Geometric Flavored Arithmetic on Jacobians of Hyperelliptic Curves

Craig Costello

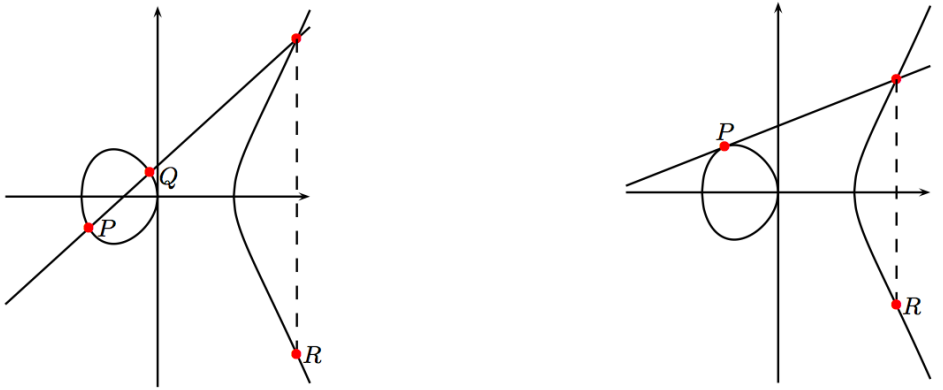
craig.costello@qut.edu.au
QUT and UCI

Joint work (in progress) with Kristin Lauter

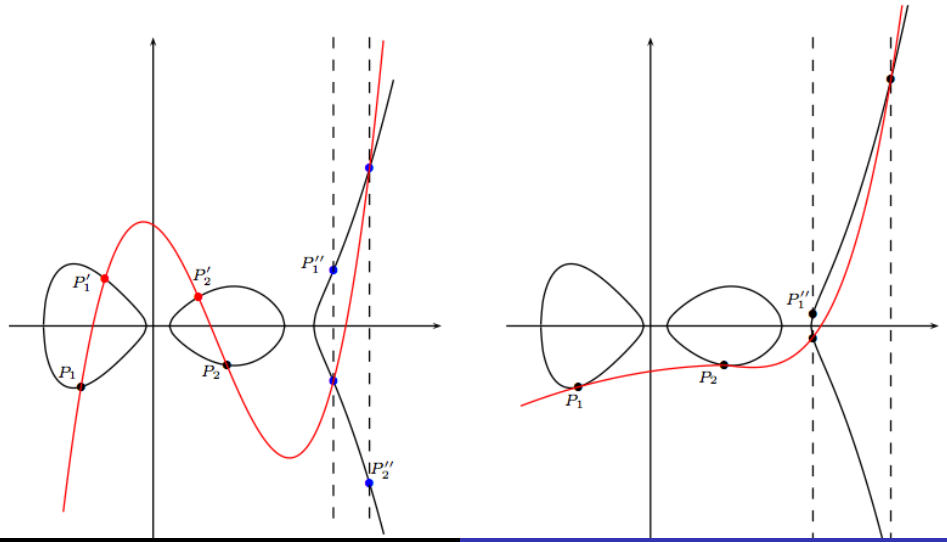
June 10, 2011

Overview

Genus 1 geometric description inspires arithmetic ("chord-and-tangent")...



Genus g geometric description hasn't influenced arithmetic...



ECC vs HECC

- 1985: Koblitz and Miller independently suggest elliptic curves for cryptographic groups
- 1987: Cantor presents algorithm for computing in the Jacobian of hyperelliptic curves
- 1989: Koblitz further suggests Jacobians of hyperelliptic curves as suitable groups (and generalizes Cantor's algorithm)
- ECC vs HECC: interesting question surfacing over last 25 years
- Cryptographic pairings also require elliptic and hyperelliptic curves
- Elliptic curves favorable in most scenarios (a lot of work done here)
- Hyperelliptic curve arithmetic (still work, but not as much)
- See talks by Bernstein and Lange (Elliptic vs. Hyperelliptic - Parts I, II, III)

Divisors on a curve

- A divisor D on C/K is a formal sum over all points

$$D = \sum_{P \in C(\overline{K})} n_P(P),$$

  where all but finitely many $n_P \in \mathbb{Z}$ are zero.
- The degree of D is given as

$$\deg(D) = \sum_{P \in C(\overline{K})} n_P$$

- The set of all divisors $\mathrm{div}(C)$ forms an Abelian group.
- For any rational function f on C, there is an associated divisor

$$\mathrm{div}(f) = \sum_{P \in C(\overline{K})} \mathrm{ord}_P(f)(P)$$

  which encodes locations and multiplicities of zeros and poles: principal divisors $\mathrm{Ppl}(C)$.
- Important theorem: $\mathrm{Ppl}(C) \subset \mathrm{Div}^0(C)$.

The Jacobian of Hyperelliptic Curves

- Take C_g/K as the genus g hyperelliptic curve defined by

$$C_g : y^2 + h(x)y = f(x)$$

$$h(x), f(x) \in K[x], \quad \deg(f) = 2g + 1, \quad \deg(h) \leq g, \quad f \text{ monic},$$

- We use the group $\mathrm{Jac}(C_g)$, which is isomorphic to the quotient group

$$\mathrm{Pic}^0(C_g) := \mathrm{Div}^0(C_g)/\mathrm{Ppl}(C_g)$$

- Elements of Jacobian are equivalence classes of $\mathrm{Div}^0(C_g)$, for which there is a unique ("*reduced*") representative

$$(P_1) + (P_2) + \ldots + (P_r) - r(P_\infty)$$

where $r \leq g$ (guaranteed by Riemann-Roch).

