Constructing irreducible polynomials using isogenies

Gaetan Bisson

COUNT Conference
Luminy, 1st March 2023

Abstract

Let S be a rational fraction and let f be a polynomial over a finite field. Consider the transform $T(f) = \text{numerator}(f(S))$. In certain cases, the polynomials f, $T(f)$, $T(T(f))\ldots$ are all irreducible. For instance, in odd characteristic, this is the case for the rational fraction $S = (x^2+1)/(2x)$, known as the R-transform, and for a positive density of all irreducible polynomials f.

We interpret these transforms in terms of isogenies of elliptic curves. Using complex multiplication theory, we devise algorithms to generate a large number of other rational fractions S, each of which yields infinite families of irreducible polynomials for a positive density of starting irreducible polynomials f.

This is joint work with Alp Bassa and Roger Oyono.

1 Iterated presentations

For a rational fraction $S \in \mathbb{Q}(x)$ and a finite field k where it has good reduction, consider

$$T_S : \begin{cases} k[x] \longrightarrow k[x] \\ f(x) \longmapsto \text{numerator}\big(f(S(x))\big). \end{cases}$$

Take for instance $Q(x) = (x^2+1)/x$ and $k = \mathbb{F}_2$; we have

$$\begin{aligned} f(x) &= x^2 + x + 1, \\ T_Q(f)(x) &= x^4 + x^3 + x^2 + x + 1, \\ T_Q^2(f)(x) &= x^8 + x^7 + x^6 + x^4 + x^2 + x + 1, \\ T_Q^3(f)(x) &= x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + x^3 + x^2 + x + 1, \end{aligned}$$

and so on; observe that all the polynomials $T_Q^i(f)$ are irreducible. When such is the case, we say that they induce an *iterated presentation* of the field

$$k^{[de^\infty]} = \bigcup_{i=0}^{\infty} k^{[de^i]}$$

where $d = \deg(f)$, $e = \deg(S)$, and $k^{[\ell]}$ denotes the degree-ℓ extension of the finite field k.

2 Prior work

Two classical results concern the so-called Q and R-transform:

$$Q(x) = \frac{x^2+1}{x}, \qquad R(x) = \frac{x^2+1}{2x}.$$

Theorem 2.1 (Varshamov 1984, Meyn 1990, Kyuregyan 2002). *Let $k/\mathbb{F}_2$ be a finite field and let $f \in k[x]$ be a monic irreducible polynomial with coefficients $(a_\ell)_{\ell=0}^{n}$. Assume* $\operatorname{tr}(a_{n-1}) = \operatorname{tr}(a_1/a_0) = 1$. *Then (Q, f) induces an iterated presentation.*

Theorem 2.2 (Cohen 1992). *Let k be a finite field of odd characteristic and let $f \in k[x]$ be a monic irreducible polynomial. Assume $f(1)f(-1)$ is not a square. If $|k| = 3 \bmod 4$, assume furthermore that* $\deg(f)$ *is even. Then (R, f) induces an iterated presentation.*

More recent work:

- Kyuregyan 2003, 2006: exhaustive study of degree-two rational fractions;
- Bassa–Menares 2019, 2023: interpretation via Galois theory of function fields.

3 Exploiting isogenies

Take:

- $\varphi : \mathscr{E}_0 \leftarrow \mathscr{E}_1$ a separable isogeny over k between elliptic curves in Weierstrass form;
- S its action on the x-coordinate;
- P a point in $\mathscr{E}_0(\overline{k})$;
- f the minimal polynomial of its x-coordinate x_P.

For any point $Q \in \varphi^{-1}(P)$, we have $x_P = S(x_Q)$; since $f(S(x_Q)) = 0$, the polynomial $T_S(f)$ is minimal for x_Q, and therefore is irreducible, as soon as it has the expected degree, that is, $\big[k(x_Q) : k(x_P)\big] = \deg\varphi$.

This holds assuming $[k(Q) : k(P)] = \deg\varphi$ and either $\deg\varphi$ odd or $[k(P) : k(x_P)] = 2$.

