_0))(\tilde{v}_1x + \tilde{v}_0) \equiv -u_0\tilde{v}_1^2 + \tilde{v}_0(u_1\tilde{v}_1 - \tilde{v}_0) \pmod{u}\end{aligned}$$

Let $w_2 = u_0 \cdot \tilde{v}_1$ and $w_3 = u_1 \cdot \tilde{v}_1$.

$$i_1 = \tilde{v}_1 \quad i_0 = w_3 - \tilde{v}_0 \quad r = \tilde{v}_0 \cdot i_0 - w_2 \cdot \tilde{v}_1$$

Then $i = i_1x + i_0$ is the ‘‘almost inverse’’ of \tilde{v} modulo u , in the sense that $i \cdot \tilde{v} \equiv r \pmod{u}$. We postpone inverting r until later.

Note that we’ve split the square in $u_0\tilde{v}_1^2$ into $(u_0\tilde{v}_1)\tilde{v}_1$. This will save one multiplication in computing s , for a total savings of 1 square.

$$\underline{k' = k'_1x + k'_0 \equiv \frac{f+hv-v^2}{u} \pmod{u}, \mathbf{3M, 1S (2M, 2S)}}$$

$$\begin{aligned}k &= \frac{(f_6x^6+f_5x^5+f_4x^4+f_3x^3+f_2x^2+\dots)+(h_3x^3+h_2x^2+h_1x+h_0)(x^3+v_1x+v_0)-(x^3+v_1x+v_0)^2}{x^2+u_1x+u_0} \\ &= \frac{(f_6+h_3-1)x^6+(f_5+h_2)x^5+(f_4+h_1+h_3v_1-2v_1)x^4+(f_3+h_0+h_2v_1+h_3v_0-2v_0)x^3+(f_2+h_1v_1+h_2v_0-v_1^2)x^2+\dots}{x^2+u_1x+u_0}\end{aligned}$$

The coefficients of $k = k_4x^4 + k_3x^3 + k_2x^2 + k_1x + k_0$ are defined, then the reduction $k' = k'_1x + k'_0 \equiv k \pmod{u}$, as below (k'_4, k'_3 , and k'_2 are used for intermediate steps in the reduction):

$$\begin{aligned}k_4 &= f_6 + h_3 - 1 & k'_4 &= k_4 \\ k_3 &= f_5 + h_2 - k_4u_1 & k'_3 &= k_3 - k'_4u_1 \\ k_2 &= f_4 + h_1 + h_3v_1 - 2v_1 - k_3u_1 - k_4u_0 & k'_2 &= k_2 - k'_3u_1 - k'_4u_0 \\ k_1 &= f_3 + h_0 + h_2v_1 + h_3v_0 - 2v_0 - k_2u_1 - k_3u_0 & k'_1 &= k_1 - k'_2u_1 - k'_3u_0 \\ k_0 &= f_2 + h_1v_1 + h_2v_0 - v_1^2 - k_1u_1 - k_2u_0 & k'_0 &= k_0 - k'_2u_0\end{aligned}$$

To reduce these equations, we use some simplifying assumptions about the coefficients in odd and even characteristic.

In odd characteristic (not equal to 3), we may assume $h(x) = 0$, $f_6 = 1$, and $f_5 = 0$. Then

$$\begin{aligned}
k_4 &= k'_4 = k_3 = k'_3 = 0 & k_2 &= k'_2 = f_4 - 2v_1 \\
k_1 &= f_3 - 2v_0 - k_2u_1 & k'_1 &= k_1 - k'_2u_1 = f_3 - 2v_0 - 2k'_2u_1 \\
k_0 &= f_2 - v_1^2 - k_1u_1 - k_2u_0 & k'_0 &= (f_2 - v_1^2 - k_1u_1 - k_2u_0) - k'_2u_0 \\
& & &= f_2 - v_1^2 - (k'_1 + k'_2u_1)u_1 - 2k'_2u_0 \\
& & &= f_2 - v_1^2 - k'_1u_1 - (u_1^2 + 2u_0)k'_2
\end{aligned}$$

Let $k'_2 = f_4 - 2v_1$, then $k'_1 = f_3 - 2v_0 - 2k'_2 \cdot u_1$ and $k'_0 = f_2 - v_1^2 - k'_1 \cdot u_1 - (w_1 + 2u_0) \cdot k'_2$, where $w_1 = u_1^2$ was computed in Step 1.