Mumford representation

- Mumford gave a convenient way to represent reduced divisors. Let D be

$$D = (P_1) + (P_2) + ... + (P_r) - r(P_\infty)$$

with $P_i = (x_i, y_i)$

- Represent D as

$$D = (u(x), v(x))$$

where $u(x_i) = 0$ and $v(x_i) = y_i$ for all i.

- In general $\deg(u) = g$ (monic) and $\deg(v) = g - 1$ (not monic).
- **Question:** why?

Example

- Consider genus 3 curve

$$C/\mathbb{F}_{521} : y^2 = x^7 + 2x^3 - 7x^2 + 5x + 1$$

- A reduced divisor on C is

$$\begin{aligned} D &= (P_1) + (P_2) + (P_3) - 3(P_\infty) \\ &= (447, 117) + (431, 96) + (388, 478) - 3(P_\infty) \end{aligned}$$

- The Mumford representation is

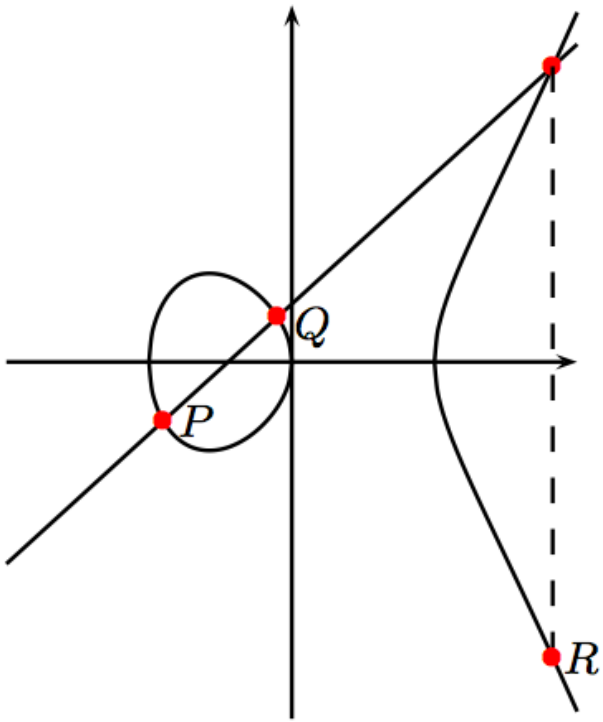
$$\begin{aligned} D &= (u(x), v(x)) \\ &= (x^3 + 297x^2 + 338x + 80, 108x^2 + 97x + 449) \end{aligned}$$

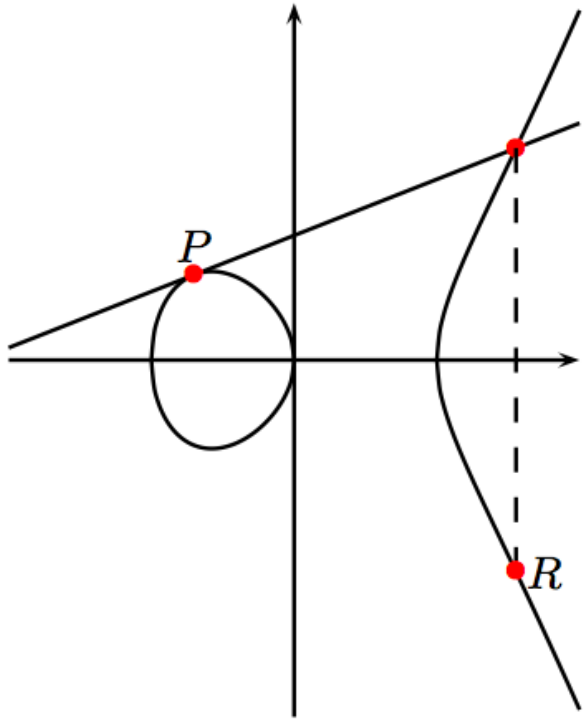
- We have

$$\begin{aligned} u(447) &= 0, & v(447) &= 117 \\ u(431) &= 0, & v(431) &= 96 \\ u(388) &= 0, & v(388) &= 478 \end{aligned}$$

- Note: going from Mumford back to (x, y) involves finding roots in $\mathbb{F}_q$

