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 the latter. 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 and strong collective features, which affords a fresh viewpoint on some algebraic dynamical constructs. We identify the basic dynamical invariants and begin the study of periodic behaviour, organizing the polynomials into an oriented graph.

1 Introduction

From the viewpoint of algebraic dynamics, a polynomial over 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 can be interchanged. 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. Equivalently, $h = f \triangleright g$ if and only if $g(x)$ divides $h(f(x))$. This relationship between f, g and h defines the *wedge operator* $\triangleright$. The action of the wedge operator is quite natural, since it perform simultaneously the time-evolution of all algebraic conjugates, which, algebraically speaking, are indistinguishable. This construction, introduced in [21], has been developed further in [3, 4, 5, 6].

The set of polynomials under study will be required to be *stable,* that is, closed with respect to the wedge operator (see Section 2 for precise definitions). We then define the

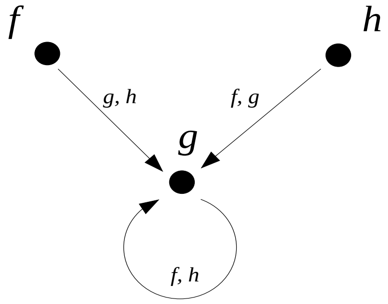

Figure 1: A stable 3-set $\{f, g, h\}$ over the finite field $\mathbf{F}_3$, with $f(x) = x^2 + 1$, $g(x) = x^2 + x + 2$, $h(x) = x^2 + 2x + 2$. The equation $f \triangleright g = h$ is represented as $g \xrightarrow{f} h$. The polynomial g is invariant under both f and h. It can be shown that while h leaves the roots of g invariant, f permutes them cyclically. This set is has self-image $\{g\}$. The sets $\{f, g\}$ and $\{h, g\}$ are stable 2-sets of type III (see Figure 2).

self-image of a subset $\{f_i\}$ of a stable set as the result of all mutual interactions, that is,

$$\mathcal{F} : \{f_i\} \mapsto \{f_i \triangleright f_j\} \qquad\qquad i, j \in J \qquad i \neq j \tag{1}$$

where J is a set of indices. The function $\mathcal{F}$ defines a dynamical systems on the power set of a stable set. Unlike in conventional constructions, here the state space generates its own dynamics. Such feature was first introduced in some abstract models of adaptive systems and chemical interactions, where functions were made to act on other functions via composition, within the framework of λ-calculus [7, 8]. A similar concept has been proposed more recently as functional dynamics on coupled map lattices [10, 11]. Here we present an algebraic variant of the same idea, whereby a polynomial function acts on the defining data of another polynomial function.

It is expedient to arrange the polynomials of a stable set as vertices of a *polynomial graph* Γ [3] (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 $f \triangleright g = h$. The dynamics (1) then becomes dynamics over Γ, resulting from the mutual interaction between vertices.

Given the overwhelming phenomenology, we shall confine our attention to a restricted range of phenomena. Our goal is to identify the simplest dynamical invariants (i.e., small stable sets), to study some structural properties of polynomial graphs, and to begin the analysis of periodic behaviour.

In the next section we define precisely wedge operator, stable sets and their graphs, and analyze the question of right and left invariance under the wedge operator; this will allow us to classify stable 2-sets. The group of translations by elements of the ground field induces a natural partition of polynomials into *blocks*, which have very organized self-images under the mapping $\mathcal{F}$. This is dealt with in Section 3, where we find that certain stable 2-sets originate from self-intersections of blocks.

The quadratic extensions are studied in detail in Section 4, resulting in a fairly complete characterization 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 the doubling map.

Some aspects of self-interaction over finite fields are dealt with in Section 5, where we construct and count periodic 2-sets, and present the results of numerical experiments.

I am much indebted with Patrick Morton, for many illuminating discussions on various matters concerning this work. This research was partially supported by the UK Engineering and Physical Sciences Research Council under grant number GR/K 17026.

2 Self-interaction

Let K be a field, let $f(x)$ and $g(x)$ be monic irreducible polynomials over K. Let α be a root of $g(x)$ in some finite separable extension of K.

We define a one-way interaction between f and g by letting $(f \triangleright g)(x)$ be the minimal polynomial of $f(\alpha)$. It can be shown 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 α of g), and whose degree is a divisor of the degree of g [21]. Specifically,

$$g(x) = \prod_{\alpha} (x - \alpha) \qquad \Longrightarrow \qquad (f \triangleright g)(x) = {\prod_{\alpha}}' \, (x - f(\alpha)) \tag{2}$$

where the primed product is taken over any maximal set of roots α of g for which all terms are distinct. As $(f \triangleright g)(0)$ is the resultant of f and g, the coefficients of $f \triangleright g$ may be regarded as generalizations of the resultant.

