JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Vefa GOKSEL

A note on the factorization of iterated quadratics over finite fields

Tome 38, nº 1 (2026), p. 163-178.
https://doi.org/10.5802/jtnb.1358

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **38** (2026), 163–178

A note on the factorization of iterated quadratics over finite fields

par Vefa GOKSEL

Résumé. Soit f un polynôme quadratique unitaire sur un corps fini de caractéristique impaire. En 2012, Boston et Jones ont construit un processus de Markov basé sur l'orbite post-critique de f et ont conjecturé que sa distribution limite explique la factorisation des grands itérés de f. Plus tard, Xia, Boston et l'auteur ont effectué de nombreux calculs avec Magma et ont trouvé certaines familles exceptionnelles de quadratiques qui ne semblent pas suivre le modèle de Markov initial conjecturé par Boston et Jones. Ils ont découvert cela en observant empiriquement que certains schémas de factorisation prédits par le modèle de Boston–Jones ne semblent jamais se produire pour ces polynômes, et ils ont proposé un modèle de Markov à plusieurs étapes qui rend compte de ces schémas de factorisation manquants. Dans cette note, nous fournissons des démonstrations pour tous ces schémas de factorisation manquants. Ce sont les premiers résultats qui expliquent pourquoi la conjecture originale de Boston et Jones ne vaut pas pour tous les polynômes quadratiques unitaires.

Abstract. Let f be a monic quadratic polynomial over a finite field of odd characteristic. In 2012, Boston and Jones constructed a Markov process based on the post-critical orbit of f and conjectured that its limiting distribution explains the factorization of large iterates of f. Later, Xia, Boston, and the author performed extensive Magma computations and found some exceptional families of quadratics that do not seem to follow the original Markov model conjectured by Boston and Jones. They discovered this by empirically observing that certain factorization patterns predicted by the Boston–Jones model never seem to occur for these polynomials, and they suggested a multi-step Markov model that accounts for these missing factorization patterns. In this note, we provide proofs for all these missing factorization patterns. These are the first results that explain why the original conjecture of Boston and Jones does not hold for all monic quadratic polynomials.

Manuscrit reçu le 14 novembre 2024, accepté le 19 septembre 2025.
2020 *Mathematics Subject Classification.* 11T55, 37P25, 12E05, 20E08.
Mots-clefs. finite fields, iteration of polynomials, Markov processes, arithmetic dynamics.

1. Introduction

Let f be a polynomial of degree $d \geq 2$ over a field K. Let K^{sep} be a separable closure of K. For $n \geq 1$, we define the n-th iterate of f by

$$f^n := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}.$$

We also make the convention that $f^0(x) = x$. Suppose that f^n is separable over K for all $n \geq 1$. One obtains a complete infinite rooted d-ary tree using the roots of $f^n(x)$ (in K^{sep}) for $n \geq 0$ as follows: For $n \geq 0$, we place the roots of f^n at the n-th level of the tree, and we draw an edge between a root α of f^n and a root β of f^{n+1} if $f(\beta) = \alpha$. We denote this tree by T_d. Note that since any Galois element $\sigma \in \text{Gal}(K^{\text{sep}}/K)$ commutes with f, it preserves the connectivity relation on the tree, which leads to a continuous homomorphism

$$\rho : \text{Gal}(K^{\text{sep}}/K) \longrightarrow \text{Aut}(T_d).$$

The map ρ is called an arboreal Galois representation. Describing the image of ρ as a subgroup of the automorphism group $\text{Aut}(T_d)$ is a major open question in arithmetic dynamics. There are natural comparisons between arboreal Galois representations and the well-established theory of ℓ-adic Galois representations, which have inspired many works on arboreal Galois representations, especially in the last two decades. We refer the reader to [14] and [2, Section 5] for a general survey of the field. Also, see [1, 3, 4, 5, 8] for a few examples of recent work on the subject. Based on the existing results, it is widely believed that $\text{im}(\rho)$ has finite index inside $\text{Aut}(T_d)$ (or in a smaller overgroup, see [3]) unless f belongs to certain exceptional families of polynomials.

Let K_n be the splitting field of f^n over K. The image of ρ can also be described as the inverse limit of the Galois groups $\text{Gal}(K_n/K)$. Suppose that K is a number field. For any prime $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$, the image of the Frobenius class $\text{Frob}_\mathfrak{p}$ can be described by describing its image in each $\text{Gal}(K_n/K)$. Let $R_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. Let $g \in \mathcal{O}_K[x]$ be a monic irreducible polynomial. Suppose that the reduced polynomial $\bar{g} \in R_\mathfrak{p}[x]$ is separable. It is well-known that for all but finitely many primes $\mathfrak{p}$, the cycle structure of the action of $\text{Frob}_\mathfrak{p}$ on the roots of g is given by the factorization type of the reduced polynomial $\bar{g} \in R_\mathfrak{p}[x]$. Since $R_\mathfrak{p}$ is always a finite field, understanding the images of Frobenius classes requires studying the factorization of iterates of f over finite fields.

This motivation led Boston and Jones [15] to study factorizations of quadratic polynomials over finite fields, which is the simplest non-trivial case. Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $f \in \mathbb{F}_q[x]$ be a monic irreducible quadratic. Boston and Jones constructed a Markov model to track the factorization of iterates of f, and conjectured that the limiting

distribution arising from their model explains the full factorization of large iterates of f. Later, Xia, Boston, and the author [9] found new empirical data through Magma, which suggested that a more complicated model is required for some exceptional families of quadratic polynomials. Based on this empirical observation, they developed a multi-step Markov model and conjectured that this new Markov model explains the factorization of large iterates of f for any monic irreducible quadratic $f \in \mathbb{F}_q[x]$.

The main motivation behind the multi-step Markov model constructed by Xia, Boston, and the author was extensive Magma computations, which suggested that certain factorization patterns predicted by the Boston–Jones model never occur for the exhibited exceptional families of polynomials. The goal of this paper is to prove that these factorization patterns indeed never occur. Our work provides the first results explaining why the Boston–Jones model does not work for all monic quadratic polynomials. In particular, it proves one of the conjectures stated in [9], after a necessary correction (see Remark 1.5).

