Polynomial Statistics, Necklace Polynomials, and the Arithmetic Dynamical Mordell-Lang Conjecture

by

Trevor Hyde

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2019

Doctoral Committee:

Professor Jeffrey Lagarias, Co-Chair
Professor Michael Zieve, Co-Chair
Professor Kartik Prasanna
Professor John Schotland
Professor John Stembridge

Trevor Hyde

tghyde@umich.edu

ORCID 0000-0002-9380-1928

© Trevor Hyde 2019

Dedication

This thesis is dedicated to Aarthi and my parents Steve and Kathy. Thank you for all the years of unwavering love and support.

Acknowledgments

The author is grateful for the guidance and encouragement of his advisers Jeff Lagarias and Mike Zieve. I am also happy to thank Weiyan Chen, Benson Farb, Nir Gadish, Jonathan Gerhard, Ofir Gorodetsky, Rafe Jones, Bob Lutz, Andy Odesky, Karen Smith, Sheila Sundaram and Phil Tosteson for their help with and interest in my work over the past six years.

The author was supported by NSF grant DMS-1162181 in the summer of 2017, the Rackham One-Term Dissertation Fellowship in the winter of 2017, the NSF grant DMS-1701576 in the summer of 2018, and the Rackham Predoctoral Fellowship for the 2018-19 academic year.

List of Figures

List of Tables

Table of Contents

Abstract

This thesis consists of six chapters representing two directions of the author's graduate research under the advisement of Jeffrey Lagarias and Michael Zieve. The first direction studies new connections between the arithmetic statistics of polynomials over a finite field and the symmetric group representations carried by the cohomology of configuration space. The second direction, joint with Michael Zieve, studies unlikely intersections of orbits on curves, culminating in a non-commutative arithmetic dynamical Mordell-Lang theorem.

Chapter 1

Introduction

This thesis consists of six chapters representing two directions of the author's graduate research under the advisement of Jeffrey Lagarias and Michael Zieve. Chapters 2, 3, and 4 are revisions of three papers written by the author; the first two of which have been published and the third of which is currently an arXiv preprint. This line of work evolved from a paper written with Lagarias [53] into several distinct but related projects. Chapters 5 and 6 are joint work with Zieve which we intend to adapt and submit for publication. These results have been announced in talks given by both Zieve and the author since 2016, but this is the first time they have appeared in writing.

Below we briefly summarize the contents of each chapter and highlight their main results.

1.1 Splitting measures and factorization statistics

Chapter 2 explores the interface between arithmetic statistics and topology. Building on the work of Church, Ellenberg, and Farb [20], we find a surprising connection between the expected values of polynomial factorization statistics over a finite field and the symmetric group representations carried by the cohomology of the space of point configurations in $\mathbb{R}^3$.

Let $\mathbb{F}_q$ be a finite field with q elements and let $\mathrm{Poly}_d(\mathbb{F}_q)$ be the set of all degree d monic polynomials in $\mathbb{F}_q[x]$. Each $f(x) \in \mathrm{Poly}_d(\mathbb{F}_q)$ factors uniquely over $\mathbb{F}_q$ into irreducible polynomials. The degrees of the irreducible factors of $f(x)$ form a partition of the degree d

called the *factorization type* of $f(x)$. A function $P : \mathrm{Poly}_d(\mathbb{F}_q) \to \mathbb{Q}$ is called a *factorization statistic* if $P(f)$ depends only on the factorization type of $f(x)$. Thus factorization statistics may also be viewed as functions on the set of partitions of d or as class functions of the symmetric group S_d.

Given any topological space X, the *ordered configuration space* $\mathrm{PConf}_d(X)$ is the space of d distinct labelled points in X. More formally,

$$\mathrm{PConf}_d(X) := \{(x_1, x_2, \ldots, x_d) \in X^d : x_i \neq x_j\}.$$

The symmetric group S_d acts freely on $\mathrm{PConf}_d(X)$ by permuting coordinates. Thus, by functoriality, the cohomology $H^*(\mathrm{PConf}_d(X), \mathbb{Q})$ forms a sequence of S_d-representation for each space X.

Theorem 1.1.1. *Let $P : \mathrm{Poly}_d(\mathbb{F}_q) \to \mathbb{Q}$ be a factorization statistic and let ψ_d^k be the character of the S_d-representation $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$. Then the expected value $E_d(P)$ of P on $\mathrm{Poly}_d(\mathbb{F}_q)$ is a polynomial in $1/q$ given explicitly by*

$$E_d(P) := \frac{1}{q^d} \sum_{f \in \mathrm{Poly}_d(\mathbb{F}_q)} P(f) = \sum_{k=0}^{d-1} \frac{\langle P, \psi_d^k \rangle}{q^k},$$

where $\langle P, \psi_d^k \rangle := \frac{1}{d!} \sum_{\sigma \in S_d} P(\sigma)\psi_d^k(\sigma)$ is the standard inner product of class functions of S_d.

We use generating function techniques to give uniform proofs of Theorem 1.1.1 and the parallel result for squarefree factorization statistics first shown by Church, Ellenberg, and Farb [20, Prop. 4.1].

1.2 Liminal reciprocity and factorization statistics

Chapter 3 studies moduli spaces of multivariate irreducible polynomials through their $\mathbb{F}_q$-point counts. We show these point counts exhibit several remarkable properties, including q-adic convergence as the the number of variables in our polynomials tends to infinity.

Let $d, n \geq 1$ and let $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ denote the set of all total degree d monic polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ which are irreducible over $\mathbb{F}_q$. We show there exists a polynomial $M_{d,n}(x) \in \mathbb{Q}[x]$ such that

$$M_{d,n}(q) = |\mathrm{Irr}_{d,n}(\mathbb{F}_q)|$$

for all prime powers q. We call the family $M_{d,n}(x)$ the *higher necklace polynomials*. Our main result in Chapter 3 is Theorem 1.2.1.

Theorem 1.2.1. *Let $d \geq 1$. The sequence of polynomials $M_{d,n}(x)$ converges coefficientwise as $n \to \infty$ to a rational function $M_{d,\infty}(x) \in \mathbb{Q}(x)$. Furthermore this limit satisfies the self-reciprocal functional equation*

$$M_{d,\infty}(x) = -M_{d,1}\left(\tfrac{1}{1-\frac{1}{x}}\right),$$

where $M_{d,1}(x)$ is the classic necklace polynomial *given explicitly by*

$$M_{d,1}(x) := \frac{1}{d}\sum_{e|d} \mu(e) x^{d/e}. \tag{1.1}$$

We use Theorem 1.2.1 to establish a connection between liminal squarefree factorization statistics and the general univariate factorization statistics introduced in Chapter 2. As a consequence we show that the symmetric group representations carried by the cohomology of point configurations in $\mathbb{R}^3$ determines the q-adic asymptotics of multivariate squarefree factorization statistics as the number of variables tends to infinity.

1.3 Cyclotomic factors of necklace polynomials

Necklace polynomials $M_d(x)$ play an important role in number theory, combinatorics, dynamics, and representation theory. In Chapter 4 we introduce and analyze the *cyclotomic factor phenomenon*: the observation that for all $d \geq 1$ the dth necklace polynomial $M_d(x) := M_{d,1}(x)$ (see (1.1)) is highly reducible over $\mathbb{Q}$ with the majority of its irreducible factors being cyclotomic polynomials. One notable manifestation of the cyclotomic factor phenomenon in number theory is the following connection to multiplicative relations in

cyclotomic units.

Theorem 1.3.1. *Let $\Phi_d(x)$ be the dth cyclotomic polynomial. Suppose that $m, d > 1$ and m does not divide d. If $M_d(\zeta_m) = 0$ for all mth roots of unity ζ_m, then $\Phi_d(\zeta_m) = 1$ for all non-trivial mth roots of unity ζ_m. Equivalently,*

$$\prod_{j \in (\mathbb{Z}/(d))^\times} (\zeta_m - \zeta_d^j) = 1.$$

We show that the cyclotomic factor phenomenon extends in two independent directions: to the G-necklace polynomials associated to a finite group G and to the higher necklace polynomials $M_{d,n}(x)$ counting multivariate irreducible polynomials over a finite field. This latter generalization leads to a curious formula for the Euler characteristic of the moduli space of multivariate irreducible polynomials over $\mathbb{R}$ and $\mathbb{C}$.

Theorem 1.3.2. *Let $d, n \geq 1$, let $M_{d,n}(x)$ be the higher necklace polynomial, and let χ_c denote the compactly supported Euler characteristic. Then*

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad \chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1) = \begin{cases} a_k & \text{if } d = 2^k \\ 0 & \text{otherwise.} \end{cases}$$

where $n = \sum_{k \geq 0} a_k 2^k$ is the unique expansion of n as an alternating sum of an even number of powers of 2.

In particular, Theorem 1.3.2 implies that for each fixed n, $M_{d,n}(\pm 1) = 0$ for all but finitely many d. This gives a geometric explanation for the prevalence of $\Phi_1(x)$ and $\Phi_2(x)$ cyclotomic factors of necklace polynomials and suggests the possibility of a rich interpretation of this phenomenon more generally.

1.4 Arithmetic dynamical Mordell-Lang

Let K be a field and let $f(x) \in K(x)$ be a rational function. A general problem in *arithmetic dynamics* is to study the algebraic and number theoretic properties of orbits of points $p \in \mathbb{P}^1(K)$ under iteration of f. In Chapter 5 we prove (in collaboration with Michael

Zieve) a conjecture of Cahn, Jones, and Spear [10] on when orbits visit arithmetically special sets.

Theorem 1.4.1 (Arithmetic Dynamical Mordell-Lang)**.** *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 with $\deg(f) \geq 2$. If $p \in \mathcal{D}(K)$, then $\{n \in \mathbb{N} : f^n(p) \in u(C(K))\}$ is a finite union of arithmetic progressions.*

In other words, if the orbit of p under f visits the u-image of the K-points on C infinitely often, then it must do so periodically.

The strategy we employ to prove Theorem 1.4.1 also leads to the following two stability results in the dynamics of curve endomorphisms. Here we state the results for $\mathbb{P}^1$ to for simplicity. See Section 5.6 for a precise statement.

Theorem 1.4.2 (Geometric Eventual Stability)**.** *Let K be a field of characteristic 0, let $f(x)$ and $u(y)$ be rational functions defined over K such that $\deg(f) \geq 2$. Then there exists an explicit bound $G(d)$ depending only on $d := \deg(u)$ such that for every $m \geq G(d)$ the irreducible components of the curve $f^m(x) = u(y)$ are all induced from the irreducible components of $f^n(x) = u(y)$ for some $n \leq G(d)$.*

Theorem 1.4.3 (Iterate Decomposition Stability)**.** *Let K be a field of characteristic 0, let $f(x)$ and $u(x)$ be rational functions defined over K with $\deg(f) \geq 2$. Then there exists an explicit bound $I(d)$ 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 $m \leq I(d)$ such that $f^m = u \circ w$ for some rational function $w(x)$.*

1.5 Noncommutative arithmetic dynamical Mordell-Lang

In Chapter 6 (also joint with Zieve) we prove a noncommutative generalization of Theorem 1.4.1 which makes a connection to the theory of formal languages. If $S := \langle f_1, f_2, \ldots, f_g \rangle$ is a noncommutative finitely generated semigroup, then elements of S may be viewed as words in the alphabet $\{f_1, f_2, \ldots, f_g\}$. As such, we may interpret subsets of S as formal languages. The *regular languages* are an important and ubiquitous class of languages

informally characterized as those collections of words which can be recognized by a memoryless finite state machine.

Theorem 1.5.1 (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 finite endomorphisms $f_i : \mathcal{D} \to \mathcal{D}$ with $\deg(f_i) \geq 2$ for each i. If $p \in \mathcal{D}(K)$, then $\{w \in S : w(p) \in u(\mathcal{C}(K))\}$ is a regular language.*

Languages over an alphabet with one letter f correspond to subsets of $\mathbb{N}$ by $f^n \leftrightarrow n$. Regular languages over an alphabet with one letter are precisely the finite unions of arithmetic progressions, hence Theorem 1.5.1 is a proper generalization of Theorem 1.4.1.

Chapter 2

Splitting measures and factorization statistics

In this chapter we use combinatorial methods from the theory of generating functions to draw a surprising connection between the expected values of arithmetic functions on $\mathbb{F}_q[x]$, combinatorial representation theory, and the cohomology of point configurations in $\mathbb{R}^3$. This chapter is a revised version of the author's paper [52] published in the *International Mathematical Research Notices*.

2.1 Introduction

Definition 2.1.1. Let $\mathrm{Poly}_d(\mathbb{F}_q)$ denote the set of degree d monic polynomials in $\mathbb{F}_q[x]$. The *factorization type* of $f(x) \in \mathrm{Poly}_d(\mathbb{F}_q)$ is the partition of d formed by the degrees of the irreducible factors of $f(x)$ over $\mathbb{F}_q$. A *factorization statistic* P is a function defined on $\mathrm{Poly}_d(\mathbb{F}_q)$ such that $P(f)$ only depends on the factorization type of $f(x)$. Note that P may also be viewed as a function defined on partitions of d, or equivalently as a class function of the symmetric group S_d.

Theorem 2.1.2. *Let ψ_d^k be the character of the S_d-representation $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ where $\mathrm{PConf}_d(\mathbb{R}^3)$ is the ordered configuration space of d distinct points in $\mathbb{R}^3$ (see Section 2.2.) Then the expected value $E_d(P)$ of a factorization statistic P on $\mathrm{Poly}_d(\mathbb{F}_q)$ is given by*

$$E_d(P) := \frac{1}{q^d} \sum_{f \in \mathrm{Poly}_d(\mathbb{F}_q)} P(f) = \sum_{k=0}^{d-1} \frac{\langle P, \psi_d^k \rangle}{q^k},$$

where $\langle P, \psi_d^k \rangle := \frac{1}{d!} \sum_{\sigma \in S_d} P(\sigma)\psi_d^k(\sigma)$ *is the standard inner product of* $\mathbb{Q}$*-valued class functions of the symmetric group* S_d*.*

Theorem 2.1.2 asserts that the expected value of any factorization statistic P on $\mathrm{Poly}_d(\mathbb{F}_q)$ may be expressed as a polynomial in $1/q$ with coefficients determined by the representation theoretic structure of the cohomology of a configuration space in a way that is uniform in q. This result provides a bridge between the arithmetic statistics of polynomials over a finite field and the combinatorial topology of the space $\mathrm{PConf}_d(\mathbb{R}^3)$.

As one application of Theorem 2.1.2 we deduce the following structural description of the total cohomology of $\mathrm{PConf}_d(\mathbb{R}^3)$ from a simple probabilistic argument.

Theorem 2.1.3. *For each* $d \geq 1$ *there is an isomorphism of* S_d*-representations*

$$\bigoplus_{k=0}^{d-1} H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}) \cong \mathbb{Q}[S_d], \tag{2.1}$$

where $\mathbb{Q}[S_d]$ *is the regular representation of* S_d*.*

Theorem 2.1.3 is known, from other perspectives, to follow from the Poincaré-Birkhoff-Witt theorem [75, Pg. 56]. We explore consequences of Theorem 2.1.3 through examples in Section 2.3.

As a second application of Theorem 2.1.2 we deduce the asymptotic stability of expected values from the *representation stability* of the family $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ of symmetric group representations.

Definition 2.1.4. Let $x_k(f)$ be the number of degree k irreducible factors of $f \in \mathrm{Poly}_d(\mathbb{F}_q)$. Then a *character polynomial* P is a factorization statistic given by a polynomial in the x_k for $j \geq 1$.

Theorem 2.1.5. *Let* P *be a character polynomial. Then*

$$\lim_{d \to \infty} E_d(P) = \sum_{k=0}^{\infty} \frac{\langle P, \psi^k \rangle}{q^k}$$

where the limit is taken $1/q$*-adically (or equivalently, coefficientwise in the formal power series ring* $\mathbb{Q}[\![1/q]\!]$*,) and* $\langle P, \psi^k \rangle := \lim_{d\to\infty} \langle P, \psi_d^k \rangle$ *is the* stable multiplicity *of* P *in* ψ_d^k *(see Section 2.2.4.)*

The connection between expected values of factorization statistics and the symmetric group representations $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ is made through a probability measure on the symmetric group. Given a partition $\lambda \vdash d$, let $\nu(\lambda)$ denote the probability of a random element of $\mathrm{Poly}_d(\mathbb{F}_q)$ having factorization type λ. The function ν is called the *splitting measure*. We prove Theorem 2.1.6 using a generating function argument in Section 2.2.

Theorem 2.1.6. *Let* ψ_d^k *be the character of the* S_d*-representation* $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ *where* $\mathrm{PConf}_d(\mathbb{R}^3)$ *is the ordered configuration space of* d *distinct points in* $\mathbb{R}^3$ *(see Section 2.2.) Then for all* $d \geq 1$ *and partitions* $\lambda \vdash d$ *we have*

$$\nu(\lambda) = \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \frac{\psi_d^k(\lambda)}{q^k},$$

where $z_\lambda := \prod_{j\geq 1} j^{m_j} m_j!$ *when* $\lambda = (1^{m_1} 2^{m_2} \cdots)$*, and* $\psi_d^k(\lambda)$ *is the value of the character* ψ_d^k *on any element of the symmetric group* S_d *with cycle type* λ*.*

Church, Ellenberg, and Farb [20] connect the first moments of factorization statistics on the set $\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)$ of *squarefree* monic degree d polynomials to the symmetric group representations carried by the cohomology of configuration space through their *twisted Grothendieck-Lefschetz formula for* $\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)$.

Theorem 2.1.7 ([20, Prop. 4.1])**.** *Let* ϕ_d^k *be the character of the* S_d*-representation* $H^k(\mathrm{PConf}_d(\mathbb{C}), \mathbb{Q})$ *where* $\mathrm{PConf}_d(\mathbb{C})$ *is the ordered configuration space of* d *distinct points in* $\mathbb{C}$*. Let* $\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)$ *denote the set of squarefree monic degree* d *polynomials in* $\mathbb{F}_q[x]$*. Then for any factorization statistic* P*,*

$$\sum_{f \in \mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)} P(f) = q^d \sum_{k=0}^{d-1} \frac{(-1)^k \langle P, \phi_d^k \rangle}{q^k}, \tag{2.2}$$

where $\langle P, \phi_d^k \rangle := \frac{1}{d!} \sum_{\sigma \in S_d} P(\sigma)\phi_d^k(\sigma)$ *is the standard inner product of* $\mathbb{Q}$*-valued class functions of the symmetric group* S_d*.*

They derive the first moment formula (2.2) from the Grothendieck-Lefschetz trace formula for étale cohomology with "twisted coefficients." Lagarias and the author [53] use Theorem 2.1.7 to establish a representation theoretic interpretation of the *squarefree splitting measure* ν^{sf}, where $\nu^{\mathrm{sf}}(\lambda)$ is the probability of a random squarefree polynomial having factorization type λ.

Theorem 2.1.8 ([53, Thm. 1.2])**.** *Let* χ_d^k *be the character of the* S_d*-representation* $H^k(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q})$ *(see Section 2.2.2.) Then for all* $d \geq 2$ *and partitions* $\lambda \vdash d$ *we have*

$$\nu^{\mathrm{sf}}(\lambda) = \frac{1}{z_\lambda} \sum_{k=0}^{d-2} \frac{(-1)^k \chi_d^k(\lambda)}{q^k},$$

where $z_\lambda := \prod_{j \geq 1} j^{m_j} m_j!$ *when* $\lambda = (1^{m_1} 2^{m_2} \cdots)$*, and* $\chi_d^k(\lambda)$ *is the value of the character* χ_d^k *on any element of the symmetric group* S_d *with cycle type* λ*.*

We give a new proof of Theorem 2.1.8 using the same method as for Theorem 2.1.6 and derive Theorem 2.1.7 as a consequence. Our proofs of Theorem 2.1.2 and Theorem 2.1.7 do not use algebraic geometry or the Grothendieck-Lefschetz trace formula.

The use of generating functions in the study of factorization statistics is not new. Church, Ellenberg, and Farb [20] use L-functions to compute the stable limits of expected values of squarefree factorization statistics. Fulman [34] uses cycle index series to derive the asymptotic formulas for first moments of squarefree factorization statistics given in [20] without using representation theory or cohomology. Chen [17, 16] further develops these methods in the more general setting of an arbitrary affine or projective variety V defined over $\mathbb{F}_q$. Carlitz [13] uses zeta functions to compute the expected values of several specific factorization statistics.

Our main innovation is connecting factorization statistics of polynomials to the cohomology of configurations in $\mathbb{R}^3$ in a way parallel to the connection established by Church, Ellenberg, and Farb [20] between factorization statistics of squarefree polynomials and the cohomology of configurations in $\mathbb{C} \cong \mathbb{R}^2$, and providing a unified generating function method to derive both results.

There have been other generalizations of Theorem 2.1.7 from squarefree polynomials to all polynomials. Gadish [35, Sec. 1.3] and Hast, Matei [45] both study expected values of functions defined on the set of all polynomials; their functions depend on both the degree of the irreducible factors and their multiplicities. We call these *weighed factorization statistics*. Gadish [35, Cor. 1.4] shows that the expected value of a weighted factorization statistic P on $\mathrm{Poly}_d(\mathbb{F}_q)$ matches the expected value of P on S_d viewed as a class function. Stated geometrically, the expected values of weighted factorization statistics on degree d polynomials correspond to the cohomology of $\mathbb{R}^d$ as an S_d-representation, while the expected values of our factorization statistics correspond to the cohomology of $\mathrm{PConf}_d(\mathbb{R}^3)$ as an S_d-representation.

2.1.1 Further questions

Church, Ellenberg, and Farb's étale cohomology approach to Theorem 2.1.7 illustrates a clear geometric connection between squarefree factorization statistics and the cohomology of ordered configurations in $\mathbb{C}$. To summarize, we start with the map of schemes

$$\mathrm{PConf}_d(\mathbb{A}^1) \longrightarrow \mathrm{Conf}_d(\mathbb{A}^1), \tag{2.3}$$

which sends an ordered configuration of d points to its counterpart in the unordered configuration space $\mathrm{Conf}_d(\mathbb{A}^1)$. The symmetric group S_d acts freely on $\mathrm{PConf}_d(\mathbb{A}^1)$ by permuting points in the ordered configuration, and the map in (2.3) is the quotient by this action. The $\mathbb{F}_q$-points of $\mathrm{Conf}_d(\mathbb{A}^1)$ are in natural correspondence with squarefree polynomials of degree d, and the $\mathbb{C}$-points of $\mathrm{PConf}_d(\mathbb{A}^1)$ give us the manifold $\mathrm{PConf}_d(\mathbb{C})$. The Grothendieck-Lefschetz trace formula connects point counts over finite fields with the étale cohomology of the scheme; general comparison theorems between cohomology theories relate the étale cohomology to the singular cohomology of the manifold $\mathrm{PConf}_d(\mathbb{C})$.