The polynomial $f \triangleright g$ can be constructed from f and g, without computing roots. We review the algorithm (see [21] for details). Let $g(x)$ have degree n, and let α be one of its roots. The extension $K(\alpha) : K$ has degree n, since $g(x)$ is irreducible. The field $K(\alpha)$ is represented canonically as the quotient of the polynomial ring $K[x]$ modulo the maximal ideal $(g(x))$ ([23], page 32)

$$K(\alpha) \cong K[x]/(g(x)), \tag{3}$$

meaning that the polynomials in $K[x]$ are replaced by their remainder upon division by $g(x)$. Under this isomorphism, the root α 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 ($\cong K[x]/(x)$). We consider the map of $K[x]/(g(x))$ into itself determined by multiplication by $f(x)$. This mapping is linear ([14], Chapter 2), and in the above basis it is represented by the matrix $M = \{m_{i,j}\}$ over K given by

$$f(x) \cdot x^{k-1} \equiv m_{1,k} + m_{2,k}x + \cdots + m_{n,k}x^{n-1} \pmod{g(x)} \qquad k = 1, \ldots, n. \tag{4}$$

It can be shown that $h(x)$ 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 $(h(x))^r$, and hence the degree of h is a divisor of that of g. If such divisor is proper, the roots of $f \triangleright g$ collapse in some subfield of the splitting field of g.

Let $e(x) = x$. The following identities are immediate

$$e \triangleright f = f \qquad\qquad f \triangleright f = e \tag{5}$$

from which it follows that $(f \triangleright f) \triangleright g = g$. On the other hand, $f \triangleright (f \triangleright g) \neq g$, in general, and hence the wedge operator is not associative (although the self-map $\mathcal{F}$ defined in (1) is). From irreducibility, we also have that

$$f \neq g \neq e \qquad \Longrightarrow \qquad f \triangleright g \neq e \qquad \text{and} \qquad f \triangleright e \neq e.$$

2.1 Stable sets and their graphs

A set S of irreducible polynomials over K is said to be *stable* if, whenever f and g belong to S and $f \neq g$, so does $f \triangleright g$. We exclude the case $f = g$ from consideration, to eliminate trivial interactions. The effect of allowing the interaction $f \triangleright f$ in a set of polynomials, is achieved by adjoining the identity e to that set, from equations (5). From equation (1), we see that a set is stable precisely when contains its self-image.

Because a polynomial over a field K leaves every algebraic extension of K invariant, stable sets are naturally constructed by means of field extensions. In particular, the set of minimal polynomials of all the elements of a finite simple extension $L : K$ is stable; we denote it by $S(f)$, where f is any irreducible monic polynomial such that $f(\alpha) = 0$ and $L = K(\alpha)$. One sees that this definition does not distinguish between conjugate fields. A prominent subset of $S(f)$ is

$$E(f) := \{g \in S(f) \mid S(g) = S(f)\} \tag{6}$$

which contains only the polynomials generating the top field. The set $E(f)$ is not stable, in general. Furthermore, $E(f)$ 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 $\mathbf{F}_3$. Thus $\{f, g, h\} = E(f) = E(g) = E(h)$.

The *graph* of a stable set 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. Each arc (g, h) is equipped with a *spectrum* $\omega = \{f_1, \ldots, f_r\}$, which is the set of all polynomials f_k such that $f_k \triangleright g = h, k = 1, \ldots, r$. The elements of the spectrum are all distinct, so that each arc represents a family of distinct arcs joining the same vertices, each associated to a specific polynomial. To make the spectrum explicit, we write $g \overset{\omega}{\to} h$ in place of (g, h), see figures 1–3. The following result bounds the size of the spectrum of an arc

Proposition 2.1 *Let ω be the spectrum of the arc (g,h), with $\deg g = n$ and $\deg h = m$. Then, for every integer d, with $1 \le d \le n$, ω contains at most m polynomials of degree d.*

Proof. Let $g, f_1, f_2 \in K[x]$ be non-constant monic polynomials, with g irreducible and $\deg f_2 \le \deg f_1 \le n$. Let α 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 $\deg l \le n$ and g is the minimal polynomial of α, 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 $d \le n$. We have shown that such f, if it exists, is unique. There are m possible choices of β 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 α, so there are no other polynomials. This completes the proof. ☐

The subgraphs of Γ of interest to us, originate from the subsets $E \subset S$ defined in (6). The *extension graph* has vertices restricted to $E(f)$. Unless specified otherwise, the same restriction applies also to the spectra. The *transition graph* between $E(f)$ and $E(g)$ has only arcs joining $E(f)$ to $E(g)$, or vice-versa.

Graphs 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 Γ is a complete 1-graph, where the spectrum of each arc consists of a single polynomial. The quadratic case is already non-trivial — see Section 4.

2.2 Invariance and stable 2-sets

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

$$(i) \quad f \triangleright g = g \qquad\qquad (ii) \quad g \triangleright f = g. \tag{7}$$

In equations (i) and (ii), we say that g is a *right* and a *left invariant* of f, respectively.

