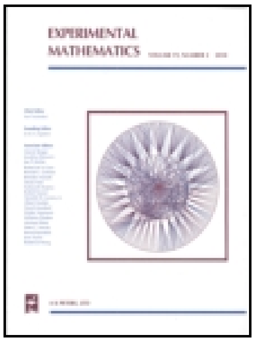

Experimental Mathematics

ISSN: 1058-6458 (Print) 1944-950X (Online) Journal homepage: https://www.tandfonline.com/loi/uexm20

A Refined Conjecture for Factorizations of Iterates of Quadratic Polynomials over Finite Fields

Vefa Goksel, Shixiang Xia & Nigel Boston

To cite this article: Vefa Goksel, Shixiang Xia & Nigel Boston (2015) A Refined Conjecture for Factorizations of Iterates of Quadratic Polynomials over Finite Fields, Experimental Mathematics, 24:3, 304-311, DOI: 10.1080/10586458.2014.992079

To link to this article: https://doi.org/10.1080/10586458.2014.992079

Published online: 23 Jun 2015.

Experimental Mathematics, 24:304–311, 2015

ISSN: 1058-6458 print / 1944-950X online
DOI: 10.1080/10586458.2014.992079

Taylor & Francis
Taylor & Francis Group

A Refined Conjecture for Factorizations of Iterates of Quadratic Polynomials over Finite Fields

Vefa Goksel[1], Shixiang Xia[2], and Nigel Boston[1]
[1]Department of Mathematics, University of Wisconsin, Madison, Wisconsin, USA
[2]Kellogg School of Management, Northwestern University, Evanston, Illinois, USA

CONTENTS

Jones and Boston conjectured that the factorization process for iterates of irreducible quadratic polynomials over finite fields is approximated by a one-step Markov model. In this paper, we find unexpected and intricate behavior for some quadratic polynomials, in particular for those whose critical orbits have large cycle and small tail. We also propose a multistep Markov model that explains these new observations better than the model of Jones and Boston.

1. INTRODUCTION

Let f be an irreducible quadratic polynomial over a finite field $\mathbb{F}_q$ of odd order q. We are interested in understanding the factorization of iterates of f. This problem was previously studied in [Gomez-Perez et al. 12, Gomez-Perez et al. 11, Ahmadi et al. 12, Odoni 88, Jones and Boston 12]. In the last cited work, the authors associated a one-step Markov process to f and conjectured that its limiting distribution explains the shape of the factorization of large iterates of f.

As an example, consider $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$. The approach of Jones and Boston was to define the *type* of a polynomial $g \in \mathbb{F}_7[x]$ (in this case, whether $g(1), g(2), g(5)$ are squares or nonsquares in $\mathbb{F}_7$). They then observed that the types of factors of $g(f(x))$ are highly constrained, but not always determined, by the type of $g(x)$. They then conjectured that the distribution of types for factors of large iterates is approximated by a one-step Markov process whereby each allowable transition of types is given equal probability in the transition matrix. See Section 2 for more details.

In this paper, we give new data that strongly suggest that a more complicated model is required in certain cases, and we propose a multistep Markov model that fits the new data well. For example, for the iterates of $x^2 + 1 \in \mathbb{F}_7[x]$, which were studied in detail in [Jones and Boston 12], it is noted that contrary to what was predicted there, certain three-step transitions of types apparently never occur. The multistep Markov model

2000 AMS Subject Classification: 11T55, 37P25, 60J20
Keywords: Iteration, quadratic polynomial, factorization, Markov process

Address correspondence to Nigel Boston, University Of Wisconsin, Madison, Mathematics, Van Vleck Hall, 480 Lincoln Drive, Madison, 53706, USA. Email: boston@math.wisc.edu

takes this into account, and it turns out that the limiting relative distribution of types predicted by this new model more closely approximates data for large iterates than the old model did. Note that the multistep model simply reduces to the one-step model for many polynomials f.

The paper is structured as follows. In Section 2, we make some definitions, give preliminary results, and recall background to the problem. In Section 3, we provide some examples with new, unexpected behavior. In Section 4, we propose a multistep Markov model to describe the factorization of iterates and conjecture that it provides a better explanation for the process. Section 5 supports this model via actual data corresponding to the examples given in Section 3. An appendix (Section 6) gives some further examples in which the multistep model reduces to the one-step model.

2. SETUP

We begin with a definition.

Definition 2.1. Let $\mathbb{F}_q$ be a finite field of odd order q. Consider a quadratic polynomial $f(x)$ defined over $\mathbb{F}_q$. For all $n \in \mathbb{N}$, we define the *nth iterate* of f to be $f^n(x) := f\left(f^{n-1}(x)\right) \in \mathbb{F}_q[x]$. We make the convention that $f^0(x) := x$.

