Arithmetic on Binary Genus 2 Curves Suitable for Small Devices

Tanja Lange

Department of Mathematics

Technical University of Denmark

t.lange@mat.dtu.dk

15.07.2005

Overview

- Arithmetic on hyperelliptic curves.
- Special case of characteristic two.
- Inversion-free coordinates.
- Compression.

Arithmetic on hyperelliptic curves

Hyperelliptic Curves

Affine equation of hyperelliptic curve of genus g (with $\mathbb{F}_q$-rational Weierstraß-point at infinity)

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

$h(x), f(x) \in \mathbb{F}_q[x]$, f monic, $\deg f = 2g + 1, \deg h \leq g$
non singular, i. e. not both partial derivatives

$$(2y + h(x) \text{ and } h'(x)y - f'(x))$$

vanish in any in $(a, b) \in C/\overline{\mathbb{F}_q}$

Examples

Concerning the arithmetic properties one can consider elliptic curves as hyperelliptic curves, i. e.

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$$

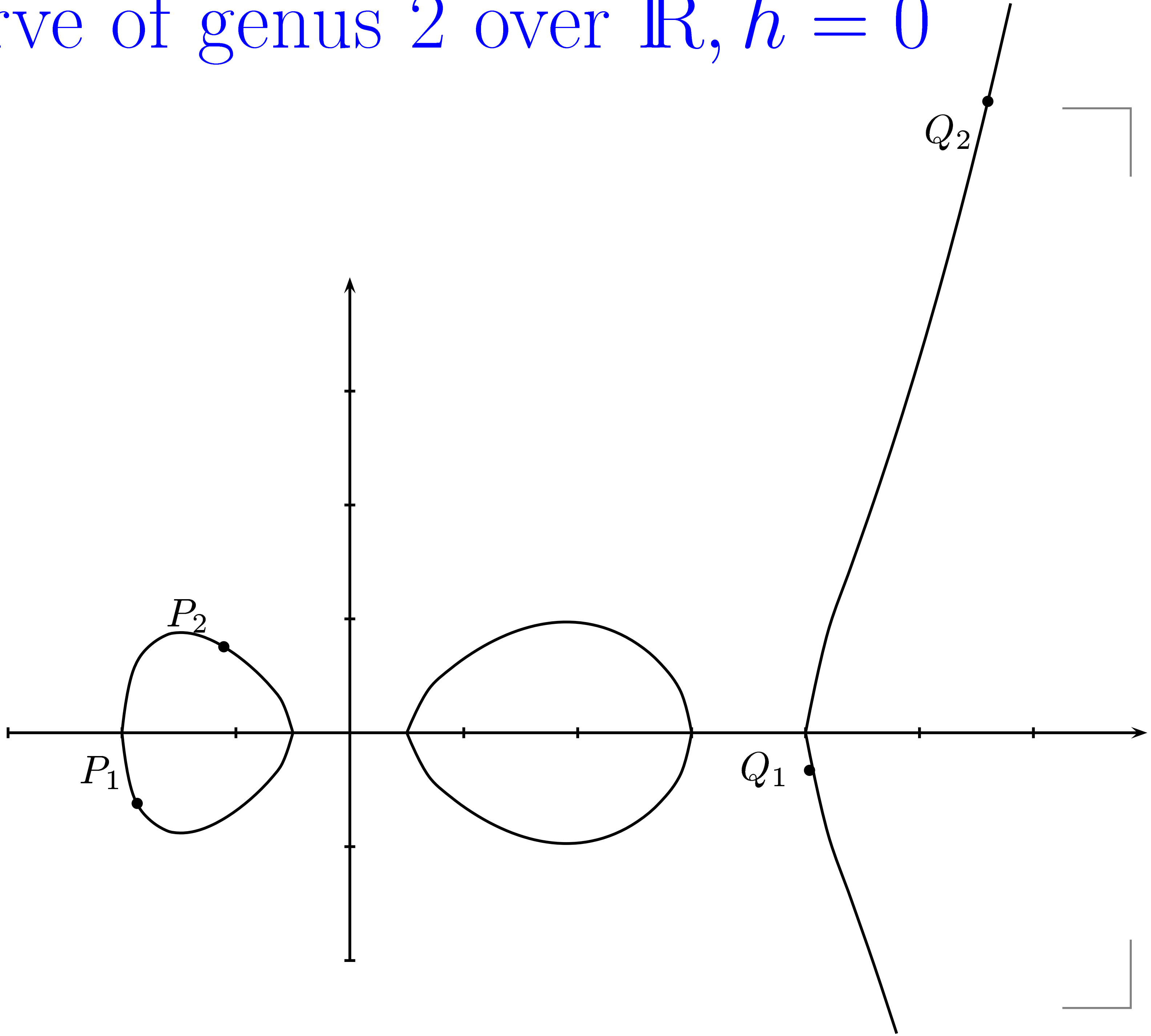
is considered as curve of genus one.