Right invariants originate from periodic points which are algebraic conjugates. Indeed, for g to be a right invariant of f, f must permute the roots of g. This follows from the irreducibility of g and the transitivity of its Galois group. If $f = e$, then ($7i$) trivially holds for any g, from equations (5). To construct non-trivial solutions g of ($7i$) for a given $f \ne e$, we proceed as follows. Let f^n be the n-th iterate of f (with $f^0 = e$); the roots of the polynomial $f^n(x) - x$ are the periodic points of f of period dividing n. To specify the

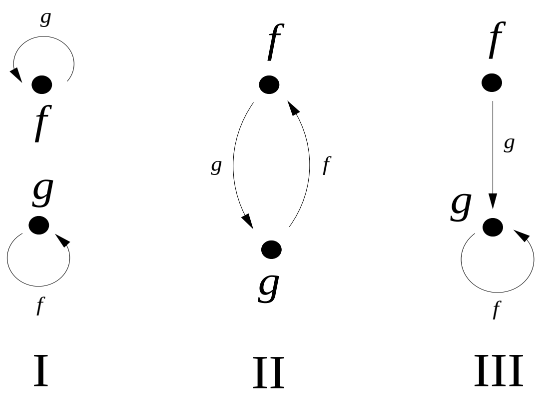

Figure 2: Stable 2-sets $\{f, g\}$. Type I: two right invariants ($f \triangleright g = g$ and $g \triangleright f = f$). Type II: two left invariants ($f \triangleright g = f$ and $g \triangleright f = g$). Type III: mixed invariants ($f \triangleright g = g$ and $g \triangleright f = g$). Types I and II are invariant under $\mathcal{F}$, while type III collapses onto $\{g\}$.

period more precisely, we consider the following polynomials [22, 2, 17]

$$\Phi_{n,f}(x) = \prod_{d\,|n} (f^d(x) - x)^{\mu(n/d)} \qquad n = 1, 2, \ldots \tag{8}$$

where μ is the Möbius function ([1], Chapter 2). (We shall often drop the subscript f in Φ.) The roots of Φ_n are periodic points of f of *essential* period n [18], which is the miminal period apart, possibly, at bifurcations [19]. It follows that every right invariant of f is an irreducible factor of Φ_n, 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 Φ_n is irreducible, then $f \triangleright \Phi_n = \Phi_n$. (The polynomial $\Phi_{n,f}$ is 'generically' irreducible, that is, irreducible over $K = \bar{\mathbb{Q}}$, when the coefficients of f are regarded as indeterminates [16].)

Left invariants (equation (7*ii*)) are associated with pre-images of zero. Let us consider the functional equation $f^k \triangleright f^n = f^{n-k}$, $n \geq k$, ignoring irreducibility for the moment (the polynomial f^n is generically irreducible over any field of characteristic zero [20]). 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 α is a root of f, then $g(g(\alpha)) = 0$, that is, f is an irreducible factor of g^2. Again, 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 $x + 2a$.

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 $\mathcal{F}$. The case of mixed invariants is denoted as type III; its self-image is the right-left invariant.

Type I stable sets are not difficult to construct. For instance, for any monic polynomial f over K, the equal-degree sets

$$\{f(x^2),\, f(x^2) - x\} \qquad \mathrm{char}(K) \neq 2 \tag{9}$$

$$\{f(x),\, f(x)-x\} \qquad \mathrm{char}(K)=2 \tag{10}$$

are stable of type I whenever the polynomials involved are irreducible (char(K) denotes the characteristic of the field K).

To see this, let $g(x)=f(x^2)$, with char$(K)\neq 2$. Then $g(x)-x=\Phi_{1,g}(x)$ is a right invariant of g. Furthermore, if α is a root of g, then $\Phi_1(\alpha)=-\alpha$ is a root of $\Phi_1 \triangleright g$. Therefore, for g to be a right invariant of Φ_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 (9) 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 divides $\Phi_{2,h}$, where $h(x)=\Phi_{1,g}(x)$. If char$(K)=2$, the polynomials in (10) are one the Φ_1-polynomial of the other.

Type II and type III stable set will be considered in sections 4 and 5, in specific settings. We will show that quadratic type III sets always exist, while type II sets appear to be rare, and require at least cubic polynomials.

3 Blocks

A *block* is a collection of polynomials whose roots differ by elements of the ground field. Blocks turn out to have well-structured self-images.

We begin with the group G of matrices

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

which we let act on irreducible polynomials as follows

$$\sigma(f)(x) = a^{-\deg f} f(ax+b). \tag{11}$$

The polynomial $\sigma(f)$ is monic and irreducible, and since $\sigma_{c,d}(\sigma_{a,b}(f)) = (\sigma_{c,d}\sigma_{a,b})(f)$, G defines an action on $E(f)$, or on its graph. The orbits of G partition the vertices of every extension graph into *clusters*.

