AWS 2000 PROJECT DESCRIPTION: A DETERMINANTAL PROCEDURE FOR CALCULATING JACOBIANS OF GENUS 1 CURVES

GREG W. ANDERSON

1. A recipe for the Jacobian of a genus one curve

1.1. **The setting.**

- Let k be a field of characteristic 0.
- Let X/k be a smooth geom. irr. proj. curve of genus 1.
- Fix $0 \neq \omega_X \in H^0(X, \Omega_X)$.
- Fix a closed point ∞ of X.
- Let $k(\infty)$ be the residue field of ∞.
- Put $n := [k(\infty) : k]$.
- Let K/k be the function field of X/k.
- Let K_∞ be the ∞-adic completion of K.
- Let $\mathcal{O}_\infty$ be the valuation subring of K_∞.
- Identify $k(\infty)$ with a subfield of K_∞ via the Teichmüller lifting.
- Fix a uniformizer $t \in K_\infty$ such that $\mathrm{trace}_{k(\infty)/k} \mathrm{Res}_\infty t^{-1}\omega_X = 1$.
- Let A be the ring of functions on X regular away from ∞.
- Let $k[\epsilon]$ be a k-algebra generated by a nilpotent element ϵ.
- Let m be the smallest nonnegative integer such that $\epsilon^{m+1} = 0$.
- Assume that $m \geq 7$.
- We use the abbreviated notation $?[\epsilon]$ for the functor $? \otimes_k k[\epsilon]$.

1.2. **Definition of E, $\wp$, z, g_2, g_3, and c_n.** Let E/k be the Jacobian of X/k. Then E/k is an elliptic curve acting on X/k in such a way as to make the latter a principal homogeneous space, and in this situation $H^0(E, \Omega_E)$ and $H^0(X, \Omega_X)$ are canonically isomorphic. Let ω_E be the differential on E corresponding to ω_X. Let O be the neutral element of E and let z be the unique uniformizer at O such that $dz = \omega_E$. Let $\wp$ be the unique function on E regular away from O such that $\wp - \frac{1}{z^2}$ vanishes to order 2 at O. There exist unique $g_2, g_3 \in k$ such that

$$\left(\frac{d\wp}{dz}\right)^2 = 4\wp^3 - g_2\wp - g_3.$$

Date: February 7, 2000.

Knowledge of the coefficients g_2 and g_3 is equivalent to knowledge of the Jacobian of X. Let

$$\frac{d\wp}{dz} = -\frac{2}{z^3} + \frac{g_2 z}{10} + \frac{g_3 z^3}{7} + \cdots = -\frac{2}{z^3} + c_1 z + c_3 z^3 + c_5 z^5 + \dots$$

be the Laurent expansion of $\frac{d\wp}{dz}$ at O in powers of z. Knowledge of the coefficients c_1 and c_3 is equivalent to knowledge of the coefficients g_2 and g_3. The c's turn out to be just a bit more convenient to work with than the g's.

1.3. **A Riemann-Roch exercise.** Given $f \in A$ with Laurent expansion

$$f = \sum_i a_i t^i \quad (a_i \in k(\infty))$$

at ∞, put

$$\lambda(f) := \frac{1}{n} \operatorname{trace}_{k(\infty)/k} a_0$$

thus defining a k-linear functional

$$\lambda : A \to k$$

such that $\lambda(1) = 1$. By the Riemann-Roch theorem, the sequence

$$0 \to k \subset A \xrightarrow{a \mapsto a + \mathcal{O}_\infty} K_\infty/\mathcal{O}_\infty \xrightarrow{f \mapsto \operatorname{trace}_{k(\infty)/k} \operatorname{Res}_\infty f\omega} k \to 0$$

is exact. It follows that there exists a unique k-linear isomorphism

$$\phi : K_\infty/\mathcal{O}_\infty \tilde{\to} A$$

such that

$$\phi(t^{-1} + \mathcal{O}_\infty) = 1$$

and

$$\phi(a + \mathcal{O}_\infty) = a - \lambda(a)$$

for all $a \in A$. For each positive integer N let

$$\phi_N : t^{-N}\mathcal{O}_\infty/\mathcal{O}_\infty \to A$$

be the restriction of ϕ to $t^{-N}\mathcal{O}_\infty/\mathcal{O}_\infty$.

