

Research Statement

Background: Curves over the real and complex numbers have been a primary object of study in mathematics since ancient times. The field of Algebraic Geometry synthesizes three perspectives on these important objects: algebra – function fields as finitely generated field extensions of transcendence degree 1, geometry – algebraic curves defined as the loci of finite sets of homogeneous equations, locally defined by independent differentials, and analysis – compact Riemann surfaces. This synthesis has led to profound advances in the field of Number Theory, with the understanding of elliptic curves as non-singular cubic plane curves isomorphic to complex tori by maps defined using the Weierstrass \wp -function, with a group structure appearing on both models. Higher genus algebraic curves are similarly connected to higher dimensional complex tori, or Jacobians, by Abel’s Theorem, with important results stemming from the algebraic structure of these Jacobians. These curves also have many special points, such as Weierstrass points and theta characteristics, which carry information relating to the function fields and differentials of the curves. In the case of curves with automorphisms, we gain further insight into these special points, as well as mapping to curves of lower genus. All of these objects then inform us about the moduli spaces, or isomorphism classes, of the algebraic curves.

Research Plans: My research is in the field of algebraic geometry, working with algebraic curves with automorphisms and their moduli spaces. Thus far I have been concentrating primarily on one particular curve, Klein’s quartic curve, \mathfrak{X} , also known as the modular curve $X(7)$, which is the genus 3 curve canonically modeled by the equation

$$X^3Y + Y^3Z + Z^3X = 0.$$

\mathfrak{X} has 168 automorphisms, the maximum for a curve of genus 3, making \mathfrak{X} the smallest genus Hurwitz curve. Also unusual is the fact that \mathfrak{X} has a split Jacobian [Pra94]. This curve has a long tradition as the subject of much study due to its diverse applications in mathematics (see [Lev99]) and computer science (see [CP07] and below).

In this statement I will describe the work I have already done, which addressed three distinct aspects of the curve. For future work, I describe below two concrete projects connected to the linear spaces associated to the pluricanonical linear systems for \mathfrak{X} which I plan to conduct in the near future, dealing with Wronskians and automorphic forms, and Geometric coding theory. Beyond those projects, Weierstrass points have been shown to have applications in Geometric coding theory. I also plan to apply my work on an arithmetic-geometric mean for \mathfrak{X} to other genus 2 and 3 curves with split Jacobians. This should give insight into the connections between the modular and algebraic points of view on \mathfrak{M}_3 . The general direction of this work is towards creating a basis of both theoretical and applied work in the moduli space of curves, the explicit properties of which are, in many cases, still unknown. Further applications of such results are in the area of Mathematical Physics, specifically in String Theory and Quantum Field Theory, both of which significantly use moduli spaces; theta functions are also important in this area for modeling the equations of String Theory.

Previous Research: In my thesis, I examined three distinct aspects of \mathfrak{X} . The first was the most geometric, looking at subvarieties of moduli spaces (higher-order Weierstrass points). The second was more transcendental, using the special symmetries of the period lattice for this curve to define a genus 3 arithmetic-geometric mean (see also [LR07], [HLP00]). The final aspect stemmed from the second, where the special properties of \mathfrak{X} , in particular the elliptic curves contained in the Jacobian [Pra94], led to a need for a greater understanding of the genus 1 arithmetic-geometric mean [Fara], an important sequence of curves in its own right [BB98].

There have been extensive studies of connections between ordinary Weierstrass points and the fixed points of non-trivial automorphisms. Specifically, the automorphisms of an algebraic curve fix as a set its Weierstrass points. There are also many connections to higher-order Weierstrass points [Acc94]. I applied the methods from [Acc94] to the types of fixed points of non-trivial automorphisms in \mathfrak{X} , with results for fixed points of involutions and automorphisms with two fixed points. I showed that my results on those two types of fixed points combined with previous results [Acc83] leads to the conclusion that of the three types of fixed points of Klein's quartic curve, two types are higher-order Weierstrass points, in fact for infinitely many orders, while the third type is not. I also determined the weights of the higher-order Weierstrass points.

The second aspect is more transcendental. The classical arithmetic-geometric mean (AGM) for elliptic curves has been generalized to genus 2 [Ric36], and more recently to genus 3 [LR07]. It has also been shown that genus 3 is the last genus for which an AGM algorithm is feasible [DL99]. Some degree of explicitness was reached for genus 3 [LR07] using recent results [CS03] which associate the bitangents of a curve to its moduli. The goal of this aspect is to develop a construction for the AGM image of \mathfrak{X} using this curve's split Jacobian and the elliptic curve AGM; the recent work of [HLP00] on attaining knowledge of such algebraic curves was instrumental in this process. I compared the resulting curve with the AGM for \mathfrak{X} given by the previously defined genus 3 AGM.

