

# Point counting using deformation

Hendrik Hubrechts

Katholieke Universiteit Leuven (Belgium)

Luminy, March 28, 2009

# Outline

Introduction: point counting via rigid cohomology

Deformation

Results with rigid cohomology

Strategies

## Problem statement.

- ▶  $p$  prime,  $\mathbb{F}_{p^n}$  finite field. We suppose here  $p \geq 3$ .
- ▶ Hyperelliptic curve (HEC)  $\mathcal{C}/\mathbb{F}_{p^n}$  of genus  $g$  (with rational Weierstrass point), affine model:  
$$Y^2 = \bar{Q}(X) \quad \text{where} \quad \bar{Q}(X) = X^{2g+1} + a_{2g}X^{2g} + \cdots + a_1X + a_0.$$
- ▶ What is  $\#\mathcal{C}(\mathbb{F}_{p^n})$ ,  $\#\text{Jac}(\mathcal{C})(\mathbb{F}_{p^n})$ ? Motivation for this problem lies in cryptography.

## Zeta functions.

- ▶ There exists some  $L(T) = p^{ng} T^{2g} + \cdots + a_1 T + 1 \in \mathbb{Z}[T]$  s.t.

$$Z(T) := \exp \left( \sum_{k=1}^{\infty} \frac{\#\mathcal{C}(\mathbb{F}_{(p^n)^k})}{k} T^k \right) = \frac{L(T)}{(1-T)(1-p^n T)}.$$

- ▶  $\#\mathcal{C}(\mathbb{F}_{p^n}) = p^n + 1 + a_1$ ,  $\#\text{Jac}(\mathcal{C})(\mathbb{F}_{p^n}) = L(1)$ .

**Conclusion:** We want to compute  $L(T)$ , given  $Y^2 = \bar{Q}(X)$ .

One approach to the point counting problem goes via *Monsky-Washnitzer (rigid) cohomology* and was initiated by Kedlaya.

**Short overview:**  $\mathcal{C} : Y^2 = \bar{Q}(X)$ , genus  $g$ , over  $\mathbb{F}_{p^n}$ .

- ▶  $p$ -adic numbers  $\mathbb{Q}_p$ , unramified extension  $\mathbb{Q}_{p^n}$ , Frobenius automorphism  $\sigma$ .
- ▶ Take *rigid lift* of  $\mathcal{C}$  to  $\mathbb{Q}_{p^n}$ , remove Weierstrass points.
- ▶ Overconvergent power series:  $A^\dagger := \frac{\mathbb{Q}_{p^n}[X, Y, Y^{-1}]^\dagger}{(Y^2 - Q(X))}$ .
- ▶ Monsky-Washnitzer cohomology of  $\mathcal{C}$ :  $H_{MW}(\mathcal{C}) := \frac{\Omega^1(A^\dagger)}{dA^\dagger}$ .
- ▶  $H_{MW}^-(\mathcal{C})$  is  $2g$ -dimensional subspace with Frobenius operator  $\mathcal{F}_{p^n}$  on it.
- ▶ Reciprocal characteristic polynomial of  $\mathcal{F}_{p^n}$  equals  $L(T)$ , numerator of the zeta function.
- ▶ We can split the operator  $\mathcal{F}_{p^n} = (\mathcal{F}_p)^n$ , on matrix level:

$$F_{p^n} = F_p \cdot F_p^\sigma \cdot F_p^{\sigma^2} \cdots F_p^{\sigma^{n-1}}.$$

Note: in practice we need  $F_{p^n}$  only modulo some finite precision  $p^{C_p \cdot n}$ .

## Families of curves.

- ▶ HEC  $\mathcal{C}_{\bar{\gamma}}$  as part of a family of HEC's over  $\mathbb{F}_{p^n}$ :

$$\mathcal{C}_{\Gamma} : Y^2 = \bar{Q}(X, \Gamma), \quad \bar{Q}(X, \Gamma) = X^{2g+1} + \sum_{i=0}^{2g} a_i(\Gamma) X^i.$$

