SETTLED POLYNOMIALS OVER FINITE FIELDS

RAFE JONES AND NIGEL BOSTON

Abstract. We study the factorization into irreducibles of iterates of a quadratic polynomial f over a finite field. We call f settled when the factorization of its nth iterate for large n is dominated by "stable" polynomials, namely those that are irreducible under post-composition by any iterate of f. We prove that stable polynomials may be detected by their action on the critical orbit of f, and that the the critical orbit also gives information about the splitting of non-stable polynomials under post-composition by iterates of f. We then define a Markov process based on the critical orbit of f and conjecture that its limiting distribution describes the full factorization of large iterates of f. This conjecture implies that almost all quadratic f defined over a finite field are settled. We give several types of evidence for our conjecture.

Let $\mathbb{F}_q$ be the finite field with q elements, and consider a polynomial $f \in \mathbb{F}_q[x]$ of degree d. In this paper we consider the iterates of f, namely the polynomials

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

Our particular interest is in understanding the factorization of these polynomials into irreducibles. We give some general results on these factorizations, and explore connections to number theory. While in general f^n has many irreducible factors, we call f *settled* if, loosely, the number of factors remains small as n grows; see Section 1 for a precise definition. A complete understanding of the factorizations, and indeed merely of settledness, appears difficult to obtain even in the case $d = 2$. However, we develop a conjectural theory in this case and give computational evidence for it. Previous work on the irreducibility of polynomial iterates (also called *stability*; see Section 2) has focused principally on the case of polynomials with coefficients in number fields. See for instance [1], [2], [3], [6], [7], [9], and [10]. Settledness was mentioned briefly in Sections 3 and 5 of [4]. The current paper is a thorough study of the phenomenon.

The organization of the paper is as follows. In Section 1 we discuss the connections to number theory, which were our original motivation. In Section 2 we give results on the factorizations of f^n in the case where f has degree 2, in particular connecting them to the presence of squares in the forward orbit of the critical point of f. Results from this section play a role in recent work of Ostafe and Shparlinski [11]. In Section 3 we develop a conjectural theory of factorizations of f^n, where irreducible factors behave in accordance with a certain Markov process, implying that essentially all quadratic polynomials are settled. Section 4 gives examples and

Date: February 2, 2011.

1991 *Mathematics Subject Classification.* 11C20, 37P25, 11R32.

The first author was partially supported by NSF DMS-0852826.

The second author was partially supported by NSA H98230-09-1-0116.

evidence for this conjecture, whilst Section 5 shows that the Markov process does not directly yield the Galois groups of the iterates.

1. Motivation and background

We motivate our work with some background on arboreal Galois representations. Say f is a polynomial with coefficients in a number field K. If $\alpha \in \overline{K}$ is a root of its nth iterate, f^n, then $f(\alpha)$ is a root of f^{n-1}. It follows that the set of roots of all iterates of f form a tree where edges are assigned between elements if f maps one to the other. We denote this tree T. For general f, T is the complete $\deg(f)$-ary rooted tree. In this case, since elements of $\mathrm{Gal}\,(\overline{K}/K)$ commute with f, we obtain a continuous map $\tau : \mathrm{Gal}\,(\overline{K}/K) \to \mathrm{Aut}(T)$ that we call an *arboreal Galois representation*. See [4] for further discussion. In order to define L-functions as in the case of linear Galois representations, one requires a conjugacy invariant quantity that encodes essential information about the images of the Frobenius elements $\mathrm{Frob}_{\mathfrak{p}}$.

The image of τ may be alternately described as the inverse limit of the groups $\mathrm{Gal}\,(K_n/K)$, where K_n is the splitting field over K of f^n. We may thus describe $\tau(\mathrm{Frob}_{\mathfrak{p}})$ by describing its images in $\mathrm{Gal}\,(K_n/K)$ as n grows. Let $g \in K[x]$ be any monic irreducible polynomial, and for a prime $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of K we recall that the residue field $\mathcal{O}_K/\mathfrak{p} := F_{\mathfrak{p}}$ is a finite field. By reducing the coefficients of g modulo $\mathfrak{p}$, one obtains a polynomial $\overline{g} \in F_{\mathfrak{p}}[x]$. It is well-known that the cycle structure of the action of $\mathrm{Frob}_{\mathfrak{p}}$ on the roots of g is given by the degrees of the irreducible factors of the polynomial $\overline{g} \in \mathbb{F}_p[x]$. Hence understanding the factorization of iterates of $f \in \mathbb{F}_q[x]$ yields information on $\tau(\mathrm{Frob}_{\mathfrak{p}})$ in $\mathrm{Gal}\,(K_n/K)$ for all n.

2. Settledness

Definition 2.1. Let K be a field and $f, g \in K[x]$. We say g is *f-stable* if $g \circ f^n$ is irreducible over K for $n = 0, 1, 2, \ldots$. We say f is *stable* if f is f-stable, i.e., all iterates of f are irreducible. We say f is *eventually stable* if some iterate of f is the product of f-stable polynomials. Finally, for fixed n, let $g_1, \ldots, g_r$ be the f-stable polynomials dividing f^n (repeated according to their multiplicity as factors of f^n), and denote by s_n the sum of their degrees. We call f *settled* if $\lim_{n\to\infty} s_n/\deg f^n = 1$.

The stability and settledness of polynomials in general has not been much studied. There are some results in special cases, such as f quadratic ([1], [2], [3], [10], [9]) and $f(x) = x^m - b$ [6]. In [9] the first author conjectures that all quadratic $f \in \mathbb{Z}[x]$ with 0 not periodic are eventually stable (considered as polynomials over $\mathbb{Q}$). Our main purpose here is to investigate settledness for polynomials over finite fields. In particular, we give evidence for the following conjecture:

Conjecture 2.2. *Let q be an odd prime power and let $f \in \mathbb{F}_q[x]$ be quadratic with $f \neq x^2$. Then f is settled.*

In this section we give some results on settledness extending those in [4] and [9]. A consequence of Conjecture 2.2 is that to each quadratic $f \in \mathbb{Z}[x]$ and odd prime q we can associate a particular (possibly infinite) partition of unity as follows. If $g_1, \ldots g_r$ are the (not necessarily distinct) stable divisors of f^n, arranged in non-increasing order by degree, then write $(\deg g_1)/2^n + \cdots + (\deg g_r)/2^n$. Taking the

limit as $n \to \infty$ yields a partition of unity by settledness. This partition encodes information about the Frobenius conjugacy class at q in the Galois group of $\bigcup K_n$ over $\mathbb{Q}$, and may be viewed as an analogue of the trace of Frobenius in the case of linear Galois representations. See [4] for more details.