The map (2.3) is unramified, simplifying the application of the Grothendieck-Lefschetz trace formula. The corresponding map of schemes in the case of all polynomials is

$$(\mathbb{A}^1)^d \longrightarrow \mathrm{Sym}_d(\mathbb{A}^1),$$

which is highly ramified. Gadish [35] adapts the étale cohomological perspective to handle ramified covers. This geometrically natural extension leads Gadish to a twisted Grothendieck-Lefschetz formula for weighted factorization statistics [35, Thm. A (1.2)].

Our factorization statistics extend those on $\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)$ in a way that is combinatorially natural but is difficult to manage from the algebro-geometric perspective. This results in a surprising connection to the cohomology of ordered configurations in $\mathbb{R}^3$ for which we have no geometric account.

Question 2.1.9. Is there a geometric explanation for the connection between factorization statistics on $\mathrm{Poly}_d(\mathbb{F}_q)$ and the cohomology of $\mathrm{PConf}_d(\mathbb{R}^3)$?

Church, Ellenberg, and Farb deduce their twisted Grothendieck-Lefschetz formula from a more general result relating factorization statistics on quotients of complements of hyperplane arrangements to the étale cohomology of said complements. Note that $\mathrm{PConf}_d(\mathbb{C})$ may be interpreted as the complement of the *braid arrangement*, consisting of the hyperplanes $z_i = z_j$ for all $i \neq j$. Given a collection of linear forms L defined over $\mathbb{Z}$ in d variables which is stable under the natural action of S_d, let $A_d(L)$ be the complement of the hyperplane arrangement determined by the vanishing sets of the linear forms. Let $B_d(L)$ denote the scheme-theoretic quotient of $A_d(L)$ by the action of S_d.

Theorem 2.1.10 ([20, Thm. 3.7])**.** *Let P be a factorization statistic. If ℓ is a prime coprime to q and τ_d^k is the character of $H^k_{\acute{e}t}(A_d(L), \mathbb{Q}_\ell)$, then*

$$\sum_{f \in B(L)_d(\mathbb{F}_q)} P(f) = \sum_{k=0}^{d} (-1)^k \langle P, \tau_d^k \rangle q^{d-k}.$$

Given that our generating function method provides a new proof of the special case Theorem 2.1.7, we ask:

Question 2.1.11. Can our methods be adapted to give a new proof of Theorem 2.1.10?

The key to answering Question 2.1.11 is to find explicit product formulas for the cycle index series of the family of representations given by the étale cohomology analogous to those used in our proof of Theorem 2.2.2. Such formulas may be known, but not to us.

2.2 Representation theoretic interpretation of splitting measures

Let q be a prime power, let $d \geq 1$ be an integer, and let $\mathrm{Poly}_d(\mathbb{F}_q)$ be the set of monic degree d polynomials in $\mathbb{F}_q[x]$. The subset of squarefree polynomials is denoted $\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q) \subseteq \mathrm{Poly}_d(\mathbb{F}_q)$. Every polynomial $f \in \mathrm{Poly}_d(\mathbb{F}_q)$ has a unique factorization into irreducible polynomials over $\mathbb{F}_q$. The degrees of the irreducible factors of f form a partition $[f]$ of the degree d which we call the *factorization type* of f. Recall that the number of degree d irreducible polynomials in $\mathbb{F}_q[x]$ is given by the *necklace polynomial*

$$M_d(q) := \frac{1}{d} \sum_{e|d} \mu(e) q^{d/e}.$$

The total number of monic degree d polynomials over $\mathbb{F}_q$ is $|\mathrm{Poly}_d(\mathbb{F}_q)| = q^d$, while the total number of squarefree polynomials is $|\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)| = q^d - q^{d-1}$ for $d \geq 2$ (see, for example, [78, Prop. 2.3].) Given a partition $\lambda \vdash d$ we define, we define the *splitting measure* $\nu(\lambda)$ to be the probability of an element $f \in \mathrm{Poly}_d(\mathbb{F}_q)$ having factorization type λ, and similarly define the *squarefree splitting measure* $\nu^{\mathrm{sf}}(\lambda)$ for $f \in \mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)$. If λ is a partition, then $m_j = m_j(\lambda)$ is the number of size j parts of λ. In other words, $\lambda = (1^{m_1} 2^{m_2} 3^{m_3} \cdots)$. Thus, using unique factorization we can express the splitting measures explicitly by

$$\nu(\lambda) := \frac{1}{|\mathrm{Poly}_d(\mathbb{F}_q)|} \prod_{j \geq 1} \left(\!\!\binom{M_j(q)}{m_j}\!\!\right) \qquad \nu^{\mathrm{sf}}(\lambda) := \frac{1}{|\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)|} \prod_{j \geq 1} \binom{M_j(q)}{m_j},$$

where

$$\left(\!\!\binom{x}{m}\!\!\right) := \frac{x(x+1)(x+2)\cdots(x+m-1)}{m!} = \binom{x+m-1}{m}.$$

Note that $\left(\!\binom{x}{m}\!\right)$ counts the number of subsets of size m chosen from an x element set with repetition.

Remark 2.2.1. The squarefree splitting measure was first defined by Lagarias and Weiss in [56] and subsequently studied by Lagarias [55] and Hyde and Lagarias [53]. The splitting measure ν is studied from a statistical point of view in [2], although not by that name.

Both splitting measures are rational functions in q for each partition λ, and furthermore

both are polynomials in $1/q$ (this is clear for $\nu(\lambda)$ and is shown for $\nu^{\mathrm{sf}}(\lambda)$ in [53, Prop. 2.4].) Recall that the partitions $\lambda \vdash d$ parametrize the conjugacy classes of the symmetric group S_d. Thus the splitting measures may be viewed as polynomial-valued class functions on S_d. Our first result Theorem 2.2.2 gives an interpretation of the coefficients of the splitting measures in terms of the representation theory of the symmetric group.

We review some terminology and notation. If χ is a character of the symmetric group S_d and λ is a partition of d, we write $\chi(\lambda)$ for the value of χ on any element $\sigma \in S_d$ of cycle type λ. This is well-defined since characters are constant on conjugacy classes. Let z_λ be the number of permutations in S_d commuting with an element $\sigma \in S_d$ of cycle type λ, then

$$z_\lambda := \prod_{j \geq 1} j^{m_j} m_j!.$$

The *rank* of a partition $\lambda \vdash d$ is $\mathrm{rk}(\lambda) := \sum_{j \geq 1} m_j - 1 = d - \ell(\lambda)$, where $\ell(\lambda)$ is the number of parts in λ.

2.2.1 Higher Lie representations

Given a positive integer d, let ζ_d be a faithful one-dimensional complex representation of the cyclic group C_d. Viewing C_d as a subgroup of the symmetric group S_d generated by a d-cycle, the *dth Lie representation* $\mathrm{Lie}(d)$ is defined as

$$\mathrm{Lie}(d) := \mathrm{Ind}_{C_d}^{S_d} \zeta_d.$$

For a partition $\lambda \vdash d$, the *higher Lie representation* Lie_λ is defined as

$$\mathrm{Lie}_\lambda := \mathrm{Ind}_{Z_\lambda}^{S_d} \bigotimes_{j \geq 1} \mathrm{Lie}(j)^{\otimes m_j(\lambda)},$$

where Z_λ is the centralizer of a permutation with cycle type λ. Finally, for $0 \leq k < d$ let Lie_d^k be the S_d-representation

$$\mathrm{Lie}_d^k := \bigoplus_{\mathrm{rk}(\lambda)=k} \mathrm{Lie}_\lambda.$$

2.2.2 Configuration spaces

Given a topological space X, let $\mathrm{PConf}_d(X)$ be the space of ordered configurations of d distinct points in X,

$$\mathrm{PConf}_d(X) := \{(x_1, x_2, \ldots, x_d) \in X^d : x_i \neq x_j \text{ when } i \neq j\}.$$

The symmetric group S_d acts freely on $\mathrm{PConf}_d(X)$ by permuting the coordinates. Thus the singular cohomology $H^k(\mathrm{PConf}_d(X), \mathbb{Q})$ is, by functoriality, an S_d-representation for all $k \geq 0$. Sundaram and Welker [88, Thm. 4.4 (iii)] show for $k \geq 0$ that for every odd $n \geq 3$

$$H^{(n-1)k}(\mathrm{PConf}_d(\mathbb{R}^n), \mathbb{Q}) \cong \mathrm{Lie}_d^k,$$

as S_d-representations (see [48, Sec. 2.3] for a discussion of this result in language closer to our presentation.) For the sake of concreteness we specialize to the case $n = 3$,

$$H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}) \cong \mathrm{Lie}_d^k.$$

If $X = \mathbb{C}$, then the unit group $\mathbb{C}^\times$ acts on $\mathrm{PConf}_d(\mathbb{C})$ by simultaneously scaling all coordinates; this action commutes with S_d, hence there is a well-defined S_d-action on the quotient $\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times$. Thus $H^k(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q})$ is an S_d-representation for all $k \geq 0$.

We now come to our first main result.

Theorem 2.2.2. *Let ψ_d^k and χ_d^k be the characters of the S_d-representations $\mathrm{Lie}_d^k \cong H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ and $H^k(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q})$ respectively.*

1. *For $d \geq 1$ and each partition $\lambda \vdash d$,*

$$\nu(\lambda) = \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \frac{\psi_d^k(\lambda)}{q^k}.$$

2. *For $d \geq 2$ and each partition $\lambda \vdash d$,*

$$\nu^{\mathrm{sf}}(\lambda) = \frac{1}{z_\lambda} \sum_{k=0}^{d-2} \frac{(-1)^k \chi_d^k(\lambda)}{q^k}.$$

Remark 2.2.3. This representation theoretic interpretation of the squarefree splitting measure was first shown in [53, Thm. 5.1] using the twisted Grothendieck-Lefschetz formula for squarefree factorization statistics of Church, Ellenberg, and Farb [20, Prop. 4.1]. We prove Theorem 2.2.2 using generating functions, leading to a new proof of the twisted Grothendieck-Lefschetz formula for squarefree factorization statistics in Theorem 2.2.8. The representation theoretic interpretation of the splitting measure $\nu(\lambda)$ appears to be new.

Proof. 1. For each integer $j \geq 1$ let p_j be a formal variable. If $\lambda = (1^{m_1}2^{m_2}\cdots)$ is a partition, let $p_\lambda := \prod_{j\geq 1} p_j^{m_j}$. Hersh and Reiner [48, Thm. 2.17] state the following identity of formal power series

$$\sum_{d\geq 0}\sum_{\lambda\vdash d}\frac{1}{z_\lambda}\sum_{k=0}^{d-1}\psi_d^k(\lambda)q^{d-k}p_\lambda t^d = \prod_{j\geq 1}\left(\frac{1}{1-p_j t^j}\right)^{M_j(q)}, \tag{2.4}$$

where $M_j(q) = \frac{1}{j}\sum_{i|j}\mu(i)q^{j/i}$ is the jth necklace polynomial and ψ_d^k is the character of Lie_d^k (see Remark 2.2.4 for a discussion of the equivalence of 2.4 and [48, Thm. 2.17].) Recall the following version of the binomial theorem for formal power series,

$$\left(\frac{1}{1-t}\right)^m = \sum_{d\geq 0}\left(\!\!\binom{m}{d}\!\!\right)t^d,$$

where $\left(\!\binom{m}{d}\!\right) = \frac{m(m+1)(m+2)\cdots(m+d-1)}{d!}$. Expanding the right hand side of (2.4) with $t = 1/q$ gives

$$\begin{aligned}\prod_{j\geq 1}\left(\frac{1}{1-p_j/q^j}\right)^{M_j(q)} &= \prod_{j\geq 1}\sum_{m_j\geq 0}\left(\!\!\binom{M_j(q)}{m_j}\!\!\right)\frac{p_j^{m_j}}{q^{jm_j}}\\ &= \sum_{d\geq 0}\sum_{\lambda\vdash d}\left(\frac{1}{q^d}\prod_{j\geq 1}\left(\!\!\binom{M_j(q)}{m_j(\lambda)}\!\!\right)\right)p_\lambda \\ &= \sum_{d\geq 0}\sum_{\lambda\vdash d}\nu(\lambda)p_\lambda.\end{aligned} \tag{2.5}$$

Comparing coefficients of p_λ we conclude that

$$\nu(\lambda) = \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \frac{\psi_d^k(\lambda)}{q^k}.$$

2. The derivation of the formula for $\nu^{\mathrm{sf}}(\lambda)$ starts with another formal power series identity from [48, Thm. 2.17]. Let ϕ_d^k be the character of the S_d-representation $H^k(\mathrm{PConf}_d(\mathbb{C}), \mathbb{Q})$. Then

$$\sum_{d\geq 0} \sum_{\lambda\vdash d} \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \phi_d^k(\lambda) q^{d-k} p_\lambda t^d = \prod_{j\geq 1} (1 + (-1)^j p_j t^j)^{M_j(-q)}.$$

The substitutions $t \mapsto -t$ and $q \mapsto -q$ simplify this to

$$\sum_{d\geq 0} \sum_{\lambda\vdash d} \frac{1}{z_\lambda} \sum_{k=0}^{d-1} (-1)^k \phi_d^k(\lambda) q^{d-k} p_\lambda t^d = \prod_{j\geq 1} (1 + p_j t^j)^{M_j(q)}. \tag{2.6}$$

By the binomial theorem, the right hand side of (2.6) expands with $t = 1/q$ as

$$\begin{aligned} \prod_{j\geq 1} (1 + p_j/q^j)^{M_j(q)} &= \prod_{j\geq 1} \sum_{m_j\geq 0} \binom{M_j(q)}{m_j} \frac{p_j^{m_j}}{q^{jm_j}} \\ &= \sum_{d\geq 0} \sum_{\lambda\vdash d} \left(\frac{1}{q^d} \prod_{j\geq 1} \binom{M_j(q)}{m_j(\lambda)} \right) p_\lambda \\ &= \sum_{d\geq 0} \sum_{\lambda\vdash d} \left(1 - \tfrac{1}{q}\right) \nu^{\mathrm{sf}}(\lambda) p_\lambda. \end{aligned} \tag{2.7}$$

Let χ_d^k be the character of the S_d-representation $H^k(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q})$. Hyde and Lagarias [53, Prop. 4.2, Thm. 4.3] showed that

$$H^k(\mathrm{PConf}_d(\mathbb{C}), \mathbb{Q}) \cong H^k(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q}) \oplus H^{k-1}(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q}),$$

as S_d-representations from which it follows that $\phi_d^k = \chi_d^k + \chi_d^{k-1}$.

Note that $H^{-1}(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q}) = H^{d-1}(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q}) = 0$. Therefore

$$\begin{aligned}\frac{1}{1-\frac{1}{q}}\sum_{k=0}^{d-1}\frac{(-1)^k\phi_d^k(\lambda)}{q^k} &= \frac{1}{1-\frac{1}{q}}\sum_{k=0}^{d-1}\frac{(-1)^k\left(\chi_d^k(\lambda)+\chi_d^{k-1}(\lambda)\right)}{q^k} \\ &= \frac{1}{1-\frac{1}{q}}\sum_{k=0}^{d-2}\frac{(-1)^k\chi_d^k(\lambda)}{q^k}+\frac{(-1)^{k+1}\chi_d^k(\lambda)}{q^{k+1}} \\ &= \sum_{k=0}^{d-2}\frac{(-1)^k\chi_d^k(\lambda)}{q^k}.\end{aligned} \tag{2.8}$$

Multiplying the degree $d \geq 2$ term of (2.7) by $\frac{1}{1-\frac{1}{q}}$ gives,

$$\sum_{\lambda\vdash d}\frac{1}{z_\lambda}\sum_{k=0}^{d-2}\frac{(-1)^k\chi_d^k(\lambda)}{q^k}p_\lambda = \sum_{\lambda\vdash d}\nu^{\mathrm{sf}}(\lambda)p_\lambda.$$

Finally, comparing coefficients of p_λ we conclude that for $d \geq 2$

$$\nu^{\mathrm{sf}}(\lambda) = \frac{1}{z_\lambda}\sum_{k=0}^{d-2}\frac{(-1)^k\chi_d^k(\lambda)}{q^k}. \qquad \square$$

Remark 2.2.4. The generating functions used in the proof of Theorem 2.2.2 are stated in terms of symmetric functions in [48]. To convert between their notation and ours one should interpret the formal variable p_j as the j symmetric power sum, and then our formal power series identity becomes an identity of symmetric functions.

Hersh and Reiner cite several sources for the origin of these generating functions. A derivation of the identity for the higher Lie characters may be found in [43, Thm. 3.7], although the characters are not called by this name there. The generating function for the cohomology of configurations in $\mathbb{C}$ is derived in [11, Cor. 4.4] with notation similar to ours but stated in a way that does not explicitly connect it with configuration space. Both product formulas result from a plethystic decomposition of the respective families of representations.

2.2.3 Factorization statistics and the cohomology of configuration space

A *factorization statistic* P is a function defined on $\mathrm{Poly}_d(\mathbb{F}_q)$ such that $P(f)$ only depends on the factorization type of $f \in \mathrm{Poly}_d(\mathbb{F}_q)$. Equivalently, P may be viewed as a function defined on the set of partitions of d or as a class function of the symmetric group S_d. Any class function P may be interpreted as a factorization statistic.

Example 2.2.5. 1. Consider the polynomials $g(x), h(x) \in \mathrm{Poly}_5(\mathbb{F}_3)$ with irreducible factorizations

$$g(x) = x^2(x+1)(x^2+1) \qquad h(x) = (x+1)(x-1)(x^3-x+1).$$

The factorization type of $g(x)$ is the partition $(1^3\,2^1)$ and the factorization type of $h(x)$ is $(1^2\,3^1)$. Note that the factorization type does not detect the multiplicity of a specific factor so that x^2 and $x(x+1)$ both have the same factorization type (1^2).

2. Let $R(f)$ be the number of $\mathbb{F}_q$-roots of $f(x) \in \mathrm{Poly}_d(\mathbb{F}_q)$. Then $R(f)$ depends only on the number of linear factors of $f(x)$, hence is a factorization statistic. Referring to the two polynomials above, $R(g) = 3$ and $R(h) = 2$.
3. For $k \geq 1$, let $x_k(f)$ be the number of degree k irreducible factors of $f \in \mathrm{Poly}_d(\mathbb{F}_q)$, then x_k is a factorization statistic. As a function on partitions $x_k(\lambda) = m_k(\lambda)$ is the number of parts of λ of size k. Note that $R = x_1$. The ring $\mathbb{Q}[x_1, x_2, \ldots]$ generated by the functions x_k for $k \geq 1$ is called the ring of *character polynomials*. We return to character polynomials in Section 2.2.4 when discussing asymptotic stability.
4. Say a polynomial $f(x)$ has *even type* if the factorization type of $f(x)$ is an even partition. In other words, suppose $\lambda = (1^{m_1}2^{m_2}3^{m_3}\cdots)$ is the factorization type of $f(x)$ and define $\mathrm{sgn}(\lambda)$ by

$$\mathrm{sgn}(\lambda) := \prod_{j \geq 1} (-1)^{m_j(j-1)},$$

then $f(x)$ has even type if $\mathrm{sgn}(\lambda) = 1$. The indicator function ET defined by

$$ET(f) = \begin{cases} 1 & f(x) \text{ has even type} \\ 0 & \text{otherwise,} \end{cases}$$

is a factorization statistic. Thus $ET(g) = 0$ and $ET(h) = 1$. □

Let $E_d(P)$ denote the expected value of a factorization statistic P on $\mathrm{Poly}_d(\mathbb{F}_q)$ and let $E_d^{\mathrm{sf}}(P)$ denote the expected value of P on $\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)$. More precisely,

$$E_d(P) := \frac{1}{|\mathrm{Poly}_d(\mathbb{F}_q)|} \sum_{f \in \mathrm{Poly}_d(\mathbb{F}_q)} P(f)$$
$$E_d^{\mathrm{sf}}(P) := \frac{1}{|\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)|} \sum_{f \in \mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)} P(f).$$

Example 2.2.6 (Quadratic excess)**.** This example is inspired by [20, Pg. 6]. Define the *quadratic excess* $Q(f)$ of a polynomial $f(x) \in \mathbb{F}_q[x]$ to be

$$\begin{aligned} Q(f) = \ & \#\{\text{reducible quadratic factors of } f(x)\} \\ & - \#\{\text{irreducible quadratic factors of } f(x)\}, \end{aligned}$$

where both counts are considered with multiplicity. Note that $Q(f)$ depends only on the number of linear and irreducible quadratic factors of $f(x)$. For instance, if $g(x) = x^2(x+1)(x^2+1)^4 \in \mathbb{F}_3[x]$, then $g(x)$ has 3 linear factors and 4 irreducible quadratic factor, hence

$$Q(g) = \binom{3}{2} - \binom{4}{1} = -1.$$

The table below gives the expected value $E_d(Q)$ for small values of d.

d	$E_d(Q)$
3	$\frac{2}{q} + \frac{1}{q^2}$
4	$\frac{2}{q} + \frac{2}{q^2} + \frac{2}{q^3}$
5	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{2}{q^4}$
6	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{3}{q^5}$
10	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{6}{q^5} + \frac{6}{q^6} + \frac{8}{q^7} + \frac{8}{q^8} + \frac{5}{q^9}$

Table 2.1: Expected values of quadratic excess.

We note a few remarkable features of these expected values. For each d, $E_d(Q)$ is a

polynomial in $\frac{1}{q}$ of degree $d-1$ with *positive integer coefficients*; one should expect the coefficients to be rational numbers, but both the positivity and integrality are not a priori evident. Evaluating the polynomial $E_d(Q)$ at $q = 1$ gives the binomial coefficient $\binom{d}{2}$. The coefficients of $E_d(Q)$ appear to stabilize as d increases with a clear pattern emerging already for $d = 10$, suggesting that the expected values $E_d(Q)$ converge coefficientwise as $d \to \infty$.

All of these observations are deduced as consequences of Theorem 2.2.7 in Section 2.3.1. □

Our second main result gives an explicit expression for the expected value $E_d(P)$ of a factorization statistic in terms of the ordered configuration space of d distinct points in $\mathbb{R}^3$.