For example, suppose $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$. Then $f^2(x) = f(f(x)) = x^4 + 2x^2 + 2$, $f^3(x) = f(f^2(x)) = x^8 + 4x^6 + x^4 + x^2 + 5$, and so on, all of which are computed over $\mathbb{F}_7$.

Definition 2.2. Let $f(x) = ax^2 + bx + c \in \mathbb{F}_q[x]$ $(a \neq 0)$, and let $\alpha = -b/2a$ be the critical point of f. The *critical orbit* of f is the set $\mathcal{O} := \{f^k(\alpha) \mid k = 1, 2, 3, \dots\}$, and the number of elements of $\mathcal{O}$ is the *orbit size* of f, denoted by o.

To illustrate the definition of the critical orbit, we consider the previous example. The critical point of $f(x) = x^2 + 1$ is 0, and $f(0) = 1$, $f^2(0) = 2$, $f^3(0) = 5$, $f^4(0) = 5$. It follows that $f^k(0) = 5$ for all $k \geq 3$. Therefore, the critical orbit for $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$ is $\{1, 2, 5\}$.

Definition 2.3. Let f be a quadratic polynomial over $\mathbb{F}_q$, and let α be the critical point of f. We define the *critical tail* of f to be the set

$$\mathcal{T} := \left\{f^k(\alpha) \mid k \geq 1,\, f^i(\alpha) \neq f^k(\alpha) \text{ for all } i \neq k\right\}.$$

Similarly, we call the number of elements of $\mathcal{T}$ the *tail size* of f and denote it by t.

Remark 2.4. This definition may seem counterintuitive, but in the case of quadratic polynomials, we cannot have $f^n(\gamma) = f^1(\gamma)$ without having $f^{n-1}(\gamma) = \gamma$, where γ is the critical point of f.

Example 2.5. Let $f(x) = x^2 + 2 \in \mathbb{F}_5[x]$. Its critical orbit is $\{2, 1, 3\}$, and so the critical tail has size 1 by the above definition.

With the choice $f(x) = x^2 + c$, the critical orbit of $f(x) \in \mathbb{F}_q[x]$ becomes $\{c, c^2 + c, (c^2 + c)^2 + c, \dots\}$.

Definition 2.6. Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible quadratic polynomial with critical orbit $\mathcal{O}$, and take $g(x) \in \mathbb{F}_q[x]$. We define the *type of* $g(x)$ at β to be s if $g(\beta)$ is a square in $\mathbb{F}_q$, and n if it is not a square. The type of g is a string of length $|\mathcal{O}|$ whose kth entry is the type of $g(x)$ at the kth entry of $\mathcal{O}$. The kth entry is also called the kth *digit*.

For instance, given $x^2 + 1 \in \mathbb{F}_7[x]$, consider $g(x) = x^2 + 2x + 2$. Then $g(1) = 5, g(2) = 3, g(5) = 2$, which implies that the type of g is nns.

Definition 2.7. Given an irreducible quadratic polynomial $f(x) \in \mathbb{F}_q[x]$ and a polynomial $g(x) \in \mathbb{F}_q[x]$, we call the factors of $g(f(x))$ the *children* of g. Also, for every natural number m, the factors of $g\left(f^m(x)\right)$ are called the *m-step descendants* of g.

Definition 2.8. Let $f(x) \in \mathbb{F}_q[x]$ be a quadratic polynomial, and let γ be any element in $\mathbb{F}_q$. We say that γ is *periodic* if there exists $i \in \mathbb{N}$ such that $f^i(\gamma) = \gamma$.

Next, we quote a lemma that is one of the building blocks of our paper.

Lemma 2.9. [Jones and Boston 12] *Suppose that $f \in \mathbb{F}_q[x]$ is quadratic with critical orbit of length o and all iterates separable. Let $g \in \mathbb{F}_q[x]$ be irreducible of even degree. Suppose that h_1h_2 is a nontrivial factorization of $g(f(x))$, and let d_i and e_i be the respective ith digits of the types of h_1 and h_2. Then there is some k, $1 \leq k \leq o$, with $d_o = e_k$ and $e_o = d_k$. Moreover, $k = o$ if and only if γ is periodic, and if γ is not periodic, then we have $k = t$, where t is the tail size of f.*

In [Jones and Boston 12], the authors modeled the distribution of types of factors (weighted by their degree) of iterates of f by a one-step Markov model as follows: They consider two processes. The first, called the *factorization process* of f, consists of the types of the irreducible factors in the actual factorization of the iterates of f and tracks how the type of a factor transitions to the types of its children. See [Jones and Boston 12, p. 1853] for details.

