Examples Coleman

Jennifer Balakrishnan and Jan Tuitman

October 29, 2017

Abstract

This text is about the Coleman Magma library for computing Coleman integrals on arbitrary smooth projective curves building on the algorithm from [2, 3]. It serves both as as collection of examples and as a user's guide.

1 An elliptic curve

The code is loaded as follows:

```
load "coleman.m";
```

A curve X is specified by a polynomial $f \in \mathbb{Z}[x][y]$ monic in y defining a (possibly singular) plane model of the curve. Moreover, the user has to choose a prime number p and an initial p-adic precision N. For example:

```
>f:=y^2-(x^3-10*x+9);
>p:=5;
>N:=10;
>data:=coleman_data(f,p,N);
```

Now `data` is a record that contains a lot of information useful for Coleman integration. For example:

```
> data‘W0;
[1 0]
[0 1]
> data‘Winf;
[    1     0]
[    0 1/x^2]
```

means that $b^0 = [1, y]$ and $b^\infty = [1, y/x^2]$ are integral bases for the function field of X over $\mathbb{Q}[x]$ and $\mathbb{Q}[1/x]$, respectively. Note that the i-th row contains the coefficients of the i-th basis vector with respect to $[1, y]$. The b^0_i should be thought of as coordinates on the affine chart $x \neq \infty$ of X and the b^∞_i as coordinates on the affine chart $x \neq 0$ of X. Moreover,

```
> data‘r;
x^3 - 10*x + 9
```

is the polynomial the zeros of which we have taken out of X (along with all points at $x = \infty$) to represent the De Rham cohomology space $\mathrm{H}^1_{\mathrm{dR}}(X)$, and

```
> data‘basis;
[
    (0 1),
    (0 x)
]
```

means that a basis for $\mathrm{H}^1_{\mathrm{dR}}(X)$ is given by $[\omega_1, \omega_2]$ where:

$$\omega_1 = (0 \cdot b^0_1 + 1 \cdot b^0_2)dx/z,$$
$$\omega_2 = (0 \cdot b^0_1 + x \cdot b^0_2)dx/z,$$

and z is $r(x)$ divided by its leading coefficient. Since in this case we have $z = r(x) = y^2$ and $b^0 = [1, y]$, this means that $[\omega_1, \omega_2] = [dx/y, dx/y^2]$, which is the well known basis from e.g. Kedlaya's algorithm. Finally,

```
> data‘F;
[ 3129195 -3784615]
[ 3553247 -3129195]
```

is the matrix of p-th power Frobenius on $\mathrm{H}^1_{\mathrm{dR}}(X)$ to p-adic precision N with respect to this basis.

Now we want to define some points. For points that do not lie in a bad disk, i.e. the residue disk modulo p of a point taken out of X, one can just specify their x and y coordinates:

```
> P1:=set_point(0,3,data);
> P2:=set_point(8,21,data);
```

When `W0` is not the identity and the point lies in a bad residue disk, one has to specify the values of x and the b^0_i if the point is finite and the values of $1/x$ and the b^∞_i if the point lies at infinity. For example:

```
> P3:=set_bad_point(1,[1,0],false,data);
> P4:=set_bad_point(0,[1,0],true,data);
```

means that `P3` is a point which is not infinite and therefore given by $x = 1, [1, y] = [1, 0]$ while `P4` is infinite and therefore given by $1/x = 0, [1, y/x^2] = [1, 0]$. Note that `P3` could also have been defined by

```
> P3:=set_point(1,0,data)
```

since `W0` is the identity matrix.

Let us now compute some integrals. To compute the integrals of ω_1, ω_2 from `P1` to `P2`:

```
> coleman_integrals_on_basis(P1,P2,data);
(-117821*5^2 + O(5^10) 1503616 + O(5^10))
9
```

Here the 9 means that the results are provably correct to absolute p-adic precision 9, i.e. in the process of computing these integrals we may have lost 1 digit of p-adic precision. It would be better to absorb this information into the Big-Oh notation, but this causes some problems, so for now the code returns every answer with a separate absolute precision and the Big-Oh's should be ignored.

If an integral involves a point in a bad disk like P3 or P4, then the Frobenius structure only converges near the boundary of this disk. To get close enough to the boundary of the disk, in the computation we have to consider points over totally ramified extensions $\mathbb{Q}_p(p^{1/e})$ for some large enough integer e. We have good bounds for how large e should be, but it is not so clear what the most efficient value is in practice. Therefore, for now the value of e is not chosen by the code but specified by the user. Note that this does not affect provable correctness of the result, since if e is too small no result or a result with no precision will be returned.

```
>coleman_integrals_on_basis(P1,P3,data:e:=100);
(O(5^10) O(5^10))
9
> coleman_integrals_on_basis(P2,P4,data:e:=100);
(117821*5^2 + O(5^10) -1503616 + O(5^10))
9
```

2 A plane quartic curve of rank 0

This time we take the plane quartic curve X from [1, Proposition 12.16] which we dehomogenise with respect to z. We again take $p = 5$ and initial p-adic precision $N = 10$.

```
f:=y^3 + (-x^2 - x)*y^2 + x^3*y - x^2 + x;
p:=5;
N:=10;
data:=coleman_data(f,p,N);
```

This time we have:

```
> data`W0;
[1 0 0]
[0 1 0]
[0 0 1]
> data`Winf;
[     1      0      0]
[     0 1/x^2      0]
[     0  -1/x 1/x^3]
```

which means that b^0 is given by $[1, y, y^2]$ (i.e. there are no singularities in the affine x, y plane) and b^∞ is given by $[1, y/x^2, -y/x + y^2/x^3]$.

