Chapter 5

Arithmetic dynamical Mordell-Lang

All results in this chapter were obtained in collaboration with Michael Zieve. A co-authored paper is in preparation.

5.1 Introduction

Suppose that X is a quasiprojective variety with an endomorphism $f : X \to X$. The dynamical Mordell-Lang conjecture asserts that if the f-orbit of a point $p \in X$ visits a subvariety $Y \subseteq X$ infinitely often, then it must do so periodically. More precisely we have the following conjecture proposed by Ghioca and Tucker [38, Conj. 1.7].

Conjecture 5.1.1 (Dynamical Mordell-Lang)**.** *Let X be a quasiprojective variety defined over $\mathbb{C}$, let f be an endomorphism of X, let $p \in X(\mathbb{C})$, and let $Y \subseteq X$ be a closed subvariety. Then the set $\{n : f^n(p) \in Y(\mathbb{C})\}$ is a finite union of arithmetic progressions.*

Conjecture 5.1.1 is an analog (of the cyclic case) of the Mordell-Lang theorem from arithmetic geometry—a seminal result due to Faltings [26, 28]. Several special cases have been established but the full conjecture remains open; we refer the reader to Bell, Ghioca, and Tucker [4] for a comprehensive overview of the dynamical Mordell-Lang conjecture and the state of progress up to 2016.

When X is an algebraic curve, a closed subvariety $Y \subseteq X$ is a finite set of points. In that case Conjecture 5.1.1 degenerates to the simple fact that if the orbit of a function f visits a finite set infinitely often, then it must do so periodically. However, Cahn, Jones, and Spear

conjectured [10, Conj. 1.6] that if $X = \mathcal{D}$ is a curve defined over a finitely generated field K of characteristic 0 and if the subvariety Y is replaced by the image of the K-points of a finite map $u : C \to \mathcal{D}$, then a non-trivial arithmetic version of Conjecture 5.1.1 should hold. Our main result settles their conjecture.

Theorem 5.1.2 (Arithmetic Dynamical Mordell-Lang)**.** *Let K be a finitely generated field of characteristic 0. Suppose C and $\mathcal{D}$ are irreducible curves with finite maps $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ defined over K. If $\deg(f) \geq 2$ and $p \in \mathcal{D}(K)$, then $\{n : f^n(p) \in u(C(K))\}$ is a finite union of arithmetic progressions.*

Remark 5.1.3. Several comments on Theorem 5.1.2:

1. An *arithmetic progression* is a subset of the natural numbers of the form $a + b\mathbb{N}$ for some $a, b \in \mathbb{N}$. A singleton is considered to be an arithmetic progression with common difference 0.
2. By an *irreducible curve* we mean a smooth geometrically irreducible projective algebraic variety of dimension 1. Some of our constructions produce singular and reducible curves, for example by taking fiber products of finite maps, but in that case we can replace each singular irreducible component curve with its normalization as we only really need to consider the curves up to birational equivalence.
3. Finitely generated fields of characteristic 0 include all number fields and function fields of algebraic varieties defined over $\overline{\mathbb{Q}}$. The finitely generated hypothesis is used exactly once in our proof to invoke Faltings' theorem relating the genus of a curve to its K-rational points. In Example 5.5.3 we show that this hypothesis is necessary.
4. The $\deg(f) \geq 2$ assumption is also necessary. If $C, \mathcal{D} = \mathbb{P}^1$, $u(x) = x^2$, and $f(x) = x + 1$, then $\{n : f^n(0) \in u(\mathbb{P}^1(\mathbb{Q}))\} = \{m^2 : m \in \mathbb{N}\}$ is not a finite union of arithmetic progressions.
5. The Riemann-Hurwitz formula implies that an irreducible curve $\mathcal{D}$ with an endomorphism of degree at least 2 must have genus $g(\mathcal{D}) \leq 1$ (see Lemma 5.3.2.) Furthermore the assumption that $\mathcal{D}$ has a K-rational point, namely $p \in \mathcal{D}(K)$, implies that $\mathcal{D}$ is isomorphic over K to the projective line $\mathbb{P}^1$ or an elliptic curve $\mathcal{E}$.

Remark 5.1.4. Two notes on related work:

1. Cahn, Jones, and Spear [10, Thm. 1.2] prove Theorem 5.1.2 in the case where $C, \mathcal{D} = \mathbb{P}^1$ and $u : \mathbb{P}^1 \to \mathbb{P}^1$ may be expressed in coordinates as $u(x) = x^m$ for $m \geq 1$. Furthermore they classify the rational functions $f(x)$ for which $L := \{n : f^n(p) \in u(\mathbb{P}^1(K))\}$ is infinite, providing detailed descriptions of L in each case. Their proof passes through their analysis of all situations where L is infinite. Our approach to Theorem 5.1.2 shows that L is a finite union of arithmetic progressions without first giving a complete census of the possible structure of L. In Section 5.1.2 we discuss some progress towards describing the structure of L.
2. Our proof of Theorem 5.1.2 was announced in a talk by Zieve [96] at the *Workshop on Interactions between Model Theory and Arithmetic Dynamics* in 2016. In early 2018 Pakovich [73] presented another proof. Pakovich's approach appears to be related to ours but is formulated in the language of orbifolds, making a direct comparison challenging.

5.1.1 Iterated fiber products

Our strategy for proving Theorem 5.1.2 is to first translate the problem into one of the dynamics of iterated fiber products. Suppose C and $\mathcal{D}$ are irreducible curves defined over a field K with a map $u : C \to \mathcal{D}$ and an endomorphism $f : \mathcal{D} \to \mathcal{D}$. Taking fiber products of the map u with iterates f^n gives a sequence $u_n : C_n \to \mathcal{D}$ of branched covers of $\mathcal{D}$, where $C_n := C \times_{u, f^n} \mathcal{D}$ and u_n is the natural projection. Note that C_n may be reducible; see Section 5.2 for background on fiber products.

$$\begin{array}{ccccccccc} C & \longleftarrow & C_1 & \longleftarrow & C_2 & \longleftarrow & C_3 & \longleftarrow & \cdots \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u_1} & & \downarrow{\scriptstyle u_2} & & \downarrow{\scriptstyle u_3} & & \\ \mathcal{D} & \xleftarrow[f]{} & \mathcal{D} & \xleftarrow[f]{} & \mathcal{D} & \xleftarrow[f]{} & \mathcal{D} & \xleftarrow[f]{} & \cdots. \end{array}$$

We view this as a dynamical system where $u_n : C_n \to \mathcal{D}$ is the nth iterate of f on $u : C \to \mathcal{D}$. Theorem 5.1.2 essentially reduces to showing that u has a finite orbit under iterated fiber products with f whenever the f-orbit of p visits $u(C(K))$ infinitely often in a nontrivial way. Thus we are interested in the dynamics of iterated fiber products of

branched covers $u : C \to \mathcal{D}$.

Theorem 5.1.5 shows that the dynamical behavior of u under iterated fiber products is dictated by the sequence of genera $g(C_n)$. Recall that a *critical value* of a map $u : C \to \mathcal{D}$ is a point $p \in \mathcal{D}(\overline{K})$ with a ramified pre-image. Let $V := \bigcup_{n\geq 0} V_n$ where V_n is the set of critical values of u_n. Given $q \in C(\overline{K})$, let $e_u(q)$ denote the ramification index, or local degree, of u at q. For each point $p \in V$ and $n \geq 0$, define m_p by

$$m_p := \sup_{n\geq 0} \operatorname*{lcm}_{q\in u_n^{-1}(p)} e_{u_n}(q).$$

Note that if $m_p < \infty$, then m_p is the largest ramification index over p under the Galois closure of any u_n with $n \geq 0$ (see Lemma 5.3.7.) We say that the map u is *f-stable* if C_n is geometrically irreducible for all $n \geq 0$.

Theorem 5.1.5. *Let K be a field of characteristic 0, and let $u : C \to \mathcal{D}$, $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K such that* $\deg(f) \geq 2$. *Suppose that u is f-stable.*

1. *If the genus $g(C_n)$ is greater than* 1 *for any $n \geq 0$, then the set of all critical values V is infinite and $g(C_{n+k}) \geq \deg(f)^k - 1$.*
2. *Otherwise the genus $g(C_n)$ is at most* 1 *for all $n \geq 0$ and*
   (a) *V contains at most 4 points.*
   (b) $\displaystyle\sum_{p\in V} 1 - \tfrac{1}{m_p} \leq 2.$
   (c) *If $v_n : \mathcal{G}_n \to \mathcal{D}$ is the Galois closure of $u_n : C_n \to \mathcal{D}$, then the genus $g(\mathcal{G}_n)$ is at most 1 for all $n \geq 0$.*

Remark 5.1.6. Theorem 5.1.5 extends some previous work of Pakovich [74]. Pakovich [74, Thm. 3.1] gives a lower bound for the genus of a fiber product of rational functions assuming irreducibility of the fiber product. Translating his results from the language of orbifolds, they imply that if $g(C_m) > 1$ for some $m \geq 0$, then $g(C_{m+n})$ tends to infinity as $n \to \infty$, which also follows from our Theorem 5.1.5 (1). Pakovich's [74, Thm. 3.1] implies that if u and f are rational functions such that u is f-stable and all C_n have genus 0, then the Galois closure of u has genus at most one; this is part of our conclusion in Theorem 5.1.5 (2c). The main innovation of Theorem 5.1.5 is the uniform bound on ramification for

all iterates u_n, which is essential for our proof of Theorem 5.1.2.

Thus, if u is f-stable, then either the genus of C_n grows exponentially and the maps u_n together have infinitely many critical values, or the genus of C_n is at most one and the maps u_n share a total of 4 critical values with tightly constrained ramification. In the latter case we appeal to topology to show these are precisely the maps with finite orbit under iterated fiber product with f.

Theorem 5.1.7. *Let K be a field of characteristic 0, and let $u : C \to \mathcal{D}$, $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K such that* $\deg(f) \geq 2$. *Suppose that u is f-stable and that the genus $g(C_n)$ is at most 1 for all $n \geq 0$. Then u has a finite orbit under iterated fiber product with f. In particular, for some k, ℓ there is an isomorphism $h : C_{k+\ell} \to C_k$ defined over K such that $u_k \circ h = u_{k+\ell}$.*

Another consequence of Theorem 5.1.5 is a result on the structure of semiconjugates, generalizing a result of Pakovich on semiconjugate rational functions [72, Thm. 1.1]; see Section 5.3.4.

Theorem 5.1.8. *Let K be a field of characteristic 0 and suppose that C and $\mathcal{D}$ are irreducible curves defined over K together with maps u, f, g for which the following diagram commutes,*

$$\begin{array}{ccc} C & \xleftarrow{g} & C \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u} \\ \mathcal{D} & \xleftarrow[f]{} & \mathcal{D} \end{array}$$

If $\deg(f) \geq 2$, *then there exists a decomposition $u = v_1 \circ v_2 \circ \cdots \circ v_k$ with $v_i : C_i \to C_{i-1}$ and maps $g_i : C_i \to C_i$ with $g_0 = f$ and $g_k = g$ such that*

$$\begin{array}{ccc} C_i & \xleftarrow{g_i} & C_i \\ {\scriptstyle v_i}\downarrow & & \downarrow{\scriptstyle v_i} \\ C_{i-1} & \xleftarrow[g_{i-1}]{} & C_{i-1} \end{array}$$

is a fiber product diagram and each v_i has Galois closure with genus at most 1.

In particular, if u has irreducible fiber product with f, then u has Galois closure of genus at most 1.

5.1.2 Arithmetic progression bounds and stability

Given Theorem 5.1.2, one would like to characterize the arithmetic progressions comprising $L := \{n : f^n(p) \in u(C(K))\}$. Theorem 5.1.9 shows these arithmetic progressions may be bounded in terms of $\deg(u)$ alone.

Theorem 5.1.9. *Let K be a finitely generated field of characteristic 0 and let $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K. Let $\deg(f) \geq 2$ and let $d := \deg(u)$. For each $p \in \mathcal{D}(K)$ the set $L := \{n : f^n(p) \in u(C(K))\}$ can be expressed as a finite union of arithmetic progressions $j + k\mathbb{N}$ such that,*

1. *There are at most d distinct positive common differences.*
2. *Each common difference k is bounded by*

$$k \leq K(d) := d!^3 d^{d^3!}.$$

3. *Each minimal value j in a non-trivial arithmetic progression is bounded by*

$$j \leq (d-1)J(d) + K(d),$$

where $J(d) = (d! - 1)(d!!^3 + \log_2(170d! - 84))$.

An important component of the bound $K(d)$ from Theorem 5.1.9 comes from the following result of independent interest.

Theorem 5.1.10 (Geometric Eventual Stability)**.** *Let K be a field of characteristic 0, let $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K such that $\deg(f) \geq 2$. Then there exists a bound $G(d)$ depending only on $d := \deg(u)$ such that for every $m \geq G(d)$ the restriction of $u_m : C_m \to \mathcal{D}$ to each K-irreducible component of C_m is f-stable.*

Furthermore $G(d)$ is given explicitly by

$$G(d) = (d-1)(d! - 1)(d!!^3 + \log_2(170d! - 84)).$$

Remark 5.1.11. Jones and Levy [54, Conj. 1.2] conjectured that for a rational function $f(x) \in K(x)$ with $\deg(f) \geq 2$ and any $b \in K$ not pre-periodic under f, the K-irreducible factorization of (the numerator of) $f^n(x) - b$ would eventually stabilize in the sense that for some $m \geq 1$ all irreducible factors of $f^{m+n}(x) - b$ are gotten by composing the irreducible factors of $f^m(x) - b$ with $f^n(x)$. They call this phenomenon *eventual stability*. Theorem 5.1.10 asserts the same conclusion with $b \in K$ replaced by a finite map u. In particular, if $f(x)$ and $u(y)$ are rational functions, then Theorem 5.1.10 says that the K-irreducible factorization of (the numerator of) $f^n(x) - u(y)$ eventually stabilizes. Thus Theorem 5.1.10 may be viewed as a geometric eventual stability result. In Lemma 5.2.6 we show that a soft version of this stability follows easily from degree considerations; the main content of Theorem 5.1.10 is the bound on the onset of stability in terms of the degree of u alone.

A closely related result shows that if an iterate of f has a decomposition $f^n = u \circ v$, then the left factor u first arises for an iterate bounded explicitly in terms of $\deg(u)$.

Theorem 5.1.12 (Iterate Decomposition Stability)**.** *Let K be a field of characteristic 0, let $u : \mathcal{C} \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K such that* $\deg(f) \geq 2$. *Then there exists a bound $S(d)$ depending only on $d := \deg(u)$ such that if u is a left factor of some iterate $f^n = u \circ v$, then there is an $m \leq S(d)$ such that $f^m = u \circ w$ for some finite map $w : \mathcal{D} \to \mathcal{C}$.*

Furthermore, $S(d)$ is given explicitly by

$$S(d) = (d-1)(d!^3 + \log_2(170d - 84)).$$

Remark 5.1.13. We expect the bounds in Theorems 5.1.9, 5.1.10, and 5.1.12 to be far from sharp. Our main point is that there exist bounds depending only on $\deg(u)$.

These results appear in Section 5.6.

5.2 Iterated fiber products and reduction to the stable case

In this section we review fiber products of curves and introduce the dynamical system of iterated fiber products of a branched cover under an endomorphism of the base. The section culminates with Theorem 5.2.8 which reduces Theorem 5.1.2 to an essential geometric case.

5.2.1 Curves and fiber products

For this chapter we define an *irreducible curve* C over a field K to be a smooth projective variety of dimension 1 over K. If $K(C)$ is the function field of C, then this is equivalent to the field extension $K(C)/K$ having transcendence degree 1. There is a well-known dual equivalence between the category of transcendence degree 1 field extensions of K (or equivalently finite extensions of $K(x)$) and the category of irreducible curves [44, Cor. 6.12] extending the correspondence $C \mapsto K(C)$.

The category of irreducible curves lacks some desirable features. For example, the fiber product of two branched covers of smooth curves is potentially reducible with singular components. As we are only interested in curves up to birational equivalence, the singular components may be replaced with their normalizations. Reducibility is a more fundamental issue. Under duality this is equivalent to the fact that the tensor product of two field extensions of K is not necessarily a field. Nevertheless, if the extensions are separable, then their tensor product is a product of separable field extensions [89, Lem. 00U3]. Thus we formally define a *(reducible) curve* over K as the dual of finite product of finite degree field extensions of $K(x)$. In practice we consider a reducible curve to be a finite union of irreducible curves.

Definition 5.2.1. Suppose $\mathcal{A}, \mathcal{B}, C$ are curves defined over a field K together with maps $f : \mathcal{A} \to C$ and $g : \mathcal{B} \to C$. The *fiber product* $\mathcal{A} \times_C \mathcal{B}$ is the universal curve defined over K together with maps to $\mathcal{A}$ and $\mathcal{B}$ making the following diagram commute.

$$\begin{array}{ccc} \mathcal{A} & \xleftarrow{\tilde{g}} & \mathcal{A} \times_C \mathcal{B} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \tilde{f}} \\ C & \xleftarrow[g]{} & \mathcal{B} \end{array} \tag{5.1}$$

The fiber product, together with its maps to $\mathcal{A}$ and $\mathcal{B}$ is unique up to unique isomorphism.

