Arboreal Galois Representations Over Finite Fields

Jasmine Camero [1], **Malike Conteh** [2], **Michaela Fitzgerald** [3], **Sarah Szafranski** [4], and Bianca Thompson [5]

[1]Emory Univeristy, [2]Pomona College, [3]Stonehill College, [4]University of Redlands, [5]Westminster College

Introduction

The study of arboreal Galois representations can be traced back to the work of Odoni in the 1980s [3, 4, 5]. He established the relationship between prime divisor densities of sequences and understanding the Galois groups attached to these trees constructed from the backwards orbit of a point. For our purposes, $f(x) = x^2 + 1$ over $\mathbb{F}_p$ for p an odd prime. The principle goal for this project was to better understand arboreal Galois trees over finite fields and their construction. Specifically, we would like to understand when the field extensions should occur in a given tree. We also get heuristic evidence towards a conjecture by Jones and Boston in [2] about how often f should be stable over $\mathbb{F}_p$.

Arboreal Galois Tree

- One thing we can study in dynamics is the **backwards orbit** of a point α : that is the pre-images of α via the function f. Equivalently, we are looking for the roots of the iterated function $f^n(x) - \alpha$.
- Backwards orbits are linked to the study of **arboreal Galois representations** of the tree. This is defined to be the action of the absolute Galois group, G_K, of a global field on trees of iterated pre-images under rational functions.
- Another property we can study here is the stability of f. We say f is stable if f^n, the nth iterate of f, is always irreducible over a field K.

Tools

- **Capelli's Lemma [2]**: For a field K and $f, g \in K[x]$, let $\beta \in \bar{K}$ where $g(\beta) = 0$. Then $g(f(x))$ is irreducible if and only if both g is irreducible over K and $f(x) - \beta$ is irreducible over $K(\beta)$.
- **Theorem by Jones-Boston [2]**: f a polynomial of degree 2 is stable if and only if $f^n(c)$ is never a square in the adjusted critical orbit over $\mathbb{F}_p$, p odd.
- a is a **quadratic residue** if $x^2 \equiv a \pmod{p}$ has solutions.
  - Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a QR of } p \\ -1 \text{ if } a \text{ is a non-QR of } p \end{cases}$$

- Critical orbit of f is

$$0 \longmapsto 1 \longmapsto 2 \longmapsto 5 \longmapsto 26 \longmapsto \cdots$$

Motivating Questions

1. Is the index $[\mathrm{Aut}(T) : G_K]$ finite?
2. As we travel along the backwards orbit in the tree, we see that sometimes we go to an extension field. We can ask as we travel from L_n to L_{n+1} of the tree, when is this extension trivial?
3. Which primes are not stable for f?