The second is a one-step Markov process, which they then conjecture models what happens to the types under the first process. This second process is a time-homogeneous one-step Markov process $Y_1, Y_2, \ldots$ related to f, which they call the *f-Markov process*. The state space is the space of types of f, namely $\{n, s\}^o$, ordered lexicographically. They define the Markov process by giving its transition matrix

$$M_1 = \left(\mathcal{P}\left(Y_m = T_j \mid Y_{m-1} = T_i\right)\right),$$

where T_i and T_j vary over all types. Note that the entries of each column of M_1 sum to 1. They define M_1 by assuming that all *allowable types* of children arise with equal probability. To define allowable type, note that f 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 mth entry as the new final entry, where m is such that $f^{o+1}(\gamma) = f^m(\gamma)$. If g has type T that begins with n, then g has only one child, and it will have type $f(T)$, the only allowable type in this case. If T begins with s, then g has two children, whose types have product $f(T)$. Among pairs of types T_1, T_2 with $T_1 T_2 = f(T)$, they call allowable those that satisfy the conclusion of Lemma 2.9, namely $d_k = e_o$ and $e_k = d_o$ with $k = o$ if γ is periodic, and $k = t$ if γ is aperiodic, where t is the tail size of f. See the examples in the following section for illustration.

Conjecture 3.6 in [Jones and Boston 12] states that the relative frequencies of all non-$n \cdots n$ states in the factorization process for f converge to those of the f-Markov process. In the current paper, we discover that the story of these descendants can be quite different in certain cases, contrary to what Jones and Boston suggested. What happens is that certain multistep transitions of types allowed by the above model apparently do not actually arise in the factorization process. To discuss this phenomenon, we need the following definition.

Definition 2.10. Let $Z_1, Z_2, \ldots$ be an arbitrary stochastic process. We define an *m-step transition matrix* as $M_m = (\mathcal{P}(Z_{m+1} = T_j \mid Z_1 = T_i))$, where T_i and T_j vary over all types.

Remark 2.11. The f-Markov process in [Jones and Boston 12] implies that $M_m = {M_1}^m$ always holds because that process is a Markov chain.

In the next section, we shall observe that for certain f, this last formula does not give m-step transition matrices that most accurately model the factorizations of large iterates.

3. NEW PHENOMENA

We now present three families of examples that indicate that a multistep Markov model better models data from large iterates of certain irreducible quadratic $f \in F_q[x]$.

Note that to check which multistep transitions of types arise in the factorization process, we wrote a simple MAGMA program that given f, inputs one million random irreducible polynomials of 2-power degree and records their types and those of their children, grandchildren, and so on. For most f, i.e., those not of the forms in Observations 3.2, 3.4, and 3.6, all multistep transitions predicted by the one-step model arose (and approximately equally often). See the appendix for details. The examples below indicate where we found glaring omissions.

Example 3.1. The first family consists of f with orbit size 3 and tail size 1. Let $f \in \mathbb{F}_q[x]$ be of the form $f(x) = x^2 + c$. Note that all c-values with orbit size 3 and tail of size 1 are roots of the polynomial given by

$$\frac{\left(f^3(c) - f(c)\right)}{1\text{cm}\left(\left(f^2(c) - f(c)\right), \left(f^2(c) - c\right)\right)},$$

which happens to be $c^2 + 1$. So the desired polynomials in this case are the quadratics of the form $f(x) = x^2 + i$, where i is a square root of -1 in $\mathbb{F}_q$. (Note that to do so, we need $q \equiv 1 \pmod 4$ and in fact $q \equiv 5 \pmod 8$ to ensure that f is irreducible.) The critical orbit is

$$\{i, i - 1, -i\}.$$

Using Lemma 2.9, the following 1-step transitions arise:

$$\begin{aligned}
&nnn \mapsto nnn, \quad nns \mapsto nsn,\\
&nsn \mapsto sns, \quad nss \mapsto sss,\\
&snn \mapsto nns/ssn \text{ or } nss/snn,\\
&sns \mapsto nns/snn \text{ or } nss/ssn,\\
&ssn \mapsto nnn/nsn \text{ or } sns/sss,\\
&sss \mapsto nnn/nnn \text{ or } nsn/nsn \text{ or } sns/sns \text{ or } sss/sss.
\end{aligned}$$

It follows that

$$M_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1/4 & 1/4 \\ 0 & 0 & 0 & 0 & 1/4 & 1/4 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1/4 & 1/4 \\ 0 & 0 & 0 & 0 & 1/4 & 1/4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/4 & 1/4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1/4 & 1/4 \\ 0 & 0 & 0 & 0 & 1/4 & 1/4 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1/4 & 1/4 \end{bmatrix}.$$

Observation 3.2. Let $q \equiv 5 \pmod 8$. Let $f(x) = x^2 + i \in \mathbb{F}_q[x]$, where i is a square root of -1. Then the following 2-step transitions were never observed:

$$nsn \mapsto nns/snn, \quad nss \mapsto nnn/nnn, \quad nss \mapsto sns/sns.$$

Thus if we adjust M_2 accordingly, it appears that the factorization process is best modeled by a process that obeys $M_2 = M_1^2 + A$, where

$$A = M_2 - M_1^2 = \begin{bmatrix} 0 & 0 & 0 & -1/4 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1/4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1/4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1/4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/4 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Note that according to the one-step model, A would be 0.