If P and Q are $\mathbb{Q}$-valued class functions on S_d, let $\langle P, Q\rangle$ denote their standard S_d-invariant inner product

$$\langle P, Q\rangle := \frac{1}{d!}\sum_{\sigma\in S_d} P(\sigma)Q(\sigma) = \sum_{\lambda\vdash d}\frac{P(\lambda)Q(\lambda)}{z_\lambda}.$$

Theorem 2.2.7. *Suppose P is a factorization statistic and $d \geq 1$. If ψ_d^k is the character of the S_d-representation* $\mathrm{Lie}_d^k \cong H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$*, then*

$$E_d(P) = \sum_{k=0}^{d-1}\frac{\langle P, \psi_d^k\rangle}{q^k}.$$

Proof. Since factorization statistics depend only on the factorization type of a polynomial, the expected value $E_d(P)$ may be written in terms of the splitting measure as

$$E_d(P) = \frac{1}{q^d}\sum_{f\in\mathrm{Poly}_d(\mathbb{F}_q)} P(f) = \sum_{\lambda\vdash d} P(\lambda)\nu(\lambda).$$

Then Theorem 2.2.2 implies,

$$\begin{aligned} E_d(P) &= \sum_{\lambda \vdash d} P(\lambda)\nu(\lambda) \\ &= \sum_{\lambda \vdash d} \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \frac{P(\lambda)\psi_d^k(\lambda)}{q^k} \\ &= \sum_{k=0}^{d-1} \frac{1}{q^k} \left(\sum_{\lambda \vdash d} \frac{P(\lambda)\psi_d^k(\lambda)}{z_\lambda} \right) \\ &= \sum_{k=0}^{d-1} \frac{\langle P, \psi_d^k \rangle}{q^k}. \end{aligned}$$

□

Church, Ellenberg, and Farb [20] relate the first moments of factorization statistics on squarefree polynomials to the ordered configuration space of d distinct points in $\mathbb{C}$. Let ϕ_d^k be the character of $H^k(\mathrm{PConf}_d(\mathbb{C}), \mathbb{Q})$ as a representation of S_d. In [20, Prop. 4.1], Church et al. show that

$$\sum_{f \in \mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)} P(f) = \sum_{k=0}^{d-1} (-1)^k \langle P, \phi_d^k \rangle q^{d-k}. \tag{2.9}$$

Dividing by $|\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)| = q^d - q^{d-1}$ gives the expected value, but also changes the coefficients on the right hand side. The calculation (2.8) in the proof of Theorem 2.2.2 shows that the identity (2.9) is equivalent to Theorem 2.2.8 below.

We give a new proof of [20, Prop. 4.1] using Theorem 2.2.2.

Theorem 2.2.8. *Suppose P is a factorization statistic and $d \geq 2$. If χ_d^k is the character of the S_d-representation $H^k(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q})$, then*

$$E_d^{\mathrm{sf}}(P) = \sum_{k=0}^{d-2} \frac{(-1)^k \langle P, \chi_d^k \rangle}{q^k}.$$

Proof. The proof is parallel to that of Theorem 2.2.7. First note that

$$E_d^{\mathrm{sf}}(P) = \frac{1}{q^d - q^{d-1}} \sum_{f \in \mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)} P(f) = \sum_{\lambda \vdash d} P(\lambda)\nu^{\mathrm{sf}}(\lambda),$$

and then use Theorem 2.2.2 to conclude

$$\begin{aligned} E_d^{\mathrm{sf}}(P) &= \sum_{\lambda \vdash d} P(\lambda)\nu^{\mathrm{sf}}(\lambda) \\ &= \sum_{\lambda \vdash d} \frac{1}{z_\lambda} \sum_{k=0}^{d-2} \frac{(-1)^k P(\lambda)\chi_d^k(\lambda)}{q^k} \\ &= \sum_{k=0}^{d-2} \frac{(-1)^k}{q^k} \left(\sum_{\lambda \vdash d} \frac{P(\lambda)\chi_d^k(\lambda)}{z_\lambda} \right) \\ &= \sum_{k=0}^{d-2} \frac{(-1)^k \langle P, \chi_d^k \rangle}{q^k}. \end{aligned}$$

□

Remark 2.2.9. The étale cohomological approach to Theorem 2.2.8 taken in [20] connects squarefree polynomials over $\mathbb{F}_q$ with the configuration space of points on the affine line. The geometric perspective seems to break down in the case of Theorem 2.2.7: There is no apparent correspondence between configurations of distinct points in $\mathbb{R}^3$ and monic polynomials over $\mathbb{F}_q$. It would be interesting to know of a geometric explanation for the relationship between the representations $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ and the expected value of factorization statistics on $\mathrm{Poly}_d(\mathbb{F}_q)$.

2.2.4 Asymptotic stability

Church [19, Thm. 1] showed that for all $k \geq 0$ and $n \geq 2$ the families of symmetric group representations $H^k(\mathrm{PConf}_d(\mathbb{R}^n), \mathbb{Q})$ are *representation stable*. We do not require the details of representation stability (the interested reader should consult [21],) only the following fact [20, Sec. 3.4] which we take as a black box: If P is a factorization statistic given by a character polynomial (see Example 2.2.5 (3)) and A_d is a sequence of S_d-representations with characters α_d which exhibit "representation stability," then the sequence of inner products $\langle P, \alpha_d \rangle$ is eventually constant. In that case we write $\langle P, \alpha \rangle$ for the limit of $\langle P, \alpha_d \rangle$ as $d \to \infty$.

Church, Ellenberg, and Farb use the representation stability of $H^k(\mathrm{PConf}_d(\mathbb{C}), \mathbb{Q})$ to prove Theorem 2.2.10. Recall that ϕ_d^k is the character of the S_d-representation $H^k(\mathrm{PConf}_d(\mathbb{C}), \mathbb{Q})$.

Theorem 2.2.10 ([20, Thm. 1])**.** *Let P be a factorization statistic given by a character polynomial and write $\langle P, \phi^k \rangle$ for the limit of $\langle P, \phi_d^k \rangle$ as $d \to \infty$. Then*

$$\lim_{d\to\infty} \frac{1}{q^d} \sum_{f \in \mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)} P(f) = \sum_{k=0}^{\infty} \frac{(-1)^k \langle P, \phi^k \rangle}{q^k}.$$

Church's theorem implies that for each k, $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ is representation stable. Hyde and Lagarias showed that $H^k(\mathrm{PConf}_d(\mathbb{C})/\mathbb{C}^\times, \mathbb{Q}) \cong \beta_{[k]}(\Pi_d)$ as S_d-representations where $\beta_{[k]}(\Pi_d)$ is the *rank-selected homology of the partition lattice*. Hersh and Reiner [48, Thm. 1.8] showed that $\beta_{[k]}(\Pi_d)$ is representation stable. Therefore we deduce the asymptotic stability of expected values from Theorems 2.2.7 and 2.2.8.

Theorem 2.2.11 (Asymptotic stability of expected values)**.** *Let P be a factorization statistic given by a character polynomial (see Section 2.2.5 (3).) Then*

$$\lim_{d\to\infty} E_d(P) = \sum_{k=0}^{\infty} \frac{\langle P, \psi^k \rangle}{q^k} \qquad \lim_{d\to\infty} E_d^{\mathrm{sf}}(P) = \sum_{k=0}^{\infty} \frac{(-1)^k \langle P, \chi^k \rangle}{q^k},$$

where the limits are taken $1/q$-adically (or equivalently coefficientwise in $\mathbb{Q}[\![1/q]\!]$.)

2.2.5 Constraint on $E_d(P)$ coefficients

Theorem 2.2.12 below identifies the total cohomology of $\mathrm{PConf}_d(\mathbb{R}^3)$ with the regular representation $\mathbb{Q}[S_d]$.

Theorem 2.2.12. *For each $d \geq 1$ there is an isomorphism of S_d-representations*

$$\bigoplus_{k=0}^{d-1} H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}) \cong \mathbb{Q}[S_d], \tag{2.10}$$

where $\mathbb{Q}[S_d]$ is the regular representation of S_d.

Proof. Let ρ be the character of $\bigoplus_{k=0}^{d-1} H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$. Then

$$\rho = \sum_{k=0}^{d-1} \psi_d^k,$$

where ψ_d^k is the character of $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$. It suffices to show that ρ is equal to the character of the regular representation, that is

$$\rho(\lambda) = \begin{cases} d! & \lambda = [1^d] \\ 0 & \text{otherwise.} \end{cases}$$

By Theorem 2.2.2 we have

$$\nu(\lambda) = \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \frac{\psi_d^k(\lambda)}{q^k},$$

where ν is the splitting measure defined by

$$\nu(\lambda) = \frac{1}{q^d} \prod_{j \geq 1} \left(\!\!\binom{M_j(q)}{m_j}\!\!\right).$$

Let ν_1 denote the splitting measure evaluated at $q = 1$. Then $\nu_1(\lambda) = \frac{\rho(\lambda)}{z_\lambda}$. On the other hand, $M_j(1) = 0$ for $j > 1$ and $M_1(1) = 1$ so

$$\nu_1(\lambda) = \prod_{j \geq 1} \left(\!\!\binom{M_j(1)}{m_j}\!\!\right) = \begin{cases} 1 & \lambda = [1^d] \\ 0 & \text{otherwise.} \end{cases}$$

Since $z_{[1^d]} = d!$ the result follows. □

Corollary 2.2.13 will be used in Section 2.3 to explain a common phenomenon that arises in expected value computations for factorization statistics.

Corollary 2.2.13. *Suppose P is a factorization statistic defined on* $\mathrm{Poly}_d(\mathbb{F}_q)$ *which, viewed as a class function of S_d, is the character of an S_d-representation V. Let $E_d(P)$ be the expected value of P on* $\mathrm{Poly}_d(\mathbb{F}_q)$.

1. *$E_d(P)$ is a polynomial in $1/q$ of degree at most $d-1$ with non-negative integer coefficients.*
2. *The evaluation of $E_d(P)$ at $q=1$ is $E_d(P)_{q=1} = \dim V = P(1^d)$.*

Proof. 1. Recall that the inner product $\langle \chi, \psi \rangle$ of characters is the dimension of the vector space of maps between the corresponding representations, hence is a non-negative integer. Thus if P is an S_d-character then Theorem 2.2.7 implies that

$$E_d(P) = \sum_{k=0}^{d-1} \frac{\langle P, \psi_d^k \rangle}{q^k},$$

has non-negative coefficients.

2. The inner product of class functions is bilinear. Therefore, by Theorem 2.2.12

$$E_d(P)_{q=1} = \sum_{k=0}^{d-1} \langle P, \psi_d^k \rangle = \langle P, \sum_{k=0}^{d-1} \psi_d^k \rangle = \langle P, \chi_{\text{reg}} \rangle.$$

It follows from the general representation theory of finite groups that $\langle P, \chi_{\text{reg}} \rangle = \dim V$. Therefore,

$$E_d(P)_{q=1} = \dim V = P(1^d). \qquad \square$$

Remark 2.2.14. The proofs of both Theorem 2.2.12 and Corollary 2.2.13 make use of evaluations at $q = 1$. Lagarias [55] and Hyde and Lagarias [53] studied properties of the squarefree splitting measure at $q = 1$ viewed as another example of phenomena associated with the non-existent field with one element $\mathbb{F}_1$. In Section 4.6 we show how the $q = 1$ evaluations are naturally associated with properties of the splitting measure over the complex numbers $\mathbb{C}$. From this perspective, Theorem 2.2.12 is equivalent to the fact that the splitting measure over $\mathbb{C}$ is entirely concentrated on the totally reducible polynomials. Similarly, Corollary 2.2.13 says that the expected value of a factorization statistic P on $\text{Poly}_d(\mathbb{C})$ is simply the value of P on the partition (1^d) corresponding to a totally reducible polynomial.

2.3 Examples

Theorems 2.2.7 and 2.2.8 form a bridge connecting polynomial factorization statistics on the one hand and representations of the symmetric group and cohomology of configuration spaces on the other. Translating information back and forth across this bridge leads to an interesting interplay between these structures. In this section we first revisit the example of quadratic excess Q to see how our results explain the properties of $E_d(Q)$ observed in the introduction. We finish with some results on expected values and the structure of $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ using the constraint provided by Theorem 2.2.12.

2.3.1 Quadratic excess

Recall the quadratic excess factorization statistic Q from Example 2.2.6: $Q(f)$ is defined as the difference between the number of reducible versus irreducible quadratic factors of f. Rephrasing this in terms of partitions, if $x_k(\lambda)$ is the number of parts of λ of size k, then

$$Q(\lambda) = \binom{x_1(\lambda)}{2} - \binom{x_2(\lambda)}{1}.$$

Let $\mathbb{Q}[d]$ be the permutation representation of the symmetric group with basis $\{e_1, e_2, \ldots, e_d\}$ and consider the representation given by the second exterior power $\bigwedge^2 \mathbb{Q}[d]$. This representation has dimension $\binom{d}{2}$ with a natural basis given by $\{e_i \wedge e_j : i < j\}$.

If $\sigma \in S_d$ is a permutation, then the trace of σ on $\bigwedge^2 \mathbb{Q}[d]$ is

$$\begin{aligned}
\mathrm{Trace}(\sigma) &= \#\{\{i,j\} : \sigma \text{ fixes } i \text{ and } j\} - \#\{\{i,j\} : \sigma \text{ transposes } i \text{ and } j\} \\
&= \binom{x_1(\sigma)}{2} - \binom{x_2(\sigma)}{1} \\
&= Q(\sigma).
\end{aligned}$$

Thus Q, viewed as a class function of S_d, is the character of $\bigwedge^2 \mathbb{Q}[d]$. It follows from Corollary 2.2.13 that the coefficients of $E_d(Q)$ are non-negative integers summing to $\binom{d}{2} = \dim \bigwedge^2 \mathbb{Q}[d]$. The coefficientwise convergence of $E_d(Q)$ follows from Theorem 2.2.11. The $1/q$-adic limit of $E_d(Q)$ as $d \to \infty$ is a rational function of q, which explains

the simple pattern emerging in the coefficients of $E_d(q)$. In particular, using [16, Cor. 10] we compute,

$$\begin{aligned}\lim_{d\to\infty} E_d(Q) &= \frac{1}{2}\left(1+\frac{1}{q}\right)\left(\frac{1}{1-\frac{1}{q}}\right)^2 - \frac{1}{2}\left(1-\frac{1}{q}\right)\left(\frac{1}{1-\frac{1}{q^2}}\right)\\ &= \tfrac{2}{q} + \tfrac{2}{q^2} + \tfrac{4}{q^3} + \tfrac{4}{q^4} + \tfrac{6}{q^5} + \tfrac{6}{q^6} + \tfrac{8}{q^7} + \tfrac{8}{q^8} + \tfrac{10}{q^9} + \dots.\end{aligned}$$

2.3.2 Identifying irreducible components

Theorem 2.2.12 gives a constraint on the cohomology of $\mathrm{PConf}_d(\mathbb{R}^3)$,

$$\bigoplus_{k=0}^{d-1} H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}) \cong \mathbb{Q}[S_d],$$

where $\mathbb{Q}[S_d]$ is the regular representation of the symmetric group. The regular representation of S_d is well-understood: the irreducible representations of S_d are indexed by partitions $\lambda \vdash d$, each irreducible $\mathcal{S}_\lambda$ is a direct summand of $\mathbb{Q}[S_d]$ with multiplicity $f_\lambda := \dim \mathcal{S}_\lambda$. Thus Theorem 2.2.12 tells us that the irreducible components $\mathcal{S}_\lambda$ of $\mathbb{Q}[S_d]$ are distributed among the various degrees of cohomology on the left hand side of (2.10). Theorem 2.2.7 implies that the filtration of the regular representation given by Theorem 2.2.12 completely determines and is determined by the expected values of factorization statistics on $\mathrm{Poly}_d(\mathbb{F}_q)$. We use Theorem 2.2.12 to identify the degrees of some of the irreducible S_d-representations in the cohomology of $\mathrm{PConf}_d(\mathbb{R}^3)$.

2.3.3 Trivial representation

Let $\mathbf{1} := \mathcal{S}_{[d]}$ be the one-dimensional *trivial representation* of S_d. The character of the trivial representation is constant equal to 1. Interpreting the trivial character as a factorization statistic we have $E_d(1) = 1$ and Theorem 2.2.7 implies

$$1 = E_d(1) = \sum_{k=0}^{d-1} \frac{\langle 1, \psi_d^k \rangle}{q^k}.$$

Comparing coefficients of $1/q^k$ we conclude that $\langle 1, \psi_d^0 \rangle = 1$ and $\langle 1, \psi_d^k \rangle = 0$ for $k > 0$. Hence, $\mathbf{1}$ is a summand of $H^0(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$. On the other hand, $\mathrm{PConf}_d(\mathbb{R}^3)$ is path connected so $H^0(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ is one-dimensional. Thus

$$H^0(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}) \cong \mathbf{1}, \tag{2.11}$$

and $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ has no trivial component for $k > 0$.

Recall that the characters χ_λ of the irreducible representations $\mathcal{S}_\lambda$ of S_d form a $\mathbb{Q}$-basis for the vector space of all class functions. If P is a factorization statistic, then there are $a_\lambda(P) \in \mathbb{Q}$ such that

$$P = \sum_{\lambda \vdash d} a_\lambda(P) \chi_\lambda,$$

where χ_λ is the character of the irreducible representation $\mathcal{S}_\lambda$. In particular if $a_1(P) := a_{[d]}(P)$ is the coefficient of the trivial character in this decomposition, then we have the following corollary.

Corollary 2.3.1. *If P is any factorization statistic and if $a_1(P)$ is the coefficient of the trivial character in the expression of P as a linear combination of irreducible S_d-characters, then*

$$a_1(P) = \lim_{q \to \infty} E_d(P).$$

Hence $a_1(P) = 0$ if and only if the expected value of P approaches 0 for large q.

2.3.4 Sign representation

Let $\mathbf{Sgn}_d := \mathcal{S}_{[1^d]}$ be the one-dimensional *sign representation*. The character of $\mathbf{Sgn}_d$ is $\mathrm{sgn}_d(\lambda) = (-1)^{d-\ell(\lambda)}$, or equivalently $\mathrm{sgn}_d([j]) = (-1)^{j-1}$ for a partition $[j]$ with one part of size j and then sgn_d extends multiplicatively to partitions with more than one part. Viewing sgn_d as a factorization statistic Theorem 2.2.7 implies

$$E_d(\mathrm{sgn}_d) = \sum_{k=0}^{d-1} \frac{\langle \mathrm{sgn}_d, \psi_d^k \rangle}{q^k}.$$

On the other hand, Corollary 2.2.13 tells us that $\langle \mathrm{sgn}_d, \psi_d^k \rangle = 1$ for exactly one k and is 0 otherwise—which value of k is it?

Theorem 2.3.2. *For each $d \geq 1$,*

$$E_d(\mathrm{sgn}_d) = \frac{1}{q^{\lfloor d/2 \rfloor}}.$$

Hence $H^{2\lfloor d/2 \rfloor}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ is the unique cohomological degree with a $\mathbf{Sgn}_d$ summand.

We prove Theorem 2.3.2 in Chapter 3 using *liminal reciprocity* which relates factorization statistics in $\mathrm{Poly}_d(\mathbb{F}_q)$ with the limiting values of *squarefree* factorization statistics for $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ as the number of variables n tends to infinity.

Remark 2.3.3. Recall that the *Liouville function* $\lambda(f)$ is defined to be -1 if f is irreducible and extended multiplicatively. Note that $\lambda(f) = (-1)^d \mathrm{sgn}_d(f)$. Carlitz [13, Sec. 3] computed the expected value of the Liouville function on $\mathrm{Poly}_d(\mathbb{F}_q)$ using zeta functions, and Theorem 2.3.2 may also be deduced from his result. See the announcement [12, Pg. 121] for a clear statement of his result. We thank Ofir Gorodetsky for bringing this work to our attention.

Theorem 2.3.2 has a surprising consequence for the even type factorization statistic. Recall that the *even type* factorization statistic ET is defined by $ET(f) = 1$ when the factorization type of f is an even partition and $ET(f) = 0$ otherwise. Thus the expected value $E_d(ET)$ is the probability of a random polynomial in $\mathrm{Poly}_d(\mathbb{F}_q)$ having even factorization type. One might guess that a polynomial should be just as likely to have an even versus odd factorization type. However, notice that

$$ET = \tfrac{1}{2}(1 + \mathrm{sgn})$$

as class functions of S_d. It follows by the linearity of expectation that

$$E_d(ET) = \tfrac{1}{2}(E_d(1) + E_d(\mathrm{sgn})) = \tfrac{1}{2}\big(1 + \tfrac{1}{q^{\lfloor d/2 \rfloor}}\big).$$

The leading term of this probability is $1/2$ as we expected, but there is a slight bias toward a polynomial having even factorization type. This bias traces back to the sign representation

and the degree of cohomology in which it appears. For comparison we remark that in the squarefree case the probability of a random polynomial in $\mathrm{Poly}_d^{\mathrm{sf}}(\mathbb{F}_q)$ having even factorization type is exactly

$$E_d^{\mathrm{sf}}(ET) = \tfrac{1}{2},$$

matching our original guess.

2.3.5 Standard representation

Let $\mathbb{Q}[d]$ be the permutation representation of S_d. The irreducible decomposition of $\mathbb{Q}[d]$ is

$$\mathbb{Q}[d] \cong \mathbf{1} \oplus \mathbf{Std},$$

where $\mathbf{Std} := \mathcal{S}_{[d-1,1]}$ is the $(d-1)$-dimensional *standard representation* of S_d. Let R be the character of $\mathbb{Q}[d]$. If $\sigma \in S_d$, then $R(\sigma)$ is the number of fixed points of σ acting on the set $\{1, 2, \ldots, d\}$; hence $R(\lambda) = x_1(\lambda)$ is the number of parts of λ of size one. Viewed as a factorization statistic, $R(f)$ counts the number of $\mathbb{F}_q$-roots of f with multiplicity.

