Iterative constructions of irreducible polynomials from isogenies

Alp Bassa [a] Gaetan Bisson [b] Roger Oyono [b]

[a] Department of Mathematics, Boğaziçi University, Turkey
[b] Laboratoire GAATI, University of French Polynesia

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, $T(f)$, $T(T(f))\dots$ 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 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 rational fractions S, each of which yields infinite families of irreducible polynomials for a positive density of starting irreducible polynomials f.

1 Introduction

Constructing finite fields depends on generating irreducible polynomials, with many applications to coding theory and cryptography focusing on the small-characteristic, large-degree case. Various techniques have thus been developed to solve this problem [15, 10, 5] beyond the standard trial-and-error method based on irreducibility testing. Further, selecting suitable irreducible polynomials is critical to obtain efficient finite field arithmetic which, again, motivated the development of advanced techniques [1].

Here, we design fast algorithms to generate irreducible polynomials of large, smooth degree. In fact, our algorithms generate infinite families of irreducible polynomials of increasing degree for the divisibility order. This enables the construction of infinite towers of field extensions, which yield explicit representations of "parts of" the algebraic closure. Such towers also have applications to the construction of high-order elements [4, 11] as well as to point counting methods on algebraic curves [13].

We build upon the following approach.

Let $S \in \mathbb{Q}(x)$ be a rational fraction and let k be a finite field where the reduction of the denominator of S does not vanish, that is, the denominator is coprime to $|k|$. For any polynomial $f \in k[x]$ we define the S-transform of f as the polynomial $T_S(f) = \text{numerator}(f(S(x)))$ and we let

$$I_S(f) = \left(T_S^i(f)\right)_{i \geqslant 0}$$

denote the family of polynomials obtained by applying the composition of i copies of T_S, which we denote by $T_S^i = T_S \circ \cdots \circ T_S$, to the polynomial f. We say that S induces an irreducible family from f if the polynomials in the family $I_S(f)$ are all irreducible.

$$\begin{tikzcd}
& \mathscr{E}_1 \arrow[ld, "\varphi"'] \arrow[rd] & \\
\mathscr{E}_0 \arrow[rd] & & \mathbb{P}^1 \arrow[ld, "S"] \\
& \mathbb{P}^1 &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
& k(Q) \arrow[ld, dash, "\deg\varphi"'] \arrow[rd, dash] & \\
k(P) \arrow[rd, dash] & & k(x_Q) \arrow[ld, dash] \\
& k(x_P) &
\end{tikzcd}$$

Figure 1: On the left, the projection of an isogeny $\mathscr{E}_0 \xleftarrow{\varphi} \mathscr{E}_1$ to its Lattès map S; on the right, the corresponding field extensions where the points satisfy $P = \varphi(Q)$.

For example, well-known transforms include the so-called Q-transform which uses the rational fraction $Q(x) = \frac{x^2+1}{x}$ and the so-called R-transform which uses the rational fraction $R(x) = \frac{x^2+1}{2x}$; more explicitly, we have

$$T_Q(f)(x) = x^{\deg(f)} \cdot f\left(\frac{x^2+1}{x}\right),$$
$$T_R(f)(x) = (2x)^{\deg(f)} \cdot f\left(\frac{x^2+1}{2x}\right).$$

Those two transforms have been studied extensively and are known to induce irreducible families.

Theorem 1.1 (Q-transform [17, 12, 8]). *Let $q = 2^r$ and let $f(x) = \sum_{i=0}^{n} a_i x^i$ be an irreducible polynomial in $\mathbb{F}_q[x]$ with $a_n = 1$. Denote by* tr *the trace from $\mathbb{F}_q$ to $\mathbb{F}_2$. Assuming* $\operatorname{tr}(a_{n-1}) = \operatorname{tr}(a_1/a_0) = 1$*, the fraction Q induces an irreducible family from f.*

Theorem 1.2 (R-transform [4]). *Let q be an odd prime power and let f be a monic irreducible polynomial in $\mathbb{F}_q[x]$. Assume that $f(1)f(-1)$ is not a square in $\mathbb{F}_q$ and, if* $q = 3 \bmod 4$*, assume additionally that* $\deg(f)$ *is even. The fraction R induces an irreducible family from f.*

Recently, there has been interest in constructing more transforms T which induce irreducible families. We note the work of Bassa and Menares using Galois theory on function fields [2] and multiplicative group theory [3].