Review: Chord-and-tangent description

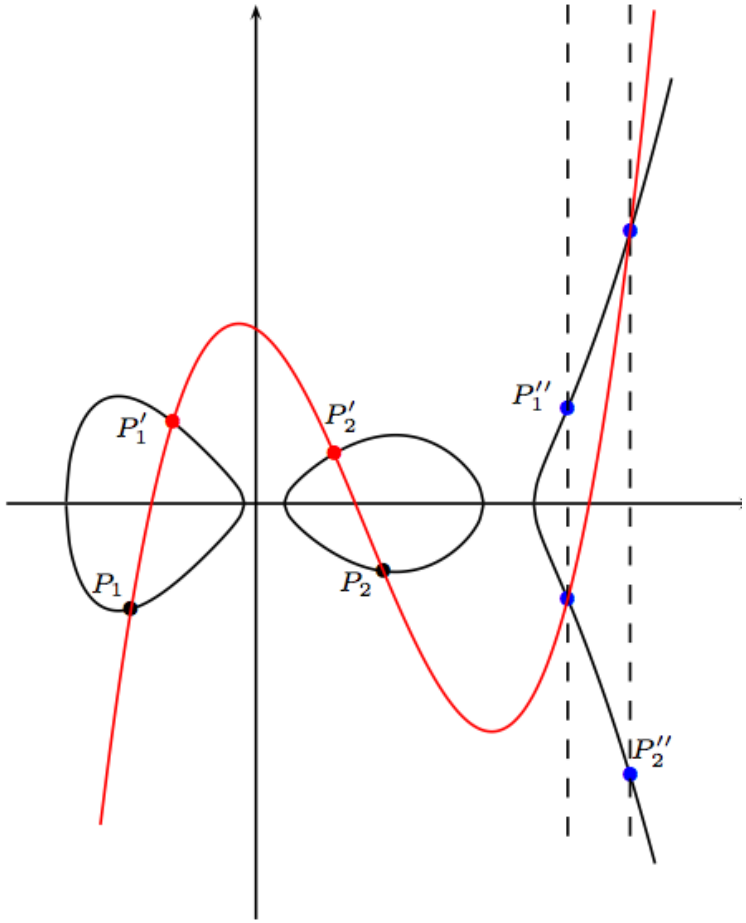




- Better (preparation for $g > 1$) to think $D_P \oplus D_Q = D_R$, where $D_P = (P) - (\infty)$

Why Mumford coordinates?

- Trying to do the same thing in (x, y) coordinates gives rise to costly operations (root finding in $\mathbb{F}_q$ required for P_1'' and P_2'')



- No root finding if we use Mumford coordinates

Why Mumford coordinates?

- Mumford coordinates are necessary to avoid root extractions in $\mathbb{F}_q$
- But now we don't have P_1, P_2, P_1' and P_2' to find the interpolating polynomial
- Cantor's algorithm is based on the classical composition of binary quadratic forms (Gauss) and uses the Mumford representation...

Cantor's algorithm (composition and reduction)

INPUT: Two divisor classes $\overline{D}_1 = [u_1, v_1]$ and $\overline{D}_2 = [u_2, v_2]$ on the curve $C : y^2 + h(x)y = f(x)$.
OUTPUT: The unique reduced divisor D such that $\overline{D} = \overline{D}_1 \oplus \overline{D}_2$.

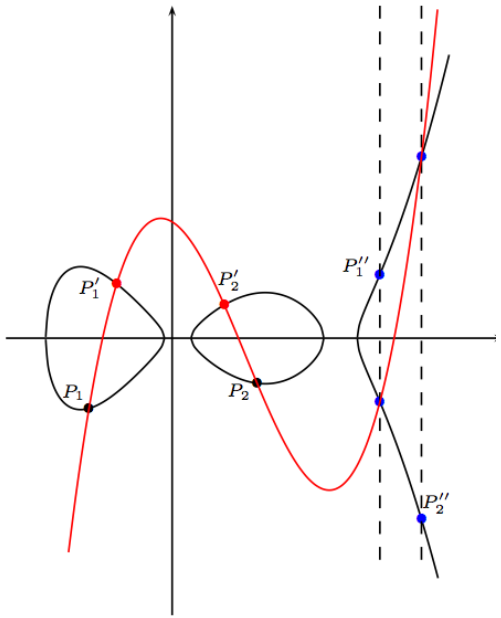
1. $d_1 \leftarrow \gcd(u_1, u_2)$ $\qquad [d_1 = e_1 u_1 + e_2 u_2]$
2. $d \leftarrow \gcd(d_1, v_1 + v_2 + h)$ $\qquad [d = c_1 d_1 + c_2(v_1 + v_2 + h)]$
3. $s_1 \leftarrow c_1 e_1$, $s_2 \leftarrow c_1 e_2$ and $s_3 \leftarrow c_2$
4. $u \leftarrow \dfrac{u_1 u_2}{d^2}$ and $v \leftarrow \dfrac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
5. **repeat**
6. $\quad u' \leftarrow \dfrac{f - vh - v^2}{u}$ and $v' \leftarrow (-h - v) \bmod u'$
7. $\quad u \leftarrow u'$ and $v \leftarrow v'$
8. **until** $\deg u \leqslant g$
9. make u monic
10. **return** $[u, v]$

Cantor's algorithm in cryptography

- Presented using polynomial arithmetic
- Requires costly operations (GCD, CRT, ...)
- 2000-2001: Harley (counting points under Gaudry) - makes polynomial arithmetic explicit
- 2001: Lange greatly improves and generalizes
- Several papers since... all still require Chinese Remainder Theorem and still based on Cantor's composition
- Explicit formulas don't benefit from geometric aid
- **Goal:** like to have "chord-and-tangent" analogue in genus $g \geq 2$ (that can be utilized like elliptic curves)

Our solution

- Our solution: essentially performs composition in Mumford coordinates analogously to composition in (x, y) coordinates
- Recall (for $g = 2$) we want to find cubic interpolating P_1, P_2, P_1' and P_2' without actually having P_1, P_2, P_1' and P_2' explicitly.



- Can we get Mumford formulas for l similar to the (x, y)-formulas???

$$\begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_1' & x_1'^2 & x_1'^3 \\ 1 & x_2' & x_2'^2 & x_2'^3 \end{pmatrix} \cdot \begin{pmatrix} l_0 \\ l_1 \\ l_2 \\ l_3 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_1' \\ y_2' \end{pmatrix} \cdot$$

Step 1: "Mumford ideals"

- Formulas arising in the function field

$$K(C) = K[x, y]/\langle C_g(x, y)\rangle$$

  can be simplified by the ideal $\langle C_g(x, y)\rangle$

- If we're dealing with formulas that are completely dependent on the Mumford representation, we wan't to be equipped to with the analogous ideals

- Most divisor class groups have a reduced representative of full degree i.e. $\deg(u(x)) = g$ and $\deg(v(x)) = g - 1$, or g elements in the support of D
- Cryptographic implementations concentrate (only) on this general case

Proposition 1: "Mumford ideals" cont...