Remark 5.2.2. Fiber products are characterized by a universal property which is usually formulated set theoretically as saying $\mathcal{A} \times_C \mathcal{B}$ is the set of all $(p, q) \in \mathcal{A} \times \mathcal{B}$ such that $f(p) = g(q)$. Since we are working with smooth curves, our fiber product is actually the normalization of the proper fiber product. This makes the uniqueness of the universal

property of fiber products fail in the following way: if p and q are critical points of f and g respectively, then there may be several points on the normalization of the fiber product which project onto (p, q). The precise situation is described by Abhyankar's lemma (see Theorem 5.3.4.) When we appeal to the universal property of fiber products in this chapter we only ever use the existence.

When discussing fiber products we emphasize the maps over the curves. For example, in the situation of (5.1) we would describe $\mathcal{A} \times_C \mathcal{B}$ as the *fiber product of f and g* and sometimes write $\mathcal{A} \times_{f,g} \mathcal{B}$ when we wish to emphasize the maps involved.

Example 5.2.3. Suppose $\mathcal{A}, \mathcal{B}, C = \mathbb{P}^1$ and let $f, g : \mathbb{P}^1 \to \mathbb{P}^1$ be given in coordinates by rational functions $f(x), g(y)$. Then the fiber product of f and g is the normalization of the irreducible components of the curve $f(x) = g(y)$. For example, if $f(x) = x^2$ and $g(y) = y^2$, then the fiber product of f and g is the reducible curve $x^2 = y^2$. The irreducible components in this case are $x = y$ and $x = -y$ which are both isomorphic to $\mathbb{P}^1$.

Lemma 5.2.4. *If $\mathcal{A} \times_C \mathcal{B}$ is a fiber product as in* (5.1)*, then* $\deg(\tilde{f}) = \deg(f)$ *and* $\deg(\tilde{g}) = \deg(g)$.

Proof. This is clear from the geometric interpretation of fiber products. Algebraically this is equivalent to the assertion that if F and G are finite dimensional A-algebras, then $F \otimes_A G$ is a finite dimensional G-algebra and $[F \otimes_A G : G] = [F : A]$. □

5.2.2 Iterated fiber products

Suppose C and $\mathcal{D}$ are irreducible curves with finite maps $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ defined over K. For $n \geq 0$ we define $u_n : C_n \to \mathcal{D}$ by the fiber product diagram,

$$\begin{array}{ccc} C & \longleftarrow & C_n \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u_n} \\ \mathcal{D} & \xleftarrow[f^n]{} & \mathcal{D}. \end{array}$$

That is, $C_n = C \times_{u, f^n} \mathcal{D}$. In this situation we say *u_n is the fiber product of u with f^n*. Note that u_n is well-defined up to an automorphism of C_n defined over K. The universal

property of fiber products implies that $u_n : C_n \to \mathcal{D}$ may also be defined recursively as the fiber product of u_{n-1} with f,

$$\begin{array}{ccc} C_{n-1} & \longleftarrow & C_n \\ {\scriptstyle u_{n-1}}\downarrow & & \downarrow{\scriptstyle u_n} \\ \mathcal{D} & \xleftarrow[f]{} & \mathcal{D}. \end{array}$$

We view this as a dynamical system where $u_n : C_n \to \mathcal{D}$ is the nth iterated fiber product of u with f.

Definition 5.2.5. If u and f are as defined above, then we say that u is *f-stable* if C_n is geometrically irreducible for all $n \geq 0$. If all C_n are K-irreducible but not necessarily geometrically irreducible, then we say u is *arithmetically f-stable*.

Lemma 5.2.6. *Let K be a field of characteristic 0, and let $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K. If $\deg(f) \geq 2$, then there exists a constant m such that the restriction of u_m to each K-irreducible component of C_m is arithmetically f-stable.*

Proof. The degrees of the restriction of u_n to the K-irreducible components of C_n form a partition λ_n of $\deg(u_n) = \deg(u)$. Note that λ_{n+1} is a refinement of λ_n and $\lambda_n \neq \lambda_{n+1}$ exactly when the restriction of u_n to some irreducible component has a reducible fiber product with f. Since there are only finitely many refinements of a given partition, it follows that the sequence λ_n is eventually constant. Let m be the first index such that $\lambda_{m+n} = \lambda_m$ for all $n \geq 0$, then the restriction of u_m to each K-irreducible component of C_m is arithmetically f-stable. □

Remark 5.2.7. In Theorem 5.6.10 we show that the m in Lemma 5.2.6 may be bounded explicitly in terms of $\deg(u)$.

Theorem 5.2.8 reduces our main result Theorem 5.1.2 to the case where u is f-stable.

Theorem 5.2.8. *If the conclusion of Theorem 5.1.2 holds for all u which are f-stable, then it holds for all u.*

Proof. If $u : C \to \mathcal{D}$ is a finite map and $p \in \mathcal{D}(K)$, then the universal property of fiber products implies that $n \in L_u := \{n : f^n(p) \in u(C_n(K))\}$ if and only if there is some

$q \in C(K)$ such that $f^n(p) = u(q)$ if and only if $p \in u_n(C_n(K))$. Thus if $m \geq 0$ and $v_1, v_2, \ldots, v_k$ are the restrictions of u_m to the K-irreducible components of C_m, then L_u is the union of a finite set and $\bigcup_{i=1}^{k} m + L_{v_i}$. Hence it suffices to prove for some $m \geq 0$ that each L_{v_i} is a finite union of arithmetic progressions.

Let m be the constant given by Lemma 5.2.6. If $v : C_v \to \mathcal{D}$ is a K-irreducible component of C_m which is not geometrically irreducible, then $C_v(K)$ is finite; any K-point must lie on the intersection of the geometrically irreducible components of C_v, which is a finite set. Thus L_v can only be infinite if p is pre-periodic under f, in which case L_u is plainly a finite union of arithmetic progressions. Hence the only irreducible components of C_m which potentially contribute infinitely many integers to L_u are those $v : C_v \to \mathcal{D}$ which are f-stable. Therefore it suffices to prove that L_u is a finite union of arithmetic progressions for f-stable maps u. □

5.3 Stable case

In this section we analyze the dynamics of f-stable maps u under iterated fiber products. Theorems 5.3.3 and 5.3.9 show there is a dichotomy based on the genera of the sequence of curves C_n: either the genera grow exponentially with n or all C_n have genus at most 1. In the latter case we show that the ramification of the iterates u_n is uniformly constrained. We end the section with Theorem 5.3.10, an application of these results to the structure of semiconjugates.

5.3.1 The Riemann-Hurwitz formula

If C is a smooth irreducible curve defined over $\mathbb{C}$, then $C(\mathbb{C})$ may be viewed as an oriented topological surface homeomorphic to a sphere with $g(C)$ "handles" attached; this number $g(C)$ is called the *genus* of C. The genus is defined algebraically over any characteristic 0 field as the dimension of the vector space of holomorphic differentials on C or as the dimension of the Jacobian variety of C. The genus $g(C)$ of an irreducible curve C governs both the arithmetic and geometry of C. Theorem 5.3.9 shows that the behavior of u under iterated fiber products with f is largely determined by the genera of the curves C_n.

If $u : C \to \mathcal{D}$ is a map of curves, then a *critical point* of u is a point $q \in C(\overline{K})$ with ramification index $e_u(q) > 1$. The image of a critical point $p = u(q)$ is called a *critical value*. Geometrically the ramification index $e_u(q)$ is the local degree of u in a small neighborhood of q. For example, if $u : \mathbb{P}^1 \to \mathbb{P}^1$ is the map defined in coordinates by $u(x) = x^d$, then $e_u(q) = 1$ if $q \neq 0, \infty$ and $e_u(q) = d$ for $q = 0, \infty$. The ramification index can be defined algebraically in several equivalent ways. For example, if $\mathcal{O}(\mathcal{D})_p$ is the local ring of functions on $\mathcal{D}$ which are regular at p, then $\mathcal{O}(C)_q$ is naturally an extension of $\mathcal{O}(\mathcal{D})_p$ and the ramification index $e_u(q)$ is the normalized valuation of the maximal ideal of $\mathcal{O}(\mathcal{D})_p$ in $\mathcal{O}(C)_q$. See Stichtenoth [87, Sec. 3.1] for more background.

A fundamental tool for analyzing maps between irreducible curves is the Riemann-Hurwitz formula. Note that if C is a curve defined over a field K, then we write "$q \in C$" as an abbreviation for $q \in C(\overline{K})$. As a general rule we will only specify the field over which the point is defined when the point is K-rational.

Theorem 5.3.1 (Riemann-Hurwitz)**.** *Let K be a field of characteristic 0 and let $u : C \to \mathcal{D}$ be a finite map between irreducible curves defined over K. If $\chi(C) := 2 - 2g(C)$ is the Euler characteristic of C, then*

$$\chi(C) = \deg(u)\chi(\mathcal{D}) - \sum_{q \in C} e_u(q) - 1.$$

Proof. See Hartshorne [44, Cor. 2.4]. □

Lemma 5.3.2 records several well-known consequences of the Riemann-Hurwitz formula for later reference.

Lemma 5.3.2. *Let K be a field of characteristic 0.*

1. *If $u : C \to \mathcal{D}$ is a finite map of irreducible curves, then $g(C) \geq g(\mathcal{D})$.*
2. *If $f : \mathcal{D} \to \mathcal{D}$ is an endomorphism of an irreducible curve $\mathcal{D}$ with degree $\deg(f) \geq 2$, then $\mathcal{D}$ has genus at most 1.*
3. *If $u : C \to \mathcal{D}$ is a finite map between irreducible genus 1 curves, then u is unramified and Galois.*

Proof. 1. Since $\chi(C) := 2 - 2g(C)$, we can express the Riemann-Hurwitz formula as

$$g(C) - 1 = d(g(\mathcal{D}) - 1) + \frac{1}{2}\sum_{q \in C} e_u(q) - 1.$$

Since the genus is a non-negative integer, it follows that $g(C) \geq g(\mathcal{D})$.

2. The Riemann-Hurwitz formula implies that

$$(\deg(f) - 1)\chi(\mathcal{D}) = \sum_{q \in \mathcal{D}} e_f(q) - 1.$$

Since the right hand side is non-negative and $\deg(f) - 1 > 0$ it follows that $\chi(\mathcal{D}) \geq 0$ which by $\chi(\mathcal{D}) = 2 - 2g(\mathcal{D})$ implies that $g(\mathcal{D}) = 0$ or 1.

3. If C and $\mathcal{D}$ have genus 1, then $\chi(C) = \chi(\mathcal{D}) = 0$ and the Riemann-Hurwitz formula implies that $e_u(q) = 1$ for all $q \in C$. For a proof that u is Galois see Silverman [82, Thm. 4.10 (c)]. □

5.3.2 Unbounded genus

Theorem 5.3.3 shows that in the f-stable case, if any iterate of u has genus larger than 1, then the genera grow exponentially in the orbit of u under iterated fiber products with f.

Theorem 5.3.3. *Let K be a field of characteristic 0, let $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K. Let $V_n \subseteq \mathcal{D}$ be the set of critical values of u_n and let $V := \bigcup_n V_n$. Suppose $d_f := \deg(f) \geq 2$ and u is f-stable. If $g(C_m) > 1$ for some $m \geq 0$, then*

1. *$g(C_{m+n}) \geq d_f^n + 1$.*
2. *$|V_{m+n}| \geq \left(\frac{2}{\deg(u)-1}\right) d_f^n$.*
3. *V is infinite.*

Thus if $g(C_m)$ is bounded, then $g(C_m) \leq 1$ for all $m \geq 0$.

Proof. Suppose $g(C_m) > 1$.

1. Let $\tilde{f}_n : C_{m+n} \to C_m$ be the map parallel to f^n in the fiber product of u_m with f^n. Note that $\deg(\tilde{f}_n) = \deg(f)^n = d_f^n$ by Lemma 5.2.4. Applying the Riemann-Hurwitz

formula to $\tilde{f_n}$ gives

$$2(g(C_{m+n})-1) = 2(g(C_m)-1)d_f^n + \sum_{q\in C_{m+n}} e_{\tilde{f_n}}(q) - 1 \geq 2d_f^n.$$

Hence $g(C_{m+n}) - 1 \geq d_f^n$.

2. Since $\mathcal{D}$ is assumed to be irreducible with an endomorphism of degree at least 2, Lemma 5.3.2 (2) implies that $g(\mathcal{D}) \leq 1$. Recall that $\sum_{q\in u^{-1}(p)} e_u(q) = \deg(u)$ for any finite map u and $p \in \mathcal{D}$, hence $e_{u_n}(q) \leq \deg(u)$ for all $n \geq 0$. Riemann-Hurwitz applied to u_{m+n} gives us

$$\begin{aligned} 2(g(C_{m+n})-1) &= 2(g(\mathcal{D})-1) + \sum_{q\in\mathcal{D}} e_{u_{m+n}}(q) - 1 \\ &\leq \sum_{q\in V_{m+n}} e_{u_{m+n}}(q) - 1 \\ &\leq (\deg(u)-1)|V_{m+n}|. \end{aligned}$$

From (1) it follows that

$$|V_{m+n}| \geq \Big(\frac{2}{\deg(u)-1}\Big) d_f^n. \tag{5.2}$$

3. Since $V = \bigcup_n V_n$ and $d \geq 2$, taking a limit of (5.2) as $n \to \infty$ shows that V is infinite. □

5.3.3 Bounded genus

We next consider the case when u is f-stable and all C_n have genus at most 1. Theorem 5.3.6 and Corollary 5.3.8 are general results on the constraints derived from u having a small genus fiber product with a high degree map. Theorem 5.3.9 applies these constraints in a dynamical setting.

Consider the fiber product diagram,

$$\begin{array}{ccc} \mathcal{A} & \xleftarrow{\tilde{g}} & \mathcal{A}\times_C \mathcal{B} \\ {\scriptstyle f}\downarrow & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle \tilde{f}} \\ C & \xleftarrow[g]{} & \mathcal{B}. \end{array} \tag{5.3}$$

The universal mapping property of fiber products implies that points $r \in \mathcal{A} \times_C \mathcal{B}$ correspond to pairs of points $p \in \mathcal{A}$ and $q \in \mathcal{B}$ such that $f(p) = g(q)$. Abhyankar's lemma determines the ramification of $h := f \circ \tilde{g} = g \circ \tilde{f}$ at a point $(p, q) \in \mathcal{A} \times_C \mathcal{B}$ in terms of the ramification indices $e_f(p)$ and $e_g(q)$.

Theorem 5.3.4 (Abhyankar's lemma)**.** *If $r \in \mathcal{A} \times_{f,g} \mathcal{B}$ corresponds to a pair (p, q) and $h := f \circ \tilde{g} = g \circ \tilde{f}$, then the ramification index of r under h is*

$$e_h(r) = \operatorname{lcm}(e_f(p), e_g(q)).$$

Proof. See, for example, Stichtenoth [87, Thm. 3.9.1]. □

Remark 5.3.5. A consequence of Abhyankar's lemma is that the number of points on the normalization of the fiber product of f and g projecting to p and q is $\gcd(e_f(p), e_g(q))$. This accounts for the failure of uniqueness of the universal property of fiber products for smooth curves.

Let B_f denote the set of all finite maps $u : C_u \to \mathcal{D}$ such that

1. C_u is irreducible, and
2. If $u' : C'_u \to \mathcal{D}$ is the fiber product of u with f, then C'_u is irreducible with genus at most 1.

For each $d \geq 1$, let $B_{f,d} \subseteq B_f$ be the subset of all $u : C \to \mathcal{D}$ with degree d. If $p \in \mathcal{D}$ and $u \in B_{f,d}$, then define m'_p by

$$m'_p := \sup_{u \in B_{f,d}} \operatorname*{lcm}_{q \in u^{-1}(p)} e_u(q).$$

Theorem 5.3.6. *Let K be a field of characteristic 0 and let $f : \mathcal{D} \to \mathcal{D}$ be an endomorphism of an irreducible curve $\mathcal{D}$ defined over K such that $d_f := \deg(f) \geq 2$. Let $V_{f,d} := \bigcup_{u \in B_{f,d}} V_u$ where V_u is the set of critical values of $u \in B_{f,d}$. Suppose d satisfies $1 \leq d < d_f/2$, then*

$$\sum_{p \in V_{f,d}} 1 - \frac{1}{m'_p} \leq \frac{2d_f - 2}{d_f - 2d}. \tag{5.4}$$

Furthermore, $V_{f,d}$ is finite with

$$|V_{f,d}| \leq \frac{4d_f - 4}{d_f - 2d}.$$

Proof. Since $f : \mathcal{D} \to \mathcal{D}$ is an endomorphism of degree $d_f := \deg(f)$ at least 2, the genus of $\mathcal{D}$ is at most 1 by Lemma 5.3.2 (2). If $\mathcal{D}$ has genus 1, then so must all C_u for $u \in B_{f,d}$. Finite maps between genus 1 curves are unramified by Lemma 5.3.2 (3). Thus $V_{f,d}$ is empty and our claim is immediate.

