Self-interacting polynomials

Franco Vivaldi

School of Mathematical Sciences, Queen Mary, University of London,
London E1 4NS, UK

Abstract

We introduce a class of dynamical systems of algebraic origin, consisting of self-interacting irreducible polynomials over a field. A polynomial $f$ is made to act on a polynomial $g$ by mapping the roots of $g$. This action identifies a new polynomial $h$, as the minimal polynomial of the displaced roots. By allowing several polynomials to act on one another, we obtain a self-interacting system with a rich dynamics, which affords a fresh viewpoint on some algebraic dynamical constructs. We identify the basic invariant sets, and study in some detail the case of quadratic polynomials. We perform some experiments on self-interacting polynomials over finite fields.

1 Introduction

From the viewpoint of algebraic dynamics, a polynomial with coefficients in a field $K$ can be interpreted in two ways. On the one hand, it defines a dynamical system over the algebraic closure $\bar{K}$ of $K$; on the other, its roots define elements of $\bar{K}$. In the former case the polynomial represents a function acting on a state space, that is, a dynamical system; in the latter, the polynomial encodes points of the state space itself.

In this paper we exploit this duality to define a new class of discrete dynamical systems resulting from the mutual interaction between irreducible polynomials. Such interaction features an active element (a function) and a passive one (a set of points, which are algebraic conjugates), whose role is interchangeable. Specifically, given two irreducible polynomials $f$ and $g$ over the same field, we define $h = f \triangleright g$ to be the minimal polynomial of the image of the roots of $g$ under $f$. This relationship between $f, g$ and $h$ defines the wedge operator $\triangleright$ (see section 2 for details). The action of the wedge operator is quite natural, since it performs simultaneously the time-evolution of all algebraic conjugates, which, algebraically speaking, are indistinguishable. This construction, introduced in [25], has been developed further in [3, 4, 6, 7].

The idea is to start from a collection of polynomials, and then allow them to act on one another via the wedge operator, thereby producing a new set of polynomials.
Unlike in conventional constructions, here the state space generates its own dynamics. Our interest in such systems is motivated by the desire of developing an algebraic variant of some abstract models of adaptive systems and chemical interactions, where functions were made to act on other functions via composition, within the framework of \( \lambda \)-calculus\textsuperscript{9} [10]. Subsequently, a similar concept was proposed as functional dynamics on coupled map lattices\textsuperscript{11} [12] using again the composition of smooth functions as interaction.

The dynamics of self-interaction presents considerable difficulties: its phenomenology is overwhelming, while the theory, still in an embryonic stage, has yet to develop adequate links with other areas of dynamics. The purpose of this paper is to explore some aspects of this problem in an algebraic context. Thus the basic question of invariance under self-interaction will lead to periodic and pre-periodic orbits polynomials, their discriminants and Galois groups, while the simplest instances of periodicity brings connections with periodicity in some strongly chaotic systems (the iterated monomial maps, which lead to roots of unity).

Specifically, we now define the self-image of a set of irreducible polynomials to be the result of all mutual nontrivial wedge interactions, that is,

\[
\mathcal{F} : \{ f_i \} \mapsto \{ f_i \triangleright f_j \} \quad i, j \in J \quad i \neq j
\]

where \( J \) is a set of indices. We have excluded the trivial action of a polynomial on itself —see below— while the choice of global coupling (as opposed to, say, nearest neighbours), eliminates topological considerations and is justified by the fact that we will be dealing mostly with small sets.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{graph}
\caption{The graph of a stable 3-set \( \{ f, g, h \} \) over the finite field \( \mathbb{F}_3 \), where \( f(x) = x^2 + 1 \), \( g(x) = x^2 + x + 2 \), \( h(x) = x^2 + 2x + 2 \). The notation \( g \triangleright h \) indicates that \( f \) maps the roots of \( g \) into those of \( h \); accordingly, this graph represents the six equations \( h \triangleright g = g, f \triangleright g = g, f \triangleright h = g, h \triangleright f = g, g \triangleright h = g, g \triangleright f = g \).}
\end{figure}

As a phase space for the dynamical system generated by \( \mathcal{F} \), we can take any superset of \( \{ f_i \} \) with the property of being stable, that is, closed with respect to the wedge operator.
It is expedient to arrange the polynomials of a stable set as vertices of a *polynomial graph* $\Gamma$ [1] (see figure 1). Two polynomials $g$ and $h$ are joined by an oriented arc $(g, h)$ if there exists a polynomial $f$ among the vertices sending the roots of $g$ onto the roots of $h$, that is, if $f \triangleright g = h$.

In this work we confine our attention to a restricted range of problems: classifying small stable sets, analyzing simple instances of periodic behaviour, and identifying algebraic mechanisms leading to highly organized self-images. In the next section we define precisely the wedge operator, stable sets and their graphs, and classify stable 2-sets in terms of right and left invariants of the wedge operator —see figure [2]. We find that stable 2-sets originate from the existence of certain relations between a polynomial, its periodic points or its pre-images of zero (or both). In section 3 we partition polynomials into *blocks*, which are obtained by shifting the roots of a polynomial by the elements of the ground field. Blocks turn out to have organized self-images, and the self-intersection of blocks leads to appearance of right-left invariants of the wedge operator (theorem 3.3).

Quadratic polynomials are studied in detail in section 4, resulting in a fairly complete characterization of their graphs (theorem 4.1), and of the dynamics of quadratic 2-sets, in terms of a three-dimensional skew map over the ground field. We show that periodic 2-sets originate from certain roots of unity, in a field-theoretic setting not dissimilar to that of monomial maps (section 4.2).

Some aspects of self-interaction over finite fields are dealt with in section 5. We count the number of blocks (theorem 5.1), and, for quadratic polynomials and odd characteristics, the number of stable and periodic 2-sets (theorems 5.4 and 5.5). We conclude by describing the results of some experiments over finite fields, concerning the occurrence of small stable sets, and one asymptotic problem on the periodicity of quadratic 2-sets.

I am much indebted with Patrick Morton, for many illuminating discussions on various matters concerning this work.

## 2 The wedge equation

Let $K$ be a field, let $f$ and $g$ be monic (unit leading coefficient) irreducible polynomials over $K$. Let $\alpha$ be a root of $g$ and let $K(\alpha)$ be the field obtained by adjoining $\alpha$ to $K$. We assume that $K(\alpha)$ is separable (the roots of $g$ are distinct).

We represent the minimal polynomial $h$ of $f(\alpha)$ as $h = f \triangleright g$; equivalently, irreducible $h = f \triangleright g$ if and only if $g(x)$ divides $h(f(x))$. We will show (see below and [25]) that $f \triangleright g$ is a monic polynomial over $K$, which is uniquely defined by $f$ and $g$ (i.e., it is independent of the choice of the root $\alpha$ of $g$), and whose degree is a divisor of the degree of $g$. Specifically,

$$g(x) = \prod_{\alpha} (x - \alpha) \quad \implies \quad (f \triangleright g)(x) = \prod_{\alpha}^{'} (x - f(\alpha)) \quad (2)$$
where the primed product is taken over any maximal set of roots \( \alpha \) of \( g \) for which all terms are distinct. As \((f \triangleright g)(0)\) is the resultant of \( f \) and \( g \) [15, chapter 1.4], the coefficients of \( f \triangleright g \) may be regarded as generalizations of the resultant.

### 2.1 Construction of \( f \triangleright g \)

We now describe an algorithm to construct the polynomial \( h = f \triangleright g \) from \( f \) and \( g \) without computing roots, using linear algebra (see [25] for details). Let \( g \) have degree \( n \), and let \( \alpha \) be one of its roots. The extension \( K(\alpha) : K \) has degree \( n \), since \( g \) is irreducible. The field \( K(\alpha) \) is represented canonically as the quotient of the polynomial ring \( K[x] \) modulo the maximal ideal \((g) \) [28, page 32]

\[
K(\alpha) \cong K[x]/(g(x)),
\]

meaning that the polynomials in \( K[x] \) are replaced by their remainder upon division by \( g(x) \). Under this isomorphism, the root \( \alpha \) is identified with the residue class of \( x \).

The polynomials \( 1, x, x^2, \ldots, x^{n-1} \) form a basis of \( K[x]/(g(x)) \) over \( K(\alpha) \)

\[
M = \{ m_{i,j} \}
\]

over \( K \) given by

\[
f(x) \cdot x^{k-1} \equiv m_{1,k} + m_{2,k}x + \cdots + m_{n,k}x^{n-1} \pmod{g(x)} \quad k = 1, \ldots, n.
\]

It can be shown that \( h \) is the minimal polynomial of \( M \), and that the Jordan form of \( M \) has \( r \) identical blocks along the diagonal, for some integer \( r \). This means that the characteristic polynomial of \( M \) takes the form \((h)^r\), and hence the degree of \( h \) is a divisor of that of \( g \). Such divisor is proper whenever the action of \( f \) on the roots of \( g \) is not injective, or, equivalently, whenever \( K(f(\alpha)) \) is a proper subfield of \( K(\alpha) \), for each root \( \alpha \) of \( g \).