Example 3.3. The second family consists of f with orbit size 4 and tail size 1. If we consider the same polynomial $f(x) = x^2 + c$ as in the first example, all c-values with orbit size 4 and tail size 1 are the roots of the polynomial given by

$$\frac{\left(f^4(c) - f(c)\right)}{\operatorname{lcm}\left(\left(f^2(c) - f(c)\right), \left(f^3(c) - c\right)\right)},$$

which happens to be $c^6 + 2c^5 + 2c^4 + 2c^3 + c^2 + 1$. Let c_0 be a root of this polynomial in some $\mathbb{F}_q$ such that $x^2 + c_0$ is irreducible. According to Lemma 2.9, the following 1-step transitions are allowable:

$$\begin{aligned} &nnnn \mapsto nnnn, \quad nnns \mapsto nnsn, \quad nnsn \mapsto nsnn, \\ &nnss \mapsto nssn, \quad nsnn \mapsto snns, \quad nsns \mapsto snss, \\ &nssn \mapsto ssns, \quad nsss \mapsto ssss, \\ &snnn \mapsto nnns/sssn \text{ or } nnss/ssnn \text{ or } nsns/snsn \\ &\quad \text{or } nsss/snnn, \\ &snns \mapsto nnns/ssnn \text{ or } nnss/sssn \text{ or } nsns/snnn \\ &\quad \text{or } nsss/snsn, \\ &snsn \mapsto nnns/snsn \text{ or } nnss/snnn \text{ or } nsns/sssn \\ &\quad \text{or } nsss/ssnn, \\ &snss \mapsto nnns/snnn \text{ or } nnss/snsn \text{ or } nsns/ssnn \\ &\quad \text{or } nsss/sssn, \\ &ssnn \mapsto nnnn/nssn \text{ or } nnsn/nsnn \text{ or } snns/ssss \\ &\quad \text{or } snss/ssns, \\ &ssns \mapsto nnnn/nsnn \text{ or } nnsn/nssn \text{ or } snns/ssns \\ &\quad \text{or } snss/ssss, \\ &sssn \mapsto nnnn/nnsn \text{ or } nsnn/nssn \text{ or } snns/snss \\ &\quad \text{or } ssns/ssss, \\ &ssss \mapsto nnnn/nnnn \text{ or } nnsn/nnsn \text{ or } nsnn/nsnn \\ &\quad \text{or } nssn/nssn \text{ or } snns/snns \text{ or } snss/snss \text{ or } \\ &\quad ssns/ssns \text{ or } ssss/ssss. \end{aligned}$$

It follows that M_1 is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \end{pmatrix}.$$

Analogously to the first example, however, we observe that once again, certain 2-step transitions are apparently forbidden.

Observation 3.4. Let c_0 be a root of $c^6 + 2c^5 + 2c^4 + 2c^3 + c^2 + 1$ in $\mathbb{F}_q$ and suppose that $f(x) = x^2 + c_0 \in \mathbb{F}_q[x]$ is irreducible. Then the following 2-step transitions were never observed:

$$
\begin{aligned}
&nsnn \mapsto nnns/ssnn, \quad nsnn \mapsto nsns/snnn,\\
&nsns \mapsto nnns/snnn, \quad nsns \mapsto nsns/ssnn,\\
&nssn \mapsto nnnn/nsnn, \quad nssn \mapsto snns/ssns,\\
&nsss \mapsto nnnn/nnnn, \quad nsss \mapsto nsnn/nsnn,\\
&nsss \mapsto snns/snns, \quad nsss \mapsto ssns/ssns.
\end{aligned}
$$

By the same reasoning as in Example 3.1, the factorization process again appears to be best modeled by a process that obeys $M_2 = {M_1}^2 + A$, where A is equal to

$$
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{8} & -\frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{8} & \frac{1}{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
$$

Note that according to the one-step model, A would be 0.