In even characteristic, we may assume $h_3 = 1$ and $h_2 = 0$. If $f_6 = 1$ (which is allowed if and only if the number of elements in the field is an *even* power of two), then we may also assume $f_5 = f_4 = f_3 = 0$. We work out the coefficient of k and k' under these assumptions; the general formulas above can be applied for other values of f_6 . Then

$$\begin{aligned}
k_4 &= k'_4 = 1 & k_3 &= u_1, \quad k'_3 = 0 \\
k_2 &= h_1 + v_1 + u_1^2 + u_0 & k'_2 &= h_1 + v_1 + u_1^2 \\
k_1 &= h_0 + v_0 + (h_1 + v_1 + u_1^2 + u_0)u_1 + u_1u_0 & k'_1 &= h_0 + v_0 + (h_1 + v_1 + u_1^2)u_1 + (h_1 + v_1 + u_1^2)u_1 \\
&= h_0 + v_0 + (h_1 + v_1 + u_1^2)u_1 & &= h_0 + v_0
\end{aligned}$$

$$\begin{aligned}
k_0 &= f_2 + h_1v_1 + v_1^2 + (h_0 + v_0 + (h_1 + v_1 + u_1^2)u_1)u_1 + (h_1 + v_1 + u_1^2 + u_0)u_0 \\
&= f_2 + (h_1 + v_1)v_1 + (h_0 + v_0)u_1 + (h_1 + v_1)u_1^2 + u_1^4 + (h_1 + v_1)u_0 + u_0u_1^2 + u_0^2 \\
&= f_2 + (h_1 + v_1)(v_1 + u_1^2 + u_0) + (h_0 + v_0)u_1 + u_0u_1^2 + (u_1^2)^2 + u_0^2 \\
k'_0 &= k_0 + (h_1 + v_1 + u_1^2)u_0 = f_2 + (h_1 + v_1)(v_1 + u_1^2) + (h_0 + v_0)u_1 + (u_1^2)^2 + u_0^2
\end{aligned}$$

Hence, $k'_1 = h_0 + v_0$ and $k'_0 = f_2 + (h_1 + v_1) \cdot (v_1 + w_1) + k'_1 \cdot u_1 + w_1^2 + u_0^2$.

$s' = s'_1x + s'_0 \equiv i \cdot k' \pmod{u}$, **4M**

We first compute $s' = rs$, then compute $s = \frac{s'}{r}$ after we've found the inverse of r .

$$\begin{aligned}
i \cdot k' &= (i_1x + i_0) \cdot (k'_1x + k'_0) \\
&= (i_1k'_1)x^2 + (i_0k'_1 + i_1k'_0)x + (i_0k'_0) \\
&\equiv (i_0k'_1 + i_1k'_0 - u_1i_1k'_1)x + (i_0k'_0 - u_0i_1k'_1) \pmod{u}
\end{aligned}$$

Using the factors w_2 and w_3 found in computing i (recalling that $i_1 = \tilde{v}_1$, we have

$$\begin{aligned}
s'_1 &= i_1 \cdot k'_0 + (i_0 - w_3) \cdot k'_1 = i_1 \cdot k_0 - \tilde{v}_0 \cdot k'_1 \\
s'_0 &= i_0 \cdot k'_0 - w_2 \cdot k'_1
\end{aligned}$$