Curve of genus 2 over field of odd characteristic

$$y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

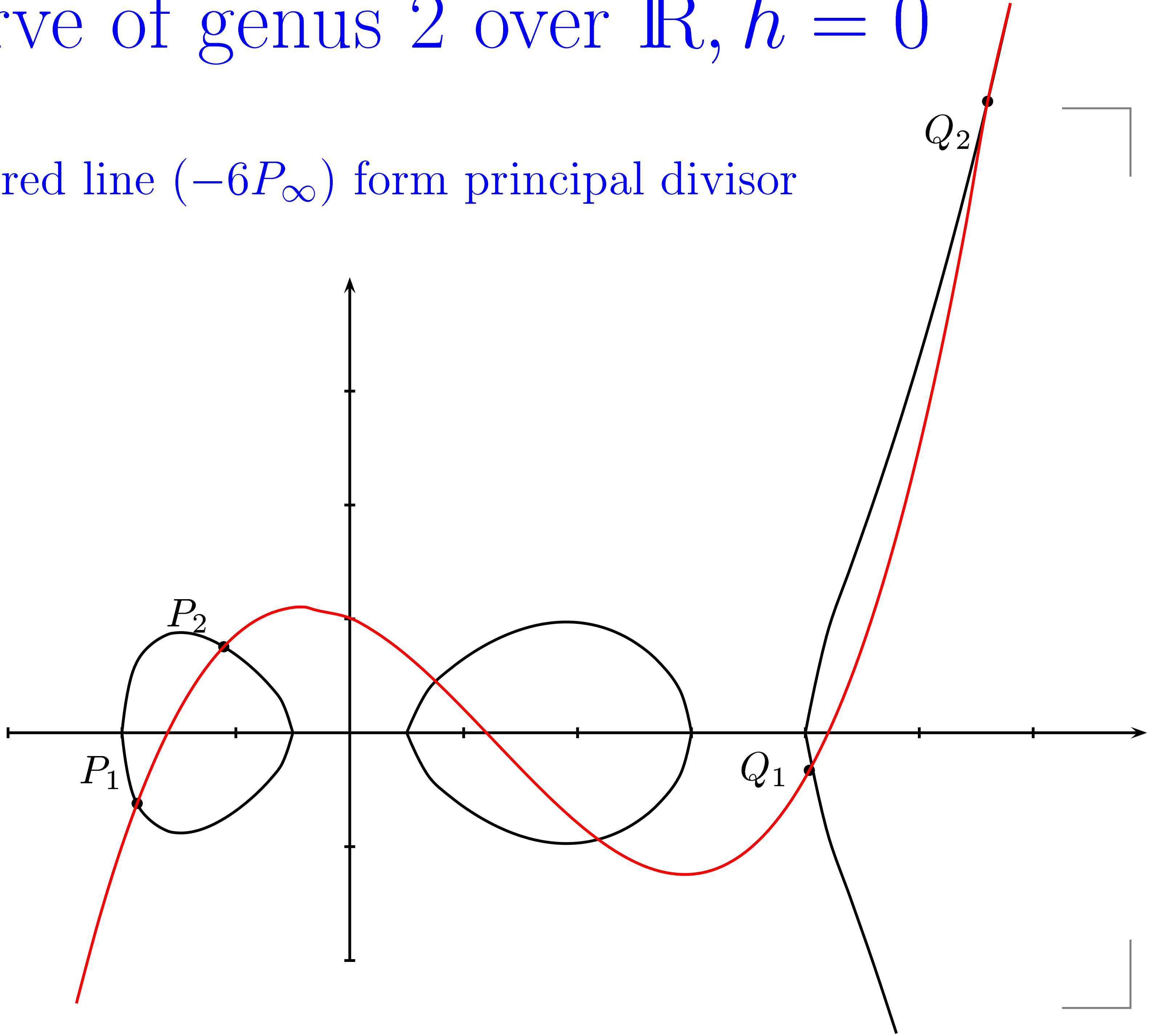
provided $f(x)$ has no multiple roots.