We consider the additive normal subgroup

$$G^+ = \{\sigma_{1,b}\} \qquad \sigma_{1,b} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \qquad b\in K. \tag{12}$$

Its orbits are *blocks*, which subdivide each cluster. Likewise, we have the multiplicative group

$$G^* = \{\sigma_{a,0}\} \qquad \sigma_{a,0} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \qquad 0\neq a\in K. \tag{13}$$

We introduce the short-hand notation

$$f_b^+ := \sigma_{1,b}(f) \qquad\qquad f_a^* := \sigma_{a,0}(f), \tag{14}$$

and we denote the block containing f by Θ_f, so that $\Theta_f = \{f_b^+ \,|\, b \in K\}$. 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.

The following two lemmas collect miscellaneous results on the action of G, to be used in later sections. We denote the discriminant of f by $\Delta(f)$.

Lemma 3.1 *Let f and g belong to a stable set, and let $n = \deg f$. The action of G enjoys the following properties*

- *(i)* *For every $\sigma \in G$ we have $\sigma(\Theta_f) = \Theta_{\sigma(f)}$.*
- *(ii)* *For every $\sigma_{a,b} \in G$ we have $\sigma_{a,b}(f) \triangleright \sigma_{a,b}(g) = \sigma_{a^n,0}(f \triangleright g)$.*
- *(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 $\sigma^+(f) = g$ 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, σ is injective, because (11) defines a group action. This proves the first assertion. To prove *(ii)*, let $g(\alpha) = 0$. With reference to (2) and (11), we find

$$\sigma_{a^n,0}(f \triangleright g)(x) = \prod_{\alpha}{}' \left(x - a^{-n} f(\alpha)\right); \qquad (\sigma_{a,b}(g))(x) = \prod_{\alpha}{}' \left(x - a^{-1}(\alpha - b)\right).$$

from which we obtain

$$(\sigma_{a,b}(f) \triangleright \sigma_{a,b}(g))\,(x) = \prod_{\alpha}{}' \left[x - a^{-n} f\left(aa^{-1}(\alpha - b) + b\right)\right] = \prod_{\alpha}{}' \left(x - a^{-n} f(\alpha)\right)$$

as required. Part *(iii)* follows from the discriminant formula for a monic polynomial ([13], Chapter 1)

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

where α_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

$$\begin{aligned} g \triangleright g_b^+ &= \sigma_{1,c}(f) \triangleright \sigma_{1,b}\sigma_{1,c}(f) \\ &= \sigma_{1,c}(f) \triangleright \sigma_{1,c}\sigma_{1,b}(f) \\ &= f \triangleright f_b^+. \end{aligned}$$

This proves (iv). $\square$

From Lemma 3.1 (ii) it follows that $\deg(\sigma_{a,b}(f) \triangleright \sigma_{a,b}(g)) = \deg(f \triangleright g)$. From (iii), we have that the discriminant is a block invariant, which we denote by $\Delta(\Theta)$. Such discriminant is non-zero, since we are dealing with separable extensions.

Lemma 3.2 *Let g be an irreducible polynomial over K. Then*

(i) *If $g = g_b^+$, for some $b \neq 0$, then char$(K) > 0$ and the degree of g is divisible by char(K).*

(ii) *If $g = g_a^*$ for $a \neq 0$ is a root of g, the degree of g is divisible by the multiplicative order of a in K.*

Proof. (i) We first show that if α, $\alpha + b$ and β are roots of g, so is $\beta + b$. Let σ be an element of the Galois group of g, sending α to β. Then $\beta + b = \sigma(\alpha) + b = \sigma(\alpha + b)$, 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 β is another root of g not of the form $\alpha + b$, $b \in K$, then the corresponding group is still H, again from the above argument. Repeating this procedure until all roots of g are accounted for, yields the result.

(ii) This proof is the multiplicative version of that given above. $\square$

3.1 Self-image of blocks

We consider the self-image of a block Θ (cf. Equation (1)), which 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 Θ. But then, if we let $\mathcal{B}(f)$ be the set of blocks of an extension, the mapping

$$\mathcal{F}_b : \mathcal{B} \to \mathcal{B} \qquad \Theta_f \mapsto \Theta_{f \triangleright f_b^+} \qquad 0 \neq b \in K \tag{15}$$

is well-defined. From Lemma 3.1 (*i*) and (*ii*) we find the commutation relation

$$\sigma_{a^n,0}(\mathcal{F}_b(\Theta)) = \mathcal{F}_{ab}(\sigma_{a,0}(\Theta))$$

where n is the degree of the block.

By means of $\mathcal{F}_b$ we can construct an oriented graph, whose vertices are blocks, and where two blocks Θ and Θ' are joined by an arc if Θ' belongs to the self-image of Θ. This graph, called the *block graph,* describes a very specific but significant class of self-interactions. We prove two results: the first provides a sufficient condition for degree invariance of the self-image of a block; the second shows that intersection of self-images lead to invariants.