### 2.2 Stable sets and their graphs

A set \( S \) of irreducible polynomials is said to be stable if it contains its self-image \( \mathcal{F}(S) \), defined via the wedge operator in [11]. Because a polynomial over a field \( K \) leaves every algebraic extension of \( K \) invariant, “large” stable sets are naturally constructed by means of field extensions. In particular, the set of minimal polynomials of all the elements of a finite extension \( K(\alpha) : K \) is stable; we denote it by \( S(f) \), where \( f \) is any irreducible monic polynomial with a root \( \beta \) such that \( K(\beta) = K(\alpha) \). One sees that this definition does not distinguish between conjugate fields. A prominent subset of \( S(f) \) is

\[
E(f) := \{ g \in S(f) \mid S(g) = S(f) \}
\]
which contains only the polynomials generating the top field. The set $E(f)$ is not stable, in general. Furthermore, given $f, g \in K[x]$, the sets $E(f)$ and $E(g)$ are either disjoint or one is contained in the other. An example is given in figure 1 where we display all quadratic irreducible polynomials over $F_3$; in this case $E(f) = E(g) = E(h) = \{f, g, h\}$.

The graph $\Gamma(S)$ of a stable set $S$ is the directed graph whose vertices are the elements of $S$, and where there exists an arc $(g, h)$ from $g$ to $h$ if $f \triangleright g = h$ for some $f$ in $S$. For each arc $(g, h)$ we consider the collection $\omega$ of all polynomials $f$ such as $f \triangleright g = h$. The cardinality of $\omega$ will be called the multiplicity of the arc $(f, g)$. To make $\omega$ explicit, we write $g \overset{\omega}{\rightarrow} h$ in place of $(g, h)$, see figures 1–3.

Graphs arising from polynomials of degree one are straightforward: for all $a, b \in K$, the polynomial $f(x) = x + b - a$ is the unique polynomial sending the root of $g(x) = x - a$ to that of $h(x) = x - b$. Thus $\Gamma$ is a complete graph, and all arcs have multiplicity one. The quadratic case is already non-trivial — see section 4. In general case, some information on $\Gamma(S)$ is obtained by restricting vertices to the subsets $E(f)$ of $S$ defined in (5); the resulting subgraphs will be called extension graphs. In an extension graph of degree $n$, the multiplicity of each arc is at most $n$. This is a consequence of the following finiteness result

**Proposition 2.1** Let $g$ and $h$ be monic irreducible polynomials of positive degree $n$ and $m$, respectively. Then, for every integer $d$, with $1 \leq d \leq n$, there are at most $m$ polynomials $f$ of degree $d$, such that $f \triangleright g = h$.

**Proof.** Let $g, f_1, f_2 \in K[x]$ be non-constant monic polynomials, with $g$ irreducible and $\deg f_2 \leq \deg f_1 \leq n$. Let $\alpha$ be a root of $g$, and let $f_1(\alpha) = f_2(\alpha)$. We begin to show that if $f_1$ and $f_2$ have the same degree, they coincide; otherwise, $\deg f_1 = n$, and $g = f_1 - f_2$.

Let $l = f_1 - f_2$. Then $l(\alpha) = 0$, and since $\deg l \leq n$ and $g$ is the minimal polynomial of $\alpha$, we have either $l = 0$ or $\deg l = n$, with $l$ a constant multiple of $g$. If $f_1$ and $f_2$ have the same degree, then the degree of $l$ is lower (because $f_1$ and $f_2$ are monic), so that $l = 0$, and $f_1 = f_2$. If their degrees are different, then $f_1$ must have degree $n$, and since $f_1$ is monic, we have $l = g$ as claimed.

Let now $\beta = f(\alpha)$ be a root of $h$, with $f$ a monic polynomial of degree $d \leq n$. We have shown that such $f$, if it exists, is unique. There are $m$ possible choices of $\beta$ among the roots of $h$, giving as many polynomials, not necessarily irreducible. The transitivity of the Galois group of $g$ means that the action of $f$ on the roots of $g$ is uniquely determined by the image of the root $\alpha$, so there are no other polynomials. This completes the proof. $\square$

5
2.3 Wedge invariants and stable 2-sets

The search for small stable sets begins from the study of right and left invariance under the wedge operator

\[(i) \quad f \triangleright g = g \quad \text{and} \quad (ii) \quad g \triangleright f = g.\]  

In equations \((i)\) and \((ii)\), we say that \(g\) is a right and a left wedge invariant of \(f\), respectively. These invariants turn out to have dynamical significance.

Right invariants. They originate from periodic points. To see this we note that if \(g\) is a right invariant of \(f\), then \(f\) maps the roots of \(g\) into themselves. In fact from the irreducibility of \(g\) and the transitivity of its Galois group, it is easy to see that \(f\) must permute the roots of \(g\), that is, the roots of \(g\) are periodic orbits of \(f\) (for Galois theory of periodic orbits see [27, 19]). To construct solutions \(g\) of (6), we let \(f^n\) be the \(n\)-th iterate of \(f\) (with \(f^0(x) = x\)). Then the roots of the polynomial \(f^n(x) - x\) are the periodic points of \(f\) of period dividing \(n\); to eliminate spurious periods, we consider the polynomial

\[
\Phi_{n,f}(x) = \prod_{d|n}(f^d(x) - x)^{\mu(n/d)} \quad n = 1, 2, \ldots
\]

where \(\mu\) is the Möbius function [1, chapter 2]. The roots of \(\Phi_{n,f}\) are periodic points of \(f\) of essential period \(n\) [20], which is the minimal period apart, possibly, at bifurcations [21]. It follows that every right invariant of \(f\) is an irreducible factor of \(\Phi_{n,f}\), for some \(n\). The converse is not true: if \(g\) is an irreducible factor of \(\Phi_{n,f}\), all we can say is that \(g\) is a right invariant of \(f^d\), for some divisor \(d\) of \(n\). In particular, if \(\Phi_{n,f}\) is irreducible, then \(f \triangleright \Phi_{n,f} = \Phi_{n,f}\). (The polynomial \(\Phi_{n,f}\) is 'generically' irreducible, that is, irreducible over \(K = \bar{Q}\), when the coefficients of \(f\) are regarded as indeterminates [18].)

Left invariants. They originate from pre-images of zero. Let us consider the functional equation \(f^k \triangleright f^n = f^{n-k}, \quad n \geq k,\) ignoring irreducibility for the moment (the polynomial \(f^n\) is generically irreducible over any field of characteristic zero [22]). Letting \(n = 2k\) and \(g = f^k\), we obtain \(g \triangleright g^2 = g\). Thus, \(g\) is a left invariant of any irreducible factor of \(g^2\). Conversely, if \(g\) is a left invariant of \(f\), and \(\alpha\) is a root of \(f\), then \(g(g(\alpha)) = 0\), that is, \(f\) is an irreducible factor of \(g^2\). This construction is straightforward in the degree one case: for all \(0 \neq a \in K\), the polynomial \(x + a\) is a left invariant of \(x + 2a\).

Right and left invariants are not completely unrelated; in section 3 we shall establish a sufficient condition for their simultaneous occurrence (theorem 3.3).

Three different types of stable 2-sets can be constructed by combining right and left invariants in all possible ways, as illustrated in figure 2. Type I and II stable 2-sets consist of two right and two left invariants, respectively; they are fixed points of the mapping \(F\) — see equation [1]. The case of mixed invariants is denoted as type III; its self-image is the right-left invariant.
Figure 2: Stable 2-sets \( \{f, g\} \). Type I: two right invariants \((f \triangleright g = g \text{ and } g \triangleright f = f)\). Type II: two left invariants \((f \triangleright g = f \text{ and } g \triangleright f = g)\). Type III: mixed invariants \((f \triangleright g = g \text{ and } g \triangleright f = g)\). Types I and II sets are invariant under \( \mathcal{F} \), while type III collapses onto \( \{g\} \).

We will arrive to a complete description of quadratic stable 2-sets in sections 4 and 5. Type I and III are easily constructed, while type II do not exist, requiring at least cubic polynomials (theorem 4.4).

A specific family of type I stable sets can be constructed, involving polynomials of arbitrarily large degree. Consider a non-constant monic polynomial \( f \) over \( K \). Then the sets

\[
\{f(x^2), f(x^2) - x\} \quad \text{char}(K) \neq 2 \\
\{f(x), f(x) - x\} \quad \text{char}(K) = 2
\]

are stable of type I whenever the polynomials involved are irreducible (\( \text{char}(K) \) denotes the characteristic of \( K \), see [15, chapter 1.2]).