Curve of genus 2 over $\mathbb{R}$, $h = 0$



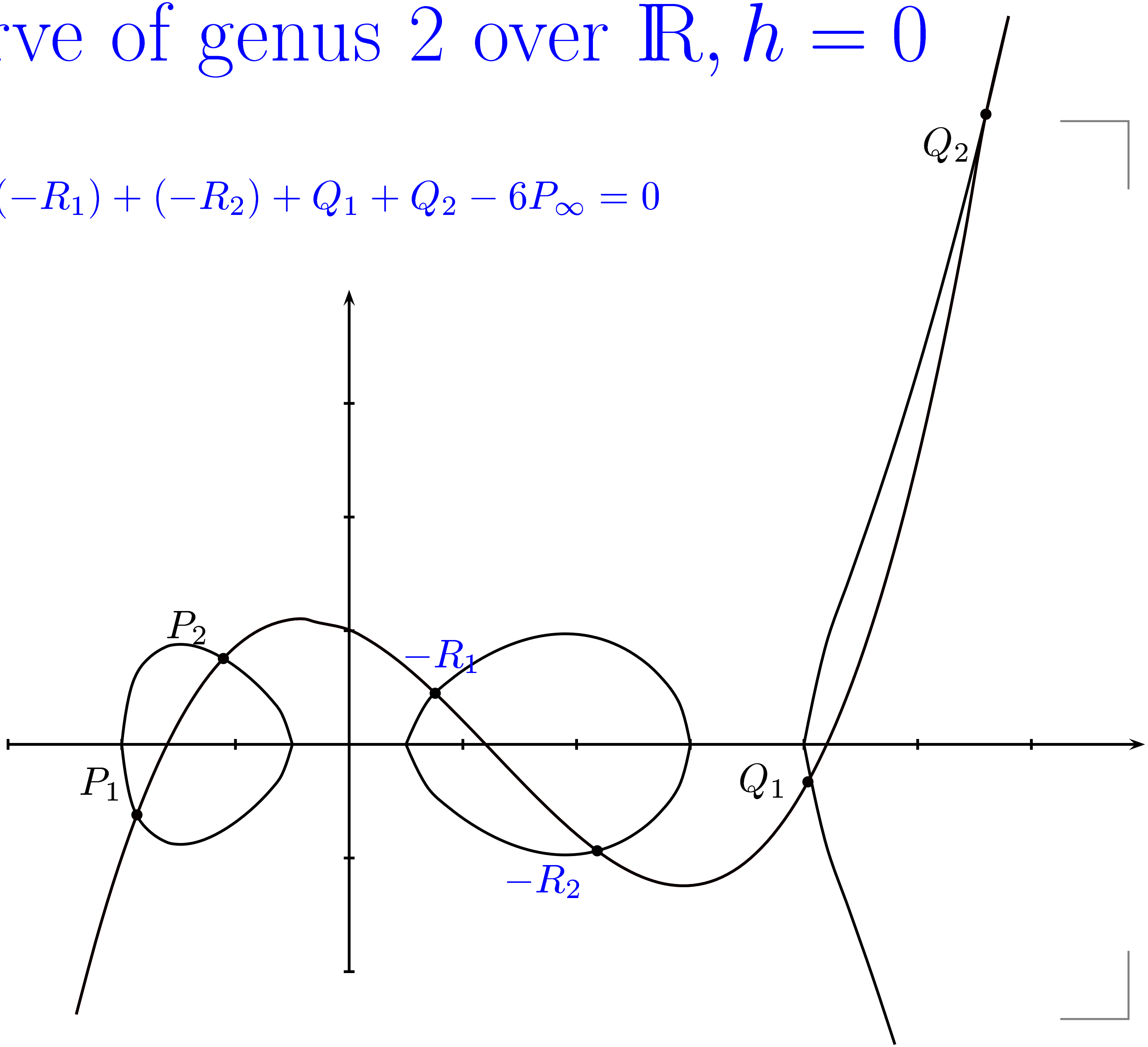
Curve of genus 2 over $\mathbb{R}$, $h = 0$