We would also like to note that, besides its aforementioned connection to arboreal Galois representations, the factorization of compositions of polynomials over finite fields is a well-studied subject in its own right. In addition to the two articles already discussed, see also [6, 7, 10, 11, 12, 17, 18] for several examples of recent work on the subject. See also Section 18 of the recent survey article [2] by Benedetto et al. for a general overview of the subject. Our main results also address a case of [2, Question 18.9].

Before stating our main results, we recall some notation and definitions. Let $f \in \mathbb{F}_q[x]$ be a monic quadratic polynomial, where $\mathbb{F}_q$ is a finite field of odd characteristic. Let $\gamma \in \mathbb{F}_q$ be the finite critical point of f. The *strict critical orbit* of f is the set

$$\mathcal{O}_f^+ = \{f(\gamma), f^2(\gamma), \dots\}.$$

We call it *strict* because it does not contain the critical point itself. Since we are working over a finite field, the critical orbit is necessarily finite. This is equivalent to saying that there exist minimal integers $m \geq 0$, $n \geq 1$, such that $f^m(\gamma) = f^{m+n}(\gamma)$. In this case, we say that f has *orbit type* (m, n). For notational convenience, we define $b_i := f^i(\gamma)$ for $i \geq 1$. Thus, the strict critical orbit of f becomes

$$\mathcal{O}_f^+ = \{b_1, b_2, \dots, b_{m+n-1}\}.$$

For simplicity, we will occasionally let $o_f := |\mathcal{O}_f^+| = m + n - 1$.

Boston and Jones defined the notion of *f-type* of a monic irreducible polynomial g over $\mathbb{F}_q$, which helps track the irreducible factors of $g(f^n(x))$ as n increases. We now recall the definition:

Definition 1.1. Let $f \in \mathbb{F}_q[x]$ be a monic quadratic with orbit type (m, n) and let $g \in \mathbb{F}_q[x]$ be an arbitrary monic polynomial. We define the *type* of g at any $\beta \in \mathbb{F}_q$ to be s if $g(\beta)$ is a square, and n if $g(\beta)$ is not a square. We then define the *f-type* of g as a string of length $m + n - 1$, where the k-th entry corresponds to the type of g at b_k (as defined above).

Example 1.2. Take $f = x^2 + 4x + 6 \in \mathbb{F}_7[x]$ and $g = x^3 + x + 1$. The critical point of f is $\gamma = 5 \in \mathbb{F}_7$, so the strict critical orbit $\mathcal{O}_f^+$ is $\{2, 4, 1\}$. Given that $g(2) = 4$, $g(4) = 6$, and $g(1) = 3$, the f-type of g is snn.

As mentioned earlier, the f-type of a polynomial g is a useful tool to understand factorizations of $g(f^n(x))$ as n gets large. For instance, for any monic irreducible polynomial $g \in \mathbb{F}_q[x]$ with even degree, if the first i entries of the f-type of g are n, then $g(f^j(x))$ is irreducible over $\mathbb{F}_q$ for all $j \leq i$ (see [15, Lemma 2.5]). On the other hand, if the first entry is s, then $g(f(x))$ factors as a product of two irreducible polynomials of equal degree over $\mathbb{F}_q$ (see [15, Proposition 2.6]). See Section 2 for more details on how the f-type of g affects the factorizations of the iterates $g(f^n(x))$.

We are now ready to present our main results.

Theorem 1.3. *Let $f \in \mathbb{F}_q[x]$ be a monic quadratic with orbit type $(2, n)$ for some $n \geq 1$. Let $g \in \mathbb{F}_q[x]$ be any monic irreducible polynomial of even degree, whose f-type begins with ns. Then, the type of each monic irreducible factor of $g(f^2(x))$ at b_n is s.*

Remark 1.4. Since the orbit type of f is $(2, n)$, evaluating $g(f^2(x))$ at b_n yields $g(f^2(b_n)) = g(b_{n+2}) = g(b_2)$, which, by hypothesis, is a square in $\mathbb{F}_q$. On the other hand, by hypothesis and using [15, Proposition 2.6], the polynomial $g(f^2(x))$ factors as $h(x - \gamma)h(-(x - \gamma))$ for some monic irreducible polynomial $h \in \mathbb{F}_q[x]$. Thus, the theorem states that although the product $h(b_n - \gamma)h(-(b_n - \gamma))$ is a square in $\mathbb{F}_q$ by hypothesis, it is impossible for both $h(b_n - \gamma)$ and $h(-(b_n - \gamma))$ to be non-squares.

Remark 1.5. Theorem 1.3 proves one of the conjectures in [9] (see Conjecture 4.5), after correcting a minor error and typo in the conjecture. Specifically, the polynomials in the conjecture must be monic, since the notion of *type* of a polynomial is not defined for non-monic polynomials, as noted in the errata published by Boston and Jones [16]. Secondly, we need to consider the iteration $g(f^2(x))$ rather than $g(f(x))$. The reason for this is that $g(f(x))$ does not factor when g has an f-type starting with ns, which would make the statement trivial, either true or false, depending solely on the f-type of g.

Remark 1.6. Quadratic polynomials over a finite field whose critical orbits have tail length 2 have shown curious properties in other contexts as well. For instance, see [13, Proposition 6.4]. The author thinks that it is worth

investigating whether there is a link between these two occurrences of this class of polynomials.

Theorem 1.7. *Let $f \in \mathbb{F}_q[x]$ be a monic quadratic with orbit type $(3,1)$, and let $g \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of even degree. Suppose the f-type of g begins with nn. If H is any monic irreducible factor of $g(f^3(x))$, then the product $H(b_1) \cdot H(b_2)$ is a square in $\mathbb{F}_q$.*

Remark 1.8. If the f-type of g is nnn, then $g(f^3(x))$ is irreducible over $\mathbb{F}_q$ by Lemma 2.5 of [15]. Since f has orbit type $(3,1)$, we obtain $H(b_1) = g(f^3(b_1)) = g(f^3(b_2)) = H(b_2)$, making the implication in Theorem 1.7 trivially true. Therefore, the interesting case is when g has f-type nns.