In this article we construct such transforms from isogenies of elliptic curves. Our main results are algorithms which generate a large diversity of transforms.

2 General framework

We first explain the relationship between the transform T_S and isogenies. Let $\mathscr{E}_0 \xleftarrow{\varphi} \mathscr{E}_1$ be an isogeny of elliptic curves in Weierstrass form defined over a finite field k; there exists a rational fraction S such that $\varphi(x, y) = (S(x), \cdot)$. We define the degree of such a rational fraction $S = u/v$ with $u, v \in k[x]$ to be $\deg S = \max\{\deg u, \deg v\}$; this definition suits our purpose since it yields the equalities $\deg \varphi = \deg S$ and $\deg T_S(f(x)) = \deg S \cdot \deg f$.

Now, consider two points $P \in \mathscr{E}_0(\overline{k})$ and $Q \in \mathscr{E}_1(\overline{k})$ satisfying $P = \varphi(Q)$ and such that $[k(Q):k(P)] = \deg\varphi$. Denote by $f(x) \in k[x]$ the minimal polynomial of x_P over k. Since $f(S(x_Q)) = f(x_P) = 0$, the polynomial $T_S(f(x))$ vanishes on x_Q; it is therefore irreducible if and only if it is the minimal polynomial of x_Q or, equivalently, if its degree is that of the extension $[k(x_Q):k]$. We have

$$\begin{aligned} & T_S(f(x)) \text{ is irreducible} \\ \iff \quad & \deg T_S(f(x)) = [k(x_Q):k] \\ \iff \quad & \deg S \cdot \deg f = [k(x_Q):k(x_P)] \cdot [k(x_P):k] \\ \iff \quad & \deg\varphi = [k(x_Q):k(x_P)]. \end{aligned}$$

Since φ commutes with the involution endomorphism $(x,y) \mapsto (x,-y)$, quotienting out by it yields the commutative diagram on the left of Figure 1 where the arrows to the projective line are the projections of points to their x-coordinate. This induces the field extensions diagram on the right of Figure 1 which shows

$$[k(Q):k(P)] \cdot [k(P):k(x_P)] = [k(Q):k(x_Q)] \cdot [k(x_Q):k(x_P)]$$

where $[k(Q):k(P)] = \deg\varphi$; furthermore, the x-coordinate of points on an elliptic curve satisfies $[k(P):k(x_P)] \in \{1,2\}$ and $[k(Q):k(x_Q)] \in \{1,2\}$. We deduce that, if either $\deg\varphi$ is odd or $[k(P):k(x_P)] = 2$, then $[k(x_Q):k(x_P)] = \deg\varphi$. Consequently, the polynomial $T_S(f(x))$ is irreducible.

To iterate this construction, we require a criterion on the isogeny φ which ensures that the condition $[k(Q):k(P)] = \deg\varphi$ holds under further compositions by φ. We begin with a simple but key lemma which describes the action of the Frobenius endomorphism in explicit terms.

Lemma 2.1. *Let $\mathscr{E}_0$ and $\mathscr{E}_1$ be elliptic curves and $\mathscr{E}_0 \xleftarrow{\varphi} \mathscr{E}_1$ be a separable isogeny defined over a finite field k. Fix a point $P \in \mathscr{E}_0(\overline{k})$ and denote by π the $k(P)$-Frobenius endomorphism on $\mathscr{E}_1$. If all points in the kernel of φ are defined over $k(P)$, then there exists a point $F \in \ker\varphi$ such that, for all points $Q \in \varphi^{-1}(P)$ and for all $n \in \mathbb{N}$, we have $\pi^n(Q) = Q + nF$.*