Now suppose that $\mathcal{D}$ has genus 0. Riemann-Hurwitz applied to f gives

$$2d_f - 2 = \sum_{q \in \mathcal{D}} e_f(q) - 1 \geq \sum_{p \in V_{f,d}} \sum_{q \in f^{-1}(p)} e_f(q) - 1 = \sum_{p \in V_{f,d}} d_f - |f^{-1}(p)|. \tag{5.5}$$

We claim that for each critical value $p \in V_{f,d}$,

$$d_f - |f^{-1}(p)| \geq \Big(d_f - 2d\Big)\Big(1 - \frac{1}{m'_p}\Big). \tag{5.6}$$

For each $p \in V_{f,d}$ and $u \in B_{f,d}$ let $m_{p,u}$ be defined by

$$m_{p,u} := \operatorname*{lcm}_{q \in u^{-1}(p)} e_u(q).$$

Then $m'_p = \sup_{u \in B_{f,d}} m_{p,u}$. Suppose that $q \in f^{-1}(p)$. If $u \in B_{f,d}$ and $e_f(q)$ is not divisible by $m_{p,u}$ then Abhyankar's lemma implies that q is a critical value of $u' : C'_u \to \mathcal{D}$, the fiber product of u with f. Since $g(C'_u) \leq 1$ by the definition of $B_{f,d}$, Riemann-Hurwitz bounds the size of $V_{u'}$, the set of critical values of u', by

$$|V_{u'}| \leq \sum_{q \in C'_u} e_{u'}(q) - 1 = 2d + 2(g(C'_u) - 1) \leq 2d.$$

Hence $m_{p,u}$ divides $e_f(q)$ for all but at most $2d$ points $q \in f^{-1}(p)$. Therefore, for $u \in B_{f,d}$,

$$|f^{-1}(p)| \leq 2d + \frac{d_f - 2d}{m_{p,u}}.$$

Since this holds for all $u \in B_{f,d}$, we have

$$|f^{-1}(p)| \leq 2d + \frac{d_f - 2d}{m'_p}$$

and (5.6) follows. Combining (5.5), (5.6), and our assumption that $d_f - 2d > 0$ gives

$$2d_f - 2 \geq \sum_{p \in V_{f,d}} \Big(d_f - 2d\Big)\Big(1 - \frac{1}{m'_p}\Big) \Longrightarrow \frac{2d_f - 2}{d_f - 2d} \geq \sum_{p \in V_{f,d}} 1 - \frac{1}{m'_p}.$$

Since $m'_p \geq 2$ for each $p \in V_{f,d}$ it follows that

$$\frac{2d_f - 2}{d_f - 2d} \geq \sum_{p \in V_{f,d}} 1 - \frac{1}{m'_p} \geq \frac{|V_{f,d}|}{2} \Longrightarrow |V_{f,d}| \leq \frac{4d_f - 2}{d_f - 2d}. \qquad \square$$

Theorem 5.3.6 shows that the collection of all maps u of a given degree having an irreducible fiber product with f of genus at most 1 share a small set of common critical values with uniformly constrained ramification. For $d = \deg(u)$ fixed, the upper bound in (5.4) approaches 2 from above as $d_f \to \infty$. In Corollary 5.3.8 we show that if d_f is sufficiently large with respect to d, then all such maps u have Galois closure with genus at most 1.

Lemma 5.3.7. *Let $u : \mathcal{C} \to \mathcal{D}$ be a finite map between irreducible curves and let $v : \mathcal{G} \to \mathcal{D}$ be the Galois closure. Then for each $p \in \mathcal{D}$, the ramification index of v at any point $r \in v^{-1}(p)$ is*

$$e_v(r) = m_{p,u} := \operatorname*{lcm}_{q \in u^{-1}(p)} e_u(q).$$

Thus the critical values of v are the same as the critical values of u.

Proof. This is easiest to see in the language of fields. The Galois closure of $K(\mathcal{C})/K(\mathcal{D})$ is the compositum of all the conjugates of $K(\mathcal{C})$. The set of ramification indices over a point $p \in \mathcal{D}$ is the same in all conjugates of $K(\mathcal{C})$, and the common ramification index in the Galois closure is the least common multiple of this set by Abhyankar's lemma (Theorem 5.3.4.) Note that this implies that any point $p \in \mathcal{D}$ which is not a critical value of u will not be a critical value for the Galois closure of v. $\square$

Corollary 5.3.8. *Let K be a field of characteristic 0, let $f : \mathcal{D} \to \mathcal{D}$ be an endomorphism of the irreducible curve $\mathcal{D}$ defined over K. If $d \geq 1$ and $d_f := \deg(f) > 170d - 84$, then*

1. $\sum_{p \in V_{f,d}} 1 - \frac{1}{m'_p} \leq 2$,
2. $V_{f,d}$ *has at most 4 elements,*
3. *If $v : \mathcal{G} \to \mathcal{D}$ is the Galois closure of $u \in B_{f,d}$, then $\mathcal{G}$ has genus at most 1.*

Proof. 1. The inequality $d_f > 170d - 84$ is equivalent to

$$\frac{2d_f - 2}{d_f - 2d} \leq 2 + \frac{1}{42}.$$

Thus by Theorem 5.3.6 we have

$$\sum_{p \in V_{f,d}} 1 - \frac{1}{m'_p} < 2 + \frac{1}{42}.$$

A well-known computation implies that if a sum of this form with m'_p positive integers is less than $2 + \frac{1}{42}$, then it is at most 2 (see, for example, Miranda [64, Lem. 3.8 (c)].) Therefore,

$$\sum_{p \in V_{f,d}} 1 - \frac{1}{m'_p} \leq 2.$$

2. Since $m'_p \geq 2$ for each $p \in V_{f,d}$, it follows that $1 - \frac{1}{m'_p} \geq \frac{1}{2}$. Hence $V_{f,d}$ has at most 4 points.

3. If $u \in B_{f,d}$ and $v : \mathcal{G} \to \mathcal{D}$ is the Galois closure of $u : C \to \mathcal{D}$, then Lemma 5.3.7 implies that $m_{p,u}$ is the common ramification index of each point $q \in v^{-1}(p)$ for $p \in \mathcal{D}$.

Therefore, by Riemann-Hurwitz applied to v we have

$$\begin{aligned} 2(g(\mathcal{G})-1) &= -2\deg(v) + \sum_{q\in\mathcal{G}} e_v(q) - 1 \\ &= \deg(v)\Big(-2 + \sum_{p\in\mathcal{D}} 1 - \frac{1}{m_{p,u}}\Big) \\ &\leq \deg(v)\Big(-2 + \sum_{p\in V_{f,d}} 1 - \frac{1}{m_p}\Big) \\ &\leq 0. \end{aligned}$$

Hence $g(\mathcal{G}) \leq 1$. □

We now apply Theorem 5.3.3 and Corollary 5.3.8 to the iterates of u under f when u is f-stable.

Theorem 5.3.9. *Let K be a field of characteristic 0 and suppose that $u : \mathcal{C} \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ are finite maps between irreducible curves defined over K such that $d_f = \deg(f) \geq 2$. Let $m_p := \sup_n \operatorname{lcm}_{q\in u_n^{-1}(p)} e_{u_n}(q)$. If u is f-stable and $g(\mathcal{C}_n) \leq 1$ for all $n \geq 0$, then*

1. *$V := \bigcup_{n\geq 0} V_n$ has at most 4 points where V_n is the set of critical values of u_n,*
2. *$\sum_{p\in V} 1 - \frac{1}{m_p} \leq 2$*
3. *For each $n \geq 0$, u_n has Galois closure $v_n : \mathcal{G}_n \to \mathcal{D}$ with $g(\mathcal{G}_n) \leq 1$.*

Proof. Let $d := \deg(u)$. Since u is f-stable with $g(\mathcal{C}_n) \leq 1$ for all $n \geq 0$ we see that for each $m \geq 1$, $u_n \in B_{f^m,d}$ for all $n \geq 0$. If $m > \log_2(170d - 84)$, then $d_f \geq 2$ implies that $\deg(f^m) > 170d - 84$. Thus $m_p \leq m'_p$ with $m'_p := \sup_{u'\in B_{f^m,d}} m_{p,u'}$ for all $p \in V$. Thus by Corollary 5.3.8 we have

$$\sum_{p\in V} 1 - \frac{1}{m_p} \leq \sum_{p\in V_{f^m,d}} 1 - \frac{1}{m'_p} \leq 2,$$

hence V has at most 4 points and each u_n has Galois closure $v_n : \mathcal{G}_n \to \mathcal{D}$ with $g(\mathcal{G}_n) \leq 1$. □

5.3.4 Semiconjugates

Before proceeding with the proof of our main result we give an application of Theorem 5.3.9 to the structure of semiconjugates. Recall that endomorphisms $f : \mathcal{D} \to \mathcal{D}$ and $g : C \to C$ are called *semiconjugates* if there is a finite map $u : C \to \mathcal{D}$ such that the following diagram commutes,

$$\begin{array}{ccc} C & \xleftarrow{g} & C \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u} \\ \mathcal{D} & \xleftarrow[f]{} & \mathcal{D} \end{array}$$

In other words, f, g, and u satisfy the functional equation $u \circ g = f \circ u$. Theorem 5.3.10 shows that if we have a semiconjugation $u \circ g = f \circ u$ and $\deg(f) \geq 2$, then u factors into a composition of maps $u = v_1 \circ v_2 \circ \cdots \circ v_k$ such that each v_i has Galois closure of genus at most 1.

Theorem 5.3.10. *Let K be a field of characteristic 0 and suppose that C and $\mathcal{D}$ are irreducible curves defined over K together with maps u, f, g for which the following diagram commutes,*

$$\begin{array}{ccc} C & \xleftarrow{g} & C \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u} \\ \mathcal{D} & \xleftarrow[f]{} & \mathcal{D} \end{array} \tag{5.7}$$

If $\deg(f) \geq 2$, then there exists a decomposition $u = v_1 \circ v_2 \circ \cdots \circ v_k$ with $v_i : C_i \to C_{i-1}$ and maps $g_i : C_i \to C_i$ with $g_0 = f$ and $g_k = g$ such that for each i, either there is some map h for which $g_i = h \circ v_i$ and $g_{i-1} = v_i \circ h$ or

$$\begin{array}{ccc} C_i & \xleftarrow{g_i} & C_i \\ {\scriptstyle v_i}\downarrow & & \downarrow{\scriptstyle v_i} \\ C_{i-1} & \xleftarrow[g_{i-1}]{} & C_{i-1} \end{array}$$

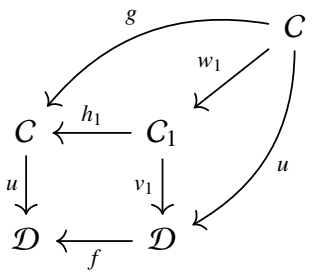
is a fiber product diagram and v_i has Galois closure with genus at most 1.

In particular, if u has irreducible fiber product with f, then u has Galois closure of genus at most 1.

Proof. We proceed by induction on $\deg(u)$. Since f has degree at least 2 it follows that $g(\mathcal{D}) \leq 1$. Hence if $\deg(u) = 1$, then u is Galois and an isomorphism so $g(C) = g(\mathcal{D}) \leq 1$. Now suppose that $\deg(u) > 1$ and that our conclusion holds for all u with smaller degree and all maps f with degree at least 2.

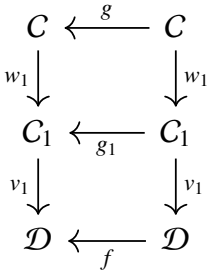
If the fiber product of u with f is irreducible, then the universal property of fiber products implies that (5.7) is a fiber product diagram. Therefore, in this case, u is fixed by f under iterated fiber product. Hence u is f-stable and $C_n = C$ has genus at most 1 for all $n \geq 0$. Then Theorem 5.3.9 implies that u has Galois closure with genus at most 1.

If the fiber product of u with f is reducible, then (5.7) factors through some irreducible component $v_1 : C_1 \to \mathcal{D}$ of the fiber product. It follows that $u = v_1 \circ w_1$ and $g = h_1 \circ w_1$ for some $w_1 : C \to C_1$ and $h_1 : C_1 \to C$.



If $\deg(v_1) = 1$, then without loss of generality we can suppose that v_1 is the identity and thus $w_1 = u$. Therefore $g = h_1 \circ u$ and $f = u \circ h_1$.

Now suppose that $\deg(v_1) > 1$. Setting $g_1 := w_1 \circ h_1$ the following diagram commutes



Since v_1 and w_1 have degree strictly smaller than u and $\deg(g_1) \geq 2$, it follows from our induction hypothesis that they each have the desired decomposition. □

As a special case of Theorem 5.3.10 we deduce a result of Pakovich for semiconjugate rational functions. We state Pakovich's result in language consistent with this chapter.

Theorem 5.3.11 ([72, Thm. 1.1])**.** *Suppose that $u(x), g(x), f(x) \in K(x)$ are rational functions such that* $\deg(f) \geq 2$ *and $u \circ g = f \circ u$, then either the fiber product of u and f is reducible or the Galois closure of u has genus at most 1.*

5.4 Finite orbits from topology

Recall that a finite map $u : C \to \mathcal{D}$ between irreducible curves may be interpreted as a branched cover of $\mathcal{D}$. Theorem 5.4.2 uses the topology of branched covers of curves to show that if u is an f-stable with an orbit of bounded genus, then u has a finite orbit up to isomorphism over K.

If $u : C \to \mathcal{D}$ is f-stable with $g(C_n) \leq 1$ for all $n \geq 0$, then Theorem 5.3.9 implies that there is a subset $V \subseteq \mathcal{D}$ with at most 4 points such that the critical values of each u_n are contained in V. Branched covers of a curve $\mathcal{D}(\mathbb{C})$ with critical values in a set V are determined topologically by permutation representations of the fundamental group of $\mathcal{D}(\mathbb{C}) \setminus V$. This correspondence may be transferred from $\mathbb{C}$ to any algebraically closed field $\overline{K}$ of characteristic 0 using standard methods.

Suppose $v : C_v \to \mathcal{D}$ and $w : C_w \to \mathcal{D}$ are branched covers defined over a field K. We say that v and w are isomorphic over an extension L/K if there is an isomorphism $h : C_v \to C_w$ defined over L such that $w \circ h = v$. If v and w are isomorphic over an extension L but potentially not over K, then we say w is a *twist* of v *split* over L. If L/K is a Galois extension, then to each twist w of v split over L we may associate a function $c_w : \mathrm{Gal}(L/K) \to \mathrm{Aut}(v)$ called a 1-*cocycle* which represents an element of the *first (non-abelian) group cohomology* of $\mathrm{Gal}(L/K)$ valued in $\mathrm{Aut}(v)$ and denoted $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(v))$.

Lemma 5.4.1. *Suppose $u : C \to \mathcal{D}$ is a finite map defined over K and L/K is a finite Galois extension.*

1. *If v and w are twists of u split over L, then v is isomorphic to w over K if and only if they determine the same cohomology class in $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(u))$.*

2. $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(u))$ *is finite and thus there are finitely many* K*-isomorphism classes of twists of* u *split over* L.

Proof. 1. See Appendix 5.8 for a proof of this claim and for a general overview of non-abelian first group cohomology and its relation to twists.

2. Since $\mathrm{Gal}(L/K)$ and $\mathrm{Aut}(u)$ are finite groups, there are finitely many possible 1-cocycles, hence $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(u))$ is finite. It then follows from the previous claim that there are finitely many twists of u split over K. □

As noted above, twists and non-abelian first group cohomology are discussed further in Appendix 5.8. We also refer the reader to Silverman [81, Sec. 4.7, 4.8].

Theorem 5.4.2. *Let* K *be a field of characteristic 0, let* $u : \mathcal{C} \to \mathcal{D}$ *and* $f : \mathcal{D} \to \mathcal{D}$ *be finite maps between irreducible curves defined over* K*. If* $\deg(f) \geq 2$*,* u *is* f*-stable, and* $g(\mathcal{C}_n) \leq 1$ *for all* $n \geq 0$*, then* u *has a finite orbit under iterated fiber product with* f *up to isomorphism over* K*. In particular, for some* j, k *with* $k \geq 1$ *there is an isomorphism* $h : \mathcal{C}_{j+k} \to \mathcal{C}_j$ *defined over* K *such that* $u_j \circ h = u_{j+k}$.

Proof. Since u is f-stable with $g(\mathcal{C}_n) \leq 1$ for all $n \geq 0$, Theorem 5.3.9 (2) implies that there is a set $V \subseteq \mathcal{D}(\overline{K})$ with at most 4 elements such that the critical values of u_n are contained in V for all $n \geq 0$. Choose some embedding $\overline{K} \hookrightarrow \mathbb{C}$ so that we may consider $\mathcal{D}$ as a curve over $\mathbb{C}$. If $V' \subseteq \mathcal{D}(\mathbb{C})$ is any finite subset of points, then the degree d irreducible branched covers $v : \mathcal{C} \to \mathcal{D}$ with critical values contained in V' correspond to sets of d elements with a transitive action of the fundamental group of $\mathcal{D}(\mathbb{C}) \setminus V'$ (see, for example, Völklein [91, Chp. 4]). Since this fundamental group is finitely generated, there are finitely many such transitive actions. Therefore there are finitely many $\mathbb{C}$-isomorphism classes of branched covers in the f-orbit of u. Each such branched cover descends uniquely up to $\overline{K}$-isomorphism to a cover defined over $\overline{K}$ [91, Thm. 7.9], hence u has a finite f-orbit up to $\overline{K}$-isomorphism.

