Point counting on K3 surfaces and applications

Andreas-Stephan Elsenhans

Universität Paderborn

Providence RI October 2015

A variation of a Kedlaya – Harvey method for K3 surfaces of degree 2.

Joint work with J. Jahnel.

Introduction

Problem
Given a homogeneous polynomial $f \in \mathbb{Z}[X_0, \ldots, X_n]$. Compute

$$\#\{x \in \mathbf{P}^n(\mathbb{F}_{p^d}) \mid f(x) = 0\}$$

for some prime p and several values of d.

Variation
Study the double cover

$$W^2 = f(X_0, \ldots, X_n)$$

instead of the variety $f = 0$.

Naive point counting

Algorithms
Evaluate f at all points of $\mathbf{P}^n$ and count zeroes.

Optimization 1
Compute roots of univariate polynomials $f(x_0, \ldots, x_{n-1}, t)$
for all $(x_0, \ldots, x_{n-1}) \in \mathbf{P}^{n-1}(\mathbb{F}_{p^d})$.

Optimization 2
Count Frobenius orbits of points instead of points.

Complexity
$O(p^{nd})$ and $O(p^{(n-1)d})$.

Optimized naive point counting

Example

$$W^2 = 6X^6 + 6X^5Y + 2X^5Z + 6X^4Y^2 + 5X^4Z^2 + 5X^3Y^3 \\ + X^2Y^4 + 6XY^5 + 5XZ^5 + 3Y^6 + 5Z^6$$

Number of points over $\mathbb{F}_7, \ldots, \mathbb{F}_{7^{10}}$:

$$60,\ 2\,488,\ 118\,587,\ 5\,765\,828,\ 282\,498\,600, \\ 13\,841\,656\,159,\ 678\,225\,676\,496,\ 33\,232\,936\,342\,644, \\ 1\,628\,413\,665\,268\,026,\ 79\,792\,266\,679\,604\,918.$$

Remark
Equation has no monomial with Y and Z.

Point counting using étale cohomology

Lefschetz Trace Formula

$$\#V(\mathbb{F}_p) = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}(\text{Frob}, \text{H}^i_{\text{ét}}(V, \mathbb{Q}_\ell))$$

for a n-dimensional projective variety V with good reduction at p.

Problem
Find explicit description of étale cohomology.

Example
Let E be an elliptic curve.
Then the ℓ^n torsion of E give an explicit description of $\text{H}^1_{\text{ét}}(E, \mathbb{Z}/\ell^n\mathbb{Z})$.

Remark
This is the starting point of the Schoof algorithm.

Point counting on cubic surfaces

27 Lines
A smooth cubic surface has 27 lines. They generate the Picard group. Via the cycle map we get the étale cohomology.

$$\operatorname{Pic}(V) \cong \mathbb{Z}^7, \ \text{H}^2_{\text{ét}}(V, \mathbb{Z}_\ell(1)) \cong \operatorname{Pic}(V) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$$

Example

```
> p := NextPrime(31^31);
> p;
17069174130723235958610643029059314756044734489
> rr<x,y,z,w> := PolynomialRing(GF(p),4);
> gl := x^3 + 2*y^3 + 3*z^3 + 5*w^3 - 7*(x+y+z+w)^3;
> time NumberOfPointsOnCubicSurface(gl);
2913567055049513379297281477203956430954204417435461480
74332970578622743757660955298550825611
Time: 1.180
```


Congruences on the number of points

Lemma
Let V be a cubic surface over $\mathbb{F}_p$. Then $\#V(\mathbb{F}_p) \equiv 1 \bmod p$.