Proof. Let $Q \in \varphi^{-1}(P)$ be a preimage of P; we have

$$\varphi(\pi(Q) - Q) = \pi(\varphi(Q)) - \varphi(Q) = \pi(P) - P = 0.$$

Thus we have $\pi(Q) = Q + F$ for some point $F \in \ker\varphi$ which does not depend on Q; indeed, for any other $Q' \in \varphi^{-1}(P)$, we have

$$\pi(Q') = \pi(Q) + \pi(Q' - Q) = (Q + F) + (Q' - Q) = Q' + F.$$

Applying π iteratively yields

$$\pi^n(Q) = \pi^{n-1}(Q + F) = \pi^{n-1}(Q) + F = \cdots = Q + nF.$$

□

We deduce the theorem below which gives precisely the criterion we required.

Theorem 2.2. *Let $\mathscr{E}_0 \xleftarrow{\varphi_0} \mathscr{E}_1 \xleftarrow{\varphi_1} \mathscr{E}_2$ be two separable isogenies of respective degree ℓ_0 and ℓ_1 defined over a finite field k. Suppose that all prime factors of ℓ_1 divide ℓ_0. Fix a point $P \in \mathscr{E}_0(\overline{k})$ and assume that the kernel* $\ker(\varphi_0 \circ \varphi_1)$ *is cyclic and that all its points are $k(P)$-rational. Then, all points $Q \in (\varphi_0 \circ \varphi_1)^{-1}(P)$ satisfying $[k(\varphi_1(Q)) : k(P)] = \ell_0$ also satisfy $[k(Q) : k(P)] = \ell_0 \ell_1$.*

Proof. Since $G = \ker(\varphi_0 \circ \varphi_1)$ is a cyclic subgroup of $\mathscr{E}_2(k(P))$ of order $\ell_0\ell_1$, it admits a unique subgroup of order ℓ_1, namely $\ell_0 \cdot G$, which by uniqueness is equal to $\ker \varphi_1$. Denote by π the $k(P)$-Frobenius endomorphism on $\mathscr{E}_2$. By Lemma 2.1, there exists a point $F \in G$ satisfying $\pi^n(Q) = Q + nF$. In particular, its order is $\mathrm{ord}(F) = [k(Q) : k(P)]$. Since $\pi(\varphi_1(Q)) = \varphi_1(\pi(Q)) = \varphi_1(Q+F) = \varphi_1(Q) + \varphi_1(F)$, we similarly have $[k(\varphi_1(Q)) : k(P)] = \mathrm{ord}(\varphi_1(F))$.

Assume now $[k(\varphi_1(Q)) : k(P)] = \ell_0$, that is, $\mathrm{ord}(\varphi_1(F)) = \ell_0$. We claim $\mathrm{ord}(F) = \ell_0\ell_1$. Suppose otherwise that $\mathrm{ord}(F) < \ell_0\ell_1$. Then, we can write $F = p \cdot T$ for some $T \in G$ and some prime p dividing $\ell_0\ell_1$. As all prime divisors of ℓ_1 are divisors of ℓ_0, we have $p \mid \ell_0$. This implies $\ell_0/p \cdot F = \ell_0 \cdot T \in \ell_0 \cdot G = \ker \varphi_1$, that is, $\varphi_1(F)$ is an ℓ_0/p-torsion point of $\mathscr{E}_1$; this contradicts $\mathrm{ord}(\varphi(F)) = \ell_0$. We thus obtain $\mathrm{ord}(F) = \ell_0\ell_1 = [k(Q) : k(P)]$ as claimed. □

Note that the simplest setting where this result can be iterated is when $\mathscr{E}_0 = \mathscr{E}_1 = \mathscr{E}_2$ and the endomorphisms φ_0 and φ_1 are identical. This yields the following corollary where we assume that $\deg \varphi$ is odd for simplicity.