The final aspect begins with the consideration of some classical results. Gauss's AGM is defined for the real numbers a and b as the common limit of the sequences $a_{n+1} = \frac{a_n+b_n}{2}$ and $b_{n+1} = (a_n b_n)^{1/2}$. Generalizing this process to the complex numbers presents a new problem: the choice of the square root defining b_{n+1} is no longer obvious. For the complex numbers, we need to make a choice for the square-root; a "right" choice can be defined [Cox84] and, as long as only finitely many "wrong" choices are made, the sequences will have an interesting (i.e. non-zero) common limit. The collection of these limits is described using Jacobi's theta functions, $\theta_{00}(\tau) = 1 + 2 \sum_{n=1}^{\infty} e^{2\pi i n^2}$ and $\theta_{01}(\tau) = 1 + 2 \sum_{n=1}^{\infty} (-1)^n e^{2\pi i n^2}$, which results from classical relations among these functions.

These relations also serve as the foundation for the elliptic curve AGM. Let $E : y_0^2 = x_0(x_0 - a_0^2)(x_0 - b_0^2) \approx \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ be an elliptic curve. Then the classically known AGM of E is the elliptic curve $E' : y_1^2 = x_1(x_1 - a_1^2)(x_1 - b_1^2) \approx \mathbb{C}/(\mathbb{Z} + 2\tau\mathbb{Z})$ [Gra89], where a_1 and b_1 are the arithmetic and geometric means of a_0 and b_0 , respectively. This process is easily seen to be moding out by the 2-torsion point, $(0, 0)$, on the algebraic model, and $1/2$ on the analytic model of E . In [Fara], I generalized this to make a similar construction moding out by the other 2-torsion points. In the case of complex values for a_0 and b_0 , the complex case for the original AGM also extends to a fuller understanding of the AGM for elliptic curves, where the choice of torsion point being divided by is given by the equivalence class of γ in $SL_2(\mathbb{Z})$ such that $\gamma\tau$ is in the fundamental domain for $\Gamma_2(4)$.

Wronskians and Automorphic Forms: The goal of this project is to determine a family of automorphic forms associated to the pluricanonical linear spaces for Klein's quartic curve. To begin, we look at the general situation. Let X be an algebraic curve of genus $g \geq 2$ with canonical divisor K . The Wronskian function is defined for a set of functions in a local coordinate z , $f_1(z), \dots, f_r(z)$, as the determinant

$$W(f_1, \dots, f_r) = \begin{vmatrix} f_1(z) & \cdots & f_r(z) \\ \frac{df_1}{dz}(z) & \cdots & \frac{df_r}{dz}(z) \\ \vdots & & \vdots \\ (\frac{d}{dz})^{r-1} f_1(z) & \cdots & (\frac{d}{dz})^{r-1} f_r(z) \end{vmatrix}.$$

In the case of the canonical linear system, $|K|$, with associated linear space, $\mathcal{L}(K)$, the zeros of $W(f_1, \dots, f_g)(dz)^{g(g+1)/2}$ are the Weierstrass points for the curve X , the multiplicities of the zeros being their Weierstrass weights [Mir95, VII.4]. The Wronskians for the pluricanonical spaces, $\mathcal{L}(nK)$, $n \geq 2$ (associated to $|nK|$) give the higher-order Weierstrass points [FK92, III.5].

Now let X be a modular curve $\Gamma \backslash \mathcal{H}^*$, for Γ a subgroup of finite index in $SL_2(\mathbb{Z})$ and \mathcal{H}^* the upper half plane with the cusps of Γ adjoined. Then the Wronskian is a modular form of weight $g(g+1)$ for Γ [Roh82]. In the pluricanonical case, the Wronskian is an automorphic form of weight $(2n-1)^2 g(g-1)/2$ [FK01, 3.1]. There appears to be no study of such forms in the case of higher order Weierstrass points.

Klein's quartic curve, as $X(7)$, has as Wronskian for $|K|$ a cusp form of weight 12 for $SL_2(\mathbb{Z})$, hence $W = \Delta$. [Roh82] proves this using facts about $\Gamma \simeq PSL_2(\mathbb{F}_7)$ and that the appropriate space of modular forms is one dimensional. Similar calculations for determining the ordinary Weierstrass points of \mathfrak{X} and other Hurwitz curves were done by [CHR99].