Proof
Let $f(X, Y, Z, W)$ be the corresponding cubic form.
$f(x, y, z, w)^{p-1} \bmod p$ is 0 or 1 by Fermat's theorem. Thus,

$$(p-1)\#V(\mathbb{F}_p) \equiv p^4 - 1 - \sum_{x,y,z,w=0,\ldots,p-1} f(x, y, z, w)^{p-1} \bmod p$$

Any monomial of $f(x, y, z, w)^{p-1}$ has degree $3(p-1)$. Thus, one of the exponents is $< p-1$. As $\sum_{x=0,\ldots,p-1} x^e \equiv 0 \bmod p$ for $e = 0, \ldots, p-2$ the sum above is zero. We get

$$(p-1)\#V(\mathbb{F}_p) \equiv -1 \bmod p.$$

□

Generalization

Remark
The approach above can be used to show that any hypersurface S in $\mathbf{P}^n(\mathbb{F}_p)$ of degree at most n satisfies $\#S(\mathbb{F}_{p^f}) \equiv 1 \bmod p$.

Resulting Algorithm
To count the number of points on the hypersurface $f = 0$ in $\mathbf{P}^n(\mathbb{F}_{p^d})$ modulo p, we need all the terms of f^{p-1} having only exponents divisible by $p-1$.

Variation
To treat $W^2 = f(X_0, \ldots, X_n)$, we have to inspect the quadratic character. Modulo p this is given by the $\frac{p-1}{2}$-th power.
For the point count modulo p we have to sum $1 + f^{\frac{p-1}{2}}$.

Interpretation
We have a p-adic approximation of $\#V(\mathbb{F}_p)$ with precision 1.

Counting points over extensions

Setup
$q = p^d$ with p odd, $f \in \mathbb{Z}[X_0, \dots, X_n]$.

The quadratic character as a power

$$f^{q-1}(x_0, \dots, x_n) \in \{0, 1\} \text{ for } x_0, \dots, x_n \in \mathbb{F}_q$$
$$f^{\frac{q-1}{2}}(x_0, \dots, x_n) \in \{0, \pm 1\} \text{ for } x_0, \dots, x_n \in \mathbb{F}_q$$

The quadratic character as a norm

$$N(f^{p-1}(x_0, \dots, x_n)) = N(f(x_0, \dots, x_n))^{p-1} \in \{0, 1\} \text{ for } x_0, \dots, x_n \in \mathbb{F}_q$$
$$N(f^{\frac{p-1}{2}}(x_0, \dots, x_n)) = N(f(x_0, \dots, x_n))^{\frac{p-1}{2}} \in \{0, \pm 1\} \text{ for } x_0, \dots, x_n \in \mathbb{F}_q$$

Conclusion
We get the numbers of points over extensions without further powering. We just have to take norms.

Philosophy

Result from cohomology
The number of points is given by the alternating sum of the traces of Frobenius on cohomology.

Can we convert the above formula to the trace of a matrix?

Extending the base field should result in the trace of a power of the matrix.

Hasse-Witt Matrix

Polynomials and linear maps
$g \in K[X]$, $\deg(g) \le m(p-1)$. $m_g \colon K[X] \to K[X]$ multiplication by g.

Special monomials

$$B_0 := \{X^0, X^1, \dots, X^m\}$$
$$B_1 := \{X^0, X^p, \dots, X^{mp}\}$$
$$B_l := \{X^0, X^{p^l}, \dots, X^{mp^l}\}$$

Let A be the matrix of m_g with domain basis B_0 and co-domain basis B_1. I.e. we combine m_g with an inclusion and a projection map. (Hasse-Witt Matrix)

Observation
Then $\mathrm{Tr}(A)$ is the sum of all coefficients of monomials of g that have degree divisible by $(p-1)$.

Hasse-Witt Matrix II

Reminder

$$B_l := \{X^0, X^{p^l}, \dots, X^{mp^l}\}$$

Remark
The matrix A represents $m_{g(X^{p^{l-1}})}$ with domain basis B_{l-1} and co-domain basis B_l.

Theorem
The matrix A^l represents $m_{g(X^{p^{l-1}}) \cdots g(X^p) g(X)}$ with domain basis B_0 and co-domain basis B_l.