points on red line $(-6P_\infty)$ form principal divisor



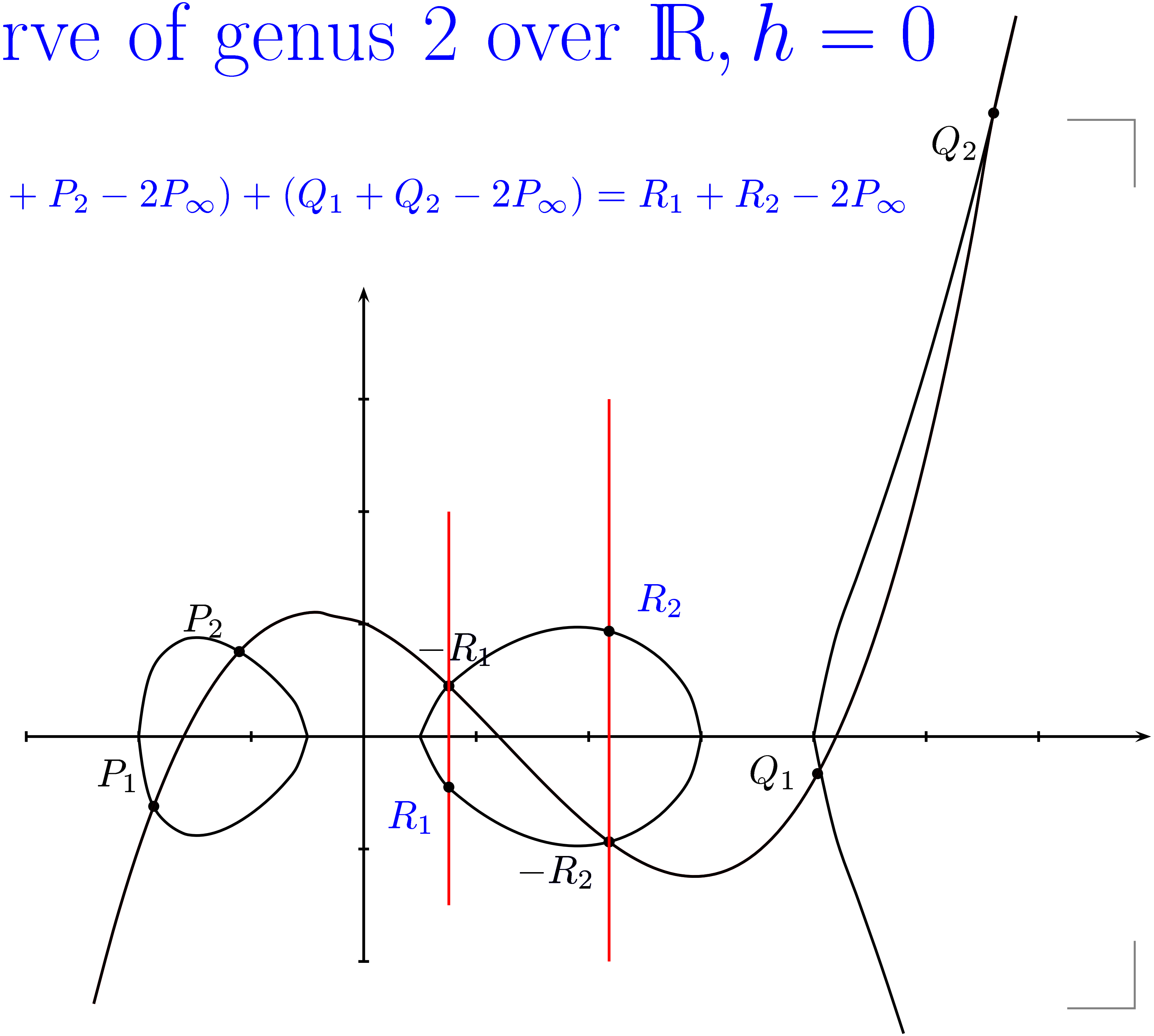
Curve of genus 2 over $\mathbb{R}$, $h = 0$