- ▶ When is  $\mathcal{C}_{\bar{\gamma}}$  for  $\bar{\gamma} \in \mathbb{F}_{p^n}$  hyperelliptic of genus  $g$ ? Iff  $r(\bar{\gamma}) \neq 0$  where the resultant  $r(\Gamma) := \text{Res}_X(\bar{Q}(X, \Gamma), \frac{\partial}{\partial X} \bar{Q}(X, \Gamma))$ .
- ▶ Consider the Monsky-Washnitzer cohomology  $H_{MW}^-(\mathcal{C}_{\Gamma})$  for the family, then the matrix of the  $p$ -th power Frobenius  $F(\Gamma)$  depends on  $\Gamma$ .
- ▶ The connection  $\frac{\partial}{\partial \Gamma}$  on  $H_{MW}(\mathcal{C}_{\Gamma})$  with matrix  $G(\Gamma)$  yields

$$\frac{\partial}{\partial \Gamma} F(\Gamma) + F(\Gamma) \cdot G(\Gamma) = p\Gamma^{p-1} G^{\sigma}(\Gamma^p) \cdot F(\Gamma). \quad (*)$$

**Conclusion.** In order to compute the zeta function of  $\mathcal{C}_{\bar{\gamma}}$ , it suffices to solve (\*) for  $F(\Gamma)$ , plug in  $\gamma$  as *Teichmüller lift* (i.e. root of unity) of  $\bar{\gamma}$  and determine the characteristic polynomial of

$$F(\gamma) \cdot F(\gamma)^{\sigma} \cdots F(\gamma)^{\sigma^{n-1}}.$$

## More on the differential equation

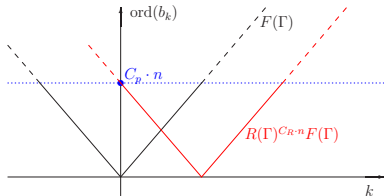
Recall:  $\frac{\partial}{\partial \Gamma} F(\Gamma) + F(\Gamma) \cdot G(\Gamma) = p\Gamma^{p-1}G^\sigma(\Gamma^p) \cdot F(\Gamma)$ .

Goal:  $F(\gamma)$  modulo  $p^{C_p \cdot n}$ .

1. What kind of object is  $G(\Gamma)$ ? In our simplified case ( $p \geq 3$ ):  
 $r(\Gamma) \cdot G(\Gamma)$  consists of polynomials of bounded degree.

2. What kind of object is  $F(\Gamma)$ ? A matrix over (with  $R(\Gamma) \approx r(\Gamma)$ )

$$S^\dagger := \left\{ \sum_{k \in \mathbb{Z}} b_k(\Gamma) R(\Gamma)^k \mid b_k(\Gamma) \in \mathbb{Q}_{p^n}[\Gamma], \liminf_k \frac{\text{ord}(b_k)}{|k|} > 0 \right\}.$$



We need  $F(\Gamma)$  modulo  $p^{C_p \cdot n}$ . There exists some  $C_R > 0$  s.t.  
 $R(\Gamma)^{C_R \cdot n} F(\Gamma) \bmod p^{C_p \cdot n}$   
is polynomial of degree  $\leq C_\Gamma \cdot n$ .

## An easier differential equation.

- Define  $K(\Gamma) := R(\Gamma)^{C_{R \cdot n}} F(\Gamma)$ , then we can rewrite the differential equation to the following form

$$A \left( \frac{\partial}{\partial \Gamma} K \right) B + AKX + YKB = 0, \quad (*)$$

with  $A, B, X, Y \in \mathbb{Q}_p^n[\Gamma]^{2g \times 2g}$  of 'small degree'  $C_\Delta$ ;  $A_0$  and  $B_0$  invertible, and such that the solution satisfies

$$K(\Gamma) \equiv \sum_{i=0}^{C_\Gamma \cdot n} K_i \Gamma^i \pmod{p^{C_p \cdot n}}.$$

- If we know  $K(0)$ , we can recover  $K(\Gamma)$  and/or  $K(\gamma)$ .

**Size of objects.** Suppose  $(*)$  is defined over  $\mathbb{Q}_p^a$  with all valuations bounded from below,  $\bar{\gamma} \in \mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^a}$ , then

- 'size of  $K(\Gamma)$ ':  $a \cdot (C_p \cdot n) \cdot (C_\Gamma \cdot n) \approx an^2$ ,
- 'size of  $K(\gamma)$ ':  $(C_p \cdot n) \cdot n \approx n^2$ .

