Efficient arithmetic on hyperelliptic curves over finite fields

Tanja Lange

Department of Mathematics

Technical University of Denmark

t.lange@mat.dtu.dk

15.08.2006

Overview

- Arithmetic on hyperelliptic curves
- Fast arithmetic for curves over odd characteristic fields.
- Fast arithmetic for curves over even characteristic fields.

Hyperelliptic curves – reminder

$\mathbb{F}_q$ is some finite field with q element. For background check talk this morning.

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. in no point $(a, b) \in C/\overline{\mathbb{F}_q}$ over the algebraic closure $\overline{\mathbb{F}_q}$ we have both partial derivatives vanishing, i.e.

$2b + h(a) = 0$ and $h'(a)b - f'(a) = 0$.

Otherwise (a, b) is called a singular point.

Mumford Representation

Group elements (divisor classes) $\bar{D}$ represented by two polynomials

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

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

$\Rightarrow$ compact representation over ground field.

Arithmetic in general case can be stated in these representatives and thus uses polynomial arithmetic.

For relations between this representation and divisors given as sums of points see my talk this morning.

Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor/Koblitz)

`IN:` $\bar{D}_1 = [u_1, v_1], \bar{D}_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$
`OUT:` $\bar{D} = [u, v]$ reduced with $\bar{D} = \bar{D}_1 \oplus \bar{D}_2$

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. $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$

This result $[u, v]$ corresponds to a semireduced divisor in the resulting divisor class.

Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor/Koblitz)

`IN:` $\bar{D}_1 = [u_1, v_1], \bar{D}_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$
`OUT:` $\bar{D} = [u, v]$ reduced with $\bar{D} = \bar{D}_1 \oplus \bar{D}_2$

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

This result $[u, v]$ corresponds to a reduced divisor.

Hyperelliptic curves in cryptography

- Group order is $\sim q^g$ for curve of genus g over $\mathbb{F}_q$.
- Same group size for smaller fields with increasing genus, e.g.
  - $g = 1, q \sim 2^{256}$ like in Dan Bernstein's talk,
  - corresponding to $g = 2, q \sim 2^{128}$,
  - corresponding to $g = 3, q \sim 2^{85}$ (Claus Diem starts having bad feelings).

  For larger genera $g \geq 4$ index calculus attacks have smaller complexity than $O(q^{g/2})$ (cf. talk by Claus Diem)
- Dan Bernstein presented fast arithmetic for elliptic curves; we do the same for genus 2 and give references for $g = 3$.

Explicit Arithmetic for $g = 2$

2000	Harley (odd char.)	$\Rightarrow$ 2 inversions
2001	L. (arbitrary char.)	
2001	Matsuo, Chao, Tsujii (faster)	
2002	Miyamoto, Doi, Matsuo, Chao, Tsujii	$\Rightarrow$ 1 inv.
2002	Takahashi	
2002	L. (arbitrary char.)	
2002	Sugizaki, Matsuo, Chao, Tsujii (even char.)	
2004	L., Stevens (even char.)	$\Rightarrow$ distinction of 3 different cases, optimal affine doubling formulae for each

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 $r =$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 $inv' = invr$: $inv'_1 = -\tilde{v}_1, inv'_0 = \tilde{v}_0 - w_3$;		
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: $w_1 = 1/(rs'_1)(= 1/r^2s_1), w_2 = rw_1(= 1/s'_1), w_3 = s'^2_1w_1(= s_1)$; $w_4 = rw_2(= 1/s_1), w_5 = w_4^2, s''_0 = s'_0w_2$;	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 $u' = s^2 + (h + 2v)s/u + (v^2 + hv - f)/u^2$: $u'_0 = s''^2_0 + w_4(h_2(s''_0 - u_1) + 2v_1 + h_1) + w_5(2u_1 - f_4), u'_1 = 2s''_0 + h_2w_4 - w_5$;	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, 22M, 5S

Elliptic curves vs. $g = 2$

- Doubling on elliptic curve needs $1I_q, 2M_q, 2S_q$.
- Doubling on genus 2 curve needs $1I_{q'}, 22M_{q'}, 5S_{q'}$.
- $\log q \sim 2 \log q'$ – naive field arithmetic $M_q = 4M_{q'}$ and $M = S \Rightarrow$ comparison depends on $1I_q <=> 1I_{q'} + 11M_{q'}$ (and on whether the naive assumptions hold).
- Theoretical analysis depends on inversion/multiplication (I/M)-ratio, S/M-ratio and ratio $M_q/M_{q'}$.
- Hard to take into account load instructions etc.
- How about precomputations?
- Comparison by implementation in general case (R. Avanzi, CHES'04) shows ECC faster.
- Remainder of this talk: tunings to become faster than ECC.