To see this, let \( g(x) = f(x^2) \), with \( \text{char}(K) \neq 2 \). Then \( g(x) - x = \Phi_{1,g}(x) \) is a right invariant of \( g \). Furthermore, if \( \alpha \) is a root of \( g \), then \( \Phi_{1,g}(\alpha) = -\alpha \) is a root of \( \Phi_{1,g} \triangleright g \). Therefore, for \( g \) to be a right invariant of \( \Phi_1 \), it suffices that \(-\alpha\) also be a root of \( g \), which is true since \( g(x) = f(x^2) \). It follows that the set (8) is a type I stable set (pending irreducibility, that is); the first polynomial induces the identity permutation of the root of the second, while the second induces 2-cycles on the roots of the first. In particular, \( g \) is an irreducible factor of \( \Phi_{2,h} \), where \( h = \Phi_{1,g} \). If \( \text{char}(K) = 2 \), the polynomials in (9) are the \( \Phi_1 \)-polynomial of each other.

For example, the polynomial \( f(x) = x^2 + 1 \) gives rise to the following stable 2-set of type I over \( \mathbb{Q} \)

\[
\{x^4 + 1, x^4 - x + 1\}.
\]
3 Blocks

A block is a maximal collection of polynomials whose roots differ by elements of the ground field. Blocks turn out to have “small” and well-structured self-images. These will be studied in section 3.2, where we derive a sufficient condition for degree invariance of the self-image of a block (proposition 3.2), and we show that intersection of a block with its self-image leads to right and left invariants of the wedge operator (theorem 3.3). Before that, we establish the notation and provide some preliminary results. Since the polynomials in a block share the same discriminant, the study of discriminants will become relevant.

3.1 Preliminaries

We begin with the group $G$ of matrices

$$
\sigma_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \quad a, b \in K, \quad a \neq 0
$$

which we let act on irreducible polynomials as follows

$$
\sigma(f)(x) = a^{-\deg f} f(ax + b). \tag{10}
$$

The polynomial $\sigma(f)$ is monic and irreducible, and since $\sigma_{c,d}(\sigma_{a,b}(f)) = (\sigma_{c,d}\sigma_{a,b})(f)$, equation (10) defines an action of $G$ on the set $E(f)$, which was defined in (5). The orbits of $G$ partition the vertices of every extension graph into clusters.

We consider the additive subgroup

$$
G^+ = \{\sigma_{1,b}\} \quad \sigma_{1,b} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad b \in K. \tag{11}
$$

Its orbits are blocks, which subdivide each cluster. We denote blocks by $\Theta$ and the block containing $f$ by $\Theta_f$. Introducing the short-hand notation

$$
f_b^+ := \sigma_{1,b}(f)
$$

we have $\Theta_f = \{f_b^+ \mid b \in K\}$. Now, if $\Theta_g = \Theta_h$, then $h = g_b^+$, for some $b$. But then $h = f \triangleright g$ with $f(x) = x - b$, that is, the action of $G^+$ can be represented in terms of the wedge operator.

Let us denote the discriminant of $f$ by $\Delta(f)$. In the following lemma we collect miscellaneous results on the action of $G$, to be used in later sections. From part (iii) we find that the discriminant is a block invariant.

**Lemma 3.1** Let $f$ and $g$ belong to a stable set, let $n = \deg f$ and let $\sigma_{a,b}$ be an arbitrary element of $G$. The following holds:
(i) \( \sigma_{a,b}(\Theta f) = \Theta \sigma_{a,b}(f) \).

(ii) \( \sigma_{a,b}(f) \triangleright \sigma_{a,b}(g) = \sigma_{a^\prime,0}(f \triangleright g) \).

(iii) \( \Delta(\sigma_{a,b}(f)) = \Delta(f)/a^n(n-1) \).

(iv) If \( f, g \in \Theta \), then, for all \( b \in K \), we have \( f \triangleright f^+ b = g \triangleright g^+_b \).

Proof. If \( g \in \Theta f \), then \( \sigma(\triangleright f^+ g) = g \) for some \( \sigma \in G^+ \), whence
\[
\sigma(g) = \sigma\sigma^+(f) = (\sigma\sigma^+\sigma^{-1})\sigma(f).
\]
Because \( G^+ \) is a normal subgroup, we have that \( \sigma\sigma^+\sigma^{-1} \in G^+ \), so that \( \sigma(g) \) is in the same block as \( \sigma(f) \). Furthermore, \( \sigma \) is bijective, because (10) defines a group action. This proves the first assertion. To prove (ii), let \( g(\alpha) = 0 \). With reference to (2) and (10), we find
\[
\sigma_{a,0}(f \triangleright g)(x) = \prod'_\alpha \left( x - a^{-n}f(\alpha) \right);
\quad
(\sigma_{a,b}(g))(x) = \prod'_\alpha \left( x - a^{-1}(\alpha - b) \right).
\]
from which we obtain
\[
(\sigma_{a,b}(f) \triangleright \sigma_{a,b}(g))(x) = \prod'_\alpha \left[ x - a^{-n}f(aa^{-1}(\alpha - b) + b) \right] = \prod'_\alpha \left( x - a^{-n}f(\alpha) \right)
\]
as required. Part (iii) follows from the discriminant formula for a monic polynomial [15, chapter 1.4]
\[
\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2
\]
where \( \alpha_k \) are the roots of \( f \), and the fact that \( \sigma_{a,b}(f) \) has the same degree as \( f \).

Now, let \( g, f \in \Theta \), so that \( g = f^+_c \), for some \( c \in K \). Then, from (ii) above, we have
\[
g \triangleright g^+_b = \sigma_{1,c}(f) \triangleright \sigma_{1,b}\sigma_{1,c}(f)
= \sigma_{1,c}(f) \triangleright \sigma_{1,c}\sigma_{1,b}(f)
= f \triangleright f^+_b.
\]
This proves (iv). \( \square \)
3.2 Self-image of blocks

The self-image $\mathcal{F}(\Theta)$ of a block $\Theta$, given by equation (1), consists of all polynomials of the type $f \triangleright f_b^+$, with $f \in \Theta$ and $b$ a non-zero element of $K$. From lemma 3.1 (iv), it follows that $f \triangleright f_b^+$ does not depend on the choice of $f$ in $\Theta$, and therefore the self-image of a block is highly degenerate. In particular, we find sufficient conditions for degree invariance, and for the existence of wedge invariants.

**Proposition 3.2** Let $\Theta$ be a block of degree $n$, where $n$ is prime and $\text{char}(K) \neq n$. Then the self-image of $\Theta$ has degree $n$.

**Proof.** Let $\Theta = \Theta_f$, and let $\alpha$ be a root of $f$. If $b \neq 0$, the polynomial $f \triangleright f_b^+$ has root $f(\alpha - b) = -n b \alpha^{n-1} + \cdots$, which is a polynomial in $\alpha$ of degree $n-1$, since, by assumption, $bn \neq 0$. Because $n$ is prime, the degree of $f(\alpha - b)$ is either $n$ or 1. In the latter case, if $f(\alpha - b) = d \in K$, then we have $f(\alpha - b) - d = 0$, which is impossible since $\alpha$ is algebraic of degree $n$. So the degree of $f \triangleright f_b^+$ is the same as that of $f$.

**Theorem 3.3** If a block $\Theta$ intersects its self-image, then $\Theta$ contains a polynomial which is a right-left invariant of two polynomials in the same block.

**Proof.** By assumption, a polynomial $f$ exists such that $f \triangleright f_b^+ = f_c^+$ for some $b, c \in K$, with $b \neq 0$. Then, letting $\theta = f_c^+$, from lemma 3.1 (iv) we obtain

$$\theta_{-b}^+ \triangleright \theta = \theta \quad \theta \triangleright \theta_b^+ = \theta,$$

that is, $\theta$ is the desired right-left invariant of the wedge operator.

If, with the above notation, one also has that $\theta_{-b}^+ \triangleright \theta = \theta$, then the self-intersection of a block yields two stable 2-sets of type III, namely $\{\theta, \theta_{-b}^+\}$. One verifies that this is the case precisely when $\theta(\alpha + b)$ and $\theta(\alpha - b)$ are algebraic conjugates, which always happens for quadratic polynomials — see section 4.1.

An instance of this phenomenon is shown in figure 1. The quadratic extension graph of $\mathbb{F}_3$ consists of a single block, which intersects (indeed, contains) its self-image, due to proposition 3.2, giving rise to the right-left invariant $g$, and to two stable 2-sets of type III.