Proposition 3.3 *Let Θ be a block of degree n, where n is prime and char$(K) \neq n$. Then the self-image of Θ has degree n.*

Proof. Let $\Theta = \Theta_f$, and let α 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 α of degree $n-1$, since, by assumption, $b\, n \neq 0$. 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 α is algebraic of degree n. $\square$

Proposition 3.4 *If a block Θ intersects its self-image, then Θ 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

$$\theta_{-b} \triangleright \theta = \theta \qquad \theta \triangleright \theta_b = \theta, \tag{16}$$

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

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 $\{\theta, \theta_{\pm b}\}$. One verifies that this is the case precisely when $\theta(\alpha + b)$ and $\theta(\alpha - b)$ are algebraic conjugate, 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 $\mathbf{F}_3$ consists of a single block, which intersects (indeed, contains) its self-image, due to Proposition 3.3, giving rise to the right-left invariant g, and to two stable 2-sets of type III.

4 Quadratic self-interactions

Throughout this section, f denotes a quadratic monic irreducible polynomial over a field K, with discriminant $\Delta(f)$. We first characterize extension and transition graphs, and construct the stable 2-sets. Then we derive a three-dimensional skew-map describing the dynamics of 2-sets, with which we compute periodic points.

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 char*$(K) \neq 2$*, then the block-graph is a complete graph, and the set of mappings* $\mathcal{F}_b$*, defined in (15), 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* Θ *to* $\mathcal{F}_{b/2}(\Theta)$*.*

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 $(f_b^+ \triangleright f)_c^+ = g$.

We need a lemma:

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

- (i) $(f \triangleright f_b^+)(x) \;=\; (x-b^2)^2 - b^2\,\Delta(f)$.
- (ii) $\Delta(f \triangleright f_b^+) \;=\; (2\,b)^2 \Delta(f)$.
- (iii) *If char*$(K) \neq 2$*, then the polynomials* $f \triangleright f_a^+$ *and* $f_b^+ \triangleright f_{b+c}^+$ *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 3.1 (ii). Then from (i) above, we have that if $f \triangleright f_a^+$ and $f_b^+ \triangleright f_{b+c}^+$ 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 $f \triangleright f_a^+ = f_b^+ \triangleright f_{b\pm a}^+ = f_b^+ \triangleright f_{b+c}^+$. $\square$

Proof of Theorem 4.1 If α is a root of f and g is an irreducible polynomial in the same extension, then the roots of g are linear expressions in α 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

$$\sigma_{a,b}(f) = \sigma_{1,c}(\sigma_{-a,b}(f)) \qquad c = \frac{2b - S}{a}$$

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 $\mathrm{char}(K) \neq 2$. To show that the block graph is complete, we consider the equation

$$\mathcal{F}_b(\Theta_f) = \Theta_{f \triangleright f_b^+} = \Theta_g$$

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 $\mathrm{char}(K) \neq 2$. Matching discriminants suffices, since we have seen that discriminants identify blocks.

We show that $\mathcal{F}_b$ is injective. If Θ and Θ' are distinct blocks, they have distinct discriminants, Δ and Δ', say. But then

$$\Delta(\mathcal{F}_b(\Theta_f)) = 2b^2\Delta \neq 2b^2\Delta' = \Delta(\mathcal{F}_b(\Theta_g))$$

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

Thus, if $\mathrm{char}(K) \neq 2$, each non-zero value of b defines a permutation of blocks. Now consider the mapping

$$\mu : b^2 \mapsto \mathcal{F}_{b/2} \qquad 0 \neq b \in K$$

sending $(K^*)^2$ to the symmetric group on $\mathcal{B}$. 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 μ associates to b^2 the permutation sending the block of discriminant Δ to that of discriminant $b^2\Delta$. Keeping this in mind, we find that

$$\mu((bc)^2) = \mathcal{F}_{bc/2} = \mathcal{F}_{b/2} \circ \mathcal{F}_{c/2} = \mu(b^2)\mu(c^2)$$

e.g., μ is a group homomorphism. Its kernel is trivial, $\mu(1^2) = \mathcal{F}_{1/2}$, and so μ defines a faithful action of $(K^*)^2$ on $\mathcal{B}$. □

Thanks to Proposition 3.4, the identity permutation $\mathcal{F}_{1/2}$ maps the whole block to a right-left invariant of the wedge operator, which, from Lemma 4.2(*ii*), is given by

$$\theta(x) = \left(x - \frac{1}{4}\right)^2 - \frac{\Delta}{4} \tag{17}$$

where Δ is the block discriminant. From Lemma 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

$$\{\theta, \theta^+_{1/2}\} \qquad \{\theta, \theta^+_{-1/2}\} \qquad \mathrm{char}(K) \neq 2 \tag{18}$$

which are 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.) If K is an infinite field, then the number of blocks of any non-trivial extension is infinite, and so we have infinitely many quadratic stable 2-sets of type III.

In the following table, we display all parametrized families of quadratic stable 2-sets, for $\mathrm{char}(K) \neq 2$.

