Point-counting and applications

Jonathan Pila

Project Descriptions
Arizona Winter School, 2023

Project 1

Synopsis. To consider some variants and special cases of the result on unlikely intersections of an asymmetric curve in $Y(1)^n$ (theorem of Habegger-Pila). This will mainly involve getting good/explicit height bounds for the unlikely intersections in suitable settings.

1. Introduction. Effectivity is often very difficult to achieve in diophantine problems even when finiteness is known. The classical example is the proof by Faltings of the Mordell Conjecture: quantitative but not effective. The André-Oort conjecture is also ineffective outside of some very special cases ([6, 7, 9, 30]), and “unlikely intersection” problems are in general ineffective (though see [25]).

In point-counting approaches, one opposes an upper bound from point-counting to a lower bound coming from arithmetic, generally some lower bound for the size of a Galois orbit. Often both bounds are ineffective. Lower bounds for Galois orbits of special points in the André-Oort conjecture are ineffective due to the famously ineffective class number bounds of Landau-Siegel. These bounds are obtained by considering separately the cases where a Riemann Hypothesis is true or false. So the bound one gets depends on some putative failure of RH. Counting results are hard to make effective in general though they do not depend on that kind of argument, and various quite general effective results are known [8, 10].

This project concerns the “unlikely intersection problems” for a curve in $X = Y(1)^3 = C^3$. Recall that a special subvariety of $Y(1)^3$ is an irreducible component of an algebraic subvariety defined by some number of equations of the form $x_i = c$, where $c$ is “special” (i.e. a singular modulus, that is, the $j$-invariant of an elliptic curve with complex multiplication), or $\Phi_N(x_j, x_k) = 0$ where $\Phi_N$ is a classical modular polynomial. (References [54, 41]).

1.1. Conjecture. (Special case of ZP) Let $V \subset X = Y(1)^3$ be a curve that is not contained in any proper special subvariety of $X$. Then the intersection of $V$ with the union $X^{[2]}$ of all special subvarieties of codimension $\geq 2$ is a finite set.

A number of partial results are known [26], [40], [20]. In general the required counting results in the counting approach are not effective, but the Galois lower bounds can be made effective in the known cases. In [26] these use isogeny estimates to get Galois lower bounds from height upper bounds.

The points $(x_1, x_2, x_3) \in V \cap X^{[2]}$ fall into a few different types, the “generic” one being that the coordinates $x_1, x_2, x_3$ are non-special with the corresponding elliptic curves being pairwise isogenous. Let’s call these “totally isogenous points”.
The project is to make the height upper bounds for totally isogenous points in [26] fully effective, at least in some special cases. Such as for curves \( X_{a,b,c} = \{(t^a, t^b, t^c) : t \in \mathbb{C}\} \) as \((a, b, c) = (1, 2, 3), \ldots\). Assuming some reasonable form for effective point-counting upper bounds one can consider how the bounds depend on \(a, b, c\).

It may be possible to get a fully effective solution to some very special cases for totally real totally isogenous points on some real arcs; see [1], and [8].

Project 2.

Synopsis. To consider generalisations/variants of some results of Jones-Thomas-Wilkie, Wilkie, Jones-Qiu on “integer-valued definable functions”. For entire (instead of definable) functions this is a classic topic going back to Pólya (1915) and many variants have been studied. It involves an interplay of complex analysis in \(\mathbb{R}\)-minimal structures with arithmetic properties.

1. Introduction. A classical theorem of Pólya asserts that the function \(2^x\) is the “smallest” entire transcendental function that takes integer values at all non-negative integer arguments.

1.1. Theorem. (Pólya [49]) Let \(f(z)\) be an entire function with \(f(\mathbb{N}) \subset \mathbb{Z}\). If

\[
\limsup_{r \to \infty} \frac{M(f, r)}{2^r} < 1
\]

then \(f(z)\) is a polynomial.

Here \(M(f, r)\) denotes the maximum modulus of \(f(z)\) at radius \(r\). The theorem is sharp in the sense that \(2^x\) has the stated growth rate. This theorem has been sharpened, strengthened, and generalised in many directions, in work of (just mentioning some early work) Hardy, Gelfond, Selberg; see [11] and the recent survey [50]. It was also influential in transcendental number theory.

A version for “definable” functions is due to Jones–Thomas–Wilkie [28], sharpened by Wilkie [51].

1.2. Theorem. ([28]) Let \(f : [0, \infty)^k\) be a definable analytic function with \(f(\mathbb{N}^k) \subset \mathbb{Z}\). Then either \(\sum_{|\pi| \leq r} |f(\pi)|\) grows faster than \(\exp(r^\delta)\), for some \(\delta > 0\), or \(f\) is a polynomial.

Here the growth exponent is not sharp, but Wilkie [52]) later gave a sharp version. To frame this result, let \(\mathcal{F}\) denote the collection of germs at \(+\infty\) of univariate function \(\mathbb{R}_{\text{an exp-definable}}\) functions.

1.3. Theorem. Let \(f \in \mathcal{F}\) and assume that \(f(n) \in \mathbb{Z}\) for all sufficiently large \(n\). Suppose that \(r\) is a real number satisfying \(0 < r < 1\) and that \(|f(x)| \leq 2^{rx}\) for all sufficiently large \(x\). Then there exists a polynomial \(P\) such that \(f(x) = P(x)\) for all sufficiently large \(x\).

The project seeks to give analogues for definable functions of some of the many variants/extension of Pólya’s theorem. Where possible, the aim is to get sharp versions in terms of the exponent, or versions as sharp as their “non-definable” counterparts (sometimes the sharp value of the growth exponent is not known).
In particular for the variants considered in [4, 27, 35, 42, 37, 38] or other variants surveyed e.g. in [50]. A more ambitious goal would be progress towards the following conjecture.

**Conjecture.** (Wilkie [52]) Let \( f : \mathbb{R} \to \mathbb{R} \) be \( \mathbb{R}_{\text{an}} \exp \)-definable and suppose that \( f(n) \in \mathbb{Z} \) for all sufficiently large positive integers \( n \). Assume further that for some \( r > 0 \), we have that \( |f(x)| \leq \exp(rx) \) for all sufficiently large \( x \in \mathbb{R} \). Then there exist polynomials \( P(x, y_1, \ldots, y_m) \) with rational coefficients, and positive real algebraic integers \( a_1, \ldots, a_m \) such that \( f(x) = P(x, a_1^x, \ldots, a_m^x) \) for all sufficiently large \( x \).

**References**

The references for the lecture notes are also included here.

48. R. Pink, A common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang, manuscript dated 17 April 2005 available from the author’s webpage.
52. A. J. Wilkie, Complex continuations of $\mathbb{R}_{an\ exp}$-definable unary functions with a diophantine application, *J. LMS* 93 (2016), 547–566.