Note that if g is f-stable, then in particular g is irreducible. The basis for many of our results on stability and settledness is a simple criterion for f-stability in characteristic not equal to two, which becomes a characterization of f-stability in the case that K is a finite field of odd characteristic. To state this criterion, we need some terminology: the *critical orbit* of a quadratic $f \in K[x]$ is the set $\{f^i(\gamma) : i = 2, 3, \ldots\}$, where γ is the critical point of f, while the *adjusted critical orbit* of f is $\{-f(\gamma)\} \cup \{f^i(\gamma) : i = 2, 3, \ldots\}$.

Proposition 2.3. *Let K have characteristic not equal to two. A quadratic polynomial $f \in K[x]$ is stable if its adjusted critical orbit contains no squares. In the case where K is a finite field, f is stable if and only if its adjusted critical orbit contains no squares.*

To prove Proposition 2.3 we need two preliminary results. The first is a well-known lemma:

Lemma 2.4 (Capelli's Lemma)**.** *Let K be a field, $f(x), g(x) \in K[x]$, and let $\beta \in \overline{K}$ be any root of $g(x)$. Then $g(f(x))$ is irreducible over K if and only if both g is irreducible over K and $f(x) - \beta$ is irreducible over $K(\beta)$.*

Our second preliminary result is similar to one appearing in [2], but we give here a slightly different statement and a more direct proof.

Lemma 2.5. *Let K be a field of odd characteristic, $f(x) = ax^2 + bx + c \in K[x]$, and $\gamma = -b/2a$ be the unique critical point of f. Suppose that $g \in K[x]$ is such that $g \circ f^{n-1}$ has degree d and is irreducible over K for some $n \geq 1$. Then $g \circ f^n$ is irreducible over K if $(-a)^d g(f^n(\gamma))$ is not a square in K. If K is finite then we may replace "if" with "if and only if."*

Proof. (cf [8, Lemma 4.13]) By Capelli's Lemma and the irreducibility of $g \circ f^{n-1}$, we have $g \circ f^n$ irreducible if for any root β of $g \circ f^{n-1}$, $\mathrm{Disc}\,(f(x) - \beta) = b^2 - 4ac + 4a\beta$ is not a square in $K(\beta)$. Now

$$\begin{aligned} N_{K(\beta)/K}(b^2 - 4ac + 4a\beta) &= (-4a)^d \prod_{\beta \text{ root of } g \circ f^{n-1}} \left(-\frac{b^2}{4a} + c - \beta \right) \\ &= (-4a)^d g \circ f^{n-1}(-b^2/4a + c) = (-4a)^d g \circ f^{n-1}(f(\gamma)). \end{aligned}$$

This proves the Lemma in the case of a general field K. Note that $N_{K(\beta)/K}$ is a multiplicative homomorphism, thus mapping squares to squares. If $K = \mathbb{F}_q$ then since $1/2$ of the elements of $\mathbb{F}_q(\beta)^*$ are squares, it follows that $\alpha \in \mathbb{F}_q(\beta)$ is a square if and only if $N_{\mathbb{F}_q(\beta)/\mathbb{F}_q}(\alpha)$ is a square in $\mathbb{F}_q$. □

Note that Proposition 2.3 follows by taking $g(x) = x$ in Lemma 2.5. The following is a new result that will help in the analysis of several examples in Section 3

Proposition 2.6. *Let $f(x) = ax^2 + bx + c \in K[x]$ and let $\gamma = -b/2a$ be the unique finite critical point of f. Suppose that $g \in K[x]$ is such that $g \circ f^{n-1}$ is irreducible*

over K for some $n \geq 1$. Then either $g \circ f^n$ is irreducible or there exists a monic $h \in K[x]$ such that

$$g \circ f^n(x) = kh(x-\gamma)h(-(x-\gamma))$$

for some $k \in K$.

Proof. Suppose that $g \circ f^n$ is reducible, and let $\deg g \circ f^n = d$. Consider the action of $G_n := \mathrm{Gal}\,(K(g \circ f^n)/K)$ on the roots of $g \circ f^n$, where $K(g \circ f^n)$ denotes the splitting field of $g \circ f^n$ over K. Since $g \circ f^n$ is reducible, this action has at least two orbits. However, since $g \circ f^{n-1}$ is irreducible, each orbit has at least $\deg g \circ f^{n-1} = d/2$ elements. Thus there are precisely two orbits.

By Capelli's Lemma, $f(x) - \beta$ is reducible over $K(\beta)$ for every root β of $g \circ f^{n-1}$. Note that

$$f(x) - \beta = ax^2 - bx + c - \beta = a((x-\gamma)^2 - (b^2 - 4ac - 4a\beta)/4a^2).$$

Let $\pm\alpha_\beta$ be the square roots of $(b^2 - 4ac - 4a\beta)/4a^2$, and choose the signs so that $\{\alpha_\beta : \beta \text{ a root of } g \circ f^{n-1}\}$ is one Galois orbit and $\{-\alpha_\beta : \beta \text{ a root of } g \circ f^{n-1}\}$ is the other. We then have

$$g \circ f^n = a^d \prod_\beta \left((x-\gamma) - \alpha_\beta\right) \prod_\beta \left((x-\gamma) + \alpha_\beta\right).$$

Since $n \geq 2$, the degree of $g \circ f^{n-1}$ is even. Thus the second product may be rewritten as $\prod_\beta(-(x-\gamma) - \alpha_\beta)$. Taking $h(x) = \prod_\beta(x - \alpha_\beta) \in K[x]$ completes the proof. □

3. A Markov model for factorizations of iterates

In this section we specialize to the case $K = \mathbb{F}_q$, still taking q to be an odd prime power and f to be quadratic. We develop a conjectural model for the factorization of f^n into irreducibles as n grows.