Theorem 2.3.4. *Let $R(f)$ be the number of $\mathbb{F}_q$-roots with multiplicity of $f \in \mathrm{Poly}_d(\mathbb{F}_q)$. Then the expected value $E_d(R)$ of R on $\mathrm{Poly}_d(\mathbb{F}_q)$ is*

$$E_d(R) = \frac{1 - \frac{1}{q^d}}{1 - \frac{1}{q}} = 1 + \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^3} + \ldots + \frac{1}{q^{d-1}}. \tag{2.12}$$

It follows that the multiplicity of **Std** *in $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ is 1 for $0 < k < d$.*

Proof. First note that

$$E_d(R) = \frac{1}{q^d} \sum_{f \in \mathrm{Poly}_d(\mathbb{F}_q)} R(f) = \sum_{\lambda \vdash d} x_1(\lambda)\nu(\lambda),$$

where ν is the splitting measure. In the course of proving Theorem 2.2.2 we derived the

following formal power series identity,

$$\sum_{d\geq 0}\sum_{\lambda\vdash d} \nu(\lambda)p_\lambda = \prod_{j\geq 1}\left(\frac{1}{1-p_j/q^j}\right)^{M_j(q)}. \tag{2.13}$$

Consider the effect of the operator $p_1\frac{\partial}{\partial p_1}$ on (2.13). On the left hand side we get

$$p_1\frac{\partial}{\partial p_1}\sum_{d\geq 0}\sum_{\lambda\vdash d}\nu(\lambda)p_\lambda = \sum_{d\geq 1}\sum_{\lambda\vdash d} x_1(\lambda)\nu(\lambda)p_\lambda.$$

On the right hand side we have

$$p_1\frac{\partial}{\partial p_1}\prod_{j\geq 1}\left(\frac{1}{1-p_j/q^j}\right)^{M_j(q)} = \frac{M_1(q)p_1}{q(1-p_1/q)}\prod_{j\geq 1}\left(\frac{1}{1-p_j/q^j}\right)^{M_j(q)}.$$

Now substitute $p_j \mapsto t^j$ for all j to arrive at

$$\sum_{d\geq 1}\sum_{\lambda\vdash d} x_1(\lambda)\nu(\lambda)t^d = \sum_{d\geq 1} E_d(R)t^d,$$

on the left and

$$\begin{aligned}\frac{M_1(q)t}{q(1-t/q)}\prod_{j\geq 1}\left(\frac{1}{1-t^j/q^j}\right)^{M_j(q)} &= \frac{t}{1-t/q}\prod_{j\geq 1}\left(\frac{1}{1-(t/q)^j}\right)^{M_j(q)}\\ &= \frac{t}{1-t/q}\cdot\frac{1}{1-t}\end{aligned}$$

on the right, where the last equality is a consequence of the *cyclotomic identity* (see Chapter 4 Section 4.4):

$$\frac{1}{1-qt} = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_j(q)}.$$

Therefore,

$$\sum_{d\geq 1} E_d(R)t^d = \frac{t}{1-t/q}\cdot\frac{1}{1-t}. \tag{2.14}$$

Expanding the right hand side of (2.14) gives

$$\frac{t}{1-t/q}\cdot\frac{1}{1-t}=\frac{1}{1-t}\sum_{d\geq 1}\frac{1}{q^{d-1}}t^d=\sum_{d\geq 1}\left(\frac{1-\frac{1}{q^d}}{1-\frac{1}{q}}\right)t^d.$$

Comparing coefficients of t^d we conclude that

$$E_d(R)=\frac{1-\frac{1}{q^d}}{1-\frac{1}{q}}=1+\frac{1}{q}+\frac{1}{q^2}+\frac{1}{q^3}+\ldots+\frac{1}{q^{d-1}}.$$

The assertions about the multiplicity of **Std** in $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3),\mathbb{Q})$ follow from Theorem 2.2.7 and (2.11). □

2.3.6 Acknowledgements

We thank Weiyan Chen, Nir Gadish, Ofir Gorodetsky, Jeff Lagarias, Will Sawin, Phil Tosteson, and Michael Zieve for helpful conversations, references, and feedback on the paper [52].

Chapter 3

Liminal reciprocity and factorization statistics

This chapter is a revised version of the author's paper [51] to appear in the journal *Algebraic Combinatorics*.

3.1 Introduction

Let $\mathbb{F}_q$ be a field with q elements. How many irreducible polynomials of degree d are there in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$? Let $M_{d,n}(q)$ denote the number of irreducible monic[1] polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of total degree d. When $n = 1$, $M_{d,1}(q)$ is given by the *dth necklace polynomial*

$$M_{d,1}(q) := \frac{1}{d} \sum_{e|d} \mu(e) q^{d/e}, \tag{3.1}$$

where μ is the number theoretic Möbius function. When $n > 1$ there does not appear to be a simple formula for $M_{d,n}(q)$ analogous to (3.1). In Lemma 3.2.1 we show that $M_{d,n}(q)$ is a recursively computable polynomial in q for all $n \geq 1$. The table below gives the low degree terms of $M_{3,n}(q)$ for small n.

The table suggests that the sequence of polynomials $M_{3,n}(q)$ converges coefficientwise as the number of variables n increases. We prove this to be the case.

Theorem 3.1.1. *Let $M_{d,n}(q)$ be the number of irreducible degree d monic polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$. Then $M_{d,n}(q)$ is a polynomial in q and for each $d \geq 1$ the sequence of*

[1] By *monic* in a multivariate polynomial ring we mean an $\mathbb{F}_q^\times$-orbit of polynomials under scaling.

n	$M_{3,n}(q)$
1	$-\frac{1}{3}q + \frac{1}{3}q^3$
2	$-\frac{1}{3}q - \frac{1}{3}q^2 + \frac{1}{3}q^3 - q^5 - \frac{2}{3}q^6 + \dots$
3	$-\frac{1}{3}q - \frac{1}{3}q^2 + q^4 + q^5 + \frac{1}{3}q^6 - q^7 + \dots$
4	$-\frac{1}{3}q - \frac{1}{3}q^2 + \frac{2}{3}q^4 + 2q^5 + \frac{7}{3}q^6 + 2q^7 + \dots$
5	$-\frac{1}{3}q - \frac{1}{3}q^2 + \frac{2}{3}q^4 + \frac{5}{3}q^5 + \frac{10}{3}q^6 + 4q^7 + \dots$
6	$-\frac{1}{3}q - \frac{1}{3}q^2 + \frac{2}{3}q^4 + \frac{5}{3}q^5 + 3q^6 + 5q^7 + \dots$
7	$-\frac{1}{3}q - \frac{1}{3}q^2 + \frac{2}{3}q^4 + \frac{5}{3}q^5 + 3q^6 + \frac{14}{3}q^7 + \dots$

Table 3.1: Low degree terms of $M_{3,n}(q)$.

polynomials $M_{d,n}(q)$ converges coefficientwise (that is, with respect to the q-adic topology) in the formal power series ring $\mathbb{Q}[\![q]\!]$ to the rational function

$$M_{d,\infty}(q) := -\frac{1}{d}\sum_{e|d}\mu(e)\left(\frac{1}{1-\frac{1}{q}}\right)^{d/e}.$$

In particular $M_{d,\infty}(q)$ satisfies the functional equation,

$$M_{d,\infty}(q) = -M_{d,1}\left(\tfrac{1}{1-\frac{1}{q}}\right). \tag{3.2}$$

Furthermore the rate of convergence of $M_{d,n}(q)$ is bounded by the congruence

$$M_{d,n}(q) \equiv M_{d,\infty}(q) \bmod q^{n+1}.$$

The fractional linear transformation $q \mapsto \frac{1}{1-\frac{1}{q}}$ is an involution, hence (3.2) is equivalent to

$$M_{d,1}(q) = -M_{d,\infty}\left(\tfrac{1}{1-\frac{1}{q}}\right).$$

This functional equation relating irreducible polynomial counts in one and infinitely many variables is the first instance of a phenomenon we call *liminal reciprocity*.

3.1.1 Liminal reciprocity for type polynomials

Let $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ denote the set of monic polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of total degree d. Since the polynomial ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ has unique factorization, each $f \in \mathrm{Poly}_{d,n}(\mathbb{F}_q)$ has a well-defined *factorization type*. The factorization type of a polynomial $f \in \mathrm{Poly}_{d,n}(\mathbb{F}_q)$ is the partition $\lambda \vdash d$ given by the degrees of the $\mathbb{F}_q$-irreducible factors of f.

Remark 3.1.2. The factorization type of a polynomial does not record the multiplicities of factors, only the degrees of the irreducible factors. For example, the polynomials x^2 and $x(x+1)$ both have factorization type (1^2) since they each have two linear factors.

Definition 3.1.3. If $\lambda \vdash d$ is a partition, then the *λ-type polynomial* $T_{\lambda,n}(q)$ is the number of elements in $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ with factorization type λ. Similarly the *squarefree λ-type polynomial* $T^{\mathrm{sf}}_{\lambda,n}(q)$ is the number of squarefree elements in $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ with factorization type λ. The type polynomials may be expressed in terms of $M_{d,n}(q)$ as

$$T_{\lambda,n}(q) := \prod_{j\geq 1} \left(\!\!\binom{M_{j,n}(q)}{m_j(\lambda)}\!\!\right) \qquad T^{\mathrm{sf}}_{\lambda,n}(q) := \prod_{j\geq 1} \binom{M_{j,n}(q)}{m_j(\lambda)},$$

where $m_j(\lambda)$ is the number of parts of λ of size j, $\binom{x}{m} := \frac{1}{m!}x(x-1)\cdots(x-m+1)$ is the usual binomial coefficient, and $\left(\!\!\binom{x}{m}\!\!\right) := \frac{1}{m!}x(x+1)\cdots(x+m-1)$. Recall that $\binom{x}{m}$ counts the number of subsets of size m in a set of size x and $\left(\!\!\binom{x}{m}\!\!\right)$ counts the number of subsets of size m with repetition in a set of size x.

It follows from Theorem 3.1.1 that the coefficientwise limits

$$T_{\lambda,\infty}(q) := \lim_{n\to\infty} T_{\lambda,n}(q) \qquad T^{\mathrm{sf}}_{\lambda,\infty}(q) := \lim_{n\to\infty} T^{\mathrm{sf}}_{\lambda,n}(q)$$

converge to rational functions. Our next result is a version of liminial reciprocity for type polynomials.

Theorem 3.1.4 (Liminal reciprocity)**.** *Let λ be a partition and let $\ell(\lambda) := \sum_{j\geq 1} m_j(\lambda)$ be*

the number of parts of λ. Then the following identities hold in $\mathbb{Q}(q)$,

$$T_{\lambda,\infty}(q) = (-1)^{\ell(\lambda)} T^{\mathrm{sf}}_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right)$$
$$T^{\mathrm{sf}}_{\lambda,\infty}(q) = (-1)^{\ell(\lambda)} T_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right)$$

These identities are involutive in the sense that we can swap the ∞ and 1 subscripts to get equivalent statements. The new feature appearing in Theorem 3.1.4 is the relationship between squarefree polynomials and general polynomials of a given factorization type. This connection is closely related to Stanley's *combinatorial reciprocity phenomenon* [85] (see Section 3.1.3.)

3.1.2 Liminal first moments of squarefree factorization statistics

A function Q defined on $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ is called a *factorization statistic* if $Q(f)$ depends only on the factorization type of f. In Chapter 2 we expressed the first moments of factorization statistics on the set of univariate polynomials ($n = 1$) in terms of the cohomology of point configurations in $\mathbb{R}^3$ viewed as a representation of the symmetric group. See Section 3.3 for precise definitions. Note that $\mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)$ denotes the subset of squarefree polynomials in $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$.

Theorem 3.1.5 ([52, Thm. 2.2, Thm. 2.3])**.** *Let Q be a factorization statistic, and let ψ_d^k, ϕ_d^k be the characters of the S_d-representations $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ and $H^k(\mathrm{PConf}_d(\mathbb{R}^2), \mathbb{Q})$ respectively. Then*

$$(1) \quad \sum_{f \in \mathrm{Poly}_{d,1}(\mathbb{F}_q)} Q(f) = \sum_{k=0}^{d-1} \langle Q, \psi_d^k \rangle q^{d-k}$$
$$(2) \quad \sum_{f \in \mathrm{Poly}^{\mathrm{sf}}_{d,1}(\mathbb{F}_q)} Q(f) = \sum_{k=0}^{d-1} (-1)^k \langle Q, \phi_d^k \rangle q^{d-k},$$

where $\langle Q, R\rangle = \frac{1}{d!}\sum_{\tau \in S_d} Q(\tau)R(\tau)$ is the standard inner product of class functions on S_d.

The squarefree case (2) of Theorem 3.1.5 is due to Church, Ellenberg, and Farb [20,

Prop. 4.1]. The general polynomial case (1) was shown by the author [52] using different methods which also led to a new proof of the squarefree case. Theorem 3.1.5 provides a bridge between the arithmetic and combinatorics of factorization statistics on one hand and the geometry and representation theory of configuration spaces on the other.

Numerical experiments suggest there are not direct analogs of Theorem 3.1.5 for polynomials in n variables with $n > 1$. However, an analog does emerge in the liminal squarefree case.

Theorem 3.1.6. *Let Q be a factorization statistic, and let σ_d^k be the character of the S_d-representation*

$$\Sigma_d^k := \bigoplus_{j=k}^{d-1} \mathbf{Sgn}_d \otimes H^{2j}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})^{\oplus \binom{j}{k}}. \tag{3.3}$$

For each n, the first moment $\sum_{f \in \mathrm{Poly}_{d,n}^{\mathrm{sf}}(\mathbb{F}_q)} Q(f)$ is a polynomial in q and

$$\lim_{n\to\infty} \sum_{f \in \mathrm{Poly}_{d,n}^{\mathrm{sf}}(\mathbb{F}_q)} Q(f) = \frac{1}{(1-q)^d} \sum_{k=0}^{d-1} (-1)^k \langle Q, \sigma_d^k \rangle q^{d-k},$$

where the limit is taken coefficientwise in $\mathbb{Q}[\![q]\!]$.

Remark 3.1.7. By considering arbitrary factorization statistics Q our results also determine higher moments of Q, as the kth moment of Q is the first moment of Q^k.

Since the limit in Theorem 3.1.6 is taken coefficientwise, the representation theoretic interpretation of first moments manifests for sufficiently large n. For example, let L be the *linear factor* statistic where $L(f)$ is the number of linear factors of f. The following table shows the first moment of L on $\mathrm{Poly}_{3,n}^{\mathrm{sf}}(\mathbb{F}_q)$ scaled by $(1-q)^3$.

From this table and the convergence bound in Theorem 3.1.1 we conclude that

$$\sum_{f \in \mathrm{Poly}_{3,n}^{\mathrm{sf}}(\mathbb{F}_q)} L(f) = \frac{q - 4q^2 + 3q^3 + O(q^{n+1})}{(1-q)^3}.$$

n	$(1-q)^3 \sum_{f \in \mathrm{Poly}_{3,n}^{\mathrm{sf}}(\mathbb{F}_q)} L(f)$
1	$q - 5q^2 + 10q^3 - 10q^4 + 5q^5 - q^6$
2	$q - 4q^2 + 2q^3 + 7q^4 - 6q^5 - 3q^6 + 2q^7 + q^8 + q^9 - q^{10}$
3	$q - 4q^2 + 3q^3 - q^4 + 7q^5 - 6q^6 - 3q^8 + 3q^9 - q^{11} + q^{12} + q^{14} - q^{15}$
4	$q - 4q^2 + 3q^3 - q^5 + 7q^6 - 6q^7 - 3q^{10} + 3q^{11} - q^{16} + q^{17} + q^{20} - q^{21}$
5	$q - 4q^2 + 3q^3 - q^6 + 7q^7 - 6q^8 - 3q^{12} + 3q^{13} - q^{22} + q^{23} + q^{27} - q^{28}$

Table 3.2: First moments of linear factor statistic.

It then follows from Theorem 3.1.6 that

$$\langle L, \sigma_3^2 \rangle = 1 \qquad \langle L, \sigma_3^1 \rangle = 4 \qquad \langle L, \sigma_3^0 \rangle = 3.$$

Note that these inner products are positive integers: this reflects that L, viewed as a class function of the symmetric group, is the character of the standard permutation representation.

Remark 3.1.8. The table above also illustrates a higher stability in the coefficients. For example, the coefficient of q^{n+2} is 7 in the numerator of the first moment of L for all $n \geq 2$. Since these exponents grow with n, these terms vanish in the limit as $n \to \infty$. This phenomenon persists more generally; it could be an interesting direction for future investigation.

Liminal reciprocity gives a new method to compute the expected values of factorization statistics for univariate polynomials. As an example application we compute the expected value of the sign function sgn_d, where $\mathrm{sgn}_d(\lambda) = (-1)^{d-\ell(\lambda)}$.

Proposition 3.1.9. *Let $d \geq 1$.*

1. *The expected value $E_{d,1}(\mathrm{sgn}_d)$ of the sign statistic on the set $\mathrm{Poly}_{d,1}(\mathbb{F}_q)$ is given by*

$$E_{d,1}(\mathrm{sgn}_d) := \frac{1}{P_{d,1}(q)} \sum_{f \in \mathrm{Poly}_{d,1}(\mathbb{F}_q)} \mathrm{sgn}_d(f) = \frac{1}{q^{\lfloor d/2 \rfloor}}.$$

2. *The limiting expected value $E_{d,\infty}^{\mathrm{sf}}(\mathrm{sgn}_d)$ of the sign statistic on the set $\mathrm{Poly}_{d,n}^{\mathrm{sf}}(\mathbb{F}_q)$ as*

$n \to \infty$ is given by

$$E^{\mathrm{sf}}_{d,\infty}(\mathrm{sgn}_d) := \lim_{n\to\infty} \frac{1}{P^{\mathrm{sf}}_{d,n}(q)} \sum_{f \in \mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)} \mathrm{sgn}_d(f) = \left(\frac{1}{1-\frac{1}{q}}\right)^{\lfloor d/2 \rfloor},$$

where the limit is taken $1/q$-adically.

Proposition 3.1.9 (1) is equivalent to a result of Carlitz arrived at by other means. See Remark 2.3.3.

3.1.3 Related work

Carlitz [14, 15] studied the asymptotic behavior of $M_{d,n}(q)$ for $n \geq 1$. In the language of this paper his main result is as follows.

Theorem 3.1.10 ([14, Sec. 3.])**.** *For $d, n \geq 1$, let $m_{d,n} := \deg M_{d,n}(q)$. Then $m_{d,n} = \binom{d+n}{d} - 1$ and the sequence $M_{d,n}(q)/q^{m_{d,n}}$ of polynomials in $1/q$ converges coefficientwise in $\mathbb{Q}[\![\frac{1}{q}]\!]$ to*

$$\lim_{n\to\infty} \frac{M_{d,n}(q)}{q^{m_{d,n}}} = \frac{1}{1-\frac{1}{q}}.$$

This work was subsequently refined and extended in [7, 22, 49, 92, 93]. Our Theorem 3.1.1 may be interpreted as a determination of the q-adic asymptotics of $M_{d,n}(q)$ as $n \to \infty$. In other words Carlitz studied the limiting behavior of the leading terms of $M_{d,n}(q)$ and we study the limiting behavior of the low degree terms. Recently Weiyan Chen [18] showed that the convergence of the high and low degree terms of $M_{d,n}(q)$ reflects stability in the cohomology of $\mathrm{Irr}_{d,n}(\mathbb{C})$, the space of degree d irreducible polynomials in n-variables over $\mathbb{C}$.

The liminal reciprocity identities (Theorem 3.1.1 and Theorem 3.1.4) were discovered empirically. We would be interested to know of a geometric or combinatorial interpretation of these results. The proof of liminal reciprocity for type polynomials (Theorem 3.1.4) passes through a well-known example of Stanley's *combinatorial reciprocity* [85, Ex. 1.1]. Combinatorial reciprocity is a family of dualities between related combinatorial problems which concretely takes the form of functional equations similar to our liminal

reciprocity identities. However, the precise relationship between liminal and combinatorial reciprocity remains unclear. Finding more examples of liminal reciprocity may shed light on this phenomenon.

The relationship between the liminal first moments of squarefree factorization statistics and representations of the symmetric group parallels our results in Chapter 2. Church, Ellenberg, and Farb [20] connect first moments of squarefree factorization statistics for univariate polynomials and the cohomology of point configurations in $\mathbb{R}^2$ with their *twisted Grothendieck-Lefschetz formula* for squarefree polynomials. They deduce the asymptotic stability of first moments (as $d \to \infty$) as a consequence of *representation stability*. We extend this connection to general univariate polynomials in Chapter 2. However, this connection does not extend to liminal first moments; the representations Σ_d^k does not exhibit representation stability.

The results in Chapter 2 are expressed in terms of expected values of factorization statistics. In this chapter we focus on first moments as they lead to a cleaner statement for Theorem 3.1.6. The only difference between expected values and first moments of factorization statistics is whether or not one divides by the "total mass" of the space of polynomials considered. This difference is simply a factor of q^d for general univariate polynomials, but is more subtle for squarefree polynomials and multivariate polynomials as it affects the family of characters given by the coefficients. The equivalence between Theorem 3.1.5 (2) and Theorem 2.1.2 follows from [53, Prop. 4.2]. Alternatively, Theorem 3.1.5 (2) appears as stated in [20, Prop. 4.1].

In Chapter 4 we study the vanishing of the polynomials $M_{d,n}(q)$ at roots of unity and the relation of $M_{d,n}(q)$ to geometry. For a field K let $\mathrm{Irr}_{d,n}(K)$ denote the collection of all K-irreducible monic polynomials of total degree d in $K[x_1, x_2, \ldots, x_n]$. If $K = \mathbb{R}$ or $\mathbb{C}$, then $\mathrm{Irr}_{d,n}(K)$ has a subspace topology from the projective space structure of all non-zero monic polynomials of degree at most d. We show that the values of $M_{d,n}(q)$ at $q = \pm 1$ compute the compactly supported Euler characteristics of these spaces.

Theorem 3.1.11 ([50])**.** *Let $d, n \geq 1$ and let χ_c be the compactly supported Euler characteristic, then*

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases}$$

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1) = \begin{cases} a_k & \text{if } d = 2^k \\ 0 & \text{otherwise.} \end{cases}$$

where $n = \sum_{k\geq 0} a_k 2^k$ is the unique expression of n as an alternating sum of an even number of powers of 2.

3.1.4 Acknowledgements

The author thanks Weiyan Chen, Nir Gadish, Ofir Gorodetsky, Jeff Lagarias, Bob Lutz, John Stembridge, Phil Tosteson, Michael Zieve, and the referee for helpful conversations and suggestions on [51].

