Point counting on singular hypersurfaces

Remke Kloosterman

Institut für Algebraische Geometrie
Leibniz Universität Hannover
Germany

Banff, May 18, 2008

Contents

Statement of problem

- Let $q = p^r$ be a prime power, $\mathbf{F}_q$ finite field with q elements.
- Let $\overline{V}/\mathbf{F}_q$ be an n-dimensional variety, $n \geq 1$.
- Let $Z(\overline{V}, T)$ be the function

$$\exp\left(\sum_{s=1}^{\infty} \#\overline{V}(\mathbf{F}_{q^s})\frac{T^i}{s}\right).$$

Determine $Z(\overline{V}, T)$ in polynomial time.

- Dwork: $Z(\overline{V}, T)$ is a rational function.
- Weil conjectures: determining $Z(\overline{V}, T)$ in polynomial time is equivalent to determining $\#\overline{V}(\mathbf{F}_q)$ in polynomial time.

Known results I (ℓ-adic)

Cases with complete solution to this problem:

- $\overline{V}$ smooth genus g curve. ($g = 0$ trivial, $g = 1$ by Schoof-Elkies-Atkin, $g > 1$ by Pila, but not practical.)
- Some exceptional cases (e.g., "Modular elliptic surfaces", Edixhoven).
- Use étale cohomology (and Lefschetz trace formula). More complicated if $n > 1$.

Known Results II (p-adic)

Other approaches:

- AGM (Mestre), Canonical Lift (Satoh). Methods for curves.
- Methods using Monsky-Washnitzer cohomology / rigid cohomology:
  - Direct Method: Kedlaya (hyperelliptic curves), Lauder-Wan (Artin-Schreier curves), Denef-Vercauteren ($C_{a,b}$-curves), Harvey (hyperelliptic curves), Abbott-Kedlaya-Roe (hypersurfaces).
  - Deformation method: Lauder (hypersurfaces), Gerkmann (hypersurfaces), Hubrechts (hyperelliptic curves).
  - Recursive method: Lauder.

Main problem: most algorithms turn out to be exponential in $\log(p)$, where p is the characteristic. But for p fixed, the complexity of p-adic algorithms is better than ℓ-adic.

Monsky-Washnitzer cohomology: Preliminaries

Assume $\overline{U}$ is a *smooth affine* variety. I.e., the coordinate ring $\overline{R}$ of $\overline{U}$ is of the form

$$\mathbf{F}_q[x_1, \ldots, x_m]/(\overline{f}_1, \ldots, \overline{f}_k).$$

Let $\mathbf{Z}_q = W(\mathbf{F}_q)$ (unramified extension of $\mathbf{Z}_p$ of degree r), π the maximal ideal of $\mathbf{Z}_q$. Let

$$R_1 := \mathbf{Z}_q[x_1, \ldots, x_m]/J$$

such that $R_1/\pi R_1 \cong \overline{R}$. (Existence follows from a theorem of Elkik.)

Monsky-Washnitzer cohomology: Overconvergent power series

Set $\mathbf{Z}_q\langle x_1,\dots,x_m\rangle^\dagger$ to be the ring of formal power series

$$\sum_{i_1,\dots,i_n=0}^{\infty} c_{i_1,\dots,i_m}\ x_1^{i_1}\dots x_m^{i_m}\ \ (c_I\in\mathbf{Z}_q)$$

such that $v(c_I)+a(i_1+\dots+i_m)>b$ for some $a>0, b$.
Let $R_1^\dagger$ be

$$\mathbf{Z}_q\langle x_1,\dots,x_m\rangle^\dagger/J\mathbf{Z}_q\langle x_1,\dots,x_m\rangle^\dagger.$$

A lift of Frobenius $F: R_1^\dagger\to R_1^\dagger$ is a $\mathbf{Z}_q$-linear map such that

$$F(x_i)\equiv x_i^q \bmod \pi.$$

(Better: take a lift of p-Frobenius, is semi-linear.)

