

On the Shioda Conjecture for Diagonal Projective Varieties over Finite Fields

Matthew Lerner-Brecher, Benjamin Church, Chunying
Huangdai, Ming Jing, Navtej Singh
Advisors: Daniel Litt, Alex Perry, Raymond Cheng

2018.08.01

Definitions and Motivations

Let p be a prime and \mathbb{F}_p the finite field of order p .

Definition

Affine space, denoted by \mathbb{A}^n is defined by

$$\mathbb{A}^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{F}_p\}.$$

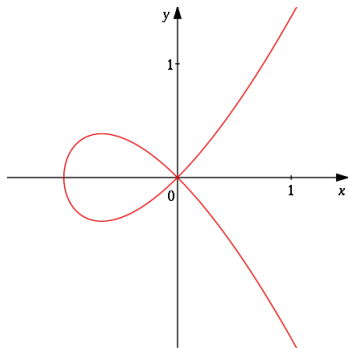
Definition

An **affine variety** is a subset of affine space on which a system S of polynomials vanish:

$$Z(S) = \{P \in \mathbb{A}^n \mid \forall f \in S : f(P) = 0\}.$$

Examples over \mathbb{R}

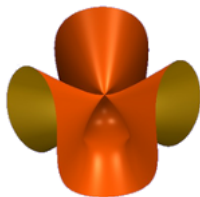
The zero set of the polynomial $y^2 = x^2(x + 1)$ in \mathbb{A}^2 gives the cubic curve¹,



¹Wikimedia Commons

Examples over \mathbb{R}

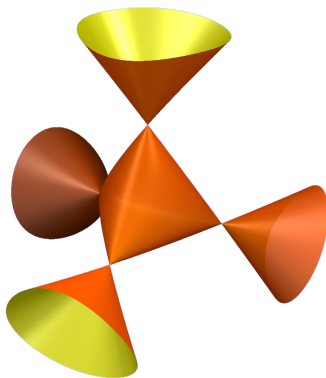
The zero set of the polynomial $z^2(z + 4) + y(y - \sqrt{3})x)(y + \sqrt{3}x)$ in \mathbb{A}^3 gives the cubic surface²,



²Richard Morris SingSurf

Examples over \mathbb{R}

The zero set of the polynomial $4(x^2 + y^2 + z^2) + 16xyz - 1$ in \mathbb{A}^3 gives the cubic surface³,



Definitions and Motivations

Definition

Projective space, denoted \mathbb{P}^n , is defined as $\mathbb{A}^{n+1} \setminus \{0\}$ under the equivalence relation

$$(x_0, \dots, x_r) \sim (\lambda x_0, \dots, \lambda x_r)$$

for $\lambda \in \mathbb{F}_p^\times$.

Definition

A **projective variety** in \mathbb{P}^n is the zero set of a system of homogeneous polynomials in $n + 1$ variables.

Note: Homogeneity is required so that $f(\lambda x) = \lambda^n f(x)$ and thus $f(x) = 0$ is well-defined.

Definitions and Motivations

Definition

A variety X defined by a diagonal equation, i.e. an equation of the form

$$x_0^{m_0} + \cdots + x_r^{m_r}$$

is called a **diagonal variety**.

Example

A patch of the diagonal hypersurface $w^5 + x^5 + y^5 + z^5 = 0$ in \mathbb{P}^3 can be visualized as:



Definitions and Motivations

Definition

A variety X is **unirational** if there exists a dominant rational map $\mathbb{P}^n \dashrightarrow X$. Such a map **parametrizes** X .

Remark

Intuitively, a dominant rational map is a map given by rational functions component-wise which is defined at “almost every” point of \mathbb{P}^n and hits “almost every” point of X .

Example

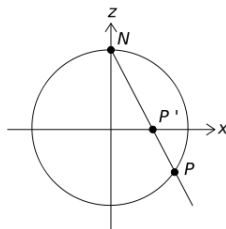
The circle as an affine variety defined by

$$x^2 + y^2 - 1$$

is unirational over \mathbb{Q} . It can be parameterized by a line via stereographic projection:

$$t \mapsto \left(\frac{2t}{t^2 + 1}, \frac{t^2 - 1}{t^2 + 1} \right).$$

4



Definitions and Motivations

Definition

A variety X is **rational** if there exist dominant rational maps $\mathbb{P}^n \dashrightarrow X$ and $X \dashrightarrow \mathbb{P}^n$ which are inverses when both are defined.

Remark

We showed the diagonal variety defined by

$$w^5 + x^5 + y^6 + z^6$$

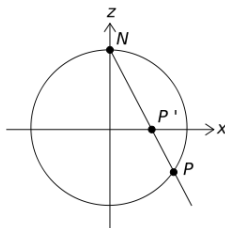
is rational over \mathbb{F}_p for all primes p .

Example

The circle $x^2 + y^2 = 1$ shown before is actually rational, not only unirational. Stereographic projection and its inverse are given by:

$$t \mapsto \left(\frac{2t}{t^2 + 1}, \frac{t^2 - 1}{t^2 + 1} \right), \quad (X, Y) \mapsto \frac{X}{1 - Y}.$$

5



Unirationality and Rationality

Remark

rational \implies unirational.