If we now let $\mathcal{B}$ be the set of blocks of an extension, the mapping

$$\mathcal{F}_b : \mathcal{B} \to \mathcal{B} \quad \Theta_f \mapsto \Theta_{f \triangleright f_b^+} \quad 0 \neq b \in K$$

is well-defined. By means of $\mathcal{F}_b$ we can construct an oriented graph, whose vertices are blocks, and where two blocks $\Theta$ and $\Theta'$ are joined by an arc if $\Theta'$ belongs to the self-image of $\Theta$. This graph, called the block graph, contains the essential information on all self-interactions: it will be studied in the next section for the quadratic case.
4 Quadratic polynomials

Throughout this section, \( f \) denotes a quadratic monic irreducible polynomial over a field \( K \), with discriminant \( \Delta(f) \). We first describe the graphs of a quadratic extension (theorem 4.1), and characterize the transitions to the ground field (proposition 4.3).

Then we construct stable two sets, and derive a three-dimensional skew-map describing the dynamics of 2-sets, with which we compute periodic points. It turns out that for periodic 2-sets to exist, the ground field \( K \) must contain certain roots of unity. In this respect, the situation is not dissimilar from that of periodic orbits of the monomial maps \( z \mapsto z^k \), for which the \( \Phi \)-polynomials —cf. equation 4— are cyclotomic polynomials.

4.1 Graphs

The quadratic extension graphs have a particularly simple form.

**Theorem 4.1** A quadratic extension graph consists of a single cluster, whose distinct blocks have distinct discriminants. If \( \text{char}(K) \neq 2 \), then the block-graph is a complete graph, and the set of mappings \( F_b \), defined in (13), form a group of permutations of blocks, isomorphic to the multiplicative group of \( K^2 \). The isomorphism associates \( b^2 \in (K^*)^2 \) to the permutation sending the block \( \Theta \) to \( F_{b/2}(\Theta) \).

The completeness of the block graph means that the diameter of the extension graph is at most two, combining polynomials of degree 1 and 2. This holds in a strong sense, namely for every quadratic polynomials \( f \) and \( g \) there exist elements \( b \) and \( c \) in \( K \) such that \( (f \circ f)^+ + b = g \).

We need a lemma:

**Lemma 4.2** For every quadratic polynomial \( f \) and every \( b \in K \), the following holds

(i) \((f \circ f^+_b)(x) = (x - b^2)^2 - b^2 \Delta(f)\).

(ii) \(\Delta(f \circ f^+_b) = (2b)^2 \Delta(f)\).

(iii) If \( \text{char}(K) \neq 2 \), then the polynomials \( f \circ f^+_a \) and \( f^+_b \circ f^+_c \) belong to the same block if and only if \( a = \pm c \), in which case they coincide.

**Proof.** The first two identities are verified by direct calculation. To prove (iii), we first reduce it to the case \( b = 0 \), from lemma 3.4(ii). Then from (i) above, we have that if \( f \circ f^+_a \) and \( f^+_b \circ f^+_c \) belong to the same block, then for some \( d \in K \)

\[(x + d - a^2)^2 - a^2 \Delta(f) = (x - c^2)^2 - c^2 \Delta(f)\]
which implies that \( d = 0 \) and \( a^2 = c^2 \). Conversely, if \( a = \pm c \), from part (i) above and lemma 3.1(ii), we have that \( f \triangleright f_a^+ = f_b^+ \triangleright f_b^+ = f_b^+ \triangleright f_b^+ \).

Proof of theorem 4.1 If \( \alpha \) is a root of \( f \) and \( g \) is an irreducible polynomial in the same extension, then the roots of \( g \) are linear expressions in \( \alpha \) with coefficients in \( K \). Thus, for some \( a, b \in K \), we have that \( \sigma_{a,b}(f) = g \), i.e., there is a single cluster. Now, from lemma 3.1(iii) we have \( \Delta(\sigma_{a,b}(f)) = \Delta(f)/a^2 \), so distinct values of \( a^2 \) correspond to distinct discriminants. Now let \( S \) be the sum of the roots of \( f(x) \). One verifies that \( \sigma_{a,b}(f) = \sigma_{1,b}(\sigma_{-a,b}(f)) \) which shows that \( \sigma_{a,b}(f) \) and \( \sigma_{-a,b}(f) \) belong to the same block, and so blocks are parametrized by discriminants.

Let \( \text{char}(K) \neq 2 \). To show that the block graph is complete, we consider the equation \( F_b(\Theta f) = \Theta f \triangleright f_b^+ = \Theta g \) where \( f \) and \( g \) are given quadratic irreducible polynomials, with \( E(f) = E(g) \). We look at discriminants. Because our extension is separable, and all discriminants are square multiples of the field discriminant, we have \( \Delta(g) = k^2\Delta(f) \), for some \( 0 \neq k \in K \). This, together with lemma 4.2(ii), gives the equation \( k^2 = (2b)^2 \), which can be solved for \( b \), since \( \text{char}(K) \neq 2 \). Matching discriminants suffices, since we have seen that discriminants identify blocks.

We show that \( F_b \) is injective. If \( \Theta \) and \( \Theta' \) are distinct blocks, they have distinct discriminants, \( \Delta \) and \( \Delta' \), say. But then

\[
\Delta(F_b(\Theta f)) = 2b^2\Delta \neq 2b^2\Delta' = \Delta(F_b(\Theta g))
\]

which shows that \( F_b(\Theta) \neq F_b(\Theta') \), as desired. To prove surjectivity, we must solve for \( f \) the equation \( F_b(\Theta f) = \Theta g \), for given \( b \) and \( g \). From what was proved above, this amounts to find \( f \) such that \( \Delta(f)(2b)^2 = \Delta(g) \); since \( \text{char}(K) \neq 2 \), we can take \( f = \sigma_{2b,0}(g) \).

Thus, if \( \text{char}(K) \neq 2 \), each non-zero value of \( b \) defines a permutation of blocks. Now consider the mapping \( \mu : b^2 \mapsto F_{b/2} \) sending \((K^*)^2\) to the symmetric group on \( B \). The choice of \( b \) among the square roots of \( b^2 \) is irrelevant, due to lemma 4.2(iii). From the same lemma, part (ii), we see that \( \mu \) associates to \( b^2 \) the permutation sending the block of discriminant \( \Delta \) to that of discriminant \( b^2\Delta \). Keeping this in mind, we find that

\[
\mu((bc)^2) = F_{bc/2} = F_{b/2} \circ F_{c/2} = \mu(b^2)\mu(c^2)
\]
e.g., \( \mu \) is a group homomorphism. Its kernel is trivial, \( \mu(1^2) = \mathcal{F}_{1/2} \), and so \( \mu \) defines a faithful action of \((K^*)^2\) on \( \mathcal{B} \).

Thanks to theorem \( \text{3.3} \), the identity permutation \( \mathcal{F}_{1/2} \) maps the whole block to a right-left invariant of the wedge operator, which, from lemma \( \text{4.2}(i) \), is given by

\[
\theta(x) = \left( x - \frac{1}{4} \right)^2 - \frac{\Delta}{4}
\]

where \( \Delta \) is the block discriminant. From lemma \( \text{4.2}(iii) \), this polynomial is unique: we call it the centre of the block. Because \( \theta = \theta \triangleright \theta^+_{1/2} = \theta \triangleright \theta^+_{-1/2} = \theta^+_{1/2} \triangleright \theta = \theta^+_{-1/2} \triangleright \theta \), we obtain the following type III stable sets

\[
\{ \theta, \theta^+_{1/2} \} \quad \{ \theta, \theta^+_{-1/2} \} \quad \text{char}(K) \neq 2
\]

which are distinct and in bi-unique correspondence with the block discriminants \( \Delta \in K \). An example is given in figure 1 with \( g = \theta, h = \theta_{1/2}, \) and \( f = \theta_{-1/2} \). (Note however, that the set \( \{ \theta, \theta^+_{1/2}, \theta^+_{-1/2} \} \), which is stable in figure 1, is not stable in general.)

In the following table, we display all parametrized families of quadratic stable 2-sets, for \( \text{char}(K) \neq 2 \). The absence of quadratic stable 2-sets of type II results from theorem \( \text{4.4} \) below.

**Table I: Quadratic Stable 2-sets**

| \( f \)       | \( g \)       | type | \( f = \Phi_{2,g} \) | \( g = \Phi_{1,f} \) |
|---------------|---------------|------|---------------------|---------------------|
| \( x^2 + r \) | \( x^2 - x + r \) | I    | \( f \)            | \( g \)            |
| \( x^2 + \frac{1}{2}x + r \) | \( x^2 - \frac{1}{2}x + r \) | III  | \( f|g^2 \)        | \( g = \Phi_{1,f} \) |
| \( x^2 - \frac{3}{2}x + \frac{1}{2} + r \) | \( x^2 - \frac{1}{2}x + r \) | III  | \( f|g^2 \)        | \( g = \Phi_{2,f} \) |

All polynomials are irreducible over \( \mathbb{Q}(r) \), where \( r \) is regarded as an indeterminate; if instead \( r \) is as a specific element of \( K \), then irreducibility must be checked. The last two columns describe the mutual relation between \( f \) and \( g \), in the notation of section \( \text{2.3} \). The type I set is of the form \( \Phi_{2,g} \), with one of the two polynomials having zero middle coefficient, as explained in section \( \text{4.2} \). The two type III sets are rooted at the block centre \( g = \theta \), and correspond to the two possible permutations of the roots of \( g \) by \( f \) (cf. equations \( \text{14,15} \), with \( r = (1 - \Delta)/4 \)).