Tree Diagram

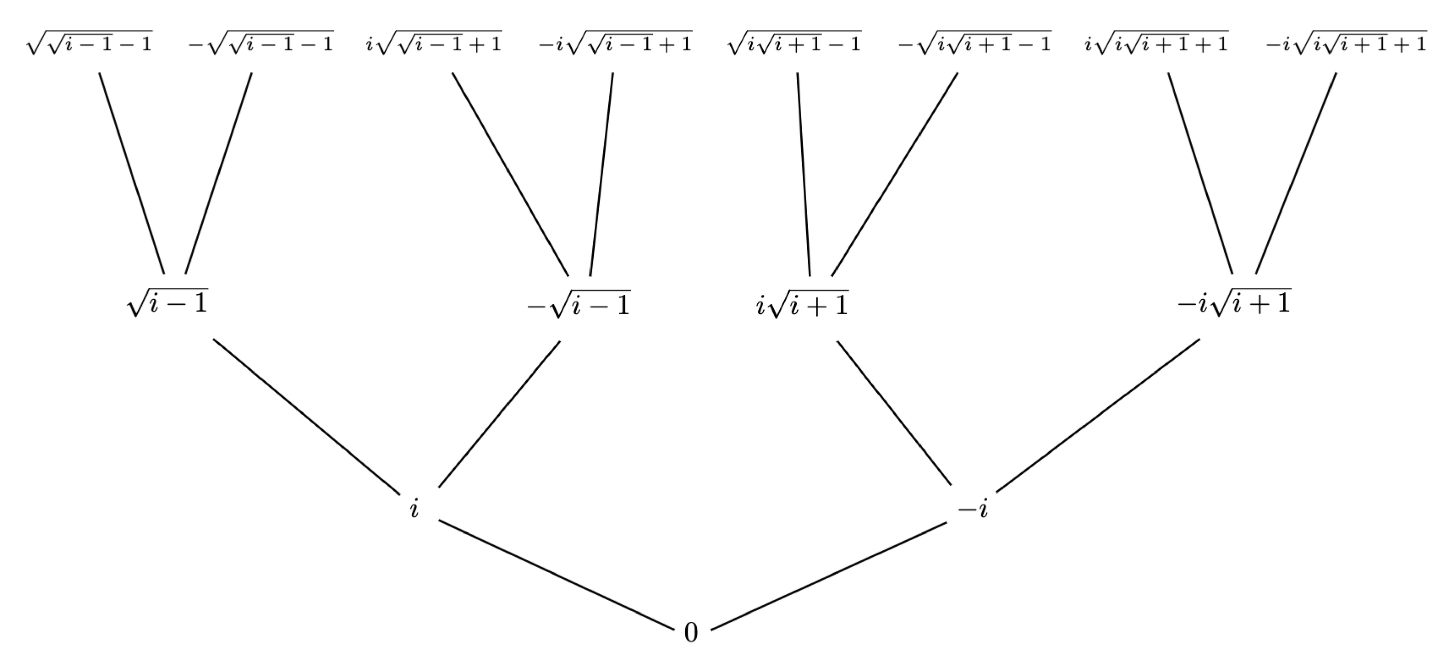

Figure: This diagram shows the first few steps of the backwards orbit produced by $f(x) = x^2 + 1$ with a pullback point of 0.

Results

- If $p \equiv 3 \pmod{4}$, then 0 will be a good pullback point for $x^2 + 1$.
- When 0 is a good pullback point we get the following properties:
  - The extension at L_1 is $\mathbb{F}_{p^2}$.
  - If $p \equiv 7 \pmod{8}$ then L_2 will have the extension $\mathbb{F}_{p^2}$.
  - If $p \equiv 3 \pmod{8}$ then L_2 will have the extension $\mathbb{F}_{p^4}$.
- The first iterate that is reducible corresponds to when the first trivial extension occurs, but after that, every iterate is reducible.
- QRs show when this first trivial extensions occur
  - $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod{4}$
  - $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \pmod{8}$
  - $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if $p \equiv \pm 1 \pmod{5}$
  - $\left(\frac{26}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{13}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{13}\right)$
  - $\left(\frac{677}{p}\right) = \left(\frac{p}{677}\right)$

Data

Primes/Level	0	1	2	3	4	5	6	7	8	9	10
3	1	2	4	8	16	32	64	128	256	512	1024
7	1	2	2	4	4	8	16	32	64	128	256
11	1	2	4	4	8	16	16	16	32	64	128
19	1	2	4	4	4	8	8	16	32	64	128
23	1	2	2	4	4	8	16	16	32	32	64
31	1	2	2	4	8	16	16	16	32	64	128
43	1	2	4	8	16	32	32	64	128	256	512
47	1	2	2	4	8	8	8	16	32	64	128

Table: The extension fields of $f(x) = x^2 + 1$ and pullback point $\alpha = 0$ over different primes.

Heuristics

We can begin ruling out primes that we know $x^2 + 1$ is not stable for by looking at the adjusted critical orbit.

$$0 \longrightarrow -1 \longrightarrow 2 \longrightarrow 5 \longrightarrow 26 \longrightarrow 677 \longrightarrow \cdots$$

	-1	**2**	**5**	**26**	**677**
Quantity Ruled Out	4783	2399	1205	602	321
Cumulative Number	4783	7182	8387	8989	9310
Cumulative Percentage	49.86%	74.87%	87.44%	93.71%	97.06%

Table: The number of primes identified as nonstable in $f = x^2 + 1$.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No DMS-2113782. We would also like to thank Pomona Research in Mathematics Experience (PRiME) for this opportunity.

References

[1] R. Jones. An iterative construction of irreducible polynomials reducible modulo every prime, 2012.

[2] R. Jones and N. Boston. Settled polynomials over finite fields. *Proceedings of the American Mathematical Society*, 140, 06 2012.

[3] R. Odoni. The galois theory of iterates and composites of polynomials. *Proceeding of London Math Society*, 51(3): 385-414, 1985.

[4] R. Odoni. On the prime divisors of the sequence $\omega_{n+1} = 1 + \omega_1 \ldots \omega_n$. *Journal of London Math Society*, 32(1):1-11, 1985.

[5] R. Odoni. Realizing wreath products of cyclic groups as galois groups. *Mathematika*, 35(1):101-113, 1968.