# The matrix of the $p^n$ -th power Frobenius.

- ▶ Let  $F := F(\gamma)$ , then we need

$$\mathcal{N}(F) = F \cdot F^\sigma \cdot F^{\sigma^2} \cdots F^{\sigma^{n-1}}.$$

- ▶ Recursive method of Kedlaya:  $F_0 := F$ ,  $F_{i+1} := F_i \cdot (F_i)^{\sigma^{2^i}}$  for  $i \leq \log_2 n$  (and some work on the binary representation of  $n$ ). It hence suffices to compute  $\sigma^k(\alpha)$  for  $\alpha \in \mathbb{Q}_{p^n}$  about  $\log n$  times.
- ▶ If we compute  $\sigma^k(\alpha)$  as  $\sigma(\sigma(\cdots(\sigma(\alpha))))$ , this takes time at least  $\mathcal{O}(kn^2) \approx \mathcal{O}(n^3)$ .

- ▶ **Theorem [Kedlaya-Umans '08]** Let  $g, h, f \in (\mathbb{Z}/r\mathbb{Z})[X]$  have degree  $\leq n$  (and some more conditions), then we can compute  $g(h(X)) \bmod f(X)$  in time  $\mathcal{O}(n^{1+\epsilon} \log^{1+\epsilon} r)$ .

- ▶ With  $\alpha(x) \in \mathbb{Q}_{p^n} \cong \mathbb{Q}_p[x]/\varphi(x)$  we have

$$\sigma^k(\alpha(x)) = \alpha(\sigma^k(x)) \bmod \varphi(x).$$

With Newton iteration and [Kedlaya-Umans] we can compute  $\sigma^k(x)$  and hence  $\sigma^k(\alpha(x))$  modulo  $p^{C_p \cdot n}$  in time  $\mathcal{O}(n^{2+\epsilon} \log^{2+\epsilon} p)$ .

## Results with rigid cohomology

All polynomial in the genus  $g$  and the prime  $p$ , curves over  $\mathbb{F}_{p^n}$ .

	time	memory	type
General hyperelliptic (or $C_{a,b}$ )	$\tilde{\mathcal{O}}(n^3)$	$\mathcal{O}(n^3)$	Kedlaya
	$\tilde{\mathcal{O}}(n^3)$	$\mathcal{O}(n^2)$	Deformation
	$\tilde{\mathcal{O}}(n^{2.5})$	$\tilde{\mathcal{O}}(n^{2.5})$	Deformation
Families over prime fields	$\mathcal{O}(n^{2+\epsilon})$	$\mathcal{O}(n^{2+\epsilon})$	Deformation
Elliptic curves	$\tilde{\mathcal{O}}(n^2)$	$\mathcal{O}(n^2)$	Deformation

$$A \left( \frac{\partial}{\partial \Gamma} K \right) B + AKX + YKB = 0, \quad (*)$$

► We write  $K(\Gamma) = \sum_{i=0}^{\infty} K_i \Gamma^i$ .

►  $K_0$  is known (assumption). Equality of  $\Gamma^0$ -coefficients gives

$$A_0 K_1 B_0 = -A_0 K_0 X_0 - Y_0 K_0 B_0,$$

hence we can compute  $K_1$ . Similarly the  $\Gamma^m$ -coefficient gives

$$(m+1)A_0 K_{m+1} B_0 = -(\text{linear combination of } K_m, K_{m-1}, \dots, K_{m-C_\Delta})$$

for a certain  $C_\Delta = \mathcal{O}_n(1)$ .

► After  $C_\Gamma \cdot n$  steps the coefficients  $K_m \bmod p^{C_p \cdot n}$  become zero.

Note that we do not need to know  $C_\Gamma \cdot n$  in advance.

**Conclusion.** If (\*) is defined over  $\mathbb{Q}_{p^a}$ , we can compute the solution  $K(\Gamma) \bmod p^{C_p \cdot n}$  in time

$$\tilde{\mathcal{O}}((C_\Gamma \cdot n) \cdot C_\Delta \cdot (a \cdot C_p \cdot n)) = \tilde{\mathcal{O}}(n^2 \cdot a).$$

## Families over small fields

- ▶ We take  $a = 1$ , namely

$$\mathcal{C}_\Gamma : Y^2 = \bar{Q}(X, \Gamma) \quad \text{with} \quad \bar{Q}(X, \Gamma) \in \mathbb{F}_p[X, \Gamma],$$

and  $\bar{\gamma} \in \mathbb{F}_{p^n}$ ; our goal is  $\mathcal{C}_{\bar{\gamma}}$ . Note:  $\mathcal{C}_0$  and  $K_0$  are 'easy'!