The last result of this section characterizes some transitions to the ground field. For \( \text{char} K \neq 2 \), this characterization is complete.
Proposition 4.3 For every quadratic polynomials \( f \) and \( g \), and every \( b \in K \), if \( E(f) \) has more than one block, then the polynomial \( (f \triangleright f^+_b) \triangleright (g \triangleright g^+_b) \) has degree one. Conversely, if \( \text{char}(K) \neq 2 \) and \( h \triangleright l \) has degree 1, with \( h \) and \( l \) quadratic not belonging to the same block, then there exists \( c \in K \) such that
\[
h = (\theta_h)^+ \quad l = (\theta_l)^+
\]
where \( \theta_h \) and \( \theta_l \) are the centres of the respective blocks.

Under the above assumptions, we have \( \mathcal{F}^2(E(f)) \not\subset E(f) \), that is, some polynomials in the second self-image of a quadratic extension collapse onto the ground field.

Proof. If \( \alpha \) is a root of \( l = g \triangleright g^+_b \), then, from lemma 4.2 (i), we have that \( (\alpha - b^2)^2 = b^2 \Delta(g) \), and therefore, letting \( h = f \triangleright f^+_b \), the root \( h(\alpha) \) of \( h \triangleright l \) is given by
\[
h(\alpha) = b^2 (\Delta(g) - \Delta(f)) \in K.
\] (16)
This proves the first statement. Conversely, assume that \( h \triangleright l \) has degree 1, and let \( \theta_h = h \triangleright h^+_{1/2} \) and \( \theta_l = l \triangleright l^+_{1/2} \) be the centres of the respective blocks. Then \( \theta_h \triangleright \theta_l \) has degree 1, from the above. Solving for \( c \) the equation \( h = (\theta_h)^+_c \), gives \( c = B/2 + 1/4 \), where \( B \) is the middle coefficient of \( h(x) \). If \( r \in K \) is the root of \( h \triangleright l \), then \( h(x) - l(x) = r \), and hence \( \Delta(h) - \Delta(l) = -4r \). The equation \( l = (\theta_l)^+_d \) now reads
\[
(x + d - \frac{1}{4})^2 - \frac{\Delta(l)}{4} = (x + d - \frac{1}{4})^2 - \frac{\Delta(h)}{4} - r = l(x) = h(x) - r
\]
with the solution \( d = B/2 + 1/4 = c \).

4.2 Periodic 2-sets

We describe the periodic behaviour of 2-sets \( \{f, g\} \), where \( f \) and \( g \) are quadratic polynomials of discriminants \( \Delta(f) \) and \( \Delta(g) \), and \( \text{char}(K) \neq 2 \). Let \( \mathcal{F}(\{f, g\}) = \{f', g'\} \), with \( f' = f \triangleleft g \) and \( g' = g \triangleleft f \). Since \( f'(0) = g'(0) = \text{Res}(f, g) \) (see remark following equation (2)), without loss of generality, we let
\[
f = x^2 + bx + r \quad g = x^2 + cx + r.
\]
The corresponding primed coefficients are computed as
\[
b' = c(b - c) \quad c' = -b(b - c) \quad r' = r(b - c)^2.
\]
Defining
\[
u = b - c \quad v = b + c \quad (17)
\]
we obtain a three-dimensional skew map over $K$

$$\Psi : K^3 \to K^3 \quad (u, v, r) \mapsto (\pm uv, -u^2, ru^2)$$

(18)

where the change of sign corresponds to exchanging $f$ and $g$, from (17). Iteration gives (ignoring sign change)

$$\Psi^t(u, v, r) = \begin{cases} (z_t/u, -z_t/v, r(z_t/uv)^2) & t \text{ odd} \\ (-u z_t, -v z_t, rz_t^2) & t \text{ even} \end{cases} \quad t > 0$$

(19)

where

$$z_t = (u^2 v)^{e_t} \quad e_t = \frac{1}{3} [2^t + (-1)^{t+1}] \quad t = 1, 2, \ldots$$

(20)

The sequence $e_t = 1, 1, 3, 5, 11, 21, 43, 85, 171, 341, \ldots$ satisfies the recursion relation $e_{t+1} = e_t + 2e_{t-1}$, with initial conditions $e_1 = e_2 = 1$.

From (18) we find

$$(u, 0, r) \mapsto (0, -u^2, ru^2) \mapsto (0, 0, 0)$$

and so, in order not to collapse to the trivial solution, we must have $u vr \neq 0$. Since the discriminants of $f$ and $g$ evolve as

$$\Delta(f') = u^2 \Delta(g) \quad \Delta(g') = u^2 \Delta(f)$$

(21)

one sees that if $f$ and $g$ are irreducible (in particular, $r \neq 0$), and their discriminants are distinct ($uv \neq 0$), these properties are preserved along the orbit.

The periodic points equation reads

$$\Psi^t(u, v, r) = (\pm u, v, r). \quad t > 0$$

(22)

We have two cases, depending on the parity of $t$. To unify the notation, we define

$$d_t = \begin{cases} 3e_t - 2 = 2^t - 1 & t \text{ odd} \\ e_t = (2^t - 1)/3 & t \text{ even} \end{cases} \quad t > 0,$$

(23)

with $e_t$ as in (20).

i) Odd period. When $t$ is odd, using (19), we find no irreducible solution corresponding to the positive sign in (22). In particular, for $t = 1$, we have

**Theorem 4.4** If $\text{Char}(K) \neq 2$, there are no quadratic stable sets of type II over $K$.

For the negative sign in (22), we find

$$v^{d_t} + 1 = 0 \quad u = \pm v$$

(24)
for one choice of sign, as changing sign amounts to exchanging polynomials. The sign alternates along each orbit, and in every element of a cycle of odd period, precisely one of the two polynomials has zero middle coefficient. We see that \( v = \zeta \), where \( \zeta \) is a \( 2d_t \)-th root of unity (for background references on roots of unity, see, e.g., [17] page 39 or [11] chapter 27). For every root of unity, there is a one-parameter family of solutions, parametrized by \( K \setminus K^2 \), which corresponds to varying \( r \) while keeping the polynomials irreducible. When \( t = 1 \), we recover the type I stable set displayed in Table I. Because \( d_t > 1 \) for \( t > 2 \), odd cycles with period greater than one can exist only if \( K \) contains non-trivial roots of unity.

\textit{ii)} Even period. When \( t \) is even, we find no solution of (22) corresponding to the negative sign (unless \( \text{char}(K) = 2 \), which we have excluded). For the positive sign, we obtain
\[
(u^2v)^{d_t} + 1 = 0
\]
that is, \( u^2v = \zeta \), where \( \zeta \) is a \( 2e_t \)-th root of unity. For each solution of this equation, we have again a one-parameter family of periodic points. Solving (25) for \( t = 2 \), gives the 2-cycle \( \{f_0, g_0\} \leftrightarrow \{f_1, g_1\} \), irreducible over \( \mathbb{Q}(r, s) \)
\[
\begin{align*}
f_0 &= x^2 - \frac{s^3 + 1}{2s} x + r \\
g_0 &= x^2 - \frac{s^3 - 1}{2s} x + r \\
f_1 &= x^2 + \frac{s^3 - 1}{2s^2} x + \frac{r}{s^2} \\
g_1 &= x^2 - \frac{s^3 + 1}{2s^2} x + \frac{r}{s^2}.
\end{align*}
\]
As above, even cycles with period greater than two require non-trivial roots of unity.

In the above construction, if \( \zeta \) is a primitive \( 2d_t \)-th root of unity, then the period \( t \) is minimal. This follows from the fact that if \( t' \) is a proper divisor of \( t \), then \( d_{t'} \) is a proper divisor of \( d_t \) —see equation (23). So \( 2d_t \)-th roots of unity are needed to build all cycles of minimal period \( t \). However, orbits of the same minimal period may originate from some roots of unity of lower order, and indeed the problem of determining the minimal order for a given period —the \( t \)-cycles of minimal complexity— is also of interest (cf. [26]). To compute such orders, we consider all divisors of \( d_t \), and remove from them the divisors of \( d_{t'} \), for all \( t' < t \) such that \( t' \) divides \( t \) and has the same parity as \( t \). Call \( D_t \) the resulting set of divisors. The parity condition is justified as follows. If \( t \) is even and \( t' \) is odd (this is the only possibility), and \( d \in D_t \) is a common divisor of \( d_t \) and \( d_{t'} \), then the set of solutions of equation (23) for the exponent \( d \) is larger than that of equation (24) for the same exponent.