Proof
The projections remove only those terms in $g(X^{p^j}) \cdots g(X^p) g(X)$ that do not contribute to the final result. $\square$

p-adic point counting I

Algorithm
Given a variety $V: f = 0$ or $C: w^2 = f$.

- Compute $g := f^{p-1}$ or $g := f^{\frac{p-1}{2}}$.
- Use the coefficients to build up the Hasse-Witt matrix A for g.
- Compute trace of the d-th power of A.
- Derive $\#V(\mathbb{F}_{p^d})$ modulo p.

Summary
We can do the point count with a p-adic precision of one digit.

More p-adic precision – Using extrapolation

Binomial formula
Let $X = \pm 1 + pE$ with $E \in \mathbb{Z}_p$ be given.

$$\begin{aligned}
X &= \pm 1 + pE \\
X^2 &= 1 \pm 2pE + p^2E^2 \\
X^3 &= \pm 1 + 3pE \pm 3p^2E^2 + p^3E^3 \\
X^4 &= 1 \pm 4pE + 6p^2E^2 \pm 4p^3E^3 + p^4E^4 \\
X^5 &= \pm 1 + 5pE \pm 10p^2E^2 + 10p^3E^3 \pm 5p^4E^4 + p^5E^5
\end{aligned}$$

Linear combinations
E.g.

$$\frac{1}{8}(15X - 10X^3 + 3X^5) = \pm 1 + \frac{5}{2}p^3E^3 \pm 15p^4E^4 + 3p^5E^5$$

gives us ± 1 with a p-adic precision 3.

Outline of the point counting algorithm

Goal
Counting solutions of $w^2 = f(x, y, z)$ with $x, y, z \in \mathbb{F}_q^*$, $q = p^d$ and $f \in \mathbb{Z}[X, Y, Z]$:

Algorithm

- $g_k := f^{(2k-1)\frac{p-1}{2}} \in (\mathbb{Z}/p^n\mathbb{Z})[X, Y, Z]$ for $k = 1, \dots, n$.
- Build the Hasse-Witt matrices A_k corresponding to g_k.
- Compute traces of powers of A_k.
- Each trace results in an approximation with p-adic precision 1.
- Use the extrapolation method to get p-adic precision n.

Example

K3-surface

$$V: w^2 = x^6 + y^6 + z^6 + (x + 2y + 3z)^6$$

Count point over $\mathbb{F}_{p^d}$ for $p = 23, 29, 31, 37$ and $d = 1, \dots, 10$.

Number of points over $\mathbb{F}_{p^{10}}$: 171615583133452715196416060\2,
17699457615111095954223311589\3, 67179052881908387990751219623\2,
231224836666117093254655628265\6

Benchmark

- Computation of $\#V(\mathbb{F}_q)$ mod p^{11}
- Highest inspected power f_6^{378} of degree 2268 with 2575315 terms
- Matrices up to size 2080×2080
- Time per prime: 2 minutes
- 1.6 GB memory usage

Abstract K3 surfaces and Picard groups

K3 surfaces
A K3 surface is a simply connected algebraic surface with trivial canonical bundle.

Hodge diamond

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 1 & & 20 & & 1 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

Example
The double covers $w^2 = f_6(x, y, z)$ are examples of K3 surfaces.

Picard group and Cohomology
For a K3 surface S over $\mathbb{C}$ we have the cycle map $\mathrm{Pic}(S) \hookrightarrow \mathrm{H}^{1,1}(S, \mathbb{C})$. Thus, $\mathrm{Pic}(S)$ is a free $\mathbb{Z}$ module of rank $1, \ldots, 20$.

Accessing the Picard group via Galois representations

The Picard group as a Galois module
The Picard group of a K3 surface S (defined over $\mathbb{Q}$) will be defined over some number field L. Thus, $\mathrm{Pic}(S)$ will be a linear representation of $\mathrm{Gal}(L/\mathbb{Q})$. All the eigenvalues of this representation will will be roots of unity.

