Background

The immergence of quantum computing, at scale, thretens to provide an efficient method of attack for current classical cryptosystems based on "trap door" problems such as discrete log. Quantum algorithms which efficiently solve the discrete log problem have been demonstrated theoretically at at small scale [https://arxiv.org/abs/1702.00249, .https://science.sciencemag.org/content/351/6277/1068.abstrac

The vulnerabilities of these cryptosystems to quantum cryptoanalytic attack poses a major threat to the security of information technology used both for commerce and national defense. Furthermore, standard cryptosystems based elliptic curve suffer similar vulnerabilities to attack by a quantum computer [https://arxiv.org/abs/quant-ph/0301141].

Moving from cryptosystems based of on pointwise logarithm problems on a single elliptic curve to protocolls which instead utilize the isogeny graph between multiple elliptic curves thwarts quantum cryptoanalytic attack based on Shor's algorithm.

A. Rostovtsev and A. Stolbunov constructed such a key-sharing isogeny-based protocol which was suggested to be resistent to attack by quantum cryptoanaylsis [https://eprint.iacr.org/2006/145.pdf].

However, A. Childs, D. Jao and V. Soukharev demonstrated (assiming the Generalized Riemann Hypothesis) a subexponential quantum attack against isogeny-based cryptosystems which employ ordinary elliptic curves [https://arxiv.org/abs/1012.4019]. However, over finite fields, there exist so called *supersingular* elliptic curves whose endomorphism rings are noncommutative and thus resist the methods of Childs et al.

Indeed, L. de Feo and J. Plut proposed Diffie-Hellman type key-exchange protocol based on finding isogenies between supersingular elliptic curves which is belived to be resistent to attack by quantum cryptoanaylsis [https://eprint.iacr.org/2011/506.pdf]

The Lüroth Problem. A central question in birational geometry is to determine the structure of *rational* varieties, those birationally equivalent to $\mathbb{P}^n$. However, this notion is too restrictive to capture the behavior of important objects such as moduli spaces. More generally, we say a variety X is *unirational* if there exists a dominant rational map $\mathbb{P}^n \dashrightarrow X$. J. Lüroth showed [1] that the notions of rationality and unirationality coincide for algebraic curves. This observation sparked the Lüroth problem asking if rationality and unirationality are equivalent for higher dimensional varieties. Intuitively, the Lüroth problem asks: if X can be parametrized almost everywhere by rational functions, can this parametrization be made (generically) one-to-one?

The answer is affirmative for surfaces over a field of characteristic zero. This follows from Castelnuovo's criterion using the fact that field extensions in characteristic zero are separable. Therefore unirational dominations are generically étale which implies that any variety dominated by $\mathbb{P}^n$ must have vanishing canonical invariants and thus must be rational by Castelnuovo's theorem. However, in positive characteristic, this argument fails due to the existence of inseparable maps and, consequently, counterexamples to the Lüroth problem exist. The best known are due to Zariski [2], defined by equations of the form $z^p = f(x, y)$, and Shioda [3], for certain Fermat surfaces of the form $x^n + y^n = z^n$. However, unlike the case of rational surfaces in which Castelnuovo's criterion applies, there are no known numerical techniques for detecting unirationality.

Supersingular Varieties. Supersingularity refers to multiple closely related[1] cohomological phenomena which occur only in positive characteristic. Let X_0 be a smooth proper variety over the finite field $\mathbb{F}_q$ and $X = X_0 \times \overline{\mathbb{F}}_q$. For a prime $\ell \nmid q$ we write $H^i(X_{\text{ét}}, \mathbb{Q}_\ell)$ for the ℓ-adic étale cohomology of X in degree i. An even cohomology class $\alpha \in H^{2r}(X_{\text{ét}}, \mathbb{Q}_\ell)$ is *an algebraic cycle* if α is a linear combination (with $\mathbb{Q}_\ell$ coefficients) of cycles $[Z]$ corresponding to codimension-r subvarieties $Z \subset X$. The subspace of algebraic cycles is of great importance in contemporary algebraic geometry being the central object of the Hodge and Tate conjectures. For smooth proper surfaces, $H^0(X_{\text{ét}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$

