UROP+ Final Paper, Summer 2017

p-Curvature Map of SL_2 Opers on Elliptic and Hyperelliptic Curves

Anlong Chua

Mentor: Pablo Boixeda Alvarez

Faculty Advisor: Professor Roman Bezrukavnikov

Abstract

In this paper, we compute the p-Curvature map of SL_2 opers on elliptic and hyperelliptic curves. On elliptic curves, the map has a simplified form, which can differentiate between ordinary and supersingular curves.

1 Introduction

Elliptic curves are widely and successfully used in cryptography. It is hence no surprise that much effort has been made to study and classify these curves. One such classification of elliptic curves is into "ordinary" and "supersingular" curves, with supersingular curves being cryptographically weaker than their ordinary counterparts. Lately, research has also been conducted into using hyperelliptic curves for cryptography, and the classification of ordinary and supersingular elliptic curves has been successfully generalized to classify hyperelliptic curves based on their Jacobian variety. Additionally, understanding opers may help in understanding parts of the Geometric Langlands program. In this paper, we compute the SL_2 opers and p-curvature maps on elliptic and hyperelliptic curves. On elliptic curves, we show that the map can be described in terms of the Frobenius map. Unfortunately, we were unable to find a simplified description of the map on hyperelliptic curves.

This paper is split into two logical sections. The first presents some background material on Algebraic Geometry and the classification of elliptic and hyperelliptic curves (Sections 2 - 5), and the second presents the results of our computations (Sections 6 - 8).

2 Basic Algebraic Geometry

This section is a summary of some basic objects in Algebraic Geometry that will be useful in the rest of this paper. Detailed proofs of facts and theorems will not be provided since one can look them up in any introductory textbook on the subject ([Har79], [Sha97]). Indeed, many definitions and theorems in this section were taken from these excellent references. In addition, we shall not give theorems and definitions of objects in their full generality, but rather tailor them for application to projective curves.

2.1 Varieties and Functions on Varieties

The basic object of study in algebraic geometry is a variety, the set of common zeroes of a set of polynomials, in our case, in two variables. To make this precise, let k be an algebraically closed field, and let $k[X]$ denote the polynomial ring $k[x, y]$. Then a variety is defined as follows:

Definition 1. *An **algebraic affine variety** (or simply variety for brevity) is the locus of common zeroes of a set S of polynomials in $k[X]$ such that the ideal generated by S is prime.*

It will be convenient to denote the set of common zeroes of an set of functions S by $Z(S)$, and the ideal of functions that vanish on all points of a set of points T by $V(T)$. In the special case where S consists of only 1 polynomial, f, the condition that the ideal of S is prime translates into the condition that f is irreducible. If, in addition, $n = 2$ (the case we are interested in), then $Z(f)$ forms an **affine curve** in $\mathbb{A}^2$. If $I(S)$ denotes the ideal generated by elements of S, then we can consider the quotient ring $k[X]/V(Z(S)) = A(S)$, which is intuitively the set of polynomial functions on points of Z, by identifying 0 with any polynomial that vanishes on all points of the variety. Ideals in $A(S)$ correspond to ideals containing $V(Z(S))$ in the original ring, and also correspond to subvarieties of $Z(S)$. This fact is encapsulated nicely in the Zariski Topology:

Definition 2. *In the **Zariski Topology**, closed sets (T) are sets such that there is an ideal $I \in A(S)$ such that $T = Z(I)$.*

With a topology, we can study functions on the variety. An important and fundamental class of functions are the regular functions, defined below:

Definition 3. *A function on a variety Y is **regular** at a point $P \in Y$ if there is an open neighborhood U with $P \in U$, and polynomials g, h, with $h \neq 0$ on U, and $f = g/h$ on U. We say that f is regular on Y if it is regular at every point of Y.*

One can check that the set of regular functions, along with the usual addition and multiplication operations, form a ring, called the ring of regular functions on Y, denoted by $\mathcal{O}_y$. It can be proven that $\mathcal{O}_y \cong A(Y)$. We may also want to consider the **local ring** $\mathcal{O}_x$ at a point $x \in Y$: the ring of functions that are regular in some open neighborhood of x. If we denote by m_x the ideal in $A(Y)$ of functions vanishing on x, we see intuitively (and it can be proven) that $\mathcal{O}_x \cong A(Y)_{m_x}$. Finally, the functions regular on some open set a variety Y are called **rational functions** and form a ring denoted $K(Y)$. This is made formal and precise as follows:

Definition 4. *Define the **function field**, $K(Y)$, of a variety Y as follows: an element of $K(Y)$ is an equivalence class of pairs $< U, f >$ where U is a nonempty open subset of Y, f is regular on U, and where two pairs $< U, f >$ and $< V, g >$ are equivalent if $f = g$ on $U \cap V$. The elements of $K(Y)$ are called **rational functions** on Y.*

Similarly, it can be shown that $K(Y) \cong A((Y))$, the fraction field of $A(Y)$. Note that this makes sense only because we required that the ideal generated be prime (see Definition 1).

Often, we will find it easier to work in projective spaces ($\mathbb{P}^n$) instead of affine spaces. To do this, we take the polynomial equations we are interested in, homogenize them by adding suitable powers of x_{n+1} to each monomial, and

consider the **homogenous** variety in $k[x_1, \ldots, x_{n+1}]$. The definitions given in Definition 1 carry over, except that we require the ideal to be homogenous. **Projective curves** and regular functions on a projective variety are defined similarly, with the same condition that ideals and polynomials should be homogenous. An important property of projective varieties is that there are no non-constant functions that are regular on the entire variety. This fact is listed in the Proposition below so it can be referenced easily later.

Proposition 1. *Let Y be a projective variety. Then $\mathcal{O}(Y) \cong k$.*

3 Derivations, Differentials and Divisors

Divisors are an extremely powerful book-keeping tool, and can be used to prove or disprove the eistence of functions satisfying certain properties. Closely related are Derivations, which provide a way to take "derivatives" algebraically, and Differentials, which are an algebraic analog of their namesakes from Analysis.