Though the previous example turned out to be unirational and rational, this does not always happen. For example,

Theorem (Clemens, Griffiths)

All smooth cubic hypersurfaces in \mathbb{P}^4 are unirational but none are rational.

The Zeta Function

Definition

The **zeta function** of a variety X defined over \mathbb{F}_p for prime p is

$$\zeta_X(T) = \exp\left(\sum_{k=1}^{\infty} N_k \frac{T^k}{k}\right)$$

where

$$N_k = \#\{(x_0, x_1, \dots, x_n) \in X \mid x_i \in \mathbb{F}_{p^k}\}$$

The Weil Conjectures

Theorem (Deligne, Dwork, Grothendieck)

The zeta function ζ_X of a variety over \mathbb{F}_p is a rational function. That is, it can be written in the form

$$\frac{P(T)}{Q(T)}$$

for integer polynomials P, Q . Furthermore, all of the roots of P, Q are of the form

$$p^{i/2}\epsilon$$

where $|\epsilon| = 1$.

Supersingularity

Definition

A variety X is called **supersingular** if all roots of its zeta function have unit part ϵ equal to a root of unity.

Supersingularity Example

Example

The zeta function $\zeta_X(T)$ for $w^4 + x^4 + y^4 + z^4$ over \mathbb{F}_3 is

$$\frac{-1}{(T-1)(9T-1)(3T-1)^{12}(3T+1)^{10}}$$

so it is supersingular.

Example

The zeta function $\zeta_X(T)$ for the same equation over \mathbb{F}_5 is

$$\frac{-1}{(T-1)(25T-1)(5T-1)^8(5T+1)^{12}(25T^2+6T+1)}$$

so it is not supersingular.

Another Example

We discovered that the variety X defined by

$$w^a + x^b + y^c + z^d$$

over \mathbb{F}_p is supersingular where

$$a = 345032748952781$$

$$b = 982348934290403$$

$$c = 2415229242669467$$

$$d = 6876442540032821$$

$$p = 1091056078844320245619195255131719$$

Shioda's Conjecture

Theorem (Shioda)

Let X be a smooth hypersurface in \mathbb{P}^3 . If X is unirational, then it is supersingular.

Conjecture (Shioda)

Let X be a smooth hypersurface in \mathbb{P}^3 . If X is supersingular, then it is unirational.

Shioda's Result

Definition

Let $F_{m,p}^r$ denote the Fermat variety defined by

$$x_0^m + \cdots + x_r^m$$

over \mathbb{F}_p .

Theorem (Shioda)

Suppose that $m \geq 4$. Then $F_{m,p}^r$ is supersingular if and only if

$$p^v \equiv -1 \pmod{m}$$

for some $v \in \mathbb{Z}$.

Theorem (Shioda)

A Fermat surface $F_{m,p}^3$ is unirational if and only if it is supersingular.

Code/Empirical

Approach

We wrote code using Sage to instantiate affine and projective varieties over various finite fields, find their zeta functions, and determine supersingularity. Analyzing patterns in the generated data helped motivate our conjectures.

Software package

We hope to publish a software package based on our development.

Methodology: Stickelberger's Theorem

Using Gaussian sums and Stickelberger's Theorem, we derived an efficient numerical condition for supersingularity.

Theorem (—)

The variety X defined by the equation,

$$a_0x_0^{n_0} + \cdots + a_rx_r^{n_r}$$

is supersingular over \mathbb{F}_p if and only if

$$\sum_{i=0}^r \sum_{j=0}^{f-1} \{\mu\alpha_i p^j\} = \frac{f(r+1)}{2}$$

for each $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $\alpha \in A(X)$ where $m = \text{lcm}(n_i)$, $f = \text{ord}_m(p)$, and

$$A(X) = \left\{ (\alpha_0, \dots, \alpha_r) \mid 0 < \alpha_i < 1 \text{ and } \alpha_i n_i \in \mathbb{Z} \text{ and } \sum_{i=0}^r \alpha_i \in \mathbb{Z} \right\}$$

Methodology: Reduction Maps

We can relate the supersingularity of one variety to another.

Proposition

Suppose there is a surjective morphism $X \rightarrow Y$. If X is supersingular, then Y is supersingular.

Corollary

Let X and Y be diagonal varieties defined by

$$x_0^{a_0} + \cdots + x_r^{a_r} \quad y_0^{b_0} + \cdots + y_r^{b_r}$$

respectively. If $b_i | a_i$ for $0 \leq i \leq r$, then there is a surjective morphism $X \rightarrow Y$. In particular, if X is supersingular, then Y is supersingular.