Reduction, Reduced Basis

$$\tilde{u} = \tilde{u}_2x^2 + \tilde{u}_1x + \tilde{u}_0 = s^2 + \frac{(h+2v)s-k}{u}$$

Even though we don't know s yet, we find what the leading coefficient of \tilde{u} in order to make \tilde{u} monic after the inversion step.

$$\begin{aligned}\tilde{u} &= (s_1x + s_0)^2 + \frac{((h_3+2)x^3+h_2x^2+(h_1+2v_1)x+(h_0+2v_0))(s_1x+s_0)-(k_4x^4+k_3x^3+k_2x^2+k_1x+k_0)}{x^2+u_1x+u_0} \\ &= (s_1^2x^2 + 2s_0s_1x + s_0^2) + \frac{((h_3+2)s_1-k_4)x^4+((h_3+2)s_0+h_2s_1-k_3)x^3+(h_2s_0+(h_1+2v_1)s_1-k_2)x^2+\dots}{x^2+u_1x+u_0}\end{aligned}$$

While it is possible to give an general formula for this division, it helps at this point to split into odd and even characteristic and use the same simplifying assumptions. We will count the multiplications in the final calculations.

In odd characteristic,

$$\begin{aligned}\tilde{u} &= (s_1^2x^2 + 2s_0s_1x + s_0^2) + \frac{2s_1x^4+2s_0x^3+(2v_1s_1-k_2)x^2+\dots}{x^2+u_1x+u_0} \\ &= (s_1^2x^2 + 2s_0s_1x + s_0^2) + (2s_1x^2 + (2s_0 - 2s_1u_1)x + (2v_1s_1 - k_2 - 2s_1u_0 - u_1(2s_0 - 2s_1u_1))) \\ &= (s_1^2 + 2s_1)x^2 + (2s_0s_1 + 2s_0 - 2s_1u_1)x + (s_0^2 + 2v_1s_1 - k_2 - 2s_1u_0 - 2s_0u_1 + 2s_1u_1^2) \\ &= (s_1(s_1 + 2))x^2 + 2(s_0 + (s_0 - u_1)s_1)x + (-k_2 + (s_0 - 2u_1)s_0 + 2(v_1 - u_0 + u_1^2)s_1)\end{aligned}$$

So for odd characteristic, let

$$\begin{aligned}\tilde{u}_2 &= s_1(s_1 + 2) \\ \tilde{u}_1 &= 2(s_0 + (s_0 - u_1)s_1) \\ \tilde{u}_0 &= -k_2' + (s_0 - 2u_1)s_0 + \tilde{v}_1s_1\end{aligned}$$

In even characteristic, assuming $h_3 = 1, h_2 = 0, f_6 = 1, f_5 = f_4 = f_3 = 0,$

$$\begin{aligned}\tilde{u} &= (s_1^2x^2 + s_0^2) + \frac{(s_1+1)x^4+(s_0+u_1)x^3+(h_1s_1+(h_1+v_1+u_1^2+u_0))x^2+\dots}{x^2+u_1x+u_0} \\ &= (s_1^2x^2 + s_0^2) + ((s_1 + 1)x^2 + ((s_0 + u_1) + u_1(s_1 + 1))x \\ &\quad + (h_1s_1 + h_1 + v_1 + u_1^2 + u_0 + u_0(s_1 + 1) + u_1((s_0 + u_1) + u_1(s_1 + 1))) \\ &= (s_1^2 + s_1 + 1)x^2 + (s_0 + u_1s_1)x + (s_0^2 + h_1s_1 + h_1 + v_1 + u_1^2 + u_0s_1 + u_1s_0 + u_1^2s_1) \\ &= (s_1^2 + s_1 + 1)x^2 + (s_0 + u_1s_1)x + (h_1 + v_1 + u_1^2 + (s_0 + u_1)s_0 + (h_1 + u_0 + u_1^2)s_1)\end{aligned}$$