There are 3 finite points:

```
P1:=set_point(1,1,data);
P2:=set_point(0,0,data);
P3:=set_point(1,0,data);
```

and 3 infinite ones:

```
P4:=set_bad_point(0,[1,0,-1],true,data);
P5:=set_bad_point(0,[1,1,0],true,data);
P6:=set_bad_point(0,[1,0,0],true,data);
```

The Jacobian of X has rank zero, so all divisors $P_i - P_j$ are torsion. The basis $[\omega_1, \ldots, \omega_6]$ for $\mathrm{H}^1_{\mathrm{dR}}(X)$ is computed in such a way that $\omega_1, \omega_2, \omega_3$ are regular 1-forms. Note that the integral of a regular 1-form over a torsion divisor vanishes. We can check this as follows:

```
 > coleman_integrals_on_basis(P1,P2,data:e:=100);
(O(5^9) O(5^9) O(5^9) 927458 + O(5^9) 119818 + O(5^9) 574741 + O(5^9))
9
> coleman_integrals_on_basis(P1,P3,data:e:=100);
(O(5^9) O(5^9) O(5^9) 834001 + O(5^9) -617662 + O(5^9) -45916*5 + O(5^9))
9
> coleman_integrals_on_basis(P1,P4,data:e:=100);
(O(5^9) O(5^9) O(5^9) -474916 + O(5^9) -59909 + O(5^9) 689644 + O(5^9))
9
> coleman_integrals_on_basis(P1,P5,data:e:=100);
(O(5^9) O(5^9) O(5^9) -779911 + O(5^9) 645229 + O(5^9) 230032 + O(5^9))
9
> coleman_integrals_on_basis(P1,P6,data:e:=100);
(O(5^9) O(5^9) O(5^9) 130951 + O(5^9) -225866 + O(5^9) 804547 + O(5^9))
9
```

3 The modular curve $X_0(44)$

So far we have only seen examples for which the plane model did not have any singularities in the affine x, y plane, i.e. W0 was always the identity matrix. However, our algorithm and implementation can be applied in complete generality. We take a defining equation for $X = X_0(44)$ from [4] and work with the prime $p = 7$ this time (for $p = 5$ our good reduction condition is not satisfied).

```
f:=y^5+12*x^2*y^3-14*x^2*y^2+(13*x^4+6*x^2)*y-(11*x^6+6*x^4+x^2);
p:=7;
N:=10;
data:=coleman_data(f,p,N);
```

Now the integral bases (i.e. the coordinates on X) are a lot more complicated:

```
> data`W0;
[                         1                                 0                              0                    0                    0]
[                         0                                 1                              0                    0                    0]
[                         0                                 0                              1                    0                    0]
[                         0                                 0                              0                  1/x                    0]
[ -10*x^3/(x^4 + 6*x^2 + 1) (-6*x^3 - 13*x)/(x^4 + 6*x^2 + 1) (x^3 + 12*x)/(x^4 + 6*x^2 + 1)  -x/(x^4 + 6*x^2 + 1)  1/(x^5 + 6*x^3 + x)]
> data`Winf;
[                         1                               0                               0                               0                    0]
[                         0                           1/x^2                               0                               0                    0]
[                         0                               0                           1/x^3                               0                    0]
[                         0                               0                               0                           1/x^4                    0]
[ -10*x^3/(x^4 + 6*x^2 + 1)  (23*x^2 + 6)/(x^5 + 6*x^3 + x)   (6*x^2 - 1)/(x^5 + 6*x^3 + x) (6*x^2 + 1)/(x^7 + 6*x^5 + x^3)  1/(x^5 + 6*x^3 + x)]
```

In particular W0 is not the identity, so the plane model has singularities at the affine x, y plane. We start by finding a couple of obvious points. First a finite point that does not lie in a bad disk:

```
P1:=set_point(1,1,data);
```

then a finite point which does lie in a bad disk (lying over a singularity of the plane model):

```
P2:=set_bad_point(0,[1,0,0,0,0],false,data);
```

and finally a point in a infinite disk:

```
P3:=set_bad_point(0,[1,0,0,0,0],true,data);
```

It turns out that `P1-P2` and `P1-P3` are torsion, so the integrals of all regular 1-forms over these divisors vanish. We can check this as follows:

```
> coleman_integrals_on_basis(P1,P2,data:e:=100);
(3*7^9 + O(7^10) O(7^9) O(7^9) O(7^9) -10971845 + O(7^9)
4086575*7^-1 + O(7^8) -16736670 + O(7^9) -4312348*7^-1 + O(7^8))
5
> coleman_integrals_on_basis(P1,P3,data:e:=100);
(O(7^9) O(7^9) O(7^9) O(7^9) -11056758 + O(7^9) 4086575*7^-1 + O(7^8)
-1605787 + O(7^9) -4312348*7^-1 + O(7^8))
7
```

4 Conclusion

The code is still very much work in progress. For example, double integrals will be added in the near future. Please email comments, suggestions and bugs to jan.tuitman@kuleuven.be.

References

[1] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80.

[2] Jan Tuitman, *Counting points on curves using a map to* $\mathbf{P}^1$, Math. Comp. **85** (2016), no. 298, 961–981.

[3] ______, *Counting points on curves using a map to* $\mathbf{P}^1$*, II*, Finite Fields Appl. **45** (2017), 301–322.

[4] Yifan Yang, *Defining equations of modular curves*, Advances in Mathematics **204** (2006), 481–508.