Reg. No: 2024/55/D/ST1/01377; Principal Investigator: dr Jędrzej Garnek

Symmetries of curves in positive characteristic

DESCRIPTION FOR THE GENERAL PUBLIC

Jędrzej Garnek

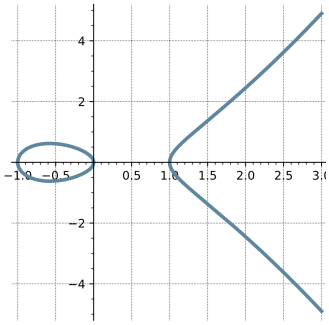

Figure 1: The curve $y^2 = x^3 - x$ over the real numbers.

This project concerns *algebraic curves* (one-dimensional sets defined by polynomial equations) and their symmetries. The coefficients of polynomials defining the curve might be e.g. real numbers (cf. Figure 1), complex 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. Given an integer it can be *reduced* to an element of $\mathbb{F}_p$ (by taking its remainder of division by p) – for instance 102 reduces to $2 \in \mathbb{F}_5$. Conversely, an element of $\mathbb{F}_p$ can be *lifted* to an integer. This however can be done in many ways – for instance $2 \in \mathbb{F}_5$ lifts e.g. to integers $2, 7, 12, 17, \ldots$.

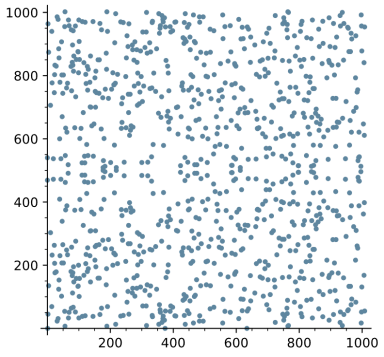

Figure 2: The curve $y^2 = x^3 - x$ over $\mathbb{F}_{1009}$.

Curves defined over $\mathbb{F}_p$ are more of a "discrete", finite object (cf. Figure 2). This makes them especially important in cryptography. Those with many symmetries can either be highly sought after or intentionally avoided, depending on the application. Similarly as above, a curve with integer coefficients can be reduced to a curve over $\mathbb{F}_p$ and a curve over $\mathbb{F}_p$ can be lifted to a curve with integer coefficients. The key question is when can be a curve over $\mathbb{F}_p$ lifted with symmetries. For instance, the curve in Figure 2 has a natural symmetry, coming from the fact that if (x, y) belongs to the curve then $(x, -y)$ is on curve as well. This can be seen as the horizontal symmetry of the corresponding picture. The curve in question lifts to the curve from Figure 1 with the considered symmetry. A celebrated conjecture of Oort states that every symmetry of a curve can be lifted in such a way. Oort's conjecture was proven in 2014 by Wewers, Obus and Pop, but there still remain many open questions. For instance, it is not clear to which set can the curve with the automorphism be lifted. Another problems are related to lifting sets of symmetries (i.e. groups) rather than a single symmetry.

In the first part of the project I want to investigate representations associated to curves. 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. In the project I want to prove a decomposition of the representation associated to a curves into simpler representations. Also, we would like to describe the "building bricks" of those representations. This might lead to showing whether classifying representations coming from curves is a solvable problem in general.

In the second part of the project, I want to study various lifting problems. A recent result shows a connection between lifting symmetries of a curve and lifting its representation. I plan to employ this new tool, as well as classical methods, to three problems in this area. Firstly, I would like to determine whether there exist symmetries of curves that can be lifted from $\mathbb{F}_p$ to $\mathbb{Z}/p^n$ (set of remainders for division by p^n), but not to $\mathbb{Z}/p^{n+1}$ for some $n > 1$. The second problem asks in which situation one can lift a set of symmetries that fix a point on the curve. I want to focus on the case, when the set of symmetries has p^3 elements. This could have also potentially some applications to *moduli spaces*, i.e. spaces that classify the curves with some symmetries. Finally, I plan to use the connection between lifting curves and representations to tackle the strong Oort conjecture, which gives a more specific set to which the symmetry lifts.