The étale situation
Galois subrepresentation $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p}) \hookrightarrow \mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l(1))$.

Interpretation
The number of Frobenius eigenvalues on $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l(1))$ that are roots of unity is an upper bound for the Picard rank of $S_{\overline{\mathbb{F}}_p}$.

Remark
By the Tate conjecture this bound is sharp. (Proved for K3 surfaces by Swinnerton-Dyer, Nygaard, Pera, Charles)

The Artin-Tate formula

Notation

- V a K3 surface over $\mathbb{F}_q$.
- ρ and Δ the rank and the discriminant of $\mathrm{Pic}(V)$.
- Φ the characteristic polynomial of Frobenius on H^2.
- $\mathrm{Br}(V)$ the Brauer group. (Order is finite and a square).

$$|\Delta| = \frac{\lim\limits_{T \to q} \frac{\Phi(T)}{(T-q)^\rho}}{q^{21-\rho} \# \mathrm{Br}(V)}$$

The Picard rank algorithm

Input:
A K3 surface S defined over $\mathbb{Q}$.

Algorithm: (Upper bound of geometric Picard rank)

- For some primes of good reduction of S compute the characteristic polynomial of the Frobenius on étale cohomology by point counting.
- Count the roots of the form $p\zeta_n$ for each polynomial.
- The minimum m is a rank bound.
- If the minimum is reached multiple times use the Artin Tate formula to compute the square classes of the discriminants of the Picard groups of the reductions.
- In case several square classes show up, $m - 1$ is a rank bound.

Remark
This algorithm was introduced by van Luijk and Kloosterman.

Testing the Picard rank algorithm I

Determinantal quartics

A generic quartic of the form

$$0 = \det \begin{pmatrix} 0 & l_1 & l_2 & l_3 \\ l_1 & 0 & l_4 & l_5 \\ l_2 & l_4 & 0 & l_6 \\ l_3 & l_5 & l_6 & 0 \end{pmatrix}$$

has 14 singularities of type A_1. For random linear forms $l_1, \ldots, l_6$ we expect the Picard rank to be 15.

Degree 2 models

Let P be a singular point of a quartic surface S in $\mathbb{P}^3$. A line through P will intersect S in two other points. This will result in degree 2 model of S blown up at P.

Testing the Picard rank algorithm II

Test

Choose at random 1600 determinantal quartics and all primes below 250. Run the Picard rank bound algorithm in all cases.

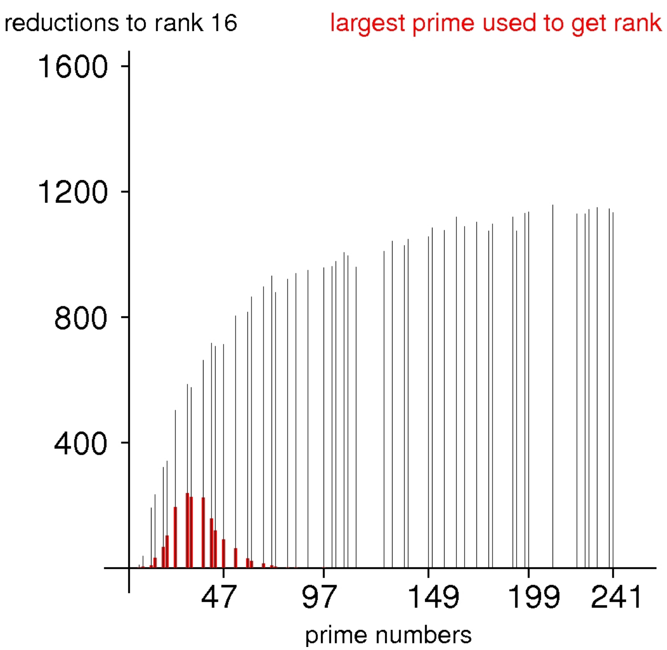
Expectation

Most of the surfaces have Picard rank 15.