1.4. **The τ-construction.** For each positive integer N and

$$f = \sum_i a_i t^i \in K_\infty \quad (a_i \in k(\infty))$$

put

$$\mathrm{trunc}_N\, f := \sum_{i \in \mathbb{Z} \cap [-N,0)} a_i t^i + \mathcal{O}_\infty \in t^{-N}\mathcal{O}_\infty/\mathcal{O}_\infty$$

thereby defining a $k(\infty)$-linear map

$$\mathrm{trunc}_N : K_\infty \to t^{-N}\mathcal{O}_\infty/\mathcal{O}_\infty.$$

Put

$$\exp(\epsilon/t) := \sum_{n=0}^{\infty} \frac{(\epsilon/t)^n}{n!} = \sum_{n=0}^{m} \frac{(\epsilon/t)^n}{n!} \in K_\infty[\epsilon]^\times.$$

For each positive integer N let $\tau_N \in k[\epsilon]$ be the determinant over $k[\epsilon]$ of the composite map

$$\left(\frac{t^{-N}\mathcal{O}_\infty}{\mathcal{O}_\infty}\right)[\epsilon] \xrightarrow{\phi_N[\epsilon]} A[\epsilon] \xrightarrow{a \mapsto \exp(\epsilon/t)a} K_\infty[\epsilon] \xrightarrow{\mathrm{trunc}_N[\epsilon]} \left(\frac{t^{-N}\mathcal{O}_\infty}{\mathcal{O}_\infty}\right)[\epsilon].$$

(This map is represented by an Nn by Nn matrix with entries in $k[\epsilon]$.) For $N \geq m$ the determinant τ_N is independent of N. We denote the common values of the τ_N for large N by τ. One has

$$\tau = \epsilon u$$

for some $u \in k[\epsilon]^\times$ well defined modulo ϵ^m. The third derivative of $\log u$ with respect to ϵ is well defined modulo ϵ^{m-3}. I am able to show that

$$-\frac{d^3 \log u}{d\epsilon^3} \equiv c_1\epsilon + c_3\epsilon^3 + \ldots \bmod \epsilon^{m-3}$$

by applying fermionic Fock space technology. In particular, one can recover c_1 and c_3 in this way and hence recover the Jacobian of X. The upshot is that the τ-construction "is" a computation of the Jacobian of X. The τ-construction is a standard item in soliton theory; for background see [Segal-Wilson].

2. Project description

2.1. **The challenge.** Turn the τ-construction into a practical method for computing Jacobians of genus one curves. Write some computer code and try to get a feeling for the complexity of the calculation by running test cases. For $n = 2$ you can check your results against Weil's calculations [Weil 1954]. For $n = 3$ and $n = 4$ you can check your results against those of McCallum and company; see the AWS

1999 web site for details and links. See also the 1999 Harvard thesis of C. O'Neil. Cassells has observed that the Jacobian of the smooth projective curve

$$Ax^3 + By^3 + Cz^3 = 0 \ \ (ABC \neq 0)$$

is

$$ABCx^3 + y^3 + z^3;$$

you could use this fact as another check of your work. (I thank Barry Mazur for bringing this last example to my attention.) For general n it is a wide open problem to design a really efficient method of computation. It seems likely that symmetric function theory will be useful; see the first chapter of [Macdonald] for an overview of basic facts. Since the fermionic Fock space technology is used to prove that the "τ-recipe" works, perhaps FFS technology will also be useful for computations; see my (ever-evolving) notes on fermionic Fock space (currently in a terse state but filled with curious examples) on my web page `www.math.umn.edu/~gwanders`. I did manage in the case $n = 2$ with the help of MAPLE to recover Weil's formulas for g_2 and g_3, but I set up the computations in a brutally inefficient way and found myself operating at the edge of combinatorial disaster. Finesse is definitely called for!

2.2. **The mystery.** Weil's computation of g_2 and g_3 in the case $n = 2$ was an inspired piece of salvage work: the necessary formulas came from the theory of invariants of binary biquadratic forms and had been written down long before Weil was born. Similar salvage work has been done in the cases $n = 3$ and $n = 4$. Can one give a satisfying explanation for this connection between 19^{th} century invariant theory and the problem of computing Jacobians of genus one curves? Can the connection be extended so as to account for all the c's for any n? By carefully analyzing the process of computing g_2 and g_3 via the calculation of τ you might be preparing yourself to make a discovery that dispels the mystery. Good luck!

2.3. **Sample calculation of τ in the case $n = 1$.** We specialize thus:

- Take $k = \mathbb{Q}(g_2, g_3)$, where g_2 and g_3 are algebraically independent.
- Take X/k to be the smooth projective plane curve with affine model $y^2 = 4x^3 - g_2x - g_3$.
- Take $\omega_X = dx/y$.
- Take ∞ to be the point at infinity.
- Take $t = 1/\sqrt{x}$.
- Assume that $m = 7$ and hence $\epsilon^8 = 0$.