Say $u_j \cong u_{j+k}$ over $\overline{K}$ with $j \geq 0$ and $k \geq 1$. This isomorphism is defined over some finite Galois extension L/K. Thus u has a finite f-orbit over L. For each $\ell \geq 0$, $u_{j+k\ell}$ is a twist of u_j split over L. Lemma 5.4.1 implies there are finitely many such twists. We conclude that u has a finite orbit over K. □

5.5 Arithmetic Dynamical Mordell-Lang

Recall the following seminal result due to Faltings.

Theorem 5.5.1 (Faltings [27, Thm. 3])**.** *Let K be a finitely generated field of characteristic 0 and suppose C is an irreducible curve defined over K. If C has infinitely many K-rational points, then $g(C) \leq 1$.*

We now prove our main result.

Theorem 5.5.2. *Let K be a finitely generated field of characteristic 0, let $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K. If $\deg(f) \geq 2$ and $p \in \mathcal{D}(K)$, then $\{n : f^n(p) \in u(C(K))\}$ is a finite union of arithmetic progressions.*

Proof. By Theorem 5.2.8 it suffices to prove the result when u is f-stable. Let $L = \{n : f^n(p) \in u(C(K))\}$. If L is finite, then we have nothing to show since a singleton is an arithmetic progression with common difference 0. If p has a finite f-orbit, then any periodic iterate $f^j(p)$ in $u(C(K))$ with period k contributes $j + k\mathbb{N}$ to L. Thus, in this case, L is clearly a finite union of arithmetic progressions.

Finally suppose that L is infinite and p has an infinite f-orbit. Then for each $n \geq 0$ there are infinitely many points $q \in \mathcal{D}(K)$ such that $f^n(q) \in u(C(K))$. It follows that the fiber product C_n has infinitely many K-rational points. Thus $g(C_n) \leq 1$ for each $n \geq 0$ by Faltings' theorem.

Therefore u is f-stable and $g(C_n) \leq 1$ for all $n \geq 0$ and hence Theorem 5.4.2 implies that u has a finite orbit up to isomorphism over K. Since fiber products are only defined up to isomorphism over K we may suppose that $u_j = u_{j+k}$ for some $j \geq 0$ and $k \geq 1$. Recall that the universal property of fiber products tells us that $n \in L$ if and only if $p \in u_n(C_n(K))$. Thus L may be expressed as the union of a finite set and finitely many arithmetic progressions with common difference k. □

Example 5.5.3. The assumption that K is finitely generated is necessary. Consider the polynomial $f(x) = x(x-1) + 1 = x^2 - x + 1$. It follows by induction that

$$f^m(2) = 1 + \prod_{k=0}^{m-1} f^k(2).$$

Hence $\gcd(f^m(2), f^n(2)) = 1$ when $m \neq n$. The polynomial $f(x)$ has a fixed point modulo 4 at -1 and $f(2) = 3 \equiv -1 \bmod 4$. It follows that $f^m(2)$ is not a square in $\mathbb{Q}$ for any $m \geq 0$. Consider the field K generated over $\mathbb{Q}$ by $\sqrt{f^{m^2}(2)}$ for $m \geq 0$. This field is not finitely generated since all pairs of iterates of 2 are coprime. Furthermore, if $u(x) = x^2$, then

$$\{n : f^n(2) \in u(\mathbb{P}^1(K))\} = \{m^2 : m \geq 0\},$$

which is not a finite union of arithmetic progressions. Therefore K must be finitely generated for the conclusion of Theorem 5.1.2 to hold. However, this hypothesis is only invoked when we appeal to Faltings's theorem.

Remark 5.5.4. The sequence $s_n = f^n(2)$ considered above is known as *Sylvester's sequence*. This sequence s_n and the polynomial $f(x)$ were studied from an arithmetic dynamical point of view by Odoni [70].

Example 5.5.5. Let $K = \mathbb{Q}$ and let $u, f : \mathbb{P}^1 \to \mathbb{P}^1$ be the rational functions given in coordinates by

$$u(x) = -x^2 \qquad\qquad f(x) = \frac{1}{1-x}\left(\frac{x^3 - x + 1}{x^3 - 2x^2 + x - 1}\right)^2 = \frac{1}{1-x}g(x)^2.$$

If $p = 2 \in \mathbb{P}^1(\mathbb{Q})$, then we claim that

$$L := \{n : f^n(2) \in u(\mathbb{P}^1(\mathbb{Q}))\} = 1 + 3\mathbb{N}.$$

The common difference of 3 comes from the period of u under iterated fiber product with f. If u_1 and u_2 are the rational functions

$$u_1(x) = 1 + x^2 \qquad\qquad u_2(x) = \frac{x^2}{x^2 + 1},$$

then one may check that $C_n \cong \mathbb{P}^1$ for all n and that there are rational functions $h_i(x)$ such that $u_i(h_i(x)) = f(u_{i+1}(x))$ for $i = 0, 1, 2$ where $u_0(x) = u(x) = -x^2$ and the subscripts are considered modulo 3. Thus u has period 3 under iterated fiber product with f. Since $f(2) = -g(2)^2 = u(g(2))$, it follows that $f^{1+3k}(2) \in u(\mathbb{P}^1(\mathbb{Q}))$ for all $k \geq 0$. This is

equivalent to $p \in u_1(\mathbb{P}^1(\mathbb{Q}))$, and in fact $p = 2 = u_1(1)$. On the other hand, neither $u_0(x) = -x^2 = 2$ nor $u_2(x) = \frac{x^2}{x^2+1} = 2$ has a solution in $\mathbb{P}^1(\mathbb{Q})$. Hence $p = 2$ is not in $u_0(\mathbb{P}^1(\mathbb{Q}))$ or $u_2(\mathbb{P}^1(\mathbb{Q}))$ and therefore $3k, 2 + 3k \notin L$ for any $k \geq 0$.

5.6 Bounds on arithmetic progressions and stability results

Theorem 5.6.11 below bounds in terms of $d := \deg(u)$ alone the minimal value, common difference, and number of distinct common differences of arithmetic progressions comprising $\{n : f^n(p) \in u(C(K))\}$. On our way to that result we deduce several others demonstrating stability phenomena arising in the dynamics of iterated fiber products. Throughout this section we make frequent reference to the following assumption.

Assumption 5.6.1. Let K be a field of characteristic 0 and let $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K such that $\deg(f) \geq 2$ and $d := \deg(u)$.

Theorem 5.6.2 shows that if sufficiently many iterates of u are geometrically irreducible with genus at most 1, then all iterates must be.

Theorem 5.6.2. *Suppose Assumption 5.6.1. There is a function $M(d)$ of $d := \deg(u)$ such that if $m > M(d)$ and the fiber product of u with f^m is irreducible with $g(C_m) \leq 1$, then u has a finite orbit and C_n is irreducible with genus $g(C_n) \leq 1$ for all $n \geq 0$. In particular, the following function will suffice,*

$$M(d) := d!^3 + \log_2(170d - 84).$$

Proof. Let $m = m_0 + m_1$ where $m_0 \geq d!^3$ and $m_1 > \log_2(170d - 84)$ are integers and suppose that the fiber product of u with $f^{m_0+m_1}$ is irreducible with genus at most one. Since $\deg(f^{m_1}) > 170d - 84$, Corollary 5.3.8 implies that there is a set $V \subseteq \mathcal{D}$ of at most 4 points such that for each $0 \leq k \leq m_0$ the map u_k has degree d and the critical values of u_k belong to V.

Degree d branched covers of $\mathcal{D}$ with critical values contained in V are determined up to isomorphism over $\overline{K}$ by a transitive action of the fundamental group $\pi_1(\mathcal{D} \setminus V)$ on a set with d elements. If $\mathcal{D}$ has genus 0, then this fundamental group is free on three generators;

if $\mathcal{D}$ has genus 1, then V is empty and the fundamental group has two generators. Since permutation representations are determined by choosing an element of the symmetric group S_d for each generator, there are no more than $d!^3$ such representations in either case. Therefore there is some $n_0 \geq 0$ and $n_1 \geq 1$ with $n_0 + n_1 \leq d!^3$ such that u_{n_0} is isomorphic to $u_{n_0+n_1}$ over $\overline{K}$. That is, u has a finite orbit under iterated fiber product with f over $\overline{K}$, which implies that C_n is irreducible with $g(C_n) \leq 1$ for all $n \geq 0$. From Theorem 5.4.2 we conclude that u has a finite orbit. □

5.6.1 Orbit bounds

Theorem 5.4.2 implies that if u is f-stable and $g(C_n) \leq 1$ for all $n \geq 0$, then u has a finite orbit over K. Corollary 5.6.6 bounds the size of the orbit in terms of d. This bound has a geometric and arithmetic component which we treat in that order. The geometric component of this bound follows immediately from the proof of Theorem 5.6.2.

Corollary 5.6.3 (Geometric Orbit Bound)**.** *Suppose Assumption 5.6.1. If u has a finite orbit under iterated fiber product with f, then the orbit has at most $d!^3$ elements up to $\overline{K}$-isomorphism.*

To bound the size of the orbit of u up to isomorphism over K we need a bound on the number of twists of u in an orbit under iterated fiber products. We show that the number of such twists is bounded in terms of $\deg(u)$ in Theorem 5.6.5.

Remark 5.6.4. The map u may have infinitely many distinct twists over K. For example, for each squarefree integer a the map $u_a : \mathbb{P}^1 \to \mathbb{P}^1$ given in coordinates by $u_a(x) = ax^2$ is an infinite family of distinct twists over $\mathbb{Q}$. Thus the content of Theorem 5.6.5 is that only finitely many distinct twists arise in an orbit under iterated fiber products with f.

Theorem 5.6.5 (Arithmetic Period Bound)**.** *Suppose Assumption 5.6.1. Suppose that u is fixed under iterated fiber product with f up to isomorphism over $\overline{K}$. That is, there is an isomorphism $h : C_1 \to C$ defined over $\overline{K}$ such that $u \circ h = u_1$. Then the orbit of u up to isomorphism over K has at most $d^{d^3!}$ elements.*

Proof. Our assumption that u is fixed under fiber product with f over $\overline{K}$ implies that C is irreducible with genus at most 1 by Theorem 5.3.9. An isomorphism between two

irreducible curves of genus at most 1 is determined by its value at 3 points. If we choose 3 points in C_1, then the functional equation $u \circ h = u_1$ implies that for each point q the image $h(q)$ must be one of the at most d fibers of u over $u_1(q)$. Therefore there are at most d^3 such isomorphisms. If $G := \mathrm{Gal}(\overline{K}/K)$, then since u and u_1 are defined over K it follows that G acts on the set of isomorphisms h satisfying $u \circ h = u_1$. We conclude that h is defined over a field of degree at most d^3, hence has Galois closure L/K of degree at most $d^3!$.

As L splits u_1 as a twist of u, it must split all u_n. The number of such twists is bounded by the size of the first non-abelian group cohomology $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(u))$, which in turn is bounded by the number of functions from $\mathrm{Gal}(L/K)$ to $\mathrm{Aut}(u)$. Galois theory implies that $|\mathrm{Aut}(u)| \leq d$. Thus the number of twists in the orbit of u under iterated fiber product with f is at most $d^{d^3!}$. □

Corollary 5.6.3 and Theorem 5.6.5 combine to give the following bound on the size of the orbit of u.

Corollary 5.6.6 (Orbit Bound)**.** *Suppose Assumption 5.6.1. If u has a finite orbit under f, then the orbit has at most $d!^3 d^{d^3!}$ elements up to isomorphism over K.*

Example 5.6.7 shows that in general the dependence on the size of the orbit on $d := \deg(u)$ cannot be improved. However we expect the explicit bounds given above to be far from sharp.

Example 5.6.7. Let $d \geq 2$ and suppose that $a \in K$ is such that the smallest positive power of a which is a dth power in K is d itself. Note that if K is a finitely generated field of characteristic 0 then such an element a always exists. Let $u_b(x) := bx^d$ for $b \in K^\times$ and let $h(x)$ be any non-constant rational function in $K(x)$. If $f(x) := a^{-1}xh(x)^d$ and $g_b(x) = xh(abx^d)$ then $f(x)$ has degree at least 2 and

$$f \circ u_{ab} = a^{-1}(abx^d)h(abx^d)^d = b\big(xh(abx^d)\big)^d = u_b \circ g_b.$$

We claim that for any $b \in K^\times$ the fiber product of u_b and f is irreducible. If not, then by Fried's Theorem (see Theorem 5.6.9 below,) u_b and f must have non-trivial left composition factors with the same Galois closure. Any left composition factor of $u_b(x) = bx^d$ must

have the form bx^e for some divisor e of d, and all such maps are Galois. Therefore f has a left composition factor of the form bx^e, which implies that e divides the ramification index of f over 0. However, from the explicit expression $f(x) = a^{-1}xh(x)^d$ we see that that the ramification index of f over 0 is congruent to 1 modulo d, hence is coprime to d—a contradiction.

Thus u_{ab} is the fiber product of u_b and f for any $b \in K^\times$. In particular, the fiber product of $u_1(x) = x^d$ with f^n is $u_{a^n}(x) = a^n x^d$. By our assumption on a it follows that d is the primitive period of $u_1(x)$ under iterated fiber product with f.

5.6.2 Iterate Decompositions

Theorem 5.6.8 shows that if some iterate f^n decomposes as $u \circ w$, then the left composition factor u must first occur in a decomposition of f^m with m bounded in terms of $\deg(u)$.

Theorem 5.6.8 (Iterate Decomposition Stability)**.** *Suppose Assumption 5.6.1. Suppose that u is a left composition factor of some iterate of f. Then there exists a function $S(d)$ depending only on $d := \deg(u)$ such that $f^m = u \circ v$ for some $m \leq S(d)$ and finite map $v : \mathcal{D} \to C$. Furthermore, $S(d) = (d-1)M(d)$ will suffice, where*

$$M(d) := d!^3 + \log_2(170d - 84).$$

Proof. Suppose $m > (d-1)(d!^3 + \log_2(170d - 84))$ is the smallest positive integer for which there exists a map $v : \mathcal{D} \to C$ such that $f^m = u \circ v$. Observe that the functional equation $f^m = u \circ v$ is equivalent to the fiber product of u with f^m having an irreducible component isomorphic to $\mathcal{D}$.

$$\begin{array}{ccc} C & \xleftarrow{v} & \mathcal{D} \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle 1} \\ \mathcal{D} & \xleftarrow[f^m]{} & \mathcal{D} \end{array}$$

For $0 \leq k \leq m$ let C_k denote the irreducible component of the fiber product of u with f^k through which v factors and let $u_k : C_k \to \mathcal{D}$ be the restriction. So $C_m = \mathcal{D}$ and $u_m = 1$. Then $\deg(u_k)$ forms a weakly decreasing sequence of positive integers starting at $d = \deg(u_0) = \deg(u)$ and ending at $1 = \deg(u_m) = \deg(1)$ with 1 appearing for the first

time as $\deg(u_m)$ by the minimality of m. Thus there are at most $d-1$ distinct values in this sequence and some value $d' > 1$ must appear at least

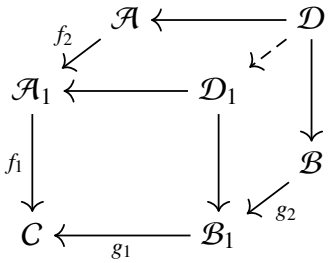
$$m' := \frac{m}{d-1} > d!^3 + \log_2(170d - 84)$$

consecutive times. If u_k is the first map with degree d', then the fiber product of u_k with $f^{m'}$ is irreducible with genus at most one. But then Theorem 5.6.2 implies that the fiber product of u_k with f^n is irreducible for all $n \geq 0$, which contradicts $\deg(u_m) = 1 < d'$. Therefore $m \leq (d-1)(d!^3 + \log_2(170d - 84))$. □

Theorem 5.6.9 is due to Fried, although Fried does not state the result in this language. In Appendix 5.7 we prove this result as stated here and discuss how it relates to Fried's original formulation.

Theorem 5.6.9 (Fried [33, Prop. 2])**.** *Let K be a field and suppose that $f : \mathcal{A} \to C$ and $g : \mathcal{B} \to C$ are finite maps between irreducible curves defined over K each with degree at least 2. If the fiber product $\mathcal{D}$ of f and g is reducible, then there is a decomposition $f = f_1 \circ f_2$ and $g = g_1 \circ g_2$ with $\deg(f_1), \deg(g_1) \geq 2$ such that*

1. *f_1 and g_1 have the same Galois closure.*
2. *The fiber product $\mathcal{D}_1$ of f_1 and g_1 is reducible.*
3. *The induced map from $\mathcal{D}$ to $\mathcal{D}_1$ is bijective on irreducible components. In other words, for each irreducible component of $\mathcal{D}_1$, there is exactly one component of $\mathcal{D}$ mapping onto it under the naturally induced map.*



As discussed in Section 5.1.2, Theorem 5.6.10 (2) may be interpreted as a geometric version of the *eventual stability* phenomenon introduced by Jones and Levy [54].

