Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Effective 2-descent using Theta Characteristics

Thibaut Misme (supervisor: Nicolas Mascot)

Computing rational points on algebraic curves

A classic problem addresses the question of finding the solutions in $\mathbb{Q}$ of **polynomial equations** such as

$$x^3y + y^3 + x = 0 \qquad \text{(Klein Quartic)}.$$

We now know that it is profitable to look at the problem in a geometrical settings. Construct the algebraic variety X from the same equation(s)

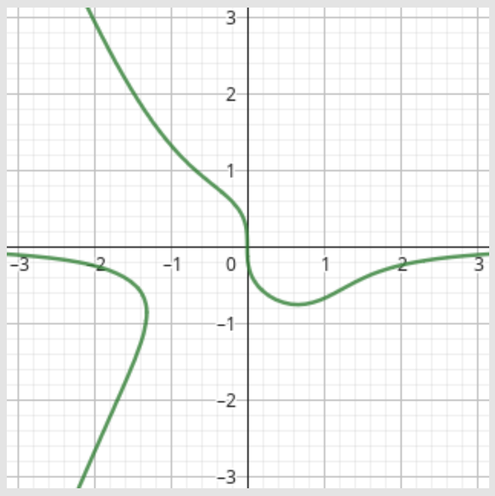

Figure 1. The real solutions of the Klein Quartic $X(\mathbb{R})$.

and try to compute its **rational points** $X(\mathbb{Q})$. In case of curves, when the dimension of the variety X is 1, some methods have been developed to do so.

What makes the study of rational points complicated is that it lacks structure: in general, it's just a set.

Historical example: Elliptic curves ($g = 1$)

Elliptic curves are the algebraic curves E of genus $g = 1$ with a rational point. Their main striking feature is that there exists a **group law** on their points. In that case, the Mordell-Weil theorem tells you that the rational points form a finitely generated group. In other words:

$$E(\mathbb{Q}) \simeq E_{tors} \times Z^r \qquad \text{(Mordell-Weil)}$$

where E_{tors} is a finite group and r is an integer called the **Mordell-Weil rank** of E. The proof can be made effective and r can be explicitly computed in most cases. This is the **descent** method.

What happens when $g \geq 2$?

The situation shifts as there is no group law nor structure on the rational points anymore. It is even showed by Faltings that

$$\text{if } g \geq 2,\ X(\mathbb{Q}) \text{ is finite} \qquad \textbf{(Faltings).}$$

Hopefully, you can embed your curve X in its **Jacobian** J which as in the case of elliptic curves is an **abelian variety** of dimension g with a group law on the points. The Mordell-Weil theorem is true as well:

$$J(\mathbb{Q}) \simeq J_{tors} \times \mathbb{Z}^r.$$

The knowledge of the precise structure i.e. of the **Mordell-Weil rank** r is valuable as it allows you to apply the **Chabauty-Coleman technique** (or some generalization):
if $\boxed{r < g}$ and $p > 2g$ is a prime of good reduction,

$$|X(\mathbb{Q})| \leq |X(\mathbb{F}_p)| + (2g - 2).$$

Once you have asked your computer to find *some* rational points on your curve, the Chabauty-Coleman technique is sometimes enough to certify that you computed them *all*. Again, the problem of finding r arises. If your curve X is of genus $g = 2$, then it is hyperelliptic and the **descent** method generalizes quite well.

2-descent: Computing the Mordell-Weil rank r

First notice that is enough to find the dim of the $\mathbb{F}_2$-vector space

$$J(\mathbb{Q})/2J(\mathbb{Q}) \simeq J[2](\mathbb{Q}) \times (\mathbb{Z}/2\mathbb{Z})^r$$

as the rational **2-torsion** $J[2](\mathbb{Q})$ can often be computed (see *Mascot* [2]).
From the short exact sequence of **Galois**-modules

$$0 \to J[2] \to J \xrightarrow{2} J \to 0 \quad (*)$$

one deduces the following one

$$0 \to 2J(\mathbb{Q}) \to J(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, J[2]).$$

