

# Hyperelliptic Curves

Peter Birkner

Technische Universiteit Eindhoven

DIAMANT Summer School on Elliptic and  
Hyperelliptic Curve Cryptography

18 September 2008

# Hyperelliptic curves

## Definition

Let  $K$  be a field and  $\bar{K}$  an algebraic closure of  $K$ . An (imaginary) hyperelliptic curve  $C$  of genus  $g$  over  $K$  can be given by an equation of the form

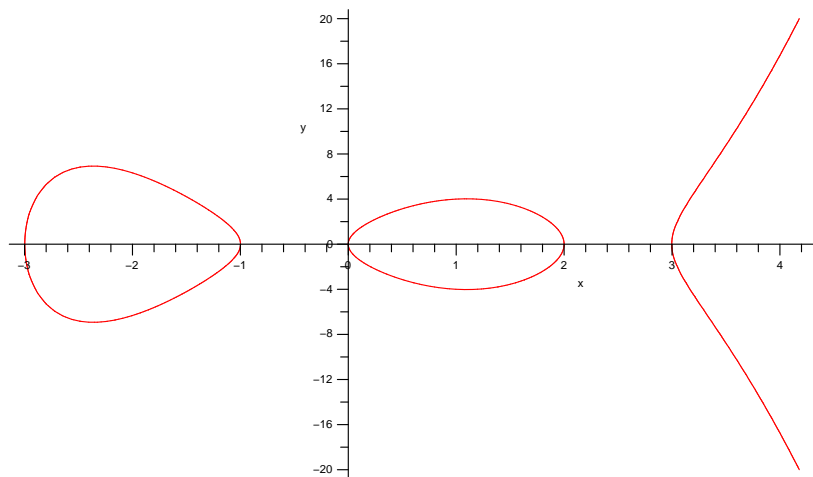
$$C : y^2 + h(x)y = f(x),$$

where

- $h \in K[x]$  is a polynomial of degree at most  $g$ ,
- $f \in K[x]$  is a monic polynomial of degree  $2g + 1$ ,
- no point on  $C$  over  $\bar{K}$  satisfies both partial derivatives  $2y + h = 0$  and  $h'y - f' = 0$ .

## Example: A hyperelliptic curve over the reals

$$C : y^2 = x^5 - x^4 - 11x^3 + 9x^2 + 18x \text{ over } \mathbb{R}$$
$$= x(x-2)(x-3)(x+1)(x+3)$$



# Divisors

## Definition

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ .

- ① A **divisor  $D$  on  $C$**  is a formal sum of points on  $C$ :

$$D = \sum_{P \in C(\overline{K})} n_P P \quad (n_P \in \mathbb{Z}, n_P = 0 \text{ for almost all } P \in C(\overline{K}))$$

- ② The **degree of the divisor  $D$  on  $C$**  is

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

The group of **degree-0 divisors on  $C$**  is denoted by  $\text{Div}_C^0(\overline{K})$ .

**Example:**  $D = 2P_1 + 3P_2$ ,  $\deg(D) = 2 + 3 = 5$

# The function field of a hyperelliptic curve

## Definition

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ .

- The **coordinate ring of  $C$  over  $K$**  is the quotient ring

$$K[C] = K[x,y]/(y^2+h(x)y-f(x)).$$

Similarly, the coordinate ring of  $C$  over  $\bar{K}$  is

$$\bar{K}[C] = \bar{K}[x,y]/(y^2+h(x)y-f(x)).$$

An element of  $\bar{K}[C]$  is called a **polynomial function on  $C$** .

- The **function field  $\bar{K}(C)$  of  $C$  over  $\bar{K}$**  is the field of fractions of  $\bar{K}[C]$ . The elements of  $\bar{K}(C)$  are called **rational functions on  $C$** .

# Uniformising parameter

## Definition

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$  and let  $P \in C(\overline{K})$ . A rational function  $u \in \overline{K}(C)$  with  $u(P) = 0$  is called a **uniformising parameter for  $P$** , if the following property holds:

For each  $0 \neq a \in \overline{K}[C]$  there exists an integer  $d$  and a function  $s \in \overline{K}(C)$  such that  $a = u^d s$  and  $s(P) \notin \{\infty, 0\}$ .