- ▶ Then  $K(\Gamma)$  can be computed in time  $\tilde{\mathcal{O}}(n^2 a) = \tilde{\mathcal{O}}(n^2)$ .

- ▶ Let  $\gamma \in \mathbb{Q}_{p^n} \cong \mathbb{Q}_p[x]/\varphi(x)$  be the Teichmüller lift of  $\bar{\gamma}$ , then

$$K(\gamma) = K(\gamma(x)) \bmod \varphi(x),$$

hence [Kedlaya-Umans] gives  $K(\gamma)$  in time  $\mathcal{O}(n^{2+\epsilon})$ .

- ▶ An obvious computation gives  $F(\gamma) = R(\gamma)^{-C_R \cdot n} \cdot K(\gamma)$ .
- ▶ As explained before, the  $p^n$ -th power Frobenius matrix can also be computed in time  $\mathcal{O}(n^{2+\epsilon})$ .
- ▶ This includes all elliptic curves, but there are more efficient ways in this case (even using deformation).

# General hyperelliptic curves — memory efficient (second strategy)

- ▶  $C_1 : Y^2 = \bar{Q}_1(X)$  over  $\mathbb{F}_{p^n}$  (target)  
 $C_0 : Y^2 = \bar{Q}_0(X)$  over  $\mathbb{F}_p$  (at will, 'easy' curve)  
 $C_\Gamma : Y^2 = \bar{Q}(X, \Gamma) = \Gamma \cdot \bar{Q}_1(X) + (1 - \Gamma) \cdot \bar{Q}_0(X)$  over  $\mathbb{F}_{p^n}$ .
- ▶ Working as before would give time and memory  $\tilde{O}(n^2 \cdot a) = \tilde{O}(n^3)$  for  $K(\gamma) = K(1) = \sum K_i$ .
- ▶ 'Sliding window'-technique:  $S_0 := K_0$  and
$$K_{m+1} = \frac{1}{m+1} \cdot A_0^{-1} \cdot (\text{linear comb. of } K_m, \dots, K_{m-C_\Delta}) \cdot B_0^{-1},$$
$$S_{m+1} = S_m + K_{m+1}.$$
- ▶ We only need to store the last  $C_\Delta$  instead of  $C_\Gamma \cdot n$  matrices.
- ▶ Result:  $S_{C_\Gamma \cdot n} = \sum_{i=0}^{C_\Gamma \cdot n} K_i \bmod p^{C_\Gamma \cdot n} = K(\gamma)$  in time  $\tilde{O}(n^3)$  but memory space only  $\mathcal{O}(n^2)$ .

## Results with rigid cohomology

All polynomial in the genus  $g$  and the prime  $p$ , curves over  $\mathbb{F}_{p^n}$ .

	time	memory	type
General hyperelliptic	$\tilde{\mathcal{O}}(n^3)$	$\mathcal{O}(n^3)$	Kedlaya
(or $C_{a,b}$ )	$\tilde{\mathcal{O}}(n^3)$	$\mathcal{O}(n^2)$	Deformation
	$\tilde{\mathcal{O}}(n^{2.5})$	$\tilde{\mathcal{O}}(n^{2.5})$	Deformation
Families over prime fields	$\mathcal{O}(n^{2+\epsilon})$	$\mathcal{O}(n^{2+\epsilon})$	Deformation
Elliptic curves	$\tilde{\mathcal{O}}(n^2)$	$\mathcal{O}(n^2)$	Deformation

## A trick of Chudnovsky and Chudnovsky

**Question:** Compute  $d_N$  from a recurrence relation  $d_{i+1} = f(i) \cdot d_i$ , with  $d_0$  given and  $f(i)$  'easy/short'.