3.2 Polynomial factorization statistics

Let $\mathbb{F}_q$ be a finite field. Recall that we define a *monic* polynomial in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ as an $\mathbb{F}_q^\times$-orbit of polynomials under scaling. Let $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ be the set of all total degree d monic polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$. For each $m \geq 1$ let $\mathrm{Poly}^m_{d,n}(\mathbb{F}_q) \subseteq \mathrm{Poly}_{d,n}(\mathbb{F}_q)$ be the subset of those polynomials with all factors of multiplicity at most m. There is a filtration

$$\mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q) := \mathrm{Poly}^1_{d,n}(\mathbb{F}_q) \subseteq \mathrm{Poly}^2_{d,n}(\mathbb{F}_q) \subseteq \mathrm{Poly}^3_{d,n}(\mathbb{F}_q) \subseteq \ldots \subseteq \mathrm{Poly}_{d,n}(\mathbb{F}_q),$$

where $\mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)$ is the set of the squarefree polynomials.

Recall that $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ every element of $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ has a unique factorization as a product of irreducible monic polynomials. The *factorization type* of $f \in \mathrm{Poly}_{d,n}(\mathbb{F}_q)$ is the partition of d given by the degrees of the $\mathbb{F}_q$-irreducible factors of f. If λ is a partition of d, then let $\mathrm{Poly}_{\lambda,n}(\mathbb{F}_q)$ denote the set of all $f \in \mathrm{Poly}_{d,n}(\mathbb{F}_q)$ with factorization type λ. For $m \geq 1$, let $\mathrm{Poly}^m_{\lambda,n}(\mathbb{F}_q) := \mathrm{Poly}^m_{d,n}(\mathbb{F}_q) \cap \mathrm{Poly}_{\lambda,n}(\mathbb{F}_q)$. If $\lambda = (d)$ is the partition with one part, let $\mathrm{Irr}_{d,n}(\mathbb{F}_q) := \mathrm{Poly}_{(d),n}(\mathbb{F}_q)$ be the set of monic, irreducible, total degree d polynomials.

Lemma 3.2.1 shows that the cardinality of each of the sets just defined is given by a polynomial in the size of the field q.

Lemma 3.2.1. *For any $d, n \geq 1$,*

1. $|\mathrm{Poly}_{d,n}(\mathbb{F}_q)| = P_{d,n}(q)$*, where*

$$P_{d,n}(q) := \frac{q^{\binom{d+n}{n}} - q^{\binom{d+n-1}{n}}}{q-1} = q^{\binom{d+n-1}{n}} \frac{q^{\binom{d+n-1}{n-1}} - 1}{q-1}.$$

2. $M_{d,n}(q) := |\mathrm{Irr}_{d,n}(\mathbb{F}_q)|$ *is a polynomial in q with rational coefficients.*
3. *For every partition $\lambda \vdash d$,*

$$|\mathrm{Poly}_{\lambda,n}(\mathbb{F}_q)| = T_{\lambda,n}(q) := \prod_{j \geq 1} \left(\!\!\binom{M_{j,n}(q)}{m_j(\lambda)}\!\!\right),$$
$$|\mathrm{Poly}^{\mathrm{sf}}_{\lambda,n}(\mathbb{F}_q)| = T^{\mathrm{sf}}_{\lambda,n}(q) := \prod_{j \geq 1} \binom{M_{j,n}(q)}{m_j(\lambda)}.$$

where $\left(\!\!\binom{x}{m}\!\!\right) := \binom{x+m-1}{m}$ is the number of subsets with repetition of size m chosen from an x element set.

Proof. (1) There are $q^{\binom{d+n}{n}}$ polynomials in n variables of degree at most d. Hence there are $q^{\binom{d+n}{n}} - q^{\binom{d+n-1}{n}}$ polynomials in n variables of degree exactly d. Taking orbits under scaling, the total number of degree d monic polynomials in n variables is

$$|\mathrm{Poly}_{d,n}(\mathbb{F}_q)| = \frac{q^{\binom{d+n}{n}} - q^{\binom{d+n-1}{n}}}{q-1}.$$

(2) We proceed by induction on d to show that $M_{d,n}(q)$ is a polynomial in q. If $d = 1$, then all polynomials are irreducible, hence

$$M_{1,n}(q) = |\mathrm{Irr}_{1,n}(\mathbb{F}_q)| = |\mathrm{Poly}_{1,n}(\mathbb{F}_q)| = \frac{q^{n+1} - q}{q-1}.$$

Suppose our claim were true for all degrees less than $d > 1$. By unique factorization, the

total number of polynomials with factorization type λ is

$$T_{\lambda,n}(q) := |\mathrm{Poly}_{\lambda,n}(\mathbb{F}_q)| = \prod_{j\geq 1} \left(\!\!\binom{M_{j,n}(q)}{m_j(\lambda)}\!\!\right). \tag{3.4}$$

Counting elements on both sides of the decomposition

$$\mathrm{Poly}_{d,n}(\mathbb{F}_q) = \bigsqcup_{\lambda\vdash d} \mathrm{Poly}_{\lambda,n}(\mathbb{F}_q),$$

gives

$$P_{d,n}(q) = M_{d,n}(q) + \sum_{\substack{\lambda\vdash d \\ \lambda\neq(d)}} T_{\lambda,n}(q).$$

If $\lambda \neq (d)$, then all parts j of λ are smaller than d, which by our inductive hypothesis implies that $M_{j,n}(q)$ is a polynomial for all such j, hence so is $T_{\lambda,n}(q)$. Thus

$$M_{d,n}(q) = P_{d,n}(q) - \sum_{\substack{\lambda\vdash d \\ \lambda\neq(d)}} T_{\lambda,n}(q) \in \mathbb{Q}[q].$$

Finally, (3) follows from equation (3.4) and (2). □

The definitions of the polynomials appearing in Lemma 3.2.1 are collected here for convenience.

Definition 3.2.2. Let $d, n \geq 1$ and $\lambda \vdash d$, then

$$\begin{aligned}
P_{d,n}(q) &:= \frac{q^{\binom{d+n}{n}} - q^{\binom{d+n-1}{n}}}{q-1} = q^{\binom{d+n-1}{n}} \frac{q^{\binom{d+n-1}{n-1}} - 1}{q-1} \\
M_{d,n}(q) &:= |\mathrm{Irr}_{d,n}(\mathbb{F}_q)| = |\mathrm{Poly}_{(d),n}(\mathbb{F}_q)| \\
T_{\lambda,n}(q) &:= |\mathrm{Poly}_{\lambda,n}(\mathbb{F}_q)| = \prod_{j \geq 1} \left(\!\!\binom{M_{j,n}(q)}{m_j(\lambda)}\!\!\right) \\
T^m_{\lambda,n}(q) &:= |\mathrm{Poly}^m_{\lambda,n}(\mathbb{F}_q)| \\
T^{\mathrm{sf}}_{\lambda,n}(q) = T^1_{\lambda,n}(q) &:= |\mathrm{Poly}^{\mathrm{sf}}_{\lambda,n}(\mathbb{F}_q)| = \prod_{j \geq 1} \binom{M_{j,n}(q)}{m_j(\lambda)} \\
P^m_{d,n}(q) &:= |\mathrm{Poly}^m_{d,n}(\mathbb{F}_q)| = \sum_{\lambda \vdash d} T^m_{\lambda,n}(q),
\end{aligned}$$

where d represents **d**egree, n the **n**umber of variables, and m the maximum **m**ultiplicity of a factor.

There is a well-known formula going back to Gauss and Schönemann for $M_{d,1}(q)$ given by counting elements in $\mathbb{F}_{q^d}$ by the field they generate (see, for example, [78, Cor. 2.1],)

$$M_{d,1}(q) = \frac{1}{d} \sum_{e|d} \mu(e) q^{d/e}. \tag{3.5}$$

The value of $M_{d,1}(k)$ for an integer $k \geq 1$ has a combinatorial interpretation as the number of aperiodic necklaces made with beads of k colors. For this reason, $M_{d,1}(q)$ is known as the dth *necklace polynomial*. There is no apparent analog of (3.5) nor a necklace interpretation for $M_{d,n}(k)$ when $n > 1$. Instead $M_{d,n}(q)$ may be computed recursively as in the proof of Lemma 3.2.1:

$$\begin{aligned}
M_{1,n}(q) &= P_{1,n}(q) = \frac{q^{n+1} - q}{q-1} \\
M_{d,n}(q) &= P_{d,n}(q) - \sum_{\substack{\lambda \vdash d \\ \lambda \neq [d]}} T_{\lambda,n}(q).
\end{aligned}$$

Our next result shows that all the polynomials listed in Definition 3.2.2 converge coefficientwise to rational functions in the ring of formal power series $\mathbb{Q}[\![q]\!]$ as the number of variables n tends to infinity. Recall that coefficientwise convergence in $\mathbb{Q}[\![q]\!]$ is equivalent to convergence with respect to the q-adic topology. All coefficientwise limits are taken with respect to the q-adic topology.

Theorem 3.2.3. *Let $d \geq 1$. Then,*

1. *The sequence $P_{d,n}(q)$ converges coefficientwise in $\mathbb{Q}[\![q]\!]$ to*

$$P_{d,\infty}(q) = \lim_{n\to\infty} P_{d,n}(q) = \begin{cases} -\frac{1}{1-\frac{1}{q}} & d = 1 \\ 0 & d > 1. \end{cases}$$

2. *For $m \geq 1$ the sequence $P^m_{d,n}(q)$ converges coefficientwise in $\mathbb{Q}[\![q]\!]$ to*

$$P^m_{d,\infty}(q) = \lim_{n\to\infty} P^m_{d,n}(q) = \begin{cases} -\left(\frac{1}{1-\frac{1}{q}}\right)^k & d = (m+1)k - m \\ \left(\frac{1}{1-\frac{1}{q}}\right)^k & d = (m+1)k \\ 0 & d \not\equiv 0, 1 \bmod m+1. \end{cases}$$

   In particular, if $m = 1$, then

$$P^{\mathrm{sf}}_{d,\infty}(q) = (-1)^d \left(\frac{1}{1-\frac{1}{q}}\right)^{\lfloor \frac{d+1}{2} \rfloor}.$$

3. *For all partitions $\lambda \vdash d$ and $m \geq 1$ the sequences $M_{d,n}(q)$, $T_{\lambda,n}(q)$, and $T^m_{\lambda,n}(q)$ converge coefficientwise in $\mathbb{Q}[\![q]\!]$ to rational functions as $n \to \infty$. Furthermore,*

$$T_{\lambda,\infty}(q) = \prod_{j\geq 1} \left(\!\!\binom{M_{j,\infty}(q)}{m_j(\lambda)}\!\!\right)$$
$$T^{\mathrm{sf}}_{\lambda,\infty}(q) = \prod_{j\geq 1} \binom{M_{j,\infty}(q)}{m_j(\lambda)}.$$

Proof. 1. By Lemma 3.2.1

$$P_{d,n}(q) = q^{\binom{d+n-1}{n}} \frac{q^{\binom{d+n-1}{n-1}} - 1}{q-1}.$$

For $d = 1$ this simplifies to

$$P_{1,n}(q) = \frac{q^{n+1} - q}{q-1}.$$

Since $\lim_{n\to\infty} q^n = 0$ in $\mathbb{Q}[\![q]\!]$, it follows that

$$P_{1,\infty}(q) = \lim_{n\to\infty} \frac{q^{n+1} - q}{q-1} = -\frac{q}{q-1} = -\frac{1}{1-\frac{1}{q}}.$$

If $d > 1$, then $\lim_{n\to\infty} \binom{d+n-1}{n} = \infty$. Thus

$$P_{d,\infty}(q) = \lim_{n\to\infty} q^{\binom{d+n-1}{n}} \frac{q^{\binom{d+n-1}{n-1}} - 1}{q-1} = 0.$$

2. Consider the generating functions

$$Z(T_n^m, t) := \sum_{d\geq 0} P_{d,n}^m(q) t^d = \sum_{d\geq 0} \sum_{\lambda\vdash d} T_{\lambda,n}^m(q) t^d,$$
$$Z(T_n, t) := \sum_{d\geq 0} P_{d,n}(q) t^d = \sum_{d\geq 0} \sum_{\lambda\vdash d} T_{\lambda,n}(q) t^d.$$

The binomial theorem allows us to formally exponentiate $1 + t$ or $\frac{1}{1-t}$ by any element $\alpha \in R$ of a binomial ring[2] in $R[\![t]\!]$ by

$$(1+t)^\alpha := \sum_{d\geq 0} \binom{\alpha}{d} t^d,$$
$$\left(\frac{1}{1-t}\right)^\alpha := \sum_{d\geq 0} \left(\!\!\binom{\alpha}{d}\!\!\right) t^d.$$

[2]A *binomial ring* R is a commutative ring with no additive torsion which is closed under taking binomial coefficients (see [25].)

The following product formulas follow by unique factorization in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$,

$$Z(T_n^m, t) = \prod_{j\geq 1}(1 + t^j + t^{2j} + \ldots + t^{mj})^{M_{j,n}(q)} = \prod_{j\geq 1}\left(\frac{1-t^{(m+1)j}}{1-t^j}\right)^{M_{j,n}(q)}$$
$$Z(T_n, t) = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_{j,n}(q)}.$$

Hence $Z(T_n, t) = Z(T_n, t^{m+1})Z(T_n^m, t)$. The coefficients of t^d for $d \geq 0$ in this identity are polynomials which converge q-adically in $\mathbb{Q}[\![q]\!]$ as $n \to \infty$. Taking a limit t-coefficientwise as $n \to \infty$, (1) implies that

$$1 - \tfrac{1}{1-\frac{1}{q}}t = Z(T_\infty, t) = Z(T_\infty, t^{m+1})Z(T_\infty^m, t) = \left(1 - \tfrac{1}{1-\frac{1}{q}}t^{m+1}\right)\sum_{d\geq 0} P_{d,\infty}^m(q)t^d.$$

Comparing coefficients we conclude that

$$P_{d+m+1,\infty}^m(q) = \frac{1}{1-\frac{1}{q}}P_{d,\infty}^m(q)$$

for all $d \geq 0$, together with the initial values

$$P_{0,\infty}^m(q) = 1$$
$$P_{1,\infty}^m(q) = -\frac{1}{1-\frac{1}{q}}$$
$$P_{d,\infty}^m(q) = 0 \text{ for } 1 < d \leq m.$$

Therefore (2) follows by induction.

3. It suffices to prove that for every $d \geq 1$ the sequence $M_{d,n}(q)$ converges q-adically to a rational function, the other claims follow by the explicit formulas given in Definition 3.2.2 and continuity. Recall the recursive formulas for $M_{d,n}(q)$ used in the proof of Lemma 3.2.1.

For all $d, n \geq 1$,

$$\begin{aligned} M_{1,n}(q) &= P_{1,n}(q) \\ M_{d,n}(q) &= P_{d,n}(q) - \sum_{\substack{\lambda \vdash d \\ \lambda \neq [d]}} \prod_{j \geq 1} \left(\!\!\binom{M_{j,n}(q)}{m_j(\lambda)}\!\!\right). \end{aligned}$$

Taking coefficientwise limits as $n \to \infty$ using (1) we have

$$\begin{aligned} M_{1,\infty}(q) &= P_{1,\infty}(q) = -\frac{1}{1-\frac{1}{q}}, \\ M_{d,\infty}(q) &= -\sum_{\substack{\lambda \vdash d \\ \lambda \neq [d]}} \prod_{j \geq 1} \left(\!\!\binom{M_{j,\infty}(q)}{m_j(\lambda)}\!\!\right). \end{aligned}$$

It follows by induction that $M_{d,\infty}(q)$ is a rational function of q for all $d \geq 1$. □

There is a surprising relationship between the number of irreducible polynomials in one variable $M_{d,1}(q)$ and the limit $M_{d,\infty}(q)$ of the number of irreducible polynomials in n variables as $n \to \infty$, which gives us an explicit formula for $M_{d,\infty}(q)$. This relationship takes the form of an involutive functional equation we call *liminal reciprocity*.

Theorem 3.2.4 (Liminal reciprocity)**.** *For all $d \geq 1$,*

$$M_{d,\infty}(q) = -M_{d,1}\left(\tfrac{1}{1-\frac{1}{q}}\right).$$

More explicitly,

$$M_{d,\infty}(q) = -\frac{1}{d}\sum_{e|d} \mu(e)\left(\frac{1}{1-\frac{1}{q}}\right)^{d/e}.$$

We make use of the following well-known lemma. See Theorem 4.4.2 in Chapter 4 for a proof and more discussion.

Lemma 3.2.5. *For any binomial ring R and any sequence $a_d \in R$ for $d \geq 0$ such that $a_0 = 1$ there exists a unique sequence $b_j \in R$ for $j \geq 1$ such that the following identity*

holds in $R[\![t]\!]$.

$$\sum_{d\geq 0} a_d t^d = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right)^{b_j}.$$

Proof of Thm. 3.2.4. Recall the generating function $Z(T_n, t)$ used in the proof of Theorem 3.2.3 (2),

$$Z(T_n, t) = \sum_{d\geq 0} P_{d,n}(q) t^d = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right)^{M_{j,n}(q)}.$$

Theorem 3.2.3 (1) implies that the t-coefficientwise limit as $n \longrightarrow \infty$ is simply

$$1 - \tfrac{1}{1-\frac{1}{q}} t = \prod_{d\geq 1} \left(\frac{1}{1-t^d}\right)^{M_{d,\infty}(q)}. \tag{3.6}$$

When $n = 1$, $P_{d,1}(q) = q^d$ and thus

$$\frac{1}{1-qt} = Z(T_1, t) = \prod_{d\geq 1} \left(\frac{1}{1-t^d}\right)^{M_{d,1}(q)}. \tag{3.7}$$

Substituting $q \mapsto \frac{1}{1-\frac{1}{q}}$ and taking reciprocals in (3.7) gives

$$1 - \tfrac{1}{1-\frac{1}{q}} t = \prod_{d\geq 1} \left(\frac{1}{1-t^d}\right)^{-M_{d,1}\left(\frac{1}{1-\frac{1}{q}}\right)}.$$

Comparing exponents with (3.6) and using the uniqueness of Lemma 3.2.5 we conclude that

$$M_{d,\infty}(q) = -M_{d,1}\left(\tfrac{1}{1-\frac{1}{q}}\right). \qquad \square$$

Remark 3.2.6. The identity (3.7) is known as the *cyclotomic identity* [63]. It also arises as the Euler product formula for the Hasse-Weil zeta function of $\mathbb{A}^1(\mathbb{F}_q)$ (see Chapter 4 Section 4.4.)

The rate of q-adic convergence of $M_{d,n}(q)$ may be determined from the proof of Theorem 3.2.4.

Corollary 3.2.7. *For all $d, n \geq 1$,*

$$M_{d,n}(q) \equiv M_{d,\infty}(q) \bmod q^{n+1}.$$

Proof. Recall that

$$P_{d,n}(q) = q^{\binom{d+n-1}{n}} \frac{q^{\binom{d+n-1}{n-1}} - 1}{q-1}.$$

Since $\binom{d+n-1}{n} \geq n+1$ for $d \geq 2$ and

$$P_{1,n}(q) = \frac{q^{n+1} - q}{q-1} \equiv -\frac{1}{1-\frac{1}{q}} \bmod q^{n+1},$$

it follows that

$$\sum_{d \geq 0} P_{d,n}(q) t^d \equiv 1 - \tfrac{1}{1-\frac{1}{q}} t \bmod q^{n+1}.$$

Thus

$$\begin{aligned} \prod_{d \geq 1} \left(\frac{1}{1-t^d} \right)^{M_{d,n}(q)} &= \sum_{d \geq 0} P_{d,n}(q) t^d \\ &\equiv 1 - \tfrac{1}{1-\frac{1}{q}} t \bmod q^{n+1} \\ &\equiv \prod_{d \geq 1} \left(\frac{1}{1-t^d} \right)^{M_{d,\infty}(q)} \bmod q^{n+1}. \end{aligned}$$

Therefore by Lemma 3.2.5,

$$M_{d,n}(q) \equiv M_{d,\infty}(q) \bmod q^{n+1}. \qquad \square$$

Remark 3.2.8. Notice that the fractional linear transformation $q \longmapsto \frac{1}{1-\frac{1}{q}}$ is an involution. Thus Theorem 3.2.4 is equivalent to

$$M_{d,1}(q) = -M_{d,\infty}\left(\tfrac{1}{1-\frac{1}{q}} \right).$$

This is the sense in which we consider Theorem 3.2.4 a "reciprocity."

Our next result combines Theorem 3.2.4 with the *combinatorial reciprocity* identity

$$\binom{-x}{m} = (-1)^m \left\langle\!\!\binom{x}{m}\!\!\right\rangle, \tag{3.8}$$

to deduce a striking relationship between factorization statistics of polynomials when $n = 1$ and $n = \infty$.

Theorem 3.2.9 (Liminal reciprocity)**.** *For any partition λ, let $\ell(\lambda) = \sum_{j\geq 1} m_j(\lambda)$ denote the number of parts of λ. Then*

$$T^{\mathrm{sf}}_{\lambda,\infty}(q) = (-1)^{\ell(\lambda)} T_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right),$$
$$T_{\lambda,\infty}(q) = (-1)^{\ell(\lambda)} T^{\mathrm{sf}}_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right).$$

Proof. Theorem 3.2.3 (3), Theorem 3.2.4, and the combinatorial reciprocity identity (3.8) imply that

$$\begin{aligned} T^{\mathrm{sf}}_{\lambda,\infty}(q) &= \prod_{j\geq 1} \binom{M_{j,\infty}(q)}{m_j(\lambda)} \\ &= \prod_{j\geq 1} \binom{-M_{j,1}\left(\frac{1}{1-\frac{1}{q}}\right)}{m_j(\lambda)} \\ &= \prod_{j\geq 1} (-1)^{m_j(\lambda)} \left\langle\!\!\binom{M_{j,1}\left(\frac{1}{1-\frac{1}{q}}\right)}{m_j(\lambda)}\!\!\right\rangle \\ &= (-1)^{\ell(\lambda)} T_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right). \end{aligned}$$

The second identity follows from a parallel computation noting that (3.8) is equivalent to

$$\left\langle\!\!\binom{-x}{m}\!\!\right\rangle = (-1)^m \binom{x}{m}. \qquad \square$$

The liminal reciprocity identity

$$T^{\mathrm{sf}}_{\lambda,\infty}(q) = (-1)^{\ell(\lambda)} T_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right)$$

relates the limiting number of squarefree polynomials with factorization type λ in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ as $n \to \infty$ to the number of polynomials $\mathbb{F}_q[x]$ with factorization type λ with no restrictions on factor multiplicity. This relationship is, to us, mysterious. It would be interesting to find a conceptual explanation for this relationship between infinite and one dimensional factorization statistics.