## Theorem

For each  $P \in C(\overline{K})$  there exists an uniformising parameter for  $P$ .

# Order of a rational function

## Definition

- ① Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ . Let  $P \in C(\overline{K})$  with uniformising parameter  $u \in \overline{K}(C)$  and let  $0 \neq a \in \overline{K}[C]$  be a **polynomial function on  $C$** . Now,  $a$  can be written as

$$a = u^d s.$$

The (unique) integer  $d$  is called the **order of  $a$  at  $P$** .

- ② Let  $r = a/b \in \overline{K}(C)^*$  be a **rational function** on  $C$  and  $P \in C(\overline{K})$ . The **order of  $r$  at  $P$**  is defined as

$$\text{ord}_P(r) = \text{ord}_P(a) - \text{ord}_P(b).$$

# Principal divisors

## Definition

Let  $r \in \overline{K}(C)^*$  be a rational function on  $C$ . The **divisor of  $r$**  is

$$\operatorname{div}(r) = \sum_{P \in C(\overline{K})} (\operatorname{ord}_P(r))P.$$

## Definition

A divisor  $D$  is called **principal** if  $D = \operatorname{div}(r)$  for some rational function  $r \in \overline{K}(C)^*$ . The set of principal divisors on  $C$  is denoted by **Princ**( $C$ ).

A principal divisor has degree 0. Hence, **Princ**( $C$ ) is a subgroup of  $\operatorname{Div}_C^0(\overline{K})$ .

# The divisor class group

## Definition

The **divisor class group of  $C$**  is the quotient group

$$\text{Pic}_C^0(\overline{K}) = \text{Div}_C^0(\overline{K}) / \text{Princ}(C).$$

It is also called the **Picard group of  $C$** . The elements of  $\text{Pic}_C^0(\overline{K})$  are called divisor classes of  $C$ .

Since our curves have only one point at infinity, the divisor class group is isomorphic to the **ideal class group of  $C$** .

# Mumford representation (part 1)

## Theorem (Mumford)

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ . Each nontrivial divisor class of  $C$  over  $K$  can be represented by a **unique pair of polynomials**  $u, v \in K[x]$ , where

- 1  $u$  is monic,
- 2  $\deg v < \deg u \leq g$ ,
- 3  $u \mid v^2 + vh - f$ .

In the genus-2 case each divisor class can be represented by the 4 coefficients  $u_1, u_0, v_1, v_0$  of the polynomials  $u$  and  $v$ .

## Mumford representation (part 2)

### Example

- We consider the hyperelliptic curve with equation  $C : y^2 = x^5 + 3x^3 + 2x^2 + 3$  over  $\mathbb{F}_5$ .
- Some points on the curve:  $P_1 = (3, 0)$ ,  $P_2 = (1, 2)$ ,  $P_3 = (4, 1)$ ,  $P_4 = (3, 0)$ .
- We define the divisors  $D_1 = P_1 + P_2 - 2P_\infty$  and  $D_2 = P_3 + P_4 - 2P_\infty$ .
- In Mumford form:  $D_1 = [x^2 + x + 3, 4x + 3]$  and  $D_2 = [x^2 + 3x + 2, x + 2]$ .
- $x$ -coordinates of the points are the zeros of the first Polynomial. Evaluating the second polynomial at the  $x$ -coordinate gives the  $y$ -coordinate of the points of the divisor.

# Cantor's algorithm (part 1)

---

**Algorithm 14.7** Cantor's algorithm

---

INPUT: Two divisor classes  $\bar{D}_1 = [u_1, v_1]$  and  $\bar{D}_2 = [u_2, v_2]$  on the curve  $C : y^2 + h(x)y = f(x)$ .

OUTPUT: The unique reduced divisor  $D$  such that  $\bar{D} = \bar{D}_1 \oplus \bar{D}_2$ .