- ▶ Naive algorithm:  $d_1 = f(0)d_0$ ,  $d_2 = f(1)d_1$ , ... Requires  $\mathcal{O}(N)$  ring operations.
- ▶ C&C: use fast polynomial arithmetic:
  1.  $\psi(X) := f(X) \cdot f(X+1) \cdot f(X+2) \cdots f(X + \sqrt{N} - 1)$  using  $\tilde{\mathcal{O}}(\sqrt{N})$  ring operations.
  2.  $d_{\sqrt{N}} = \psi(0)d_0$ ;  $d_{2\sqrt{N}} = \psi(\sqrt{N})\psi(0)d_0$ ; ...;

$$d_N = d_0 \cdot \prod_{i=0}^{\sqrt{N}-1} \psi(\sqrt{N} \cdot i).$$

Fast multipoint evaluation gives all  $\psi(\sqrt{N} \cdot i)$  in  $\tilde{\mathcal{O}}(\sqrt{N})$  ring operations.

3. Conclusion: we can compute  $d_N$  in  $\tilde{\mathcal{O}}(\sqrt{N})$  ring operations.

$$\begin{aligned} & \left( f(0)f(1)f(2) \cdots f(\sqrt{N} - 1) \right) \cdot \left( f(\sqrt{N}) \cdots f(2\sqrt{N} - 1) \right) \cdots \left( f(N - \sqrt{N}) \cdots f(N - 1) \right) \\ &= \psi(0) \quad \cdot \quad \psi(\sqrt{N}) \quad \cdots \quad \psi(N - \sqrt{N}). \end{aligned}$$

**Note.** Via  $\sqrt{N}! \bmod (N = pq)$  we find a  $\tilde{\mathcal{O}}(N^{1/4})$  RSA-factoring algorithm.

- $d_{i+1} = f_0(i)d_i + f_1(i)d_{i-1} + \cdots + f_\ell(i)d_{i-\ell}$ . Compute  $d_N$ .

$$\mathcal{D}_i := \begin{bmatrix} d_i \\ d_{i-1} \\ \vdots \\ d_{i-\ell} \end{bmatrix} \Rightarrow \mathcal{D}_{i+1} = \begin{bmatrix} f_0^{(i)} & f_1^{(i)} & \cdots & f_{\ell-1}^{(i)} & f_\ell^{(i)} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \mathcal{D}_i.$$

The same C&C trick works with matrix polynomials.

- We will also need  $\sum_{i=0}^N d_i =: \sigma_N$ , representable via

$$\mathcal{D}'_i := \begin{bmatrix} d_i \\ d_{i-1} \\ \vdots \\ d_{i-\ell} \\ \sigma_{i-1} \end{bmatrix} \Rightarrow \mathcal{D}'_{i+1} = \begin{bmatrix} f_0^{(i)} & f_1^{(i)} & \cdots & f_{\ell-1}^{(i)} & f_\ell^{(i)} & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} \mathcal{D}'_i.$$

- Conclusion:  $\sigma_N$  can be computed in  $\tilde{O}(\sqrt{N})$  ring operations, assuming  $\ell$  is bounded.
- The above even works if all  $d_i$  and  $\sigma_i$  are vectors themselves.

### Third strategy, an $\tilde{O}(n^{2.5})$ -algorithm

- ▶ Recall:  $\mathcal{C}_\Gamma : Y^2 = \bar{Q}(X, \Gamma)$ , a deformation from  $\mathcal{C}_0/\mathbb{F}_p$  to  $\mathcal{C}_1/\mathbb{F}_{p^n}$ .
- ▶ As before we need to compute  $K(1) = \sum_{i=0}^{C_\Gamma \cdot n} K_i$  from the diff. eq.

$$A \left( \frac{\partial}{\partial \Gamma} K \right) B + AKX + YKB = 0,$$

- ▶ Non-commutativity of matrix multiplication prohibits us from using C&C directly on

$$K_{i+1} = \frac{1}{i+1} A_0^{-1} \left( \sum_j \cdots K_{i-j} \cdots \right) B_0^{-1}. \quad (*)$$

- ▶ Solution: write  $K_i$  as one large  $4g^2 \times 1$  vector, and rewrite (\*) in this representation:

$$K_{i+1} = \sum_{j=0}^{C_\Delta} f(j) \cdot K_{i-j}.$$

Then apply the fast computations (including the sum  $\sum K_i$ ) of before, using  $\tilde{O}(\sqrt{C_\Gamma \cdot n})$  operations in  $\mathbb{Q}_{p^n} \bmod p^{C_p \cdot n}$ .

**Conclusion.** We can compute  $K(1)$  in time  $\tilde{O}(n^{2.5})$ . The same holds then for the zeta function of  $\mathcal{C}_1$ .