Proposition 1: On the Jacobian of a genus g hyperelliptic curve, the dense set of divisor classes with reduced representatives of full degree g can be described exactly as the intersection of g hypersurfaces in $2g$ variables.

Proposition 1: "Mumford ideals" cont... (an example)

$$C/\mathbb{F}_{37} : y^2 = x^5 + 2x^3 - 7x^2 + 5x + 1$$

General divisor $D = (x^2 + u_1 x + u_0, v_1 x + v_0) \in \mathrm{Jac}(C)$

$$\begin{aligned}(v_1 x + v_0)^2 - (x^5 + 2x^3 - 7x^2 + 5x + 1) & \\ \equiv \Psi_1 x + \Psi_0 & \mod \langle x^2 + u_1 x + u_0 \rangle \\ \equiv 0 & \mod \langle x^2 + u_1 x + u_0 \rangle,\end{aligned}$$

where

$$\Psi_1 = 3\,u_0 {u_1}^2 - {u_1}^4 - {u_0}^2 + 2\,v_0 v_1 - {v_1}^2 u_1 + 2\,(u_0 - {u_1}^2) - 7u_1 - 5,$$

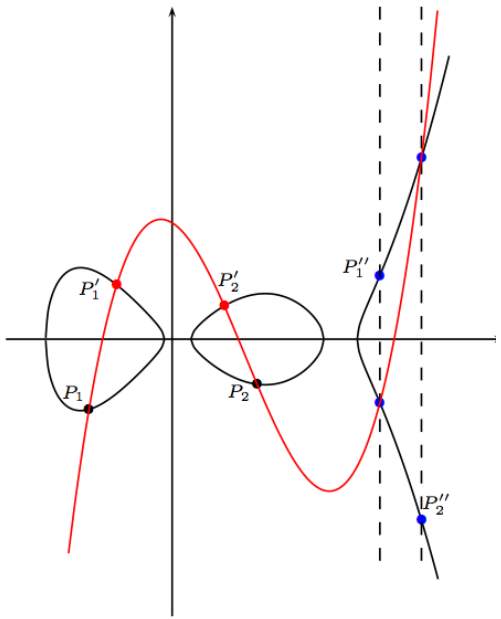
$$\Psi_0 = {v_0}^2 - {v_1}^2 u_0 + 2\,{u_0}^2 u_1 - {u_1}^3 u_0 - 2u_1 u_0 - 7u_0 - 1.$$

$\#$ Tuples $(u_0, u_1, v_0, v_1) \in \mathbb{F}_{37}$ satisfying $\Psi_1 = \Psi_2 = 0$ is 1373, which equals $\#$ degree 2 divisors on $\mathrm{Jac}(C)$. Total $\#\mathrm{Jac} = 1412$.

$\langle \Psi_1 \rangle$, $\langle \Psi_0 \rangle$ are "Mumford ideals".

Proposition 2: Addition function

Proposition 2: Let D and D' be reduced divisors of degree g on $\mathrm{Jac}(C_g)$ such that $\mathrm{supp}(D) = \{P_1, ..., P_g\} \cup \{\infty\}$, $\mathrm{supp}(D') = \{P'_1, ..., P'_g\} \cup \{\infty\}$ and $\mathrm{supp}(D) \cap \mathrm{supp}(D') = \{\infty\}$. A function f on C_g with divisor $\mathrm{div}(f)$ such that $(\mathrm{supp}(D) \cup \mathrm{supp}(D')) \subseteq \mathrm{supp}(\mathrm{div}(f))$ can be determined by a **linear system** of $2g$ equations which is comprised entirely of the Mumford coordinates of D and D'.



Proposition 2: Addition function cont... (an example)

Take genus 3 curve $C/\mathbb{F}_{71} : y^2 = x^7 + 1$

$$D = \big(u(x), v(x)\big) = \big(x^3 + 6x^2 + 41x + 33, 29x^2 + 22x + 47\big),$$
$$D' = \big(u'(x), v'(x)\big) = \big(x^3 + 18x^2 + 15x + 37, 49x^2 + 46x + 59\big).$$

Let $l(x) = \sum_{i=0}^{5} l_i x^i$ be the polynomial interpolating both supports (which we don't know).

For D, we have $\qquad l(x) - v(x) \equiv 0 \bmod \langle u(x) \rangle,$

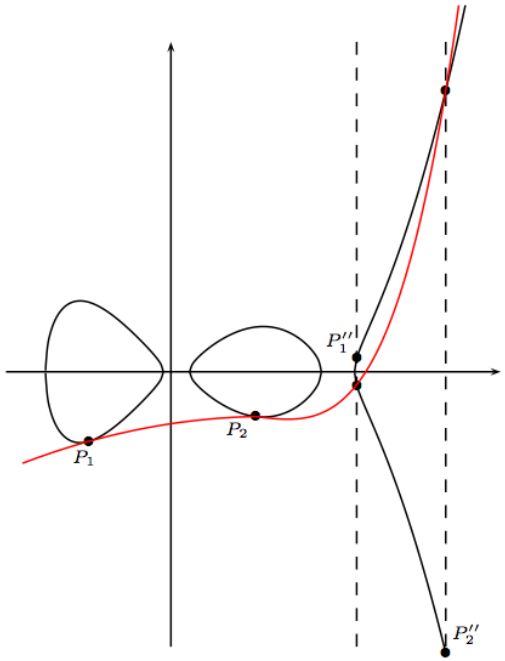
$$\sum_{i=0}^{5} l_i x^i - (29x^2 + 22x + 47) \equiv 0 \bmod \langle u(x) \rangle$$

$$\begin{aligned} 0 \equiv\ & (l_2 + 65l_3 + 66l_4 + 30l_5 - 29)x^2 \\ & + (l_1 + 30l_3 + 48l_5 - 22)x \\ & + l_0 + 38l_3 + 56l_4 + 23l_5 - 47, \end{aligned}$$

Similarly for D' we get another 3 linear equations. Together solve to give $l(x) = 21x^5 + x^4 + 36x^3 + 46x^2 + 64x + 57$.