$P_1 + P_2 + (-R_1) + (-R_2) + Q_1 + Q_2 - 6P_\infty = 0$



Curve of genus 2 over $\mathbb{R}$, $h = 0$

$$(P_1 + P_2 - 2P_\infty) + (Q_1 + Q_2 - 2P_\infty) = R_1 + R_2 - 2P_\infty$$



Mumford Representation

Elements $D \in \mathbf{Cl}(C/\mathbb{F}_q)$ represented by two polynomials

$$D = [u(x), v(x)]; u, v \in \mathbb{F}_q[x],$$

u monic, $\deg v < \deg u \leq g, \quad u | v^2 + vh - f.$

$\Rightarrow$ compact representation.

Relation to points in support via

$$P_i = (x_i, y_i) \Leftrightarrow u(x_i) = 0, v(x_i) = y_i \text{ with multiplicity}$$

Arithmetic uses "only" arithmetic on polynomials ... but is far less efficient than on elliptic curves (if applied directly).

Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor/Koblitz)

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$
`OUT:` $D = [u, v]$ reduced with $D \sim D_1 + D_2$

1. compute $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$
3. let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
4. $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
5. let $u' = \frac{f - vh - v^2}{u} \quad b' = (-h - v) \bmod u'$
6. if $\deg u' > g$ put $u := u', v := v'$ goto step 5
7. make u monic

Explicit Arithmetic in $\mathbf{Cl}(C/\mathbb{F}_q)$

$$\left.\begin{array}{ll} 2000 & \text{Harley (odd char.)} \\ 2001 & \text{L. (arbitrary char.)} \\ 2001 & \text{Matsuo, Chao, Tsujii (faster)} \end{array}\right\} \Rightarrow 2 \text{ inversions}$$

$$\left.\begin{array}{ll} 2002 & \text{Miyamoto, Doi, Matsuo, Chao, Tsujii} \\ 2002 & \text{Takahashi} \\ 2002 & \text{L. (arbitrary char.)} \\ 2002 & \text{Sugizaki, Matsuo, Chao, Tsujii} \\ & \quad \text{(even char.)} \end{array}\right\} \Rightarrow 1 \text{ inv.}$$

General formulae lead to speeds comparable to ECC (Lange, Avanzi).

$$\left.\begin{array}{ll} 2004 & \text{L., Stevens} \end{array}\right\} \Rightarrow \begin{array}{l} \text{distinction of 3 different cases,} \\ \text{optimal affine doubling formulae for each.} \end{array}$$

General doubling, $g = 2$

Doubling, $\deg u = 2$			
Input	$[u, v], u = x^2 + u_1x + u_0, v = v_1x + v_0$		
Output	$[u', v'] = 2[u, v]$		