Corollary 2.3. *Let $\mathscr{E}$ be an elliptic curve, $\varphi : \mathscr{E} \to \mathscr{E}$ a separable endomorphism of odd degree defined over a finite field k, and $P \in \mathscr{E}(\overline{k})$ a point. Suppose that the subgroup* $\ker(\varphi \circ \varphi)$ *is cyclic and that all its points are $k(P)$-rational. Denote by S the x-coordinate map of φ and by f the minimal polynomial of x_P over k. Then, if $T_S(f)$ is irreducible, so are all polynomials in the family $I_S(f)$.*

The map S is what is known as a Lattès map [9]: it is the projection of an endomorphism $\varphi : \mathscr{E} \to \mathscr{E}$ through a finite separable cover $\mathscr{E} \to \mathbb{P}^1$, in this case, the projection on the x-coordinate.

Remark 2.4. *The condition that* $\ker(\varphi \circ \varphi)$ *be cyclic is equivalent to no isogeny factor of φ being dual to another. This holds whenever* $\deg(\varphi)$ *is squarefree. Indeed, if a factor ψ were dual to another, it would necessarily be itself and we would then have $2\psi = \psi + \widehat{\psi} = [\mathrm{tr}\,\psi]$; taking determinants shows that* $\deg \psi$ *would be a square, which contradicts the assumption.*

2.1 Möbius transforms

For any matrix m in the linear group $\mathrm{GL}_2(\mathbb{Z})$ of invertible two-by-two matrices with integer coefficients, define the rational fraction

$$M_m(x) = \frac{\alpha x + \beta}{\gamma x + \delta}, \qquad \text{where } m = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

If S is a rational fraction in $\mathbb{Q}(x)$, we define the corresponding Möbius transform of S as the composition $S' = M_{m^{-1}} \circ S \circ M_m$. Note that the fraction S induces an irreducible family from a given polynomial f if and only if S' does. Thus we may apply Möbius transforms to any rational fraction while preserving its ability to induce irreducible families, for instance in order to try and reduce the size of its coefficients.

```
INPUT:  An elliptic curve $\mathscr{E}$ defined over a finite field $\mathbb{F}_q$.
OUTPUT: The $x$-coordinate map of the Verschiebung endomorphism.
    1. Compute the division polynomial $\varphi_q(x)$
       for the multiplication-by-$q$ map on $\mathscr{E}$.
    2. Return $\varphi_q(x^{1/q})$.
```

Algorithm 1: Computing the Lattès map of the Verschiebung endomorphism of an elliptic curve defined over a finite field.

Our efforts will from now on be focused on finding isogenies $\varphi : \mathscr{E} \to \mathscr{E}$ which satisfy the conditions of Corollary 2.3 and obtaining the corresponding rational fractions S; we will purposely not look for associated points P and polynomials f. Nevertheless, in Section 6, we will compute for each selected rational fraction S, the density of irreducible polynomials of a given degree in a given finite field for which S induces irreducible families.

3 The Verschiebung endomorphism

Let $\varphi : \mathscr{E} \to \mathscr{E}$ be a separable endomorphism of prime degree ℓ defined over a finite field $k = \mathbb{F}_q$. In this section we consider the case where ℓ divides q. Since the multiplication-by-q map satisfies $[q] = \pi\widehat{\pi}$, the endomorphism is either a factor of the Frobenius π, which is purely inseparable, or of its dual, the Verschiebung $\widehat{\pi}$, which is separable if and only if the elliptic curve $\mathscr{E}$ is ordinary.

We thus specialize Corollary 2.3 to the case $\varphi = \widehat{\pi}$. By Remark 2.4, when q is prime, the condition that $\ker(\varphi \circ \varphi)$ be cyclic holds. We obtain:

Proposition 3.1. *Let $\mathscr{E}$ be an ordinary elliptic curve defined over a prime field $\mathbb{F}_p$ with $p > 2$. Denote by S the x-coordinate map of its Verschiebung endomorphism $\widehat{\pi}$. The rational fraction S induces irreducible families from all polynomials f which:*

- *are minimal polynomials of the x-coordinate of some $P \in \mathscr{E}(\overline{k})$ such that $\ker(\widehat{\pi} \circ \widehat{\pi}) \subset \mathscr{E}(k(P))$; and*
- *verify that $T_S(f)$ is irreducible.*

In order to compute the x-coordinate of the Verschiebung endomorphism on an elliptic curve $\mathscr{E}$, we use Algorithm 1.