Proposition 3: Doubling function

Proposition 3: Let D be a divisor of degree g representing a class on $\mathrm{Jac}(C_g)$ with $\mathrm{supp}(D) = \{P_1, ..., P_g\} \cup \{\infty\}$. A function f on C_g such that each non-trivial element in $\mathrm{supp}(D)$ occurs with multiplicity two in $\mathrm{div}(f)$ can be determined by a linear system of $2g$ equations which are comprised entirely of the $2g$ Mumford coordinates of D.



In proof, use derivatives to show linear. In practice, we found simpler expressions reducing mod $\langle u(x)^2 \rangle$ and using Mumford ideals to linearize.

Proposition 3: Doubling function

$C : y^2 = x^7 + 5x + 1$ over $\mathbb{F}_{257}$

$$D = (u(x), v(x)) = (x^3 + 57x^2 + 26x + 80, 176x^2 + 162x + 202).$$

Interpolating the three elements in $\mathrm{supp}(D)$ gives 3 equations exactly before. The other 3 equations come from the derivative

$$\frac{7x^6 + 5}{2y} = 5l_5x^4 + 4l_4x^3 + 3l_3x^2 + 2l_2x + l_1$$

$$\frac{7x^6 + 5}{2(176x^2 + 162x + 202)} \equiv 5l_5x^4 + 4l_4x^3 + 3l_3x^2 + 2l_2x + l_1$$

$$\begin{aligned} 0 \equiv (76l_5 + 2541l_4 + 254l_3 + 166)x^2 + (209 + 255l_2 + 104l_4 + 186l_5)x \\ +73l_5 + 63l_4 + 256l_1 + 31 \mod \langle x^3 + 57x^2 + 26x + 80 \rangle. \end{aligned}$$

Together they solve to give
$l(x) = 84x^5 + 213x^3 + 78x^2 + 252x + 165.$

How to generate explicit formulas: genus 2

- Do exactly as before with arbitrary inputs
  $D = (x^2 + u_1 x + u_0, v_1 x + v_0)$ and
  $D' = (x^2 + u_1' x + u_0', v_1' x + v_0')$.
- Make use of the Mumford ideals when formulas get big

$$\Psi_0 = {v_0}^2 - a_0 + a_2 u_0 - {v_1}^2 u_0 + 2\,{u_0}^2 u_1 - u_1 a_3 u_0 - {u_1}^3 u_0,$$
$$\Psi_1 = 2\,v_0 v_1 - a_1 - {v_1}^2 u_1 + a_2 u_1 - a_3({u_1}^2 - u_0) + 3\,u_0 {u_1}^2 - {u_1}^4 - {u_0}^2.$$

- Be sure to exploit nice linear systems that arise

$$\begin{pmatrix} 1 & 0 & -u_0 & u_1 u_0 \\ 0 & 1 & -u_1 & u_1^2 - u_0 \\ 1 & 0 & -u_0' & u_1' u_0' \\ 0 & 1 & -u_1' & {u_1'}^2 - u_0' \end{pmatrix} \cdot \begin{pmatrix} l_0 \\ l_1 \\ l_2 \\ l_3 \end{pmatrix} = \begin{pmatrix} v_0 \\ v_1 \\ v_0' \\ v_1' \end{pmatrix}.$$

Genus 2 explicit formulas: affine addition

Input:	$D = (u_1, u_0, v_1, v_0, uu_1 = u_1^2, uu_0 = u_1 u_0)$, $D' = (u_1', u_0', v_1', v_0', uu_1' = u_1'^2, uu_0' = u_1' u_0')$.		Operations in $\mathbb{F}_q$
	$\sigma_1 \leftarrow u_1 + u_1', \quad \Delta_0 \leftarrow v_0 - v_0', \quad \Delta_1 \leftarrow v_1 - v_1',$ $M_1 \leftarrow uu_1 - u_0 - uu_1' + u_0', \quad M_2 \leftarrow uu_0' - uu_0, \quad M_3 \leftarrow u_1 - u_1', \quad M_4 \leftarrow u_0' - u_0,$ $t_1 \leftarrow (M_2 - \Delta_0) \cdot (\Delta_1 - M_1), \quad t_2 \leftarrow (-\Delta_0 - M_2) \cdot (\Delta_1 + M_1),$		**2M**
	$t_3 \leftarrow (-\Delta_0 + M_4) \cdot (\Delta_1 - M_3), \quad t_4 \leftarrow (-\Delta_0 - M_4) \cdot (\Delta_1 + M_3),$		**2M**
	$r_1 \leftarrow t_1 - t_2 \quad r_2 \leftarrow t_4 - t_3, \quad r_3 \leftarrow t_3 + t_4 - t_1 - t_2 - 2(M_2 - M_4) \cdot (M_1 + M_3),$		**1M**
	$l_2 \leftarrow r_1/2, \quad l_3 \leftarrow -r_2/2, \quad d \leftarrow r_3/2,$ $A \leftarrow 1/(d \cdot l_3), \quad B \leftarrow d \cdot A, \quad C \leftarrow d \cdot B, \quad D \leftarrow l_2 \cdot B, \quad E \leftarrow l_3^2 \cdot A, \quad CC \leftarrow C^2,$		**I** + 5**M** + 2**S**
	$u_1'' \leftarrow 2D - CC - \sigma_1, \quad u_0'' \leftarrow D^2 + C \cdot (v_1 + v_1') - ((u_1'' - CC) \cdot \sigma_1 + (uu_1 + uu_1'))/2,$		2**M** + 1**S**
	$uu_1'' \leftarrow u_1''^2, \quad uu_0'' \leftarrow u_1'' \cdot u_0'',$		1**M** + 1**S**
	$v_1'' \leftarrow D \cdot (u_1 - u_1'') + uu_1'' - u_0'' - uu_1 + u_0, \quad v_0'' \leftarrow D \cdot (u_0 - u_0'') + uu_0'' - uu_0,$		2**M**
	$v_1'' \leftarrow E \cdot v_1'' + v_1 \quad v_0'' \leftarrow E \cdot v_0'' + v_0.$		2**M**
Output:	$D'' = \rho(D \oplus D') = (u_1'', u_0'', v_1'', v_0'', uu_1'' = u_1''^2, uu_0'' = u_1'' u_0'')$.	**Total**	**I** + 17**M** + 4**S**