So for even characteristic, let

$$\begin{aligned}\tilde{u}_2 &= s_1^2 + s_1 + 1 \\ \tilde{u}_1 &= s_0 + u_1s_1 \\ \tilde{u}_0 &= k_2' + (s_0 + u_1)s_0 + \tilde{v}_1s_1\end{aligned}$$

Inversion Step, compute $I = (r \cdot \tilde{u}'_2)^{-1}, \frac{1}{\tilde{u}_2}, \frac{1}{r}, s_0,$ and $s_1, \mathbf{1I}, \mathbf{6M}, \mathbf{2S} (\mathbf{1I}, \mathbf{7M}, \mathbf{1S})$

We now need to find the inverses of r and \tilde{u}_2 . Since we only know $s'_1 = rs_1$, we must find the inverse of $\tilde{u}'_2 = r^2\tilde{u}_2$ instead. In odd characteristic,

$$\tilde{u}'_2 = (s'_1 + r)^2 - r^2$$

In even characteristic,

$$\tilde{u}'_2 = s_1'^2 + s_1' r + r^2 = s_1' \cdot (s_1' + r) + r^2$$

In any characteristic, we compute the following expressions:

$$\begin{aligned} I &= (r \cdot \tilde{u}'_2)^{-1} \\ \frac{1}{\tilde{u}_2} &= r \cdot r^2 \cdot I \\ \frac{1}{r} &= \tilde{u}'_2 \cdot I \\ s_0 &= \frac{1}{r} \cdot s'_0 \\ s_1 &= \frac{1}{r} \cdot s'_1 \end{aligned}$$

$u' = x^2 + u'_1 x + u'_0$, **5M**

u' is \tilde{u} made monic, so $u'_1 = \frac{\tilde{u}_1}{\tilde{u}_2}$ and $u'_0 = \frac{\tilde{u}_0}{\tilde{u}_2}$.

In odd characteristic,

$$\begin{aligned} u'_1 &= \frac{1}{\tilde{u}_2} \cdot (2(s_0 + (s_0 - u_1) \cdot s_1)) \\ u'_0 &= \frac{1}{\tilde{u}_2} \cdot (-k'_2 + (s_0 - 2u_1) \cdot s_0 + \tilde{v}_1 \cdot s_1) \end{aligned}$$

In even characteristic,

$$\begin{aligned} u'_1 &= \frac{1}{\tilde{u}_2} \cdot (s_0 + u_1 \cdot s_1) \\ u'_0 &= \frac{1}{\tilde{u}_2} \cdot (k'_2 + (s_0 + u_1) \cdot s_0 + \tilde{v}_1 \cdot s_1) \end{aligned}$$

$v' = x^3 + v'_1 x + v_0$, **5M, 1S**

We start by calculating the coefficients of $\underline{v} = h - v - su$ before reducing modulo u' to get v' .

$$\begin{aligned} \underline{v} &= (h_3 x^3 + h_2 x^2 + h_1 x + h_0) - (x^3 + v_1 x + v_0) - (s_1 x + s_0)(x^2 + u_1 x + u_0) \\ &= (h_3 - s_1 - 1)x^3 + (h_2 - s_0 - s_1 u_1)x^2 + (h_1 - v_1 - s_0 u_1 - s_1 u_0)x + (h_0 - v_0 - s_0 u_0) \end{aligned}$$

Let $\underline{v}_3 = h_3 - s_1 - 1$, $\underline{v}_2 = h_2 - s_0 - s_1 u_1$, $\underline{v}_1 = h_1 - v_1 - s_0 u_1 - s_1 u_0$, and $\underline{v}_0 = h_0 - v_0 - s_0 u_0$.