Remark 1.9. Theorem 1.3 and Theorem 1.7 together provide an explanation for all of the exceptional families of polynomials empirically observed in [9]. In particular, if f is as in Theorem 1.3 or Theorem 1.7, and $g \in \mathbb{F}_q[x]$ is any monic irreducible polynomial of even degree, then the f-types of irreducible factors of $g(f^2(x))$ (resp. $g(f^3(x))$) must form a smaller set than what was assumed in the original Boston–Jones model [15, Proposition 2.6]. See Section 4 (particularly Corollaries 4.1 and 4.3) for more details on this. The nature of the calculations in the proofs seems to indicate that these exceptions may result from algebraic coincidences rather than a more general pattern. In this sense, our results can also be thought of as evidence for the following conjecture, which appeared in an earlier version of [9].

Conjecture 1.10. *Let $f \in \mathbb{F}_q$ be a monic quadratic polynomial, where $\mathbb{F}_q$ is a finite field of odd characteristic. The distribution of factorizations of f converges to limiting distributions arising from the Boston–Jones model, except when f has orbit type $(3,1)$ or $(2,n)$ for some $n \geq 1$.*

The organization of the paper is as follows: In Section 2, we provide the necessary background. In Section 3, we prove a few auxiliary lemmas. In Section 4, we prove Theorem 1.3 and Theorem 1.7.

Acknowledments. The author thanks the anonymous referees for their useful comments and suggestions.

2. Background

In this section, we provide some background and recall definitions and results that we will use in the rest of the paper.

Let $f \in \mathbb{F}_q[x]$ be a monic quadratic polynomial with the unique critical point $\gamma \in \mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field of odd characteristic. The *type space* of f is the set $S_f := \{s,n\}^{o_f}$. For instance, if $f = x^2 + 1 \in \mathbb{F}_3$, we have $S_f = \{ss, sn, ns, nn\}$, as f has strict critical orbit size of 2. The polynomial f has a natural action on the type space. If t is a type, we obtain $f(t)$ by shifting each entry one position to the left, with the former

k-th entry becoming the new final entry. Here, k is the index such that $f^{o_f+1}(\gamma) = f^k(\gamma)$. Note that this action depends only on the orbit type of f.

Let $g \in \mathbb{F}_q[x]$ be any monic irreducible polynomial of even degree. Any irreducible factor $h \in \mathbb{F}_q[x]$ of $g(f(x))$ is called an *immediate descendant* of g. If the f-type of g starts with n, then $g(f(x))$ is irreducible over $\mathbb{F}_q$ (by [15, Lemma 2.5]), and g has only one immediate descendant. On the other hand, if the f-type of g starts with s, then $g(f(x))$ factors as the product of two irreducible polynomials of the same degree in $\mathbb{F}_q[x]$ (by [15, Proposition 2.6]), and g has two immediate descendants in this case.

As shown by Boston and Jones [15, Proposition 3.4], some types cannot occur as immediate descendants of polynomials with certain types. The following lemma is a variant of [15, Proposition 3.4] with our notation.

Lemma 2.1. *Let $f \in \mathbb{F}_q[x]$ be a monic quadratic with the critical point γ. Assume f has orbit type (m, n). Suppose $g \in \mathbb{F}_q$ is a monic irreducible polynomial of even degree, and that $g(f^i(x))$ is separable for every $i \geq 1$. Let $a_1 a_2 \dots a_{m+n-1}$ be the f-type of an irreducible factor of $g(f^i(x))$ for some $i \geq 0$. If $a_1 = s$, then $d_1 d_2 \dots d_{m+n-1}$ cannot occur as an immediate descendant of a polynomial with f-type $a_1 \dots a_{m+n-1}$, unless one of the following conditions holds:*

(1) $m = 0$.
(2) $m > 0$ *and* $d_{m-1} d_{m+n-1} = a_m$.

The following definition is crucial for the rest of the paper.

Definition 2.2. Let $f \in \mathbb{F}_q[x]$ be a monic quadratic, and let $g \in \mathbb{F}_q[x]$ be a monic polynomial of even degree. Let $k \geq 2$ be an integer. For each $0 \leq i \leq k-1$, let $g(f^i(x)) \in \mathbb{F}_q[x]$ have t_i irreducible factors with f-types $a_{i1}, a_{i2}, \dots, a_{it_i}$. Then we define the chain

$$a_{01}/a_{02}/\cdots/a_{0t_0} \longrightarrow a_{11}/a_{12}/\cdots/a_{1t_1} \longrightarrow \cdots \longrightarrow a_{(k-1)1}/a_{(k-1)2}/\cdots/a_{(k-1)t_{k-1}}$$

to be a $(k-1)$-*step transition*.

Boston and Jones constructed the Markov model for factorization of iterates of monic quadratic polynomials, assuming that if a type satisfies one of the conditions listed in Lemma 2.1, it will always occur as an immediate descendant. However, Boston, Xia, and the author [9] later found through Magma computations that certain 2-step and 3-step transitions never occur for some exceptional families of polynomials f, even though they satisfy one of the conditions in Lemma 2.1. Our goal in the remaining sections is to prove that these transitions never occur for the exceptional families of quadratics identified in [9].

3. Auxiliary lemmas

For any $F \in \overline{\mathbb{F}}_q[x]$, we let $V(F)$ be the vanishing set of F over $\overline{\mathbb{F}}_q$. The following lemma, along with its corollary, will play an important role in proving Theorem 1.3 and Theorem 1.7. In particular, together, they will be used to justify that certain expressions lie in $\mathbb{F}_q$, which is crucial for proving Theorem 1.3 and Theorem 1.7. The first part of the lemma is given in [15, Proposition 2.6], but we restate it here for the reader's convenience, as it will be used in the subsequent parts of the lemma.