To define these objects, we begin with the notion of the **tangent space** at a point. Consider a variety $Y = Z(I)$ where I is an ideal in $k[X]$. By the Hilbert Basis Theorem, $k[X]$ is noetherian and hence I is finitely generated: $I = (f_1, \ldots, f_k)$. We wish to define the tangent space at a point $x \in Y$ to be the set of lines through x tangent to X, in accordance with our geometric intuition. By a change of coordinates, it suffices to define tangency at the point $0 \in \mathbb{A}^n$. Fix some nonzero point $a \in \mathbb{A}^n$. Then all lines through 0 are of the form ta where $t \in k$. We arrive at the following definition:

Definition 5. *Define the **intersection multiplicity** of a line ta with a variety Y at 0 to be the highest power of t that divides all the $f_i(ta)$. A line is then tangent at 0 if its intersection multiplicity is greater than 1. The locus of points on lines tangent to Y at some point $x \in Y$ is called the **tangent space** to Y at x, and is denoted $T_x(Y)$.*

An alternative (but equivalent) definition of the tangent space at a point $p = (a_1, \ldots, a_n)$ in a variety with ideal generated by $f_1, \ldots, f_k$ is as follows:

Definition 6. *Let H_i be the hyperplane defined by $\sum_k \frac{\partial f_i}{\partial x_i}(p)(x_i - a_i)$. Then we define the tangent space to be $\cap_1^n L_i$.*

Now, we shall introduce the concept of **derivations** and explain its relation with the tangent space at a point.

Definition 7. *Let R be a ring and M be an R-module. A **derivation** of R into M is a map*

$$d : A \to M$$

satisfying the Leibniz rule:

$$d(ab) = adb + bda$$

If R and M are vector spaces over a field k, then we also require that $da = 0$ for $a \in k$. We can make the set of derivations into an R-module with the map $d \mapsto rd$ for $r \in R$. This R-module is denoted $Der_k(A, R)$

If we let $R = A(Y)$ and view k as the residue field at a point $x \in Y$ (which is an R-module by the rule $f \cdot \alpha = f(x) \cdot \alpha$), then we can prove that $Der_k(A(Y), k) \cong T_x(Y)$. In other words, the tangent space can be thought of as the set of derivations from $\mathcal{O}_x$ to k.

Now that we have defined derivations, we can discuss **differentials**. Let $f(X)$ be a polynomial, and x be a point in $\mathbb{A}^n$. Then f has a Taylor series expansion $f(X) = f(x) + f^{(1)}(x) + \dots$.

Definition 8. *The linear form $f^{(1)}$ is the **differential** of f at x, and is denoted df.*

Note that taking the differential of a function is a derivation.

Now, if we view some regular function g on Y as the restriction of a polynomial $G \in k[X]$, then the rule $dg = dG$ is not well defined because we can add df for $f \in I(Y)$ arbritrarily; however, if we restrict to the tangent space at x, we see that $df = 0$ for $f \in I(Y)$, and hence this restriction is well defined. In other words,

$$dg = dG|_{T_x(Y)}$$

defines a homomorphism $d : A(Y) \to \Omega_x$ where Ω_x is the space of differential forms on $T_x(Y)$. Since $A(Y)$ is spanned by the monomials $x_1, \dots, x_n$, it is then not hard to see that due to the Leibniz rule, Ω_x is spanned by the differentials dx_i.

Note that the space of differentials is dual to the space of derivations: given a differential df and a derivation D, we send $(df, D) \mapsto D(f)$. Therefore the space of differentials can be identified with the cotangent space of the variety.

Finally, we are ready to discuss divisors. In the rest of this paper, let "curve" refer to a smooth, projective curve. Since a polynomial function is determined (up to a constant factor) by its roots, a rational function is determined (up to a constant factor) by the positions of its zeroes and poles. We capture this information in divisors as follows:

Definition 9. *Let Y be an irreducible curve ($n = 2$). A divisor on Y is a finite formal sum of the form*

$$\sum n_i P_i,$$

with $n_i \in \mathbb{Z}$ and P_i points on the curve.

The set of points P_i for which $n_i \neq 0$ is called the **support** of D, and a divisor is called **effective** if $n_i \geq 0$ for all i. The degree of D is defined as the sum of the coefficients of P_i:

$$\deg D = \sum n_i.$$

Now, consider a rational function, $f \in K(Y)$ on a smooth projective curve. At each point p_i, we consider the local ring $\mathcal{O}_{p_i}$, which can be shown to be a discrete valuation ring, and set $n_i = v_{p_i}(f)$. Divisors of this form are called **principal divisors**, and are denoted (f). Intuitively, the valuation tells us the "rate" of vanishing or "blowing up" of a rational function at a point. Indeed, if $n_i > 0$ then we say that f has a zero of order n_i at P_i, and we say that f has a pole of order $-n_i$ at P_i if $n_i < 0$. (Of course, to be completely rigorous, one needs to check that there are only a finite number of points where f can have poles or zeroes, but proofs of this fact can be found in any of the references listed at the beginning of this section.) Finally, one can show that $\deg(f) = 0$ for any rational function on a curve.

To better work with principal divisors, it is convenient to recall the following facts, all of which follow from the definition of a discrete valuation:

1. $(fg) = (f) + (g)$.
2. $(f/g) = (f) - (g)$.
3. $v_{P_i}(f+g) \geq \min(v_{P_i}(f), v_{P_i}(g))$, with equality if $v_{P_i}(f) \neq v_{P_i}(g)$.

Now, one can check that the set of all divisors on a curve form an abelian group (under the operation of addition), and that the set of principal divisors form an abelian subgroup of the group of divisors. These groups are named $\operatorname{Div} Y$ and $\operatorname{Princ} Y$ respectively. The quotient group $\operatorname{Div} Y / \operatorname{Princ} Y$ is denoted $\operatorname{Cl} Y$, the class group of Y. Two divisors D, D' are said to be equivalent if they are equal in $\operatorname{Cl} Y$. If this is the case, we write $D \sim D'$.

Now, one can define the divisor of a differential form in a similar manner.

Definition 10. *If ω is a differential form on Y, then for any $P_i \in Y$, choose a local coordinate t and write $\omega = f\,dt$. Then $n_i = v_{P_i}(f)$.*

The divisor of a globally defined differential form (so that its divisor is effective) is called a **canonical divisor**.