Table: Explicit formulas for a general addition $D'' = D \oplus D'$ involving two degree 2 divisors on $\mathrm{Jac}(C_2)$.

Genus 2 explicit formulas: affine doubling

Input:	$D = (u_1, u_0, v_1, v_0, uu_1 = u_1^2, uu_0 = u_1 u_0)$.		Operations
	$vv \leftarrow v_1^2, \quad v\alpha \leftarrow (v_1 + u_1)^2 - vv - uu_1,$		2**S**
	$M_1 \leftarrow 2v_0 - 2v\alpha, \quad M_2 \leftarrow 2v_1 \cdot (u_0 + 2uu_1), \quad M_3 \leftarrow -2v_1, \quad M_4 \leftarrow v\alpha + 2v_0,$		1**M**
	$z_1 \leftarrow a_2 + 2uu_1 \cdot u_1 + 2uu_0 - vv, \quad z_2 \leftarrow a_3 - 2u_0 + 3uu_1,$		1**M**
	$t_1 \leftarrow (M_2 - z_1) \cdot (z_2 - M_1), \quad t_2 \leftarrow (-z_1 - M_2) \cdot (z_2 + M_1),$		2**M**
	$t_3 \leftarrow (M_4 - z_1) \cdot (z_2 - M_3), \quad t_4 \leftarrow (-z_1 - M_4) \cdot (z_2 + M_3),$		2**M**
	$r_1 \leftarrow t_1 - t_2, \quad r_2 \leftarrow t_4 - t_3, \quad r_3 \leftarrow t_3 + t_4 - t_1 - t_2 - 2(M_2 - M_4) \cdot (M_1 + M_3),$		1**M**
	$l_2 \leftarrow r_1/2, \quad l_3 \leftarrow -r_2/2, \quad d \leftarrow r_3/2,$		
	$A \leftarrow 1/(d \cdot l_3), \quad B \leftarrow d \cdot A, \quad C \leftarrow d \cdot B, \quad D \leftarrow l_2 \cdot B, \quad E \leftarrow l_3^2 \cdot A,$		**I** + 5**M** + 1**S**
	$u_1'' \leftarrow 2D - C^2 - 2u_1, \quad u_0'' \leftarrow (D - u_1)^2 + 2C \cdot (v_1 + C \cdot u_1),$		2**M** + 2**S**
	$uu_1'' \leftarrow u_1''^2, \quad uu_0'' \leftarrow u_1'' \cdot u_0'',$		1**M** + 1**S**
	$v_1'' \leftarrow D \cdot (u_1 - u_1'') + uu_1'' - uu_1 - u_0'' + u_0, \quad v_0'' \leftarrow D \cdot (u_0 - u_0'') + uu_0'' - uu_0,$		2**M**
	$v_1'' \leftarrow E \cdot v_1'' + v_1, \quad v_0'' \leftarrow E \cdot v_0'' + v_0.$		2**M**
Output:	$D'' = \rho([2]D) = (u_1'', u_0'', v_1'', v_0'', uu_1'' = u_1''^2, uu_0'' = u_1'' u_0'')$.	**Total**	**I** + 19**M** + 6**S**