Lemma 3.1. *Let $f \in \mathbb{F}_q[x]$ be a monic quadratic with critical point $\gamma \in \mathbb{F}_q$, and let $g \in \mathbb{F}_q[x]$ be any irreducible polynomial. Suppose that $g(f^i(x)) \in \mathbb{F}_q[x]$ is separable for all $i \geq 1$. For some $i \geq 1$, assume that $g(f^i(x)) \in \mathbb{F}_q[x]$ is irreducible, and $g(f^{i+1}(x)) \in \mathbb{F}_q[x]$ is reducible. Then the following three statements are true:*

(a) *$g(f^{i+1}(x)) = Ch(x-\gamma)h(-(x-\gamma))$, where C is the leading coefficient of $g \in \mathbb{F}_q[x]$, and $h \in \mathbb{F}_q[x]$ is a monic irreducible polynomial.*

(b) *Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ and $2\gamma - \alpha_1, 2\gamma - \alpha_2, \ldots, 2\gamma - \alpha_k \in \overline{\mathbb{F}}_q$ be the distinct roots of $g(f(x))$. For $1 \leq j \leq k$, define the sets*

$$A_j := V(h(x-\gamma)) \cap V(f^i - \alpha_j)$$

and

$$B_j := V(h(x-\gamma)) \cap V(f^i - (2\gamma - \alpha_j)).$$

Let $A_{f,g}^{(i)} := \{A_1, A_2, \ldots, A_k\}$ and $B_{f,g}^{(i)} := \{B_1, B_2, \ldots, B_k\}$. Set $C_{f,g}^{(i)} = A_{f,g}^{(i)} \cup B_{f,g}^{(i)}$. Any Galois element $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ naturally induces a map $\tau_\sigma : C_{f,g}^{(i)} \to C_{f,g}^{(i)}$, which defines a transitive group action on the set $C_{f,g}^{(i)}$.

(c) *With the notation from part (b), for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and $1 \leq j_1, j_2 \leq k$, we have $\tau_\sigma(A_{j_1}) = A_{j_2}$ if and only if $\tau_\sigma(B_{j_1}) = B_{j_2}$.*

Proof.

(a). See [15, Proposition 2.6].

(b). Note that by the definition of f, it follows that $\beta \in V(f^i - \alpha_j)$ if and only if $2\gamma - \beta \in V(f^i - \alpha_j)$ for any $1 \leq j \leq k$. By the definition of h, this forces exactly half of the elements of $V(f^i - \alpha_j)$ to lie in $V(h(x-\gamma))$, as otherwise it would contradict the separability assumption on $g(f^{i+1}(x))$. Similarly, exactly half of the elements of $V(f^i - 2\gamma + \alpha_j)$ lie in $V(h(x-\gamma))$. Hence, for $1 \leq j \leq k$, we can let $A_j := \{\beta_{j1}, \beta_{j2}, \ldots, \beta_{j\ell}\}$ and $B_j := \{\beta'_{j1}, \beta'_{j2}, \ldots, \beta'_{j\ell}\}$, where $\ell = 2^{i-1}$. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, define the map $\tau_\sigma : C_{f,g}^{(i)} \to C_{f,g}^{(i)}$ as follows: for $X, Y \in C_{f,g}^{(i)}$, if $\sigma(\theta) = \zeta$ for some $\theta \in X$ and $\zeta \in Y$, then we set $\tau_\sigma(X) = Y$. To prove that τ_σ defines a group action

on the set $C_{f,g}^{(i)}$, the only non-trivial matter to check is to show that τ_σ is well-defined, as other conditions of a group action would then immediately follow from the action of σ on the roots of $h(x-\gamma)$.

To prove that the map τ_σ is well-defined, consider a Galois element $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, any $X \in C_{f,g}^{(i)}$, and two arbitrary elements $\beta, \theta \in X$. Suppose that $\sigma(\beta) = y \in Y$ for some $Y \in C_{f,g}^{(i)}$. By definition, we have

$$f^i(\beta) = \alpha, \quad f^i(\sigma(\beta)) = \alpha'$$

for two roots α, α' of $g(f(x))$. Since f is defined over the base field $\mathbb{F}_q$, we have σ commuting with f, hence these two equalities immediately yield

$$\sigma(\alpha) = \alpha'. \tag{3.1}$$

Now let $\sigma(\theta) = z \in Z$ for some $Z \in C_{f,g}^{(i)}$. This yields

$$f^i(\theta) = \alpha, \quad f^i(\sigma(\theta)) = \alpha''$$

for a root α'' of $g(f(x))$. This similarly gives

$$\sigma(\alpha) = \alpha''. \tag{3.2}$$

Combining (3.1) and (3.2) implies $\alpha' = \alpha''$, which proves the equality $Y = Z$ by the definitions of Y and Z. Hence, the map τ_σ is well-defined. This completes the proof that τ_σ defines a group action on $C_{f,g}^{(i)}$. Finally, note that this action is transitive because the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on the roots of $h(x-\gamma)$ is transitive, completing the proof of part (b).

(c). For some $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and $\beta \in A_{j_1}, \beta' \in A_{j_2}$, let $\tau_\sigma(\beta) = \beta'$. By the proof of part (b), this is equivalent to $\sigma(\alpha_{j_1}) = \alpha_{j_2}$. Similarly, if $\tau_\sigma(\omega) = \omega'$ for some $\omega \in B_{j_1}, \omega' \in B_{j_3}$, we have $\sigma(2\gamma - \alpha_{j_1}) = 2\gamma - \alpha_{j_3}$, which is equivalent to $\sigma(\alpha_{j_1}) = \alpha_{j_3}$ since $\gamma \in \mathbb{F}_q$. This shows $j_2 = j_3$ because $f(g(x))$ is separable over $\mathbb{F}_q$, which immediately proves the implication

$$\tau_\sigma(A_{j_1}) = A_{j_2} \implies \pi_\sigma(B_{j_1}) = B_{j_2}.$$

The other direction follows very similarly, hence we are done. □

The following corollary of Lemma 3.1 will be useful for justifying that certain expressions, which arise in the proofs of Theorem 1.3 and Theorem 1.7, lie in the base field $\mathbb{F}_q$.

