Examples Coleman

Jennifer Balakrishnan and Jan Tuitman

December 4, 2017

Abstract

This text is about the Coleman Magma library for computing Coleman integrals on arbitrary smooth projective curves building on the algorithm from [3, 4]. 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:

$$\omega_1 = (0 \cdot b_1^0 + 1 \cdot b_2^0)dx/z,$$
$$\omega_2 = (0 \cdot b_1^0 + x \cdot b_2^0)dx/z,$$

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_i^0 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);
(O(5^9) 6 + O(5^9))
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.

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);
(-38429*5^2 + O(5^9) 89903*5 + O(5^9))
9
> coleman_integrals_on_basis(P2,P4,data:e:=100);
(-38429*5^2 + O(5^9) 449509 + O(5^9))
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) 306527 + O(5^9) -574266 + O(5^9) -919117 + O(5^9))
9
> coleman_integrals_on_basis(P1,P3,data:e:=100);
(O(5^9) O(5^9) O(5^9) 919669 + O(5^9) -746256 + O(5^9) 34467*5 + O(5^9))
9
> coleman_integrals_on_basis(P1,P4,data:e:=100);
(O(5^9) O(5^9) O(5^9) 497571 + O(5^9) 287133 + O(5^9) -517003 + O(5^9))
9
> coleman_integrals_on_basis(P1,P5,data:e:=100);
(O(5^9) O(5^9) O(5^9) 383416 + O(5^9) 747277 + O(5^9) -172334 + O(5^9))
9
> coleman_integrals_on_basis(P1,P6,data:e:=100);
(O(5^9) O(5^9) O(5^9) 38594 + O(5^9) -804083 + O(5^9) -114889 + 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 [5] 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);
(O(7^5) O(7^5) O(7^5) O(7^5) 6775 + O(7^5) -14701*7^-1 + O(7^5)
3239 + O(7^5) 41632*7^-1 + O(7^5))
5
> coleman_integrals_on_basis(P1,P3,data:e:=100);
(O(7^7) O(7^7) O(7^7) O(7^7) -329870 + O(7^7) 2808875*7^-1 + O(7^7)
-38631 + O(7^7) -76017*7^-1 + O(7^7))
7
```

4 A superelliptic curve

We now consider the curve $y^3 = x^5 - 2x^4 - 2x^3 - 2x^2 - 3x$. Using work of Poonen and Schaefer implemented by Creutz, Magma can show that the rank of the Jacobian of this curve is equal to 1:

```
> Qx<x>:=PolynomialRing(RationalField());
> RankBounds(x^5 - 2*x^4 - 2*x^3 - 2*x^2 - 3*x,3);
1 1
```

We take $p = 7$ and initial precision $N = 20$:

```
> load "coleman.m";
> Q:=y^3 - (x^5 - 2*x^4 - 2*x^3 - 2*x^2 - 3*x);
> p:=7;
> N:=20;
> data:=coleman_data(Q,p,N);
```

There are 5 obvious rational points on the curve:

```
> P1:=set_point(1,-2,data);
> P2:=set_point(0,0,data);
> P3:=set_point(-1,0,data);
> P4:=set_point(3,0,data);
> P5:=set_bad_point(0,[1,0,0],true,data);
```

We now compute some integrals:

```
IP1P2,N2:=coleman_integrals_on_basis(P1,P2,data:e:=50);
IP1P3,N3:=coleman_integrals_on_basis(P1,P3,data:e:=50);
IP1P4,N4:=coleman_integrals_on_basis(P1,P4,data:e:=50);
IP1P5,N5:=coleman_integrals_on_basis(P1,P5,data:e:=50);
```

The integrals from P_1 to P_2 do not (all) vanish:

```
> IP1P2;
(12586493*7 + O(7^10) 19221514*7 + O(7^10) -19207436*7 + O(7^10)
-10636635*7 + O(7^10) 128831118 + O(7^10) 67444962 + O(7^10)
-23020322 + O(7^10) 401602170*7^-1 + O(7^10))
> N2;
10
```

Since the rank of the curve is 1, the class of $P_1 - P_2$ generates a finite index subgroup of the Mordell Weil group of the Jacobian. We can find the annihilating differentials by setting the integrals from P_1 to P_2 to zero:

```
> K:=pAdicField(p,Minimum([N2,N3,N4,N5]));
> M:=Matrix(4,1,Vector(K,[IP1P2[i]: i in [1..4]]));
> v,_:= Kernel(M);
> v1:=v.1;
> v2:=v.2;
> v3:=v.3;
> v1;
(1 + O(7^9) O(7^9) O(7^9) -18106419 + O(7^9))
> v2;
(O(7^9) 1 + O(7^9) O(7^9) 12452015 + O(7^9))
> v3;
(O(7^9) O(7^9) 1 + O(7^9) 8834289 + O(7^9))
```

Note that `v1`,`v2`,`v3` are vectors with respect to our chosen basis $\omega_1, \ldots, \omega_g$ of the regular 1-forms. We can now check that the integral of the 1-form corresponding to `v1` vanishes between all of the points $P_1, \ldots, P_5$:

```
> DotProduct(v1,Vector(K,[IP1P3[i]: i in [1..4]]));
> DotProduct(v1,Vector(K,[IP1P4[i]: i in [1..4]]));
> DotProduct(v1,Vector(K,[IP1P5[i]: i in [1..4]]));
O(7^10)
O(7^10)
O(7^10)
```

and similarly for `v1`,`v2`.

We can also look for the rational points up to height 1000 and then compute the 1-forms that vanish on the differences of these points as well as their common zeros automatically:

```
> L,v:=effective_chabauty(data:bound:=1000,e:=50);
```

This way we find the annihilating differentials:

```
> v;
[
    [ 1 + O(7^10), O(7^10), O(7^10), 22247188 + O(7^10) ],
    [ O(7^10), 1 + O(7^10), O(7^10), -27901592 + O(7^10) ],
    [ O(7^10), O(7^10), 1 + O(7^10), -71872925 + O(7^10) ]
]
```

and a list of candidate points:

```
> L;
[
    rec<recformat<x, b, inf, xt, bt, index> |
        x := O(7^20),
        b := [ 1 + O(7^20), O(7^8), O(7^16) ],
        inf := true>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := O(7^20),
        b := [ 1 + O(7^20), O(7^9), O(7^18) ],
        inf := false>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := 3 + O(7^20),
        b := [ 1 + O(7^20), O(7^9), O(7^18) ],
        inf := false>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := -1 + O(7^20),
        b := [ 1 + O(7^20), O(7^9), O(7^18) ],
        inf := false>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := 1 + O(7^9),
        b := [ 1 + O(7^20), -2 + O(7^9), 4 + O(7^9) ],
        inf := false>
]
```

Since there are only 5 candidate points and we have already found 5 points $P_1, \ldots, P_5$ our list is complete!

5 Poonen-Schaefer-Stoll

In [2] Poonen, Schaefer and Stoll want to find the rational points on 10 plane quartics $C_1, \ldots, C_{10}$. They first determine the ranks of these curves by descent and then find the rational points by a combination of effective Chabauty and Mordell-Weil sieving. Our algorithms can do the effective Chabauty part automatically, which already allows one to find the rational points on $C_1, C_2, C_3, C_8, C_9, C_{10}$. For the other curves one needs some Mordell-Weil sieving to rule out candidate points which do not come from rational points. We take $p = 5$ and initial precision $N = 15$:

```
> load "coleman.m";
> Q:=6*x^3*y+y^3+x;
> p:=5;
> N:=15;
> data:=coleman_data(Q,p,N);
```

We can search for the rational points up to height 10^4 as follows:

```
> Qpoints:=Q_points(data,10^4);
> Qpoints;
[
    rec<recformat<x, b, inf, xt, bt, index> |
        x := 0,
        b := [ 1 + O(5^15), 0, 0 ],
        inf := false>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := -15258789062 + O(5^15),
        b := [ 1 + O(5^15), 15258789062 + O(5^15), -7629394531 + O(5^15) ],
        inf := false>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := 0,
        b := [ 1 + O(5^15), 0, 0 ],
        inf := true>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := 0,
        b := [ 1 + O(5^15), 0, -6 + O(5^15) ],
        inf := true>
]
```

This gives 2 finite points and 2 infinite ones. Now we compute the annihilating differentials and candidate points:

```
L,v:=effective_chabauty(data:Qpoints:=Qpoints,e:=25);
```

The annihilating differentials are

```
> v;
[
    [ 1 + O(5^5), O(5^5), -868 + O(5^5) ],
    [ O(5^5), 1 + O(5^5), 16 + O(5^5) ]
]
```

and the candidate points are

```
 > L;
[
    rec<recformat<x, b, inf, xt, bt, index> |
        x := O(5^4),
        b := [ 1 + O(5^15), O(5^15), O(5^15) ],
        inf := true>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := O(5^8),
        b := [ 1 + O(5^15), O(5^4), -6 + O(5^15) ],
        inf := true>,
    rec<recformat<x, b, inf, xt, bt, index> |
        x := O(5^9),
        b := [ 1 + O(5^15), O(5^3), O(5^6) ],
        inf := false>,
```

```
    rec<recformat<x, b, inf, xt, bt, index> |
        x := -312 + O(5^4),
        b := [ 1 + O(5^15), 1562 + O(5^5), -781 + O(5^5) ],
        inf := false>
]
```

Since there are only 4 candidate points and we have already found 4 points our list is complete! Details for the other curves can be found in `./examples/pss.m`.

6 Conclusion

The code is still very much work in progress. For example, double integrals and related functionality will be added in the near future. Please send 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] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2+y^3=z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158.

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

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

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