Step	Expression	odd	even
1	compute $\tilde{v} \equiv (h + 2v) \bmod u = \tilde{v}_1x + \tilde{v}_0$: $\tilde{v}_1 = h_1 + 2v_1 - h_2u_1$, $\tilde{v}_0 = h_0 + 2v_0 - h_2u_0$;		
2	compute resultant $r = \text{res}(\tilde{v}, u)$: $w_0 = v_1^2$, $w_1 = u_1^2$, $w_2 = \tilde{v}_1^2$, $w_3 = u_1\tilde{v}_1$, $r = u_0w_2 + \tilde{v}_0(\tilde{v}_0 - w_3)$;	2S, 3M $(w_2 = 4w_0)$	2S, 3M (see below)
3	compute almost inverse $inv' = inv r$: $inv'_1 = -\tilde{v}_1$, $inv'_0 = \tilde{v}_0 - w_3$;		
4	compute $k' = (f - hv - v^2)/u \bmod u = k'_1x + k'_0$: $w_3 = f_3 + w_1$, $w_4 = 2u_0$, $k'_1 = 2(w_1 - f_4u_1) + w_3 - w_4 - h_2v_1$; $k'_0 = u_1(2w_4 - w_3 + f_4u_1 + h_2v_1) + f_2 - w_0 - 2f_4u_0 - h_1v_1 - h_2v_0$;	1M	2M (see below)
5	compute $s' = k'inv' \bmod u$: $w_0 = k'_0inv'_0$, $w_1 = k'_1inv'_1$, $s'_1 = (inv'_0 + inv'_1)(k'_0 + k'_1) - w_0 - w_1(1 + u_1)$, $s'_0 = w_0 - u_0w_1$;	5M	5M
6	compute $s'' = x + s_0/s_1$ and s_1: $w_1 = 1/(rs'_1)(= 1/r^2s_1)$, $w_2 = rw_1(= 1/s'_1)$, $w_3 = {s'}_1^2w_1(= s_1)$; $w_4 = rw_2(= 1/s_1)$, $w_5 = w_4^2$, $s''_0 = s'_0w_2$;	I, 2S, 5M	I, 2S, 5M
7	compute $l' = s''u = x^3 + l'_2x^2 + l'_1x + l'_0$: $l'_2 = u_1 + s''_0$, $l'_1 = u_1s''_0 + u_0$, $l'_0 = u_0s''_0$;	2M	2M
8	compute $u' = s^2 + (h + 2v)s/u + (v^2 + hv - f)/u^2$: $u'_0 = {s''_0}^2 + w_4(h_2(s''_0 - u_1) + 2v_1 + h_1) + w_5(2u_1 - f_4)$, $u'_1 = 2s''_0 + h_2w_4 - w_5$;	S, 2M	S, M
9	compute $v' \equiv -h - (l + v) \bmod u' = v'_1x + v'_0$: $w_1 = l'_2 - u'_1$, $w_2 = u'_1w_1 + u'_0 - l'_1$, $v'_1 = w_2w_3 - v_1 - h_1 + h_2u'_1$; $w_2 = u'_0w_1 - l'_0$, $v'_0 = w_2w_3 - v_0 - h_0 + h_2u'_0$;	4M	4M
total			each I, 5S, 22M

Different Coordinates $g = 2$, odd q

affine $\mathcal{A}$:

$$D \sim [x^2 + u_1 x + u_0, v_1 x + v_0] \sim [u_1, u_0, v_1, v_0]$$

projective $\mathcal{P}$: Miyamoto, Doi, Matsuo, Chao, and Tsujii; L.; all 2002

$$D \sim [U_1, U_0, V_1, V_0, Z] \sim [U_1/Z, U_0/Z, V_1/Z, V_0/Z]$$

new $\mathcal{N}$: L. 2002, contains also mixed coordinates

$$D \sim [U_1, U_1, V_1, V_0, Z_1, Z_2] \sim [U_1/Z_1^2, U_0/Z_1^2, V_1/(Z_1^3 Z_2), V_0/(Z_1^3 Z_2)]$$