We wish to iterate this.

$$\begin{tikzcd}
\mathscr{E}_0 \arrow[d] & \mathscr{E}_1 \arrow[l, "\varphi_0"'] \arrow[d] & \mathscr{E}_2 \arrow[l, "\varphi_1"'] \arrow[d] & {} \arrow[l, dotted] \\
\mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "S_0"] & \mathbb{P}^1 \arrow[l, "S_1"] & {} \arrow[l, dotted]
\end{tikzcd}$$

Theorem 3.1. *Let $\mathscr{E}_0 \xleftarrow{\varphi_0} \mathscr{E}_1 \xleftarrow{\varphi_1} \mathscr{E}_2$ be two separable isogenies of degree ℓ_0 et ℓ_1 defined over a finite field k. Suppose all prime factors of ℓ_1 divide ℓ_0. Suppose also that the kernel of their composition* $\ker(\varphi_0 \circ \varphi_1)$ *is cyclic and that all its points are defined over $k(P)$ for some $P \in \mathscr{E}_0(\overline{k})$. Then, for all points $Q \in (\varphi_0 \circ \varphi_1)^{-1}(P)$ we have*

$$[k(\varphi_1(Q)) : k(P)] = \ell_0 \quad \Longrightarrow \quad [k(Q) : k(P)] = \ell_0 \ell_1.$$

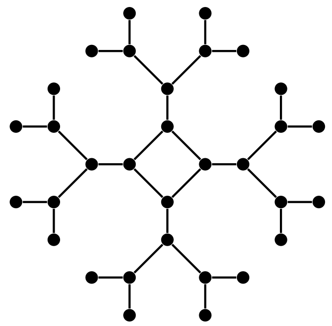
Iterate with $\varphi_0 = \varphi_1$ an endomorphism. If $\deg(\varphi)$ is prime, $\ker(\varphi^2)$ cyclic $\Leftrightarrow \varphi \neq \widehat{\varphi}$.

We look for such φ and ignore associated P's for now.

4 Volcanoes and cycles

We look for a cycle $\varphi : \mathscr{E} \to \mathscr{E}$ in the isogeny graph where no edge is dual to another.

Assuming E ordinary and ℓ prime, the ℓ-isogeny graph is a volcano



The only cycle lies at the rim formed by elliptic curves with maximal endomorphism ring locally at ℓ. By CM theory, this is the Cayley graph of the subset of ideals of norm ℓ in the class group of $\mathbb{Q}(\pi)$.

The easiest construction is when this cycle is trivial: fix a finite field k and a prime ℓ; enumerate small discriminants Δ for which ℓ splits into principal ideals; compute the corresponding elliptic curve and isogeny via CM theory.

q	ℓ	S
2	3	$(x^3+1)/x^2$
5	3	$x/(x^3+x^2+1)$
11	2	$x/(x^2+1)$

Other constructions: prime ideals of order two; principal products of prime ideals; supersingular case. And my favorite: characteristic zero!

Proposition 4.1 (Silverman 1994)**.** *There are three isomorphism classes of elliptic curves over $\mathbb{Q}$ which admit a degree-two endomorphism, namely:*

(i) $E : y^2 = x^3 + x, \quad j = 1728, \quad \alpha = 1 + \sqrt{-1},$
$$[\alpha](x,y) = \left(\alpha^{-2}\left(x + \frac{1}{x}\right), \alpha^{-3} y \left(1 - \frac{1}{x^2}\right)\right);$$

(ii) $E : y^2 = x^3 + 4x^2 + 2x, \quad j = 8000, \quad \alpha = \sqrt{-2},$
$$[\alpha](x,y) = \left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3} y \left(1 - \frac{2}{x^2}\right)\right);$$

(iii) $E : y^2 = x^3 - 35x + 98, \quad j = -3375, \quad \alpha = \dfrac{1+\sqrt{-7}}{2},$
$$[\alpha](x,y) = \left(\alpha^{-2}\left(x - \frac{7(1-\alpha)^4}{x+\alpha^2-2}\right), \alpha^{-3} y \left(1 + \frac{7(1-\alpha)^4}{(x+\alpha^2-2)^2}\right)\right).$$

Extended to degree three and four by Reitsma 2017.

5 Density of transforms

For each rational fraction S we compute the density of irreducible polynomials f of degree d over the finite field with q elements which induce an iterated presentation. The Chebotarev theorem can be used to prove the asymptotic density of certain columns.