Monsky-Washnitzer cohomology

Let $R^\dagger := R_1^\dagger \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$. Consider the de Rham complex

$$0 \to R^\dagger \xrightarrow{d} \Omega^1_{R^\dagger} \xrightarrow{d} \cdots \xrightarrow{d} \Omega^n_{R^\dagger} \to 0.$$

Monsky-Washnitzer cohomology is the cohomology of the above complex, i.e.,

$$H^i(\overline{V}, \mathbf{Q}_q) = \frac{\ker(d : \Omega^i_{R^\dagger} \to \Omega^{i+1}_{R^\dagger})}{\operatorname{im}(d : \Omega^{i-1}_{R^\dagger} \to \Omega^i_{R^\dagger})}.$$

The lift F of Frobenius induces an action on $\Omega^i_{R^\dagger}$ and on $H^i(\overline{U}, \mathbf{Q}_q)$. Lefschetz Trace Formula gives

$$\#\overline{U}(\mathbf{F}_{q^s}) = \sum_{i=0}^{n} (-1)^i \operatorname{trace}(q^{ns} F^{-ns} \mid H^i(\overline{U}, \mathbf{Q}_q)).$$

Hypersurfaces

- $\overline{f} \in \mathbf{F}_q[X_0, \ldots, X_{n+1}]$ be a degree d homogeneous polynomial.
- $\overline{V} \subset \mathbf{P}^{n+1}$ be the zero-set of $\overline{f}$.
- $\overline{U} = \mathbf{P}^{n+1} \setminus \overline{V}$. Then

$$Z(\overline{U}, T)Z(\overline{V}, T) = Z(\mathbf{P}^{n+1}, T) = \prod_{i=0}^{n+1}(1 - p^i T).$$

- $\overline{U}$ is smooth and affine, hence $H^i(\overline{U}, \mathbf{Q}_q)$ exists.
- Lefschetz hyperplane theorem (together with Poincaré duality on $\overline{V}$), gives for $\overline{V}$ *smooth*

$$H^i(\overline{U}, \mathbf{Q}_q) = 0 \text{ for } i \neq 0, n+1.$$

- $H^0(\overline{U}, \mathbf{Q}_q)$ is one-dimensional, F acts trivially.
- In the smooth case: suffices to determine $H^{n+1}(\overline{U}, \mathbf{Q}_q)$.

Direct method, example

Direct method (following AKR).

- Take $q = p$ an odd prime.
- Let $\overline{V} : \overline{f} := w^2 + x^2 + y^2 + z^2 = 0$ in $\mathbf{P}^3$.
- Let $f := w^2 + x^2 + y^2 + z^2 \in \mathbf{Z}_p[w, x, y, z]$ be a lift of $\overline{f}$.
- Let Ω be

$$wxyz \left(\frac{dx}{x} \wedge \frac{dy}{y} \wedge \frac{dz}{z} - \frac{dw}{w} \wedge \frac{dy}{y} \wedge \frac{dz}{z} + \dots \right.$$
$$\left. \dots + \frac{dw}{w} \wedge \frac{dx}{x} \wedge \frac{dz}{z} - \frac{dw}{w} \wedge \frac{dx}{x} \wedge \frac{dy}{y} \right).$$

- $H^3(\overline{U}, \mathbf{Q}_p)$ is one dimensional, spanned by

$$\omega := \frac{1}{f^2}\Omega.$$

Lift of Frobenius

- Set $F(w) = w^p, F(x) = x^p, F(y) = y^p, F(z) = z^p$.
- Hence $F(\frac{dx}{x}) = p\frac{dx}{x}$.
- Set $\Delta := f(w,x,y,z)^p - f(w^p,x^p,y^p,z^p)$. Then using geometric series we obtain

$$F(\omega) = \left(\sum_{k=0}^{\infty}(k+1)\frac{(wxyz)^{p-1}\Delta^k}{f^{p(k+2)}}\right)p^3\Omega.$$

- From $\Delta \equiv 0 \bmod p$ it follows that $v(c_I)$ is around $(i_1+i_2+i_3+i_4)/p$ (and that this series is overconvergent).
- Aim: compute the class of $F(\omega)$ in $H^3(\overline{U},\mathbf{Q}_q)$ modulo p^N.
- Need to start with $F(\omega) \mod p^{N+M}$ with M roughly $\log_p N$.