Corollary 3.2. *Assume the notation in Lemma 3.1. For $1 \le j \le k$, let $A_j := \{\beta_{j1}, \beta_{j2}, \dots, \beta_{j\ell}\}$ and $B_j = \{\omega_{j1}, \omega_{j2}, \dots, \omega_{j\ell}\}$, where $\ell = 2^{i-1}$. Let $S := S(x_1, x_2, \dots, x_\ell)$ be a symmetric function in ℓ variables. Define the polynomials $P_{f,S}^{(i)}$ and $Q_{f,S}^{(i)}$ by*

$$P_{f,S}^{(i)}(x) := \prod_{j=1}^{k} (x - S(\beta_{j1}, \beta_{j2}, \dots, \beta_{j\ell}) - S(\omega_{j1}, \omega_{j2}, \dots, \omega_{j\ell}))$$

and

$$Q_{f,S}^{(i)}(x) := \prod_{j=1}^{k}(x - S(\beta_{j1}, \beta_{j2}, \ldots, \beta_{j\ell}))(x - S(\omega_{j1}, \omega_{j2}, \ldots, \omega_{j\ell})).$$

Then $P_{f,S}^{(i)}$ and $Q_{f,S}^{(i)}$ are both defined over $\mathbb{F}_q$.

Proof. Since S is a symmetric function, and by part (b) of Lemma 3.1, combined with part (c) of the same lemma, it follows immediately that any Galois element $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ permutes the roots of both $P_{f,S}^{(i)}$ and $Q_{f,S}^{(i)}$. Therefore, the polynomials $P_{f,S}^{(i)}$ and $Q_{f,S}^{(i)}$ are invariant under the action of any $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. This implies that all their coefficients lie in the base field $\mathbb{F}_q$, as required. □

The following lemma provides special identities satisfied by the strict critical orbit elements of f when f has orbit type $(2, n)$ or $(3, 1)$. This lemma will play a key role in the calculations in the next section, which will ultimately lead to the proof that the corresponding expressions in Theorem 1.3 and Theorem 1.7 are squares in $\mathbb{F}_q$.

Lemma 3.3. *Let $f \in \mathbb{F}_q[x]$ be a monic quadratic polynomial with critical point $\gamma \in \mathbb{F}_q$. Write $f(x) = (x - \gamma)^2 + \gamma + c$ for some $c \in \mathbb{F}_q$. Then the following two statements are true:*

(a) *Suppose that f has orbit type $(2, n)$ for some $n \geq 1$, and let $\mathcal{O}_f^+ = \{b_1, b_2, \ldots, b_{n+1}\}$. Then,*

$$(b_n - \gamma)^2 = -2c.$$

(b) *Suppose that f has orbit type $(3, 1)$, and let $\mathcal{O}_f^+ = \{b_1, b_2, b_3\}$. Then, we have*

$$(b_1 - \gamma)^2(b_2 - \gamma)^2 = 2(b_2 - \gamma)$$

and

$$(b_1 - \gamma)^2 + (b_2 - \gamma)^2 = -2c.$$

Proof.

(a). It follows from the fact that $b_{n+1} = 2\gamma - b_1$. The details are skipped.

(b). It follows from the fact that $(b_3 - \gamma) = -(b_2 - \gamma)$. The details are skipped. □

4. Proofs of main results

We are now ready to prove Theorem 1.3 and Theorem 1.7.

Proof of Theorem 1.3. By part (a) of Lemma 3.1, we have

$$g(f^2(x)) = h(x-\gamma)h(-(x-\gamma)) \tag{4.1}$$

for some monic irreducible polynomial $h \in \mathbb{F}_q[x]$. Evaluating both sides of equation (4.1) at $x = b_n$, since f has orbit type $(2, n)$, we obtain

$$g(b_2) = h(b_n-\gamma)h(-(b_n-\gamma)).$$

Since the f-type of g starts with ns, it follows that $g(b_2)$ is a square in $\mathbb{F}_q$. Thus, we have

$$h(b_n-\gamma)(\mathbb{F}_q^\times)^2 = h(-(b_n-\gamma))(\mathbb{F}_q^\times)^2.$$

Therefore, to prove the statement, it suffices to show that $h(b_n-\gamma)$ is a square in $\mathbb{F}_q$. For simplicity, we let $c_n := b_n - \gamma$ for the remainder of the proof.

Let $\alpha_1, \alpha_2, \ldots, \alpha_k, 2\gamma-\alpha_1, 2\gamma-\alpha_2, \ldots, 2\gamma-\alpha_k \in \overline{\mathbb{F}}_q$ be the (distinct) roots of $g(f(x))$. For each $1 \le j \le k$, define

$$V(h(x-\gamma)) \cap V(f-\alpha_j) = \{\beta_{j1}\} \tag{4.2}$$

and

$$V(h(x-\gamma)) \cap V(f-2\gamma+\alpha_j) = \{\beta_{j2}\}. \tag{4.3}$$

For each $1 \le j \le k$ and $i = 1, 2$, let $\theta_{ji} := \beta_{ji} - \gamma$. Using equations (4.2) and (4.3), we immediately obtain

$$\theta_{j1}^2 + \theta_{j2}^2 = -2c. \tag{4.4}$$

It also follows that

$$h(x) = \prod_{j=1}^{k} (x-\theta_{j1})(x-\theta_{j2}). \tag{4.5}$$

Using equation (4.5), we compute

$$\begin{aligned} h(c_n) &= \prod_{j=1}^{k}(c_n-\theta_{j1})(c_n-\theta_{j2}) \\ &= \prod_{j=1}^{k}(c_n^2-c_n(\theta_{j1}+\theta_{j2})+\theta_{j1}\theta_{j2}) \\ &= \frac{1}{2^k}\prod_{j=1}^{k}\Big(2c_n^2-2c_n(\theta_{j1}+\theta_{j2})+2\theta_{j1}\theta_{j2}\Big) \\ &= \frac{1}{2^k}\prod_{j=1}^{k}\Big((c_n-\theta_{j1}-\theta_{j2})^2+c_n^2-\theta_{j1}^2-\theta_{j2}^2\Big) \\ &= \frac{1}{2^k}\left(\prod_{j=1}^{k}(c_n-\theta_{j1}-\theta_{j2})\right)^2, \end{aligned}$$

where we used the first part of Lemma 3.3 and equation (4.4) in the last equality. We now define

$$F(x) := \prod_{j=1}^{k}(x-\theta_{j1}-\theta_{j2}) = \prod_{j=1}^{k}(x-(\beta_{j1}+\beta_{j2})+\gamma).$$