TABLE I: QUADRATIC STABLE 2-SETS

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

There are no quadratic stable 2-sets of type II, as we will prove in the next section. All polynomials are irreducible over $K(r)$, where r is transcendental over K. It should be clear that if instead r is regarded as a specific element of K, irreducibility must be checked. The last two columns describe the mutual relation between f and g, in the notation of section 2.2. The type I set is of the form (9), with one of the two polynomials having zero middle coefficient, as explained in Section 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 (17,18), with $r = (1 - \Delta)/4$).

The last result of this section characterizes some transitions to the ground field. For char $K \neq 2$, this characterization is complete.

Proposition 4.3 *For every $b \in K$, the polynomial $(f \triangleright f^+_b) \triangleright (g \triangleright g^+_b)$ has degree one. Conversely, if char$(K) \neq 2$ and $h \triangleright l$ has degree 1, then there exists $c \in K$ such that*

$$h = (\theta_h)^+_c \qquad l = (\theta_l)^+_c$$

where θ_h and θ_l are the centres of the respective blocks.

Proof. If α 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

$$h(\alpha) \;=\; b^2\,(\Delta(g) - \Delta(f)) \;\in\; K. \tag{19}$$

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 $\Delta(h) - \Delta(l) = -4\,r$. The equation $l = (\theta_l)_d^+$ now reads

$$\left(x + d - \frac{1}{4}\right)^2 - \frac{\Delta(l)}{4} = \left(x + d - \frac{1}{4}\right)^2 - \frac{\Delta(h)}{4} - r = l(x) = h(x) - r$$

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 $\mathrm{char}(K) \neq 2$. Let $\mathcal{F}(\{f, g\}) = \{f', g'\}$, with $f' = f \triangleright g$ and $g' = g \triangleright f$. Since $f'(0) = g'(0) = \mathrm{Res}(f, g)$ (see remark following equation (2)), without loss of generality, we let

$$f = x^2 + bx + r \qquad\qquad g = x^2 + cx + r.$$

The corresponding primed coefficients are computed as

$$b' = c(b - c) \qquad\quad c' = -b(b - c) \qquad\quad r' = r(b - c)^2.$$

Defining

$$u = b - c \qquad\qquad v = b + c \tag{20}$$

we obtain a three-dimensional skew map over K

$$\Psi : K^3 \to K^3 \qquad\qquad (u, v, r) \;\mapsto\; (uv, -u^2, ru^2). \tag{21}$$

Iteration gives

$$\Psi^t(u, v, r) \;=\; \begin{cases} (z_t/u, -z_t/v, r(z_t/uv)^2) & t \text{ odd} \\ (-uz_t, -vz_t, rz_t^2) & t \text{ even} \end{cases} \qquad t > 0 \tag{22}$$

where

$$z_t = (u^2 v)^{e_t} \qquad\quad e_t = \frac{1}{3}\left[2^t + (-1)^{t+1}\right] \qquad\quad t = 1, 2, \ldots \tag{23}$$

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 (21) 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 $uvr \neq 0$. Since the discriminants of f and g evolve as

$$\Delta(f') = u^2\Delta(g) \qquad\qquad \Delta(g') = u^2\Delta(f) \tag{24}$$

one sees that if f and g are irreducible, so are all the elements of their orbit.

The periodic points equation reads

$$\Psi^t(u, v, r) \;=\; (\pm u, v, r) \qquad\quad t > 0 \tag{25}$$

where the negative sign corresponds to exchanging f and g, from (20). When the period t is odd, using (22), we find no irreducible solution corresponding to the positive sign in (25). In particular, for $t = 1$, this implies the non-existence of quadratic stable sets of type II. For the negative sign in (25), we find

$$v = \pm u \qquad\quad u^{3e_t - 2} \pm 1 = 0 \tag{26}$$

where the signs n both equations alternate along each orbit. So in every element of a cycle of odd period, precisely one of the two polynomials has zero middle coefficient. We see that $u = \zeta$, where ζ is either a $(3e_t - 2)$-th or a $2(3e_t - 2)$-th root of unity; these roots of unity belong to the same field, since $3e_t - 2$ is odd (equation (23)). (For background refereces on roots of unity, see, e.g., [15], page 39, or [9], Chapter 27.) When $t = 1$, we recover the type I stable set displayed in Table I. Because $e_t > 1$ for $t > 2$, odd cycles with period greater than 1 can exist only if K contains non-trivial roots of unity.