3.3 Liminal first moments of squarefree factorization statistics

A *factorization statistic* is a function Q defined on $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ such that $Q(f)$ only depends on the factorization type of $f \in \mathrm{Poly}_{d,n}(\mathbb{F}_q)$. Equivalently, Q is a function defined on the partitions of the degree d, or a class function of the symmetric group S_d. In Chapter 2 we determined explicit formulas for the first moments of factorization statistics on $\mathrm{Poly}_{d,1}(\mathbb{F}_q)$ and $\mathrm{Poly}^{\mathrm{sf}}_{d,1}(\mathbb{F}_q)$ in terms of the characters of symmetric group representations carried by the cohomology of point configurations in $\mathbb{R}^3$.

If X is a topological space, then *ordered configuration space of d points in X* is defined as

$$\mathrm{PConf}_d(X) := \{(a_1, a_2, \ldots, a_d) \in X^d : a_i \neq a_j\}.$$

The symmetric group S_d acts on $\mathrm{PConf}_d(X)$ by permuting the labels of points, and thus the singular cohomology $H^k(\mathrm{PConf}_d(X), \mathbb{Q})$ is a linear representation of S_d for each cohomological degree k.

Theorem 3.3.1 combines Theorem 2.2.7 with liminal reciprocity to express the limiting first moments of squarefree factorization statistics in terms of characters of symmetric group representations.

Theorem 3.3.1. *Let Q be a factorization statistic, and let σ_d^k be the character of the S_d-representation*

$$\Sigma_d^k = \bigoplus_{j=k}^{d-1} \mathbf{Sgn}_d \otimes H^{2j}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})^{\oplus \binom{j}{k}}. \tag{3.9}$$

Then

$$\lim_{n\to\infty} \sum_{f\in \mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)} Q(f) = \frac{1}{(1-q)^d} \sum_{k=0}^{d} (-1)^k \langle Q, \sigma_d^k \rangle q^{d-k}.$$

Theorem 3.3.1 follows from the following representation theoretic interpretation of the liminal squarefree type polynomials $T^{\mathrm{sf}}_{\lambda,\infty}(q)$. Recall that for a partition λ the liminal squarefree type polynomial $T^{\mathrm{sf}}_{\lambda,\infty}(q)$ is defined by

$$T^{\mathrm{sf}}_{\lambda,\infty}(q) := \lim_{n\to\infty} T^{\mathrm{sf}}_{\lambda,n}(q),$$

where $T^{\mathrm{sf}}_{\lambda,n}(q)$ is the number of monic squarefree polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ with factorization type λ.

Theorem 3.3.2. *Let $\lambda \vdash d$ be a partition, and let σ_d^k be the character of the S_d-representation Σ_d^k defined in* (3.9)*. Then*

$$T^{\mathrm{sf}}_{\lambda,\infty}(q) = \frac{1}{z_\lambda (1-q)^d} \sum_{k=0}^{d-1} (-1)^k \sigma_d^k(\lambda) q^{d-k},$$

where $z_\lambda := \prod_{j\geq 1} j^{m_j(\lambda)} m_j(\lambda)!$ is the number of permutations in S_d commuting with a permutation of cycle type λ.

Proof. Let ψ_d^k be the character of the S_d-representation $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$. In Theorem 2.1.6 we showed that for all partitions $\lambda \vdash d$,

$$T_{\lambda,1}(q) = \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \psi_d^k(\lambda) q^{d-k}.$$

Thus, Theorem 3.2.9 gives

$$\begin{aligned}
T^{\mathrm{sf}}_{\lambda,\infty}(q) &= (-1)^{\ell(\lambda)} T_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right) \\
&= \frac{1}{z_\lambda} \sum_{j=0}^{d-1} (-1)^{\ell(\lambda)} \psi^j_d(\lambda) \left(\frac{1}{1-\frac{1}{q}}\right)^{d-j} \\
&= \frac{1}{z_\lambda (1-q)^d} \sum_{j=0}^{d-1} (-1)^{d-\ell(\lambda)} \psi^j_d(\lambda) q^{d-j} (q-1)^j \\
&= \frac{1}{z_\lambda (1-q)^d} \sum_{j=0}^{d-1} \mathrm{sgn}_d(\lambda) \psi^j_d(\lambda) q^{d-j} \sum_{k=0}^{j} (-1)^k \binom{j}{k} q^{j-k} \\
&= \frac{1}{z_\lambda (1-q)^d} \sum_{k=0}^{d-1} (-1)^k \left(\sum_{j=k}^{d} \binom{j}{k} \mathrm{sgn}_d(\lambda) \psi^j_d(\lambda) \right) q^{d-k} \\
&= \frac{1}{z_\lambda (1-q)^d} \sum_{k=0}^{d-1} (-1)^k \sigma^k_d(\lambda) q^{d-k}. \qquad \square
\end{aligned}$$

We now prove Theorem 3.3.2.

Proof. Since Q depends only on factorization type, the limiting first moment of Q may be rewritten as

$$\lim_{n\to\infty} \sum_{f \in \mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)} Q(f) = \lim_{n\to\infty} \sum_{\lambda \vdash d} Q(\lambda) T^{\mathrm{sf}}_{\lambda,n}(q) = \sum_{\lambda \vdash d} Q(\lambda) T^{\mathrm{sf}}_{\lambda,\infty}(q).$$

Then Theorem 3.3.2 implies

$$\begin{aligned}
\sum_{\lambda \vdash d} Q(\lambda) T^{\mathrm{sf}}_{\lambda,\infty}(q) &= \sum_{\lambda \vdash d} \frac{1}{z_\lambda (1-q)^d} \sum_{k=0}^{d-1} (-1)^k Q(\lambda) \sigma^k_d(\lambda) q^{d-k} \\
&= \frac{1}{(1-q)^d} \sum_{k=0}^{d-1} (-1)^k \sum_{\lambda \vdash d} \frac{Q(\lambda) \sigma^k_d(\lambda)}{z_\lambda} q^{d-k} \\
&= \frac{1}{(1-q)^d} \sum_{k=0}^{d-1} (-1)^k \langle Q, \sigma^k_d \rangle q^{d-k}. \qquad \square
\end{aligned}$$

The coefficients of $T^{\mathrm{sf}}_{\lambda,1}(q)$ also have representation theoretic interpretations, which suggests that we might hope for a version of Theorem 3.3.2 for the limiting first moments of factorization statistics on $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$. However, computations show that the coefficients of $T_{\lambda,\infty}(q)$ are determined by virtual characters, unlike those of $T^{\mathrm{sf}}_{\lambda,\infty}(q)$.

In Chapter 2 we pose the question of finding a geometric interpretation of Theorem 2.2.7 which explains the connection between the configuration space $\mathrm{PConf}_d(\mathbb{R}^3)$ and factorization statistics of degree d polynomials over $\mathbb{F}_q$. Furthermore, we would like a conceptual interpretation of Theorem 3.3.2, be it geometric or combinatorial. The family of representations Σ^k_d is unfamiliar to us; we collect some of their basic properties in Proposition 3.3.4.

3.3.1 Example

We demonstrate the liminal reciprocity identity of Theorem 3.2.9 by computing the expected value of the sign statistic sgn_d on degree d univariate polynomials $\mathrm{Poly}_{d,1}(\mathbb{F}_q)$ and the limiting expected value of sgn_d on squarefree degree d polynomials $\mathrm{Poly}^{\mathrm{sf}}_{d,\infty}(\mathbb{F}_q)$.

Let sgn_d be the sign character of S_d. Note that $\mathrm{sgn}_d(\lambda) = (-1)^d(-1)^{\ell(\lambda)}$, where $\ell(\lambda) = \sum_{j\geq 1} m_j(\lambda)$ is the number of parts of λ. Recall that $P_{d,n}(q) = |\mathrm{Poly}_{d,n}(\mathbb{F}_q)|$ and $P^{\mathrm{sf}}_{d,n}(q) = |\mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)|$.

Proposition 3.3.3. *Let $d \geq 1$.*

1. *The expected value $E_{d,1}(\mathrm{sgn}_d)$ of the sign statistic on the set $\mathrm{Poly}_{d,1}(\mathbb{F}_q)$ is given by*

$$E_{d,1}(\mathrm{sgn}_d) := \frac{1}{P_{d,1}(q)} \sum_{f\in \mathrm{Poly}_{d,1}(\mathbb{F}_q)} \mathrm{sgn}_d(f) = \frac{1}{q^{\lfloor d/2\rfloor}}.$$

2. *The limiting expected value $E^{\mathrm{sf}}_{d,\infty}(\mathrm{sgn}_d)$ of the sign statistic on the set $\mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)$ as $n \to \infty$ is given by*

$$E^{\mathrm{sf}}_{d,\infty}(\mathrm{sgn}_d) := \lim_{n\to\infty} \frac{1}{P^{\mathrm{sf}}_{d,n}(q)} \sum_{f\in \mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)} \mathrm{sgn}_d(f) = \left(\frac{1}{1-\frac{1}{q}}\right)^{\lfloor d/2\rfloor},$$

where the limit is taken q-adically.

Proof. 1. Since $\mathrm{sgn}_d(f)$ depends only on the factorization type of f we have

$$\sum_{f\in \mathrm{Poly}_{d,1}(\mathbb{F}_q)} \mathrm{sgn}_d(f) = \sum_{\lambda\vdash d} \mathrm{sgn}(\lambda) T_{\lambda,1}(q).$$

Theorem 3.2.9 gives the identity

$$(-1)^{\ell(\lambda)} T_{\lambda,1}(q) = T^{\mathrm{sf}}_{\lambda,\infty}\Big(\tfrac{1}{1-\frac{1}{q}}\Big),$$

from which we deduce for each $d \geq 1$

$$\begin{aligned}\sum_{\lambda\vdash d} \mathrm{sgn}(\lambda) T_{\lambda,1}(q) &= \sum_{\lambda\vdash d} (-1)^d (-1)^{\ell(\lambda)} T_{\lambda,1}(q)\\ &= \sum_{\lambda\vdash d} (-1)^d T^{\mathrm{sf}}_{\lambda,\infty}\Big(\tfrac{1}{1-\frac{1}{q}}\Big)\\ &= (-1)^d P^{\mathrm{sf}}_{d,\infty}\Big(\tfrac{1}{1-\frac{1}{q}}\Big).\end{aligned}$$

Theorem 3.2.3 (2) tells us

$$P^{\mathrm{sf}}_{d,\infty}(q) = (-1)^d \Big(\tfrac{1}{1-\frac{1}{q}}\Big)^{\lfloor \frac{d+1}{2}\rfloor}.$$

Thus,

$$\sum_{\lambda\vdash d} \mathrm{sgn}_d(\lambda) T_{\lambda,1}(q) = (-1)^d P^{\mathrm{sf}}_{d,\infty}\Big(\tfrac{1}{1-\frac{1}{q}}\Big) = q^{\lfloor \frac{d+1}{2}\rfloor}.$$

Since $P_{d,1}(q) = q^d$ and $d - \lfloor (d+1)/2\rfloor = \lfloor d/2\rfloor$ it follows that

$$E_{d,1}(\mathrm{sgn}_d) = \frac{1}{P_{d,1}(q)} \sum_{f\in \mathrm{Poly}_{d,1}(\mathbb{F}_q)} \mathrm{sgn}(f) = \frac{1}{q^{\lfloor d/2\rfloor}}.$$

2. For each $n \geq 1$,

$$E^{\mathrm{sf}}_{d,n}(\mathrm{sgn}_d) := \frac{1}{P^{\mathrm{sf}}_{d,n}(q)} \sum_{f\in \mathrm{Poly}^{\mathrm{sf}}_{d,n}(\mathbb{F}_q)} \mathrm{sgn}_d(f) = \frac{1}{P^{\mathrm{sf}}_{d,n}(q)} \sum_{\lambda\vdash d} \mathrm{sgn}(\lambda) T^{\mathrm{sf}}_{\lambda,n}(q).$$

Taking a limit as $n \to \infty$,

$$E^{\mathrm{sf}}_{d,\infty}(\mathrm{sgn}_d) = \frac{1}{P^{\mathrm{sf}}_{d,\infty}(q)} \sum_{\lambda \vdash d} \mathrm{sgn}_d(\lambda) T^{\mathrm{sf}}_{\lambda,\infty}(q).$$

Theorem 3.2.9 gives us

$$(-1)^{\ell(\lambda)} T^{\mathrm{sf}}_{\lambda,\infty}(q) = T_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right).$$

Therefore,

$$\begin{aligned}
\sum_{\lambda \vdash d} \mathrm{sgn}_d(\lambda) T^{\mathrm{sf}}_{\lambda,\infty}(q) &= \sum_{\lambda \vdash d} (-1)^d (-1)^{\ell(\lambda)} T^{\mathrm{sf}}_{\lambda,\infty}(q) \\
&= \sum_{\lambda \vdash d} (-1)^d T_{\lambda,1}\left(\tfrac{1}{1-\frac{1}{q}}\right) \\
&= (-1)^d \left(\tfrac{1}{1-\frac{1}{q}}\right)^d.
\end{aligned}$$

Since $P^{\mathrm{sf}}_{d,\infty}(q) = (-1)^d \left(\frac{1}{1-\frac{1}{q}}\right)^{\lfloor (d+1)/2 \rfloor}$ and $d - \lfloor (d+1)/2 \rfloor = \lfloor d/2 \rfloor$ we conclude that

$$E^{\mathrm{sf}}_{d,\infty}(\mathrm{sgn}_d) = \frac{1}{P^{\mathrm{sf}}_{d,\infty}(q)} \sum_{\lambda \vdash d} \mathrm{sgn}_d(\lambda) T^{\mathrm{sf}}_{\lambda,\infty}(q) = \left(\frac{1}{1-\frac{1}{q}}\right)^{\lfloor d/2 \rfloor}. \qquad \square$$

3.3.2 The S_d-representations Σ^k_d

Theorem 3.3.1 relates the limiting first moments of factorization statistics on squarefree polynomials with a family of symmetric group representations Σ^k_d. Recall that

$$\Sigma^k_d := \bigoplus_{j=k}^{d-1} \mathbf{Sgn}_d \otimes H^{2j}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})^{\oplus \binom{j}{k}}.$$

We conclude with Proposition 3.3.4 which records some observations about the representations Σ^k_d.

Proposition 3.3.4. *Let σ^k_d be the character of Σ^k_d. Then*

1. *The dimension of* Σ_d^k *is*

$$\dim \Sigma_d^k = \sum_{i=k}^{d-1} \begin{bmatrix} d \\ d-i \end{bmatrix} \binom{i}{i-k},$$

where $\begin{bmatrix} m \\ n \end{bmatrix}$ *is an unsigned Stirling number of the first kind (see below for a definition.)*

2. *The representation*

$$\bigoplus_{k=0}^{d-1} \Sigma_d^k$$

has dimension $(2d-1)!! := (2d-1)(2d-3)\cdots 3 \cdot 1$.

3. Σ_d^0 *is isomorphic to the regular representation* $\mathbb{Q}[S_d]$.

Remark 3.3.5. The sequence $\dim \Sigma_d^k$ appears as A088996 in the *Online Encyclopedia of Integer Sequences* [84].

Proof. 1. The dimension of a representation is given by evaluating its character on the identity, hence

$$\dim \Sigma_d^k = \sigma_d^k(1^d).$$

Theorem 3.3.2 implies that

$$T^{\mathrm{sf}}_{(1^d),\infty}(q) = \frac{1}{d!(1-q)^d} \sum_{k=0}^{d-1} (-1)^k \sigma_d^k(1^d) q^{d-k}.$$

On the other hand, we may compute $T^{\mathrm{sf}}_{(1^d),\infty}(q)$ directly as

$$T^{\mathrm{sf}}_{(1^d),\infty}(q) = \binom{M_{d,\infty}(q)}{d} = \binom{-\frac{1}{1-\frac{1}{q}}}{d}.$$

The *unsigned Stirling numbers of the first kind* are defined as the coefficients in the expansion of a binomial coeffcient $\binom{x}{d}$,

$$\binom{x}{d} = \frac{1}{d!} \sum_{k=0}^{d-1} (-1)^k \begin{bmatrix} d \\ d-k \end{bmatrix} x^{d-k}.$$

Thus,

$$\begin{aligned} T^{\mathrm{sf}}_{(1^d),\infty}(q) &= \frac{1}{d!}\sum_{i=0}^{d-1}(-1)^i \begin{bmatrix} d \\ d-i \end{bmatrix} \left(-\frac{1}{1-\frac{1}{q}}\right)^{d-i} \\ &= \frac{1}{d!(1-q)^d}\sum_{i=0}^{d-1}(-1)^i \begin{bmatrix} d \\ d-i \end{bmatrix} q^{d-i}(1-q)^i \\ &= \frac{1}{d!(1-q)^d}\sum_{i=0}^{d-1}\sum_{j=0}^{i}(-1)^{i+j} \begin{bmatrix} d \\ d-i \end{bmatrix} \binom{i}{j} q^{d-(i-j)}. \end{aligned}$$

Let $k = i - j$ and write the sum in terms of i and k to get

$$T^{\mathrm{sf}}_{(1^d),\infty}(q) = \frac{1}{d!(1-q)^d}\sum_{k=0}^{d-1}(-1)^k \left(\sum_{i=k}^{d-1} \begin{bmatrix} d \\ d-i \end{bmatrix} \binom{i}{i-k}\right) q^{d-k}.$$

Comparing coefficients in our two expressions for $T^{\mathrm{sf}}_{(1^d),\infty}(q)$ we conclude that

$$\dim \Sigma^k_d = \sigma^k_d(1^d) = \sum_{i=k}^{d-1} \begin{bmatrix} d \\ d-i \end{bmatrix} \binom{i}{i-k}.$$

(2) Let ψ^k_d be the character of $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$. Then using the definition of Σ^k_d and switching the order of summation we have

$$\sum_{k=0}^{d-1}\sigma^k_d(1^d) = \sum_{k=0}^{d-1}\sum_{j=k}^{d}\binom{j}{k}\psi^j_d(1^d) = \sum_{j=0}^{d-1}\sum_{k=0}^{j}\binom{j}{k}\psi^j_d(1^d) = \sum_{j=0}^{d-1} 2^j \psi^j_d(1^d).$$

Note that by Theorem 2.2.2 (1),

$$\sum_{j=0}^{d-1}\frac{\psi^j_d(1^d)}{q^j} = d!\frac{T_{(1^d),1}(q)}{q^d} = \frac{d!}{q^d}\binom{q+d-1}{d}. \tag{3.10}$$

Evaluating (3.10) at $q = \frac{1}{2}$ implies

$$\sum_{j=0}^{d-1} 2^j \psi_d^j(1^d) = 2^d d! \binom{d - \frac{1}{2}}{d} = (2d-1)(2d-3)\cdots 3 \cdot 1 = (2d-1)!!.$$

Therefore $\dim \bigoplus_{k=0}^{d} \Sigma_d^k = (2d-1)!!$.

3. By definition we have

$$\Sigma_d^0 \cong \mathbf{Sgn}_d \otimes \bigoplus_{j=0}^{d-1} H^{2j}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}).$$

In Theorem 2.2.12 we showed that

$$\bigoplus_{j=0}^{d-1} H^{2j}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}) \cong \mathbb{Q}[S_d],$$

where $\mathbb{Q}[S_d]$ is the regular representation. The claim follows from

$$\mathbf{Sgn}_d \otimes \mathbb{Q}[S_d] \cong \mathbb{Q}[S_d]. \qquad \square$$

Chapter 4

Cyclotomic factors of necklace polynomials

This chapter is a revised version of the author's preprint [50].

4.1 Introduction

The d**th necklace polynomial** $M_d(x)$ for $d \geq 1$ an integer is defined by

$$M_d(x) := \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}, \tag{4.1}$$

where μ is the number theoretic Möbius function. Necklace polynomials arise naturally in number theory, combinatorics, dynamics, geometry, representation theory, and algebra. For example, if q is a prime power and $\mathbb{F}_q$ is a finite field with q elements, then $M_d(q)$ is the number of $\mathbb{F}_q$-irreducible monic polynomials of degree d in $\mathbb{F}_q[x]$; if $k \geq 1$ is a natural number, then $M_d(k)$ is the number of aperiodic necklaces of length d one can make with beads in k colors. See Section 4.2 for a more interpretations of necklace polynomials.

We begin with the observation that necklace polynomials are highly reducible over $\mathbb{Q}$.

Example 4.1.1. Let $d = 3 \cdot 5 \cdot 7 = 105$, then

$$\begin{aligned} M_{105}(x) &= \tfrac{1}{105}(x^{105} - x^{35} - x^{21} - x^{15} + x^7 + x^5 + x^3 - x) \\ &= f(x)(x^4 + 1)(x^2 + x + 1)(x^2 - x + 1)(x^2 + 1)(x + 1)(x - 1)x, \end{aligned}$$

where $f(x) \in \frac{1}{105}\mathbb{Z}[x]$ is an irreducible polynomial of degree 92.

With only one exception, the low degree irreducible factors of $M_d(x)$ in Example 4.1.1 are cyclotomic polynomials. Recall that the m**th cyclotomic polynomial** $\Phi_m(x)$ is the $\mathbb{Q}$-minimal polynomial of a primitive mth root of unity. Below we have an explicit formula for $\Phi_m(x)$ which is useful for computations,

$$\Phi_m(x) = \prod_{n|m} (x^{m/n} - 1)^{\mu(n)}.$$

This preponderance of cyclotomic factors of $M_d(x)$ is not isolated to specific choices of d, it occurs to some extent for all d.

Example 4.1.2. There are irreducible, non-cyclotomic polynomials $f(x), g(x), h(x) \in \frac{1}{d}\mathbb{Z}[x]$ with degrees $3, 210, 708$ respectively such that

$$\begin{aligned}
M_{10}(x) &= \tfrac{1}{10}(x^{10} - x^5 - x^2 + x) \\
&= f(x) \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x \\
M_{253}(x) &= \tfrac{1}{253}(x^{253} - x^{23} - x^{11} + x) \\
&= g(x) \cdot \Phi_{24} \cdot \Phi_{22} \cdot \Phi_{11} \cdot \Phi_{10} \cdot \Phi_8 \cdot \Phi_5 \cdot \Phi_2 \cdot \Phi_1 \cdot x \\
M_{741}(x) &= \tfrac{1}{741}(x^{741} - x^{247} - x^{57} - x^{39} + x^{19} + x^{13} + x^3 - x) \\
&= h(x) \cdot \Phi_{20} \cdot \Phi_{18} \cdot \Phi_{12} \cdot \Phi_9 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x.
\end{aligned}$$

In this chapter we study the cyclotomic factors of necklace polynomials, the way this phenomenon extends to generalizations of necklace polynomials, and how it connects number theory, combinatorics, and geometry. We begin with a conjecture on which our subsequent work is predicated on. Recall the factorizations

$$x^m - 1 = \prod_{n|m} \Phi_n(x) \qquad x^m + 1 = \prod_{\substack{n|2m \\ n\nmid m}} \Phi_n(x).$$

Conjecture 4.1.3. *If $\Phi_m(x)$ divides $M_d(x)$ for some $m, d \geq 1$, then either $x^m - 1$ divides $M_d(x)$ or m is even and $x^{m/2} + 1$ divides $M_d(x)$.*

Conjecture 4.1.3 implies that it suffices to study factors of $M_d(x)$ of the form $x^m \pm 1$.