For $f \in \mathbb{F}_q[x]$, define c_f to be the number of distinct elements of the critical orbit of f, i.e., one less than the smallest integer k such that $f^k(\gamma) = f^j(\gamma)$ with $k > j \geq 1$. It follows from Proposition 2.5 that the factorization of iterates of f is determined by the presence of squares in the finite sequence consisting of the first $c_f + 1$ terms of the adjusted critical orbit, i.e., $-f(\gamma), f^2(\gamma), \ldots, f^{c_f+1}(\gamma)$. Indeed, if the first element of this sequence that is a square is the ith one, then f^i is the first reducible iterate of f. More generally, if $h \in \mathbb{F}_q[x]$ is irreducible, then by Proposition 2.5 we have that when $\deg h$ is odd, then h is f-stable if and only if the sequence $-h(f(\gamma)), h(f^2(\gamma)), \ldots, h(f^{c_f+1}(\gamma))$ contains no squares. When $\deg h$ is even, as is the case when $h = f^i$ for some $i \geq 1$, we need only consider the sequence $h(f(\gamma)), h(f^2(\gamma)), \ldots, h(f^{(c_f}\gamma))$. Moreover, in either case if the first element of the appropriate sequence that is a square is the ith one, then $h \circ f^i$ is reducible and $h \circ f^j$ is irreducible for $j < i$.

Example 3.1. Let $f = x^2+1$ and $K = \mathbb{F}_q$. When $q = 3$, we have $f(\gamma) = 1, f^2(\gamma) = 2$, and $f^3(\gamma) = 2$. Here $c_f = 2$, and the sequence $-f(\gamma), f^2(\gamma), f^3(\gamma), f^4(\gamma)$ is just $2, 2, 2, 2$. This contains no squares, and thus f is stable. When $q = 7$, the critical orbit is $1 \to 2 \to 5 \to 5 \to \cdots$. The relevant sequence is $6, 2, 5, 5$. Since the second element is a square, we conclude that f is irreducible but f^2 factors. Note also that $h = x^2 + x + 4$ divides f^3, and since $\deg h$ is even and $h(f(\gamma)), h(f^2(\gamma)), h(f^3(\gamma)) = 6, 3, 6$ contains no squares, we conclude that h is f-stable.

Let $f \in \mathbb{F}_q[x]$ be quadratic, and suppose that all iterates of f are separable over $\mathbb{F}_q$ (equivalently, 0 is not in the forward orbit of the critical point of f). Consider the tree V defined as follows. The vertices consist of all irreducible $h \in \mathbb{F}_q[x]$ such that $h \mid f^n$ for some $n \geq 0$, where we take $f^0 = x$. There is an edge connecting h_1 and h_2 precisely if h_2 divides $h_1 \circ f$. We call the factor(s) of $h \circ f$ the *immediate descendant(s)* of h (there may be one or two). Denote by V_n the vertices of distance n from f_0, so that $V_n = \{h \in \mathbb{F}_q[x] : h \text{ irreducible and } h \mid f^n\}$. The graph furnishes a natural map $V_{n+1} \to V_n$, and we take $L = \varprojlim V_n$ to be the inverse limit of this directed system. We refer to the elements of L as *ends* of the tree V. If we assign the discrete topology to each V_n, then L becomes a profinite topological space. Moreover, we assign a probability measure to each V_n by taking $\mu_n(h) = 2^{-n} \deg h$. These measures are compatible with the maps $V_{n+1} \to V_n$, and it follows that we have a measure μ on L that restricts to μ_n for each n. We thus have a probability space L, μ, B, where B denotes the Borel σ-algebra on L.

We now wish to label almost all vertices of the aforementioned graph with a *type*, which is a string of letters taken from the alphabet $\{n, s\}$. Let $g \in \mathbb{F}_q[x]$ be irreducible of even degree. Recall that the critical orbit of f has c_f elements. The type of g is a string of length c_f consisting of the letters n and s according to whether each element of the set $\{h(f(\gamma)), h(f^2(\gamma)), \ldots, h(f^{c_f}(\gamma))\}$ is a non-square or a square. We sometimes wish to multiply types, which we do by identifying n with -1 and s with 1. Clearly the type of an even-degree irreducible factor h of f^n encodes certain splitting information about the portion of the graph V emanating from h. In the case where $\deg h$ is odd, or equivalently $\deg h = 1$, we must assign a string of length $c_f + 1$ to encode the same information. For simplicity we leave these vertices unlabeled. Note that an end of V whose projections in V_n have degree 1 for every n yields a sequence $\alpha_1, \alpha_2, \ldots$ of elements of $\mathbb{F}_q$ with $f(\alpha_n) = \alpha_{n-1}$ for $n \geq 2$ and $f(\alpha_1) = 0$. Thus $\alpha_n = \alpha_m$ for some $n \geq m$, implying that $0 = f^m(\alpha_n) = \alpha_{n-m}$. Therefore 0 is periodic under iteration of f, whence $\alpha_n = 0$ for infinitely many n, i.e., the polynomial x occurs for infinitely many projections (powers of x cannot occur since all iterates of f are separable). It follows that there can be at most one such end. Thus for any end belonging to a cofinite subset of L, only a finite number of the associated vertices are unlabeled.

We denote by π_n the natural restrictions $L \to V_n$. Consider random variables $X_n : L \to \{n, s\}^{c_f}$ defined by $X_n(l) = \phi(\pi_n(l))$. Thus X_n simply returns the labeling of the nth vertex associated to the end l. By the remarks in the second paragraph of this section, we have that the stochastic process $X_1, X_2, \ldots$ completely determines the factorizations of the iterates of f. Moreover, we have the following characterization: f is settled if and only if

$$\lim_{n \to \infty} \mu(X_n = (n \cdots n)) = 1. \tag{3.1}$$

We call the process $X_1, X_2, \ldots$ the *factorization process* of f.

In the factorization process, some types cannot occur as immediate descendants of certain other types, because of Proposition 2.6. The next proposition gives the precise constraints.

Proposition 3.2. *Suppose that $\mathbb{F}_q$ is a finite field of odd characteristic, and $f \in \mathbb{F}_q[x]$ is quadratic with critical orbit of length m and all iterates separable. Let $g \in \mathbb{F}_q[x]$ be irreducible of even degree. Suppose that $h_1 h_2$ is a non-trivial factorization of $g \circ f$, and let d_i (resp. e_i) be the ith digit of the type of h_1 (resp. h_2). Then*

there is some k, $1 \leq k \leq m$, with $d_m = e_k$ and $e_m = d_k$. Moreover, $k = m$ if and only if γ is periodic.

Remark 3.3. When γ is not periodic, the value of k is the length of the *tail* of the orbit of γ under f. In other words, k is the smallest positive integer with $f^k(\gamma) \neq f^i(\gamma)$ for all i, but $f^{k+1}(\gamma) = f^i(\gamma)$ for some i.