Field of odd characteristic

Specialization $g = 2$, odd q

- If q is odd, transform $y \mapsto \tilde{y} - h(x)/2$

$$(\tilde{y} - h(x)/2)^2 + h(x)(\tilde{y} - h(x)/2) =$$
$$\tilde{y}^2 + (-h(x) + h(x))\tilde{y} + (1/4 - 1/2)h(x)^2 = f(x)$$

  and sort, to obtain curve equation of form

$$\tilde{y}^2 = \tilde{f}(x).$$

- $P = (a, b)$, then $-P = (a, -b)$
- ADD takes $1I, 22M, 3S$, DBL needs $1I, 22M, 5S$.
- Dan Bernstein says: inversions are expensive!!!
- So, avoid inversions.

How does it work?

- Get an idea:
  - Start with normal inputs, at some point one needs to invert.
  - Put the element to be inverted in Z.
  - Adjust all following steps to have denominator Z.
- Start with input having $Z \neq 1$.
  - For ADD this means a lot of adjustments because they have different Z-values.
  - DBL suffers less.
  - ADD might be mixed – one input has $Z = 1$, e.g. the base point in a DL system. Mixed ADD faster.
- Try different weights.

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

Arithmetic a la Pierrick Gaudry

ePrint Report 2005/314
Fast genus 2 arithmetic based on Theta functions

- Needs full 2-torsion group, i. e. cofactor 16.
- Shows that approach valid over general fields.
- ADD + DBL = 25M – no inversion!!!
  (cf. affine ADD: 22M + 3S + 1I, DBL: 22M + 5S + 1I)
- is faster than elliptic curves in Montgomery form.
- Application of formulas is straightforward, only background is more involved.

Field of characteristic 2

Genus 2 curves over $\mathbb{F}_{2^n}$

$$C : y^2 + (h_2x^2 + h_1x + h_0)y = f(x), \deg(f) = 5.$$

Formulas stated earlier hold for general equation. Get higher efficiency by specializing to degree of h.

- $h = 0$ belongs to singular curves, so not hyperelliptic.
- $\deg h = 0$: the curve is supersingular (cf. Pairings in my next talk, choices of curves in last talk by Dan Bernstein).
- $\deg(h) = 1$: group has co-factor 2, no weaknesses up to our present knowledge.
- 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. $\deg h = 1$:
Changes of the form $y \to y' + ax'^2 + bx', x \to cx + d$ allow $f_4 = f_1 = 0$ and some more.

Usual situation:

$$C : y^2 + h_1xy = x^5 + f_3x^3 + f_2x^2 + f_0.$$

If $\mathbb{F}_q = \mathbb{F}_{2^n}$ with odd n one can additionally achieve $h_1 = 1, f_2 \in \mathbb{F}_2$.

In scalar multiplications DBL more important than ADD (use precomputation) $\Rightarrow$ speed up DBL.

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: $z_0 = u_0^2$, $k_1' = u_1^2 + f_3$; $w_0 = f_0 + v_0^2 (= rs_1'/h_1^3)$;	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		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.

Avoid inversions like in odd characteristic.

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

Other curves

- Similar study for $\deg(h) = 2$.
- Similar studies for $g = 3$.
  - In characteristic 2 also $h \in \mathbb{F}_q$ for $g = 3$ possible (not supersingular).
  - affine:
    Kuroki, Gonda, Matsuo, Chao, Tsujii (2002),
    Pelzl, Wollinger (2002), Guyot, Patankar (2003)
  - projective:
    Fan and T. Wollinger and Y. Wang
- There are works on non-hyperelliptic curves – so far not competitive, DLP weaker than on hyperelliptic curves.
- Larger genus looks insecure – arithmetic can be used in attacks (Weil descend).