The Riemann-Roch Theorem, given in the next section, allows one to use divisors to reason about the existence (or non-existence) of certain functions on the curve.

3.1 The Riemann-Roch and Riemann-Hurwitz Theorems

We begin with the discussion of the Riemann-Roch Theorem. Before giving the statement of the theorem, we must first give some basic definitions.

Let D be a divisor on an irreducible variety Y. Then the Riemann-Roch space, denoted $\mathcal{L}(D)$, is defined as follows:

Definition 11. $\mathcal{L}(D) = \{f | f \in K(Y), (f) + D \geq 0\}$.

The dimension of this space (as a k-vector space) is denoted $l(D)$. We now give the Riemann-Roch theorem:

Theorem 2 (Riemann-Roch)**.** *Let Y be a variety of genus g with canonical divisor K. Then*

$$l(D) - l(K - D) = \deg(\mathrm{D}) - g + 1.$$

On a curve, it can be shown that any canonical divisor has degree $2g - 2$, and that all canonical divisors are linearly equivalent.

Next, we give the statement of the Riemann-Hurwitz theorem. It will be useful in determining the equation of a hyperelliptic curve.

Theorem 3 (Riemann-Hurwitz)**.** *Let S' be a ramified N cover of a surface S. If the cover has n preimages at almost every point, with 1 preimage at finitely many points (denoted e_P), then denoting the genera of S' and S $g(S')$ and $g(S)$ respectively, we have the formula:*

$$2g(S') - 2 = N(2g(S) - 2) + \sum_{P \in S'} (e_P - 1).$$

These theorems will be useful in the analysis of elliptic and hyperelliptic curves in the next two sections.

4 Classification of Elliptic Curves

An elliptic curve is a smooth, projective, algebraic curve of genus 1. Over a field of characteristic not 2 or 3, it can be defined by an equation of the form $y^2 = x^3 + ax + b = f(x)$, with f not having any repeated roots. An elliptic curve can be thought of as consisting of the points on the affine variety $y^2 = x^3 + ax + b$, together with a point O - the point at "infinity". In this section, let the variety given by this elliptic curve be X.

The elliptic curve is the most famous example of a group variety. The Riemann-Roch theorem provides us with a neat way to understand this structure:

Proposition 4. *Let P_0 be the point at infinity. Let D be a divisor of degree 0. Then there is a unique point P on X such that $D \sim P - P_0$.*

Proof. We apply Riemann-Roch with $D + P_0$. We get:

$$l(D + P_0) - l(K - D - P_0) = 1.$$

We also have that $l(K - D - P_0) = 0$ since $\deg(K - D - P_0) = -1$. Therefore $l(D + P_0) = 1$. This means that there is a unique effective divisor linearly equivalent to $D + P_0$. Moreover, since its degree is 1, it must be a single point. This proves the proposition. □

Proposition 4 therefore tells us that the map $P \mapsto (P - P_0)$ gives a bijective correspondence between points on the curve and and the subgroup of $\mathrm{Cl}\, X$ consisting of degree 0 divisors. This gives a group structure on the points of X.

With this group structure, it then makes sense to speak of "adding" points on elliptic curves. In particular, define $E[p]$ to be the subgroup of $p-torsion$ points on X: the points that, when added to itself p times, gives the identity. It can be shown that the only two possibilities are $|E[p]| = 1$ or $|E[p]| = p$. The curve is called **ordinary** if $|E[p]| = p$, and **supersingular** otherwise.

5 Classification of Hyperelliptic Curves

A hyperelliptic curve is a smooth, projective, algebraic curve of genus $g > 1$. Over a field of characteristic not 2 or 3, it can be defined by an equation of the form $y^2 = f(x)$, with f not having any repeated roots. The projective variety given directly by this equation will have a singularity at the point at infinity, P_∞; however, this point can be removed by normalization of the curve, and the resulting curve can be described as being covered by 2 affine charts: one given by

$$y^2 = f(x),$$

and the other given by

$$w^2 = v^{2g+2} f(1/v),$$

with the transition function being $(x, y) \mapsto (1/x, y/x^{g+1})$. When the degree of f is odd, the curve is called an **imaginary** hyperelliptic curve, and has a ramification point at P_∞; and when the degree of f is even, the curve is termed a **real** hyperelliptic curve, and has two "points at infinity". In this paper, we work exclusively with imaginary hyperelliptic curves. Since we can transform any real hyperelliptic curve (given by $\deg f = 2g + 2$) into a corresponding imaginary one, we are not losing any generality by doing this. We can use the Riemann-Hurwitz theorem to easily calculate the degree of f in terms of the

genus of the curve. Since the curve is a ramified double covering of $\mathbb{P}^1$, with ramification points at the roots of f and at P_∞, we get:

$$2 - 2g = 4 - (\deg f + 1),$$

and therefore that $\deg f = 2g + 1$.

We wish to extend the above classification to hyperelliptic curves. However, the main problem is that there is no way to define a group structure on the points of the hyperelliptic curve. Therefore we need to consider the Jacobian variety of the curve instead. First, we fix a prime characteristic p of the ground field k greater than 3. Then on the Jacobian variety, we can define the p-rank: the integer s such that the kernel of multiplication by p has p^s points. On the Jacobian variety, the p-torsion points are in bijective correspondence with the order p elements of the class group, which are in turn in bijective corresponence with the logarithmic differential forms (which can be defined to be the differential forms that are fixed by the Cartier-Manin operator, defined below).

One may therefore compute the rank of the Hasse-Witt matrix (a matrix that represents the operation of the Cartier-Manin operator) to obtain an upper bound on the p-rank; however, it is in general hard to compute the p-rank exactly. We now explain how to compute the Hasse-Witt matrix.

To do this, it will be convenient to use a different, but equivalent definition of the hyperelliptic curve: we define it to be the unique smooth, projective algebraic curve with the function field $K(y^2 - f(x))$. Then we can define the Cartier-Manin operator as follows:

Definition 12. *The Cartier-Manin operator (or simply Cartier operator, for brevity) is defined as the endomorphism of the space of differentials Ω ($C : \Omega \mapsto \Omega$) with the following properties: for all $\omega, \omega_1, \omega_2 \in \Omega$ and all $z \in K(y^2 - f(x))$:*

1. $C(\omega_1 + \omega_2) = C(\omega_1) + C(\omega_2)$.
2. $C(z^p \omega) = zC(\omega)$.
3. $C(dz) = 0$.
4. $C(dz/z) = dz/z$.