Proof. By Proposition 2.6, there is $h \in \mathbb{F}_q[x]$ with $h_1 = h(x-\gamma)$ and $h_2 = h(-x+\gamma)$. A straightforward calculation shows that $h_1(-x+2\gamma) = h_2(x)$ and $h_1(x) = h_2(-x+2\gamma)$. Hence a relation among elements of the form $h_1(f^i(\gamma))$ and those of the form $h_2(f^j(\gamma))$ occurs when

$$f^i(\gamma) = -f^j(\gamma) + 2\gamma \tag{3.2}$$

for some i, j. If $f^i(\gamma) = f^j(\gamma)$ then $2f^i(\gamma) = 2\gamma$, and γ is periodic, with m being the smallest positive integer satisfying $f^m(\gamma) = \gamma$. Then $h_1(\gamma) = h(0) = h_2(\gamma)$ implies that $d_m = e_m$. If $f^i(\gamma) \neq f^j(\gamma)$, then writing $f(x) = (x-\gamma)^2 + \delta$ and applying it to both sides of (3.2) shows that $f^{i+1}(\gamma) = f^{j+1}(\gamma)$. Thus γ is not periodic under f, and $k = \min\{i, j\}$ is the smallest positive integer such that $f^k(\gamma)$ is not periodic. Note that $k \leq m-1$ in this case. □

Consider now a time-homogeneous Markov process $Y_1, Y_2, \ldots$ related to f, which we call the *f-Markov process* and define as follows. The state space is the type space of f, namely $\{n, s\}^{c_f}$. We define the f-Markov process by giving its transition matrix $M = (\mathcal{P}(Y_n = t_j | Y_{n-1} = t_i))$, where t_i and t_j vary over all types, and this completely determines the process. Note that the columns of M must sum to 1 (we remark that many authors take the transition matrix to be the transpose of M). We define M by assuming that all *allowable types* of immediate descendants have equal probability. To define allowable types, note that f naturally acts on its critical orbit, and thus also on the set of types. Indeed, if t is a type, then $f(t)$ is obtained by shifting each entry one position to the left and using the former nth entry as the new final entry, where n is such that $f^{c_f+1}(\gamma) = f^n(\gamma)$. If $g \in V$ has type t and t begins with n, then there is only one immediate descendant of g, and it will have type $f(t)$. This is the only allowable type in this case. If t begins with s, then g has two descendants whose types must multiply to $f(t)$. Among pairs of types t_1, t_2 with $t_1 t_2 = f(t)$, we call allowable those that satisfy the conclusion of Proposition 3.2, namely $d_k = e_m$ and $e_k = d_m$ with $k = m$ if γ is periodic, and k the length of the tail of the orbit of γ if γ is not periodic. See Examples 4.1 and 4.2 for examples of f-Markov processes. The following proposition gives a characterization of allowable types.

Proposition 3.4. *Let $f \in \mathbb{F}_q[x]$ be quadratic with critical point γ, critical orbit of length m, and all iterates separable. Let k be the length of the tail of the orbit of γ under f, with $k = m$ if γ is periodic, and let $a_1 \cdots a_m$ be a type with $a_1 = s$. Then the type $d_1 \cdots d_m$ is an allowable type of immediate descendant of $a_1 \cdots a_m$ if and only if $k = m$ or $k < m$ and $d_k d_m = a_{k+1}$.*

Proof. Let $g \in \mathbb{F}_q[x]$ be irreducible with even degree and type $a_1 \cdots a_m$, where $a_1 = s$. Then $g \circ f = h_1 h_2$, and the types $d_1 \cdots d_m, e_1 \cdots e_m$ of h_1, h_2 must multiply to $f(a_1 \cdots a_m)$, which is $a_2 \cdots a_m a_1$ if $k = m$ and $a_2 \cdots a_m a_{k+1}$ if $k < m$. In particular we have $d_m e_m = a_1$ if $k = m$ and $d_k e_k = d_m e_m = a_{k+1}$ if $k < m$.

If $k = m$, then by Proposition 3.2 we must have $d_m = e_m$. But this is equivalent to $d_m e_m = s$, which is already assured since $d_m e_m = a_1 = s$. Therefore $d_1 \cdots d_m$ is

allowable. Suppose that $k < m$. If $d_1 \cdots d_m$ is allowable, then by Proposition 3.2 we have $e_k = d_m$. From $d_k e_k = a_{k+1}$ we thus have $d_k d_m = a_{k+1}$. If $d_k d_m = a_{k+1}$, then we have $d_k e_k = d_k d_m$ and $d_k d_m = d_m e_m$, implying that $d_1 \cdots d_m$ is allowable. □

From the definition of allowable types, we see that the type $n \cdots n$ is fixed under the action of f and has only one descendant and hence is an *absorbing state* of the f-Markov process (that is, $\mathcal{P}(Y_n = n \cdots n \,|\, Y_{n-1} = n \cdots n) = 1$). We wish to show that the f-Markov process is in fact an *irreducible absorbing Markov process*, namely that every non-absorbing state transitions to every other state with non-zero probability after a finite number of steps.

Corollary 3.5. *Let $f \in \mathbb{F}_q[x]$ be quadratic with all iterates separable. Then the f-Markov process is an irreducible absorbing Markov process.*

Proof. Let γ be the critical point of f, and m the length of the critical orbit. Suppose that $a_1 \cdots a_m$ is a type with $a_1 = s$. We show that every type is an allowable descendant of an allowable descendant of $a_1 \cdots a_m$. This is enough to establish the corollary since each non-absorbing type with first entry n transitions to a type with first entry s with probability one after a finite number of steps.

Let k be the length of the tail of the critical orbit of f, with $k = m$ if the critical point is periodic. If $k = m$, the corollary follows immediately from Proposition 3.4. If $k < m$, then $a_1 \cdots a_m$ has at least one descendant $d_1 \cdots d_m$ with $d_{k+1} = n$ and at least one with $d_{k+1} = s$. The corollary now follows from Proposition 3.4. □

Absorbing Markov processes are well-studied, and we recall some of their properties; see [12, page 236] for details. Most saliently, any initial state lands on an absorbing state after finitely steps with probability 1. Hence for the f-Markov process $Y_1, Y_2, \ldots$,

$$\lim_{i \to \infty} \mathcal{P}(Y_i = n \cdots n) = 1. \tag{3.3}$$

In the case where the process is irreducible, the probability of being in a non-absorbing state decreases by a factor of λ each time, where λ is the largest eigenvalue of M less than 1. Moreover, if we denote by M^* the sub-matrix of M obtained by deleting the rows and columns corresponding to absorbing states, then M^* has λ as an eigenvalue of multiplicity one and the entries of any non-trivial corresponding right eigenvector give the asymptotic relative frequencies of each non-absorbing state, known as the *quasi-stationary distribution*. See examples 4.1 and 4.2.