When t is even, we find no solution of (25) corresponding to the negative sign (unless $\mathrm{char}(K) = 2$, which we have excluded). For the positive sign, we obtain

$$(u^2v)^{e_t} + 1 = 0 \tag{27}$$

that is, $u^2v = \zeta$, where ζ is a $2e_t$-th root of unity. For every choice of ζ, this equation defines an algebraic curve of genus 0 over the e_t-th cyclotomic field over K, and the points on this curve correspond to the t-cycles. Solving (27) for $t = 2$, gives the 2-cycle $\{f_0, g_0\} \longleftrightarrow \{f_1, g_1\}$, irreducible over $K(r, s)$

$$f_0 = x^2 - \frac{s^3+1}{2\,s}\,x + r \qquad\qquad g_0 = x^2 - \frac{s^3-1}{2\,s}\,x + r$$

$$f_1 = x^2 + \frac{s^3-1}{2\,s^2}\,x + \frac{r}{s^2} \qquad\qquad g_1 = x^2 - \frac{s^3+1}{2\,s^2}\,x + \frac{r}{s^2}.$$

As above, even cycles with period greater than 2 require non-trivial roots of unity. We define

$$d_t \;=\; \begin{cases} 3e_t - 2 = 2^t - 1 & t \text{ odd} \\ e_t = (2^t - 1)/3 & t \text{ even} \end{cases} \qquad t > 0. \tag{28}$$

If in the above construction ζ is a primitive d_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 (equation (28)). So the d_t-th cyclotomic field is the smallest fields containing all cycles of mimimal period t. Clearly, there may be cyclotomic fields of lower order containing *some* orbits of the same minimal period. To compute their order, we consider all divisors of d_t, and remove from them the divisors of $d_{t'}$, for all t' which divide t and have the same parity as t. The restriction on the parity is due to the fact that if t is even, t' is odd, and d is a common divisor of d_t and $d_{t'}$, then the solutions of equation (27) corresponding to the d-th roots of unity differ from those of equation (26), as long as $u \neq \pm v$.

In the table below, we display the order of the cyclotomic field(s) supporting periodic 2-sets of minimal period t, for $t = 1, \ldots, 14$. The order of the corresponding roots of unity is twice that of the field.

TABLE II: CYCLOTOMIC FIELDS FOR MINIMAL PERIODS

t	order
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 these fields and the periodic orbit fields of the doubling map $z \mapsto z^2$ on the complex plane, for which $d_t = 2^t - 1$.

5 Self-interaction over finite fields

In this section we consider self-interacting polynomials over a finite extension of a finite field $K = \mathbf{F}_q$. We denote the set of irreducible polynomials of degree n by $E(q^n)$ (cf. Equation (6)). Their number is given by

$$\#E(q^n) = \frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d} \tag{29}$$

where μ is the Möbius function ([13], theorem 3.25).

Each block contains at most q polynomials, but it may even consist of a single polynomial, namely an affine q-polynomial over $\mathbf{F}_q$ (see [13], Chapter 3.4). However, if $\gcd(q,n) = 1$, from Lemma 3.2 (i) we see that no irreducible polynomial of degree n over $\mathbf{F}_q$ can have roots differing by elements of $\mathbf{F}_q$. So if $f \in E(q^n)$, the q polynomials f_a^+, $a \in \mathbf{F}_q$ are all distinct, and form a block of order q. We have proved

Proposition 5.1 *If $gcd(q,n) = 1$ with $n > 1$, the extension graph of degree n over $\mathbf{F}_q$ decomposes into the union of $\#E(q^n)/q$ blocks of order q, where $\#E(q^n)$ is given by (29).*

For q odd and $n = 2$, this gives $(q-1)/2$ blocks. Every quadratic block has a centre, which gives rise to two stable sets of type III (Equation 18). So, for odd q, there are $q-1$ quadratic stable sets of type III over $\mathbf{F}_q$.

To count periodic 2-sets when $q \equiv 3 \pmod 4$, we shall use the following

Lemma 5.2 *Let $q \equiv 3 \pmod 4$, and let a be a non-zero element of F_q. Then there are $(q-3)/4$ values of $x \in \mathbf{F}_q$ such that x and $x + a$ are both non-zero and both non-squares.*

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

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

From Euler criterion, for any $x \in \mathbf{F}_q$, precisely one of $F(x)$, $G(x)$, $H(x)$ is zero. Furthermore, $\deg F = (q-3)/2$, $\deg G = (q-1)/2$, $\deg H = 2$, and hence $\deg L = q$, so that L splits completely over $\mathbf{F}_q$ and 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 $x \mapsto \iota(x) = -(x + a)$, acting on the roots of F. This map changes simultaneously the quadratic character x and $x + a$, since it interchanges them and changes sign (recall that -1 is not a square, because $q \equiv 3 \pmod 4$). Furthermore, ι has no fixed points, for if r is one of them, then $r = -(r + a) = a/2$, which is impossible since r and $r+a$ have the same quadratic character. So, for half of the roots x of F, x and $x+a$ are simultaneously non-squares. □

Applying the lemma with $a = b^2 - c^2$, $x = c^2 - 4r$, and $b^2 \neq c^2$, we conclude that there are $(q-3)/4$ values of r for which both polynomials x^2+bx+r and x^2+cx+r are irreducible. (Plainly, if $b^2 = c^2$, there are $(q-1)/2$ such values.) Now, interchanging b and c changes the sign of a, so there are $(q-1)/2$ non-zero values of a, each leading to $q-1$ unordered pairs (b,c). Furthermore, a 2-set with $b^2 \neq c^2$ cannot be periodic, see remark after Equation (23). We conclude that if $q \equiv 3 \pmod 4$, there are at most $(q-1)^2(q-3)/8$ quadratic 2-sets that are periodic.