---

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

## Cantor's algorithm (part 2)

### Example

Consider the hyperelliptic curve  $C$  over  $\mathbb{F}_{11}$  with equation

$$C : y^2 = x^5 + 3x^3 + 7x^2 + x + 2$$

and 2 divisors  $D_1 = [x^2 + 7x + 10, x + 9]$  and  $D_2 = [x^2 + 10, 7x + 9]$ .

- In Steps 1-3:  $d_1 = d = 1$ .
- Step 4:  $u := u_1 u_2 = x^4 + 7x^3 + 9x^2 + 4x + 1$  and  $v := (s_1 u_1 v_2 + s_2 u_2 v_1) \bmod u = 4x^2 + 7x + 5$  (Not yet reduced!)
- Steps 5-7:  $u' := (f - v^2)/u = x + 10$ ,  $v' := -v \bmod u' = 6$

We have  $D_1 + D_2 = [x + 10, 6]$  in Mumford representation.

## How efficient is Cantor's algorithm?

- Cantor's algorithm is completely general and holds for any field and any genus.
- Let's consider special cases to improve the speed of Cantor, e.g. fix the characteristic of the field, the genus of the curve etc.
- For different forms of the curve equations we have different speeds for Cantor, e.g. treat different degrees of  $h(x)$  separately.
- **Result:** For some special cases we get explicit addition and doubling formulas which are very efficient.

# Doubling for genus 2 and arbitrary characteristic

<b>Doubling, deg <math>u = 2</math></b>			
Input Output	$[u, v], u = x^2 + u_1x + u_0, v = v_1x + v_0$ $[u', v'] = 2[u, v]$		
Step	Expression	odd	even
1	compute $\bar{v} \equiv (h + 2v) \bmod u = \bar{v}_1x + \bar{v}_0$ ; $\bar{v}_1 = h_1 + 2v_1 - h_2u_1, \bar{v}_0 = h_0 + 2v_0 - h_2u_0$ ;		
2	compute resultant $r = \text{res}(\bar{v}, u)$ ; $w_0 = v_1^2, w_1 = u_1^2, w_2 = \bar{v}_1^2, w_3 = u_1\bar{v}_1, r = u_0w_2 + \bar{v}_0(\bar{v}_0 - w_3)$ ;	2S, 3M ( $w_2 = 4w_0$ )	2S, 3M (see below)
3	compute almost inverse $inv' = invr$ ; $inv'_1 = -\bar{v}_1, inv'_0 = \bar{v}_0 - w_3$ ;		
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 $s_1$ ; $w_1 = 1/(rs'_1) (= 1/r^2s_1), w_2 = rw_1 (= 1/s'_1), w_3 = s_1^2w_1 (= s_1)$ ; $w_4 = rw_2 (= 1/s_1), w_5 = w_4, s''_0 = s'_0w_2$ ;	1, 2S, 5M	1, 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 $v' \equiv -h - (l + v) \bmod u' = v'_1x + v'_0$ ; $w_1 = l'_2 - u'_1, w_2 = u'_1w_1 + u'_0 - l'_1, v'_1 = w_2w_3 - v_1 - h_1 + h_2u'_1$ ; $w_2 = u_0^2w_1 - l'_0, v'_0 = w_2w_3 - v_0 - h_0 + h_2u'_0$ ;	4M	4M
<b>total</b>		<b>each 1, 5S, 22M</b>	

(T. Lange: Formulae for Arithmetic on Genus 2 Hyperelliptic Curves, 2004)