By taking $i=1$ and $S=x$ for the polynomial $P_{f,S}^{(i)}$ given in Corollary 3.2, and noting that $\gamma \in \mathbb{F}_q$, it follows that the coefficients of F lie in $\mathbb{F}_q$. Since g is a polynomial of even degree, it also follows that k is even. This shows that $h(c_n) = h(b_n-\gamma)$ is a square in $\mathbb{F}_q$, as desired. □

Corollary 4.1. *Let $f \in \mathbb{F}_q[x]$ be a monic quadratic with orbit type $(2,n)$. Let g be any irreducible factor of f^i for some $i \geq 1$. Suppose that g has f-type starting with ns. Then the 2-step transitions of the form*

$$ns\ldots \longrightarrow s\ldots \longrightarrow \cdots nn/\cdots nn,$$

$$ns\ldots \longrightarrow s\ldots \longrightarrow \cdots ns/\cdots nn,$$

and

$$ns\ldots \longrightarrow s\ldots \longrightarrow \cdots ns/\cdots ns$$

never occur for g.

Proof. By [15, Proposition 2.6], any irreducible factor g of f^i has even degree. Therefore, in any 2-step transition, Theorem 1.3 implies that the penultimate entry for the f-type of any irreducible factor of $g(f^2(x))$ cannot be n, completing the proof of Corollary 4.1. □

Remark 4.2. Let g be as in Corollary 4.1. By using Lemma 2.1 and Corollary 4.1, we can immediately observe that precisely half of the 2-step transitions of g that are assumed to occur in the Boston–Jones model actually do not occur. This provides an explanation for the discrepancy between the data predicted by the Boston–Jones model and the actual factorization data for iterates of the corresponding family of quadratic polynomials.

Proof of Theorem 1.7. Using Remark 1.8, we can assume without loss of generality that g has f-type nns. By part (a) of Lemma 3.1, we have

$$g(f^3(x)) = h(x-\gamma)h(-(x-\gamma)) \tag{4.6}$$

for some monic irreducible polynomial $h \in \mathbb{F}_q[x]$.

Since f has orbit type $(3,1)$, if we evaluate both sides of (4.6) at $x = b_1$ and $x = b_2$, we obtain

$$g(b_3) = h(b_1-\gamma)h(-(b_1-\gamma)) \tag{4.7}$$

and

$$g(b_3) = h(b_2-\gamma)h(-(b_2-\gamma)). \tag{4.8}$$

Thus, (4.7) and (4.8) together yield

$$h(b_1-\gamma)h(b_2-\gamma)(\mathbb{F}_q^\times)^2 = h(-(b_1-\gamma))h(-(b_2-\gamma))(\mathbb{F}_q^\times)^2.$$

Therefore, to prove the statement, it suffices to show that the product $h(b_1-\gamma)h(b_2-\gamma)$ is a square in $\mathbb{F}_q$. For simplicity, we let $c_i := b_i - \gamma$ for $i = 1, 2$ for the remainder of the proof.

Let $\alpha_1, \alpha_2, \ldots, \alpha_k, 2\gamma-\alpha_1, 2\gamma-\alpha_2, \ldots, 2\gamma-\alpha_k \in \overline{\mathbb{F}}_q$ be the (distinct) roots of $g(f(x))$. For $1 \le j \le k$, let

$$V(h(x-\gamma)) \cap V(f^2-\alpha_j) = \{\beta_{j1}, \beta_{j2}\} \tag{4.9}$$

and

$$V(h(x-\gamma)) \cap V(f^2-2\gamma+\alpha_j) = \{\beta_{j3}, \beta_{j4}\}. \tag{4.10}$$

For $1 \le j \le k$ and $i = 1, 2, 3, 4$, let $\theta_{ji} := \beta_{ji} - \gamma$. The equations (4.9) and (4.10) immediately yield

$$\theta_{j1}^2 + \theta_{j2}^2 = \theta_{j3}^2 + \theta_{j4}^2 = -2c. \tag{4.11}$$

It also follows that we have

$$h(x) = \prod_{j=1}^{k}\left(\prod_{i=1}^{4}(x-\theta_{ji})\right). \tag{4.12}$$

Our goal is to show that the product $h(c_1)h(c_2)$ is a square in $\mathbb{F}_q$. To that end, we will now study the products $(c_i-\theta_{j1})(c_i-\theta_{j2})$ and $(c_i-\theta_{j3})(c_i-\theta_{j4})$ for $1 \le j \le k$ and $i = 1, 2$.

We have

$$\begin{aligned}(c_1-\theta_{j1})(c_1-\theta_{j2}) &= c_1^2 - c_1(\theta_{j1}+\theta_{j2}) + \theta_{j1}\theta_{j2}\\ &= \frac{1}{2}\Big(2c_1^2 - 2c_1(\theta_{j1}+\theta_{j2}) + 2\theta_{j1}\theta_{j2}\Big)\\ &= \frac{1}{2}\Big((c_1-\theta_{j1}-\theta_{j2})^2 + c_1^2 - \theta_{j1}^2 - \theta_{j2}^2\Big)\\ &= \frac{1}{2}\Big((c_1-\theta_{j1}-\theta_{j2})^2 + c_2 + c\Big), \qquad (4.13)\end{aligned}$$

where we used (4.11) in the last equality. A similar calculation yields

$$(c_2-\theta_{j1})(c_2-\theta_{j2}) = \frac{1}{2}\Big((c_2-\theta_{j1}-\theta_{j2})^2 + c_3 + c\Big). \qquad (4.14)$$