We now describe 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 (28). These roots of unity belong to all finite fields only for $t=2$, as described in Section 4.2. For $t>2$, we obtain the condition $q \equiv 1 \pmod{d_t}$, from the fact that the multiplicative group of $\mathbf{F}_q$ is cyclic. From Dirichlet's theorem on arithmetic progressions, 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 ζ (ϕ is Euler's function), 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 ζ. The equation $u^2 v = \zeta$ can be solved for u precisely when ζ/v is a square, that is, when v has the same quadratic character as ζ. 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 $(u,v) = (\pm\sqrt{\zeta/v_i}, v_i)$, from which we recover two distinct (b,c)-pairs, with b and c interchanged, corresponding to interchanging polynomials. Finally, for each pair (b,c) we form all triples (b,c,r) with the property that the discriminants b^2-4r and c^2-4r are simultaneously non-squares. If $q \equiv 3 \pmod 4$, there are $(q-3)/4$ such values of r, from Lemma (5.2), while if $p \equiv 1 \pmod 4$ this will happen for approximately one quarter of the non-zero values of r. In total, there are some $\phi(d_t) \cdot (q-1)/2 \cdot \lfloor (q-1)/4 \rfloor$ points of minimal period t associated to primitive $2d_t$-th roots of unity (see Table III, below).

For illustration, let $t=6$. From Table II we find $d_6 = 21$, and letting $q = p \equiv 1 \pmod{21}$, we have the sequence of primes $p = 43, 127, 211, \ldots$. We choose $p = 43$. The smallest primitive element is $\eta = 3$, and in this case the desired $\phi(42) = 12$ primitive 42nd roots of unity coincide with the primitive elements of $\mathbf{F}_{43}$: $\zeta = \eta = 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34$. The above formula gives a total of 2520 points (b,c,r) of minimal period 6 over $\mathbf{F}_{43}$, corresponding to as many polynomial 2-sets. According to Table II, the minimal cyclotomic field for the period $t=6$ has order 3, and the smallest finite field containing it is $\mathbf{F}_7$. There is just one 6-cycle modulo 7: $\{f_t, g_t\}$, $t = 0, \ldots, 5$, which is displayed below:

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

$K = \mathbf{F}_7$.

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 $\mathbf{F}_p$ 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.

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

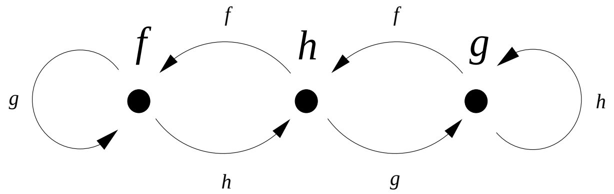

Figure 3: The graph of the invariant 3-set $\{f, g, h\}$ of degree 4 over $\mathbf{F}_5$, given in (30).

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. Type II sets seem rare; we know they do not exist for $n = 2$, and the table shows that $n = 3$ suffices, e.g., $f = x^3 + x^2 + 2$, $g = x^3 + 2x^2 + 1$, over $\mathbf{F}_3$. Type I is more common. For quadratic extensions, its occurrence depends on the simultaneous irreducibility modulo p of f and g of Table I; accordingly there are $(p-3)/4$ such stable sets if $p \equiv 3 \pmod 4$ (Lemma 5.2), while if $p \equiv 1 \pmod 4$ there are approximately $(p-1)/4$ of them. Type III is the most abundant: there are $p - 1$ such sets for quadratic extension — see discussion following Proposition 5.1. 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

$$f = x^4 + x + 4, \quad g = x^4 + 2x + 4, \quad h = x^4 + 3x + 4 \qquad f, g, h \in \mathbf{F}_5[x] \tag{30}$$

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

We close with a remark on computational complexity. 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 finite field. This problem may well be intractable, that is, not solvable in polynomial time. Specifically, even in its simplest form — determining the periods of quadratic 2-sets — this problem seems at least as difficult as that of computing the period of the doubling map over a finite field (cf. comment at the end of Section 4.2), which requires knowledge of the discrete logarithm [12].

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

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

[7] W. Fontana, Algorithmic Chemistry, in *Artificial Life II,* SFI Studied in the Sciences of Complexity, vol X, (1990) 150–209.

[8] 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.

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

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

[11] N. Kataoka and K. Kaneko, Functional Dynamics II: Syntactic structure preprint `http://arXiv.org/abs/adap-org/9907005` (2001) (subm. to *Physica D*).

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

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

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

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

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

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

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

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

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

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

[22] F. Vivaldi and S. Hatjispyros, Galois theory of periodic orbits of rational maps, *Nonlinearity* **5** (1992) 961–978.

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