# Doubling for genus 2 and characteristic 2

<b>Doubling</b> $\deg h = 1, \deg u = 2$				
Input	$[u, v], u = x^2 + u_1x + u_0, v = v_1x + v_0; h_1^2, h_1^{-1}$			
Output	$[u', v'] = 2[u, v]$			
Step	Expression	$h_1 = 1$	$h_1^{-1}$ small	$h_1$ arbitrary
1	compute $rs_1$ : $z_0 = u_0^2, k'_1 = u_1^2 + f_3$ ; $w_0 = f_0 + v_0^2 (= rs_1'/h_1^3)$ ;	3S	3S	3S
2	compute $1/s_1$ and $s_0''$ : $w_1 = (1/w_0)z_0 (= h_1/s_1)$ ; $z_1 = k'_1 w_1, s_0'' = z_1 + u_1$ ;	I, 2M	I, 2M	I, 2M
3	compute $u'$ : $w_2 = h_1^2 w_1, u'_1 = w_2 w_1$ ; $u'_0 = s_0''^2 + w_2$ ;	2S	S, 2M	S, 2M
4	compute $v'$ : $w_3 = w_2 + k'_1$ ; $v'_1 = h_1^{-1}(w_3 z_1 + w_2 u'_1 + f_2 + v_1^2)$ ; $v'_0 = h_1^{-1}(w_3 u'_0 + f_1 + z_0)$ ;	S, 3M	S, 3M	S, 5M
total		<b>I, 6S, 5M</b>	I, 5S, 7M	I, 5S, 9M

(Lange and Stevens: Efficient Doubling on Genus Two Curves over Binary Fields, 2005)

## Inversion-free doubling (1)

Inversion is expensive compared to multiplication (e. g. in hardware applications). Can we avoid inversions?

- **Affine** coordinates: A divisor class is given by the coefficients of  $u$  and  $v$ :  $[u_1, u_0, v_1, v_0]$
- **Projective** coordinates: Use  $[U_1, U_0, V_1, V_0, Z]$  with  $u_i = U_i/Z$  and  $v_i = V_i/Z$
- **New** coordinates:  $[U_1, U_0, V_1, V_0, Z_1, Z_2, z_1, z_2, z_3, z_4]$  with  $u_i = U_i/Z_1^2, v_i = V_i/Z_1^3 Z_2$  and precomputations  $z_1, z_2, z_3, z_4$
- **Recent** coordinates:  $[U_1, U_0, V_1, V_0, Z, z]$  with  $u_i = U_i/Z$  and  $v_i = V_i/Z^2$  and the precomputation  $z = Z^2$

Inversion-free doubling can be achieved in Recent, New and Projective coordinates!

## Inversion-free doubling (2)

Divisor class doubling in Recent coordinates **without inversions!**

**Setting:** Genus-2 curve over binary field and  $\deg(h) = 1$ .

Input:	$\bar{D} = [U_1, U_0, V_1, V_0, Z, z]$ , precomputed values $h_1^2$ and $h_1^{-1}$	
Output	$[U'_1, U'_0, V'_1, V'_0, Z', z'] = 2[U_1, U_0, V_1, V_0, Z, z]$	
Step	Expression	Complexity
1	Precomputations $Z_4 \leftarrow z^2, y_0 \leftarrow U_0^2, t_1 \leftarrow U_1^2 + f_3 z, w_0 \leftarrow Z_4 f_0 + V_0^2,$ $\bar{Z} \leftarrow z w_0, w_1 \leftarrow y_0 Z_4, y_1 \leftarrow t_1 y_0 z, s_0 \leftarrow y_1 + U_1 w_0 Z$ $w_2 \leftarrow h_1^2 w_1, w_3 \leftarrow w_2 + t_1 w_0$	10M + 4S
2	Compute $U'$ $U'_1 \leftarrow w_2 w_1, w_2 \leftarrow w_2 \bar{Z}, U'_0 \leftarrow s_0^2 + w_2$	2M + S
3	Compute $V'$ $Z' \leftarrow \bar{Z}^2, V'_1 \leftarrow h_1^{-1} (w_2 U'_1 + (w_3 y_1 + f_2 Z' + (V_1 w_0)^2) Z')$ $V'_0 \leftarrow h_1^{-1} (\bar{Z} (w_3 U'_0 + y_0 w_0 Z')), z' \leftarrow Z'^2$	11M + 3S
<b>Total</b>		<b>23M + 8S</b>

If  $h_1 = 1$ , one can even achieve  $20M + 8S$ .