Lift of Frobenius II

- $F(\omega) \bmod p^{N+M}$ equals:

$$\sum_{j=0}^{N+M} \sum_{k=j}^{N+M} (k+1) \binom{k}{j} \frac{(wxyz)^{p-1} f(w^p, x^p, y^p, z^p)^j}{f^{p(j+2)}} p^3 \Omega.$$

- Reduction of pole order: g polynomial of degree $2t-4$, $t>2$, write $g := f_w g_1 + f_x g_2 + f_y g_3 + f_z g_4$. (Possible since $\mathbf{Q}_q[w,x,y,z]/(f_w, f_x, f_y, f_z) = \mathbf{Q}_q \cdot \overline{1}$.) Then

$$\frac{g}{f^t}\Omega = \frac{(g_1)_w + (g_2)_x + (g_3)_y + (g_4)_z}{(t-1)f^{t-1}}\Omega.$$

- Need $p(N+M+2)-2$ reductions to have pole order 2. Exponential in $\log(p)$.
- In this case we obtain $F(\omega) = p^2\omega$ and $\#\overline{V}(\mathbf{F}_p) = p^2 + 2p + 1$.

Improvements

- Method works for affine varieties. Better: cover $\overline{V}$ with affine varieties, and count on each affine piece. Computations take place in a polynomial ring with one variable less.
- Using that expressions like

$$\sum_{j=0}^{N+M}\sum_{k=j}^{N+M}(k+1)\binom{k}{j}\frac{(xyzw)^{p-1}f(w^p,x^p,y^p,z^p)^j}{f^{p(j+2)}}p^3\Omega.$$

are sparse, Harvey obtained in the hyperelliptic case an algorithm with complexity $O(\sqrt{p})$ $(g,r$ fixed).

Improvements (Dwork's ψ-function I)

- Can replace F by ψ such that $\psi \circ F$ is the identity on $\Omega^i_{R_{\mathbf{Q}_p}}$ (left-inverse).
- Since F on $H^{n+1}(\overline{U}, \mathbf{Q}_q)$ is invertible, we have that $\psi = F^{-1}$ on $H^{n+1}(\overline{U}, \mathbf{Q}_q)$.
- Definition of ψ: $\psi(\frac{dx}{x}) = \frac{1}{p}\frac{dx}{x}$ and

$$\psi(w^h x^i y^j z^k) = \begin{cases} w^{h/p} x^{i/p} y^{j/p} z^{k/p} & h, i, j, k \equiv 0 \bmod p. \\ 0 & \text{otherwise.} \end{cases}$$

Improvements (Dwork's ψ-function II)

- Hence $\psi(\omega)$ equals

$$\sum_{k=0}^{\infty} \frac{\psi((-\Delta)^k f^{p-2} wxyz)}{f^{k+2}} \frac{\Omega}{p^3 wxyz}$$

- Note $v(c_I) \geq i_1 + i_2 + i_3 + i_4 - 2$.
- $\psi(\omega)$ converges p times faster than $F(\omega)$.
- Gain a factor p in the reduction algorithm, the reduction part is polynomial in $\log(p)$.

Improvements (Dwork's ψ-function III)

- Expanding yields that $\psi(\omega)$ (modulo p^{N+M-3}) equals

$$\sum_{j=0}^{N+M} \sum_{k=j}^{N+M} \frac{(-1)^j \binom{k}{j} \psi(f^{(j+1)p-2} wxyz)}{f^{j+1}} \frac{\Omega}{p^3 wxyz}$$

- Need to calculate $f(w,x,y,z)^{p(N+M+1)-2}$ in order to calculate $\psi(\omega)$.
  - Exponential in $\log p$.
  - Prevents applying Harvey's method.
- ψ is defined for any n-dimensional smooth affine variety, namely $\psi := \frac{1}{p^n} F^{-1} \circ \mathrm{trace}_{R^\dagger / F(R^\dagger)}$.
- ψ is crucial for studying singular varieties.