$S=\dfrac{x^2+1}{x}$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=2$	1	0	1/3	1/3	2/9
$q=3$	2/3	0	5/9	0	15/29
$q=5$	0	0	0	0	0
$q=7$	8/21	0	12/49	0	≈ 0.25
$q=11$	8/55	≈ 0.12	≈ 0.13	≈ 0.12	≈ 0.12
$q=13$	2/13	11/91	≈ 0.13	≈ 0.13	≈ 0.13

$S=\dfrac{1}{2}\dfrac{x^2+1}{x}$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=3$	2/3	0	5/9	0	15/29
$q=5$	3/5	1/2	13/25	1/2	≈ 0.50
$q=7$	4/7	0	25/49	0	≈ 0.50
$q=11$	6/11	0	≈ 0.50	0	≈ 0.50
$q=13$	7/13	1/2	≈ 0.50	1/2	≈ 0.50
$q=17$	9/17	1/2	≈ 0.50	1/2	≈ 0.50

$S=\alpha^{-2}\left(x+4+\dfrac{2}{x}\right)$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=3$	0	1/2	0	1/2	0
$q=11$	0	1/2	0	1/2	0
$q=17$	0	0	0	0	0
$q=19$	0	1/2	0	1/2	0
$q=41$	0	0	0	0	0
$q=43$	0	1/2	0		

$S=\alpha^{-2}\left(x-\dfrac{7(1-\alpha)^4}{x+\alpha^2-2}\right)$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=7$	1	1	1	1	1
$q=11$	16/55	≈ 0.26	≈ 0.26	≈ 0.25	≈ 0.25
$q=23$	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25
$q=29$	8/29	≈ 0.25	≈ 0.25		
$q=37$	≈ 0.26	≈ 0.25	≈ 0.25		
$q=43$	≈ 0.25	≈ 0.25	≈ 0.25		

References

[1] Alp Bassa, Gaetan Bisson, and Roger Oyono. *Iterative constructions of irreducible polynomials from isogenies*. 2023. arXiv: 2302.09674.

[2] Alp Bassa and Ricardo Menares. "Galois theory and iterative construction of irreducible polynomials." In: (2022). In preparation.

[3] Alp Bassa and Ricardo Menares. "The R-transform as a power map and its generalisations to higher degree." In: (2019). URL: https://arxiv.org/abs/1909.02608.

[4] Stephen D. Cohen. "The explicit construction of irreducible polynomials over finite fields." In: *Designs, Codes and Cryptography* 2 (1992), pages 169–174. DOI: 10.1007/BF00124895.

[5] Melsik K. Kyuregyan. "Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics." In: *Finite Fields and their Applications* 9.1 (2003), pages 39–58. DOI: 10.1016/S1071-5797(02)00005-9.

[6] Melsik K. Kyuregyan. "Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics, II." In: *Finite Fields and their Applications* 12.3 (2006), pages 357–378. DOI: 10.1016/j.ffa.2005.07.002.

[7] Melsik K. Kyuregyan. "Recurrent methods for constructing irreducible polynomials over GF(2^s)." In: *Finite Fields and their Applications* 8.1 (2002), pages 52–68. DOI: 10.1006/ffta.2001.0323.

[8] Helmut Meyn. "On the construction of irreducible self-reciprocal polynomials over finite fields." In: *Applicable Algebra in Engineering, Communication and Computing* 1.1 (1990), pages 43–53. DOI: 10.1007/BF01810846.

[9] Berno Reitsma. "Endomorphisms of degree 2, 3 and 4 on elliptic curves." Bachelor's thesis. Rijksuniversiteit Groningen, 2017. URL: https://fse.studenttheses.ub.rug.nl/15691/1/Bsc_Math_2017_Reitsma_B.pdf.

[10] Joseph Hillel Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Volume 151. Graduate Texts in Mathematics. Springer, 1994. DOI: 10.1007/978-1-4612-0851-8.

[11] Rom Rubenovich Varshamov. "A general method of synthesis for irreducible polynomials over Galois fields." In: *Proceedings of the USSR Academy of Sciences* 275.5 (1984), pages 1041–1044. URL: http://mi.mathnet.ru/eng/dan/v275/i5/p1041.