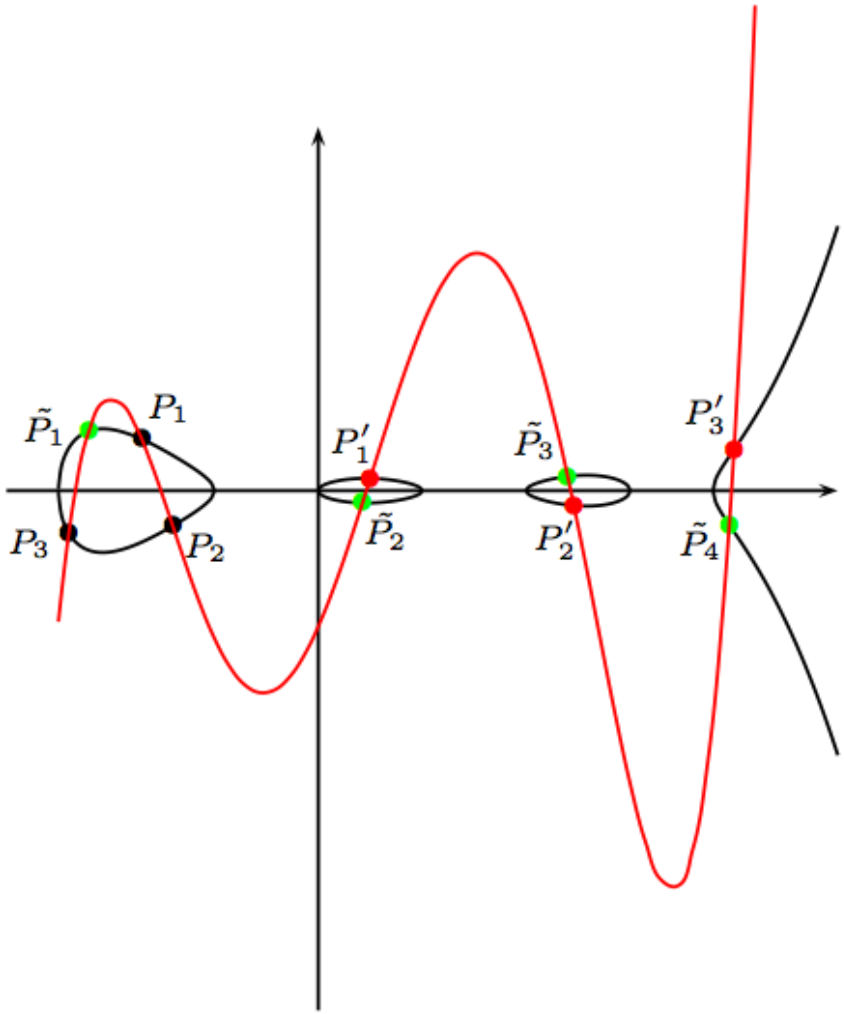
Table: Explicit formulas for a general doubling $D'' = [2]D$ of a degree 2 divisor on $\mathrm{Jac}(C_2)$.

Genus 2 explicit formulas: comparison

$\mathbb{F}_q$ inversions	Previous work	**General Jacobian addition**		**General Jacobian doubling**	
		$\mathbb{F}_q$ muls (**M**)	$\mathbb{F}_q$ sqrs (**S**)	$\mathbb{F}_q$ muls (**M**)	$\mathbb{F}_q$ sqrs (**S**)
2**I**	Harley	24	3	30	-
	Lange'01	24	3	24	6
	Matsuo *et al.*	25	-	27	-
1**I**	Takahashi	23	2	24	3
	Lange'05	22	3	22	5
	This work	**17**	**4**	**19**	**6**

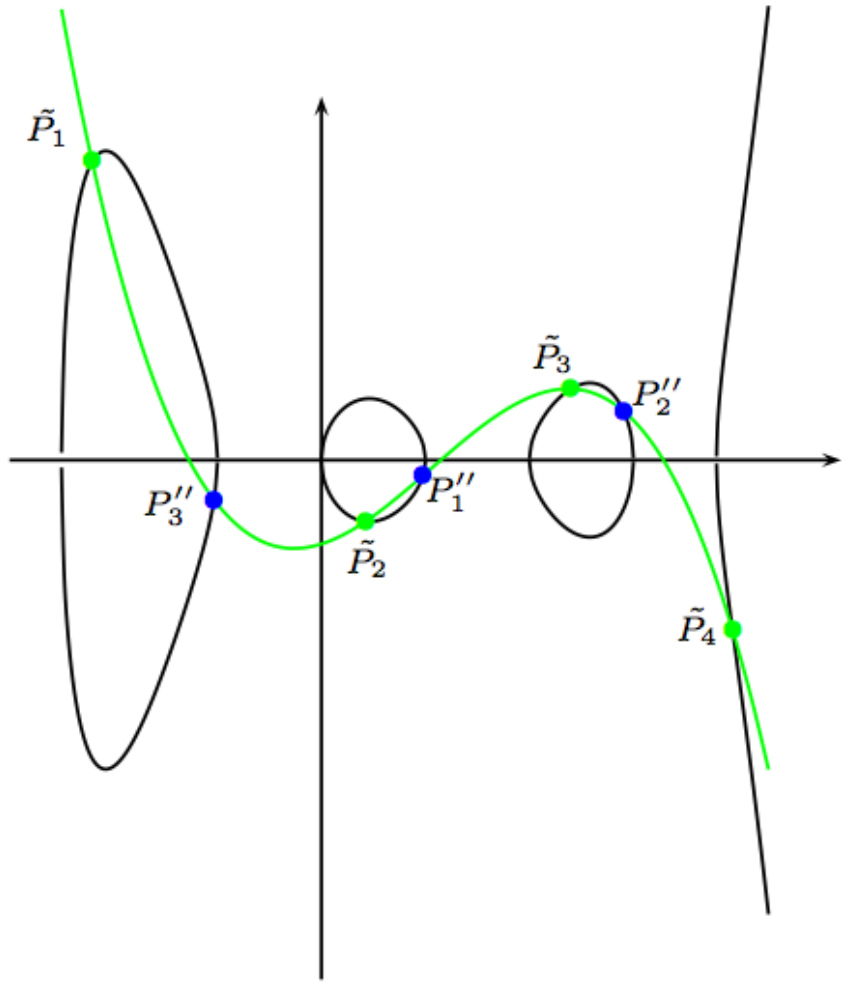
Table: Comparisons between geometrically inspired explicit formulas for genus 2 curves over prime fields and previous formulas based on Cantor's algorithm.