$\mathcal{P}$ and $\mathcal{N}$: no inversions

Comparison - odd characteristic

Doubling		Addition	
operation	costs	operation	costs
$2\mathcal{N} = \mathcal{P}$	7S, 38M	$\mathcal{N} + \mathcal{N} = \mathcal{P}$	7S, 51M
$2\mathcal{P} = \mathcal{P}$	6S, 38M	$\mathcal{N} + \mathcal{P} = \mathcal{P}$	4S, 51M
$2\mathcal{N} = \mathcal{N}$	7S, 34M	$\mathcal{N} + \mathcal{N} = \mathcal{N}$	7S, 47M
$2\mathcal{P} = \mathcal{N}$	6S, 34M	$\mathcal{N} + \mathcal{P} = \mathcal{N}$	4S, 48M
		$\mathcal{P} + \mathcal{P} = \mathcal{P}$	4S, 47M
		$\mathcal{P} + \mathcal{P} = \mathcal{N}$	4S, 44M
		$\mathcal{A} + \mathcal{N} = \mathcal{P}$	5S, 40M
		$\mathcal{A} + \mathcal{P} = \mathcal{P}$	3S, 40M
		$\mathcal{A} + \mathcal{N} = \mathcal{N}$	5S, 36M
		$\mathcal{A} + \mathcal{P} = \mathcal{N}$	3S, 37M
$2\mathcal{A} = \mathcal{A}$	1I, 5S, 22M	$\mathcal{A} + \mathcal{A} = \mathcal{A}$	1I, 3S, 22M

Implementations and Comparison

- software: for $\log_2 p \sim 40 - 60$ inversions cheap, use $\mathcal{A}$ for $g = 1, 2$.
  Comparison depends on I/M genus
  Paper by Roberto Avanzi (Bochum) at CHES '04, (tailored implementation for the small p used here) shows:

  small advantage of EC over $g = 2$, genus 3 too slow.

- hardware: usually expensive inversions, compute multiple of affine point via $2\mathcal{N} = \mathcal{N}, \mathcal{A} + \mathcal{N} = \mathcal{N}$, compute multiple of non-normalized point via $2\mathcal{N} = \mathcal{N}, \mathcal{N} + \mathcal{P} = \mathcal{N}$.
  - First implementation by Kim Nguyen at ECC'02
  - Many results at RUB, ... close to break even of ECC and $g = 2$.

Field of even characteristic

Joint work with Marc Stevens

Curves over $\mathbb{F}_{2^n}$

$$C : y^2 + (h_2x^2 + h_1x + h_0)y = f(x), \deg h \geq 1.$$

Above formulas hold for general equation. Get higher efficiency by specializing to type of h.

If $\deg h = 1$ the curve has 2-rank 1, which is a special property but does not weaken the system up to our present knowledge. For odd n one can make h monic.

If $\deg h = 2$ and h has a root then one can achieve $h(x) = x^2 + h_1x$, otherwise $h(x) = x^2 + h_1x + h_0$. In the former case the group order is divisible by 4, in the latter by 2.

Isomorphic transformations

Consider e. g. $\deg g = 1$:
$x \to x' + h_0/h_1,\ y \to y'$ gives

$$\begin{aligned} {y'}^2 + h_1(x' + \frac{h_0}{h_1})y' + h_0 y' &= (x' + \frac{h_0}{h_1})^5 + f_4(x' + \frac{h_0}{h_1})^4 + \cdots \\ {y'}^2 + h_1 x' y' &= {x'}^5 + \tilde{f}_4 {x'}^4 + \tilde{f}_3 {x'}^3 + \tilde{f}_2 {x'}^2 + \tilde{f}_1 x' + \tilde{f}_0. \end{aligned}$$

Changes of the form $y \to y' + a{x'}^2 + bx'$ allow $f_4 = f_1 0$ and some more.
If $\mathbb{F}_q = \mathbb{F}_{2^n}$ with n one can additionally achieve
$h_1 = 1, f_2 \in \mathbb{F}_2$.
Usual situation:

$$C : y^2 + h_1 xy = x^5 + f_3 x^3 + f_2 x^2 + f_0.$$

Doubling, $g = 2$, $\deg h = 1$

Doubling $\deg h = 1$, $\deg u = 2$	
Input	$[u, v], u = x^2 + u_1 x + u_0, v = v_1 x + v_0$; h_1^2, h_1^{-1}
Output	$[u', v'] = 2[u, v]$

