Applications of the Mordell-Weil Sieve

Michael Stoll

In this talk, we consider the following situation.

- A is an abelian variety over $\mathbb{Q}$ (for simplicity, we could work over a number field instead);
- $X \subset A$ is a closed subvariety not containing any translates of subabelian varieties of A of positive dimension (this implies that $X(\mathbb{Q})$ is finite);
- We know (explicit generators of) the Mordell-Weil group $A(\mathbb{Q})$.

Of course, the last requirement is highly nontrivial in practice.

The typical situation is when X is a curve of genus $g \geq 2$ embedded into its Jacobian variety A. When $g = 2$, we can determine $A(\mathbb{Q})$ in many cases.

1. The Mordell-Weil Sieve

The idea of the Mordell-Weil Sieve is to combine our 'global' knowledge of $A(\mathbb{Q})$ with 'local' information on how X sits inside A, in order to obtain information on $X(\mathbb{Q})$. The simplest instance uses a finite set S of primes of good reduction for X and A and considers the following diagram.

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook] \arrow[d] & A(\mathbb{Q}) \arrow[d, "\beta"] \\
\prod\limits_{p \in S} X(\mathbb{F}_p) \arrow[r, hook, "\alpha"] & \prod\limits_{p \in S} A(\mathbb{F}_p)
\end{tikzcd}$$

If the images of the maps α and β above are disjoint, then $X(\mathbb{Q})$ must be empty.

Conversely, we can ask, if $X(\mathbb{Q})$ is empty, can we expect the images of α and β to be disjoint if S is sufficiently large?

Bjorn Poonen has come up with some heuristic considerations that indicate a positive answer. Roughly, the argument is as follows. Let $B > 0$ be a parameter (which we will choose large later) and let S_B be the set of good primes $p \leq B^2$ such that $\#A(\mathbb{F}_p)$ is B-smooth. We expect $\#S_B \geq \delta\pi(B^2)$ when B is large, for some $\delta > 0$. Then one can work out that

$$\#\prod_{p \in S_B} A(\mathbb{F}_p) \approx e^{\delta B^2 \dim A}\,, \quad \#\prod_{p \in S_B} X(\mathbb{F}_p) \approx e^{\delta B^2 \dim V}\,, \quad \#\operatorname{im}(\beta) \approx e^{2rB \dim A}\,,$$

where r is the rank of $A(\mathbb{Q})$. The expected size of $\operatorname{im}(\alpha) \cap \operatorname{im}(\beta)$ is about $e^{2rB \dim A - \delta B^2 \operatorname{codim}_A X}$, which tends to zero very quickly as $B \to \infty$. For details, see [3].

So we have as a **first application** that we can prove $X(\mathbb{Q}) = \emptyset$ for curves X of higher genus (say). The Mordell-Weil sieve was first developed in this context by Scharaschkin [5], who applied it to some twists of the Fermat quartic. It was improved by Flynn [2], who applied it to a number of genus 2 curves, and further improved by Bruin and Stoll [1] in the context of a project which (successfully) aimed at deciding for every genus 2 curve given by an equation

$$y^2 = f_6 x^6 + \cdots + f_1 x + f_0$$

with integral coefficents $|f_j| \leq 3$ whether it has rational points or not.

2. Improvements and Refinements

In practice, instead of the maps in the diagram above, we compute the maps in the following diagram, with a suitable choice of N.

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook] \arrow[d] & A(\mathbb{Q})/NA(\mathbb{Q}) \arrow[d, "\beta_N"] \\
\prod\limits_{p \in S} X(\mathbb{F}_p) \arrow[r, hook, "\alpha_N"] & \prod\limits_{p \in S} A(\mathbb{F}_p)/NA(\mathbb{F}_p)
\end{tikzcd}$$

We work our way up to this N, by starting with $N_0 = 1$ and multiplying by a prime factor at a time, keeping track of $\beta_N^{-1}(\mathrm{im}(\alpha_N))$ at each stage.

We can use more information than just what we get modulo p for good primes. Instead of looking at the image $X(\mathbb{F}_p)$ of $X(\mathbb{Q}_p)$ in the quotient $A(\mathbb{F}_p)$ of $A(\mathbb{Q}_p)$, we can consider any finite quotient of $A(\mathbb{Q}_p)$ and the image of $X(\mathbb{Q}_p)$ in it. This allows us to use information at bad primes (e.g., we can use the component group), and also information modulo higher powers of p.

In this way, we can restrict our attention to potential rational points on X lying in certain residue classes (even modulo bad primes). We can then use the Mordell-Weil sieve to prove that such points do not exist, even when X does have rational points.

This **second application** proved to be very useful in completing the proof that there are no unknown primitive solutions to $x^2 + y^3 = z^7$, see [4]. There, we had to rule out the existence of rational points satisfying certain congruences mod 2 and 3 on a plane quartic that has rational points and whose Jacobian has Mordell-Weil rank 3.

In a similar way, we can rule out the existence of rational points on X that are in a specified coset of $nA(\mathbb{Q})$ in $A(\mathbb{Q})$, by taking N above to be a multiple of n and restricting to the relevant cosets. This provides a **third application**: if we know a number n such that no two rational points on X are in the same coset mod $nA(\mathbb{Q})$, then we can hope to determine $X(\mathbb{Q})$ — for each coset, we can find a point if one exists and rule out the existence of points if there is no point.

In particular, when X is a curve of genus g and the Mordell-Weil rank of its Jacobian A is less than g, then such an n can be found by Chabauty's approach: if, for every $P \in X(\mathbb{F}_p)$, there is a differential $\omega \in \Omega_X(\mathbb{Q}_p)$ that kills the Mordell-Weil group such that its reduction $\bar{\omega}$ modulo p does not vanish at P, then we can take $n = \#A(\mathbb{F}_p)$. This works very well in practice when $g = 2$ and the rank is 1.

3. Information on Rational Points

When X has rational points and we do not know a number n that 'separates' the points as in the third application above, we still can use the Mordell-Weil sieve in order to obtain information on potential unknown rational points on X. Namely, if all the elements we find in $\beta_N^{-1}(\mathrm{im}(\alpha_N))$ come from known rational points on X, then we can deduce that for every potential unknown point $P \in X(\mathbb{Q})$, there must be a known $Q \in X(\mathbb{Q})$ such that $P - Q$ is divisible by N in $A(\mathbb{Q})$. This in turn can be translated into a lower bound on the height of any unknown rational point on X, which can be made more or less arbitrarily large.

Combining this with upper bounds obtained using Baker's method, we have as a **fourth application** a way of determining the set of all integral points on a hyperelliptic curve (say), even when its rank is too large to use methods that determine the set of rational points. This is an ongoing project with Bugeaud, Mignotte, Siksek, and Tengely.

References

[1] N. Bruin, M. Stoll, *Deciding existence of rational points on curves: an experiment*, to appear in Experiment. Math.

[2] E.V. Flynn, *The Hasse Principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), 437–466.

[3] B. Poonen, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), 415–420.

[4] B. Poonen, E.F. Schaefer, M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), 103–158.

[5] V. Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, Ph.D. thesis, University of Michigan (1999).