Toward that end our first result is Theorem 4.1.4.

Theorem 4.1.4. *Let $m, d \geq 1$ be integers.*

1. *If p is a prime dividing d such that $p \equiv 1 \bmod m$, then $x^m - 1$ divides $M_d(x)$.*

2. *If $x^m - 1$ divides $M_d(x)$, then $x^m - 1$ divides $M_{de}(x)$ for all $e \geq 1$.*

3. *If $x^m + 1$ divides $M_d(x)$, then $x^m + 1$ divides $M_{de}(x)$ for all odd $e \geq 1$.*

4. *If c is the squarefree part of d (c is the product of all distinct prime factors of d), then all cyclotomic factors of $M_d(x)$ are **induced** from cyclotomic factors of $M_c(x)$ (see Definition 4.2.11.) In other words, it suffices to determine the cyclotomic factors of $M_d(x)$ for d squarefree.*

5. *If $x^m - 1$ divides $M_d(x)$, then m divides $\varphi(d)$, where φ is the Euler totient function.*

4.1.1 Minimal cyclotomic factors

Theorem 4.1.4 reduces us to the case where d is squarefree with at least two prime factors such that $x^m \pm 1$ does not divide $M_e(x)$ for any proper factor e of d. Say $x^m \pm 1$ **minimally divides** $M_d(x)$ if $x^m \pm 1$ divides $M_d(x)$ and does not divide $M_e(x)$ for any proper divisor e of d.

Theorem 4.1.5. *Let $m \geq 1$ be an integer.*

1. *Let $d = pq$ for distinct primes p and q.*
   (a) *There are no m such that $x^m - 1$ minimally divides $M_d(x)$. That is, if $x^m - 1$ divides $m_{pq}(x)$, then $x^m - 1$ divides either $M_p(x)$ or $M_q(x)$.*

   (b) *$x^m + 1$ minimally divides $M_d(x)$ if and only if $p, q \not\equiv 1 \bmod 2m$ and*

$$pq \equiv 1 + m \bmod 2m$$
$$p \equiv q + m \bmod 2m.$$

For example, if $p \equiv m-1 \bmod 2m$ and $q \equiv -1 \bmod 2m$, then x^m+1 minimally divides $M_{pq}(x)$.

2. *If $d = pqr$ for distinct primes p, q, r such that $p, q, r \not\equiv 1 \bmod m$ and*

$$p^2 \equiv q^2 \equiv r^2 \equiv 1 \bmod m$$
$$pqr \equiv 1 \bmod m,$$

then $x^m - 1$ minimally divides $M_d(x)$.

Example 4.1.6. Let $m = 15$. Then the prime factors of $d = 11 \cdot 19 \cdot 29 = 6061$ satisfy the congruences in Theorem 4.1.5 (3), hence $x^{15} - 1$ minimally divides $M_{6061}(x)$. In fact

$$\begin{aligned} M_{6061}(x) =& \tfrac{1}{6061}(x^{6061} - x^{551} - x^{319} - x^{209} + x^{29} + x^{19} + x^{11} - x) \\ =& f(x) \cdot (x^{15} - 1) \cdot \Phi_{60} \cdot \Phi_{30} \cdot \Phi_{28} \cdot \Phi_{20} \cdot \Phi_{18} \cdot \Phi_{14} \cdot \Phi_{12} \\ & \cdot \Phi_{10} \cdot \Phi_9 \cdot \Phi_7 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot x, \end{aligned}$$

where $f(x)$ is an irreducible, non-cyclotomic polynomial of degree 5964.

It would be interesting to know the extent to which minimal $x^m \pm 1$ divisors of necklace polynomials can be classified into infinite families cut out by congruences.

4.1.2 Differences of necklace polynomials

After clearing denominators, the differences between necklace polynomials often have cyclotomic factors.

Example 4.1.7. There is an irreducible, non-cyclotomic polynomial $f(x) \in \mathbb{Z}[x]$ of degree 83 such that

$$\begin{aligned} 91M_{91}(x) - 6M_6(x) &= x^{91} - x^{13} - x^7 - x^6 + x^3 + x^2 \\ &= f(x) \cdot \Phi_5(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \cdot x^2. \end{aligned}$$

This implies, for example, that $91M_{91}(\zeta_5) = 6M_6(\zeta_5)$ for any 5th root of unity ζ_5. Note that $\Phi_5(x)$ is not a common divisor of $M_{91}(x)$ and $M_6(x)$.

In line with Conjecture 4.1.3 we expect these cyclotomic factors to be accounted for by factors of $dM_d(x) - eM_e(x)$ of the form $x^m \pm 1$. Theorem 4.1.8 identifies the source of this phenomenon. Say integers d and e are **primewise congruent modulo** m if

$$d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \qquad e = q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$$

for some $k \geq 1$ and primes p_i, q_i such that $p_i \equiv q_i \bmod m$ for each i.

Theorem 4.1.8. *Let $d, e \geq 1$ be integers. If d and e are primewise congruent modulo m, then*

$$dM_d(x) \equiv eM_e(x) \bmod x^m - 1.$$

Example 4.1.9. Returning to Example 4.1.7, note that $91 = 7 \cdot 13$ and $6 = 2 \cdot 3$ are primewise congruent modulo 5. Hence $x^5 - 1$ divides $91M_{91}(x) - 6M_6(x)$.

4.1.3 Mahler algebra and functional equations

Our main tool for analyzing cyclotomic factors of necklace polynomials is an algebra of operators we call the **Mahler algebra**. The Mahler algebra, denoted Ψ, is the ring freely generated as an additive abelian group by symbols $[m]$ for $m \in \mathbb{N}$ subject to the multiplicative relations $[m][n] = [mn]$. Equivalently Ψ is the monoid ring $\mathbb{Z}[\mathbb{N}^\times]$ where $\mathbb{N}^\times$ is the multiplicative monoid of natural numbers. We name Ψ after Mahler because of the role these operators play in the study of Mahler equations (see [68].)

There is an action of Ψ on polynomials given by $[m]f(x) := f(x^m)$. Every polynomial in $f(x) = \sum_{k=0}^{d} a_k x^k \in \mathbb{Z}[x]$ has a unique expression as $f(x) = [f]x$ where

$$[f] := \sum_{k=0}^{d} a_k [k] \in \Psi.$$

The operator $[M_d]$ associated to the necklace polynomial $M_d(x)$ factors in Ψ according to the prime factorization of d.

Theorem 4.1.10. *Suppose that* $d = \prod_{p|d} p^{e_p}$ *is the prime factorization of* d*. Then*

$$[M_d] = \frac{1}{d}\varphi[d] = \frac{1}{d}\prod_{p|d}[p^{e_p}] - [p^{e_p-1}] \in \Psi.$$

The factorization of $[M_d]$ is equivalent to the necklace polynomials satisfying a family of functional equations studied by Metropolis and Rota [63] (see Section 4.1.4 below.) Theorem 4.1.11 demonstrates a sense in which the cyclotomic factor phenomenon should be associated more generally to the operator $\varphi[d] \in \Psi$.

Theorem 4.1.11. *Let* R *be any commutative ring and let* $f(x) \in R[x]$ *be a polynomial.*

1. *If* $x^m - 1$ *divides* $M_d(x)$*, then*

$$x^m - 1 \text{ divides } \varphi[d]f(x) := \sum_{e|d} \mu(e) f(x^{d/e}).$$

2. *If* $x^m + 1$ *divides* $M_d(x)$ *and* $f(x)$ *is an odd polynomial, then*

$$x^m + 1 \text{ divides } \varphi[d]f(x) := \sum_{e|d} \mu(e) f(x^{d/e}).$$

Example 4.1.12. In Example 4.1.2 we saw that $x^{22} - 1$ divides $M_{253}(x)$. It follows for any polynomial $f(x)$ that

$$x^{22} - 1 \text{ divides } \varphi[243]f(x) = f(x^{253}) - f(x^{23}) - f(x^{11}) + f(x).$$

4.1.4 Cyclotomic factors of $\Phi_d(x) - 1$

The operator $[f]$ associated to a polynomial $f(x)$ typically does not factor in Ψ. Factorizations of $[f]$ correspond to functional equations satisfied by $f(x)$. For example, the factorization of $[M_d]$ given in Theorem 4.1.10 is equivalent to $M_d(x)$ satisfying the following relations (see Theorem 4.2.7.) Let p be a prime integer.

1. If p does not divide d, then

$$M_{dp}(x) = \frac{1}{p}\big(M_d(x^p) - M_d(x)\big).$$

2. If p divides d, then

$$M_{dp}(x) = \frac{1}{p}M_d(x^p).$$

Cyclotomic polynomials satisfy a multiplicative version of the same identities. Again let p be a prime integer.

1. If p does not divide d, then

$$\Phi_{dp}(x) = \frac{\Phi_d(x^p)}{\Phi_d(x)}.$$

2. If p divides d, then

$$\Phi_{dp}(x) = \Phi_d(x^p).$$

These identities are equivalent to

$$\log \Phi_d(x) = \varphi[d] \log(x-1).$$

Thus Theorem 4.1.11 suggests that cyclotomic factors of $M_d(x)$ should also divide $\log \Phi_d(x)$, or equivalently $\Phi_d(x) - 1$. This does not follow formally from Theorem 4.1.11 since $\log(x-1)$ is not a polynomial, however we recover the following result along these lines.

Theorem 4.1.13. *Suppose that $m, d > 1$ are integers and $x^m - 1$ divides $M_d(x)$, then $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$.*

Example 4.1.14. In Example 4.1.6 we showed that $x^{15}-1$ divides $M_{6061}(x)$. Thus Theorem 4.1.13 implies that $\frac{x^{15}-1}{x-1}$ divides $\Phi_{6061}(x) - 1$. Hence if ζ_{15} is any non-trivial 15th root of unity and ζ_{6061} is a primitive 6061th root of unity, then the following product identity holds in $\overline{\mathbb{Q}}$,

$$\prod_{\gcd(k,6061)=1} (\zeta_{15} - \zeta_{6061}^k) = \Phi_{6061}(\zeta_{15}) = 1. \tag{4.2}$$

Since $\gcd(15, 6061) = 1$ the difference $\zeta_{15}^j - \zeta_{6061}^k$ is an algebraic unit for each k coprime to 6061. Hence (4.2) is a non-trivial relation satisfied by these units.

4.1.5 Trace formula

A cyclotomic factor $\Phi_m(x)$ of $M_d(x)$ is equivalent to the vanishing $M_d(\zeta_m) = 0$ for any primitive mth root of unity m. Although $M_d(x)$ vanishes at only finitely many roots of unity, Theorem 4.1.15 shows that $M_d(\zeta_m)$ is approximately zero (in a sense) for all but finitely many m.

Theorem 4.1.15. *Let $m, d \geq 1$ and let $\mathrm{Tr}_m : \mathbb{Q}(\zeta_m) \to \mathbb{Q}$ be the $\mathbb{Q}$-linear trace map (where $\mathrm{Tr}_m(\alpha)$ is the sum over the orbit of α under $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.) Then*

1. *The trace of $M_d(\zeta_m)$ is given by*

$$\mathrm{Tr}_m(M_d(\zeta_m)) = \begin{cases} \mu(m/d) & \text{when } d \text{ divides } m \\ 0 & \text{otherwise.} \end{cases}$$

2. *If d does not divide m and $M_d(\zeta_m)$ is rational, then $M_d(\zeta_m) = 0$.*
3. *In particular we have the following evaluations of $M_d(\pm 1)$,*

$$M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & \text{otherwise,} \end{cases} \qquad M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & \text{otherwise.} \end{cases}$$

Since $M_1(x) = x$, the trace computation in Theorem 4.1.15 specializes when $d = 1$ to the well-known formula for the trace of a primitive mth root of unity ζ_m,

$$\mathrm{Tr}_m(\zeta_m) = \mu(m).$$

We view Theorem 4.1.15 as a generalization of this classic identity. The evaluations of $M_d(\pm 1)$ in Theorem 4.1.15 (3) are given geometric interpretations in Section 4.6.

4.1.6 G-necklace polynomials

Aspects of the cyclotomic factor phenomenon extend to two independent generalizations of the necklace polynomials $M_d(x)$: the G-necklace polynomials $M_G(x)$ associated to

a finite group G, and the higher necklace polynomials $M_{d,n}(x)$ enumerating irreducible polynomials in a multivariate polynomial ring over $\mathbb{F}_q$.

Let G be a finite group and let X be a finite set. An **X-coloring of G** or a **G-necklace with X colors** is simply a function from G to X. The group G acts on X^G, the set of all X-colorings of G. A **primitive** G-necklace is an element of X^G with trivial stabilizer. If the set X has x elements, then the total number of orbits of primitive G-necklaces with X colors is given by a polynomial $M_G(x)$ in x called the **G-necklace polynomial**. An explicit formula for $M_G(x)$ is given by

$$M_G(x) = \frac{1}{|G|} \sum_{H \subseteq G} \mu(H) x^{|G|/|H|},$$

where $\mu(H)$ is the value of the Möbius function of the subgroup lattice of G on the interval of subgroups between 1 and H (see Section 4.3.)

When $G = C_d$ is the cyclic group of order d, a C_d-necklace reduces to the usual notion of a necklace of length d and $M_{C_d}(x) = M_d(x)$. Hence $M_G(x)$ is a natural generalization of $M_d(x)$. For certain classes of groups G the polynomials $M_G(x)$ exhibits a cyclotomic factor phenomenon similar to the cyclic case.

Example 4.1.16. Let D_{20} be the dihedral group with 20 elements. Then $M_{D_{20}}(x)$ factors over $\mathbb{Q}$ as

$$M_{D_{20}}(x) = \tfrac{1}{20}(x^{20} - 11x^{10} + 10x^5 - x^4 + 11x^2 - 10x) = f(x)(x^2 + 1)(x + 1)(x - 1)x,$$

where $f(x) \in \mathbb{Z}[x]$ is an irreducible, non-cyclotomic polynomial of degree 15.

Dress and Siebeneicher [24] introduced the G-necklace polynomials in the course of constructing an isomorphism between the G-necklace algebra and the G-Burnside-Witt ring. Oh [71] studied the G-necklace polynomials in depth, generalizing the functional identities for the classic necklace polynomials $M_d(x)$ to G-necklace polynomials.

Oh's results provide new insights into these functional equations, highlighting their relation to the structure of the group G. When G is solvable we show that Oh's functional equations for $M_G(x)$ translate into a product formula for $[M_G]$ in the Mahler algebra. This factorization of $[M_G]$ gives rise to cyclotomic factors of $M_G(x)$.

Theorem 4.1.17. *Suppose G is a finite group with subgroup K and a chain of normal subgroups*

$$K = N_0 \triangleleft N_1 \triangleleft \dots N_k \triangleleft N_{k+1} = G$$

such N_{i+1}/N_i is cyclic of prime order p_i. Let c_i be the number of non-trivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$.

1. *Let $M_G(x)$ be the G-necklace polynomial, then*

$$M_G(x) = \frac{1}{[G:K]}\Big(\prod_{i=0}^{k}[p_i] - c_i[1]\Big)M_K(x).$$

2. *If $c_i = 1$, then $x^{p_i-1} - 1$ divides $M_G(x)$. If G is solvable and $K = 1$, then $c_0 = 1$ and this implies that $M_G(x)$ has cyclotomic factors.*
3. *If $c_i > 1$, then $x^{p_i-1} - 1$ divides $|G|M_G(x)$ in $\mathbb{Z}/(c_i - 1)[x]$.*

Example 4.1.18. The dihedral group D_{20} has a cyclic normal subgroup $C_{10} \triangleleft D_{20}$ of index 2 and there are 10 non-trivial subgroups in D_{20} which intersect trivially with C_{10}, hence

$$M_{D_{20}}(x) = \frac{1}{2}([2] - 10[1])M_{10}(x) = \frac{1}{2}(M_{10}(x^2) - 10M_{10}(x)).$$

On the other hand, $M_{D_{20}}(x) = \frac{1}{10}\varphi[10]\frac{1}{2}(x^2 - 10x)$, so Theorem 4.1.11 implies that $M_{D_{20}}(x)$ is divisible by $x^m - 1$ whenever $M_{10}(x)$ is. Note that $x^3 + 1$ divides $M_{10}(x)$ but not $M_{D_{20}}(x)$; this is due to $\frac{1}{2}(x^2 - 10x)$ not being an odd polynomial.

4.1.7 Higher necklace polynomials

Let $\mathbb{F}_q$ be a finite field and let $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ be the set of monic, $\mathbb{F}_q$-irreducible, total degree d polynomials in $\mathbb{F}_q[x_1, x_2, \dots, x_n]$. By a monic polynomial in a multivariate polynomial ring we mean an $\mathbb{F}_q^\times$-orbit of polynomials under scaling. Since $\mathbb{F}_q$ is finite, $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ is a finite set. In Chapter 3 we constructed a polynomial $M_{d,n}(x) \in \mathbb{Q}(x)$ such that $M_{d,n}(q) = |\mathrm{Irr}_{d,n}(\mathbb{F}_q)|$ for any prime power q. For $d, n \geq 1$ we call $M_{d,n}(x)$ the **higher necklace polynomials**.

The first (implicit) reference to $M_{d,n}(x)$ we have found is due to Carlitz [14, 15] who studied the asymptotic behavior of $M_{d,n}(x)$ as $n \to \infty$. In Chapter 3 we analyzed the

x-adic asymptotic behavior of $M_{d,n}(x)$, showing that $M_{d,n}(x)$ converges coefficientwise as $n \to \infty$ to a simple rational function related to the classic necklace polynomial $M_d(x)$ in a surprising way.

When $n = 1$ the higher necklace polynomials reduce to the classic case $M_{d,1}(x) = M_d(x)$. If $n > 1$, then there is no known explicit formula for $M_{d,n}(x)$ analogous to the simple expression (4.1) for $M_d(x)$. Furthermore $[M_{d,n}] \in \Psi$ does not appear to factor in the same way as $[M_d]$ and $[M_G]$ do, which we used to explain the cyclotomic factor phenomenon in those cases. Nevertheless we observe that $M_{d,n}(x)$ does generally have cyclotomic factors for $d, n \geq 1$.

For each fixed $n > 1$, instead of seeing many different cyclotomic factors of $M_{d,n}(x)$ as we vary d, we see the same factors for all but finitely many d. When $n = 1$ the only cyclotomic factors that divide $M_d(x)$ for all but finitely many d are $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. Theorem 4.1.19 below demonstrates this phenomenon.

Let $b, n \geq 1$ be integers. A **balanced base b expansion of n** is an expression

$$n = b^{k_1} - b^{k_2} + b^{k_3} - \ldots + b^{k_{i-1}} - b^{k_i},$$

where i is even and $k_1 > k_2 > k_3 > \ldots > k_i \geq 0$ is a decreasing sequence of integers and the coefficients on the right hand side alternate between ± 1. Equivalently, n has a balanced base b expansion if all of the base b digits of n are 0 or $b - 1$,

$$n = (b-1)b^{\ell_1} + (b-1)b^{\ell_2} + \ldots + (b-1)b^{\ell_j}.$$

In that case, the balanced base b expansion of n is gotten by expanding each $(b-1)b^k = b^{k+1} - b^k$ and collecting coefficients.

Theorem 4.1.19. *Let $d, n \geq 1$ and suppose p is a prime such that n has the balanced base p expansion*

$$n = \sum_{k=0}^{m} a_k p^k.$$

Let ζ_p be a primitive pth root of unity. Then

$$M_{d,n}(\zeta_p) = \begin{cases} a_k & \text{if } d = p^k \\ 0 & \text{otherwise.} \end{cases}$$

If n has a balanced base p expansion, then $x^p - 1$ divides $M_{d,n}(x)$ for all but finitely many d.

Example 4.1.20. If $n = 104$, then n has the balanced base 5 expansion

$$104 = 5^3 - 5^2 + 5 - 1.$$

Therefore, if ζ_5 is a primitive 5th root of unity, then

$$M_{d,104}(\zeta_5) = \begin{cases} 1 & d = 5, 125 \\ -1 & d = 1, 25 \\ 0 & \text{otherwise.} \end{cases}$$

Hence $M_{d,104}(x)$ is divisible by $\Phi_5(x)$ for all but finitely many d.

The lack of functional equations or explicit formulas for $M_{d,n}(x)$ requires us to use another method to analyze cyclotomic factors of $M_{d,n}(x)$. The following "combinatorial Euler product formula" gives an indirect way to study the higher necklace polynomials.

Theorem 4.1.21. *Let $P_{d,n}(x) \in \mathbb{Q}[x]$ be the polynomial such that $P_{d,n}(q)$ is the number of total degree d monic polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$, namely*

$$P_{d,n}(x) := \frac{x^{\binom{d+n}{n}} - x^{\binom{d+n-1}{n}}}{x - 1}.$$

Then for each $n \geq 1$ the following identity holds in the ring of formal power series with coefficients in $\mathbb{Q}[x]$,

$$\sum_{d \geq 0} P_{d,n}(x) t^d = \prod_{j \geq 1} \left(\frac{1}{1 - t^j} \right)^{M_{j,n}(x)},$$

where exponentiation by $M_{j,n}(x)$ on the right hand side is defined by the binomial theorem,

$$\left(\frac{1}{1-t}\right)^a := \sum_{d\geq 0} \left(\!\!\binom{a}{d}\!\!\right) t^d,$$

where $\left(\!\!\binom{x}{d}\!\!\right) := \frac{1}{d!}x(x+1)\cdots(x+d-1)$.