Result

- 1503 surfaces have rank 15.
- 93 surfaces have rank 16.
- 3 surfaces have rank 17.
- 1 surface has rank 18.

We have additional lines and conics on the 97 surfaces with rank > 15.



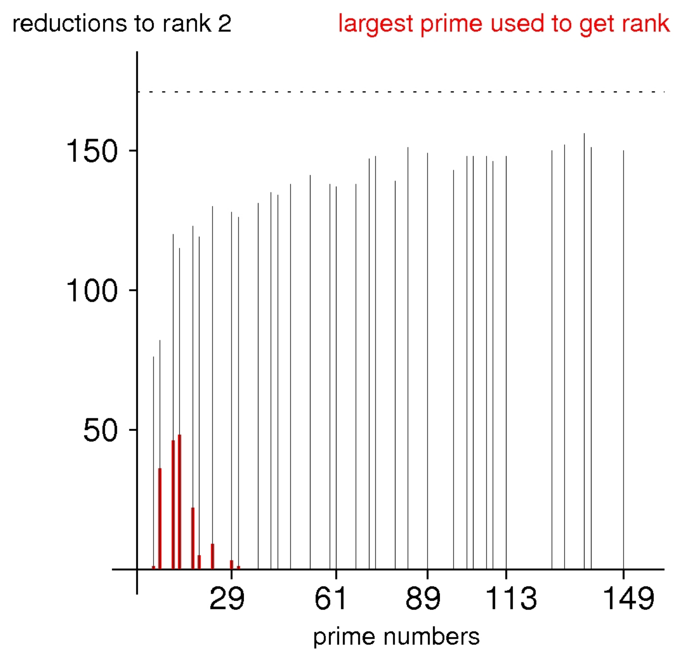
Testing the Picard rank algorithm III

Sample

200 sextic curves with coefficients $\{0, \pm 1\}$.
171 of them turned out to be smooth. We inspect only thouse.

Result

- Two of them have a splitting line resulting in Picard rank 2.
- All the others have Picard rank 1.



Ordinary and non ordinary-primes

Definition
The reduction modulo p of a variety V is called ordinary, iff

$$\#V(\mathbb{F}_p) \not\equiv 1 \bmod p\,.$$

Observation
To detect ordinary primes we need the point count with p-adic precision 1.

Test
We have to compute the coefficient of $(XYZ)^{p-1}$ modulo p in $f_6^{\frac{p-1}{2}}$.

Remark
This can be done without computing all the coefficients of the power by using the linear relations between the coefficients of f^n and f^{n+1}.

(Non-)ordinary primes of elliptic curves

Setup
Let E be an elliptic curve over $\mathbb{Q}$.

Recall
A prime p is called ordinary if $\#E(\mathbb{F}_p) \not\equiv 1 \bmod p$.

Theorem
In case E has complex multiplication, ordinary primes have density $\frac{1}{2}$.
All the inert primes of the CM-field are non-ordinary.

Theorem (Serre)
In case E does not have complex multiplication, ordinary primes have density 1.

Non-ordinary primes: Example

Sample
The 1600 singular quartics from above.

Compute
Non-ordinary primes up to 1000. Takes 6 seconds for each surface.

Result

- The surfaces have 0 to 7 non-ordinary primes.
- 154 out of 167 primes occur as non-ordinary at least once.

Idea
Search for examples with many non-ordinary primes.

Example 1

Equation

$$S\colon w^2 = xyz(7x^3 - 7x^2y + 49x^2z - 21xyz + 98xz^2 + y^3 - 7y^2z + 49z^3)$$

Properties

- The cubic is the norm of a linear form.
- We have 15 singularities of type A_1.
- Surface has geometric Picard rank 16.
- Not Kummer.
- Bad primes: 2,7

Conjecture
Surface has complex multiplication with

$$K = \mathbb{Q}(i, \zeta_7 + \zeta_7^{-1}) = \mathbb{Q}(\zeta_{28} + \zeta_{28}^{13}) \cong \mathbb{Q}[X]/(X^6 + 5X^4 + 6X^2 + 1)\,.$$

Observation
The L-series of S is similar to a Hecke L-series attached to K.