Then reducing $\underline{v} = h - v - su$ modulo u' results in

$$\begin{aligned} v' &\equiv x^3 + (\underline{v}_2 - u'_1(\underline{v}_3 - 1))x^2 + (\underline{v}_1 - u'_0(\underline{v}_3 - 1))x + \underline{v}_0 \\ &\equiv x^3 + (\underline{v}_1 - u'_0(\underline{v}_3 - 1) - u'_1(\underline{v}_2 - u'_1(\underline{v}_3 - 1)))x + (\underline{v}_0 - u'_0(\underline{v}_2 - u'_1(\underline{v}_3 - 1))) \end{aligned}$$

Hence, $v'_1 = \underline{v}_1 - u'_0(\underline{v}_3 - 1) - u'_1(\underline{v}_2 - u'_1(\underline{v}_3 - 1))$ and $v'_0 = \underline{v}_0 - u'_0(\underline{v}_2 - u'_1(\underline{v}_3 - 1))$.

In odd characteristic,

$$\begin{aligned} v'_1 &= (-v_1 - s_0 u_1 - s_1 u_0) - u'_0(-s_1 - 2) - u'_1(-s_0 - s_1 u_1 - u'_1(-s_1 - 2)) \\ &= -v_1 + 2u'_0 - 2u_1'^2 + ((u'_0 - u_0) - u'_1(u'_1 - u_1))s_1 + (u'_1 - u_1)s_0 \\ v'_0 &= -v_0 - s_0 u_0 - u'_0(-s_0 - s_1 u_1 - u'_1(-s_1 - 2)) \\ &= -v_0 - 2u'_0 u'_1 + (u'_0 - u_0)s_0 - (u'_1 - u_1)s_1 u'_0 \\ &= -v_0 + (u'_0 - u_0)s_0 - (2u_1' + (u'_1 - u_1)s_1)u'_0 \end{aligned}$$

To optimize this calculation, let $z_0 = u'_0 - u_0$, $z_1 = u'_1 - u_1$, $w_0 = z_0 \cdot s_0$, and $w_1 = z_1 \cdot s_1$. Then

$$\begin{aligned} v'_1 &= -v_1 + 2u'_0 - 2u_1'^2 + (z_0 - u'_1 z_1)s_1 + z_1 s_0 \\ &= -v_1 + 2u'_0 - 2u_1'^2 + (z_0 + z_1) \cdot (s_0 + s_1) - w_0 - (u'_1 + 1) \cdot w_1 \\ v'_0 &= -v_0 + w_0 - (2u'_1 + w_1) \cdot u'_0 \end{aligned}$$

In even characteristic,

$$\begin{aligned} v'_1 &= (h_1 + v_1 + s_0 u_1 + s_1 u_0) + u'_0(s_1 + 1) + u'_1(s_0 + s_1 u_1 + u'_1(s_1 + 1)) \\ &= h_1 + v_1 + u'_0 + u_1'^2 + (u'_1 + u_1)s_0 + ((u'_0 + u_0) + u'_1(u'_1 + u_1))s_1 \\ v'_0 &= (h_0 + v_0 + s_0 u_0) + u'_0(s_0 + s_1 u_1 + u'_1(s_1 + 1)) \\ &= h_0 + v_0 + u'_0 u'_1 + (u'_0 + u_0)s_0 + (u'_1 + u_1)u'_0 s_1 \\ &= h_0 + v_0 + (u'_0 + u_0)s_0 + (u'_1 + (u'_1 + u_1)s_1)u'_0 \end{aligned}$$

Once again, let $z_0 = u'_0 + u_0$, $z_1 = u'_1 + u_1$, $w_0 = z_0 \cdot s_0$, and $w_1 = z_1 \cdot s_1$. Then

$$\begin{aligned} v'_1 &= h_1 + v_1 + u'_0 + u_1'^2 + z_1 s_0 + (z_0 + u'_1 z_1)s_1 \\ &= h_1 + v_1 + u'_0 + u_1'^2 + (z_0 + z_1) \cdot (s_0 + s_1) + w_0 + (u'_1 + 1) \cdot w_1 \\ v'_0 &= h_0 + v_0 + w_0 + (u'_1 + w_1) \cdot u'_0 \end{aligned}$$

This completes the reduction.