Step	Expression	$h_1 = 1$	h_1^{-1} small	h_1 arbitrary
1	compute rs_1:	3S	3S	3S
	$z_0 = u_0^2$, $k_1' = u_1^2 + f_3$;			
	$w_0 = f_0 + v_0^2 (= rs_1'/h_1^3)$;			
2	compute $1/s_1$ and s_0'':	I, 2M	I, 2M	I, 2M
	$w_1 = (1/w_0) z_0 (= h_1/s_1)$;			
	$z_1 = k_1' w_1$, $s_0'' = z_1 + u_1$;			
3	compute u':	2S	S, 2M	S, 2M
	$w_2 = h_1^2 w_1$, $u_1' = w_2 w_1$;			
	$u_0' = s_0''^2 + w_2$;			
4	compute v':	S, 3M	S, 3M	S, 5M
	$w_3 = w_2 + k_1'$;			
	$v_1' = h_1^{-1}(w_3 z_1 + w_2 u_1' + f_2 + v_1^2)$;			
	$v_0' = h_1^{-1}(w_3 u_0' + f_1 + z_0)$;			
total		I, 6S, 5M	I, 5S, 7M	I, 5S, 9M

Results

Overview

	$h = X$	$h = h_1 X$, h_1^{-1} small	$h = h_1 X$	$h = X^2 + h_1 X$, h_1^{-1} small
f_4 small	I, 6S, 5M	I, 5S, 7M	I, 5S, 9M	I, 6S, 10M
f_4 not small	n. a.	n. a.	n. a.	I, 6S, 12M

	$h = X^2 + h_1 X$	$h = X^2 + h_1 X + h_0$	all
f_4 small	I,5S, 15M	I, 6S, 21M	I, 5S, 22M
f_4 not small	I, 5S, 17M	n. a.	n. a.

Inversion-free coordinates

Inversion Free Coordinates – $h = x$

$\mathcal{P}$: projective $u_i = U_i/Z, v_i = V_i/Z$,

$\mathcal{N}$: new $u_i = U_i/Z_1^2, v_i = V_i/Z_1^3 Z_2$

$\mathcal{R}$: recent $u_i = U_i/Z, v_i = V_i/Z^2$

Doubling		Addition	
Operation	Costs	Operation	Costs
$2\mathcal{N} = \mathcal{N}$	$28\text{M} + 5\text{S}$	$\mathcal{R} + \mathcal{R} = \mathcal{R}$	$49\text{M} + 8\text{S}$
$2\mathcal{P} = \mathcal{P}$	$22\text{M} + 6\text{S}$	$\mathcal{P} + \mathcal{P} = \mathcal{P}$	$49\text{M} + 4\text{S}$
$2\mathcal{R} = \mathcal{R}$	$20\text{M} + 8\text{S}$	$\mathcal{N} + \mathcal{N} = \mathcal{N}$	$42\text{M} + 6\text{S}$
—	—	$\mathcal{A} + \mathcal{R} = \mathcal{R}$	$42\text{M} + 7\text{S}$
—	—	$\mathcal{A} + \mathcal{P} = \mathcal{P}$	$39\text{M} + 4\text{S}$
—	—	$\mathcal{A} + \mathcal{N} = \mathcal{N}$	$36\text{M} + 6\text{S}$
$2\mathcal{A} = \mathcal{A}$	$\text{I} + 5\text{M} + 6\text{S}$	$\mathcal{A} + \mathcal{A} = \mathcal{A}$	$\text{I} + 21\text{M} + 3\text{S}$

Before best result: $2\mathcal{N} = \mathcal{N}$, 6S, 35M for $\deg h = 1$.

Compression

Small storage

For ECC:
store (x, y) by x and a bit to find right choice of y in $y^2 = f(x)$.

For HECC:
first idea (Hess, Seroussi, Smart):
use correspondence of $[u, v]$ to points on C and idea from ECC
$\Rightarrow$ requires work in extension fields.

Nice idea (Colin Stahlke, odd characteristic):
use resultants and work in field of definition.

This work:
generalization to even characteristic,
works only for special case (as far as I know ...).

The End

The END

Thanks!