Table 1 gives rational fractions obtained using this algorithm, including by composing with the Möbius map. More specifically, for small $q = |k|$, it gives the number N of such transforms and a representative element selected for having lowest Hamming weight. We include the case $q = 2^d$ since, while not covered by Proposition 3.1, it still induces irreducible families.

Note that for $q = 2$ this method yields the well-known Q-transform.

4 Isogenies of ordinary curves over finite fields

We now turn to separable endomorphisms $\varphi : \mathscr{E} \to \mathscr{E}$ of squarefree degree ℓ which are coprime to the characteristic. Elliptic curves $\mathscr{E}/\mathbb{F}_q$ which admit such endomorphisms may be efficiently enumerated as their j-invariants are exactly the roots of the modular polynomial

q	N	REPRESENTATIVE FRACTION
2	6	$x/(x^2+1)$
4	180	$(x^4+x^2+1)/(x^3+x)$
8	3528	$(x^7+x)/(x^8+x^6+x^4+x^2+1)$
3	36	$(x^3+x^2+x+2)/x^2$
5	345	$(2x^5+x)/(x^4+2)$
7	1428	$(5x^7+x^4+6x)/(x^6+x^3+3)$
11	8250	$(8x^{11}+x^9+7x^7+4x^3+10x)/(x^{10}+x^8+2x^4+7x^2+8)$

Table 1: Some rational fractions which induce irreducible families, computed as Lattès maps of Verschiebung endomorphisms.

$\Phi_\ell(X,X) \in \mathbb{F}_q[X]$. Vélu's formula [18] can then be used to compute φ from its kernel, itself found as a subgroup of $\mathscr{E}[\ell](\mathbb{F}_q)$.

The situation is particularly explicit when $\mathscr{E}/\mathbb{F}_q$ is ordinary. Its endomorphism ring $\operatorname{End}(\mathscr{E})$ is then an order in the imaginary quadratic field $K = \mathbb{Q}(\pi)$ containing $\mathbb{Z}[\pi]$. Isogenies $\varphi : \mathscr{E} \to \mathscr{E}'$ of prime degree $\ell \nmid q$ fall into one of two categories:

1. So-called *horizontal* isogenies satisfy $\operatorname{End}(\mathscr{E}) = \operatorname{End}(\mathscr{E}')$ and are described by the theory of complex multiplication [14] which states that the ideal class group $\operatorname{cl}(\mathcal{O})$ acts faithfully and transitively on the set of isomorphism classes of elliptic curves $\mathscr{E}$ satisfying $\operatorname{End}(\mathscr{E}) \simeq \mathcal{O}$.

2. Other prime-degree isogenies are said to be *vertical* and display the so-called volcano structure [7, 6].

Connected components of degree-ℓ isogeny graphs thus have the shape illustrated by Figure 2: elliptic curves with locally maximal endomorphism ring are connected by horizontal isogenies which form a cycle (the rim of the volcano) of length the order in the class group of an ideal of norm ℓ; other elliptic curves are located on trees formed of vertical isogenies hanging from maximal curves; the graph is regular of degree $\ell + 1$ except at the leaves.

Let us now state two applications of this structure to the construction of endomorphisms which satisfy the hypothesis of Corollary 2.3.

4.1 Endomorphisms of prime degree

Let $\mathscr{E}$ be an ordinary elliptic curve defined over a finite field. By complex multiplication theory, endomorphisms $\varphi : \mathscr{E} \to \mathscr{E}$ of prime degree ℓ correspond to principal ideals of order ℓ in the class group of $\operatorname{End}(\mathscr{E})$. By Remark 2.4, the resulting subgroup $\ker(\varphi \circ \varphi)$ is always cyclic.