Theorem 5.6.10 (Geometric Eventual Stability)**.** *Suppose Assumption 5.6.1.*

1. *There exists a function $G(d)$ depending only on $d := \deg(u)$ such that if $m \geq G(d)$ and the fiber product of u with f^m is irreducible, then C_n is irreducible for all $n \geq 0$. Furthermore, $G(d) := S(d!)$ will suffice, where*

$$S(d) := (d-1)(d!^3 + \log_2(170d - 84)).$$

2. *If $m \geq (d-1)G(d)$, then the restriction of $u_m : C_m \to \mathcal{D}$ to each irreducible component of C_m is f-stable.*

Proof. Suppose that $m > G(d)$ is the smallest positive integer such that u and f^m have a reducible fiber product. Then Theorem 5.6.9 implies that there are decompositions $u = u_1 \circ u_2$ and $f^m = f_1 \circ f_2$ such that

1. $\deg(u_1), \deg(f_1) > 1$,
2. u_1 and f_1 have the same Galois closure.
3. The fiber product of u_1 and f_1 is reducible.

Since u_1 and f_1 have the same Galois closure we see that

$$\deg(f_1) \leq \deg(u_1)! \leq d!.$$

Theorem 5.6.8 asserts there is some $m' \leq S(d!) = G(d)$ for which f_1 is a left composition factor of $f^{m'}$. Therefore the fiber product of u with $f^{m'}$ factors through the fiber product of u_1 with f_1 and hence is reducible. This contradicts the minimality of m.

Therefore if $m > G(d)$ and the fiber product of u and f^m is irreducible, then the fiber product of u and f^n is irreducible for all $n \geq 0$.

Suppose $m > (d-1)G(d)$ and that the restriction of some irreducible component of u_m is not f-stable, which is to say that some iterate of u under fiber product with f is reducible. Arguing as in the proof of Theorem 5.6.8 we see there must be some $n_0 < m$ and $n_1 > G(d)$ such that the fiber product of the restriction of u_{n_0} to an irreducible component with f^{n_1} is irreducible. But then the above argument shows that the fiber product with all iterates of f are irreducible, which is a contradiction. □

5.6.3 Bounds on arithmetic progressions

The results from this section culminate in Theorem 5.6.11 where we apply them to bound the arithmetic progressions arising in Theorem 5.5.2.

Theorem 5.6.11. *Let K be a finitely generated field of characteristic 0 and let $u : C \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K. Let* $\deg(f) \geq 2$ *and let $d := \deg(u)$. For each $p \in \mathcal{D}(K)$ the set $L := \{n : f^n(p) \in u(C(K))\}$ can be expressed as a finite union of arithmetic progressions $j + k\mathbb{N}$ such that,*

1. *There are at most d distinct positive common differences.*
2. *Each common difference k is bounded by*

$$k \leq K(d) := d!^3 d^{d^3!}.$$

3. *Each minimal value j in a positive arithmetic progression is bounded by*

$$j \leq (d-1)G(d) + K(d),$$

where $G(d)$ is as in Theorem 5.6.10.

Proof. 1. The proof of Theorem 5.2.8 shows that the eventual periods of restrictions of u_n to f-stable components may be taken as the non-trivial common differences k. Since u has degree d, there are at most d distinct irreducible components of each C_n. Thus there are at most d positive common differences.

2. Since $k \neq 0$ may be chosen as the eventual periods of restrictions of u_n to f-stable components, it suffices to bound the finite orbits of these restrictions. Corollary 5.6.6 implies that $k \leq d!^3 d^{d^3!}$.

3. The minimal value j in each non-trivial arithmetic progression is at most $m_0 + m_1$ where m_0 is the smallest integer for which the restriction of u_{m_0} to all irreducible components is f-stable and m_1 is the maximal size of a finite orbit of one of these restrictions. Theorem 5.6.10 gives us $m_0 \leq (d-1)G(d)$ and Corollary 5.6.6 gives $m_1 \leq K(d)$. □

5.7 Appendix: Fried's Theorem

Fried proves the following theorem in [33, Prop. 2]:

Theorem 5.7.1 (Fried)**.** *Let K be a field and let $f(x), g(y)$ be polynomials defined over K with non-vanishing derivatives. Then there exist polynomials $f_1(u), g_1(v), f_2(x), g_2(y)$ defined over K such that*

$$f = f_1 \circ f_2$$
$$g = g_1 \circ g_2$$

and the field extensions $K(u), K(v)$ of $K(t)$ formed by adjoining roots of $f_1(u) - t$ and $g_1(v) - t$ to $K(t)$ have the same Galois closure. Furthermore, if

$$f_1(u) - g_1(v) = \prod_{i=1}^{m} h_i(u, v)$$

is an irreducible factorization over K, then

$$f(x) - g(y) = \prod_{i=1}^{m} h_i\big(f_2(x), g_2(y)\big)$$

is an irreducible factorization over K. That is, $h_i\big(f_2(x), g_2(y)\big)$ is irreducible over K for each i.

Theorem 5.7.1 is a powerful tool for studying the reducibility of separated variable polynomials like $f(x) - g(y)$, which arise as defining equations for fiber products. For example, Bilu and Tichy [6, Thm. 8.1] use Fried's theorem in their determination of all polynomials $f(x), g(y)$ such that $f(x) = g(y)$ has infinitely many integral solutions. In this appendix we formulate and prove Fried's theorem in a more general setting. We end by showing how both Fried's original result Theorem 5.7.1 and our Theorem 5.6.9 follow as specializations.

G-Sets and Fried's Theorem

Galois theory gives a unifying perspective on the categories of algebraic extensions of a field K and of branched covers of an irreducible curve C: both are equivalent to the category of transitive G-sets for some group G. In the former case G is an absolute Galois group, and in the latter case G is a fundamental group. Theorem 5.7.3 below is a formulation of Fried's theorem in the setting of G-sets, which may then be translated through Galois theory into more familiar algebraic and geometric settings.

Let G be a group. Recall that a *G-set* X is a set on which G acts by permutations. For $g \in G$ and $x \in X$ we write gx for the image of x under g. If X and Y are G-sets, then a *G-map* $f : X \to Y$ is a function which is "G-linear" in the sense that $f(gx) = gf(x)$. Together G-sets and the G-maps between them form a category.

If $N \trianglelefteq G$ is a normal subgroup and Y is a G-set, then we can quotient Y by the action of N to get a G-set NY defined by $NY := \{Ny : y \in Y\}$. Since N is normal, NY inherits a G-action and the map $q : Y \to NY$ sending $q : y \mapsto Ny$ is a G-map. We call $N \trianglelefteq G$ a *normal stabilizer* of Y if N fixes every point in Y. The largest normal stabilizer N_Y of Y is the *Galois group* of Y. Note that $N \subseteq N_Y$ iff N is a normal stabilizer of Y.

If G acts transitively on a set Z, we say Z is *irreducible*, and otherwise *reducible*. Given an irreducible G-set Z and a G-map $f : Y \to Z$, we say Y is a G-set *over* Z. If Y is over Z, and N is a normal stabilizer of Z, then $f : Y \to Z$ factors as $f = q \circ p$, where $p : Y \to NY$ is the projection defined above and $q : NY \to Z$ is defined by $q(Ny) = Nf(y) = f(y)$.

Suppose $f : X \to Y$ is a G-map. Then every orbit of X is mapped onto an orbit of Y, giving us a well-defined function from the orbits of X to the orbits of Y. We say f is *injective, surjective, or bijective on components* if the induced function on orbits has the respective property. These three properties are stable under composition.

If X and Y are G-sets over Z with maps $f : X \to Z$ and $b : Y \to Z$, then the *fiber product* $X \times_Z Y$ is defined in the usual way by

$$X \times_Z Y := \{(x, y) \in X \times Y : f(x) = g(y)\}.$$

The fiber product is a G-set with natural projections to X and Y.

Lemma 5.7.2. *Let X and Y be G-sets over Z, and let N be a normal stabilizer of X. If $p : Y \to NY$ is the natural projection, then $1_X \times p$ is bijective on components.*

$$\begin{array}{ccccc} X & \longleftarrow & X \times_Z NY & \xleftarrow{1_X \times p} & X \times_Z Y \\ \downarrow & & \downarrow & & \downarrow \\ Z & \xleftarrow[q]{} & NY & \xleftarrow[p]{} & Y \end{array}$$

Proof. Since 1_X and p are both surjective, their product is surjective on components. We check that $1_X \times p$ is injective on components. Suppose $(x_1, y_1), (x_2, y_2) \in X \times Y$ are points whose image under $1_X \times p$ lie in the same component. Then there exists a $g \in G$ such that

$$g \cdot (x_1, Ny_1) = (x_2, Ny_2).$$

Hence $g \cdot x_1 = x_2$ and $g \cdot Ny_1 = Ny_2$. So there exists $n \in N$ for which $gn \cdot y_1 = y_2$. Since N is a normal stabilizer for X, we have

$$gn \cdot x_1 = g \cdot x_1 = x_2.$$

So $gn \cdot (x_1, y_1) = (x_2, y_2)$ implying that (x_1, y_1) and (x_2, y_2) are in the same component of $X \times Y$. □

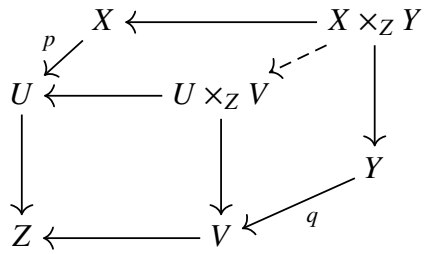
If $f : Y \to Z$ is a G-map, then for each $y \in Y$, there is an inclusion of stabilizer groups $G_y \subseteq G_{f(y)}$; we call the index $[G_{f(y)} : G_y]$ the *degree* of f at y, denoted $\deg_y(f)$. The degree depends only on the irreducible component of y. We define $\deg(f)$ to be the sum of the degrees of f on each irreducible components of Y. The degree of f is the size of any fiber, hence the name. We say Y is *finite over* Z if $f : Y \to Z$ has finite degree and denote it by $|Y/Z|$ when f is implicit.

Theorem 5.7.3 (Fried for G-sets)**.** *Let X, Y, Z be G-sets such that X and Y are finite over Z. Then there exist G-sets U and V finite over Z and surjective G-maps*

$$p : X \to U$$
$$q : Y \to V$$

such that

1. *U and V have the same Galois group.*
2. *The map $p \times q : X \times_Z Y \to U \times_Z V$ is bijective on components.*



Proof. We proceed by induction on the sum of degrees $|X/Z| + |Y/Z|$. Let N_X and N_Y be the Galois groups of X and Y respectively. If $N_X = N_Y$, then we are done with $X = U$ and $Y = V$. So suppose $N_X \not\subseteq N_Y$. Let $r : Y \to N_X Y$ be the natural map. Observe that $|N_X Y/Z| < |Y/Z|$; otherwise N_X is a normal stabilizer of Y, which implies $N_X \subseteq N_Y$. Lemma 5.7.2 shows that $1 \times r : X \times_Z Y \to X \times_Z N_X Y$ is bijective on components. By induction, the conclusion holds for X and $N_X Y$. The result follows since bijectivity on components is stable under composition. □

Corollary 5.7.4 reflects how we use Theorem 5.7.3 in practice.

Corollary 5.7.4. *Let X, Y, Z be G-sets such that X and Y are irreducible and finite over Z. If $X \times_Z Y$ is reducible, then the U and V provided by Theorem 5.7.3 both have degree greater than 1 over Z.*

Proof. We prove the contrapositive. If V has degree 1 over Z, then $V \cong Z$. Thus $U \times_Z V \cong U$ is irreducible. Since $p \times g : X \times_Z Y \to U \times_Z V$ is bijective on components it follows that $X \times_Z Y$ is irreducible. □

Translation to Field Theory

Let K be a field. Under the Galois theory correspondence, finite degree field extensions of K correspond to finite *transitive* G-sets for G the absolute Galois group of K. The subcategory of transitive G-sets is not closed under fiber products, making it an unsuitable setting for Fried's theorem. The Galois correspondence extends to the full category of

G-sets if we replace algebraic field extensions of K with *étale K-algebras*. Recall that an étale K-algebra is a finite product of separable field extensions of K. See Lenstra [60] for an account of this expanded Galois theory following Grothendieck.

Given an étale K-algebra A/K, the set of K-algebra maps $\mathrm{Hom}_K(A, K^{\mathrm{sep}})$, where K^{sep} is a separable closure of K. inherits an action of $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ by post-composition. This function $A \mapsto \mathrm{Hom}_K(A, K^{\mathrm{sep}})$ extends naturally to a contravariant functor giving one direction of the Galois correspondence. In the other direction it suffices to say how to construct a field extension from a transitive G-set X: choosing a point $x \in X$, let H be the stabilizer of x and let L/K be the fixed field of H in K^{sep}. Different choices of point in X give isomorphic extensions with different embeddings in K^{sep}. Since the Galois correspondence is a dual equivalence, disjoint unions of G-sets correspond to products of K-algebras and products of G-sets correspond to tensor products of K-algebras.

Let A/K be a finite étale algebra over K. The *degree* of A/K is the dimension of A as a K-vector space. We say A is *irreducible* if A/K is a field extension; otherwise A is a product of field extensions and we call A *reducible*. If $A = \prod_{i=1}^m L_i$ is a decomposition of A as a product of field extensions L_i/K, then the *Galois closure* of A/K is the product of the Galois closures of each L_i/K. The spectrum of an étale K-algebra is a finite set comprised of the spectra of the field factors of A. That is, if $A = \prod_{i=1}^m L_i$, then

$$\mathrm{Spec}(A) = \bigsqcup_{i=1}^{m} \mathrm{Spec}(L_i).$$

Recall that a map of K-algebras $f : B \to A$ induces a map $f^* : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$. We say that f is *injective*, *surjective*, or *bijective on components* if the corresponding dual map on spectra has the respective property as a function of finite sets.

Applying the Galois correspondence to Theorem 5.7.3 yields Theorem 5.7.5.

Theorem 5.7.5 (Fried for K-algebras)**.** *Let A and B be finite étale K-algebras. Then there are finite étale K-algebras C and D and injective K-algebra maps*

$$i : C \to A$$
$$j : D \to B$$

such that

1. *C and D have the same Galois closure.*
2. *The map $i \otimes j : C \otimes_K D \to A \otimes_K B$ is bijective on components.*

Likewise, we have a translation of Corollary 5.7.4.

Corollary 5.7.6. *Let A and B be finite field extensions of K. If $A \otimes_K B$ is reducible, or equivalently if A and B are not linearlly disjoint over K, then the field extensions C and D provided by Theorem 5.7.5 both have degree greater than 1 over K.*

Neither Theorem 5.7.3 nor Theorem 5.7.5 is stated in the language used by Fried. To recover his version of the result we apply Theorem 5.7.5 with $K(t)$ as our ground field, where K is a field and t is transcendental over K. Given a rational function $f(x) \in K(x)$ with non-vanishing derivative, $K(x)$ is the separable field extension of $K(t)$ formed by adjoining a root of $f(x) - t$. If x, y, t are transcendental and algebraically independent over K, then for rational functions $f(x)$ and $g(y)$ with coefficients in K and non-vanishing derivatives we get two finite, separable field extensions $K(x)/K(t)$ and $K(y)/K(t)$; the tensor product $K(x) \otimes_{K(t)} K(y)$ is an étale $K(t)$-algebra presented over K by

$$K(x) \otimes_{K(t)} K(y) \cong \frac{K[x, y]}{\big(f(x) - g(y)\big)}.$$

The irreducible factors of the numerator of $f(x) - g(y)$ correspond to the fields in a product decomposition of this $K(t)$-algebra.

Theorem 5.7.7 (Fried)**.** *Let K be a field and $f(x), g(y)$ be non-constant rational functions over K. Then there exist rational functions $f_1(u), f_2(x), g_1(v), g_2(y)$ with coefficients in K and a decomposition*

$$f = f_1 \circ f_2$$
$$g = g_1 \circ g_2$$

such that

1. *The field extensions $K(u)/K(t)$ and $K(v)/K(t)$ have the same Galois closure, and*

2. *If $h_i(u, v)$ are the irreducible factors of the numerator of $f_1(u) - g_1(v)$, then $h_i\big(f_2(x), g_2(y)\big)$ have irreducible numerators.*

Proof. We apply Theorem 5.7.5 to find fields $U \subseteq K(x)$ and $V \subseteq K(y)$ with the same Galois closure of $K(t)$. By Lüroth's theorem [87, Prop. 3.5.9], we may write $U = K(u)$ and $V = K(v)$ for transcendentals u, v. Then $t \in K(u), K(v)$ implies there are rational functions $f_1(u)$ and $g_1(v)$ such that $t = f_1(u)$ in $K(u)$ and $t = g_1(v)$ in $K(v)$. Similarly, $u \in K(x)$ and $v \in K(y)$ give us $u = f_2(x)$ and $v = g_2(y)$ in the respective fields. From $t = f(x)$ in $K(x)$ and $t = g(y)$ in $K(y)$ respectively, the functional decompositions follow.