The Hasse-Witt matrix represents the action of the Cartier operator restricted to the space of holomorphic differentials (those with effective associated divisors). It can be shown that this space (as a vector space over k) has dimension g, with basis $\{\omega_i = x^{i-1}dx/y\}$. By $1/p$-linearity of C, it suffices to check the action of

C on elements of this basis. We hence compute:

$$\begin{aligned} C(\omega_i) &= C(\frac{x^i}{y}dx/x) \\ &= (\frac{x^i}{y})^{1/p}\frac{dx}{y}\frac{y}{x} \\ &= (x^{i-p}f^{\frac{p-1}{2}})^{1/p}\frac{dx}{y}. \end{aligned}$$

Therefore the entries of the matrix representing the action of the Cartier operator on the basis can be computed by calcuating the corresponding coefficients of the powers of x in $f^{\frac{p-1}{2}}$. This allows one to compute an upper bound of the p-rank of a hyperelliptic curve, as discussed above.

6 The p-Curvature Map

In this paper, we examine the p-curvature map of opers. First, we recall a few basic definitions.

Definition 13. *An SL_n oper with marking on a curve C can be described in terms of vector bundles as follows: it consists of the data $(E, E_{ii=1,\dots,n}, \nabla, \phi)$ where E is a rank n vector bundle on C, $E_1 \subset E_2 \subset \cdots \subset E_n = E$ is a complete flag, ∇ is a connection on E, and $\phi : E_1 \simeq \omega^{(n-1)/2}$ is an isomorphism, such that*

1. *$\nabla(E_i) \subset E_{i+1} \otimes \omega$.*
2. *For each i, the induced morphism $gr_i(E) \xrightarrow{gr_i(\nabla)} gr_{i+1}(E) \otimes \omega$ is an isomorphism.*
3. *The connection ∇ is given by traceless matrices on its local trivializations.*

Definition 14. *Given a connection ∇, the p-curvature of ∇ is given by*

$$v \mapsto \nabla(v)^p - \nabla(v^p).$$

In this paper, we study SL_2 opers, and the p-curvature map of the space of such opers. For an SL_2 oper, the definition says that we should have a vector bundle $\mathcal{E} = E_2 \supset E_1$ where E_2 is a rank 2 vector bundle, E_1 is a rank 1 vector bundle, $\mathcal{E}_1 \cong \omega^{1/2}$, and $\omega^{1/2} \cong \mathcal{E}_1 \cong \mathcal{E}/\mathcal{E}_1 \otimes \omega$. This gives us the short exact sequence:

$$0 \to \omega^{1/2} \to \mathcal{E} \to \omega^{-1/2} \to 0. \tag{1}$$

Since $\mathcal{E}$ is an extension of $\omega^{1/2}$ with $\omega^{-1/2}$, there is only one class of nontrivial (not the same as $\omega^{1/2} \oplus \omega^{-1/2}$) bundle $\mathcal{E}$ up to equivalence.

Hence we shall adopt the following strategy to compute the p-curvature map:

1. Identify a suitable vector bundle that is an extension of (1).
2. Compute the set of "allowed" opers on the bundle.
3. Classify the set of "allowed" opers up to equivalence by examining automorphisms of the bundle.
4. Find representatives for each equivalence class that simplify computation of the p-curvature map.
5. Compute the p-curvature map.

7 Computations for Elliptic Curves

By the short exact sequence (1), we are looking for an extension of the trivial bundle on elliptic curves. As will be shown below, opers exist on the trivial bundle. Since it can be shown that the opers cannot exist on both the trivial and nontrivial extensions, it suffices to give the opers on the trivial bundle.

In the case of the trivial bundle, we can specify the connection on the entire curve, in which case the matrix will consist of global sections on the entire projective curve, i.e. constants. For an SL_2 oper, we also have the additional condition that the matrix have trace 0. Thus the connections in the SL_2 case are conjugate to those given by matrices of the form:

$$\begin{bmatrix} \lambda & 0 \\ 0 & -\lambda \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

by a standard result from linear algebra. The case for GL_2 can be handled similarly (without the condition that the matrix is traceless).

Now that we have a concrete description of the opers on elliptic curves, we wish to compute the p-curvature map. Fix a prime characteristic $p > 3$ for the ground field k. The p-curvature map is defined by

$$v \mapsto \nabla(v)^p - \nabla(v^p),$$

for some derivation v in the tangent space of the curve. The first term, $\nabla(v)^p$, is computed in the proposition below.

Proposition 5. *Let ∇ be a connection given by $\nabla = d + M\frac{dx}{2y}$. Then*

$$\nabla(v)^p = v^p + M^p \left(\frac{dx}{2y}\right)^p + Mv^p \left(\frac{dx}{2y}\right).$$

Proof. Note that $\nabla(v)^p$ can be written as a sum of terms of the form

$$M^j v^{(k)} \left(\frac{dx}{2y}\right)^{l_{(k)}} v^i$$

with (k) being a multi-index: $(k) = (k_1, k_2, \dots)$ with each index k_i representing the result of applying v i times to $\frac{dx}{2y}$. Let the coefficient of such a term be represented by a_{jki}. On each application of $\nabla(v)$, each term is either multiplied by $M\frac{v(x)}{2y}$, of has v applied to it. Using the Leibniz rule, we can choose one of the factors of each term to apply v to, counting with appropriate multiplicity (l_{k_i}) when we apply v to the term $v^{k_i}(\frac{dx}{2y})^{l_{k_i}}$.

First, notice that $\binom{p}{i} \mid a_{jki}$: to form such a term, we can choose i out of p applications of $\nabla(v)$ to contribute to the v^i factor. Since $p \mid \binom{p}{i}$ if $i \neq 0$ and $i \neq p$, we only need to consider the terms where $i = p$ and $i = 0$. In the case where $i = p$, all applications of $\nabla(v)$ were applications of v, so $j = k = 0$. Note also that there is only 1 way to do this. This gives the v^p term in the sum.