## Inversion-free coordinates — Overview

In the genus-2 case with  $h(x) = x$  over a binary field, we have the following complexities for addition and doubling:

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

## The torsion subgroup in char 2 (part 1)

- The curve equation is  $C : y^2 + h(x)y = f(x)$ , where  $h(x) \neq 0$  to avoid singularities.
- Let's look at the 2-torsion subgroup of the divisor class group of a genus-2 curve.
- How many divisor classes of order 2 do we have in  $\text{Div}_C^0(\mathbb{F}_{2^k})$ ?
- For a divisor class  $\bar{D} = [u, v]$  with order 2 we have that  $[2]\bar{D} = [1, 0]$ , which is equivalent to

$$[u, v] = \bar{D} = -\bar{D} = [u, -v - h] = [u, v + h].$$

## The torsion subgroup in char 2 (part 2)

- 1  $\deg(h) = 0$  and  $h(x) \neq 0$ , so  $h(x) = c$  for some constant  $c$ , i.e. there is no such divisor and the 2-torsion subgroup is **trivial** (supersingular curves).
- 2  $\deg(h) = 1$ , i.e.  $h$  has one root. Hence  $[u, v] = [u, v + h]$  for a point on the curve, and we have one divisor class with order 2 and  $[1, 0]$ . Thus  $\text{Div}_C^0(\mathbb{F}_{2^k})[2] \cong \mathbb{Z}/2$ .
- 3  $\deg(h) = 2$ , i.e.  $h$  has two zeros  $x_1$  and  $x_2$ , which leads to 3 divisor classes of order 2:  $\bar{D}_1 = [x - x_1, v_1]$ ,  $\bar{D}_2 = [x - x_2, v_2]$  and  $\bar{D}_1 + \bar{D}_2 = [(x - x_1)(x - x_2), v_3]$ . Hence we have  $\text{Div}_C^0(\mathbb{F}_{2^k})[2] \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ .

**Result:** In characteristic 2, the structure of the 2-torsion subgroup depends on the degree of the polynomial  $h$  in the curve equation.

## The torsion subgroup in char $\neq 2$ ? (part 1)

- In characteristic  $\neq 2$  the curve equation can be simplified to  $C : y^2 = f(x)$ .
- How does the 2-torsion subgroup look like in this case?
- Let's first find points of order 2, i.e. points with  $y$ -coordinate equals 0.
- Then let's find zeros of  $f(x)$ . Are there any over the ground field?
- Next we construct divisors of order 2 from the points of order 2.

## The torsion subgroup in char $p \neq 2$ ? (part 2)

Curve equation:  $C : y^2 = f(x)$

How many divisors of order 2 do we have in the genus-2 case?

### Example 1

- Let's assume  $f(x)$  splits into **one linear factor  $x - x_0$  and one factor of degree 4**, i.e.  $P = (x_0, 0)$  is a point with  $y$ -coordinate 0. And it's the only one!
- Hence, the divisor  $\bar{D} = [x - x_0, 0]$  is a divisor of order 2, because in Cantor's algorithm  $2\bar{D}$  becomes  $[1, 0]$ .
- The 2-torsion subgroup is isomorphic to  $\mathbb{Z}/2$ .

## The torsion subgroup in char $p \neq 2$ ? (part 3)

Curve equation:  $C : y^2 = f(x)$

### Example 2

- Let's assume  $f(x)$  splits into **two linear factors**  $x - x_0, x - x_1$  and **one factor of degree 3**, i.e.  $P_1 = (x_0, 0)$  and  $P_2 = (x_1, 0)$  are points with  $y$ -coordinate 0.
- Hence, the divisors  $\bar{D}_1 = [x - x_0, 0]$  and  $\bar{D}_2 = [x - x_1, 0]$  are divisors of order 2, and  $\bar{D}_1 + \bar{D}_2$  is a divisor of order 2.
- Thus the 2-torsion subgroup is isomorphic to  $\mathbb{Z}/2 \times \mathbb{Z}/2$ .

Thank you for your attention!