Then the two claims follow from Theorem 5.7.5 and the discussion beginning this section. □

Remark 5.7.8. Fried stated his version of the result with f and g polynomials. Since a polynomial $f(x)$, viewed as endomorphisms of $\mathbb{P}^1$, is a rational function with a totally ramified point, the same must be true for any composition factors of f. Hence, after a linear change of coordinates, we may assume that any decomposition of a polynomial has polynomial factors. Theorem 5.7.7(2) then has a cleaner statement, since we then simply refer to the irreducible factors without specifying the numerator.

Finally, Theorem 5.6.9 follows either by translating Theorem 5.7.3 through the Galois correspondence for branched covers of curves or by translating Theorem 5.7.5 through the algebro-geometric duality.

5.8 Appendix: Twists and Non-Abelian Group Cohomology

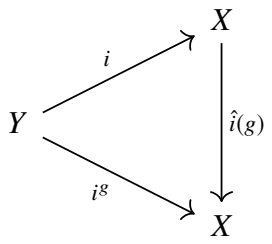
In this appendix we review first non-abelian group cohomology and its relation to twists in a general setting.

Suppose G is a group acting functorially on a groupoid $\mathcal{G}$. That is, for each $g \in G$ and isomorphism $i : X \to Y$ we get an isomorphism $i^g : X^g \to Y^g$, and the action respects composition. The essential family of examples to keep in mind is when $\mathcal{G}$ is a groupoid of objects "defined over" an algebraic closure $\overline{K}$ with algebraic morphisms and $G := \mathrm{Gal}(\overline{K}/K)$; in that case the absolute Galois group acts naturally on objects and morphisms. Following this example we say an object or morphism is *defined over K* when

it is fixed by G. In an abstract setting K does not refer to a specific field, this is just a useful expression to keep us grounded (Neukirch uses similar terminology in his abstract development of class field theory [67].)

Let us furthermore suppose that every object and morphism in $\mathcal{G}$ has a finite index stabilizer in G. Intuitively this corresponds to all objects and morphisms being defined over some finite extension of K. If X and Y are objects defined over K and isomorphic in $\mathcal{G}$ but potentially not isomorphic over K, then we say Y is a *twist* of X. If $i : X \to Y$ is an isomorphism, then by our assumption i is defined over some finite extension L/K and we say that this twist is *split* over L.

We are interested in classifying the twists of a given object X in $\mathcal{G}$ defined over K. Suppose Y is defined over K and $i : Y \to X$ is an isomorphism. Thus G fixes X and Y and acts on the isomorphisms between them. Let $\mathrm{Aut}(X)$ denote the automorphism group of X in $\mathcal{G}$. We define a function $\hat{i} : G \to \mathrm{Aut}(X)$ by $\hat{i}(g) := i^g \circ i^{-1}$, which we suggestively write as $\hat{i}(g) = i^{g-1}$. This is equivalent to $\hat{i}(g)$ making the following diagram commute.



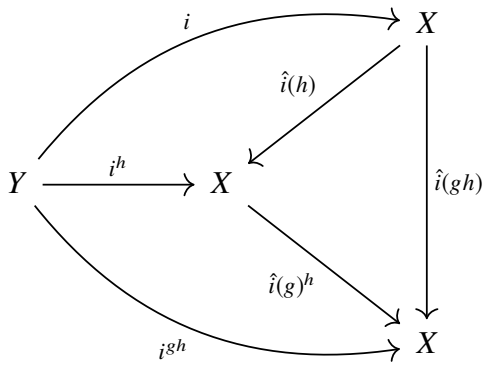
(5.8)

The function $\hat{i}$ satisfies the following *cocycle condition* for all $g, h \in G$,

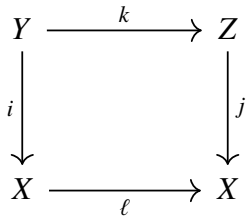
$$\hat{i}(gh) = \hat{i}(g)^h \circ \hat{i}(h) \qquad \text{(or equivalently } i^{gh-1} = i^{gh-h} \circ i^{h-1}.)$$

To see this relation first note that the diagram (5.8) uniquely determines $\hat{i}$ and then express

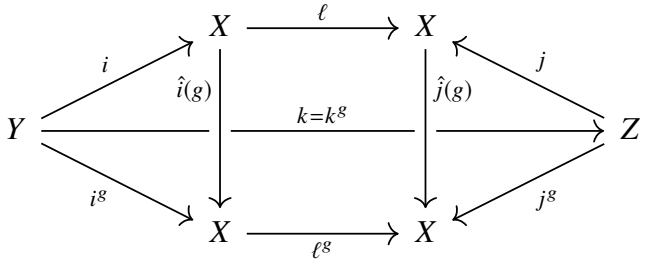
$\hat{i}(gh)$ in two ways:



Suppose $j : Z \to X$ is another twist of X and $k : Y \to Z$ is an isomorphism defined over K, which is to say that Y and Z define essentially the same twist of X. Then $\ell := j \circ k \circ i^{-1}$ is an automorphism of X making the following diagram commute:



Since k is fixed by the action of G it follows that for all $g \in G$ the following diagram commutes.



(5.9)

Thus $\hat{j}(g) = \ell^g \circ \hat{i}(g) \circ \ell^{-1}$ for all $g \in G$. Conversely, if $i : Y \to X$ and $j : Z \to X$ are twists and there exists an automorphism $\ell \in \mathrm{Aut}(X)$ for which (5.9) holds, then it follows that $j \circ \ell \circ i : Y \to Z$ is fixed under the action of G, hence is defined over K. We call such an automorphism ℓ a *coboundary from $\hat{i}$ to $\hat{j}$*. The existence of a coboundary between cocycles determines an equivalence relation on cocycles which we call a *first cohomology*

class.

Define $H^1(G, \mathrm{Aut}(X))$ to be the collection of all first cohomology classes. Note that we are not assuming that $\mathrm{Aut}(X)$ is abelian and thus $H^1(G, \mathrm{Aut}(X))$ does not have a natural group structure. When $\mathrm{Aut}(X)$ is abelian, these constructions simplify to the more familiar definitions of group cohomology (see Brown [9].) Our discussion above shows that K-isomorphism classes of twists of X give rise to distinct first cohomology classes. A simple observation which we employ in Sections 5.5 and 5.6 is that if G and $\mathrm{Aut}(X)$ are finite groups, then there are finitely many possible cocycles, hence $H^1(G, \mathrm{Aut}(X))$ is finite.

Chapter 6

Noncommutative arithmetic dynamical Mordell-Lang

The results in this chapter were obtained in collaboration with Michael Zieve. A co-authored paper is in preparation.

6.1 Introduction

In Chapter 5 we proved an arithmetic analog of the (cyclic) dynamical Mordell-Lang conjecture (Conjecture 5.1.1). We refer to this as the *cyclic* case of dynamical Mordell-Lang as it pertains to the action of a cyclic semigroup $\langle f \rangle$ on a variety X. A proper dynamical generalization of the Mordell-Lang conjecture should consider the action of more general semigroups of endomorphisms on X. Bell, Ghioca, and Tucker pose Question 6.1.1 as one possible generalization of Conjecture 5.1.1. They note several cases where Question 6.1.1 has an affirmative and negative answer.

Question 6.1.1 ([4, Qu. 3.6.0.1])**.** Let X be a quasiprojective variety defined over $\mathbb{C}$ and let $S = \langle f_1, f_2, \ldots, f_g \rangle$ be a finitely generated semigroup of commuting endomorphisms of X. If $p \in X(\mathbb{C})$ and $U \subseteq X$ is a subvariety, then is it true that $\{(n_1, n_2, \ldots, n_g) : f_1^{n_1} f_2^{n_2} \cdots f_g^{n_g}(p) \in U(\mathbb{C})\}$ is a finite union of sets of the form $\hat{a} + B$, where $\hat{a} \in \mathbb{N}^g$ and $B \subseteq \mathbb{N}^g$ is a subsemigroup?

Our main result in this chapter is Theorem 6.1.2, a noncommutative semigroup generalization of Theorem 5.1.2. To formulate the conclusion we need the notion of a *regular*

language from theoretical computer science. Let $A := \{a_1, a_2, \ldots, a_g\}$ be a finite set and let $A^* := \langle a_1, a_2, \ldots, a_g \rangle$ be the free noncommutative semigroup generated by A. Then elements of A^* are simply words formed from the alphabet A. A *(formal) language over* A is a subset $\mathcal{L} \subseteq A^*$. *Regular languages* are a simple and fundamental class of formal languages which may be informally characterized as those languages $\mathcal{L}$ recognized by a finite state machine without memory (see Section 6.2 for a formal definition.) If $\mathcal{D}$ is an irreducible curve and $S := \langle f_1, f_2, \ldots, f_g \rangle$ is a finitely generated (noncommutative) semigroup of endomorphisms $f_i : \mathcal{D} \to \mathcal{D}$, then subsets of S may be interpreted as formal languages over the alphabet $\{f_1, f_2, \ldots, f_g\}$.

Theorem 6.1.2 (Noncommutative Arithmetic Dynamical Mordell-Lang)**.** *Let K be a finitely generated field of characteristic 0, let $u : \mathcal{C} \to \mathcal{D}$ be a finite map between irreducible curves defined over K, and let $S = \langle f_1, f_2, \ldots, f_g \rangle$ be a finitely generated semigroup of endomorphisms $f_i : \mathcal{D} \to \mathcal{D}$, such that* $\deg(f_i) \geq 2$ *for all i. If $p \in \mathcal{D}(K)$ is a point, then $\{w \in S : w(p) \in u(\mathcal{C}(K))\}$ is a regular language.*

Remark 6.1.3. Languages over an alphabet with one letter f are equivalent to subsets of the natural numbers by $f^n \leftrightarrow n$. In Example 6.2.7 we show that a regular language over an alphabet with one letter is equivalent to a finite union of arithmetic progressions. Thus Theorem 6.1.2 is a proper generalization of Theorem 5.1.2.

We refer the reader to Chapter 5 for background on curves, fiber products, and twists.

6.2 Regular languages and finite automata

Let $A = \{a_1, a_2, \ldots, a_g\}$ be an alphabet and recall that a formal language is a subset $\mathcal{L} \subseteq A^*$ of the free noncommutative semigroup generated by A. The class Reg of *regular languages* is defined recursively as the smallest set of languages such that every finite language is in Reg and if $\mathcal{L}$, $\mathcal{L}_1$ and $\mathcal{L}_2$ are in Reg, then

1. The union $\mathcal{L}_1 \cup \mathcal{L}_2$ is in Reg,
2. The concatenation $\mathcal{L}_1\mathcal{L}_2 := \{w_1 w_2 : w_i \in \mathcal{L}_i\}$ is in Reg, and
3. The *Kleene star* $\mathcal{L}^* := \bigcup_{n \geq 0} \mathcal{L}^n = \{w_1 w_2 \cdots w_n : w_i \in \mathcal{L}\}$ is in Reg.

A regular language may also be defined as the collection of all words matching a *regular expression*. Regular expressions are defined recursively as any expression e which is either a word in A^* or

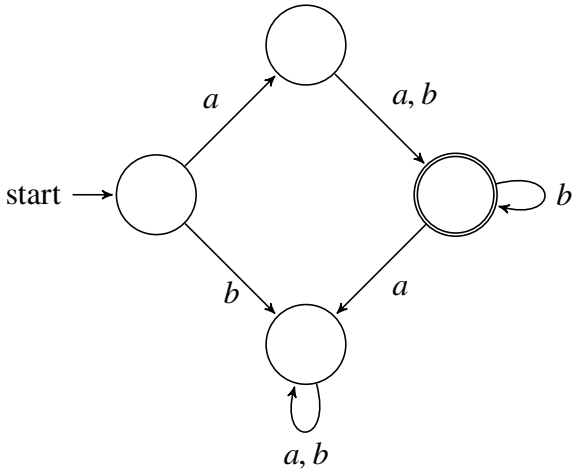
1. e is a disjunction $e = e_1|e_2$ where $e_1, e_2 \in \text{Reg}$,
2. e is a concatenation $e = e_1e_2$ where $e_1, e_2 \in \text{Reg}$, or
3. e is a *Kleene star* $e = e_1^*$ where $e_1 \in \text{Reg}$.

A regular expression e should be interpreted as a pattern describing a language $\mathcal{L}(e)$ of all words $w \in A^*$ which match the pattern e.

Example 6.2.1. If $A := \{a, b\}$ is our alphabet, then $e := a(a|b)b^*$ is a regular expression describing the language of all words that start with an a, followed by either an a or b, and then followed by any number of b's,

$$\mathcal{L}(e) = \{aa, ab, aab, abb, aabb, \ldots\}. \tag{6.1}$$

A useful way to define a formal language is to construct a "machine" that recognizes the language. A *deterministic finite automata* or *DFA over the alphabet A* is a machine modelled by a finite directed graph with vertices interpreted as *states* and such that for each letter $a \in A$ and each state q, there is exactly one directed arrow labelled by a from q to another state (or possibly back to q.) Every DFA M has a distinguished *start state* and a set of *accept states*. An example of a DFA over the alphabet $A = \{a, b\}$ is shown below. The start state is labelled and the accept state is the distinguished state on the right.



We think of M as a machine which processes words in A^*. Given a word $w = a_1 a_2 \cdots a_\ell$ we begin at the start state of M and use letters in w as instructions for which state to transition to. If we are on an accept state when we finish processing w, then we say that M *accepts* w and otherwise not.

Remark 6.2.2. A word w can be read from either the left or right when defining an automata. Whether a language is regular does not depend on the direction in which it is read, although this is not immediately clear [1, Cor. 4.3.5].

The collection of all words accepted by M is called the *language of* M and denoted $\mathcal{L}(M)$. Returning to the DFA M shown above, we see that the word $w_1 = aabb$ is accepted by M while $w_2 = baab$ is not. Furthermore, the language of M is precisely the regular language $L(e)$ from (6.1). The following fundamental result shows that regular languages are exactly the languages accepted by finite automata.

Theorem 6.2.3 (Kleene's Theorem)**.** *If M is a DFA, then $\mathcal{L}(M)$ is a regular language and if L is a regular language, then there is a DFA M such that $L = \mathcal{L}(M)$.*

Proof. See Allouche and Shallit [1, Thm. 4.1.5]. □

Kleene's theorem allows us to show a language L is regular by explicitly constructing a deterministic finite automata which accepts L. However, in practice the determinism of a DFA can be cumbersome to work around. A *non-deterministic finite automata* or *NFA* is

a DFA where there can be multiple directed arrows with any given label emanating from each state. Words are processed by an NFA N by following all possible paths with the appropriate edge labelings; the word is accepted if any one of those paths ends at an accept state. The added flexibility of non-determinism can significantly improve the efficiency of the automaton recognizing a language, but the overall class of languages recognized is the still the regular languages.

The Pumping Lemma is an essential tool in the study of regular languages. Given a word $w = a_1 a_2 \dots a_\ell$ we write $|w| := \ell$ for the length of w.

Lemma 6.2.4 (Pumping Lemma)**.** *If L is a regular language, then there is a constant $P > 0$ called the* pumping length *of L such that for any word $w \in L$ with $|w| > P$ we may factor w as $w = xyz$ where*

1. *$|y| > 0$,*
2. *$|xy| \leq P$,*
3. *$xy^n z \in L$ for any $n \geq 0$.*

Proof. See, for example, [1, Lem. 4.2.1]. □

Lemma 6.2.4 says that in a regular language L every sufficiently long word w contains a subword y which may be removed or repeated any number of times to obtain another word in L.

6.2.1 Reinterpretation of finite automata

Regular languages are typically associated with computer science but have appeared several times in connection with pure mathematics. For example, in the positive characteristic version of the Skolem-Mahler-Lech theorem [23], in the Gröbner theory of representations of combinatorial categories [79, Sec. 5], and in the description of the algebraic closure of formal power series rings in positive characteristic [1, Chp. 12]. Proposition 6.2.5 gives another characterization of regular languages which explains why we should expect to see this concept commonly in a pure mathematical context. If S is a semigroup, then an *S-set* is a set on which S acts by endomorphisms.

Proposition 6.2.5. *Let S be a finitely generated semigroup and let M be a finite S-set. If $p \in M$ and $U \subseteq M$ is a subset, then $\{w \in S : w(p) \in U\}$ is a regular language over the alphabet of generators of S.*

Proof. A finite S-set M with a choice of an element $p \in M$ and a subset $U \subseteq M$ is equivalent to the data required to specify a DFA with start state p and accept states U. More precisely, if we let the elements of M be our states, then for each generator f of S and $q \in M$ we include an arrow from q to $f(q)$ labelled f. If w is a word in the alphabet of generators and $q \in M$, then $w(q)$ is the state we arrive at by following the transitions from the letters of w one at a time (read from the right.) The language accepted by this DFA is $\{w \in S : w(p) \in U\}$ is regular by Kleene's theorem. □

Remark 6.2.6. The proof of Proposition 6.2.5 shows that DFAs are essentially equivalent to finite S-sets with a choice of starting and accepting elements. This representation theoretic perspective extends to other variants of DFAs. For example, an NFA is equivalent to a finite dimensional $\mathbb{B}$-linear S-representation N where $\mathbb{B} := \{0, 1\}$ is the Boolean semiring together with a starting vector $v \in N$ and an accepting dual vector $a^* \in N^*$.