When $i = 0$, all applications of $\nabla(v)$ were multiplication by $M\frac{v(x)}{2y}$, or application of v to one of the $\frac{v^{k_i}(x)}{2y}$ terms (note that in this case, M is a matrix of constants, and so $v(M) = 0$). To analyze this case, fix some term a_{jki} and consider the largest i such that k_i is nonzero. To obtain one such $\frac{v^{k_i}(x)}{2y}$ term in the product, we must have multiplied by $M\frac{v(x)}{2y}$ once, and then applied v to the $\frac{v(x)}{2y}$ term $k_i - 1$ times. This gives a string of k_i operations that can be interspersed in the total of p operations we are allowed on the term. Note that we could have chosen this $\frac{v^{k_i}(x)}{2y}$ in l_{k_i} different ways. Therefore we get the result that $\frac{1}{l_{k_i}}\binom{p}{k_i} \mid a_{jki}$. (Note that this extends inductively to a formula to calculate the coefficient explicitly, but we do not need that here.) Therefore a_{jki} is divisible by p unless $k_i = 1$ or $k_i = p$. Note that again, there is only one way to form each of these terms. The proposition follows. □

Since the tangent space is a line bundle, it suffices to determine the determinant of the p-curvature map for a convenient choice of v. We shall take $v = 2y\partial_x + f'(x)\partial_y$. Since the curve is elliptic, $v^p = cv$ where v is the Hasse invariant of the curve. Applying it to the map, we obtain:

$$\nabla(v)^p - \nabla(v^p) = \begin{bmatrix} (\lambda)^p - c\lambda & 0 \\ 0 & (-\lambda)^p - c\lambda \end{bmatrix}.$$

In particular, c is 0 if and only if the curve is supersingular, and therefore the p-Curvature map corresponds to the Frobenius p-power map if and only if the curve is supersingular.

8 Computations for Hyperelliptic Curves

Let the defining equation of the hyperelliptic curve be $y^2 = f(x)$, with $f(x)$ being a monic polynomial of degree $2g + 1$ without multiple roots. We will for simplicity consider only the imaginary hyperelliptic curves since they only have one "point at infinity"; since we can transform any real hyperelliptic curve (given by $\deg f = 2g+2$) into a corresponding imaginary one, we are not losing any generality by doing this. Then the curve is covered by two affine charts, one defined by the given equation, and the other given by $w^2 = v^{2g+2} f(1/v)$. The glueing map on the intersection is given by $(v, w) \mapsto (1/v, w/v^{g+1})$.

We wish to find a function that vanishes with order 1 at P_∞. To do this, we compute some convenient divisors:

Proposition 6. *The function x has a pole of order 2 at P_∞, and y has a pole of order $2g + 1$ at P_∞.*

Proof. First we show that on the affine portion, when $y = 0$, y is a local parameter, and that elsewhere, x is a local parameter. Recall that the defining equation of the affine portion is $y^2 = f(x)$. Taking differentials on both sides, we obtain:

$$2ydy = f'(x)dx.$$

Since dx and dy span the space of differentials, they can't both be 0. When $y = 0$, we must have $f(x) = 0$ and therefore $f'(x) \neq 0$ since f has no roots of multiplicity greater than 1. Therefore we obtain $dx = 0$ and hence dy must be nonzero. This means that y is a local parameter at this point. Similarly, if $y \neq 0$, $dx = 0$ would imply that $dy = 0$. Therefore $dx \neq 0$ and x is a local parameter, as claimed.

Now, since x and y generate principal divisors, their degrees as divisors must be 0. First consider the case $f(0) \neq 0$. Then x vanishes at 2 points on the affine part, corresponding to the solutions $y^2 = f(0)$. At each of these points, x is a local parameter. Therefore,

$$(x) = P_1 + P_2 - 2P_\infty.$$

In the case where $f(0) = 0$, we must have $y^2 = xg(x)$. Then when x vanishes, $y = 0$ and y is a local parameter, so x vanishes with order 2 since $g(x)$ doesn't vanish. We hence obtain

$$(x) = 2P_1 - 2P_\infty.$$

Similarly, y vanishes at $2g + 1$ points on the affine part, corresponding to the roots of f: $f(P_i) = 0$. At these points, y is a local parameter. Therefore,

$$(y) = \sum_1^{2g+1} P_i - (2g + 1)P_\infty,$$

as claimed. □

Therefore $\frac{x^g}{y}$ will vanish with order 1 at P_∞. Indeed,

$$\begin{aligned}\left(\frac{x^g}{y}\right) &= g(x) - (y) \\ &= gP_1' + gP_2' + P_\infty - \sum_1^{2g+1} P_i.\end{aligned}$$

Next, we proceed in a fashion similar to the hyperelliptic curve case to determine the vector bundle $\mathcal{E}$ we are interested in. By definition, we must have $\mathcal{E}_1 \hookrightarrow \mathcal{E}$, $\mathcal{E}_1 \cong \omega^{1/2}$, and $\omega^{1/2} \cong \mathcal{E}_1 \cong \mathcal{E}/\mathcal{E}_1 \otimes \omega$. This gives us the short exact sequence:

$$0 \to \omega^{1/2} \to \mathcal{E} \to \omega^{-1/2} \to 0.$$

Since $\mathcal{E}$ is an extension of $\omega^{1/2}$ with $\omega^{-1/2}$, there is only one class of nontrivial (not the same as $\omega^{1/2} \oplus \omega^{-1/2}$) bundle $\mathcal{E}$ up to equivalence.