Our Results

A Generalization of Shioda's Condition

Definition

Let X be a diagonal variety. Define the **LCM extension** X_ℓ and **GCD reduction** X_g of X by

$$X_\ell = F_{\text{lcm}(n_i)}^r \text{ and } X_g = F_{\text{gcd}(n_i)}^r$$

respectively. Then there exist surjective morphisms

$$X_\ell \longrightarrow X \longrightarrow X_g$$

Applying Shioda's theorem, we get the following.

Theorem (—)

Let X be a diagonal variety. Then X is supersingular over \mathbb{F}_p if there exists $v \in \mathbb{Z}$ such that $p^v \equiv -1 \pmod{\text{lcm}(n_i)}$ and X is not supersingular if for all $v \in \mathbb{Z}$ we have $p^v \not\equiv -1 \pmod{\text{gcd}(n_i)}$.

A Generalization of Shioda's Condition

However, these conditions are not sufficient!

On Special Families

Theorem (—)

Let a, b be coprime integers. Then the variety defined by the equation

$$w^a + x^a + y^b + z^b$$

is rational in characteristic zero and thus supersingular over \mathbb{F}_p for every prime p .

Example

The variety defined by

$$w^5 + x^5 + y^6 + z^6$$

is rational.

New Supersingular Varieties

Using our code, we managed to come up with some previously unknown families of supersingular varieties! For example the variety

$$w^7 + x^{13} + y^{21} + z^{39}$$

over \mathbb{F}_{19} and the variety

$$w^{385} + x^5 + y^7 + z^{11}$$

over \mathbb{F}_{17} .

Two Important Families

More generally, we found new results pertaining to the supersingularity of two families of varieties:

$$w^a + x^b + y^{ac} + z^{bc}$$

and

$$w^{abc} + x^a + y^b + z^c$$

where a, b, c are primes. We studied these families for two reasons:

- 1) These were the first examples of varieties we found that didn't satisfy the converse to the generalization of Shioda's theorem.
- 2) Many diagonal surfaces can be projected down to one of these two families, so understanding them would give us a lot of general information!

Conjecture 1

Let a, b, c be powers of distinct primes and let p be a prime. The variety X over \mathbb{F}_p defined by the equation

$$w^a + x^b + y^{ac} + z^{bc}$$

is supersingular if and only if $p^v \equiv -1 \pmod{abc}$ for some v or if $a, b, p \equiv 1 \pmod{c}$ and p is a primitive root modulo both a, b .

Conjecture 1: Partial Result

We have proven the \Rightarrow part of this conjecture.

Theorem (—)

Let a, b, c be powers of distinct primes and let p be a prime. The variety X over \mathbb{F}_p defined by the equation

$$w^a + x^b + y^{ac} + z^{bc}$$

is supersingular if $p^v \equiv -1 \pmod{abc}$ for some v or if $a, b, p \equiv 1 \pmod{c}$ and p is a primitive root modulo both a, b .

Remark

This result gives an infinite family of varieties and an infinite number of primes for each one which do not satisfy the sufficient condition given by the generalization of Shioda's condition.

Conjecture 2

Let a, b, c, p be distinct primes. Let

$f = \text{ord}_{abc}(p)$, $f_1 = \text{ord}_a(p)$, $f_2 = \text{ord}_b(p)$, $f_3 = \text{ord}_c(p)$ and let $2^r, 2^s, 2^t$ be the largest powers of 2 dividing f_1, f_2, f_3 , respectively.








If $r \geq s \geq t$, the variety X defined by the equation

$$w^{abc} + x^a + y^b + z^c$$

is supersingular if and only if $p^{f/2} \equiv -1 \pmod{abc}$ or if the below conditions 1 and 2, and either of 3 or 4 hold.

1. $r > s$ and $\frac{f_1}{2^r}, \frac{f_2}{2^s}, \frac{f_3}{2^t}$ are pairwise coprime.
2. $f_2 = b - 1, f_3 = c - 1$ and there exists an integer k such that $p^k \equiv c \pmod{ab}$
3. $s = t = 1$ and there exists an integer v such that $p^v \equiv b \pmod{ac}$
4. $s = 2, t = 1, f_1 = a - 1$, and there exists an integer v such that $p^v \equiv a \pmod{bc}$ or $p^v \equiv b \pmod{ac}$

References

-  S. Chowla, On Gaussian Sums, *Proceedings of the National Academy of Sciences*, 48 (7), 1127-8, 1962.
-  R. Evans, Generalizations of a Theorem of Chowla on Gaussian Sums, *Houston Journal of Mathematics*, 3, 1977.
-  N. Koblitz, p-adic variation of the zeta-function over families of varieties defined over finite fields, *Compositio Mathematica*, 31, 119-218, 1975.
-  S. Lang, *Algebraic Number Theory*, Springer, 1994.
-  T. Shioda, An example of Unirational Surfaces in Characteristic p , *Mathematische Annalen*, 221, 233-236, 1974.
-  T. Shioda, T. Katsura, On Fermat Varieties, *Tohoku Math Journal*, 31, 97-115, 1979.
-  A. Weil, Numbers of Solutions of Equations in Finite Fields, *Bulletin of the American Mathematical Society*, 55 (5), 497-508, 1949