In the table below, we display the (half)-orders \( d_t \) of the roots of unity needed to construct periodic 2-sets of quadratic polynomials, for all periods \( t \leq 14 \).
Table II: Roots of unity for quadratic periodic 2-sets

| period t | order $d_t$ |
|----------|-------------|
| 1        | 1           |
| 2        | 1           |
| 3        | 7           |
| 4        | 5           |
| 5        | 31          |
| 6        | 21, 7, 3    |
| 7        | 127         |
| 8        | 85, 17      |
| 9        | 511, 73     |
| 10       | 341, 31, 11 |
| 11       | 2047, 89, 23|
| 12       | 1365, 455, 273, 195, 105, 91, 65, 39, 35, 15, 13 |
| 13       | 8191        |
| 14       | 5461, 127, 43 |

Of note are the large fluctuations of arithmetical origin, and the close relation between the fields $K$ needed to construct these periodic sets, and the fields that contain the periodic points of the monomial maps $z \mapsto z^2$, which are $(2^t - 1)$th roots of unity.

5 Finite fields

In this section we consider self-interacting polynomials over a finite field $K = \mathbb{F}_q$ with $q$ elements, where $q = p^k$, $p$ prime (for background information on finite fields, see [15]). Because a finite field has a unique extension of degree $n$ for any $n$, any stable set consisting of polynomials of bounded degree is also finite. Here we address some natural counting questions (number and size of blocks, number of stable 2-sets, number of periodic orbits, etc.). Furthermore, we construct explicitly the periodic quadratic 2-sets described in the previous section, and investigate numerically the occurrence of stable sets of higher degree.

We denote the stable set of all irreducible polynomials of degree $n$ over $\mathbb{F}_q$ by $E(q^n)$, without reference to polynomials — cf. equation (5). Clearly, each block of $E(q^n)$ contains at most $q$ polynomials, but it may have fewer of them, and in some cases a block may even consist of a single polynomial, a so-called affine $q$-polynomial [15 chapter 3.4]. However, if $n$ is coprime to $q$, the block size is maximal, and we have

**Theorem 5.1** If $\gcd(q, n) = 1$, then the number of blocks in the extension graph of degree $n > 1$ over $\mathbb{F}_q$ is given by

$$\frac{1}{nq} \sum_{d|n} \mu(d) q^{n/d}$$

(26)
where $\mu$ is the M"{o}bius function.

The proof of this theorem will require the following lemma.

**Lemma 5.2** Let $g$ be an irreducible polynomial over a field $K$. If $g = g_0^+$, for some $b \neq 0$, then $\text{char}(K) > 0$ and the degree of $g$ is divisible by $\text{char}(K)$.

**Proof.** We first show that if $\alpha$, $\alpha + b$ and $\beta$ are roots of $g$, so is $\beta + b$. Let $\tau$ be an element of the Galois group of $g$, sending $\alpha$ to $\beta$. Then $\beta + b = \tau(\alpha) + b = \tau(\alpha + b)$, showing that $\beta + b$ is conjugate to $\alpha + b$. Now, let $H$ be the collection of elements $b$ of $K$ for which $\alpha + b$ is a root of $g$. Then $H \neq \{0\}$, by hypothesis, and it is an additive group, as seen from repeated applications of the above argument. It follows that $\text{char}(K) > 0$ and that the subgroup $\langle b \rangle$ of $H$ has order $p := \text{char}(K)$, and so the order of $H$ is divisible by $p$.

If $\beta$ is another root of $g$ not of the form $\alpha + b$, $b \in K$, then the corresponding group has the same order as $H$, again from the above argument. Repeating this procedure until all roots of $g$ are accounted for, yields the result. \qed

**Proof of theorem 5.1.** The number of irreducible polynomials of degree $n$ over the finite field $F_q$ is given by \cite[theorem 3.25]{15}

$$\#E(q^n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}. \quad (27)$$

From lemma 5.2 if $q$ and $n$ are coprime, no irreducible polynomial of degree $n$ over $F_q$ can have roots differing by elements of $F_q$. So if $f \in E(q^n)$, the $q$ polynomials $f_a^+$, $a \in F_q$ are all distinct, and form a block of order $q$. \qed

Our next task is to count quadratic stable sets. The following lemma will be needed to check the simultaneous irreducibility of pairs of quadratic polynomials.

**Lemma 5.3** Let $q$ be odd, and let $a$ be a non-zero element of $F_q$. If $q \equiv 3 \pmod{4}$, then there are $(q-3)/4$ values of $x \in F_q$ such that $x$ and $x + a$ are both non-zero and both non-squares. If $q \equiv 1 \pmod{4}$ then the number of such values of $x$ is equal to $(q-1)/4$ if $a$ is a square, and to $(q-5)/4$ if $a$ is not a square.

**Proof.** The case $q = 3$ is trivial, so we assume $q > 3$. Consider the polynomial $L(x) = F(x)G(x)H(x)$ where

$$F(x) = x^{(q-1)/2} - (x + a)^{(q-1)/2}; \quad G(x) = x^{(q-1)/2} + (x + a)^{(q-1)/2}; \quad H(x) = x(x + a).$$

From Euler’s criterion, for any $x \in F_q$, precisely one of $F(x)$, $G(x)$, $H(x)$ is zero: if $H(x)$ is non-zero, then $F(x)$ is zero when $x$ and $x + a$ have the same quadratic character.
(they are both squares or non-squares) and non-zero otherwise, and conversely for \( G(x) \).

Furthermore, \( \deg F = (q - 3)/2 \), \( \deg G = (q - 1)/2 \), \( \deg H = 2 \), and hence \( \deg L = q \), so that all roots of \( L \) are distinct. It follows that \( L \) is a constant multiple of \( x^q - x \). So the \( (q - 3)/2 \) roots of \( F \) are the values of \( x \) for which \( x \) and \( x + a \) are both non-zero, and have the same quadratic character.

Consider the involution \( x \mapsto \iota(x) = -(x + a) \). We have two cases.

i) If \( q \equiv 3 \pmod{4} \), then \( F(\iota(x)) = F(x) \), and moreover \(-1\) is not a square. Thus, if \( \alpha \) is a root of \( F \) so is \( \iota(\alpha) \), and these two roots have opposite quadratic character. For this reason the involution \( \iota \) cannot fix any root of \( F \), and hence exactly half of such values of \( \alpha \), \( (q - 3)/4 \) in number, are such that both \( \alpha \) and \( \alpha + a \) are non-squares.

ii) If \( q \equiv 1 \pmod{4} \), then \( G(\iota(x)) = G(x) \), and \( x \) and \(-x\) have the same quadratic character. If \( \alpha \) is a root of \( G \), then \( \iota(\alpha) \) is another root of \( G \) with opposite quadratic character. So \( \iota \) cannot fix any root of \( G \), and therefore half of the roots of \( G \) are squares, and half are non-squares. The remaining \( (q - 1)/4 \) non-squares are subdivided between the roots of \( F \) and the root \(-a\) of \( H \), whose quadratic character is the same as \( a \). One sees that if \( a \) is a square, then there are \( (q - 1)/4 \) roots of \( F \) which are non-squares, and if \( a \) is not a square then the number of such roots is \( (q - 1)/4 - 1 = (q - 5)/4 \).

We can now count quadratic stable sets for odd \( q \).

**Theorem 5.4** Let \( q \) be odd, and let \( N_i(q) \) be the number of stable quadratic 2-sets of type \( i \) \( (i = I, II, III) \) over \( \mathbb{F}_q \). We have

\[
N_I(q) = \begin{cases} 
(q - 1)/4 & \text{if } q \equiv 1 \pmod{4} \\
(q - 3)/4 & \text{if } q \equiv 3 \pmod{4};
\end{cases}
\]

\[N_{II}(q) = 0;\]

\[N_{III}(q) = q - 1.\]

**Proof.** The case of type II is a specialization of theorem 4.4. For type III, theorem 5.1 for \( q \) odd and \( n = 2 \) gives \((q - 1)/2 \) blocks. Now, every quadratic block has a centre, which gives rise to two distinct stable sets of type III according to equation (15).

For type I, with reference to table I, we have to verify the simultaneous irreducibility of \( f \) and \( g \), whose discriminant is \(-4r\) and \( 1 - 4r \), respectively. Because \( r \) is an arbitrary non-zero element of \( \mathbb{F}_q \) and \( q \) is odd, each discriminant assumes \( q - 1 \) distinct values. Our result now follows from lemma 5.3 with \( a = 1 \). \( \square \)

We finally turn to periodic 2-sets.

