The de Rham cohomology of p-group covers
DESCRIPTION FOR THE GENERAL PUBLIC

Jędrzej Garnek

My research focuses on *algebraic curves* (one-dimensional sets defined by polynomial equations) and their symmetries. The coefficients of polynomials defining the curve might be complex, real or rational numbers, but also they might belong to $\mathbb{F}_p$ for a prime number p. Recall that $\mathbb{F}_p$ is the set of remainders for division by p with the operations of addition modulo p and multiplication modulo p. Curves defined over $\mathbb{F}_p$ are especially important in cryptography. Those with many symmetries can either be highly sought after or intentionally avoided, depending on the application.

The following three concepts are essential to understand obtained results: *group*, *representation* and *cohomology*. The concept of a *group* or a *group action* provides a formal framework for analyzing the symmetries of an object. Specifying the set of symmetries of a curve X (i.e. a group action on X) is equivalent to giving a "nice" map (called a *branched cover*) from X to another curve Y. In a cover there is the same number of points of X over almost every point of Y. The remaining points are called *branch points* (see Figure 1 for an example). Another key concept is a *representation*. A representation encodes elements of a given group (the "symmetries") as matrices. Even though representations to real or complex matrices are well-understood, the representations to matrices over $\mathbb{F}_p$ are considered to be impossible to classify in most situations. *Cohomology* is a classic invariant of manifolds in topology and algebraic varieties in algebraic geometry. In topology this concept allows to count the "numbers of holes" of a given manifold. Even though this intuition is no longer valid over $\mathbb{F}_p$, there is still a way of defining the cohomology of an algebraic curve modulo p. Since any symmetry acting on curve yields a matrix acting on the cohomology of a curve, this leads to a representation of the considered group.

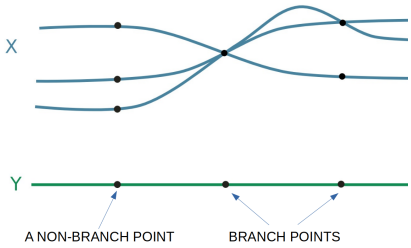

Figure 1: A cover of curves.

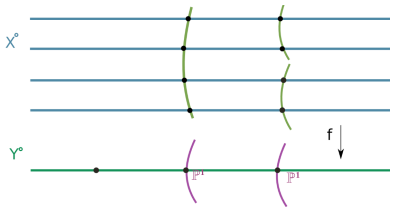

Figure 2: Cover from Figure 1 can be approximated by Harbater–Katz–Gabber covers (vertical curves) and a trivial cover

The first two obtained results concern cohomologies of curves over $\mathbb{F}_p$. My main result shows that for most curves the representation coming from cohomology decomposes as a global part (which depends only on the shape of the cover) and a sum of local parts. The local parts can be described in terms of *Harbater–Katz–Gabber covers*, i.e. covers of the line branched only over one point that approximate the considered cover (see Figure 2). The mentioned result has several significant applications. For instance, given a group one may ask what are the possible cohomologies of curves with an action of this group. The question seems hard, but I have proven (using the above results) that almost always there are infinitely many "building bricks" for those cohomologies. This suggests that the world of the representations coming from algebraic curves is as vast as the world of all representations over $\mathbb{F}_p$.

In order to explain the final result, recall that every curve embeds into a *Jacobian*, i.e. a variety whose points can be added in an algebraic way. Every Jacobian yields a representation of the absolute Galois group, i.e. one of the central objects in number theory. These representations play a central role, for example, in the proof of Fermat's Last Theorem and in the Langlands program (a set of far-reaching conjectures about connections between number theory and geometry). The image of the representation associated to a Jacobian should be controlled by the shape of the curve, as predicted by the *Mumford–Tate conjecture*. This conjecture may also be seen as a bridge between two other major open problems of algebraic geometry – Tate conjecture and Hodge conjecture, one of seven millennium problems. In the project I studied the curves of the form $y^\ell = f(x)$, where ℓ is a prime number and $f(x)$ is a polynomial with rational coefficients. I managed to show that Mumford–Tate, Hodge and Tate conjectures usually hold for such curves.