We will give evidence that, when n is large, the factorization process of f behaves quite similarly to the f-Markov process. One such similarity is that for quadratic $f \in \mathbb{F}_q[x]$ with all iterates separable, the only absorbing state of the factorization process is $n \cdots n$ (see the second paragraph of this section). We make the following far more expansive conjecture. The first part immediately implies Conjecture 2.2 in the case where all iterates of f are separable, by equations (3.1) and (3.3).

Conjecture 3.6. *Let $f \in \mathbb{F}_q[x]$ be quadratic with all iterates separable.*

1. *The distribution of the factorization process of f converges to that of the f-Markov process, namely the distribution having all its mass on $n \cdots n$.*
2. *Suppose f is not eventually stable, i.e., no iterate of f factors as a product of f-stable polynomials. Let $X_1, X_2, \ldots$ be the factorization process for f and λ be the largest eigenvalue less than 1 of the transition matrix M of*

the f-Markov process. Then we have

$$\lim_{n\to\infty} \frac{\sum_t \mathcal{P}(X_n = t)}{\sum_t \mathcal{P}(X_{n-1} = t)} = \lambda,$$

where the sums are taken over all states except $n \cdots n$.

(3) *Under the hypotheses of part (2), the relative frequencies of all non-$n \cdots n$ states in the factorization process for f converge to those of the f-Markov process.*

4. Examples and evidence

We first treat the few cases where the factorization process can be completely described, and then give computational evidence for Conjecture 3.6 in more complicated cases (Examples 4.1 and 4.2). The simplest possible case is when the critical orbit of $f \in \mathbb{F}_q[x]$ consists of a single point, i.e., the critical point is a fixed point. This occurs precisely when f is conjugate to x^2, i.e. $f = (x+u)^2 - u$ for some $u \in \mathbb{F}_q$. In this case one can choose a lift of f to a polynomial $\tilde{f} \in \mathcal{O}_L[x]$, where L is some number field. In this case the Galois groups of iterates of $\tilde{f}$ can be explicitly computed (they are subgroups of the affine group $AGL_1(\mathbb{Z}_2)$, which is isomorphic to $\mathbb{Z}_2 \rtimes \mathbb{Z}_2^*$). One can thus write down the cycle types of all Frobenius conjugacy classes, and hence in particular the factorizations of $f^n \in \mathbb{F}_q[x]$ (see [4, Section 4] for a discussion of the case where q is prime and $\tilde{u} \in \mathbb{Z}$ is chosen to be prime).

The next simplest case is when the critical orbit contains two points. Every quadratic polynomial in odd characteristic is conjugate to one of the form $f_c(x) = x^2 + c$, and solving for c with $f_c^3(0) = f_c(0)$ and $f_c^3(0) = f_c^2(0)$ shows that a two-element critical orbit occurs only when f is conjugate to $x^2 - 2$ or $x^2 - 1$. In these cases, we have critical orbits that are translates of $-2 \to 2 \to 2 \to \cdots$ and $-1 \to 0 \to -1 \to \cdots$, respectively. In the former case, the Galois groups of lifts are also subgroups of $AGL_1(\mathbb{Z}_2)$, and the analysis is similar to that of the previous paragraph.

Hence the simplest case where the factorization of iterates cannot be determined explicitly via a finite amount of data occurs when f is of the form $(x+u)^2 - u - 1$. In order to have f irreducible over $\mathbb{Z}$, we take $u = 1$. We note that the Galois groups over $\mathbb{Q}$ of the iterates of f have been studied in [4, Section 4]. Their inverse limit is conjecturally large enough to have nonzero Hausdorff dimension in $\mathrm{Aut}(T)$ and is related to the well-known Basilica group. The splitting fields over $\mathbb{Q}$ of the iterates of f are 2-extensions unramified outside 2 and ∞. Understanding the images of Frobenius in this arboreal Galois representation, and thus understanding the factorization process of $f \in \mathbb{F}_p[x]$ for various primes p, is the next step in analyzing this situation.

Example 4.1. Let $f = (x+1)^2 - 2 \in \mathbb{F}_q[x]$, where q is a prime power. In this case f has finite critical orbit even over $\mathbb{Z}$, so the critical orbit is the same for all q, namely $-2 \to -1 \to -2 \to \cdots$. We have $f(nn) = nn, f(ns) = sn, f(sn) = ns$, and $f(ss) = ss$. Because the critical point -1 is periodic, by Proposition 3.4 all types of immediate descendants are allowable from the states sn and ss, giving:

$$\begin{aligned} &nn \mapsto nn, \qquad ns \mapsto sn, \\ &sn \mapsto sn/nn \text{ or } ss/ns, \\ &ss \mapsto nn/nn \text{ or } ns/ns \text{ or } sn/sn \text{ or } ss/ss \end{aligned}$$

Ordering lexicographically (here nn, ns, sn, ss), the two matrices

$$M_1 = \begin{pmatrix} 1 & 0 & 0.25 & 0.25 \\ 0 & 0 & 0.25 & 0.25 \\ 0 & 1 & 0.25 & 0.25 \\ 0 & 0 & 0.25 & 0.25 \end{pmatrix} \qquad M_1^* = \begin{pmatrix} 0 & 0.25 & 0.25 \\ 1 & 0.25 & 0.25 \\ 0 & 0.25 & 0.25 \end{pmatrix}$$

are, respectively, the transition matrix of the f-Markov process and its submatrix corresponding to the non-absorbing states. The matrix M_1 has eigenvalues approximately $-0.3090, 0, 0.8090, 1$, where $\lambda = (\sqrt{5}+1)/4 \approx 0.8090$ is half the golden ratio. A right λ-eigenvector of M_1^* is $(1, \sqrt{5}, 1)$. Hence the masses in states ns and ss are ultimately about the same, say α_k for the value at time k. The mass in state sn at time k is about $\sqrt{5}\alpha_k$, and $\alpha_{k+1} \approx 0.8090\alpha_k$.