**Theorem 5.5** For odd \( q \), the number of periodic 2-sets of degree 2 over \( \mathbb{F}_q \) is at most \((q - 1)^2 \cdot (q - 3)/8\).
Proof. We use the results and notation of section 4.2. A periodic 2-set \( \{f, g\} \) of degree 2 has the form

\[
f = x^2 + bx + r, \quad g = x^2 + cx + r, \quad uvr = (b^2 - c^2)r \neq 0. \tag{28}
\]

Interchanging the polynomials changes the sign of \( u \), and so the number of pairs \((u, v)\) to be considered is equal to \((q - 1)^2/2\).

We now apply lemma 5.3, considering that the difference between the discriminants of \( f \) and \( g \) is \( uv \). There are two cases.

i) If \( q \equiv 3 \pmod{4} \), then for every pair \((u, v)\) there are \((q - 3)/4\) values of \( r \) for which \( f \) and \( g \) are both irreducible.

ii) If \( q \equiv 1 \pmod{4} \), then, given \((u, v)\), the number of values of \( r \) with the stated property is equal to \((q - 1)/4\) if \( uv \) is a square, and to \((q - 5)/4\) if it is not. So the total number of irreducible pairs of eventually periodic polynomials of the form (28) is given by

\[
\frac{(q - 1)^2}{4} \left( \frac{q - 1}{4} + \frac{q - 5}{4} \right) = \frac{(q - 1)^2(q - 3)}{8}.
\]

This gives the result. \( \square \)

We close this section by describing the construction of periodic 2-sets of degree two, over a finite field of odd characteristic. For the sake of brevity, we consider only the case of even period \( t \), which is the most interesting. For these cycles to exist, the field \( \mathbf{F}_q \) must contain the \( d_t \)-th roots of unity, with \( d_t \) given by (23). These roots of unity belong to all finite fields only for \( t = 2 \), as described in section 4.2, for \( t > 2 \), the fields are restricted by the \( t \)-dependent condition \( q \equiv 1 \pmod{d_t} \), which follows from the fact that the multiplicative group of a finite field is is cyclic [15, theorem 2.8]. From Dirichlet’s theorem on arithmetic progressions [8, chapter 10], we obtain at once infinitely many fields \( \mathbf{F}_q \) supporting orbits of a given even period. Each of these fields contains \( \phi(2d_t) = \phi(d_t) \) primitive \( 2d_t \)-th roots of unity \( \zeta \) (\( \phi \) is Euler’s function [11, chapter 2]), which are constructed from a primitive element \( \eta \in \mathbf{F}_q \), by letting \( \zeta = \eta^i \) for all \( i \) such that \((q - 1)/\gcd(i, q - 1) = 2d_t\).

Now, fix a root of unity \( \zeta \) of order \( 2d_t \). The equation \( u^2v = \zeta \) can be solved for \( u \) precisely when \( \zeta/v \) is a square, that is, when \( v \) and \( \zeta \) are both squares or non-squares. Accordingly, we let \( v = v_i = \eta^i \), with \( i \) of the appropriate parity, to obtain \((q - 1)/2\) distinct values \( v_i \). For each \( v_i \), we obtain two distinct solutions \((u, v) = (\pm \sqrt{\zeta/v_i}, v_i)\). However, changing the sign of \( u \) corresponds to interchanging \( b \) and \( c \), that is, interchanging polynomials. So we get \((q - 1)/2\) distinct unordered pairs \((b, c)\); for each pair we form all triples \((b, c, r)\) with the property that the discriminants \( b^2 - 4r \) and \( c^2 - 4r \) are simultaneously non-squares. Using again lemma 5.3, we find that there are \( \phi(d_t)(q - 1)(q - 3)/8 \) points of minimal period \( t \) associated to primitive \( 2d_t \)-th roots of unity.
For illustration, let \( t = 6 \). From Table II we find that constructing a full set of 6-cycles requires the 42nd roots of unity. We also see that the minimal order for that period is \( d_6 = 3 \), and the smallest finite field containing 3rd (hence 6th) roots of unity is \( \mathbb{F}_7 \). The above formula gives at most \( \phi(3)(7 - 1)(7 - 3)/8 = 6 \) points of minimal period 6, so there is just one 6-cycle over \( \mathbb{F}_7 \), \( \{f_t, g_t\}, t = 0, \ldots, 5 \), which is displayed below.

\[
\begin{array}{ccc}
    t & f_t & g_t \\
    0 & x^2 + 2x + 3 & x^2 + x + 3 \\
    1 & x^2 + x + 3 & x^2 + 5x + 3 \\
    2 & x^2 + x + 6 & x^2 + 4x + 6 \\
    3 & x^2 + 2x + 5 & x^2 + 3x + 5 \\
    4 & x^2 + 4x + 5 & x^2 + 2x + 5 \\
    5 & x^2 + 4x + 6 & x^2 + 6x + 6 \\
\end{array}
\]

We note that the difference of the middle coefficients (the variable \( u \) in (17) runs through the entire multiplicative group of \( \mathbb{F}_7 \)).

### 5.1 Some experiments

We have explored with Maple the occurrence of stable sets over various finite fields. In the following table we display the number of stable 2-sets for all extensions \( E(p^n) \) of a prime fields \( \mathbb{F}_p \) containing fewer than 500 polynomials. Here \( n \) is the degree of the extension, \( \#E \) denotes the number of irreducible polynomials of degree \( n \), while I, II, III denote the type of stable set.

![Figure 3: The graph of the invariant 3-set \( \{f, g, h\} \) of degree 4 over \( \mathbb{F}_5 \), given in (29).](image)

Figure 3: The graph of the invariant 3-set \( \{f, g, h\} \) of degree 4 over \( \mathbb{F}_5 \), given in (29).
Table III: Number of Stable 2-sets

| $p$ | $n$ | $\#E$ | I | II | III |
|-----|-----|--------|---|----|-----|
| 2   | 3   | 2      | − | −  | 1   |
| 2   | 6   | 9      | − | −  | 1   |
| 2   | 7   | 18     | − | −  | 1   |
| 2   | 9   | 56     | − | −  | 2   |
| 2   | 10  | 99     | − | 1  | −   |
| 2   | 12  | 335    | − | −  | 1   |
| 3   | 2   | 3      | − | −  | 2   |
| 3   | 3   | 8      | − | 3  | −   |
| 3   | 4   | 18     | − | −  | 5   |
| 3   | 5   | 48     | 2 | −  | −   |
| 3   | 6   | 116    | − | −  | 11  |
| 3   | 7   | 312    | − | 1  | −   |
| 5   | 2   | 10     | 1 | −  | 4   |
| 5   | 4   | 150    | 2 | 1  | 14  |
| 7   | 2   | 21     | 1 | −  | 6   |
| 7   | 3   | 112    | 2 | −  | −   |
| 11  | 2   | 55     | 2 | −  | 10  |
| 11  | 3   | 440    | − | 4  | −   |
| 13  | 2   | 78     | 3 | −  | 12  |
| 17  | 2   | 136    | 4 | −  | 16  |
| 19  | 2   | 171    | 4 | −  | 18  |
| 23  | 2   | 253    | 5 | −  | 22  |
| 29  | 2   | 406    | 7 | −  | 28  |

If a row in the table is missing (e.g., $p = 2$, $n = 2$), it means that there are no stable 2-sets in that extension. For $p \neq 2$, the data for quadratic extension follow from theorem 5.4, which, in particular, explains the absence of type II sets and the abundance of type III. Beyond the quadratic case, type II sets seem rare; however, $n = 3$ suffices, e.g., $f = x^3 + x^2 + 2$, $g = x^3 + 2x^2 + 1$, over $\mathbb{F}_3$. We observe that in the above table, for $p$ odd, type III stable sets occur only for extensions of even degree.

Combinations of stable 2-sets may lead to interesting invariant 3-sets, such as the one displayed in figure 3. It is given by

$$ f = x^4 + x + 4, \quad g = x^4 + 2x + 4, \quad h = x^4 + 3x + 4 \quad K = \mathbb{F}_5 $$

and it contains two stable 2-sets: $\{f, h\}$ (type II), and $\{g, h\}$ (type III).

We close with some remarks and computations on periodic orbits. The dynamics of self-interactions over a finite field is eventually periodic, and a natural problem is to determine the structure of periodic sets over a given field. Even in its simplest form —determining
the period of the limit cycle of a quadratic 2-set—this problem seems at least as difficult as that of computing the period of the squaring map \( x \mapsto x^2 \) over a finite field, see comment at the end of section 4.2. Some formulae and asymptotic expressions concerning the periodicity of the squaring map (and, more generally, of repeated exponentiation) have been obtained in [5].