Since f has orbit type $(3,1)$, we have $c_3 = -c_2$. Using this in (4.13), we obtain

$$\begin{aligned}(c_1-\theta_{j1})(c_1-\theta_{j2}) &= \frac{1}{2}\Big((c_1-\theta_{j1}-\theta_{j2})^2 + c_2 + c\Big)\\ &= \frac{1}{2}\Big((c_1-\theta_{j1}-\theta_{j2})^2 - c_3 + c\Big)\\ &= \frac{1}{2}\Big((c_1-\theta_{j1}-\theta_{j2})^2 - c_2^2\Big)\\ &= \frac{1}{2}(c_1-c_2-\theta_{j1}-\theta_{j2})(c_1+c_2-\theta_{j1}-\theta_{j2}). \qquad (4.15)\end{aligned}$$

A similar calculation using (4.14) also yields

$$(c_2-\theta_{j1})(c_2-\theta_{j2}) = \frac{1}{2}(c_2-c_1-\theta_{j1}-\theta_{j2})(c_1+c_2-\theta_{j1}-\theta_{j2}). \qquad (4.16)$$

Because of (4.11), it is clear that the same calculations hold for the products $(c_1-\theta_{j3})(c_1-\theta_{j4})$ and $(c_2-\theta_{j3})(c_2-\theta_{j4})$. Hence, we also have the identities

$$(c_1-\theta_{j3})(c_1-\theta_{j4}) = \frac{1}{2}(c_1-c_2-\theta_{j3}-\theta_{j4})(c_1+c_2-\theta_{j3}-\theta_{j4}) \qquad (4.17)$$

and

$$(c_2-\theta_{j3})(c_2-\theta_{j4}) = \frac{1}{2}(c_2-c_1-\theta_{j3}-\theta_{j4})(c_1+c_2-\theta_{j3}-\theta_{j4}). \qquad (4.18)$$

Let

$$F(x) := \prod_{j=1}^{k}(x-\theta_{j1}-\theta_{j2})(x-\theta_{j3}-\theta_{j4}).$$

Using (4.15), (4.16), (4.17), and (4.18) in (4.12), we obtain

$$h(c_1)h(c_2) = \frac{1}{2^{4k}}F(c_1-c_2)F(c_2-c_1)(F(c_1+c_2))^2.$$

Let

$$G(x) := \prod_{j=1}^{k}(x-\theta_{j1}-\theta_{j2}) = \prod_{j=1}^{k}(x-\beta_{j1}-\beta_{j2}+2\gamma)$$

and

$$H(x) := \prod_{j=1}^{k}(x-\theta_{j3}-\theta_{j4}) = \prod_{j=1}^{k}(x-\beta_{j3}-\beta_{j4}+2\gamma).$$

By taking $i=2, S=x+y$ for the polynomial $Q_{f,S}^{(i)}$ given in Corollary 3.2, and noting that $\gamma \in \mathbb{F}_q$, it follows that $F(x)=G(x)H(x)$ has coefficients in $\mathbb{F}_q$. Hence, to finish the proof, it suffices to show that $F(c_1-c_2)F(c_2-c_1)$ is a square in $\mathbb{F}_q$. To that end, we will now do some calculations related to this product.

We have

$$\begin{aligned}(c_1-c_2-\theta_{j1}-\theta_{j2})(c_2-c_1-\theta_{j1}-\theta_{j2}) &= (\theta_{j1}+\theta_{j2})^2-(c_1-c_2)^2\\ &= 2(c_1c_2+\theta_{j1}\theta_{j2}),\end{aligned} \tag{4.19}$$

where we used the second part of Lemma 3.3 and (4.11) in the last equality. Similarly, we also obtain

$$(c_1-c_2-\theta_{j3}-\theta_{j4})(c_2-c_1-\theta_{j3}-\theta_{j4}) = 2(c_1c_2+\theta_{j3}\theta_{j4}). \tag{4.20}$$

Setting $A=F(c_1-c_2)F(c_2-c_1)$, and using (4.19) and (4.20), we get

$$\begin{aligned}A &= 2^{2k}\prod_{j=1}^{k}(c_1c_2+\theta_{j1}\theta_{j2})(c_1c_2+\theta_{j3}\theta_{j4})\\ &= 2^{2k}\prod_{j=1}^{k}\Big((c_1c_2)^2+c_1c_2(\theta_{j1}\theta_{j2}+\theta_{j3}\theta_{j4})+\theta_{j1}\theta_{j2}\theta_{j3}\theta_{j4}\Big)\\ &= 2^{k}\prod_{j=1}^{k}\Big(2(c_1c_2)^2+2c_1c_2(\theta_{j1}\theta_{j2}+\theta_{j3}\theta_{j4})+2\theta_{j1}\theta_{j2}\theta_{j3}\theta_{j4}\Big)\\ &= 2^{k}\prod_{j=1}^{k}\Big((c_1c_2+\theta_{j1}\theta_{j2}+\theta_{j3}\theta_{j4})^2+(c_1c_2)^2-(\theta_{j1}\theta_{j2})^2-(\theta_{j3}\theta_{j4})^2\Big).\end{aligned} \tag{4.21}$$

By definition, $\pm\theta_{j1}, \pm\theta_{j2}$ are the roots of the quartic equation

$$t^4+2ct^2+b_2-\alpha_j = 0,$$

hence $(\theta_{j1}\theta_{j2})^2 = b_2 - \alpha_j$. Similarly, we also obtain $(\theta_{j3}\theta_{j4})^2 = b_2 + \alpha_j - 2\gamma$. If we use these two equalities in (4.21), it gives

$$\begin{aligned} A &= 2^k \prod_{j=1}^{k} \Big((c_1c_2 + \theta_{j1}\theta_{j2} + \theta_{j3}\theta_{j4})^2 + (c_1c_2)^2 - 2c_2 \Big) \\ &= 2^k \left(\prod_{j=1}^{k} (c_1c_2 + \theta_{j1}\theta_{j2} + \theta_{j3}\theta_{j4}) \right)^2, \end{aligned} \tag{4.22}$$

where we used the second part of Lemma 3.3 in the last equality.