Of course the calculation of τ in this special case does not reveal anything you don't already know about the Jacobian of X, but it might give you some ideas for setting up (and checking) τ-calculations in a way that a standard software package like MAPLE could handle. Anyway, it turns out that you can obtain τ by multiplying a certain 7 by 14 matrix by a certain 14 by 7 matrix, and then calculating the determinant of the resulting 7 by 7 matrix. Here's the first matrix:

$$\begin{bmatrix}
1 & 0 & 0 & 0 & -\frac{g_2}{8} & 0 & -\frac{g_3}{8} & 0 & -\frac{g_2^2}{128} & 0 & -\frac{g_2 g_3}{64} & 0 & -\frac{g_3^2}{128} - \frac{g_2^3}{1024} & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & -\frac{g_2}{8} & 0 & -\frac{g_3}{8} & 0 & -\frac{g_2^2}{128} & 0 & -\frac{g_2 g_3}{64} & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -\frac{g_2}{8} & 0 & -\frac{g_3}{8} & 0 & -\frac{g_2^2}{128} & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.$$

The entries of this matrix are derived in a more or less obvious way from the Laurent expansion

$$y = t^{-3}\left(1 - \frac{g_2}{8}t^4 - \frac{g_3}{8}t^6 - \frac{g_2^2}{128}t^8 - \frac{g_2 g_3}{64}t^{10} + \left(-\frac{g_3^2}{128} - \frac{g_2^3}{1024}\right)t^{12} + \dots\right).$$

Here's the second matrix:

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\epsilon & 1 & 0 & 0 & 0 & 0 & 0 \\
1/2\,\epsilon^2 & \epsilon & 1 & 0 & 0 & 0 & 0 \\
1/6\,\epsilon^3 & 1/2\,\epsilon^2 & \epsilon & 1 & 0 & 0 & 0 \\
1/24\,\epsilon^4 & 1/6\,\epsilon^3 & 1/2\,\epsilon^2 & \epsilon & 1 & 0 & 0 \\
\frac{1}{120}\,\epsilon^5 & 1/24\,\epsilon^4 & 1/6\,\epsilon^3 & 1/2\,\epsilon^2 & \epsilon & 1 & 0 \\
\frac{1}{720}\,\epsilon^6 & \frac{1}{120}\,\epsilon^5 & 1/24\,\epsilon^4 & 1/6\,\epsilon^3 & 1/2\,\epsilon^2 & \epsilon & 1 \\
\frac{1}{5040}\,\epsilon^7 & \frac{1}{720}\,\epsilon^6 & \frac{1}{120}\,\epsilon^5 & 1/24\,\epsilon^4 & 1/6\,\epsilon^3 & 1/2\,\epsilon^2 & \epsilon \\
0 & \frac{1}{5040}\,\epsilon^7 & \frac{1}{720}\,\epsilon^6 & \frac{1}{120}\,\epsilon^5 & 1/24\,\epsilon^4 & 1/6\,\epsilon^3 & 1/2\,\epsilon^2 \\
0 & 0 & \frac{1}{5040}\,\epsilon^7 & \frac{1}{720}\,\epsilon^6 & \frac{1}{120}\,\epsilon^5 & 1/24\,\epsilon^4 & 1/6\,\epsilon^3 \\
0 & 0 & 0 & \frac{1}{5040}\,\epsilon^7 & \frac{1}{720}\,\epsilon^6 & \frac{1}{120}\,\epsilon^5 & 1/24\,\epsilon^4 \\
0 & 0 & 0 & 0 & \frac{1}{5040}\,\epsilon^7 & \frac{1}{720}\,\epsilon^6 & \frac{1}{120}\,\epsilon^5 \\
0 & 0 & 0 & 0 & 0 & \frac{1}{5040}\,\epsilon^7 & \frac{1}{720}\,\epsilon^6 \\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{5040}\,\epsilon^7
\end{bmatrix}$$

You get

$$\tau = \epsilon - \frac{g_2}{240}\,\epsilon^5 - \frac{g_3}{840}\epsilon^7$$

after multiplying the preceding matrices and taking the determinant.

3. Other suggested reading

Students need to have a grasp of the basic theory of algebraic functions of one variable up to and including the notion of the adèle ring of a function field; for this material I suggest the book [Artin]. The papers [Tate] and [AdCK] are crucially important steps in the evolution of the notion of fermionic Fock space.

References

[AdCK] Arbarello E., de Concini, C., Kac, V.: *The infinite wedge representation and the reciprocity law for algebraic curves.* in: Theta functions—Bowdoin 1987, Part 1 (Brunswick, ME 1987), 171–190.

[Artin] Artin, E.: *Algebraic Numbers and Algebraic Functions.* Gordon and Breach, New York 1967

[Macdonald] *Symmetric Functions and Hall Polynomials*, 2^{nd} ed., Oxford University Press 1995.

[Segal-Wilson] Segal, G., Wilson, G.: *Loop groups and equations of KdV type.* Inst. Hautes Etudes Sci. Publ. Math. **61**(1985)5–65

[Tate] Tate, J.: *Residues of differentials on curves.* Ann. Sci. Ecole Norm. Sup. (4) 1 (1968) 149–159

[Weil 1954] Weil, A.: *Remarques sur un mémoire d'Hermite.* Arch. d. Math. **5**(1954)197-202 (=[1954a], Collected Papers, Vol. II, Springer Verlag, New York 1980, ISBN 0-387-90330-5.)

University of Minnesota, Minneapolis, MN 55455
E-mail address: gwanders@math.umn.edu