To find it, consider a vector bundle that trivializes on 2 opens (U_1, U_2) of the curve: the first given by the affine given by $y^2 = f(x)$, and the second given by the affine given by $w^2 = v^{2g+2} f(1/v)$, with the points P_1', P_2', and P_i removed, so that $\left(\frac{x^g}{y}\right)\Big|_{U_2} = P_\infty$. Then setting $r = (\frac{x^g}{y})^{g-1}$, the transition matrix C on $U_1 \cap U_2$ can be written in the form:

$$\begin{bmatrix} r & s \\ 0 & r^{-1} \end{bmatrix},$$

with s a regular function on $U_1 \cap U_2$. Now, suppose there are invertible matrices A and B on U_1 and U_2 respectively such that $BCA^{-1} = \begin{bmatrix} r & 0 \\ 0 & r^{-1} \end{bmatrix}$, i.e.

$$\begin{aligned}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} r & s \\ 0 & r^{-1} \end{bmatrix} &= \begin{bmatrix} rb_{11} & sb_{11} + r^{-1}b_{12} \\ rb_{21} & sb_{21} + r^{-1}b_{22} \end{bmatrix} \\ &= \begin{bmatrix} r & 0 \\ 0 & r^{-1} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \\ &= \begin{bmatrix} ra_{11} & ra_{12} \\ r^{-1}a_{21} & r^{-1}a_{22} \end{bmatrix}.\end{aligned}$$

The following proposition places restrictions on some entries of A and B:

Proposition 7. *Suppose that $\mathcal{E}$ is isomorphic to $\omega^{1/2} \oplus \omega^{-1/2}$. Then a_{11} and a_{22} are nonzero constants and a_{21} is 0.*

Proof. Since a_{11} is regular on U_1, it can only have zeroes but no poles on that cover. Therefore, we must have $v_\infty(a_{11}) \leq 0$. However, since b_{11} is regular

on U_2, it can only have zeroes but no poles on U_2. Therefore, we must have $v_\infty(b_{11}) \geq 0$. Therefore, we have

$$v_\infty(ra_{11}) \leq g-1$$
$$v_\infty(rb_{11}) \geq g-1,$$

and therefore that $v_\infty(ra_{11}) = g-1$ which implies that a_{11} is a constant. Similarly, suppose that $a_{21} \neq 0$. Then $v_\infty(r^{-1}a_{21}) \leq -g+1$. However, we also have $v_\infty(rb_{21}) \geq g-1$, which gives a contradiction. Therefore $a_{21} = 0$. Next, note that since A is invertible, a_{12} and a_{11} cannot both be 0. Lastly, setting $a_{21} = 0$, one uses the same argument to show that a_{22} is a nonzero constant. This proves the proposition. □

This allows us to find a bundle that is not isomorphic to $\omega^{1/2} \oplus \omega^{-1/2}$.

Proposition 8. *Setting $s = \left(\frac{y}{x^g}\right)^g$ gives a bundle that is not isomorphic to $\omega^{1/2} \oplus \omega^{-1/2}$.*

Proof. By Proposition 7, we have

$$\begin{bmatrix} rk & sk + r^{-1}b_{12} \\ 0 & r^{-1}k' \end{bmatrix} = \begin{bmatrix} rk & ra_{12} \\ 0 & r^{-1}k' \end{bmatrix},$$

with k a nonzero constant. We have $v_\infty(s) = -g$, and $v_\infty(r^{-1}b_{12}) \geq -(g-1)$. Therefore we must have $v_\infty(ra_{12}) = -g$, and $v_\infty(a_{12}) = -2g+1$, that is: $a \in \mathcal{L}((2g-1)P_\infty)$. By the Riemann-Roch theorem, this space has dimension $2g-1-g+1 = g$, and so $1, x, \ldots, x^{g-1}$ form a basis for this space. However, each of the basis elements has a pole of even order at P_∞, and so there is no element with a pole of odd order in this space, and a_{12} cannot exist. This proves the proposition. □

Next, we determine the connections allowed on this bundle. As is the case for elliptic curves, the ismorphism $\mathcal{E}_1 \cong \mathcal{E}/\mathcal{E}_1 \otimes \omega$ forces the bottom left entry of our matrix to be a constant. However, the computations for hyperelliptic curves are more complicated because we have 2 case, depending on whether $p \mid g-1$. We first handle the case where $p \nmid g-1$.

Proposition 9. *Let the connection on U_1 be given by*

$$\nabla_1 = d + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{dx}{2y},$$

with a, b, d regular on U_1, and c a nonzero constant. Further suppose that $p \nmid g-1$. Let K be the divisor of $\frac{dx}{2y}$. Then we must have $a, d \in \mathcal{L}(K)$ and we can write $b = kx^{2g-1} + k'yx^{g-2} + b'$ with k, k' determined and $b' \in \mathcal{L}(2K)$. Additionally, c takes on a unique value.

Proof. We compute:

$$\begin{aligned}\nabla_2 &= C\nabla_1 C^{-1} \\ &= d + C(C^{-1})' + CM_1C^{-1} \\ &= d + \begin{bmatrix} -r^{-1}dr & -rds + sdr \\ 0 & r^{-1}dr \end{bmatrix} + \begin{bmatrix} a + r^{-1}sc & r^2b + rsd - rsa - s^2c \\ r^{-2}c & d - r^{-1}sc \end{bmatrix} r^2 \left(r^{-2}\frac{dx}{2y} \right).\end{aligned}$$

To continue, we have to compute dr:

$$\begin{aligned} dr &= d\left(\left(\frac{x^g}{y} \right)^{g-1} \right) \\ &= \left(d\left(\frac{x^g}{y} \right) \right)(g-1)\left(\frac{x^g}{y} \right)^{g-2} \\ &= \frac{x^g}{y}\left(\frac{gdx}{x} - \frac{dy}{y} \right)(g-1)\left(\frac{x^g}{y} \right)^{g-2} \\ &= (g-1)r^3\left(\frac{2gy}{x} - \frac{f'(x)}{y} \right)\left(\frac{dx}{2y}r^{-2} \right) \\ &= (g-1)r^3\left(\frac{2gf(x) - xf'(x)}{xy} \right)\left(\frac{dx}{2y}r^{-2} \right). \end{aligned}$$