Example 3.5. Finally, we look at the family of examples with orbit size 3 and tail size 2. We again consider the polynomial $f(x) = x^2 + c$. In this case, all c-values satisfying these sizes are roots of the polynomial given by

$$
\frac{\left(f^3(c) - f^2(c)\right)}{c \operatorname{lcm}\left(\left(f^2(c) - f(c)\right), \left(f(c) - c\right)\right)},
$$

which happens to be $c^3 + 2c^2 + 2c + 2$. Using Lemma 2.9, the 1-step transitions are as given below:

$$
\begin{aligned}
&nnn \mapsto nnn, \quad nns \mapsto nss, \quad nsn \mapsto sns,\\
&nss \mapsto sss, \quad snn \mapsto nsn/sns \text{ or } nns/ssn,\\
&sns \mapsto nnn/snn \text{ or } sss/nss,\\
&ssn \mapsto nns/nsn \text{ or } sns/ssn,\\
&sss \mapsto nnn/nnn \text{ or } nss/nss \text{ or } snn/snn \text{ or } sss/sss.
\end{aligned}
$$

It follows that

$$
M_1 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1/4 & 0 & 1/4\\
0 & 0 & 0 & 0 & 1/4 & 0 & 1/4 & 0\\
0 & 0 & 0 & 0 & 1/4 & 0 & 1/4 & 0\\
0 & 1 & 0 & 0 & 0 & 1/4 & 0 & 1/4\\
0 & 0 & 1 & 0 & 0 & 1/4 & 0 & 1/4\\
0 & 0 & 0 & 0 & 1/4 & 0 & 1/4 & 0\\
0 & 0 & 0 & 0 & 1/4 & 0 & 1/4 & 0\\
0 & 0 & 0 & 1 & 0 & 1/4 & 0 & 1/4
\end{bmatrix}.
$$

Observation 3.6. Let c_1 be a root of $c^3 + 2c^2 + 2c + 2$ in $\mathbb{F}_q$. Let $f(x) = x^2 + c_1 \in \mathbb{F}_q[x]$ be irreducible. Then the following 3-step transitions were never observed:

$$
\begin{aligned}
&nns \mapsto nss \mapsto sss \mapsto nss/nss,\\
&nns \mapsto nss \mapsto sss \mapsto snn/snn.
\end{aligned}
$$

In this case, on adjusting M_3 accordingly, it appears that the factorization process is best modeled by a process that obeys $M_3 = M_1^3 + A$, where

$$
A = M_3 - M_1^3 = \begin{pmatrix}
0 & 1/4 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -1/4 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -1/4 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1/4 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
$$

Note that according to the one-step model, A would be 0.

4. MULTISTEP MARKOV MODEL

The investigations in the previous section indicate that a one-step Markov model does not always fit the factorization process for iterates of quadratic polynomials. We need a multistep (refined) model to explain the process, and we propose the following: Let f be an irreducible quadratic polynomial defined over $\mathbb{F}_q$ with critical tail size $a - 1$ and orbit size b. We define a stochastic process $Z_1, Z_2, \ldots$ by giving its m-step transition matrices $M_m = (\mathcal{P}(Z_{m+1} = T_j \mid Z_1 = T_i))$, as T_i and T_j vary over all types.

Definition 4.1. The *a-step Markov model* based on two given matrices A and B of fixed size $2^b \times 2^b$ is the Markov model having m-step transition matrices satisfying

$$
M_{m+a} = M_{m+a-1} B + M_m A \tag{4–1}
$$

with $M_{-a+1} = \cdots = M_{-2} = M_{-1} = 0$, $M_0 = I$.

Remark 4.2. It easily follows that $M_1 = B$, $M_i = M_1^i$ for $i = 1, 2, \ldots, a-1$, and $M_a = M_1^a + A$. Note that if $A = 0$, then this model is simply the old one-step model.

We conjecture that the multistep Markov model given above describes the factorization process for the iterates of f, provided that we choose the correct A and B depending on f. The choice of B is easy: it is the matrix M_1 furnished by Lemma 2.9. As for A, we know what it should be in the following situation, but the general rule is unclear (in particular, the appendix indicates that $A = 0$ often).

Definition 4.3. Suppose that f has tail size 1 and orbit size b. Let A be the $2^b \times 2^b$ matrix whose entries are all 0 except for those in the 2^{b-2} columns whose labeling begins ns. For those columns, exactly half the entries in the ith row are zero, and the rows are as follows: $0, \ldots, 0, -2^{1-b}, \ldots, -2^{1-b}$ if $i \leq 2^{b-1}$ and $1 \pmod 4$ or $i > 2^{b-1}$ and $2 \pmod 4$; $-2^{1-b}, \ldots, -2^{1-b}, 0, \ldots, 0$ if $i \leq 2^{b-1}$ and $2 \pmod 4$ or $i > 2^{b-1}$ and $1 \pmod 4$; $0, \ldots, 0, 2^{1-b}, \ldots, 2^{1-b}$ if $i \leq 2^{b-1}$ and $3 \pmod 4$ or $i > 2^{b-1}$ and $0 \pmod 4$; $2^{1-b}, \ldots, 2^{1-b}, 0, \ldots, 0$ if $i \leq 2^{b-1}$ and $0 \pmod 4$ or $i > 2^{b-1}$ and $3 \pmod 4$. Then A is called the *discrepancy matrix* of f.

