Hindes, Wade

The arithmetic of curves defined by iteration. (English) Zbl 1330.14032

Acta Arith. 169, No. 1, 1-27 (2015).

Given an irreducible quadratic polynomial $f(x) = f_c(x) = x^2 + c \in \mathbb{Q}[x]$ whose n-th iterate f^n has distinct roots, let $\mathbb{T}_n$ be $\{0\} \coprod f^{-1}(0) \coprod \cdots \coprod f^{-n}(0)$. This becomes a 2-ary rooted tree when we draw an edge between α and β whenever $f(\alpha) = \beta$. The Galois group G_n of f^n acts on $\mathbb{T}_n$, and we can ask for which c finiteness of $[\mathrm{Aut}(\mathbb{T}_n) : G_n]$ holds (and in the limit $n = \infty$). This is a dynamical analog of Serre's open image conjecture.

This paper focuses on two aspects of this problem. First, in Theorem 1.1, he studies c's for which $n = 4$ is the first non-maximality, i.e. $G_3 = \mathrm{Aut}(\mathbb{T}_3)$ but $G_4 \neq \mathrm{Aut}(\mathbb{T}_4)$. In particular, no such c exists for $c \in \mathbb{Z}$, and only such $c \in \mathbb{Q}$ is $\frac{2}{3}$ and $-\frac{6}{7}$ as long as a certain curve has no rational points above a certain height. Secondly, the author shows in Theorem 1.2 that the Hall–Lang conjecture implies finiteness of $[\mathrm{Aut}(\mathbb{T}_\infty) : G_\infty]$ for integers c which are not negatives of squares, and shows that this index is 2 when $c = 3$.

To prove these results, the author considers curves $C_{c,n} : y^2 = f_c^n(x)$ and $B_{c,n} : y^2 = (x-c)f_c^n(x)$, as well as their twists. By using *M. Stoll*'s criterion [Arch. Math. 59, No. 3, 239–244 (1992; Zbl 0758.11045)], the author relates the non-maximality to rational points on certain curves. More specifically, for Theorem 1.2, he constructs rational points on twists of $C_{c,n}$ and $B_{c,1}$. For Theorem 1.1, he shows that $\sqrt{f_c^4(0)}$ must be fixed by one of the 7 distinct index-2 subgroups of G_3 if $n = 4$ is the first non-maximality, resulting in a rational point on the corresponding hyperelliptic curves. Then standard techniques such as Chabauty and Runge's method are used to find rational points.

In addition to these results, the author provides a detailed analysis of $B_{-2,n}$ and their Jacobians. In this Chebyshev case, he constructs characteristic polynomial of Frobenius for primes $\equiv \pm 3 \pmod 8$ and determines $B_{-2,n}(\mathbb{Q})$. This leads to the decomposition of $J(C_{c,n})$ into simple factors when $f_c \equiv x^2 - 2$ modulo such primes.

Reviewer: Yu Yasufuku (Tokyo)

MSC:

14G05	Rational points
37P05	Arithmetic and non-Archimedean dynamical systems involving polynomial and rational maps
12F10	Separable extensions, Galois theory
37P15	Dynamical systems over global ground fields
11G30	Curves of arbitrary genus or genus $\neq 1$ over global fields
11G05	Elliptic curves over global fields
14H45	Special algebraic curves and curves of low genus
20E08	Groups acting on trees
37P55	Arithmetic dynamics on general algebraic varieties
14H25	Arithmetic ground fields for curves

Keywords:

quadratic polynomial; dynamical arboreal representation; Hall-Lang conjecture; rational points on curves

Software:

Magma; SageMath

Full Text: DOI arXiv

References:

1 W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system 1: The user language, J. Symbolic Comput. 24 (1997), 235–265 (also see Magma homepage at http://magma.maths.usyd.edu.au/magma/handbook/text/1398). · Zbl 0898.68039

2 N. Boston and R. Jones, The image of an arboreal Galois representation, Pure Appl. Math. Quart. 5 (2009), 213–225. · Zbl 1167.11011