Deformation method I

Second idea (*Deformation method*):

- Assume $p \nmid d$. Let

$$f_t := (1-t)(x_0^d + \cdots + x_{n+1}^d) + tf.$$

- $f_0 := x_0^d + \cdots + x_{n+1}^d$
- $f_1 = f$.
- Action of $F_0 := F$ on $H^{n+1}(\overline{U}_0)$ is easy to calculate.
- Take $\overline{t_0} \in \mathbf{F}_q$ such that $f_{\overline{t_0}}$ is smooth.
- $t_0 \in \mathbf{Q}_q$ the Teichmüller lift of $\overline{t_0}$ ($t_0^q = t_0$ and $t_0 \equiv \overline{t_0} \bmod \pi$).

Deformation method II

- Can find a Picard-Fuchs equation (differential equation associated with a family of varieties).
- Let $A(t)$ be a solution of the Picard-Fuchs equation with $A(0) = I$.
- The action of F on $H^{n+1}(\overline{U}_{\overline{t_0}})$ equals

$$\lim_{t \to t_0} A(t)^{-1} F_0 A(t^q).$$

- Advantage: A is a function in one variable, computation in $\mathbf{Q}_q\langle t\rangle^\dagger$ instead of $\mathbf{Q}_q\langle x_0, \dots, x_{n+1}\rangle^\dagger$.
- Memory-efficient.
- Time complexity still $O(p)$ (r, d, n fixed).

Deformation method, example

- Consider the family

$$x^2 + y^2 + z^2 + (1-t)w^2$$

- The Picard-Fuchs equation equals

$$\frac{\partial A}{\partial t} = \frac{-1}{2(t-1)} A$$

- Hence $A(t) = (1-t)^{-1/2}$.
- $F_t = A(t)^{-1} F_0 A(t^q) = p^2 \frac{\sqrt{1-t}}{\sqrt{1-t^q}}$ and

$$F_{t_0} = \begin{cases} p^2 & \text{if } 1 - t_0 \bmod p \text{ is a square} \\ -p^2 & \text{if } 1 - t_0 \bmod p \text{ is not a square} \\ p^{3/2} & \text{if } t_0 = 1 \end{cases}$$

Singular hypersurfaces

What goes wrong?

- Poincaré duality for $\overline{V}$ might fail.
- Hence it is possible that $H^i(\overline{U}, \mathbf{Q}_q) \neq 0$ for $1 \leq i \leq n$.
- Need approaches to calculate $H^i(\overline{U}, \mathbf{Q}_p)$ for $1 \leq i \leq n$.
- Today we ignore this issue. There are classes of singular varieties for which $H^i(\overline{U}, \mathbf{Q}_q) = 0$ for $i \neq 0, n+1$ holds. E.g., $\overline{V}$ is a surface with so-called ADE singularities.
- Assume for the rest of this talk that $H^i(\overline{U}, \mathbf{Q}_p) = 0$ for $i \neq 0, n+1$.

Direct method

- The reduction part of the direct method uses certain relations between cohomology classes. E.g.,

$$\frac{gf_x}{f^t}\Omega = \frac{g_x}{(t-1)f^{t-1}}\Omega$$

- If $\overline{V}$ is singular then there are "more" relations.
- Ambitious solution: identify those extra relations. Very hard.
- Naive solution: pretend that $\overline{V}$ were smooth and look what happens.
- To work with finite-dimensional vectors spaces we need that $\oplus_k R(f)_{kd-n-2}$ is finite-dimensional where

$$R(f) := \mathbf{Q}_q[x_0, \ldots, x_{n+1}]/(f_{x_0}, \ldots, f_{x_{n+1}}).$$

Direct method: Naive solution

- We need that f is smooth lift of $\overline{f}$.
- E.g., choose f such that $f \bmod \pi^2$ is smooth, i.e, $f_{x_0} \equiv 0 \bmod \pi^2, \ldots, f_{x_n} \equiv 0 \bmod \pi^2$ has no solution.
- In the smooth case we have

$$H^{n+1}(\overline{U}, \mathbf{Q}_q) = \oplus_{k=1}^{n+1} R(f)_{kd-n-2}.$$

In singular case we have that

$$\oplus_{k=1}^{n+1} R(f)_{kd-n-2} \to H^{n+1}(\overline{U}, \mathbf{Q}_q)$$

is surjective. The kernel corresponds to the missing relations between cohomology classes.
- Naive approach: calculate F on $R(f)_{kd-n-2}$.