Remark 4.4. Explicit discrepancy matrices for $b = 3, 4$ are given in Examples 3.1 and 3.3 respectively.

To show that the above matrix A gives the correct discrepancy matrix for our 2-step Markov model amounts to showing that certain 2-step transitions of types do not arise. This is equivalent to the following conjecture.

Conjecture 4.5. *Let f be an irreducible quadratic polynomial over $\mathbb{F}_q$ with tail size $t = 1$ and orbit size o, and let g be an even irreducible polynomial over $\mathbb{F}_q$ whose type begins with ns. Then the $(o-1)$th digit of the type of each irreducible factor of $g(f(x))$ is s.*

Example 4.6. We now prove Conjecture 4.5 in a special case with $f(x) = x^2 + c$. Note that tail size being 1 means that $f^o(0) = f^2(0)$ and $f^o(0) \neq f^1(0)$, so the oth digit is $-c$, and thus the $(o-1)$th digit is α, where $\alpha^2 + c = -c$, i.e., $\alpha^2 = -2c$. Suppose that $g(x) = x^4 + ax^2 + b$. Then $g(x^2 + c)$ factors as $h(x)h(-x)$, since the type g begins with ns, and we must show that $h(\alpha)$ is a square. If $h(x) = x^4 + px^3 + qx^2 + rx + s$, then by comparing coefficients, we eliminate q, s, a, which yields

$$h(\alpha) = \left(\alpha^2 + \frac{p\alpha}{2} + \frac{r}{p}\right)^2 = \left(-2c + \frac{r}{p} + \frac{p\alpha}{2}\right)^2.$$

Note that if $p = 0$, then one computes $a^2 - 4b = 0$, implying that g is the square of a polynomial, which is not the case.

Remark 4.7. Conjecture 4.5 applies to $f(x) = x^2 - 2$, which is the simplest polynomial of the form $x^2 + c$ with tail size 1. It is, however, vacuous for factors of iterates of $x^2 - 2$ itself, because, as indicated in [Jones and Boston 12], the factors are entirely of type nn after a finite number of iterates, whatever q is.

With this preamble, we can now state the main conjecture of our paper.

Conjecture 4.8. *The limiting behavior of the a-step Markov model is the same as the limiting behavior of the factorization process.*

We can provide evidence for Conjecture 4.5 by computing factorizations of large iterates of given f and comparing the distribution of factors to that of the limiting behavior of the a-step Markov model. In particular, the multistep Markov model predicts that in the limit, 100% of the factorizations of the iterates will be of type $nn\ldots n$ (the unique sink), and it also allows us to compute the limiting relative proportions of the other types as follows.

We fix an arbitrary natural number m and define v_i to be the vector whose entries are the proportions of all 2^b types (lexicographically ordered) for the $(m+i)$th iterate of the polynomial f. Say $v = (v_1, v_2, \ldots, v_a)$. Then using (1), we see that the next such a-tuple will, according to the model, be the vector $(v_2, v_3, \ldots, v_a, Av_1 + Bv_a)$. Denoting the associated $a2^b \times a2^b$ transition matrix by T, we have

$$T = \begin{pmatrix} 0 & I & \cdots & 0 \\ & & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ & & & I \\ A & 0 & \cdots & B \end{pmatrix}.$$

We can thereby interpret this multistep Markov model as a Markov process on a larger number of states, with transition matrix T. The limiting frequencies of the nonabsorbing states are given, up to scaling, by the entries of an eigenvector of T corresponding to its largest eigenvalue less than 1 [Seneta 06].

Combining this fact with the following lemma indicates how the limiting proportions can be computed.

Lemma 4.9. *With the notation as above, let e be an eigenvector of the transition matrix T corresponding to*

Iterate	nns	nsn	nss	snn	sns	ssn	sss
20	0.0251	0.1748	0.1163	0.0271	0.2541	0.1143	0.2883
21	0.0268	0.1661	0.1221	0.0267	0.2635	0.1222	0.2726
22	0.0300	0.1725	0.1253	0.0271	0.2487	0.1282	0.2681
23	0.0256	0.1689	0.1223	0.0253	0.2508	0.1226	0.2846
24	0.0238	0.1686	0.1240	0.0238	0.2542	0.1239	0.2817
25	0.0276	0.1669	0.1217	0.0272	0.2598	0.1220	0.2748
26	0.0263	0.1699	0.1276	0.0282	0.2526	0.1256	0.2697
27	0.0263	0.1677	0.1237	0.0269	0.2502	0.1231	0.2821

TABLE 1. Relative proportions of types (other than *nnn*) for factors of iterates of $f(x) = x^2 + 2 \in \mathbb{F}_5[x]$.

eigenvalue λ, and let e_1 denote its first 2^b entries. Then $e = \big(e_1, \lambda e_1, \lambda^2 e_1, \ldots, \lambda^{a-1} e_1\big)$.