Concretely, given a prime power q and a prime ℓ, we construct such endomorphisms by looking for small discriminants Δ for which ℓ splits into primes of order one in the class group of $\mathbb{Q}(\sqrt{\Delta})$; we then use the Hilbert class polynomial H_Δ to generate elliptic curves over $\mathbb{F}_q$ with endomorphism algebra $\mathbb{Q}(\sqrt{\Delta})$; finally, we compute the corresponding degree-ℓ isogeny and extract its x-coordinate.

This yields Table 2 where, again, we select the lowest Hamming-weight representative for each rational fraction S under Möbius action.

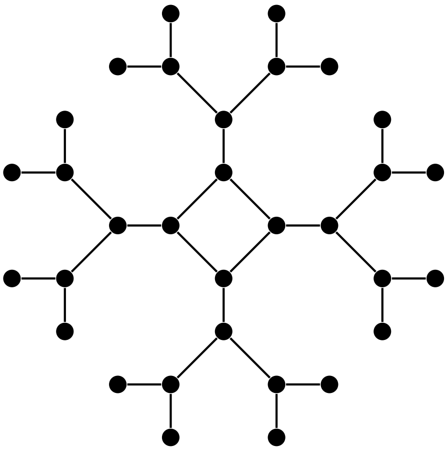

Figure 2: A connected component of a degree-2 isogeny graph displaying the so-called volcano structure; the order in the class group of both primes of norm two is four (the length of the rim) and the conductor $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ has valuation three at two (the height of the trees).

q	ℓ	REPRESENTATIVE FRACTION
2	3	$(x^3+1)/x^2$
5	3	$x/(x^3+x^2+1)$
7	5	$(x^5+x^4+x^3+6x^2+x)/(x^4+x^3+4x^2+x+1)$
11	2	$x/(x^2+1)$
11	5	$(x^5+9x^4+10x^3+4x+1)/(x^5+x^3+9)$
17	5	$(15x^5+3x^3+x)/(x^5+3x^4+15x^3+x^2+1)$

Table 2: Some rational fractions which induce irreducible families, computed as cyclic endomorphisms of prime degree.

q	REPRESENTATIVE FRACTION
2	$(x^7+x^3+x)/(x^9+x^6+x^5+x^2+1)$
7	$(2x^{10}+4x^9+x^6+x^5+3x^4+2x+3)/(x^9+6x^8+5x^5+x^2+4x)$
17	$(13x^9+4x^7+x^5+8x)/(x^8+13x^4+11x^2+15)$
17	$(9x^9+3x^7+13x^5+10x^3+9x)/(x^8+x^6+x^4+4x^2+4)$
19	$(11x^4+17x^2+8)/(x^4+1)$
19	$(18x^9+x^7+14x^5+11x^3+12x)/(x^{10}+5x^8+x^6+7x^4+5x^2+11)$
19	$(13x^5+10x^3+10x)/(x^6+1)$
19	$(11x^3+11x)/(x^4+1)$
19	$(16x^3+x)/(x^4+4x^2+17)$
19	$(16x^{10}+13x^6+12x^4+1)/(x^9+x^7+10x^5+4x^3+16x)$
19	$(8x^6+14x^4+14x^2+8)/(x^5+x^3+x)$
19	$(x^4+7)/(x^4+14x^2+12)$

Table 3: Some rational fractions which induce irreducible families, computed as cyclic endomorphisms of small degree.

4.2 Endomorphisms of small degree

Endomorphisms of ordinary elliptic curve $\mathscr{E}$ defined over finite fields may also be constructed by composing multiple horizontal isogenies which form a cycle in the isogeny graph. That boils down to searching for products of prime ideals which are principal in the class group of $\mathrm{End}(\mathscr{E})$; the corresponding isogeny cycle can then be constructed via complex multiplication theory.

Here, we simply search for such endomorphisms, select those with cyclic kernel and small degree, and apply Möbius transforms to reduce the Hamming weight of the rational fraction describing their action on the x-coordinate. Among others, we find the rational fractions of Table 3. Note that, as expected, the number of rational fractions this generates grows with q.