We are interested in a specific probabilistic phenomenon. Given a set \( z = \{f, g\} \) of two quadratic irreducible polynomials over \( \mathbb{Z} \), with the same constant coefficient, and such that the sum and difference of their middle coefficients is non-zero, we consider the orbit of \( z \) over the field \( \mathbb{F}_p \), \( p \) prime. This orbit is eventually periodic: how long are the transient and the period of the limit cycle?

Here we are pursuing an analogy with Artin’s problem on primitive roots [23], which we now describe from a dynamical systems perspective. Given an integer \( a \), not a square, we consider the map \( x \mapsto ax \pmod{p} \), for \( p \) coprime to \( a \). The period of the orbit of any non-zero point \( x \in \mathbb{F}_p \) is given by \( \text{ord}_p(a) \), the order of \( a \) modulo \( p \). We define the normalized period \( T(p) = \text{ord}_p(a)/(p-1) \). Regarding \( T \) as a random variable, one is interested in its distribution function \( D(x) \), which is the probability that \( T \) assumes a value not exceeding \( x \) for a prime \( p \) chosen at random. Such a probability is computed using the natural density over the primes. Artin conjectured\(^1\) that \( D \) exists, and is a step function with positive steps at the reciprocal of each natural number: 1, 1/2, 1/3, \ldots (figure 4). Furthermore, \( D \) does not depend on \( a \), as long as \( a \) is square-free, and has only a mild \( a \)-dependence otherwise.

---

\[ 0.2 \quad 0.4 \quad 0.6 \quad 0.8 \]
\[ x \]

**Figure 4:** Distribution function for the normalized period of the orbits of the map \( x \mapsto 2x \pmod{p} \), computed over the first 20,000 odd primes. The height of the step at \( x = 1 \) is the so-called Artin’s constant: \( \prod_{p \geq 2} (1 - (p^2 - p)^{-1}) = 0.37395 \ldots \) [24. p. 303].

\(^1\)The validity of this conjecture is now known to follow from the generalized Riemann hypothesis.
Figure 5: Top: distribution function for the normalized period of the limit cycle of the orbit of the pair \( z \) of equation (30). The distribution function has been computed over a set of 25037 primes. Bottom: magnifications. The step at \( x = 1/4 \) features secondary steps leading to it (left); that at \( x = 1/2 \) has more regular climb (right).

We have considered the orbit of the following pair of polynomials

\[
z = \{f, g\} \quad f = x^2 + x - 1, \quad g = x^2 + 2x - 1. \tag{30}
\]

The discriminants are \( \Delta(f) = 5, \Delta(g) = 8 \). Using quadratic reciprocity and the Chinese remainder theorem, we find that \( f \) and \( g \) are simultaneously irreducible modulo \( p \) for \( p \equiv 3, 13, 27, 37 \mod 40 \). Excluding \( p = 3 \) (for which the sum of the middle coefficients of \( f \) and \( g \) vanish), at all these primes, the orbit of \( z \) consists of quadratic polynomials. Accordingly we have considered, among the first 100,000 primes, \( (p > 3) \) those belonging to the aforementioned residue classes —25037 primes in all. For each prime \( p \) we have computed the normalized period \( T(p) = t(p)/(p-1) \), where \( t(p) \) is the period of the limit cycle of the orbit of \( z \) over \( \mathbb{F}_p \).

In figure 5 we display the distribution function \( D(x) \). Its value reaches 1 at \( x = 1/2 \), indicating that the cycle length does not exceed \( (p - 1)/2 \) in a significant number of cases (in fact, we found \( T(p) = 1 \) only for \( p = 163 \)). This function has steps at the reciprocal
of even integers. Some steps have a clear sub-structure of secondary steps \((x = 1/4, 1/8,\) see figure 5, bottom left), while others appear to be ‘smoother’ \((x = 1/2, 1/6,\) see figure 5, bottom right). There are no steps for odd denominators \(x = 1, 1/3, 1/5, 1/7.\) The orbit of \(z\) was found to be either periodic (in very nearly 3/8 of cases), or to have a transient of 1 or 2 (in 3/8 and 1/4 of cases, respectively). This tight organization of transients was unexpected, and we found it only for this specific value of \(z;\) in other examples we found instead a rapidly decaying distribution of transient lengths, consistent with the existence of a finite average transient. We remark that the finiteness of the average transient length has been proved for the squaring map (see [5, theorem 2]).

We found that the distribution function does depend on the choice of initial conditions, although its basic structure remains the same. The study of this function lies beyond the scope of this paper. Here we merely observe that, since \(uvz \neq 0,\) the auxiliary map \((18)\) can be transformed into an affine map of \((\mathbb{Z}/(q - 1)\mathbb{Z})^{3},\) using discrete logarithms. In this setting, it should be possible to develop a qualitative analysis, although quantitative results are bound to be a lot more difficult.

References

[1] T. M. Apostol, Introduction to analytic number theory, Springer Verlag, New York (1976).

[2] T. Bousch, Sur quelques problèmes de la dynamique holomorphe, Ph.D. thesis, Université de Paris-Sud, Centre d’Orsay (1992).

[3] A. Batra and P. Morton, Algebraic dynamics of polynomial maps on the algebraic closure of a finite field I, *Rocky Mountain J. of Math.* 24 (1994) 453–481.

[4] A. Batra and P. Morton, Algebraic dynamics of polynomial maps on the algebraic closure of a finite field II, *Rocky Mountain J. of Math.* 24 (1994) 905–932.

[5] W.-S. Chou and I. E. Shparlinski, On the cycle structure of repeated exponentiation modulo a prime *J. Number Theory* 107 (2004) 345–356.

[6] S. D. Cohen and D. Hachenberger, Actions of linearized polynomials on the algebraic closure of a finite field, *Contemporary Mathematics* 225 (1999) 17–32.

[7] S. D. Cohen and D. Hachenberger, The dynamics of linearized polynomials, *Proc. Edimb. Math. Soc.* 43 (2000) 113–128.

[8] H. Cohn, *Advanced number theory*, Dover, New York (1980).

[9] W. Fontana, Algorithmic Chemistry, in *Artificial Life II*, SFI Studied in the Sciences of Complexity, vol X (1990) 150–209.
[10] W. Fontana and L. W. Buss, “The arrival of the fittest”, toward a theory of biological organization, *Bulletin of Mathematical Biology* 56 (1994) 1–64.

[11] H. Hasse, *Number theory*, Springer-Verlag, New York (2000).

[12] N. Kataoka and K. Kaneko, Functional Dynamics I: Articulation process, *Physica D* 138 (2000) 225–250.

[13] N. Kataoka and K. Kaneko, Functional Dynamics II: Syntactic structure *Physica D* 149 (2001) 174–196.

[14] N. Koblitz, *Algebraic aspects of cryptography*, Springer-Verlag, New York (1997).

[15] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Math. and its Appl., vol. 20, Addison-Wesley, Reading, Mass. (1983).

[16] D. A. Marcus, *Number fields*, Springer-Verlag, New York (1977).

[17] P. J. McCarthy, Algebraic extensions of fields, Dover, New York (1966).

[18] P. Morton, On certain algebraic curves related to polynomial maps, *Compos. Math.* 103 (1996) 319–350.

[19] P. Morton and P. Patel, The Galois theory of periodic points of polynomial maps, *Proc. London Math. Soc.* 68 (1994) 225–263.

[20] P. Morton and J. H. Silverman, Periodic points, multiplicities, and dynamical units, *J. fuer reine und angew. Math* 461 (1995) 81–122.

[21] P. Morton and F. Vivaldi, Bifurcations and discriminants for polynomials maps, *Nonlinearity* 8 (1995) 571–584.

[22] R. W. K. Odoni, The Galois theory of iterates and composites of polynomials, *Proc. London Math. Soc.* 51 (1985) 385–414.

[23] M. RamMurty, Artin’s conjecture for primitive roots, *Math. Intelligencer* 10 (1988) 59–67.

[24] P. Ribenboim, *The book of prime number records* Springer-Verlag, New York (1988).

[25] F. Vivaldi, Dynamics over irreducible polynomials, *Nonlinearity* 5 (1992) 941–960.

[26] F. Vivaldi, The arithmetic of discretized rotations, in *p-adic Mathematical Physics*, A. Y. Khrennikov, Z. Rakic, I. V. Volovich editors, AIP Conference Proceedings 826, AIP, Melville, New York (2006) 162–173.
[27] F. Vivaldi and S. Hatjispyros, Galois theory of periodic orbits of rational maps, *Nonlinearity* 5 (1992) 961–978.

[28] B. L. van der Waerden, *Algebra*, Springer-Verlag, New York (1991).