Example 6.2.7. Suppose our alphabet consists of one letter $A = \{f\}$ and let $S := A^* = \langle f \rangle$. A language over A is equivalent to a subset of $\mathbb{N}$ by $f^n \leftrightarrow n$. Note that a finite S-set is equivalent to a finite set M with a function $f : M \to M$. Since every $q \in M$ has a finite orbit under f it follows that a regular language over A is equivalent to a finite union of arithmetic progressions.

6.3 Noncommutative arithmetic dynamical Mordell-Lang

In this section we prove Theorem 6.3.6. Along the way we deduce several intermediate results of independent interest. Theorem 6.3.1 characterizes the language of all words in a finitely generated semigroup of endomorphisms of projective space which map a point p into a finite set.

Theorem 6.3.1. *Let K be a field of characteristic 0 and let $S := \langle f_1, f_2, \ldots, f_g \rangle$ be a finitely generated semigroup of endomorphisms $f_i : \mathbb{P}^n \to \mathbb{P}^n$ of projective space defined*

over K such that $\deg(f_i) \geq 2$ *for all i. If $p \in \mathbb{P}^n(K)$ and $U \subseteq \mathbb{P}^n(K)$ is a finite set, then $\{w \in S : w(p) \in U\}$ is a regular language.*

We require Lemma 6.3.2, due to Moriwaki, which asserts the existence of height functions on projective space over any finitely generated field K of characteristic 0.

Lemma 6.3.2 (Moriwaki [66])**.** *If K is a finitely generated field of characteristic 0, then there exists a* height function $h : \mathbb{P}^n(K) \to \mathbb{R}_{\geq 0}$ *such that,*

1. *For any endomorphism f of degree d and point $p \in \mathbb{P}^n(K)$ there is a constant C_f depending only on f such that*

$$h(f(p)) \geq dh(p) + C_f.$$

2. *For any $b > 0$ there are finitely many points in $\mathbb{P}^n(K)$ with height less than b.*

Proof of Thm. 6.3.1. The finite set of generators of S, the finite set $U \subseteq \mathbb{P}^n(K)$, and the point p are all defined over some finitely generated subfield K' of K and thus every element of S and the full orbit of p under S is defined over K'. Therefore without loss of generality we may assume that K is a finitely generated field. Since regular languages are closed under union it also suffices to prove the result when U consists of a single point q.

Let h be a height function on $\mathbb{P}^n(K)$ as in Lemma 6.3.2. Since S is finitely generated, there are constants $b > 0$ and $c > 1$ such that for each generator f_i of S, if $r \in \mathbb{P}^n(K)$ and $h(r) > b$, then $h(f_i(r)) > ch(p)$. Let $B \subseteq \mathbb{P}^n(K)$ be the set of all points with height larger than b. Then $S(B) \subseteq B$ and the complement of B is a set of bounded height hence is finite.

The exponential growth of heights in B under S implies that $A := S^{-1}(q) \cap B$, the set of all elements in B which map to q by some word in S, is finite. Let M be the finite set theoretic quotient of $\mathbb{P}^n(K)$ given by equating all elements in $B \setminus A$. This quotient is S-equivariant, hence M is a finite S-set. It follows from Proposition 6.2.5 by interpreting p and q as elements of M that $L = \{w \in S : w(p) = q\}$ is a regular language. □

Theorem 6.3.3 is the noncommutative semigroup generalization of Theorem 5.4.2.

Theorem 6.3.3. *Let K be a field of characteristic 0 and let $S := \langle f_1, f_2, \ldots, f_g \rangle$ be a finitely generated semigroup of endomorphisms $f_i : \mathcal{D} \to \mathcal{D}$ of an irreducible curve $\mathcal{D}$ with genus*

at most 1 defined over K such that $\deg(f_i) \geq 2$ *for all* i. *For each* $d \geq 1$ *there is a finite subset* $V \subseteq \mathcal{D}$ *with size depending only on* d *and* g, *and a finite set* M *of* K*-isomorphism classes of finite maps* $v : C_v \to \mathcal{D}$ *such that,*

1. *If* $u : C_u \to \mathcal{D}$ *is a finite map with* $\deg(u) \leq d$ *such that the fiber product of* u *with a word* $w \in S$ *of length* $\ell > \log_2(2d)$ *is irreducible with genus at most 1, then* u *is ramified over* V.
2. *If* $u : C_u \to \mathcal{D}$ *is a finite map ramified over* V *with* $\deg(u) \leq d$ *for which the fiber product of* u *with some* $w \in S$ *has an irreducible component* $u_w : C_w \to \mathcal{D}$ *with genus at most 1, then the* K*-isomorphism class of* u_w *belongs to* M.

Proof. 1. If $\mathcal{D}$ has genus 1, then any irreducible component of a fiber product with genus at most 1 must also have genus 1 and thus be unramified by Lemma 5.3.2. In this case we can take $V := \emptyset$.

Now suppose that $\mathcal{D}$ has genus 0. Let $\ell > \log_2(2d)$ be an integer. The Riemann-Hurwitz formula implies that there are at most 4 points q in $\mathcal{D}$ for which f_i has at most 1 unramified pre-image: each such q contributes at least $\frac{\deg(f_i)-1}{2}$ toward the right hand side of

$$2\deg(f_i) - 2 = \sum_{q \in \mathcal{D}} \deg(f_i) - |f_i^{-1}(q)|.$$

Let A_i be the set of all such points for f_i, and let V be the union of the set of images of $\bigcup_{i=1}^{g} A_i$ under all words in S of length at most ℓ. Note that $|V|$ is bounded in terms of ℓ and g the number of generators of S.

Suppose that $u : C_u \to \mathcal{D}$ has $\deg(u) \leq d$ and that the fiber product $u_w : C_w \to \mathcal{D}$ of u with some word $w \in S$ of length ℓ is irreducible with genus at most 1. If q is a critical value of u not contained in V, then by construction q must have at least $2^\ell > 2d$ unramified pre-images under w. Abhyankar's lemma (Theorem 5.3.4) implies that each of these unramified pre-images is a critical value of u_w. However, Riemann-Hurwitz implies that u_w has at most $2\deg(u_w) \leq 2d$ critical values. Hence all the critical values of u must belong to V.

2. This proof has a geometric and arithmetic part. We first obtain a finite set $\overline{M}$ satisfying the conclusion over $\overline{K}$ (the geometric part) and then use this to construct a finite set M for which the conclusions holds over K (the arithmetic part.)

As discussed in Section 5.4, there are finitely many $\overline{K}$-isomorphism classes of irreducible branched covers $u : C_u \to \mathcal{D}$ with degree at most d and critical values contained in the finite set V. Let $\overline{M}_V$ denote this finite set of isomorphism classes.

Let $\overline{M}$ be the set of all $\overline{K}$-isomorphism classes of finite maps $v : C_v \to \mathcal{D}$ which are the restriction to a genus at most 1 component of a fiber product of $u \in \overline{M}_V$ with a word $w \in S$ of length at most $d\ell$. Recall that ℓ is defined to be an integer satisfying $\ell > \log_2(2d)$. Then $\overline{M}$ is finite with size bounded in terms of d and g.

We claim that for any $u \in \overline{M}_V$ and $w \in S$, if the fiber product $u_w : C_w :\to \mathcal{D}$ has an irreducible component with genus at most 1, then it is $\overline{K}$-isomorphic to an element of $\overline{M}$. We prove this by induction on the length of w. If $|w| \leq d\ell$, then this holds by the definition of $\overline{M}$. Suppose $m := |w| > d\ell$ and that the claim is true for all shorter words. If $w = f_{i_1} f_{i_2} \cdots f_{i_m}$ where each f_{i_j} is a generator of S, then let $u_k : C_k \to \mathcal{D}$ be the restriction of the fiber product of u with $f_{i_1} f_{i_2} \cdots f_{i_k}$ to the irreducible component C_k mapped onto by C_w.

$$\begin{array}{ccccccccc} C & \longleftarrow & C_1 & \longleftarrow & C_2 & \longleftarrow & C_3 & \longleftarrow & \cdots \\ {\scriptstyle u}\downarrow & & {\scriptstyle u_1}\downarrow & & {\scriptstyle u_2}\downarrow & & {\scriptstyle u_3}\downarrow & & \\ \mathcal{D} & \xleftarrow[f_{i_1}]{} & \mathcal{D} & \xleftarrow[f_{i_2}]{} & \mathcal{D} & \xleftarrow[f_{i_3}]{} & \mathcal{D} & \xleftarrow[f_{i_4}]{} & \cdots. \end{array}$$

Then each C_k has genus at most 1 and the sequence of degrees $\deg(u_k)$ is weakly decreasing. The degrees decrease less than $\deg(u) \leq d$ times; if each degree occurred no more than ℓ times then that would imply $m \leq d\ell$. Hence there is some v_k with $k > 0$ and a subword w' of w with length ℓ for which the fiber product of v_k with w' is irreducible with genus at most 1. It follows that v_k belongs to $\overline{M}_V$. Therefore u_w is a component of the fiber product of u_k with the word $f_{i_{k+1}} f_{i_{k+2}} \cdots f_{i_m}$ which is shorter than w. Hence our inductive hypothesis implies that u_w is $\overline{K}$-isomorphic to an element of $\overline{M}$. This concludes the geometric part of the argument.

Suppose that u is isomorphic to an element of $\overline{M}_V$ and defined over K. Let M_u be the set of K-isomorphism classes of restrictions to genus at most 1 components in the S-orbit of u under iterated fiber products. We aim to show that M_u is finite. To that end we first prove Claim 6.3.4.

Claim 6.3.4. For each $\overline{K}$-isomorphism class κ in $\overline{M}$ and $v \in \kappa$ defined over K, the S-orbit of v contains finitely many K-isomorphism classes contained in κ.

With v and κ as above define $\mathcal{L}_\kappa$ to be the language of all words $w \in S$ such that $v_w \in \kappa$. If $w \in \mathcal{L}_\kappa$, then since $v_{w'} \in \overline{M}$ for all initial subwords w' of w and $\overline{M}$ is finite, it follows from Proposition 6.2.5 that $\mathcal{L}_\kappa$ is a regular language. Let P be the pumping length of $\mathcal{L}_\kappa$ provided by Lemma 6.2.4. Now consider the collection of all words w_0, w_1 such that $|w_0 w_1| \leq P$ and $v_{w_0 w_1} \cong v_{w_0}$ over $\overline{K}$. Since S is finitely generated there are finitely many such words and therefore there exists a finite Galois extension L/K over which all the isomorphisms $v_{w_0 w_1} \cong v_{w_0}$ are defined.

We prove by induction on the length of a word that $v_w \cong v$ over L for all $w \in \mathcal{L}_\kappa$. If $w \in \mathcal{L}_\kappa$ has length at most P, then setting $w_0 = 1$ and $w_1 = w$ we have by definition of L that $v_w \cong v$ over L. Suppose for induction that $w \in \mathcal{L}_\kappa$ has length larger than P and that our claim has been shown for all shorter words. Lemma 6.2.4 gives a factorization $w = xyz$ where $|xy| \leq P$ and $xz \in \mathcal{L}_\kappa$. Letting $w_0 = x$ and $w_1 = y$ we see that the isomorphism $v_{xy} \cong v_x$ is defined over L. Thus taking fiber products with z we have $v_w = v_{xyz} \cong v_{xz}$ over L. Since $xz \in \mathcal{L}_\kappa$ is strictly shorter than w, our inductive hypothesis implies that $v_{xz} \cong v$ over L. Composing these isomorphisms shows that $v_w \cong v$ over L, completing our induction.

Therefore every element of the S-orbit of v in κ is a twist of v split over L. As L/K is a finite Galois extension and $\mathrm{Aut}(v)$ is a finite group, there are finitely many twists of v split over L (see Appendix 5.8.) This concludes the proof of Claim 6.3.4.

Letting $X := M_u$, $Y := \overline{M}$, and $r : X \to Y$ be the restriction to $\overline{K}$-isomorphism classes map, Claim 6.3.4 shows the hypotheses of Lemma 6.3.5 hold. We conclude that $M := M_u$ is finite, finishing our proof. □

Lemma 6.3.5. *Let S be a finitely generated semigroup, let X and Y be S-sets with Y finite, and let $r : X \to Y$ be an S-equivariant map. If for each $y \in Y$ and $x \in r^{-1}(y)$ the orbit of x visits $r^{-1}(y)$ finitely many times, then the S-orbit of each $x \in X$ is finite.*

Proof. It suffices to prove the result when S is a finitely generated free semigroup. The advantage of a free semigroup is that each $w \in S$ has a well-defined length $|w|$. Fix an element $x \in X$. Our assumption implies that once an orbit of x visits a fiber $r^{-1}(y)$,

there are only finitely many possibilities for the orbit to subsequently visit the same fiber. Therefore it is enough to show there exists an absolute bound ℓ such that for each $y \in Y$ and each $z \in r^{-1}(y)$ in the S-orbit of x, there exists a word $w \in S$ with length $|w| \leq \ell$ such that $z = wx$. Since there are finitely many words of bounded length, this implies the orbit of x is finite.

We proceed by induction on the number of r-fibers visited in traversing from x to z. If only one fiber is visited on our way from x to z, then $r(x) = y = r(z)$; since $Sx \cap r^{-1}(y)$ is finite, there is some ℓ_1 and a word $w \in S$ with length at most ℓ_1 such that $z = wx$. Now suppose that for any z in the S-orbit of x which can be reached after visiting at most m fibers of r, there is some ℓ_m such that there exists a word $w \in S$ with $|w| \leq \ell_m$ and $z = wx$. There are finitely many words of length at most ℓ_m and therefore finitely many z_1 which may be reached by a word of length $\ell_m + 1$. For each such z_1 let $y_1 = r(z_1)$; if $z_2 \in Sz_1 \cap r^{-1}(y_1)$, then there is a shortest word w such that $wz_1 = z_2$. Let b be an upper bound on the length of these shortest words as we vary over all such z_1. If z is in the S-orbit of x and may be reached after visiting $m + 1$ fibers of r, then there is some z_0 and z_1 such that

1. $r(z_1) = r(z)$,
2. z_0 can be reached after at most m fibers of r, and
3. $z_1 = az_0$ for some generator a of S.

It follows that there is a word $w \in S$ with $|w| \leq \ell_{m+1} := \ell_m + 1 + b$ such that $wx = z$, completing our induction. As Y is finite, there are at most $n := |Y|$ fibers visited by the orbit of x may visit, hence $\ell := \ell_n$ proves our claim. □

We now turn to the proof of our main result, Theorem 6.3.6.

Theorem 6.3.6 (Noncommutative arithmetic dynamical Mordell-Lang)**.** *Let K be a finitely generated field of characteristic 0, let $u : C \to \mathcal{D}$ be a finite map between irreducible curves defined over K, and let $S = \langle f_1, f_2, \ldots, f_g \rangle$ be a finitely generated semigroup of endomorphisms $f_i : \mathcal{D} \to \mathcal{D}$, such that* $\deg(f_i) \geq 2$ *for all i. If $p \in \mathcal{D}(K)$ is a point, then $\{w \in S : w(p) \in u(C(K))\}$ is a regular language.*

Proof. Let V and M be the finite sets provided by Theorem 6.3.3. Let N be the set of all K-isomorphism classes of restrictions to irreducible components of fiber products of elements of M with generators of S which do not belong to M. Since M is finite and S is

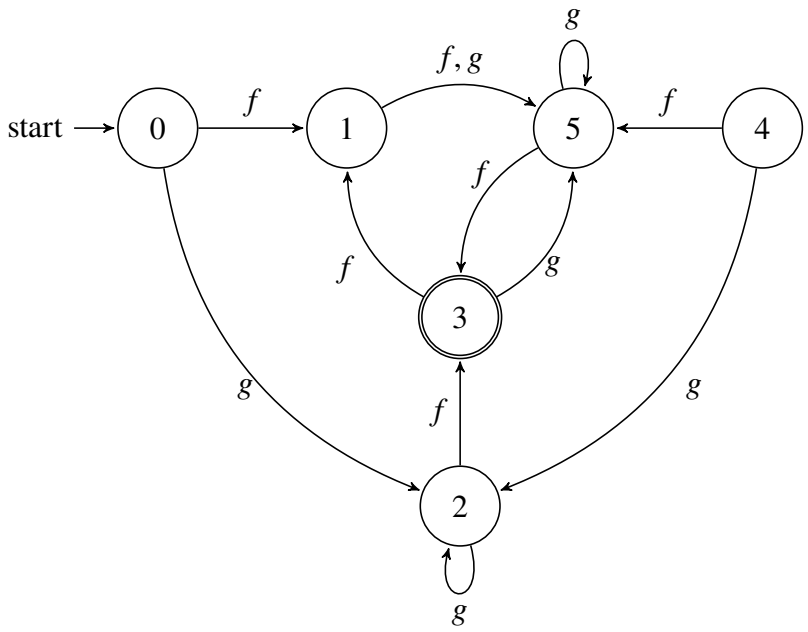
finitely generated, N is also finite. If $v : C_v \to \mathcal{D}$ represents a class in N, then $C_v(K)$ must be finite; if $C_v(K)$ were infinite, then Faltings' theorem implies that C_v has genus at most 1 and thus v would belong to M.