[1] by various conjectures, for instance the Tate conjectures

and $H^4(X_{\text{ét}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-2)$ are immediately generated by algebraic cycles so we are primarily interested in the algebraic cycles in $H^2(X_{\text{ét}}, \mathbb{Q}_\ell)$ which correspond to $\text{NS}(X) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ where $\text{NS}(X)$ is the Néron-Severi group defined as the group of line bundles up to algebraic equivalence. Furthermore, the Picard number is its rank: $\rho(X) = \text{rank}(\text{NS}(X))$. Therefore, the even cohomology of a smooth proper surface X is generated by algebraic cycles iff $\rho(X) = b_2(X) := \dim_{\mathbb{Q}_\ell} H^2(X_{\text{ét}}, \mathbb{Q}_\ell)$ motivating Shioda's definition:

Definition. A smooth proper surface X over $\mathbb{F}_q$ is *Shioda supersingular* if its Picard number equals its second Betti number: $\rho(X) = b_2(X)$.

Taking into account the Galois action, $[Z]$ is naturally an element of $H^{2r}_{\text{ét}}(X, \mathbb{Q}_\ell(r))$ where coefficients are twisted r times by the cyclotomic character. Therefore, the Galois group acts on algebraic cycles via multiplication by roots of unity. According to the Tate conjecture, this condition on the Galois action exactly characterizes algebraic cycles.

Definition. A smooth proper variety over $\mathbb{F}_q$ is *supersingular* if, for each i, the eigenvalues of Frobenius on $H^i(X_{\text{ét}}, \mathbb{Q}_\ell)$ are $q^{i/2}$ times a root of unity.

Assuming the Tate conjecture, we see that supersingularity and Shioda supersingularity coincide for smooth proper surfaces. However, the latter definition is more easily verified algorithmically. According to Grothendieck's proof of the Weil conjectures, the Zeta function is a rational function in terms of the Frobenius F action on compactly supported étale cohomology,

$$\zeta_X(t) := \exp\left(\sum_{k=0}^{\infty} \#\left[X(\mathbb{F}_{q^k})\right] \frac{t^k}{k}\right) = \prod_{i=0}^{2n} \det\left(\text{id} - tF^* \mid H^i_c(X_{\text{ét}}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}}$$

and thus $\zeta_X(t)$ has roots and poles of the form $(1 - \alpha t)$ with α the eigenvalues of Frobenius. In particular, since the zeta function $\zeta_X(s)$ may be computed explicitly, we can determine if X is supersingular by inspecting its roots.

The Conjecture of Shioda. We would like to find sufficient computable invariants to determine unirationality. Since Frobenius action is preserved under rational domination, unirationality implies supersingularity. In important known cases the converse holds as well. For example, the converse is proven for K3 surfaces[2] [4], Kummer surfaces [5], and Fermat surfaces [6]. Due to these examples, Shioda formulated [5] the following conjecture,

Conjecture. Let X be a surface over $\mathbb{F}_q$ with $\pi_1^{\text{ét}}(X) = 0$. Then X is unirational if and only if X is Shioda supersingular.

Research Plan

I plan to investigate the Shioda conjecture in special case of diagonal weighted-projective hypersurfaces. Explicitly, these are hypersurfaces in $\mathbb{P}(q_0, q_1, q_2, q_3)$ cut out by an equation of the form,

$$a_0 X_0^{n_0} + a_1 X_1^{n_1} + a_2 X_2^{n_2} + a_3 X_3^{n_3} = 0$$

These surfaces are well-suited to studying the Shioda conjecture because, by a seminal result of André Weil [7], their zeta functions may be efficiently computed in terms of Jacobi sums. I propose the following broad goals:

(1) employ a computer search to find new examples of supersingular hypersurfaces
(2) classify these explicit examples into infinite families of supersingular examples
(3) determine which of these examples are unirational.