Direct Method: Naive Solution (Reduction)

- For the reduction algorithm we need to write g of "high degree" as

$$g = \sum g_i f_{x_i}, \text{ for some } g_i \in \mathbf{Q}_q[x_0, \ldots, x_{n+1}].$$

- We chose f to be smooth, hence $R(f)$ is finite dimensional. So g_i exist.
- Since $\overline{V}$ is singular we have

$$R(\overline{f}) = \mathbf{F}_q[x_0, \ldots, x_{n+1}]/(\overline{f}_{x_0}, \ldots, \overline{f}_{x_{n+1}})$$

  is infinite-dimensional.
- If $g \in \mathbf{Z}_q[x_0, \ldots, x_{n+1}]$ is such that $\overline{g}$ in $R(\overline{f})$ is non-zero, then some of the g_i need to have coefficients with negative valuation.

Direct Method: Naive Solution (Use ψ)

- Serious amount of division by elements of π in the reduction algorithm.
- The convergence of $F(\omega)$ is not sufficient to compensate.
- It is likely that for some ω, the reduction of $F(\omega)$ will diverge.
- F^{-1} acting on $\oplus R(f)_{kd-n-2}$ has a non-trivial kernel.
- Use ψ to determine kernel of F^{-1}.

Direct Method: Naive Solution (Result)

- Recall that ψ on $H^{n+1}(\overline{U}, \mathbf{Q}_q)$ is invertible, hence K_1 the kernel of $\psi : \oplus R(f)_{kd-n-2} \to \oplus R(f)_{kd-n-2}$ is a subspace of

$$K := \ker\left(\oplus R(f)_{kd-n-2} \to H^{n+1}(\overline{U}, \mathbf{Q}_q)\right).$$

- Can find examples where $\dim K = \dim K_1$. (See proceedings)
- If $\dim K = \dim K_1$ then

$$\mathrm{trace}(\psi \mid \oplus R(f)_{kd-n-2}) = \mathrm{trace}(\psi \mid H^{n+1}(\overline{U}, \mathbf{Q}_q))$$

- AKR with ψ counts the number of points correctly.

Deformation at singular varieties

- Recall: Family of HS $\overline{V}_t$ with complements $\overline{U}_t$.
- Assume $\overline{V}_1$ is singular.
- Dimension of H^{n+1} drops, i.e., $\dim H^{n+1}(\overline{U}_1, \mathbf{Q}_p) < \dim H^{n+1}(\overline{U}_0, \mathbf{Q}_p)$.
- Naively applying deformation method yields an operator

  $$\lim_{t \to 1} F_t$$

  on a vector space of dimension equal to $\dim H^{n+1}(\overline{U}_0, \mathbf{Q}_p)$.
- Expect F_t to have poles at $t = 1$.
- Possible solution to these problems: calculate $F_{t_0}^{-1} := \lim_{t \to 1} F_t^{-1}$. Ignore its kernel K and hope that $\dim K = \dim H^{n+1}(\overline{U}_0, \mathbf{Q}_p) - \dim H^{n+1}(\overline{U}_1, \mathbf{Q}_p)$.
- Not sufficient: there exist examples such that $\dim K < \dim H^{n+1}(\overline{U}_0, \mathbf{Q}_p) - \dim H^{n+1}(\overline{U}_t, \mathbf{Q}_p)$. (Even when AKR works.) Analytic continuation / Non-uniqueness of completion.