According to Conjecture 3.6, this behavior should be reflected in the factorization process for f. In this case, the critical orbit of f is the same for all q, and in Table 1 we give the masses for all states in the factorization process at large iterates for several prime values of q.

prime	iterate	nn	sn	ns	ss
3	24	0.9910	0.0046	0.0019	0.0024
3	25	0.9928	0.0037	0.0018	0.0017
3	26	0.9942	0.0032	0.0013	0.0013
3	27	0.9953	0.0026	0.0010	0.0011
3	28	0.9962	0.0019	0.0010	0.0010
5	24	0.9941	0.0034	0.0013	0.0013
5	25	0.9952	0.0026	0.0011	0.0011
5	26	0.9961	0.0020	0.0009	0.0010
5	27	0.9969	0.0017	0.0007	0.0007
5	28	0.9975	0.0013	0.0006	0.0006
7	24	0.9884	0.0062	0.0028	0.0027
7	25	0.9906	0.0049	0.0023	0.0022
7	26	0.9923	0.0041	0.0018	0.0019
7	27	0.9937	0.0033	0.0015	0.0015
7	28	0.9949	0.0027	0.0012	0.0012
11	24	0.9839	0.0081	0.0037	0.0043
11	25	0.9873	0.0069	0.0029	0.0029
11	26	0.9898	0.0055	0.0024	0.0024
11	27	0.9915	0.0041	0.0021	0.0022
11	28	0.9931	0.0039	0.0015	0.0015

TABLE 1. Masses in each state of the factorization process for $f(x) = (x+1)^2 - 2 \in \mathbb{F}_q[x]$ for various primes q.

Example 4.2. We turn to an example with critical orbit of length 3. As in Example 3.1, let $f = x^2 + 1$ and $K = \mathbb{F}_7$. The behavior of types beginning with n is determined by noting that $f(nnn) = nnn, f(nns) = nss, f(nsn) = snn$, and $f(nss) = sss$. In the notation of Proposition 3.4, we have $k = 2$, and so the allowable descendants of snn are the types $d_1d_2d_3$ with $d_2d_3 = n$, i.e. nns, nsn, sns, and ssn. Performing similar analyses for sns, ssn, sss and using lexicographic ordering

of types gives the transition matrix

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0.25 & 0 & 0.25 \\ 0 & 0 & 0 & 0 & 0.25 & 0 & 0.25 & 0 \\ 0 & 0 & 0 & 0 & 0.25 & 0 & 0.25 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0.25 & 0 & 0.25 \\ 0 & 0 & 1 & 0 & 0 & 0.25 & 0 & 0.25 \\ 0 & 0 & 0 & 0 & 0.25 & 0 & 0.25 & 0 \\ 0 & 0 & 0 & 0 & 0.25 & 0 & 0.25 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0.25 & 0 & 0.25 \end{pmatrix}.$$

We remark that there are only three distinct f-Markov processes for f with critical orbit of length 3, one corresponding to each possible length of the periodic part of the critical orbit. The matrix M_2 has largest eigenvalue (other than 1) equal to approximately 0.9010, one quarter of the largest root $t \approx 3.6039$ of $x^3 - 2x^2 - 8x + 8 = 0$. Looking at a suitably normalized corresponding right eigenvector of M_2^*, we see that nns, nsn, sns, ssn should each account for about the same proportion of the factorization of f^k, say α_k, that nss, snn should each account for about

Iterate	nnn	nns	nsn	nss	snn	sns	ssn	sss
2	0.0000	0.0000	0.5000	0.0000	0.0000	0.5000	0.0000	0.0000
3	0.2500	0.0000	0.0000	0.0000	0.7500	0.0000	0.0000	0.0000
4	0.2500	0.1250	0.2500	0.0000	0.0000	0.2500	0.1250	0.0000
5	0.3750	0.0625	0.0625	0.1250	0.3750	0.0000	0.0000	0.0000
6	0.3750	0.0625	0.1250	0.0625	0.0625	0.1250	0.0625	0.1250
7	0.5625	0.0312	0.0000	0.0625	0.1875	0.0312	0.0625	0.0625
8	0.5781	0.0781	0.0469	0.0312	0.0156	0.0469	0.0781	0.1250
9	0.6641	0.0469	0.0391	0.1094	0.1016	0.0000	0.0078	0.0312
10	0.6953	0.0391	0.0117	0.0469	0.0391	0.0156	0.0430	0.1094
11	0.7480	0.0098	0.0215	0.0410	0.0176	0.0312	0.0195	0.1113
12	0.8320	0.0107	0.0137	0.0137	0.0352	0.0078	0.0049	0.0820
13	0.8564	0.0137	0.0059	0.0215	0.0186	0.0063	0.0142	0.0635
14	0.8787	0.0046	0.0061	0.0396	0.0164	0.0117	0.0103	0.0327
15	0.8987	0.0068	0.0033	0.0129	0.0110	0.0065	0.0100	0.0508
16	0.9161	0.0059	0.0077	0.0188	0.0146	0.0046	0.0028	0.0296
17	0.9224	0.0069	0.0015	0.0179	0.0159	0.0018	0.0072	0.0264
18	0.9288	0.0051	0.0062	0.0105	0.0120	0.0064	0.0054	0.0256
19	0.9369	0.0041	0.0059	0.0131	0.0132	0.0045	0.0028	0.0195
20	0.9437	0.0045	0.0035	0.0079	0.0128	0.0035	0.0044	0.0196
21	0.9510	0.0047	0.0040	0.0077	0.0080	0.0040	0.0047	0.0160
22	0.9581	0.0033	0.0031	0.0085	0.0076	0.0030	0.0033	0.0131
23	0.9629	0.0025	0.0029	0.0058	0.0067	0.0029	0.0026	0.0137
24	0.9677	0.0026	0.0022	0.0053	0.0056	0.0021	0.0025	0.0121
25	0.9721	0.0018	0.0020	0.0053	0.0049	0.0023	0.0021	0.0097
26	0.9760	0.0018	0.0017	0.0040	0.0044	0.0017	0.0017	0.0086
27	0.9790	0.0016	0.0015	0.0036	0.0039	0.0015	0.0015	0.0074

TABLE 2. Masses in each state of the factorization process for $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$.

$(t-1)\alpha_k \approx 2.6039\alpha_k$, and sss for about $(t^2-t-5)\alpha_k \approx 4.3840\alpha_k$. Moreover, $\alpha_{k+1} = (t/4)\alpha_k \approx 0.9010\alpha_k$. Table 2 contains data for the first 27 iterates of f.