[2] A. J. de Jong has privately informed me that an error has been identified in Liedtke's proof, however the result is still believe to hold.

Of these goals, the third presents the biggest challenge since there are not good tools available to determine unirationality. It may be more tractable to determine the density of rational curves on a surface. We say a variety is rationally-connected if each pair of points lies on a rational curve. We expect unirational surfaces to be rationally connected and non-unirational surfaces to have finitely many rational curves. Therefore, investigating the families of rational curves on X gives insight into this problem. To address this we use methods of (USE METHODSSS)

Intellectual Merit

In the Columbia 2018 REU [8], my team and I, working on a related problem, successfully implemented Weil's method completing goal (1) and gave a partial answer for (2). In particular, we discovered two infinite families of supersingular diagonal hypersurfaces which have the form $(n_0, n_1, n_2, n_3) = (p, q, ps, qs)$ for distinct primes p, q such that $p, q \equiv 1 \mod s$ and of the form $(n_0, n_1, n_2, n_3) = (p, q, r, pqr)$ for distinct primes pqr. We proved that surfaces of these forms are supersingular when the characteristic satisfies an explicit numerical criterion. Because any surface dominated by a supersingular surface is again supersingular, classifying which diagonal surfaces whose exponents are combinations of a small number of primes are supersingular will provide information about a much wider class of diagonal surfaces.

Due to Shioda [6], we already know an infinite family of examples, namely the Fermat surfaces such that $p^\nu \equiv -1 \mod n$ and any diagonal surface which may be dominated by a Fermat surface of this form. However, these examples are already known to be unirational. Thus, the real success of our methods is the discovery of additional infinite families of supersingular surfaces which are not of the above form.

Over the summer of 2020, I worked with Prof. Aise Johan de Jong to determine if these new examples are unirational as the Shioda conjecture would imply. Although this has not produced a concrete answer, we have reduced the question of rational-connectedness to one about certain loci in the moduli space of cyclic 3-covers of $\mathbb{P}^1$ which we hope to be more tractable.

Broader Impact

One of the main reasons Shioda's conjecture remains mysterious is the dearth of known examples of supersingular or unirational surfaces. Completion of this work will either disprove Shioda's conjecture or provide new infinite families of positive examples. In either case, this will greatly improve our understanding of the phenomena of nonrational unirational surfaces in positive characteristic. Furthermore, diagonal hypersurfaces provide an underutilized source of examples and the proposed classification would elucidate these examples for future researchers and produce a large well-understood class of supersingular surfaces. Lastly, examples of supersingular varieties have recently become of significant interest for designing cryptosystems. The primary example is supersingular isogeny-based cryptography which is intended to be resistant to attacks by quantum cryptoanalysis [9]. These methods employ supersingular elliptic curves defined over finite fields and isogenies between these curves as an analogue of the discrete log problem to implement key-exchange or other cryptographic protocols.

References

[1] Jakob Lüroth. Beweis eines satzes über rationale curven. *Mathematische Annalen*, 9(2):163–165, 1875.

[2] Oscar Zariski. On castelnuovo's criterion of rationality $p_a = p_2 = 0$ of an algebraic surface. *Illinois J. Math.*, 2(3):303–315, 09 1958.

[3] Tetsuji Shioda. An example of unirational surfaces in characteristic p. *Mathematische Annalen*, 211(3):233–236, 1974.

[4] Christian Liedtke. Supersingular k3 surfaces are unirational. *Inventiones mathematicae*, 200(3):979–1014, 2015.

[5] Tetsuji Shioda. Some results on unirationality of algebraic surfaces. *Mathematische Annalen*, 230(2):153–168, 1977.
[6] Tetsuji Shioda and Toshiyuki Katsura. On fermat varieties. *Tohoku Math. J. (2)*, 31(1):97–115, 1979.
[7] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55(5):497–508, 05 1949.
[8] B. Church, C. Huangdai, M. Jing, M. Lerner-Brecher, and N. Sing. On the shioda conjecture for diagonal projective varieties. *Columbia REU Final Presentations*, 2018.
[9] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.