Similarly, we have:

$$\begin{aligned} ds &= g\left(\frac{y}{x^g} \right)^{g-1}\left(\frac{dy}{x^g} - \frac{gydx}{x^{g+1}} \right) \\ &= rg\left(\frac{xf'(x) - 2gf(x)}{x^{g+1}} \right)\left(\frac{dx}{2y}r^{-2} \right), \end{aligned}$$

and therefore

$$\begin{aligned} sdr - rds &= (g-1)r^2\left(\frac{xf'(x) - 2gf(x)}{x^{g+1}} \right)\left(\frac{dx}{2y}r^{-2} \right) + r^2 g\left(\frac{xf'(x) - 2gf(x)}{x^{g+1}} \right)\left(\frac{dx}{2y}r^{-2} \right) \\ &= (2g-1)r^2\left(\frac{xf'(x) - 2gf(x)}{x^{g+1}} \right)\left(\frac{dx}{2y}r^{-2} \right). \end{aligned}$$

We compute $v_\infty(r^3\left(\frac{2gf(x)-xf'(x)}{xy}\right))$. Note that $2gf(x)-xf'(x)$ has degree $2g+1$ and hence a pole of order $4g+2$ at P_∞. Thus $v_\infty(r^3\left(\frac{2gf(x)-xf'(x)}{xy}\right)) = 3g-3+2g+3-4g-2 = g-2$. Therefore $r^{-1}dr = F(x,y)(r^{-2}\frac{dx}{2y})$ with $v_\infty(F(x,y)) = -1$. Similarly, we have $v_\infty(r^2\left(\frac{xf'(x)-2gf(x)}{x^{g+1}}\right)) = 2g-2+2g+2-2(2g+1) = -2$, and $sdr - rds = G(x)(r^{-2}\frac{dx}{2y})$ with $v_\infty(G(x)) = -2$.

We now examine the restrictions on a, b, c, d. First, $r^2a + rsc - F(x,y)$ must be regular on U_2. We only have to check behavior at P_∞. $F(x,y)$ has a pole of

order 1 at P_∞, and so does rsc (recall that c is a nonzero constant). Therefore $v_\infty(r^2 a) \geq -1$ and $v_\infty(a) \geq 1 - 2g$. As reasoned in the proof of Proposition 8, a can't have a pole of order $2g-1$ at P_∞ and thus we have $a \in \mathcal{L}(K)$. Since we are working with SL_2 opers, we require that the matrix of the connection be traceless; i.e. $a = -d$. This gives the same restriction for d. Lastly, note that the pole from rsc must cancel the pole from $F(x, y)$. This gives us a unique value for c.

Next, $r^4 b + r^3 sd - r^3 sa - r^2 s^2 c + G(x)$ must be regular on U_2. Again, it suffices to check regularity at P_∞. Note that since $a, d \in \mathcal{L}(K)$, $r^3 sd - r^3 sa$ has a pole of order at most 1 at P_∞. Now, c was chosen so that $rsc - F(x, y)$ has no pole at P_∞. Multiplying throughout by $rs = \frac{y}{x^g}$, we find that $r^2 s^2 c - \frac{g-1}{2g-1} G(x)$ has no pole at P_∞, so $-r^2 s^2 c + G(x)$ has a pole of order 2 at P_∞. Therefore $v_\infty(r^4 b) = -2$ and $v_\infty(b) = 2 - 4g$, and $b \in \mathcal{L}((4g-2)P_\infty)$. Again, by Riemann-Roch, $l((4g-2)P_\infty) = 3g - 1$. Therefore $1, x, \ldots, x^{2g-1}, y, yx, \ldots, yx^{g-2}$ is a basis for this space. Hence by choosing the coefficient of x^{2g-1} appropriately, we can cancel the pole at P_∞. Furthermore, since $G(x)$ is a rational function in x, it will not have a pole of odd order. This means that after the cancellation, $G(x) - kx^{2g-1}$ will not have a pole at P_∞. Finally, to cancel the pole of order 1 contributed by $r^3 sd - r^3 sa$, we will need a yx^{g-2} term. Hence we can write $b = kx^{2g-1} + k' yx^{g-2} + b'$ where $b' \in \mathcal{L}(2K)$. This proves the proposition. $\square$

Finally, we determine c and k. We compute:

$$F(x, y) + krs = \frac{(g-1)x^{g(2g-2)+g-1}(2gf(x) - xf'(x)) + ky^{2g}}{x^g y^{2g-1}}.$$

It suffices to cancel the highest power term in the numerator, $x^{(2g+1)g}$. Using the relation $y^2 = f(x)$, and the assumption that f is monic, we get that $c = (g-1)$. Similarly, to find k, we compute:

$$\begin{aligned} &G(x, y) - (g-1)(y/x^g)^2 + kr^4 x^{2g-1} \\ &= \frac{-(g-1)y^{2+4(g-1)} - (2g-1)x^{2g(g-1)+g-1} y^{2(g-1)}(xf'(x) - 2gf(x)) + kx^{4g(g-1)+2g-1+2g}}{y^{4(g-1)} x^{2g}}. \end{aligned}$$

Therefore we can set $k = g$.

Remark 10. *Note that since $r^{-1}dr$ has a pole of order 1 at P_∞, one can show that oper-like connections do not exist on $\omega^{1/2} \oplus \omega^{-1/2}$.*

Now, in the case where $p \mid g - 1$, we have $dr = 0$. This means that the pole contributed by rsc can't be cancelled by $r^{-1}dr$; hence opers cannot exist on the nontrivial extension. The only possibility then is for opers to exist on the trivial extension. The next proposition handles this case.

Proposition 11. *Let the connection on U_1 be given by*

$$\nabla_1 = d + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{dx}{2y},$$

with a, b, d regular on U_1, and c a nonzero constant. Further suppose that $p \mid g-1$. Let K be the divisor of $\frac{dx}{2y}$. Then we must have $a, d \in \mathcal{L}(K)$ and $b \in \mathcal{L}(2K)$, and c a nonzero constant.