We now return to Example 4.1 and examine some related issues. First, since the critical orbit of $f = (x+1)^2 - 2 \in \mathbb{F}_q[x]$ is the same for all q, one can use Chebotarev's Density Theorem to study how varying q over prime values changes the factorization behavior of a given iterate. Note that this is different from the question of being settled, which involves fixing the prime and varying the depth. For example, suppose that q is a prime that is 5 (mod 8), so that f has type sn and so f^2 splits into two factors h_1h_2. Then $h_1(-1) = h_2(-1)$ and both are nonsquares since $h_1(-1)h_2(-1) = f^2(-1) = -1$ and -1 has no 4th root (mod q). Thus sn always decays to sn/nn at this level. The nn factor is f-stable but what about the decay of the new sn factor? It turns out that it leads to ss/ns if and only if $g = x^{16} - 4x^{12} + 4x^8 + 8x^4 + 4$ has a linear factor (mod q). Looking at the Galois group of g of order 128, we see that exactly half of the primes that are 5 (mod 8) have ss/ns at the next level.

Second, we wish to give additional evidence that the factorization process of $f = (x+1)^2 - 2$ mimics a Markov process, beyond the content of Conjecture 3.6. Here we examine at the kth iterate how many irreducible factors of type sn decay to sn/nn and how many to ss/ns. The Markov model suggests that either possibility should be equally likely. Likewise, we can perform the same calculation with irreducible factors of type ss. Table 3 contains the corresponding data. Note

		sn		ss			
prime	iterate	sn/nn	ss/ns	nn/nn	sn/sn	ns/ns	ss/ss
3	23	168	163	80	86	92	106
3	24	221	227	132	136	110	160
3	25	291	321	208	184	200	182
3	26	433	379	234	272	222	278
3	27	657	569	306	306	358	344
5	23	117	122	46	78	72	60
5	24	168	151	96	106	80	82
5	25	235	233	108	120	110	128
5	26	293	293	160	172	154	208
5	27	414	394	268	276	218	240
7	23	182	239	90	94	88	142
7	24	255	234	188	182	208	184
7	25	371	393	212	214	216	194
7	26	527	500	270	290	260	354
7	27	716	710	384	462	410	452
11	23	158	169	92	78	78	96
11	24	209	207	136	136	108	150
11	25	311	281	188	182	174	170
11	26	413	395	226	212	228	236
11	27	506	574	310	320	292	340

TABLE 3. Decay data for the factorization process of $f(x) = (x+1)^2 - 2 \in \mathbb{F}_q[x]$ for various primes q.

that the numbers in each row of the sn/nn and ss/ns columns are approximately equal, in accordance with the Markov process. The same is true of the numbers in each row of the last four columns.

As a final check that the factorization process behaves like a Markov process for large iterates, we check that there is no bias over two steps. An irreducible factor of type sn can arise from a previous sn, ns, or ss. For each of these we see how many sn decay to sn/nn and how many to ss/ns. The data can be found in Table 4. Note that the numbers in the sn/nn and ss/ns columns from Table 3 are broken

		sn from sn		sn from ns		sn from ss	
prime	iterate	sn/nn	ss/ns	sn/nn	ss/ns	sn/nn	ss/ns
3	23	63	48	65	75	40	40
3	24	85	83	97	97	39	47
3	25	120	101	115	140	56	80
3	26	156	135	174	163	103	81
3	27	224	209	295	226	138	134
3	28	331	326	282	319	166	140
3	29	356	423	455	472	241	201
3	30	542	510	577	668	334	300
5	23	47	54	47	43	23	25
5	24	60	57	62	62	46	32
5	25	90	78	96	98	49	57
5	26	122	113	111	120	60	60
5	27	140	153	172	171	102	70
5	28	207	207	234	213	137	139
7	23	73	89	75	108	34	42
7	24	98	84	108	105	49	45
7	25	130	125	150	177	91	91
7	26	196	175	215	227	116	98
7	27	264	263	304	305	148	142
7	28	374	342	360	400	234	228
11	23	47	73	72	59	39	37
11	24	84	74	90	90	35	43
11	25	108	101	134	113	69	67
11	26	164	147	164	151	85	97
11	27	192	221	207	248	107	105

TABLE 4. Two-step decay data for the factorization process of $f(x) = (x+1)^2 - 2 \in \mathbb{F}_q[x]$ for various primes q.

up according to where the sn entry producing them came from. Once again, in each row of each pair of columns the numbers are approximately equal, in accordance with the Markov process, which would say that what happens at one level should be independent of the past.

5. The Markov process and Galois groups

Recall that any polynomial conjugate to $x^2 - 1$ yields the same transition matrix M_1 for any prime p. We might then expect that the Markov process determines

the density of cycle structures in the Galois groups of iterates and hence the Galois groups themselves. This turns out to be often but not always true.

Definition 5.1. A *level n type sequence* is a partition of 2^n into powers of 2 together with a map from each term of the partition to the set of types. If two terms are equal, we do not order them. A *level n datum* is a level n type sequence together with a rational number between 0 and 1 (called its *probability* of occurring). The *level n data* is a collection of these for which the sum of the probabilities is 1.

For example, if $n = 5$ and we consider the partition $2^5 = 16 + 8 + 4 + 4$, then the map sending 16 to nn, 8 to sn, and each 4 to ss defines a level 5 type sequence which we will write $[nn, 16][sn, 8][ss, 4]^2$. Associating the rational number $1/128$ to it yields a level 5 datum.

Now suppose $f(x) = (x+t)^2 - (t+1)$ and p is a prime. The factorization of f^n modulo p yields a level n type sequence s where the partition is given by the degrees and the types by the types of the corresponding irreducible factors. Attaching to s the density of primes p yielding the type sequence s then produces a level n datum.

The advantage of the approach using level n data is that one can both read off the possible cycle structures with their densities (often allowing determination of the Galois group) and also apply the Markov process to obtain level $n+1$ data. The goal then is to start with level 1 data and iteratively obtain level n data for every n and hence the Galois groups. We will assume that f is generic, meaning that t is not of the form $m^2, m^2 - 1, 2m^2$, or $2m^2 - 1$. This will ensure that the Galois groups of its iterates are as large as possible.