3 N. Bruin and M. Stoll, The Mordell–Weil sieve: proving non-existence of rational points on curves, LMS J. Comput. Math. 13 (2010), 272–306. · Zbl 1278.11069

4 A. Carocca, H. Lange, and R. Rodriguez, Jacobians with complex multiplication, Trans. Amer. Math. Soc. 363 (2011), 6159–6175. · Zbl 1285.11089

5 H. Cohen, Number Theory. Vol. 1: Tools and Diophantine Equations, Grad. Texts in Math. 239, Springer, 2007.

6 H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.), Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall/CRC, 2006. Arithmetic of curves defined by iteration27

7 D. Dummit and R. Foote, Abstract Algebra, 3rd ed., Wiley, 2004.

8 N. Elkies, List of integers x, y with x < 1018and 0 < |x3- y2| < x1/2, http://www .math.harvard.edu/\tilde{}elkies/hall.html.

9 J. Gebel, A. Peth˝o, and H. Zimmer, Computing integral points on Mordell's elliptic curves, Collect. Math. 48 (1997), 115–136. · Zbl 0865.11084

10 C. Gratton, K. Nguyen, and T. Tucker, ABC implies primitive prime divisors in arithmetic dynamics, Bull. London Math. Soc. 45 (2013), 1194–1208. · Zbl 1291.37121

11 W. Hindes, Points on elliptic curves parametrizing dynamical Galois groups, Acta Arith. 159 (2013), 149–167. · Zbl 1296.14017

12 N. Hurt, Many Rational Points: Coding Theory and Algebraic Geometry, Math. Appl. 564, Kluwer, 2003. · Zbl 1072.11042

13 B. Hutz and P. Ingram, On Poonen's conjecture concerning rational preperiodic points of quadratic maps. Rocky Mountain J. Math. 43 (2013), 193–204. · Zbl 1316.37042

14 R. Jones, Galois representations from pre-image trees: an arboreal survey, in: Publ. Math. Besan\c{}con Alg'ebre Th\'{}eor. Nombres, Presses Univ. Franche-Comt\'{}e, 2013, 107–136.

15 R. Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, J. London Math. Soc. 78 (2008), 523–544. · Zbl 1193.37144

16 N. Katz, Galois properties of torsion points on abelian varieties, Invent. Math. 62 (1981), 481–502. · Zbl 0471.14023

17 S. Lang, Abelian Varieties, Springer, 1983.

18 W. McCallum and B. Poonen, The Method of Chabauty and Coleman, in: Explicit Methods in Number Theory, Panor. Synth'eses 36, Soc. Math. France, 2012, 99–117; also available at http://www-math.mit.edu/\tilde{}poonen/papers/chabauty.pdf. · Zbl 1377.11077

19 J. Paulhus, Decomposing Jacobians of curves with extra automorphisms, Acta Arith. 132 (2008), 231–244. · Zbl 1142.14017

20 B. Poonen, The classification of rational preperiodic points of quadratic polynomials over Q: a refined conjecture, Math. Z. 228 (1998), 11–29. · Zbl 0902.11025

21 J. Silverman, The Arithmetic of Dynamical Systems, Grad. Texts in Math. 241, Springer, 2007.

22 J. Silverman, Arithmetic of Elliptic Curves, Grad. Texts in Math. 106, Springer, 1986; 2nd ed., 2009.

23 W. Stein, Sage: Open Source Mathematical Software (Version 2.10.2), The Sage Group, 2008, http://www.sagemath.org.

24 M. Stoll, Galois groups over Q of some iterated polynomials, Arch. Math. (Basel) 59 (1992), 239–244. · Zbl 0758.11045

25 M. Stoll, Rational points on curves, J. Th\'{}eor. Nombres Bordeaux 23 (2011), 257–277.

26 J. Wetherell, Bounding the number of points on certain curves of high rank, Ph.D. thesis, Univ. of California at Berkeley, 1997.

27 Yu. G. Zarhin, Hyperelliptic Jacobians without complex multiplication, Math. Res. Lett. 7 (2000), 123–132. · Zbl 0959.14013