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 rationality and unirationality coincide for algebraic curves. Likewise, the Lüroth problem asks if rationality and unirationality are equivalent for higher dimensional varieties or, informally, 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 and the fact that field extensions in characteristic zero are separable so generically finite dominations are generically étale. However, in positive characteristic, this argument fails due to the existence of inseparable maps and, consequently, counterexamples to the Lüroth problem exist. 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 closely related cohomological phenomena which occur only in positive characteristic. Let X_0 be a smooth proper variety over $\mathbb{F}_q$ and $X = X_0 \times \overline{\mathbb{F}}_q$. For a prime $\ell \not| \, q$ we write $H^i(X_{\text{ét}}, \mathbb{Q}_\ell)$ for the ℓ-adic étale cohomology of X. An even cohomology class $\alpha \in H^{2r}(X_{\text{ét}}, \mathbb{Q}_\ell)$ is *an algebraic cycle* if α is a $\mathbb{Q}_\ell$-linear combination of cycles $[Z]$ corresponding to codimension-r subvarieties $Z \subset X$. For smooth proper surfaces, we need only consider algebraic cycles in $H^2(X_{\text{ét}}, \mathbb{Q}_\ell)$ which are linear combinations of divisors. This space corresponds 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. Thus even cohomology of X is generated by algebraic cycles if the Picard number $\rho(X) = \text{rank}(\text{NS}\,(X))$ equals the second betti number $b_2(X) := \dim_{\mathbb{Q}_\ell} H^2(X_{\text{ét}}, \mathbb{Q}_\ell)$ in which case we say that X is *Shioda supersingular.* 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 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. Thus, X_0 is *supersingular* if 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, supersingularity and Shioda supersingularity coincide. However, the second notion can be more directly 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.

We would like to find sufficient computable invariants to determine unirationality. Since Frobenius action is preserved under finite domination, unirationality implies supersingularity. Shioda conjectured [2] that the converse holds and thus supersingularity is such an invariant:

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 for diagonal weighted-projective hypersurfaces. Explicitly, these are hypersurfaces in $\mathbb{P}(q_0, q_1, q_2, q_3)$ cut out by an equation:

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

These surfaces are well-suited to studying the Shioda conjecture because, by a seminal result of André Weil [3], 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.

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 these surfaces. 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. I intend to continue my efforts on this related problem attempting to adapt the methods of [4] based on Bogomolov's finiteness results.

Intellectual Merit. In the Columbia 2018 REU [5], my team and I 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.

From Shioda's work [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. Johan de Jong to determine if these new examples are unirational as the Shioda conjecture would imply. 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 reason 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 [7]. 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] Tetsuji Shioda. Some results on unirationality of algebraic surfaces. *Mathematische Annalen*, 230(2):153–168, 1977.

[3] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55(5):497–508, 05 1949.

[4] Julien Grivaux, Juliana Restrepo Velasquez, and Erwan Rousseau. On lang's conjecture for some product-quotient surfaces. *arXiv preprint arXiv:1611.03001*, 2016.

[5] 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.

[6] Tetsuji Shioda and Toshiyuki Katsura. On fermat varieties. *Tohoku Math. J. (2)*, 31(1):97–115, 1979.

[7] 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.