COMPUTING OBSTRUCTIONS TO THE HASSE PRINCIPLE FOR CURVES IN MAGMA – I: ELLIPTIC CURVES

WILLIAM B. HART AND SAMIR SIKSEK

Abstract. We compute obstructions to the Hasse principle for curves, using the example of elliptic curves. The computations are done using MAGMA.

1. The Algorithm

The method we will use to compute examples of obstructions to the Hasse Principle for curves is described in [1]. We will be working with coverings of elliptic curves which are genus 1 curves of the form

$$X : y^2 = f(x), \text{ with } f(x) \in \mathbb{Z}[x].$$

As a first example, we will work over $\mathbb{Q}_p$ (later we will want to work over the localization of a number field).

If we denote $X_p := X \times \mathbb{Q}_p$ then the first step of the method is to compute an $\mathbb{F}_p$ basis of $Pic(X_p)/nPic(X_p)$ for a certain n.

This is accomplished by finding such a basis on the elliptic curve E which is the Jacobian of X. Thus in particular, we compute explictly a parameterization

$$\rho : E(\mathbb{Q}_p) \to X(\mathbb{Q}_p).$$

Firstly we set up the curve X in MAGMA. We define it intially over the rationals and later find points on it over $\mathbb{Q}_p$.

```
p:=5;n:=3;
Qp:=pAdicField(p);
P<x,y,z>:=ProjectiveSpace(Rationals(),2);
PQp<y1>:=PolynomialRing(Qp);
X:=Curve(P,x^3*y^2+x^3*z^2-z^5);
```

In order to construct the parameterization ρ above we need to find a $\mathbb{Q}_p$ rational point **pt** on X_p. We do this by solving explicitly the equation defining X, over $\mathbb{Q}_p$.

```
i:=1;
repeat
ex,root:=HasRoot((Qp!i)^3*y1^2+(Qp!i)^3-1);
i:=i+1;
until ex eq true;
pt:=[Qp!i,root,Qp!1];
```

Now we are able to compute the elliptic curve E and a map **toE** (the inverse of ρ) which takes the point **pt** to the origin of E. We also ensure that E is defined over $\mathbb{Q}_p$.

```
E,toE:=EllipticCurve(X,pt);
EQp:=ChangeRing(E,Qp);
```

Next we compute the order of an $\mathbb{F}_p$ basis for $E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)$. This is given by the formula

$$\dim_{\mathbb{F}_p} E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) = \dim_{\mathbb{F}_p} E(Q_p)[n] + \delta,$$

where $E(Q_p)[n]$ is the Q_p rational n-torsion of E and where δ is 0 for $p \neq n$ and 1 if $p = n$.

```
G:=TorsionSubgroupScheme(E,n);
BasSize:=0;
while p^BasSize ne #G do
BasSize:=BasSize+1;
end while;
if n eq p then BasSize:=BasSize+1; end if;
```

The final step of the algorithm finds "random" Q_p-rational points on X_p, maps them to E via **toE** and checks whether they already lie in the $\mathbb{F}_p$ span of the points found so far. If not, then they are added to the basis until it has the required number of elements, as computed above.

To check whether a newly found point **PonE** is in the $\mathbb{F}_p$ span of the points in the basis so far $\{P_1, P_2, \ldots, P_r\}$, we construct the vector space V of dimension r over $\mathbb{F}_p$ and iterating through all the vectors $x = (x_1, x_2, \ldots, x_r) \in V$ we check that **PonE** is not in the same class of $E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)$ as $x_1P_1 + x_2P_2 + \cdots + x_rP_r$.

```
EqToE:=DefiningEquations(toE);
Bas:=[];VBas:=[pt];
while #Bas ne BasSize do
ex,root:=HasRoot((Qp!i)^3*y1^2+(Qp!i)^3-1);
if ex eq true then
point:=[Qp!i,root,Qp!1];
PonE:=[Evaluate(EqToE[1],point),Evaluate(EqToE[2],point),Evaluate(EqToE[3],point)];
bool,PonE:=IsPoint(EQp,PonE);
different:=true;
GFp:=GaloisField(p);
V:=VectorSpace(GFp,#Bas);
for x in V do
LinComb:=Id(EQp);
for j:=1 to #Bas do
LinComb=LinComb+ElementToSequence(x)[j]*Bas[j];
end for;
P2:= PonE-LinComb;
if IsDivisibleBy(P2,n) eq true then different:=false; end if;
end for;
if different eq true then Bas[#Bas+1]:=PonE; VBas[#Bas+1]:=point; end if;
end if;
i:=i+1;
end while;
```

At the end of this algorithm, **VBas** contains the point **pt** as its first element, followed by a complete F_p basis for $Pic(X_p)/nPic(X_p)$.

References

[1] Bright, Martin; Siksek, Samir *Functions, Reciprocity and the Obstruction to Divisors on Curves* Preprint (2006)

[2] Acciaro, Vincenzo and Klüners, Jürgen *Computing Local Artin Maps, and Solvability of Norm Equations* J. Symb. Comp. (2000) **11**, 1-14

E-mail address: w.b.hart@maths.warwick.ac.uk