Alternatively, using the model for \mathfrak{X} given by $w^7 = z(z-1)^2$, we can explicitly write down a basis for $\mathcal{L}(K)$ [FK92, VII.3]:

$$\left\{ \frac{1}{w^3}, \frac{z-1}{w^5}, \frac{z-1}{w^6} \right\}.$$

It is this basis I plan to use to find bases for the pluricanonical spaces $\mathcal{L}(nK)$ for \mathfrak{X} . I have observed that for $2 \leq n \leq 5$, pairwise multiplication of the elements of this basis leads to exactly $\dim \mathcal{L}(nK) = (2n-1)(g-1) - 1$ independent differentials. For example, for $n=2$, pairwise multiplication of the basis elements of $\mathcal{L}(K)$ above led to

$$\left\{ \frac{1}{w^6}, \frac{1}{wz(z-1)}, \frac{1}{zw^3}, \frac{1}{w^2z(z-1)}, \frac{1}{w^4z}, \frac{1}{w^5z} \right\},$$

the Wronskian of which has exactly the roots predicted by [Farb]. With these explicit bases I plan to determine the automorphic forms appearing as the Wronskians for the pluricanonical spaces for \mathfrak{X} .

Geometric Goppa Codes: The explicit bases for the linear spaces associated to the pluricanonical linear systems for \mathfrak{X} discussed above will also be a fundamental part of the project I am proposing for applications in Geometric coding theory. Coding theory is concerned with the encoding and decoding of information such that errors that occur in transmission can be detected and corrected during the decoding phase. Applications of this type of process include satellite transmissions, transferring information within a computer system and data storage [CLO05, Chap. 9]. The encoding process is described as an injective map

$$C : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$$

where k is the rank of the code and n the length of the code [Pre98, Chap. 5]. Choosing $n > k$ builds redundancy into the coding system, which allows for error-correcting.

The use of algebraic geometry in defining coding systems was established by Goppa ([Gop81], [Gop82]). Geometric Goppa codes are linear error-correcting codes obtained by evaluating the rational functions in a linear space on an algebraic curve X ([Pre98, Chap. 5], [Pre09]). More precisely, let X be an algebraic curve over a finite field \mathbb{F}_q , and let $D = P_1 + \dots + P_n$ and G be divisors with disjoint rational support on X . Primary (or differential) Goppa codes are defined by

$$C_\Omega(D, G) = \{ (Res_{P_1}(\omega), \dots, Res_{P_n}(\omega)) : \omega \in \Omega(G - D) \},$$

though it is common to first introduce dual (or functional) Goppa codes, which are defined by

$$C_L(D, G) = \{ (g(P_1), \dots, g(P_n)) : g \in \mathcal{L}(G) \}.$$

Curves with automorphisms are useful for defining codes, as the automorphism group of the curve and the permutation automorphism group of the codes are in many cases the same [JK06]. Klein's

quartic curve has been an important example in Geometric coding theory ([CP07], [Han87], [HR96], [RTL91]).

A key point in defining Geometric Goppa codes is the need to find explicit bases for linear spaces $\mathcal{L}(G)$. There have been some advances on this topic ([HI94]), but it remains a difficult problem. I plan to use the same explicit bases for $\mathcal{L}(K)$ as described above to define pluricanonical linear spaces over finite fields for Klein's quartic curve. This project is reasonable since so many results on linear systems and their corresponding spaces of functions extend from characteristic zero fields into positive characteristic, one important example being the Riemann-Roch Theorem (see [Sti09, 1.5]). On a related note, [JvOS94] found the bitangents of \mathfrak{X} as the same over \mathbb{C} and \mathbb{F}_7 , where the intersections of the curve and the bitangents with multiplicity give the canonical divisor for the curve [Acc94]. Another property of the curve, which also translates to some finite fields [Cox83], is that of having sets of 4 concurrent bitangents [FK91]. Similar work was proposed in [CHR99] for the canonical linear space, with a goal of finding Weierstrass points of \mathfrak{X} over finite fields for use in Geometric coding theory.

References

- [Acc83] Robert D. M. Accola, *On generalized Weierstrass points on Riemann surfaces*, Modular functions in analysis and number theory, Lecture Notes Math. Statist., vol. 5, Univ. Pittsburgh, Pittsburgh, PA, 1983, pp. 1–19.
- [Acc94] ———, *Topics in the theory of Riemann surfaces*, Lecture Notes in Mathematics, vol. 1595, Springer-Verlag, Berlin, 1994.
- [BB98] Jonathan M. Borwein and Peter B. Borwein, *Pi and the AGM*, Canadian Mathematical Society Series of Monographs and Advanced Texts, 4, John Wiley & Sons Inc., New York, 1998.
- [CHR99] Philippe Carbonne, Thierry Hénocq, and Francis Rigal, *Points de Weierstrass de deux familles de courbes*, Comm. Algebra **27** (1999), no. 11, 5235–5254.
- [CLO05] David A. Cox, John Little, and Donal O'Shea, *Using algebraic geometry*, second ed., Graduate Texts in Mathematics, vol. 185, Springer, New York, 2005.
- [Cox83] H. S. M. Coxeter, *My graph*, Proc. London Math. Soc. (3) **46** (1983), no. 1, 117–136.
- [Cox84] David A. Cox, *The arithmetic-geometric mean of Gauss*, Enseign. Math. (2) **30** (1984), no. 3-4, 275–330.
- [CP07] Drue Coles and Emma Previato, *Goppa codes and Tschirnhausen modules*, Advances in coding theory and cryptography, Ser. Coding Theory Cryptol., vol. 3, World Sci. Publ., Hackensack, NJ, 2007, pp. 81–100.
- [CS03] Lucia Caporaso and Edoardo Sernesi, *Recovering plane curves from their bitangents*, J. Algebraic Geom. **12** (2003), no. 2, 225–244.
- [DL99] Ron Donagi and Ron Livné, *The arithmetic-geometric mean and isogenies for curves of higher genus*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), no. 2, 323–339.
- [Fara] Eleanor Farrington, *A Complete Arithmetic-Geometric Mean for E/\mathbb{C}* , Submitted to Archiv der Mathematik.