5 Isogenies of ordinary curves over number fields

Let $\mathscr{E}$ be an elliptic curve defined over a number field K which admits a rational endomorphism $\alpha : \mathscr{E} \to \mathscr{E}$ with cyclic kernel. For all places $\mathfrak{p}$ of good reduction where the localization of α still has cyclic kernel, the reduction of α to $K/\mathfrak{p}$ yields an endomorphism φ_1 to which Theorem 2.2 may be applied. By the Cebotarev density theorem, the rational fraction defining α in characteristic zero can thus be applied to a positive density of finite fields.

Endomorphisms of degree two. The simplest case concerns elliptic curves defined over the rationals and endowed with an endomorphism of degree two. Their j-invariants are the roots of the modular polynomial $\Phi_2(j,j)$ and their endomorphisms can be computed explicitly, resulting in the following theorem. See, for instance, [16, Proposition 2.3.1].

Proposition 5.1. *There are exactly three isomorphism classes of elliptic curves over $\mathbb{C}$ which possess an endomorphism of degree 2. The following are representatives for these curves and endomorphisms.*

	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$i=0$	1/3	1/2	4/9	1/2	14/29
$i=1$	0	1/2	0	1/2	0
$i=\infty$	2/3	0	5/9	0	15/29

Table 4: Density of irreducible polynomials of degree d over $\mathbb{F}_3$ which remain irreducible under only just i iterations of the map T_S where $S=(x^2+1)/x$.

$$\begin{aligned}
&\text{(i)} && E: y^2 = x^3 + x, \quad j = 1728, \quad \alpha = 1+\sqrt{-1},\\
& && [\alpha](x,y) = \left(\alpha^{-2}\left(x + \frac{1}{x}\right), \alpha^{-3} y \left(1 - \frac{1}{x^2}\right)\right);\\
&\text{(ii)} && E: y^2 = x^3 + 4x^2 + 2x, \quad j = 8000, \quad \alpha = \sqrt{-2},\\
& && [\alpha](x,y) = \left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3} y \left(1 - \frac{2}{x^2}\right)\right);\\
&\text{(iii)} && E: y^2 = x^3 - 35x + 98, \quad j = -3375, \quad \alpha = \frac{1+\sqrt{-7}}{2},\\
& && [\alpha](x,y) = \left(\alpha^{-2}\left(x - \frac{7(1-\alpha)^4}{x+\alpha^2-2}\right), \alpha^{-3} y \left(1 + \frac{7(1-\alpha)^4}{(x+\alpha^2-2)^2}\right)\right).
\end{aligned}$$

We note that the first endomorphism corresponds to the well-known Q-transform.

Endomorphisms of degree three. The same approach applies to higher-degree endomorphisms although the explicit formulas describing them are much heavier that in the above degree-two case.

Consider for instance the elliptic curve $E: y^2 + 6xy + 4y = x^3$ with j-invariant 54000. Since it is a root of the modular polynomial $\Phi_3(j,j)$, it admits a degree-three endomorphism. Indeed, this endomorphism can be written explicitly as $\varphi \circ \phi$ where $\alpha = \frac{1+\sqrt{-3}}{2}$ and

$$\begin{aligned}
\phi(x,y) &= \left(x + \frac{24}{x} + \frac{16}{x^2}, y - \frac{64}{x^3} - \frac{24(6x+y+4)}{x^2}\right),\\
\varphi(x,y) &= \left(-\frac{1}{3}x - 4, -\frac{1}{3\sqrt{-3}}y + \frac{3-\sqrt{-3}}{3}x - \frac{2}{3\sqrt{-3}} + 10\right).
\end{aligned}$$

6 Density of irreducible families

Let S be a rational fraction over a fixed finite field $\mathbb{F}_q$. We are interested in computing the density of irreducible polynomials f of small degree d from which S induces irreducible families. Through the Cebotarev density theorem, the conditions Corollary 2.3 may be used to compute these densities asymptotically. However this is burdensome and thus most entries in the tables below were obtained through exhaustive computations.