Example 2

Equation

$$S\colon w^2 = xyz(x^3 + 6x^2z - 3xy^2 - 3xyz + 9xz^2 + y^3 - 3yz^2 + z^3)$$

Properties

- The cubic is the norm of a linear form.
- We have 15 singularities of type A_1.
- Surface has geometric Picard rank 16.
- Not Kummer.
- Bad primes: 2, 3

Conjecture
Surface has complex multiplication with

$$K = \mathbb{Q}(i, \zeta_9 + \zeta_9^{-1}) = \mathbb{Q}(\zeta_{36} + \zeta_{36}^{17}) \cong \mathbb{Q}[X]/(X^6 + 6X^4 + 9X^2 + 1)\,.$$

Observation
The L-series of S is similar to a Hecke L-series attached to K.

Numerical evidence – primes up to 997

Common properties of both examples:

non-ordinary primes
$\#S(\mathbb{F}_p) \equiv 1 \bmod p \iff$ inertia degree of p in K is bigger than one.

Picard rank of reduction

- Reduction has Picard rank 16 or 22.
- Rank 22 $\Leftrightarrow$ inertia degree of p in K is even $\Leftrightarrow p \equiv 3 \bmod 4$.

Frobenius eigenvalues at ordinary prime

- p ordinary $\Rightarrow$ Frobenius eigenvalues are in K.
- Let $(\mathfrak{p})$ be a prime in K above p.
- One of $\pm p\frac{\overline{\mathfrak{p}}}{\mathfrak{p}}$ is a Frobenius eigenvalue.

Determination of sign

Example 1

- $S\colon w^2 = xyz(7x^3 - 7x^2y + 49x^2z - 21xyz + 98xz^2 + y^3 - 7y^2z + 49z^3)$
- $\mathfrak{p}_2$ and $\mathfrak{p}_7$ primes in $K = \mathbb{Q}(\zeta_{28} + \zeta_{28}^{13})$ above 2 and 7.

$$G := (\{x \in \mathcal{O}/(2\mathfrak{p}_2\mathfrak{p}_7) \mid x \equiv 1 \bmod 2, x \notin \mathfrak{p}_7\}, \cdot)\,.$$

- Let p be an ordinary prime of S and $(\mathfrak{p})$ a prime of K above p.
- All Frobenis eigenvalues at p are of the form $\pm p\frac{\overline{\mathfrak{p}}}{\mathfrak{p}}$.
- The sign is determined by a coset of a subgroup of G.

Example 2

- $S\colon w^2 = xyz(x^3 + 6x^2z - 3xy^2 - 3xyz + 9xz^2 + y^3 - 3yz^2 + z^3)$
- $K = \mathbb{Q}(\zeta_{36} + \zeta_{36}^{17})$
- $G := (\{x \in \mathcal{O}/(2\mathfrak{p}_2) \mid x \equiv 1 \bmod 2\}, \cdot) \cong (\mathbb{Z}/2\mathbb{Z}, +)^3$
- The signs of the Frobenius eigenvalues at ordinary primes are given by an index 2 subgroup of G.

Summary

Point Counting
p-adic approach results in a practical point counting algorithm for K3 surfaces of degree 2.

Picard group computation
We can compute Picard ranks of random examples.

Special examples
We found examples of real or complex multiplication by $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{13}), \mathbb{Q}(\zeta_{28} + \zeta_{28}^{13}), \mathbb{Q}(\zeta_{36} + \zeta_{36}^{17})$.

Observation
All examples of K3 surfaces with real multiplication found have the property:

Endomorphism field $\subset$ Field of definition of Picard group