It is therefore sufficient to bound the image of the map δ. In order to do so, you can cut out the infinite space $H^1(\mathbb{Q}, J[2])$ by local conditions from your curve X to obtain a **finite** group called the 2-**Selmer group**. Indeed, similarly than over $\mathbb{Q}$, for every prime p, one deduces from $(*)$ the following commutative diagram

$$\begin{array}{ccc} J(\mathbb{Q})/2J(\mathbb{Q}) & \xhookrightarrow{\delta} & H^1(\mathbb{Q}, J[2]) \\ \downarrow \mathrm{res}_p & & \downarrow \mathrm{res}_p \\ J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \hookrightarrow & H^1(\mathbb{Q}_p, J[2]). \end{array}$$

The Selmer group is defined to be

$$Sel^{(2)}(\mathbb{Q}) := \bigcap_p res_p^{-1}(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)).$$

You can verify that

$$J(\mathbb{Q})/2J(\mathbb{Q}) \hookrightarrow Sel^{(2)}(\mathbb{Q}) \subset H^1(\mathbb{Q}, J[2]).$$

In practise, thanks to the p-adic nature of the finite vector spaces $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ that makes them within computational reach, the Selmer group as well can often be explicitly computed.

How to generalize explicit descent to non-hyperelliptic curves ?

As soon as $g \geq 3$, unlike to the (hyper)elliptic case, the descent map $J(\mathbb{Q})/2J(\mathbb{Q}) \to H^1(\mathbb{Q}, J[2])$ and the space $H^1(\mathbb{Q}, J[2])$ itself are complicated to determine and to represent for general curves. *Bruin, Poonen and Stoll* offered in [1] to project $H^1(\mathbb{Q}, J[2])$ in a more computationally handy Galois cohomology group $H^1(\mathbb{Q}, \mu_2^{\Delta_{Odd}}/\mu_2)$ built upon the **Odd Theta Characteristics** Δ_{Odd} and to apply the same method to compute an equivalent *Fake Selmer group*

$$J(\mathbb{Q})/2J(\mathbb{Q}) \to Sel_{Fake} \subset H^1(\mathbb{Q}, \mu_2^{\Delta_{Odd}}/\mu_2).$$

On a plane quartic (non-hyperelliptic curve of genus $g = 3$), the Odd Theta Characteristics are in bijection with the **bitangents** of the curve. They took advantage of this geometrical interpretation to perform explicitly the 2-descent method in this fashion on "random" curves and even succeeded to recover the sets of rational points.

Theta Characteristics

Definitions:

* Let X be a curve and let K_0 be its canonical class. A (class of) *Theta Characteristic* is a class β of the Picard group Pic_X such that
$$2\beta = K_0.$$
* A Theta Characteristic β is said to be *odd* if the corresponding Riemann-Roch space $H^0(\beta)$ has odd dimension.

The difference of two Theta Characteristics $\beta_1 - \beta_2 \in J[2]$ is a 2-torsion point. This is the link that Bruin, Poonen and Stoll exploited to construct a map $H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, \mu_2^{\Delta_{Odd}}/\mu_2)$.
It also shows that Theta Characteristics form a finite set: $|\Delta_{TC}| = 2^{2g}$. Furthermore, $|\Delta_{Odd}| = 2^{g-1}(2^g - 1)$.

When $g \geq 4$,
the geometrical interpretation of the OTC is more complicated to leverage and makes them more complicated to represent and to determine. **I implemented an algorithm** (upcoming article) based on [2] designed to compute all the Theta Characteristics Δ_{TC} along with their classic invariants (parity, quadratic form, bitangents and etale algebra) allowing to ease explicit 2-descent in the Bruin-Poonen-Stoll framework in the case $g \geq 3$.

2-descent using all Theta Characteristics

This algorithm also allows us to take $\Delta = \Delta_{TC}$ and to obtain a similar projection $H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, \mu_2^{\Delta_{TC}}/\mu_2)$. This descent map has always a smaller kernel than the equivalent one using only Odd Theta Characteristics. This is beneficial as an **injective descent map** enables to skip some computation steps and ensures better chance of success for the 2-descent method.

References

Nils Bruin, Bjorn Poonen, and Michael Stoll.
Generalized explicit descent and its application to curves of genus 3.
In *Forum of Mathematics, Sigma*, volume 4, page e6. Cambridge University Press, 2016.

Nicolas Mascot.
Hensel-lifting torsion points on jacobians and galois representations.
Mathematics of Computation, 89(323):1417–1455, 2020.