The first twist is that the Markov process must be modified depending on whether p is $1 \pmod 4$ or $3 \pmod 4$ because, as noted in Lemma 2.5, linear factors behave differently under iteration, depending on whether -1 is a square modulo p. For example, if p is $1 \pmod 4$, then an $[nn, 1]$ factor will always yield an $[nn, 2]$ factor, whereas if p is $3 \pmod 4$, then it will yield $[nn, 1][ss, 1]$ or $[ns, 1][sn, 1]$ equiprobably. In the first case, the probability of the type sequence will stay the same (unless it has other factors behaving nondeterministically when it will change accordingly); in the second case, the probability of each possibility will be half the original probability (again modified by the behavior of other factors). A datum associated to $1 \pmod 4$ (respectively $3 \pmod 4$) primes will be called even (respectively odd).

The even level one data are then:

$$([[nn, 1], [nn, 1]], 1/32), ([[nn, 1], [sn, 1]], 1/16), ([[nn, 2]], 1/8), ([[ns, 1], [ns, 1]], 1/32),$$
$$([[ns, 1], [ss, 1]], 1/16), ([[sn, 1], [sn, 1]], 1/32), ([[sn, 2]], 1/8), ([[ss, 1], [ss, 1]], 1/32)$$

The odd level one data are:

$$([[nn, 1], [ns, 1]], 1/16), ([[nn, 1], [ss, 1]], 1/16), ([[ns, 1], [sn, 1]], 1/16),$$
$$([[ns, 2]], 1/8), ([[sn, 1], [ss, 1]], 1/16), ([[ss, 2]], 1/8)$$

Note that the sum of the probabilities associated with the partition $2^1 = 1 + 1$ is $1/2$ and likewise for the partition $2^1 = 2$. This illustrates the (trivial) fact that the only permutation group of degree 2 with cycle structures with those densities is the cyclic group of order 2.

Applying the Markov processes to the 8 even and 6 odd data yields 22 even and 14 odd level 2 data. The only permutation group of degree 4 with cycle structures with densities matching this data is the dihedral group of order 8 and this is indeed the Galois group of f^2.

The Markov processes applied to the level 2 data yields 120 even and 56 odd level 3 data. The only permutation group of degree 8 with cycle structures with densities matching this data is the Sylow 2-subgroup of $Sym(8)$ of order 128 and this is indeed the Galois group of f^3. The Markov processes applied to the level 3 data yields 1793 even and 577 odd level 4 data. The only permutation group of degree 16 with cycle structures with densities matching this data is a certain group of order 2^{13} and this is indeed the Galois group of f^4.

This works well at level 5 too, yielding cycle structure densities that match the known Galois group of f^5 of order 2^{25}. Apparently this is the only such permutation group of degree 32, but checking all 2-subgroups of $Sym(32)$ of that order is prohibitive (see [5] for a database of the approximately 2.8 million transitive groups of degree 32).

When we apply the Markov processes to obtain level 6 data, however, a second twist emerges. There are too many data for us to obtain all of them but the analysis of data corresponding to the cycle structure of the identity element is simple enough. In particular it corresponds to a group of order 2^{49}. The Galois group of f^6, however, has order 2^{47}. In fact, it contains the 6th quotient of the Basilica group with quotient the Klein 4-group. This has fixed field the biquadratic field $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$.

The emerging picture appears to be as follows. Let B_n denote the nth quotient of the Basilica group ($n \geq 6$). Let N_n denote its normalizer in the Sylow 2-subgroup of $Sym(2^n)$. If we can prove, as computation suggests, that N_n/B_n is elementary abelian of order 2^{n-2}, then it follows that the Galois group G_n of f^n over $\mathbb{Q}$ contains B_n with index 4 and that the quotient is a Klein 4-group corresponding to $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$.

On the other hand, the level n data for $n \geq 6$ predicts a group of order $2^{3(2^{n-2})+1}$, which is (for $n > 6$) even bigger than N_n. The cycle structure densities still appear to match well for the level n data corresponding to partitions involving 2^{n-1}, but not for the partition $2^n = 1 + ... + 1$ as indicated above.

References

1. Nidal Ali, *Stabilité des polynômes*, Acta Arith. **119** (2005), no. 1, 53–63. MR MR2163517 (2006h:11125)
2. Mohamed Ayad and Donald L. McQuillan, *Irreducibility of the iterates of a quadratic polynomial over a field*, Acta Arith. **93** (2000), no. 1, 87–97. MR MR1760091 (2001c:11031)
3. ———, *Corrections to: "Irreducibility of the iterates of a quadratic polynomial over a field" [Acta Arith. **93** (2000), no. 1, 87–97]*, Acta Arith. **99** (2001), no. 1, 97. MR MR1845367 (2002d:11125)
4. Nigel Boston and Rafe Jones, *Arboreal galois representations*, Geom. Dedicata **124** (2007), no. 1, 27–35 (electronic).
5. John J. Cannon and Derek F. Holt, *The transitive permutation groups of degree 32*, Experiment. Math. **17** (2008), no. 3, 307–314. MR MR2455702 (2009j:20003)
6. Lynda Danielson and Burton Fein, *On the irreducibility of the iterates of $x^n - b$*, Proc. Amer. Math. Soc. **130** (2002), no. 6, 1589–1596 (electronic). MR 1887002 (2002m:12001)
7. Burton Fein and Murray Schacher, *Properties of iterates and composites of polynomials*, J. London Math. Soc. (2) **54** (1996), no. 3, 489–497. MR MR1413893 (97h:12007)
8. Rafe Jones, *Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set*, Compos. Math. **143** (2007), no. 5, 1108–1126. MR MR2360312 (2008i:11131)
9. ———, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. Lond. Math. Soc. (2) **78** (2008), no. 2, 523–544. MR MR2439638
10. ———, *An iterative construction of irreducible polynomials reducible modulo every prime*, ArXiv e-prints (2010).

11. Alina Ostafe and Igor E. Shparlinski, *On the length of critical orbits of stable quadratic polynomials*, Proc. Amer. Math. Soc. **138** (2010), no. 8, 2653–2656. MR 2644881
12. E. Seneta, *Non-negative matrices and Markov chains*, Springer Series in Statistics, Springer, New York, 2006, Revised reprint of the second (1981) edition [Springer-Verlag, New York; MR0719544]. MR 2209438

Department of Mathematics and CS, College of the Holy Cross, Worcester, MA
E-mail address: rjones@holycross.edu

Department of Mathematics, University of Wisconsin Madison, WI
E-mail address: boston@math.wisc.edu