If $w(p) \in u(C(K))$, then the universal property of fiber products implies there is a K-point q on some component $v : C_v \to \mathcal{D}$ of the fiber product of u with w such that $v(q) = p$. Thus either v belongs to M and w is a word in the regular language $\{w \in S : u_w : C_w \to \mathcal{D}$ has a genus at most 1 component$\}$ or w factors as $w = xyz$ such that

1. x is a word such that $u_x : C_x \to \mathcal{D}$ has a component v_1 belonging to M,
2. y is a generator of S and the fiber product of v_1 with y has a component $v_2 : C_{v_2} \to \mathcal{D}$ belonging to N, and
3. z is a word such that $z(p)$ is an element of the finite set $v_2(C_{v_2}(K))$.

For a fixed $v_1 \in M$, the language of all such words x is regular since M is finite. For a fixed $v_2 \in N$ Theorem 6.3.1 implies (after choosing some projective embedding of $\mathcal{D}$) that the language of all such words z is regular since $v_2(C_{v_2}(K))$ is finite. As M and N are finite, together these observations imply that $\{w \in S : w(p) \in u(C(K))\}$ is a finite union of regular languages, hence is regular. □

Example 6.3.7. Let $K = \mathbb{Q}$ and let $S = \langle f, g \rangle$ where $f(x) = 3x^4$ and $g(x) = 9x^3$. If $u(x) = 27x^6$ and $p = 1 \in \mathbb{P}^1(\mathbb{Q})$, then $\mathcal{L} = \{w \in S : w(1) \in u(\mathbb{P}^1(\mathbb{Q}))\}$ is the regular language accepted by the following deterministic finite automata M.



For example $w_1 = fgf$ and $w_2 = fg^2$ belong to L (reading words from the right) and

$$w_1(1) = 3^{21} = u(3^3)$$
$$w_2(1) = 3^{33} = u(3^5).$$

To see that $\mathcal{L} = \mathcal{L}(M)$, note that every element in the orbit of $p = 1$ is a power of 3. Thus the orbit intersects the image of $u(x) = 27x^6$ precisely when its 3-adic valuation is congruent to 3 mod 6. If v_3 is the 3-adic valuation and $q \in \mathbb{P}^1(\mathbb{Q})$, then we have

$$v_3(f(q)) = v_3(3q^4) = 4v_3(q) + 1$$
$$v_3(g(q)) = v_3(9q^3) = 3v_3(q) + 2.$$

The DFA above encodes the action of the linear functions $f : v \mapsto 4v+1$ and $g : v \mapsto 3v+2$ on residues modulo 6. Our states are labelled by residues of the 3-adic valuation modulo 6.

As a corollary of Theorems 6.3.1, 6.3.6, and general properties of regular languages we deduce a more robust version of our main result. Given an irreducible curve $\mathcal{D}$ defined

over a finitely generated field K of characteristic 0, define the algebra of *K-constructible subsets* of $\mathcal{D}(K)$ as the smallest collection of subsets containing the images $u(C(K))$ of maps $u : C \to \mathcal{D}$ (both constant and finite) defined over K and closed under intersection, union, and complements.

Corollary 6.3.8. *Let K be a finitely generated field of characteristic 0, let U be a K-constructible subset of an irreducible curve $\mathcal{D}$, and let $S = \langle f_1, f_2, \ldots, f_g \rangle$ be a finitely generated semigroup of endomorphisms $f_i : \mathcal{D} \to \mathcal{D}$, such that $\deg(f_i) \geq 2$ for all i. If $p \in \mathcal{D}(K)$ is a point, then $\{w \in S : w(p) \in u(C(K))\}$ is a regular language.*

Proof. If U is the image of a constant or finite map, then the result follows from Theorem 6.3.1 and Theorem 6.3.6 respectively. It is well-known that the family of regular languages is closed under union, intersection, and complement. Thus the conclusion holds for all K-constructible sets U. □

Bibliography

[1] J.-P. Allouche and J. Shallit. *Automatic sequences: theory, applications, generalizations*. Cambridge University Press, 2003.

[2] R. Arratia, A. D. Barbour, and S. Tavaré. On random polynomials over finite fields. *Math. Proc. Camb. Philos. Soc*, 114, 1993.

[3] R. Arratia, A. D. Barbour, and S. Tavaré. *Logarithmic combinatorial structures: a probabilistic approach*, volume 1. European Mathematical Society, 2003.

[4] J. P. Bell, D. Ghioca, and T. J. Tucker. *The dynamical Mordell-Lang conjecture*, volume 210 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2016.

[5] J. Berstel and D. Perrin. The origins of combinatorics on words. *European J. Combin.*, 28:996–1022, 2007.

[6] Y. Bilu and R. Tichy. The diophantine equation $f(x) = g(y)$. *Acta. Arith.*, 95:261–288, 2000.

[7] A. Bodin. Number of irreducible polynomials in several variables over finite fields. *Am. Math. Mon.*, 115:653–660, 2008.

[8] J. M. Borger. Witt vectors, semirings, and total positivity. *arXiv e-prints*, page arXiv:1310.3013, Oct. 2013.

[9] K. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 1982.

[10] J. Cahn, R. Jones, and J. Spear. Powers in orbits of rational functions: cases of an arithmetic dynamical Mordell-Lang conjecture. *Canad. J. Math.*, 2017. To appear.

[11] A. R. Calderbank, P. Hanlon, and R. W. Robinson. Partitions into even and odd block size and some unusual characters of the symmetric groups. *Proc. Lond. Math. Soc.*, 3:288–320, 1986.

[12] L. Carlitz. The arithmetic of polynomials in a Galois field. *Proc. Natl. Acad. Sci. U.S.A.*, 17:120–122, 1931.

[13] L. Carlitz. The arithmetic of polynomials in a Galois field. *Am. J. Math.*, 54:39–50, 1932.

[14] L. Carlitz. The distribution of irreducible polynomials in several indeterminates. *Illinois J. Math.*, 7:371–375, 1963.

[15] L. Carlitz. The distribution of irreducible polynomials in several indeterminates II. *Canad. J. Math.*, 17:261–266, 1965.

[16] W. Chen. Twisted cohomology of configuration spaces and spaces of maximal tori via point-counting. *arXiv e-prints*, page arXiv:1603.03931, Mar. 2016.

[17] W. Chen. Analytic number theory for 0-cycles. *Math. Proc. Camb. Philos. Soc.*, 166:123–146, 2019.

[18] W. Chen. Stability in the cohomology of the space of complex irreducible polynomials in several variables. *arXiv e-prints*, page arXiv:1902.01882, Feb 2019.

[19] T. Church. Homological stability for configuration spaces of manifolds. *Invent. Math.*, 188:465–504, 2012.

[20] T. Church, J. Ellenberg, and B. Farb. Representation stability in cohomology and asymptotics for families of varieties over finite fields. *Contemp. Math.*, 620:1–54, 2014.

[21] T. Church and B. Farb. Representation theory and homological stability. *Adv. Math.*, 245:250–314, 2013.

[22] S. D. Cohen. The distribution of irreducible polynomials in several indeterminates over a finite field. *P. Edinburgh Math. Soc.*, 16:1–17, 1968.

[23] H. Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math.*, 168:175–224, 2007.

[24] A. W. M. Dress and C. Siebeneicher. The Burnside ring of the infinite cyclic group and its relation to the necklace algebra, λ-rings, and the universal ring of Witt vectors. *Adv. Math.*, 78:1–41, 1989.

[25] J. Elliott. Binomial rings, integer-valued polynomials, and λ-rings. *J. Pure Appl. Algebra*, 207:165–185, 2006.

[26] G. Faltings. Diophantine approximation on abelian varieties. *Ann. Math.*, 133:549–576, 1991.

[27] G. Faltings. Complements to Mordell. In G. Faltings and G. Wüstholz, editors, *Rational points*, pages 203–227. Vieweg+ Teubner Verlag, 1992.

[28] G. Faltings. The general case of S. Lang's conjecture. In V. Cristante and W. Messing, editors, *Barsotti Symposium in Algebraic Geometry*, volume 15 of *Perspectives in Mathematics*, pages 175–182. Elsevier, 1994.

[29] B. Farb and J. Wolfson. Topology and arithmetic of resultants, I. *New York J. Math.*, 22:801–821, 2016.

[30] B. Farb and J. Wolfson. Topology and arithmetic of resultants, II: the resultant 1 hypersurface. *Algebraic Geometry*, 4:337–352, 2017.

[31] B. Farb and J. Wolfson. Étale homological stability and arithmetic statistics. *Quart. J. Math*, 69:951–974, 2018.

[32] N. J. Fine. Binomial coefficients modulo a prime. *Am. Math. Monthly*, 54:589–592, 1947.

[33] M. Fried. The field of definition of function fields and a problem in the reducibility of polynomials in two variables. *Illinois J. Math.*, 17:128–146, 1973.

[34] J. Fulman. A generating function approach to counting theorems for square-free polynomials and maximal tori. *Ann. Comb.*, 20:587–599, 2016.

[35] N. Gadish. A trace formula for the distribution of rational G-orbits in ramified covers, adapted to representation stability. *New York J. Math*, 23:987–1011, 2017.

[36] W. Gaschütz. Die Eulersche Funktion Endlicher Auflösbarer Gruppen. *Ill. J. Math.*, 3:469–476, 1959.

[37] C. F. Gauss. Allgemeine Untersuchungen über die Congruenzen. In *Untersuchungen über höhere Arithmetik*. Chelsea Publishing Co., New York, 2nd edition, 1965. Translated by H. Maser.

[38] D. Ghioca and T. Tucker. Periodic points, linearizing maps, and the dynamical Mordell-Lang problem. *J. Number Theory*, 129:1392–1403, 2009.

[39] A. Granville. The anatomy of the integers. Available at `http://www.dms.umontreal.ca/~andrew/MSI/AnatomyForTheBook.pdf`.

[40] A. Grothendieck. La théorie des classes de Chern. *Bull. Soc. Math. France*, 86:137–154, 1958.

[41] K. Habiro. Cyclotomic completions of polynomial rings. *Publications of the Research Institute for Mathematical Sciences*, 40:1127–1146, 2004.

[42] P. Hall. *The Edmonton Notes on Nilpotent Groups*. Queen Mary College Mathematics Notes. Mathematics Department, Queen Mary College, London, 1969.

[43] P. Hanlon. The action of S_n on the components of the Hodge decomposition of Hochschild homology. *Michigan Math. J.*, 37:105–124, 1990.

[44] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2013.

[45] D. Hast and V. Matei. Higher moments of arithmetic functions in short intervals: a geometric perspective. *Int. Math. Res. Not.*, 2018.

[46] A. Hatcher. *Algebraic topology*. Cambridge University Press, 2002. Available at `http://pi.math.cornell.edu/~hatcher/AT/AT.pdf`.

[47] T. Hawkes, I. M. Isaacs, and M. Özaydin. On the Möbius function of a finite group. *Rocky Mt. J. of Math.*, 19:1003–1034, 1989.

[48] P. Hersh and V. Reiner. Representation stability for cohomology of configuration spaces in $\mathbb{R}^d$. *Int. Math. Res. Not.*, 2017:1433–1486, 2016.

[49] X.-D. Hou and G. Mullen. Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields. *Finite Fields Appl.*, 15:304–331, 2009.

[50] T. Hyde. Cyclotomic factors of necklace polynomials. *arXiv e-prints*, page arXiv:1811.08601, Nov. 2018.

[51] T. Hyde. Liminal reciprocity and factorization statistics. *Alg. Comb.*, 2018. to appear.

[52] T. Hyde. Polynomial factorization statistics and point configurations in $\mathbb{R}^3$. *Int. Math. Res. Not.*, 2018.

[53] T. Hyde and J. C. Lagarias. Polynomial splitting measures and cohomology of the pure braid group. *Arnold. Math. J.*, 3:219–249, 1983.

[54] R. Jones and A. Levy. Eventual stabile rational functions. *Int. J. Number Theory*, 13:2299–2318, 2017.

[55] J. C. Lagarias. A family of measures on symmetric groups and the field with one element. *J. Number Theory*, 161:311–342, 2016.

[56] J. C. Lagarias and B. L. Weiss. Splitting behavior of S_n polynomials. *Research in Number Theory*, 1, 2015.

[57] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 1986.

[58] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2002.

[59] H. W. Lenstra. Construction of the ring of Witt vectors. Available at `http://pub.math.leidenuniv.nl/~lenstrahw/PUBLICATIONS/witt.pdf`.

[60] H. W. Lenstra. Galois theory for schemes. Available at `https://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`.

[61] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Am. J. Math.*, 1:289–321, 1878.

[62] I. G. MacDonald. The Poincaré polynomial of a symmetric product. *Math. Proc. Camb. Philos. Soc.*, 58:563–568, 1962.

[63] N. Metropolis and G.-C. Rota. Witt vectors and the algebra of necklaces. *Adv. Math.*, 50:95–125, 1983.

[64] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, 1995.

[65] C. Moreau. Sur les permutations circulaires distinctes. *Nouvelles annales de mathématiques, journal des candidats aux écoles polytechnique et normale, Sér. 2*, 11:309–314, 1872.

[66] A. Moriwaki. Arithmetic height functions over finitely generated fields. *Invent. Math.*, 140:101–142, 2000.

[67] J. Neukirch. *Class field theory*, volume 280 of *A Series of Comprehensive Studies in Mathematics*. Springer-Verlag, Berlin, 1986.

[68] K. Nishioka. *Mahler functions and transcendence*, volume 1631 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.

[69] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 2013.

[70] R. W. K. Odoni. On the prime divisors of the sequence $w_n + 1 = 1 + w_1 \cdots w_n$. *J. London Math. Soc.*, 2:1–11, 1985.

[71] Y.-T. Oh. Group-theoretical generalization of necklace polynomials. *J. Algebr. Comb.*, 35:389–420, 2012.

[72] F. Pakovich. On semiconjugate rational functions. *Geom. Funct. Anal.*, 26:1217–1243, 2016.

[73] F. Pakovich. Algebraic curves $A^{\circ l}(x) - U(y) = 0$ and arithmetic of orbits of rational functions. *arXiv e-prints*, page arXiv:1801.01985, Jan. 2018.

[74] F. Pakovich. On algebraic curves $A(x) - B(y) = 0$ of genus 0. *Math. Z.*, 288:299–310, 2018.

[75] V. Reiner, F. Saliola, and V. Welker. *Spectra of symmetrized shuffling operators*, volume 228. American Mathematical Society, 2014.

[76] C. Reutenauer. *Free Lie algebras*, volume 7 of *London Mathematical Society Monographs*. 1993.

[77] C. Reutenauer. On symmetric functions related to Witt vectors and the free Lie algebra. *Adv. Math.*, 110:234–246, 1995.

[78] M. Rosen. *Number theory in function fields*, volume 120 of *Graduate Texts in Mathematics*. Springer Science & Business Media, New York, 2013.

[79] S. Sam and A. Snowden. Gröbner methods for representations of combinatorial categories. *J. Amer. Math. Soc.*, 30:159–203, 2017.

[80] T. Schönemann. Grundzüge einer allgemeinen theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist. *J. Reine Angew. Math.*, 31:269–325, 1846.

[81] J. H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2007.

[82] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2009.

[83] W. Sinnott. On the Stickelberger ideal and the circular units of a cyclotomic field. *Ann. Math.*, 108:107–134, 1978.

[84] N. J. A. Sloane. The on-line encyclopedia of integer sequences, 2018. Accessed: 11-29-2018 at `https://oeis.org/A088996`.

[85] R. P. Stanley. Combinatorial reciprocity theorems. *Adv. Math.*, 14:194–253, 1974.

[86] R. P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[87] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2nd edition, 2009.

[88] S. Sundaram and V. Welker. Group actions on arrangements of linear subspaces and applications to configuration spaces. *Trans. Amer. Math. Soc.*, 349:1389–1420, 1997.

[89] The Stacks Project Authors. Stacks project. http://stacks.math.columbia.edu/tag/00U3, 2018.

[90] R. Vakil. Arizona winter school notes. Available at `http://swc.math.arizona.edu/aws/2015/2015VakilNotes.pdf`.

[91] H. Volklein. *Groups as Galois groups: an introduction*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1996.

[92] J. von Zur Gathen, A. Viola, and K. Ziegler. Counting reducible, powerful, and relatively irreducible multivariate polynomials over finite fields. *Siam J. Discrete Math.*, 27:855–891, 2013.

[93] D. Wan. Zeta functions of algebraic cycles over finite fields. *Manuscripta Math.*, 74:413–444, 1992.

[94] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 1997.

[95] E. Witt. Treue Darstellung Liescher Ringe. *J. Reine Angew. Math.*, 177:152–160, 1937.

[96] M. Zieve. An arithmetic dynamical Mordell-Lang conjecture. Workshop on Interactions between Model Theory and Arithmetic Dynamics, 2016.