If we now set

$$T(x) = \prod_{j=1}^{k} (x + \theta_{j1}\theta_{j2} + \theta_{j3}\theta_{j4}),$$

we obtain

$$A = 2^k (T(c_1c_2))^2.$$

Taking $i = 2, S_1 = -x_1x_2, S_2 = -y_1y_2$ in Corollary 3.2, and recalling again that $\gamma \in \mathbb{F}_q$, it immediately follows that T has its coefficients in $\mathbb{F}_q$. Recalling that k is even (since g has even degree), it now follows that $A = F(c_1 - c_2)(c_2 - c_1)$ is a square in $\mathbb{F}_q$, completing the proof of Theorem 1.7. □

Corollary 4.3. *Let $f \in \mathbb{F}_q[x]$ be a monic irreducible quadratic with orbit type $(3, 1)$. Let g be any irreducible factor of f^i for some $i \geq 1$. Then the 3-step transitions of the form*

$$nns \longrightarrow nss \longrightarrow sss \longrightarrow nss/nss$$

and

$$nns \longrightarrow nss \longrightarrow sss \longrightarrow snn/snn$$

never occur for g.

Proof. By [15, Proposition 2.6], any irreducible factor g of f^i has even degree. Considering the missing 3-step transitions that we want to prove, we can assume without loss of generality that $g(f^2(x))$ is irreducible, and $g(f^3(x))$ is reducible over $\mathbb{F}_q$. By the action of f on the type space, it follows that any such g must have f-type nns. Let $\mathcal{O}_f^+ = \{b_1, b_2, b_3\}$. Theorem 1.7 implies that for any irreducible factor H of $g(f^3(x))$, the type of H at b_1 and b_2 are equal to each other, which shows that the 3-step transitions given above can never occur, as desired. □

Remark 4.4. Let g be as in Corollary 4.3. Similar to the previous case, Lemma 2.1 and Corollary 4.3 together imply that exactly half of the 3-step transitions of g that are assumed to occur in the Boston–Jones model do not actually occur. This explains why the factorization data predicted by the Boston–Jones model does not match the actual factorization data for iterates of the corresponding family of quadratic polynomials.

References

[1] F. Ahmad, R. Benedetto, J. Cain, G. Carroll & L. Fang, "The arithmetic basilica: a quadratic PCF arboreal Galois group", *J. Number Theory* **238** (2022), p. 842-868.

[2] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman & T. J. Tucker, "Current trends and open problems in arithmetic dynamics", *Bull. Am. Math. Soc.* **56** (2019), no. 4, p. 611-685.

[3] A. Bridy, J. R. Doyle, D. Ghioca, L.-C. Hsia & T. J. Tucker, "A question for iterated Galois groups in arithmetic dynamics", *Can. Math. Bull.* **64** (2021), no. 2, p. 401-417.

[4] A. Bridy & T. J. Tucker, "Finite index theorems for iterated Galois groups of cubic polynomials", *Math. Ann.* **373** (2019), no. 1-2, p. 37-72.

[5] A. Ferraguti & G. Micheli, "An equivariant isomorphism theorem for mod p reductions of arboreal Galois representations", *Trans. Am. Math. Soc.* **373** (2020), no. 12, p. 8525-8542.

[6] A. Ferraguti, G. Micheli & R. Schnyder, "On sets of irreducible polynomials closed by composition", in *Arithmetic of finite fields. 6th international workshop, WAIFI 2016*, Lecture Notes in Computer Science, vol. 10064, Springer, 2016, p. 77-83.

[7] ———, "Irreducible compositions of degree two polynomials over finite fields have regular structure", *Q. J. Math.* **69** (2018), no. 3, p. 1089-1099.

[8] A. Ferraguti & C. Pagano, "Constraining Images of Quadratic Arboreal Representations", *Int. Math. Res. Not.* **2020** (2020), no. 22, p. 8486-8510.

[9] V. Goksel, S. Xia & N. Boston, "A refined conjecture for factorizations of iterates of quadratic polynomials over finite fields", *Exp. Math.* **24** (2015), no. 3, p. 304-311.

[10] D. Gomez & A. P. Nicolás, "An estimate on the number of stable quadratic polynomials", *Finite Fields Appl.* **16** (2010), no. 6, p. 401-405.

[11] D. Gómez-Pérez, A. Ostafe & I. E. Shparlinski, "On irreducible divisors of iterated polynomials", *Rev. Mat. Iberoam.* **30** (2014), no. 4, p. 1123-1134.

[12] D. R. Heath-Brown & G. Micheli, "Irreducible polynomials over finite fields produced by composition of quadratics", *Rev. Mat. Iberoam.* **35** (2019), no. 3, p. 847-855.

[13] R. Jones, "An iterative construction of irreducible polynomials reducible modulo every prime", *J. Algebra* **369** (2012), p. 114-128.

[14] ———, "Galois representations from pre-image trees: an arboreal survey", in *Actes de la conférence « Théorie des nombres et applications », CIRM, Luminy, 16-20 janvier 2012*, Publications Mathématiques de Besançon. Algèbre et Théorie des Nombres, 2013, p. 107-136.

[15] R. Jones & N. Boston, "Settled polynomials over finite fields", *Proc. Am. Math. Soc.* **140** (2012), no. 6, p. 1849-1863.

[16] ———, "Errata to "Settled polynomials over finite fields", *Proc. Am. Math. Soc.* **148** (2020), no. 2, p. 913-914.

[17] A. Ostafe & I. E. Shparlinski, "On the length of critical orbits of stable quadratic polynomials", *Proc. Am. Math. Soc.* **138** (2010), no. 8, p. 2653-2656.

[18] L. Reis, "On the factorization of iterated polynomials", *Rev. Mat. Iberoam.* **36** (2020), no. 7, p. 1957-1978.

Vefa Goksel
Towson University
Towson, MD 21252, USA
E-mail: vgoksel@towson.edu
URL: https://sites.google.com/view/goksel/home