Genus 3 and beyond



More reduction required!!!

Genus 3 and beyond (cont...)



Corollary: In general, the number of rounds of reduction required to form the reduced divisor is $\lfloor \frac{g-1}{2} \rfloor$.

How best to solve the linear systems???

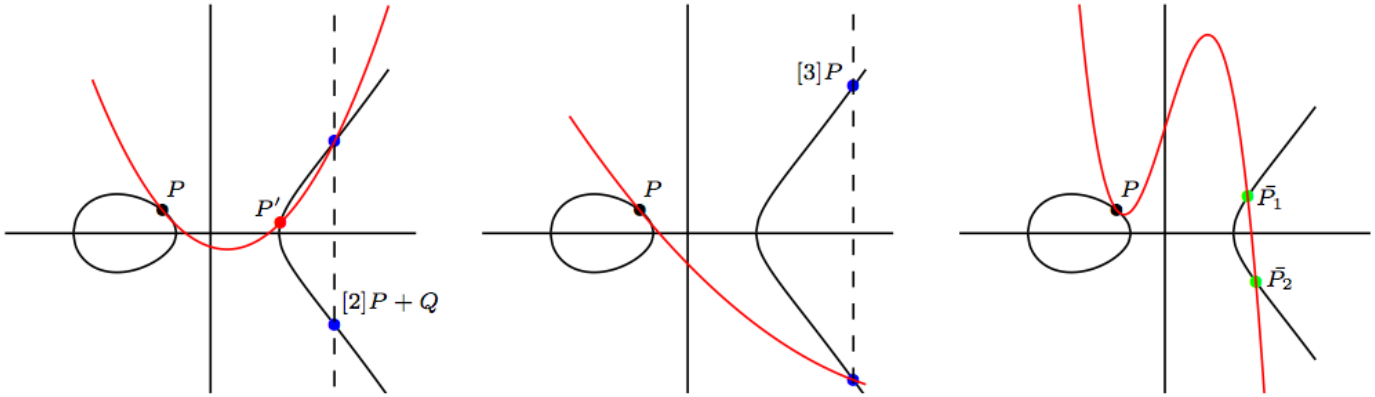
- If we were able to use (x, y) coordinates, the linear system would be a Vandermonde matrix ($V_{i,j} = a_i^{j-1}$).

$$V = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \dots & \alpha_m^{n-1} \end{bmatrix}$$

- In Mumford coordinates, the matrix turns out to be a sum of Vandermonde(ish) matrices...
- Current ponderings: can we do better than standard solving (inverting $\mathbb{F}_q^{g \times g}$)?

Back to genus 1

- Doing arithmetic by specifying zeros and poles is more general than just doublings and additions. Do whatever you like by just specifying zeros with multiplicities.



- $[2]P + Q$, $[3]P$, $[3]P + Q$, $[4]P$, ...
- Some done before, but by merging affine computations. Our method naturally recovers these formulas.
- E.g. second fastest tripling for ECC $3M + 10S$, second only to Doche-Icart-Kohel tripling oriented curves $6M + 6S$
- Double and add very useful in pairings (merged parabola saves computations)
- Fast quadrupling with x coordinate only ($X - Z$ only in projective space)

Simplied hyperelliptic pairing description

- General description carries polynomial representations right through...

Algorithm 3 Miller's algorithm (base 2)

INPUT: $S = \sum_{i=0}^{B} S_i 2^i$, d, $D_1 = [u_1, v_1]$, $D_2 = [u_2, v_2]$.
OUTPUT: Pairing value $f_{S,D_1}(\epsilon(D_2))^d$

1: $D \leftarrow [u_1, v_1]$
2: $f \leftarrow 1$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$, $f_3 \leftarrow 1$
3: **for** $i \leftarrow B-1$ **downto** 0 **do**
4: $\quad f_1 \leftarrow f_1^2 \bmod u_2$, $f_2 \leftarrow f_2^2 \bmod u_2$, $f_3 \leftarrow f_3^2$
5: $\quad D, [h_1, h_2, h_3] \leftarrow$ Miller Step(D, D, D_2)
6: $\quad f_1 \leftarrow f_1 \cdot h_1 \bmod u_2$, $f_2 \leftarrow f_2 \cdot h_2 \bmod u_2$, $f_3 \leftarrow f_3 \cdot h_3$
7: $\quad$ **if** $S_i = 1$ **then**
8: $\quad\quad D, [h_1, h_2, h_3] \leftarrow$ Miller Step(D, D_1, D_2)
9: $\quad\quad f_1 \leftarrow f_1 \cdot h_1 \bmod u_2$, $f_2 \leftarrow f_2 \cdot h_2 \bmod u_2$, $f_3 \leftarrow f_3 \cdot h_3$
10: $\quad$ **end if**
11: **end for**
12: $f \leftarrow \mathrm{Res}(u_2, f_1)/(f_3^{\deg(u_2)} \cdot \mathrm{Res}(u_2, f_2))$
13: **return** f^d

- Don't carry through elements of $\mathbb{F}_{q^k}(C_g)$ or $\mathbb{F}_q(C_g)$
- Interpolants naturally simplify description to be similar to genus 1
- New description bridges the gap between description and fast implementation

Future work...

- Merging computations in genus 2 and beyond (double-add, triple, quadruple, etc)
- Projective formulas, genus 3 explicit, characteristic 2, etc
- Real hyperelliptic curves (two points at infinity)
- Other curves not admitting standard Mumford representation (e.g. superelliptic) ??

Questions...?

Questions?...

comments?...

suggestions?...

ideas?...

corrections?....

complaints?...

counterexamples?.....