Proof. We compute:

$$\begin{aligned} \nabla_2 &= C\nabla_1 C^{-1} \\ &= d + C(C^{-1})' + CM_1C^{-1} \\ &= d + \begin{bmatrix} -r^{-1}dr & 0 \\ 0 & r^{-1}dr \end{bmatrix} + \begin{bmatrix} a & r^2 b \\ r^{-2}c & d \end{bmatrix} r^2 \begin{pmatrix} r^{-2}\frac{dx}{2y} \end{pmatrix}. \end{aligned}$$

As discussed above, since $p \mid g-1$, $dr = 0$ and therefore the only restrictions are r^2a, r^2d and r^4b are regular at P_∞. The proposition follows. □

Next, we determine the automorphisms of $\mathcal{E}$ that preserve the transition matrix to determine the isomorphic connections. First, notice that if A is an automorphism of the vector bundle on U_1, then the automorphism B on U_2 is completely determined: $B = CAC^{-1}$. The following proposition makes use of this fact to determine the set of such automorphism:

Proposition 12. *Let $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be an automorphism of the bundle on U_1 such that the transition matrix is preserved. Then $a_{21} = 0$, $a_{11} = k_1$ and $a_{22} = k_2$ (where k_1 and k_2 are nonzero constants), and $a_{12} \in \mathcal{L}(K)$. Further suppose that $p \nmid g-1$. Then we must also have $k_1 = k_2$.*

Proof. We compute:

$$\begin{aligned} B &= \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ &= \begin{bmatrix} r & s \\ 0 & r^{-1} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} r^{-1} & -s \\ 0 & r \end{bmatrix} \\ &= \begin{bmatrix} a_{11} + r^{-1}sa_{21} & r^2a_{12} + rsa_{22} - rsa_{11} - s^2a_{21} \\ r^{-2}a_{21} & -sr^{-1}a_{21} + a_{22} \end{bmatrix}. \end{aligned}$$

First consider the case of the nontrivial extension. Since b_{21} must be regular on U_2, it can't have a pole at P_∞. Therefore we must have $a_{21} = 0$. Then this means that a_{11} and a_{22} are both regular on U_2 too, and hence are nonzero constants (as A must be an invertible matrix). Finally, $r^2a_{12} + rs(a_{22} - a_{11})$ must be regular on U_2. However, rs will have a pole of order 1 at P_∞. Additionally,

as reasoned in the proof of Proposition 8, a can't have a pole of order $2g-1$ at P_∞ and hence we must have $a_{22} = a_{11}$. This then implies that $a_{12} \in \mathcal{L}(K)$, as asserted.

Next, if the extension is trivial, $s = 0$. Then the only restrictions are that $a_1 1$, $a_2 2$ are regular on the entire variety and hence constants, and that $r^2 a_{12}$ has no pole at P_∞. The proposition follows. □

Next, we conjugate the connection with the automorphisms. Let $A = \begin{bmatrix} k & t \\ 0 & k \end{bmatrix}$. Then we obtain:

$$\begin{aligned} \nabla_1' &= A\nabla_1 A^{-1} \\ &= d + A(A^{-1})' + A \begin{bmatrix} a & b \\ c & -a \end{bmatrix} A^{-1} \\ &= d + \begin{bmatrix} 0 & -kdt \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a + \frac{tc}{k} & b + \frac{td}{k} - t^2 c - kta \\ c & -a - \frac{tc}{k} \end{bmatrix}. \end{aligned}$$

Notice that by setting $t = -\frac{ka}{c}$, we obtain a connection given by a matrix with both top left and bottom right entries 0. Additionally, if we originally had $a = 0$, then conjugation by an automorphism cannot give a different matrix with a still equal 0. Finally, in the notation used in Proposition 9, notice that k' was chosen to cancel the pole contributed by $r^3 sd - r^3 sa$. However, when we have $a = d = 0$, we will have $k' = 0$. In addition, if $p \mid g-1$, then we can choose the top left entry and bottom left entry to be different. By setting $a_{11} = \sqrt{c}$ and $a_{22} = 1/\sqrt{c}$, we can set the bottom left entry of the matrix of the connection to 1. Hence we have obtained a description of all connections up to isomorphism. This discussion is summed up in the proposition below.

Proposition 13. *The connections, up to isomorphism, can be given by matrices of the form*

$$\begin{bmatrix} 0 & kx^{2g-1} + b \\ c & 0 \end{bmatrix},$$

with c and k nonzero constants uniquely determined, and $b \in \mathcal{L}(2K)$. If, in addition, $p \mid g-1$, then we have $c = 1$ and $k = 0$. Otherwise, $k = g$ and $c = g-1$.

To calculate the p-curvature map, we can reuse the method used in the proof of Proposition 5, the only difference being that we can differentiate the matrix in this case. The following proposition naturally follows.

Proposition 14. *Let ∇ be a connection given by $\nabla = d + M\frac{dx}{2y}$. Then*

$$\nabla(v)^p = v^p + M^p \left(\frac{v(x)}{2y}\right)^p + Mv^p \left(\frac{dx}{2y}\right) + v^{p-1}(M)\frac{v(x)}{2y}.$$

Unfortunately, we have not been able to find a good choice of v that makes computation of the $v^{p-1}M$ easy.

9 Acknowledgements

I would like to thank my mentor, Pablo Boixeda, for guiding and helping me with this project. I would also like to thank my faculty advisor, Professor Roman Bezrukavnikov, for suggesting this excellent project. In addition, I would like to thank the MIT Department of Mathematics for organizing this UROP+ program. Finally, I would like to thank the Ralph L. Evans (1948) Endowment Fund for supporting and funding this project.

10 References

References

[BTCZ16] Roman Bezrukavnikov, Roman Travkin, Tsao-Hsien Chen, and Xinwen Zhu. Quantization of hitchin integrable system via positive characteristic, 2016.

[FKO87] Voloch Jos Felipe and Sthr Karl-Otto. A formula for the cartier operator on plane algebraic curves. *Journal fur die reine und angewandte Mathematik (Crelles Journal)*, 1987(377), 1987.

[Har79] Robin Hartshorne. *Algebraic geometry, Arcata 1974:*. American Mathematical Society, 1979.

[Man65] Ju. I. Manin. The hasse-witt matrix of an algebraic curve. *Fifteen Papers on Algebra American Mathematical Society Translations: Series 2*, page 245264, 1965.

[Sha97] Igor Rostislavovich Shafarevich. *Basic algebraic geometry*. Springer-Verlag, 1997.

[Sil09] Joseph H. Silverman. *Arithmetic of Elliptic Curves (Graduate texts in mathematics ; 106)*. Springer, 2009.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Springer, 2009.

[Was08] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. Chapman Hall/CRC, 2008.