Proof. This lemma is a consequence of [Dennis et al. 76, Theorem 3.2] (or it can be easily proven directly). □

Again with the notation above, consider the eigenvector e of T, corresponding to the largest eigenvalue less than 1, such that the entries of e_1 except the first one sum to 1. The entries of e_1 are the limiting proportions of the types that are not $nn \ldots n$.

5. DATA

In this section, we provide data corresponding to Examples 3.1, 3.3, and 3.5. In each case, we use the smallest q for which the corresponding difference polynomial has a root and yields an irreducible quadratic. Comparing the limiting proportions predicted by the refined model with the data for each example, we will illustrate how well the multistep Markov model fits. Table 1 gives data for Example 3.1.

By comparison, if we consider the related block matrix in the previous section, the first part e_1 of an eigenvector for the eigenvalue $\lambda \approx 0.9333801995$ is

$$\begin{bmatrix} -1.0000000000\cdots \\ 0.026110931\cdots \\ 0.170493119\cdots \\ 0.123960675\cdots \\ 0.026110931\cdots \\ 0.254036800\cdots \\ 0.123960675\cdots \\ 0.275326866\cdots \end{bmatrix}.$$

Table 2 gives data for Example 3.3.

If we compute the appropriate eigenvector of the related 32×32 matrix, its first block e_1 of size 16 is

$$\begin{bmatrix} -1.0000000000\cdots \\ 0.018669399\cdots \\ 0.079050806\cdots \\ 0.049246267\cdots \\ 0.099196036\cdots \\ 0.018669399\cdots \\ 0.110198525\cdots \\ 0.049246267\cdots \\ 0.018669399\cdots \\ 0.119717366\cdots \\ 0.049246267\cdots \\ 0.079050806\cdots \\ 0.018669399\cdots \\ 0.130925265\cdots \\ 0.049246267\cdots \\ 0.110198525\cdots \end{bmatrix}.$$

Table 3 gives data for Example 3.5.

Iterate	*nnns*	*nnsn*	*nnss*	*nsnn*	*nsns*	*nssn*	*nsss*	*snnn*	*snns*	*snsn*	*snss*	*ssnn*	*ssns*	*sssn*	*ssss*
21	0.0180	0.0932	0.0446	0.0809	0.0203	0.1194	0.0536	0.0129	0.1114	0.0501	0.0845	0.0230	0.1227	0.0505	0.1152
22	0.0177	0.0705	0.0483	0.1086	0.0187	0.1039	0.0483	0.0137	0.1021	0.0486	0.0811	0.0210	0.1450	0.0497	0.1228
23	0.0178	0.0816	0.0414	0.0934	0.0182	0.1135	0.0476	0.0180	0.1305	0.0465	0.0870	0.0171	0.1272	0.0435	0.1166
24	0.0232	0.0804	0.0493	0.1044	0.0189	0.0992	0.0524	0.0183	0.1116	0.0559	0.0763	0.0169	0.1348	0.0527	0.1057
25	0.0190	0.0859	0.0469	0.1007	0.0191	0.1138	0.0486	0.0185	0.1254	0.0487	0.0769	0.0199	0.1187	0.0464	0.1114
26	0.0188	0.0739	0.0486	0.1056	0.0199	0.1020	0.0500	0.0173	0.1217	0.0493	0.0776	0.0194	0.1332	0.0514	0.1115
27	0.0178	0.0828	0.0497	0.0963	0.0189	0.1107	0.0493	0.0176	0.1266	0.0505	0.0792	0.0186	0.1218	0.0489	0.1115

TABLE 2. Relative proportions of types (other than *nnnn*) for factors of iterates of $f(x) = x^2 + 3 \in \mathbb{F}_{11}[x]$.

Iterate	nns	nsn	nss	snn	sns	ssn	sss
26	0.0731	0.0728	0.1673	0.1827	0.0718	0.0722	0.3601
27	0.0760	0.0727	0.1695	0.1863	0.0699	0.0732	0.3523
28	0.0736	0.0754	0.1798	0.1734	0.0747	0.0729	0.3502
29	0.0654	0.0761	0.1639	0.1873	0.0772	0.0665	0.3636
30	0.0747	0.0762	0.1757	0.1876	0.0730	0.0714	0.3414
31	0.0714	0.0772	0.1735	0.1772	0.0766	0.0707	0.3535
32	0.0715	0.0713	0.1818	0.1910	0.0703	0.0706	0.3434
33	0.0716	0.0756	0.1720	0.1738	0.0783	0.0743	0.3544
34	0.0711	0.0708	0.1859	0.1863	0.0715	0.0718	0.3426

TABLE 3. Relative proportions of types (other than *nnn*) for factors of iterates of $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$.