First consider the rational fraction $S=(x^2+1)/x$ over $\mathbb{F}_3$. Table 4 indicates, for selected integers i and d, the density of irreducible polynomials of degree d which remain irreducible under only just i iterations of the transform S. Each column adds up to one.

In Table 5, we only give the density of irreducible polynomials of degree d over $\mathbb{F}_q$ from which the rational fraction S induces irreducible families. In the particular case where $S=(x^2+1)/x$ and $q=3$, this corresponds to the line $i=\infty$ of Table 4.

$$S = \frac{x^2+1}{x}$$

	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=2$	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

$$S = \frac{1}{2}\frac{x^2+1}{x}$$

	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=3$	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

$$S = \alpha^{-2}\left(x - \frac{7(1-\alpha)^4}{x+\alpha^2-2}\right) \text{where } \alpha = \frac{1+\sqrt{-7}}{2}$$

	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=11$	16/55	13/55	≈ 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	≈ 0.25	≈ 0.25
$q=37$	≈ 0.26	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25
$q=43$	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25
$q=53$	≈ 0.26	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25

Table 5: Density of irreducible polynomials of degree d over $\mathbb{F}_q$ from which the rational fraction S induces irreducible families.

Acknowledgments

The authors thank the anonymous referees for their valuable comments.

Gaetan Bisson was supported by *Agence Nationale de la Recherche* under grant ANR-20-CE40-0013.

References

[1] Stéphane Ballet, Alexis Bonnecaze, and Bastien Pacifico. "A strategy to optimize the complexity of Chudnovsky-type algorithms over the projective line." In: *Contemporary Mathematics* 779 (2022), pages 13–32. DOI: 10.1090/conm/779/15668.

[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] Jean-Marc Couveignes and Reynald Lercier. "Fast construction of irreducible polynomials over finite fields." In: *Israel Journal of Mathematics* 194 (2013), pages 77–105. DOI: 10.1007/s11856-012-0070-8.

[6] Mireille Fouquet and François Morain. "Isogeny volcanoes and the SEA algorithm." In: *Algorithmic Number Theory — ANTS-V*. Edited by Claus Fieker and David Russell Kohel. Volume 2369. Lecture Notes in Computer Science. Springer, 2002, pages 47–62. DOI: 10.1007/3-540-45455-1_23.

[7] David Russell Kohel. "Endomorphism rings of elliptic curves over finite fields." PhD thesis. University of California at Berkeley, 1996. URL: http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf.

[8] 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.

[9] Samuel Lattès. "Sur l'itération des substitutions rationnelles et les fonctions de Poincaré." In: *Comptes rendus de l'académie des sciences de Paris* 166 (1918), pages 26–28.

[10] San Ling, Enver Ozdemir, and Chaoping Xing. "Constructing irreducible polynomials over finite fields." In: *Mathematics of Computation* 81 (2012), pages 1663–1668. DOI: 10.1090/S0025-5718-2011-02567-6.

[11] Helmut Meyn. "Explicit N-polynomials of 2-power degree over finite fields, I." In: *Designs, Codes and Cryptography* 6.2 (1995), pages 107–116. DOI: 10.1007/BF01398009.

[12] 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.

[13] Josep M. Miret, Jordi Pujolàs, and Nicolas Thériault. "On ℓ-th roots and division by ℓ." In: (2024). URL: https://arxiv.org/abs/2403.06619.

[14] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*. Volume 6. Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, 1961.

[15] Victor Shoup. “Fast Construction of Irreducible Polynomials over Finite Fields.” In: *Journal of Symbolic Computation* 17.5 (1994), pages 371–391. DOI: 10.1006/jsco.1994.1025.

[16] 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.

[17] 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.

[18] Jacques Vélu. “Isogénies entre courbes elliptiques.” In: *Comptes rendus de l'académie des sciences de Paris*. A 273 (1971), pages 238–241.