- [Farb] ———, *Higher Weierstrass Points of Klein's Quartic*, Submitted to Algebra Colloquium.
- [FK91] Hershel M. Farkas and Irwin Kra, *Branched two-sheeted covers*, Israel J. Math. **74** (1991), no. 2-3, 169–197.
- [FK92] ———, *Riemann surfaces*, second ed., Graduate Texts in Mathematics, vol. 71, Springer-Verlag, New York, 1992.
- [FK01] ———, *Theta constants, Riemann surfaces and the modular group*, Graduate Studies in Mathematics, vol. 37, American Mathematical Society, Providence, RI, 2001.
- [Gop81] V. D. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), no. 6, 1289–1290.
- [Gop82] ———, *Algebraic-geometric codes*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 4, 762–781, 896.
- [Gra89] Daniel R. Grayson, *The arithogeometric mean*, Arch. Math. (Basel) **52** (1989), no. 5, 507–512.
- [Han87] Johan P. Hansen, *Codes on the Klein quartic, ideals, and decoding*, IEEE Trans. Inform. Theory **33** (1987), no. 6, 923–925.
- [HI94] Ming-Deh Huang and Doug Ierardi, *Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve*, J. Symbolic Comput. **18** (1994), no. 6, 519–539.
- [HLP00] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364.
- [HR96] Thierry Henocq and Denis Rotillon, *The theta divisor of a Jacobian variety and the decoding of geometric Goppa codes*, J. Pure Appl. Algebra **112** (1996), no. 1, 13–28.
- [JK06] David Joyner and Amy Ksir, *Automorphism groups of some AG codes*, IEEE Trans. Inform. Theory **52** (2006), no. 7, 3325–3329.
- [JvOS94] R. H. Jeurissen, C. H. van Os, and J. H. M. Steenbrink, *The configuration of bitangents of the Klein curve*, Discrete Math. **132** (1994), no. 1-3, 83–96.
- [Lev99] Silvio Levy (ed.), *The eightfold way*, Mathematical Sciences Research Institute Publications, vol. 35, Cambridge University Press, Cambridge, 1999.
- [LR07] D. Lehavi and C. Ritzenthaler, *An explicit formula for the arithmetic-geometric mean in genus 3*, Experiment. Math. **16** (2007), no. 4, 421–440.
- [Mir95] Rick Miranda, *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics, vol. 5, American Mathematical Society, Providence, RI, 1995.
- [Pra94] Despina T. Prapavessi, *On the Jacobian of the Klein curve*, Proc. Amer. Math. Soc. **122** (1994), no. 4, 971–978.
- [Pre98] Oliver Pretzel, *Codes and algebraic curves*, Oxford Lecture Series in Mathematics and its Applications, vol. 8, The Clarendon Press Oxford University Press, New York, 1998.

- [Pre09] E. Previato, *Vector bundles in error-correcting for geometric goppa codes*, Algebraic Aspects of Digital Communications, IOS Press, Amsterdam, 2009.
- [Ric36] F. Richelot, *Essai sur une méthode générale pour déterminer la valeur des intégrales ultraelliptiques, fondée sur des transformations remarquables de ces transcendentes*, C. R. Acad. Sci. Paris 2 (1836), 622–627.
- [Roh82] David E. Rohrlich, *Some remarks on Weierstrass points*, Number theory related to Fermat’s last theorem (Cambridge, Mass., 1981), Progr. Math., vol. 26, Birkhäuser Boston, Mass., 1982, pp. 71–78.
- [RTL91] D. Rotillon and J.-A. Thiong Ly, *Decoding of codes on the Klein quartic*, Eurocode ’90 (Udine, 1990), Lecture Notes in Comput. Sci., vol. 514, Springer, Berlin, 1991, pp. 135–149.
- [Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.