Deformation method: Main obstruction

- Non-uniqueness of completion.
- Given a family of abstract varieties $\overline{V}_t$, for $t \neq 1$. If we require that $\overline{V}_1$ is smooth, then $\overline{V}_1$ is (essentially) unique (if it exists).
- If we do not require that $\overline{V}_1$ is smooth then $\overline{V}_1$ is non-unique.
- The output of the deformation method is determined by $\overline{V}_t$, for t close to 0.
- Conclusion: there is a good change the deformation method will count the number of points of a different family.

Deformation method: Example

- (Different from conference proceedings)
- Consider $\overline{V}_t : w^2 + x^2 + y^2 + z^+ t(t-2)w^2 \subset \mathbf{P}^3$, and $\overline{V}'_t \subset \mathbf{P}^6$ given by the vanishing of: $(s = 1 - t)$

$$-x_5x_6 + x_4^2 - sx_1x_4, -x_4x_5 + x_3x_6 + sx_2x_4, x_2x_6 - x_1x_4,$$

$$-x_5^2 + x_3x + 4 + s^2x_2^2, -x_2x_4 + x_1x_5 + sx_1x_2, -x_2x_5 + sx_2^2 + x_1x_3$$

- $\overline{V}_t \cong \overline{V}'_t \cong \mathbf{P}^1 \times \mathbf{P}^1$ for $t \neq 1$.
- $\overline{V}_1$ is a cone over a conic.
- $\overline{V}'_1$ is the so-called second Hirzebruch surface (smooth). Actually, $\overline{V}'_1 \to \overline{V}_1$ is a resolution of singularities and $\#\overline{V}'_1(\mathbf{F}_q) = q^2 + 2q + 1 = \#\overline{V}_1(\mathbf{F}_q) + q$.

Deformation method: Example

- Since $\overline{V}_t = \overline{V}'_t$ for t small, both families have the same Picard-Fuchs equation.
- Subtlety: some poles of F_t can be resolved by changing the basis for $H^n(\overline{V}_t, \mathbf{Q}_q)$ in a neighborhood of $t = 0$.
- One choice of basis for $H^n(\overline{V}_t, \mathbf{Q}_q)$ yields the following Picard-Fuchs equation

$$\frac{\partial y}{\partial t} = \begin{pmatrix} \frac{-1}{1-t} & 0 \\ 0 & 0 \end{pmatrix} y.$$

Output: $q^2 + q + 1$. $(= \#\overline{V}_1(\mathbf{F}_q).)$

- A second choice of basis yields

$$\frac{\partial y}{\partial t} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} y.$$

Output: $q^2 + 2q + 1$. $(= \#\overline{V}'_1(\mathbf{F}_q).)$

Deformation method: Example

- Issue: choice of basis.
- To get a good analytic continuation of $A(t^q)F_0A(t)^{-1}$ at $t = t_0$ in the smooth case we need to kill all possible singularities at $t = t_0$.
- In the singular case, might need to kill some of the singularities of PF-equation at $t = t_0$.
- Seems hard to decide which singularities to kill and which not.
- In terms of differential equations: Suppose we have a differential equation $y' = \frac{a}{(1-t)}y$ then changing basis (for $H^n(\overline{V}_t, \mathbf{Q}_q)$) corresponds to replace a with $a + k$, for an integer k.
- Can get rid of integral residues.

Conclusion

- AKR (slightly altered) extends to a class of singular varieties.
- There is an obstruction to extend the deformation method of Lauder and Gerkmann to singular varieties, due to the non-uniqueness of completion of families.
- The deformation method can be used in particular cases to calculate the number of points of a stable reduction, or a partial resolution of singularities of a singular hypersurface.

Open questions

- Determine precisely for which classes varieties the above phenomena occur, specifically:
- Find classes of varieties for which AKR (with ψ) works.
- Find classes of varieties for which Lauder-Gerkmann calculates the number of points of a resolution of singularities.
- Find methods to calculate $H^i(\overline{U}, \mathbf{Q}_q)$ for $1 \leq i \leq n$, if $\overline{V}$ is singular.

Thank you for your attention.

A corrected version of my paper will be soon available at
`http://www.iag.uni-hannover.de/~kloosterman`

Leibniz Universität Hannover