As mentioned before, in [Jones and Boston 12], the authors proposed a one-step Markov process, and they supported this claim by the example $x^2 + 1$ over $\mathbb{F}_7$. However, the result given in Observation 3.6 does not follow this claim. To illustrate how the multistep Markov model gives a better fit, Table 4 compares the limiting proportions predicted by the one-step Markov model and those predicted by the multistep Markov model.

It is particularly striking how much better the refined model fits the data for sss.

6. APPENDIX

The following list gives other cases investigated but not covered in previous sections. In each instance, we found a particular irreducible f with orbit size o and tail size t, and beginning with one million random irreducible polynomials g of 2-power degree, we recorded their types and those of their children, grandchildren, and so on.

Example 6.1. **($o = 4$, $t = 2$.)** All c-values giving these sizes are roots of $c^3 + c^2 - c + 1$. The first example is $x^2 + 4 \in \mathbb{F}_7[x]$. This has no missing 3-step transitions and appears to follow the one-step Markov model.

Types	Markov Model	
	One-Step	Multistep
nns	$0.073573805\cdots$	$0.071981460\cdots$
nsn	$0.073573805\cdots$	$0.071981460\cdots$
nss	$0.191577027\cdots$	$0.178322872\cdots$
snn	$0.191577027\cdots$	$0.178322872\cdots$
sns	$0.073573805\cdots$	$0.071981460\cdots$
ssn	$0.073573805\cdots$	$0.071981460\cdots$
sss	$0.322550722\cdots$	$0.355428413\cdots$

TABLE 4. Limiting proportions of types (other than *nnn*) for factors of iterates of $x^2 + 1 \in \mathbb{F}_7[x]$ predicted by the one-step Markov model and the multistep Markov model.

Example 6.2. **($o = 5$, $t = 2$.)** All c-values giving these sizes are roots of $c^{12} + 6c^{11} + 14c^{10} + 18c^9 + 18c^8 + 16c^7 + 10c^6 + 6c^5 + 5c^4 + 2c^3 + 1$. The first example is $x^2 + 12 \in \mathbb{F}_{17}[x]$. This has no missing 3-step transitions and appears to follow the one-step Markov model.

Example 6.3. **($o = 4$, $t = 3$.)** All c-values giving these sizes are roots of $c^7 + 4c^6 + 6c^5 + 6c^4 + 6c^3 + 4c^2 + 2c + 2$. The first example is $x^2 + 2 \in \mathbb{F}_7[x]$. This has no missing 4-step transitions and appears to follow the one-step Markov model.

Example 6.4. **($o = 5$, $t = 3$.)** All c-values giving these sizes are roots of $c^8 + 4c^7 + 6c^6 + 6c^5 + 4c^4 + 1$. The first example is $x^2 + 1 \in \mathbb{F}_{11}[x]$. This has no missing 4-step transitions and appears to follow the one-step Markov model.

ACKNOWLEDGMENTS

The authors owe Rafe Jones a debt of gratitude for his valuable comments on this work during the preparation of the manuscript.

REFERENCES

[Ahmadi et al. 12] Omran Ahmadi, Florian Luca, Alina Ostafe, and Igor E. Shparlinski. "On Stable Quadratic Polynomials." *Glasgow Mathematical Journal* 54 (2012), 359–369.

[Dennis et al. 76] J. E. Dennis, Jr., J. F. Traub, and R. P. Weber. "The Algebraic Theory of Matrix Polynomials." *SIAM Journal on Numerical Analysis and Applications* 13 (1976), 831–845.

[Gomez-Perez et al. 11] Domingo Gomez-Perez, A. P. Nicolas, A. Ostafe, and D. Sadornil. "Stable Polynomials over Finite Fields." Preprint, 2011.

[Gomez-Perez et al. 12] Domingo Gomez-Perez, Alina Ostafe, and Igor E. Shparlinski, "On Irreducible Divisors of Iterated Polynomials." Preprint, 2012.

[Jones and Boston 12] Rafe Jones and Nigel Boston. "Settled Polynomials over Finite Fields." *Proc. Amer. Math. Soc.* 140 (2012), 1849–1863.

[Odoni 88]R. W. K. Odoni. "Realising Wreath Products of Cyclic Groups as Galois Groups." Mathematika 35 (1988), 101–113.

[Seneta 06] E. Seneta. *Non-negative Matrices and Markov Chains*, Springer Series in Statistics, revised reprint of the second (1981) edition. Springer, 2006.