When $n = 1$ we have $P_{d,1}(x) = x^d$ and Theorem 4.1.21 specializes to the well-known **cyclotomic identity** [63, Sec. 5],

$$\frac{1}{1-xt} = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_j(x)}.$$

Therefore Theorem 4.1.21 is a generalization of the cyclotomic identity.

4.1.8 Geometric interpretations

We interpret the values $M_{d,n}(\pm 1)$ geometrically as Euler characteristics of the spaces of irreducible polynomials over $\mathbb{R}$ and $\mathbb{C}$. For any field K let $\mathrm{Irr}_{d,n}(K)$ be the space of all monic total degree d irreducible polynomials in $K[x_1, x_2, \ldots, x_n]$. When $K = \mathbb{R}$ or $\mathbb{C}$, $\mathrm{Irr}_{d,n}(K)$ inherits a topology from its inclusion in the projective space $\mathrm{Poly}_{\leq d,n}(K)$ of all degree at most d monic polynomials in n variables.

Theorem 4.1.22. *Let $d, n \geq 1$ and let χ_c be the compactly supported Euler characteristic, then*

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad \chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1) = \begin{cases} a_k & \text{if } d = 2^k \\ 0 & \text{otherwise.} \end{cases}$$

where $n = \sum_{k\geq 0} a_k 2^k$ is the balanced base 2 expansion of n.

Example 4.1.23. Suppose $n = 13$. The balanced binary expansion of 13 is

$$13 = 2^4 - 2^2 + 2 - 1.$$

Hence Theorem 4.1.22 implies

$$\chi_c(\mathrm{Irr}_{d,13}(\mathbb{R})) = \begin{cases} 1 & d = 2, 16 \\ -1 & d = 1, 4 \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 4.1.22 suggests that the singular cohomology of $\mathrm{Irr}_{d,n}(\mathbb{R})$ depends in a subtle way on the additive structure of the parameter n. It would be interesting to determine the cohomology of this space.

When $n = 1$ we can use our understanding of the irreducible polynomials in $\mathbb{C}[x]$ and $\mathbb{R}[x]$ to compute $M_d(\pm 1)$ geometrically (see Corollary 4.6.8.) In particular since there are no irreducible polynomials in $\mathbb{C}[x]$ or $\mathbb{R}[x]$ with degree $d > 2$ it follows that $M_d(\pm 1) = 0$ for all such d. This gives an interpretation of the cyclotomic factors $\Phi_1(x)$ and $\Phi_2(x)$ of necklace polynomials $M_d(x)$. We would be interested to know interpretations, geometric or otherwise, of the values $M_{d,n}(\zeta_m)$ for $m > 2$.

4.1.9 Acknowledgements

I am happy to thank Suki Dasher and Andrew O'Desky for asking a question about the factorization of necklace polynomials that prompted this work. I also thank Weiyan Chen, Nir Gadish, Bob Lutz, and Phil Tostesson for helpful conversations and feedback on the manuscript. I thank David Cox for his help on references to the work of Gauss and Schönemann. Finally I thank Jeff Lagarias for his generous advice and encouragement.

4.2 Necklace polynomials

Recall that the dth necklace polynomial is defined by

$$M_d(x) = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}. \tag{4.3}$$

Necklace polynomials play an important role in several areas of mathematics. Below we list some examples familiar to us.

1. If $x = k$ is a natural number, then $M_d(k)$ counts the number of primitive necklaces formed with d beads in k possible colors. A necklace (a coloring of a cyclically ordered set) not invariant under any proper rotation is called **primitive**. This interpretation of $M_d(k)$ gives necklace polynomials their name. Metropolis and Rota [63, Pg. 95] attribute this interpretation of $M_d(x)$ to the French colonel Moreau [65]; the M in the notation is presumably in his honor.

2. If $x = q$ is a prime power, then $M_d(q)$ is the number of irreducible monic polynomials in $\mathbb{F}_q[x]$ of degree d. This interpretation was found by Gauss [37, Pg. 611] and later independently found by Schönemann [80, Sec. 48, Pp. 51-52].

3. A Lyndon word in a totally ordered alphabet with ℓ letters is a word that is lexicographically minimal among all of its cyclic permutations. The number of Lyndon words of length d formed from ℓ letters is $M_d(\ell)$. See Berstel and Perrin [5, Sec. 4.2].

4. If $x = g$ is a natural number, then Witt [95, Satz 3] showed that $M_d(g)$ is the dimension of the degree d homogeneous component of the free Lie algebra on g generators. In this context (4.3) is sometimes called Witt's formula [5, Pg. 1005]. Reutenaur [76, Thm. 4.9, Thm. 5.1] gave a combinatorial proof of this result by constructing an explicit basis for the free Lie algebra from Lyndon words.

5. If $f(x) \in \mathbb{C}[x]$ is a generic degree m polynomial, then the total number of length d periodic orbits of $f(x)$ under iteration is $M_d(m)$. See Silverman [81, Rmk. 4.3].

6. Metropolis and Rota [63] derived functional equations satisfied by $M_d(x)$ and used them to construct the necklace ring $\mathrm{Nr}(R)$ from any commutative ring R. They proved [63, Prop. 1, Pg. 114] that $\mathrm{Nr}(R)$ is isomorphic to $W(R)$ the ring of big Witt vectors of R whenever R is a **binomial ring** (see Section 4.4.)

Despite the prevalence of necklace polynomials, the observation of their reducibility and cyclotomic factors seems to have been overlooked. In this section we initiate the study of the cyclotomic factor phenomenon. We found several equivalent ways to approach this problem, all fundamentally reducing to the functional equations discovered by Metropolis and Rota [63]. We reinterpret these relations using the Mahler algebra defined below.

4.2.1 The Mahler Algebra

The **Mahler algebra** Ψ is the $\mathbb{Z}$-algebra generated by symbols $[n]$ for $n \geq 0$ subject to the multiplicative relations $[m][n] = [mn]$. The Mahler algebra is canonically isomorphic to the monoid algebra $\mathbb{Z}[\mathbb{N}^\times]$, where $\mathbb{N}^\times$ is the multiplicative monoid of natural numbers. There is a natural ring endomorphism action of Ψ on polynomial rings given by

$$[n]f(x) := f(x^n).$$

Thus $\mathbb{Z}[x]$ is a Ψ-module and furthermore a Ψ-algebra. For example, if $\alpha = 3[2]+5[7] \in \Psi$ and $f(x) \in \mathbb{Z}[x]$ is a polynomial, then

$$\alpha f(x) = (3[2] + 5[7])f(x) = 3f(x^2) + 5f(x^7).$$

Observe that $\mathbb{Z}[x]$ is cyclic as a Ψ-module since if $f(x) = \sum_{i=0}^{j} a_i x^i$, then

$$f(x) = [f]x := \Big(\sum_{i=0}^{j} a_i [i] \Big) x.$$

Note that $[1] = 1$ but $[0] \neq 0$ in Ψ since $[0]f(x) = f(x^0) = f(1)$ while $0f(x) = 0$.

Our terminology is inspired by the Frobenius operators in the theory of Witt vectors. Metropolis and Rota [63] construct the necklace ring $\mathrm{Nr}(\mathbb{Z})$ as a combinatorial model of the integral Witt vectors $W(\mathbb{Z})$. In this model they show that the nth Frobenius operator $[n]$ (which they denote F_n) acts on the dth necklace polynomial $M_d(x)$ by $[n]M_d(x) = M_d(x^n)$. The Ψ in the notation for the Mahler algebra is a reference to the Adams operations ψ_m, which are the name for the Frobenius operators in the context of K-theory. We adopt this

notation following Borger [8, Eq. (4.3.1)].

If $m, n \geq 0$ are integers, then $x^m - 1$ divides $x^{mn} - 1$. Let $(x^m - 1)$ be a principal ideal in $\mathbb{Z}[x]$, then $\Psi(x^m - 1) \subseteq (x^m - 1)$. Hence $\mathbb{Z}[x]/(x^m - 1)$ inherits a Ψ-module structure. Similarly, if n is odd, then $x^m + 1$ divides $x^{mn} + 1$ (and this can fail if n is even.) Let Ψ^{odd} be the subalgebra of Ψ generated by $[n]$ for n odd. Then $\Psi^{\text{odd}}(x^m + 1) \subseteq (x^m + 1)$ and thus $\mathbb{Z}[x]/(x^m + 1)$ inherits a Ψ^{odd}-module structure. We now construct simpler models for these modules to facilitate our analysis.

Let $\Psi[m]$ denote the quotient of Ψ as a Ψ-module by "congruence modulo m inside brackets." That is $[a] = [b]$ in $\Psi[m]$ if and only if $a \equiv b \bmod m$. This quotient is clearly Ψ-equivariant since multiplication happens within brackets and preserves congruences. If $\alpha, \beta \in \Psi$, then we suggestively write

$$\alpha \equiv \beta \bmod [m]$$

when $\alpha = \beta$ in $\Psi[m]$. We caution that $\Psi[m]$ is *not* the quotient of Ψ by the principal ideal generated by $[m]$. To see the difference note that $[2] \equiv [7] \bmod [5]$, but $[5]$ does not divide the difference $[2] - [7]$ in Ψ. Next define $\Psi[m]_\pm$ to be the Ψ^{odd}-module defined as the quotient of $\Psi[2m]$ by the relation $[b+m] = -[b]$ for all $b \geq 0$. The restriction of the action to Ψ^{odd} avoids unintended consequences: if we multiply the identity $[b+m] = -[b]$ by $[2]$, then we get

$$-[2b] = [2b + 2m] = [2b] \Longrightarrow 2[2b] = 0.$$

On the other hand, as a Ψ^{odd}-module, $\Psi[m]_\pm$ has no additive torsion. If $\alpha, \beta \in \Psi$, then we write

$$\alpha \equiv \beta \bmod [m]_\pm$$

when $\alpha = \beta$ in $\Psi[m]_\pm$. Note that although $\Psi[m]_\pm$ is only a Ψ^{odd}-module, there is an element $[b] \in \Psi[m]_\pm$ for all integers $b \geq 0$. The restriction comes in when we consider the multiplicative action of Ψ. For example, $[6]$ is an element of $\Psi[10]_\pm$ and in this module we can write $[6] = [3][2]$ with the understanding that the product comes from the multiplicative action; in this case $[2]$ is an element of $\Psi[10]_\pm$ and $[3] \in \Psi^{\text{odd}}$. On the other hand, we technically cannot write $[6] = [2][3]$ since $[2]$ is not an element of Ψ^{odd}.

Proposition 4.2.1. *Let $m \geq 1$.*

1. *The map $\alpha \mapsto \alpha x$ defines an isomorphism between $\Psi[m]$ and $\mathbb{Z}[x]/(x^m - 1)$ as Ψ-modules.*
2. *The map $\alpha \mapsto \alpha x$ defines an isomorphism between $\Psi[m]_{\pm}$ and $\mathbb{Z}[x]/(x^m + 1)$ as Ψ^{odd}-modules.*

Proof. 1. To show the map is well-defined it suffices to observe that for all $b \geq 0$,

$$[b+m]x = x^{b+m} \equiv x^b = [b]x \bmod x^m - 1.$$

If $\alpha \in \Psi$ maps to the kernel of $\alpha \mapsto \alpha x$ in the quotient $\Psi \to \Psi[m]$, then

$$\alpha x = (x^m - 1)\Big(\sum_{k=0}^{n} a_k x^{b_k}\Big) = \sum_{k=0}^{n} a_k (x^{b_k+m} - x^{b_k}).$$

Thus $\alpha = \sum_{k=0}^{n} a_k([b_k + m] - [b_k])$ which implies $\alpha \equiv 0 \bmod [m]$. Hence the map $\Psi[m] \to \mathbb{Z}/[x]/(x^m + 1)$ is both injective and surjective, therefore an isomorphism.

2. To show this map is well-defined, first note that $\mathbb{Z}[x]/(x^m + 1)$ is naturally a quotient of $\mathbb{Z}[x]/(x^{2m} - 1)$. Then by (1) it suffices to observe that for all $b \geq 0$,

$$[b+m]x = x^{b+m} \equiv -x^b = -[b]x \bmod x^m + 1.$$

The proof that the kernel is trivial follows just as the previous case with a change of sign. □

Corollary 4.2.2. *Let $m \geq 1$ and let $\alpha \in \Psi$.*

1. *If $\alpha \equiv 0 \bmod [m]$, then $x^m - 1$ divides $\alpha f(x)$ for all $f(x) \in \mathbb{Z}[x]$.*
2. *If $\alpha \equiv 0 \bmod [m]_{\pm}$, then $x^m + 1$ divides $\alpha f(x)$ for all odd polynomials $f(x) \in \mathbb{Z}[x]$.*

Proof. Let $[f] \in \Psi$ be such that $f(x) = [f]x$.

1. If $\alpha \equiv 0 \bmod [m]$, then by Proposition 4.2.1 (1) $\alpha f(x) \bmod x^m - 1$ corresponds to $\alpha[f] \in \Psi[m]$. Since $\Psi[m]$ is a Ψ-module, we have

$$\alpha[f] \equiv [f](\alpha) \equiv [f]0 \equiv 0 \bmod [m].$$

Thus $x^m - 1$ divides $\alpha f(x)$.

2. If $\alpha \equiv 0 \bmod [m]_\pm$, then by Proposition 4.2.1 (2) $\alpha f(x) \bmod x^m + 1$ corresponds to $\alpha[f]$ in $\Psi[m]_\pm$. In this case, we can only express $\alpha[f]$ as $[f]$ multiplied by α if $[f]$ belongs to Ψ^{odd}, which is equivalent to $f(x)$ being an odd polynomial. In that case the calculation proceeds as above and we conclude that $x^m + 1$ divides $\alpha f(x)$. □

Example 4.2.3. Proposition 4.2.1 may seem abstract, but in practice it simply gives us a convenient shorthand for detecting factors of the form $x^m \pm 1$. For example, let $\alpha = [10]-2[7]+[4] \in \Psi$. Then by reducing modulo 3 inside brackets we see that $\alpha \equiv 0 \bmod [3]$. Hence $x^3 - 1$ divides $\alpha f(x) = f(x^{10}) - 2f(x^7) + f(x^4)$ for all polynomials $f(x)$.

Example 4.2.4. Corollary 4.2.2 (2) can fail if $f(x)$ is not an odd polynomial. For example, if $m = 2$ then $\alpha = [2] + [0]$ satisfies $\alpha \equiv 0 \bmod [2]_\pm$ since

$$[2] = [0 + 2] \equiv -[0] \bmod [2]_\pm.$$

If $f(x) = x^3$, then

$$\alpha f(x) = ([2] + [0])x^3 = x^6 + 1 \equiv 0 \bmod x^2 + 1,$$

but if $f(x) = x^2$, then

$$\alpha f(x) = ([2] + [0])x^2 = x^4 + 1 \not\equiv 0 \bmod x^2 + 1.$$

Recall that the dth necklace polynomial $M_d(x)$ is defined by

$$M_d(x) = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}. \tag{4.4}$$

Let $S_d(x) := dM_d(x) \in \mathbb{Z}[x]$. The denominator of $M_d(x)$ plays no role in the factorization of this polynomial and adds unnecessary clutter, so we work with $S_d(x)$ for simplicity. In the literature $S_d(x)$ is called the **dth cyclic polynomial** [63, Pg. 97].

Let $\varphi[d]$ denote the operator $[S_d] \in \Psi$. Equation (4.4) gives us the explicit formula

$$\varphi[d] := \sum_{e|d} \mu(e)[d/e].$$

Recall the classic identity [69, Pg. 195, (4.1)]

$$\varphi(d) = \sum_{e|d} \mu(e)(d/e), \tag{4.5}$$

where $\varphi(d)$ is the Euler totient function of d, defined as the number of multiplicative units in $\mathbb{Z}/(d)$. The multiplicativity of the Möbius function allows us to factor (4.5) as

$$\varphi(d) = \prod_{p|d} p^{e_p} - p^{e_p - 1}$$

where the product is over prime divisors of d and e_p is the maximum multiplicity of p as a divisor of d. Since the Frobenius operators are multiplicative, it follows that $\varphi[d]$ factors similarly.

Proposition 4.2.5. *Let $d \geq 1$ and let $\varphi[d] := [S_d] = \sum_{e|d} \mu(e)[d/e] \in \Psi$. Then*

$$\varphi[d] = \prod_{p|d} [p^{e_p}] - [p^{e_p - 1}].$$

Proposition 4.2.5 justifies the notation $\varphi[d]$ for $[S_d]$. Note that $\varphi[d] \neq [\varphi(d)]$. In Section 4.2.2 we combine this factorization of $\varphi[d]$ with Corollary 4.2.2 to characterize factors of $M_d(x)$ of the form $x^m \pm 1$, which conjecturally account for all cyclotomic factors of necklace polynomials (see Conjecture 4.2.9.) While discussing the connection between the identity (4.5) and necklace polynomials we record one related observation.

Proposition 4.2.6. *Let $d \geq 1$ and let $M'_d(x)$ denote the derivative of $M_d(x)$, then*

$$M'_d(1) = \frac{\varphi(d)}{d} = \prod_{p|d} 1 - \frac{1}{p}.$$

Proof. Taking the derivative of (4.4) we have

$$M_d'(x) = \frac{1}{d} \sum_{e|d} \mu(e)(d/e)x^{d/e-1}.$$

Evaluating at $x = 1$ gives

$$M_d'(1) = \frac{1}{d} \sum_{e|d} \mu(e)(d/e) = \frac{\varphi(d)}{d}.$$ □

The factorization of $\varphi[d]$ given in Proposition 4.2.5 is equivalent to $S_d(x)$ satisfying a family of functional equations. These identities were discovered by Metropolis and Rota [63, Thm. 3] who proved them combinatorially using necklace interpretation of $M_d(x)$.

Proposition 4.2.7. *Let $d \geq 1$ and let p be a prime.*

1. *If p does not divide d, then*

$$S_{dp}(x) = S_d(x^p) - S_d(x).$$

2. *If p divides d, then*

$$S_{dp}(x) = S_d(x^p).$$

Proof. (1) If p does not divide d, then $\varphi[dp] = ([p] - [1])\varphi[d]$. Hence

$$S_{dp}(x) = \varphi[dp]x = ([p] - [1])\varphi[d]x = ([p] - [1])S_d(x) = S_d(x^p) - S_d(x).$$

(2) If p divides d, then $\varphi[dp] = [p]\varphi[d]$. Hence

$$S_{dp}(x) = \varphi[dp]x = [p]\varphi[d]x = [p]S_d(x) = S_d(x^p).$$ □

Our proof of Proposition 4.2.7 shows that, more generally, if $f(x) = [f]x$ and $[f] = [g][h]$ factors in Ψ, then $f(x)$ satisfies the functional equation $f(x) = [g]h(x)$.

The two functional equations given in Proposition 4.2.7 are closely related to functional equations satisfied by cyclotomic polynomials. In particular, let $d \geq 1$ and let p be a prime, then

1. If p does not divide d, then
$$\Phi_{dp}(x) = \frac{\Phi_d(x^p)}{\Phi_d(x)}.$$
2. If p divides d, then
$$\Phi_{dp}(x) = \Phi_d(x^p).$$

We return to this connection between necklace and cyclotomic polynomials in Proposition 4.2.28.

Theorem 4.2.8 applies Corollary 4.2.2 to show that the cyclotomic factor phenomenon for $M_d(x)$ is associated more generally to the operator $\varphi[d]$.

Theorem 4.2.8. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial.*

1. *If $x^m - 1$ divides $M_d(x)$, then $x^m - 1$ divides $\varphi[d]f(x) = \sum_{e|d} \mu(e) f(x^{d/e})$.*
2. *If $x^m + 1$ divides $M_d(x)$ and $f(x)$ is an odd polynomial, then $x^m + 1$ divides $\varphi[d]f(x) = \sum_{e|d} \mu(e) f(x^{d/e})$.*

4.2.2 Cyclotomic Factors

Recall that the mth cyclotomic polynomial $\Phi_m(x) \in \mathbb{Z}[x]$ is the monic polynomial defined by
$$\Phi_m(x) := \prod_{n|m} (x^{m/n} - 1)^{\mu(n)}.$$
Equivalently $\Phi_m(x)$ is determined by the identity
$$x^m - 1 = \prod_{n|m} \Phi_n(x). \tag{4.6}$$
Since $x^{2m} - 1 = (x^m - 1)(x^m + 1)$ it follows from (4.6) that
$$x^m + 1 = \prod_{\substack{n|m \\ 2n \nmid m}} \Phi_{2n}(x).$$

We conjecture that cyclotomic factors of $M_d(x)$ may be accounted for by factors of the form $x^m \pm 1$.

Conjecture 4.2.9. *If $\Phi_m(x)$ divides $M_d(x)$ for some $m, d \geq 1$, then either $x^m - 1$ divides $M_d(x)$ or m is even and $x^{m/2} + 1$ divides $M_d(x)$.*

We have computationally verified Conjecture 4.2.9 for $1 \leq m \leq 300$ and $1 \leq d \leq 5000$. Example 4.2.23 shows that the $x^{m/2} + 1$ factors are necessary since $\Phi_6(x)$ divides $M_{10}(x)$ but $x^6 - 1$ does not.

The goal of this section is to study the pairs of integers (m, d) such that $x^m \pm 1$ divides $M_d(x)$. If Conjecture 4.2.9 holds, then these factors account for all cyclotomic factors of necklace polynomials.

Proposition 4.2.10 shows that for a fixed m, the set of all d such that $x^m \pm 1$ divides $M_d(x)$ is closed under scaling.

Proposition 4.2.10. *Let $m, d \geq 1$.*

1. *If $x^m - 1$ divides $M_d(x)$, then $x^m - 1$ divides $M_{de}(x)$ for all $e \geq 1$.*
2. *If $x^m + 1$ divides $M_d(x)$, then $x^m + 1$ divides $M_{de}(x)$ for all odd $e \geq 1$.*

Proof. 1. Our assumption that $x^m - 1$ divides $M_d(x)$ is equivalent $\varphi[d] \equiv 0 \bmod [m]$. Proposition 4.2.5 implies that $\varphi[d]$ divides $\varphi[de]$ in Ψ, hence $\varphi[de] \equiv 0 \bmod [m]$. Thus Corollary 4.2.2 (1) implies $x^m - 1$ divides $M_{de}(x)$.

2. Similarly $x^m + 1$ dividing $M_d(x)$ is equivalent to $\varphi[d] \equiv 0 \bmod [m]_\pm$. If e is odd, then $\varphi[de]/\varphi[d] \in \Psi^{\text{odd}}$. Since $\Psi[m]_\pm$ is a Ψ^{odd}-module it follows that $\varphi[de] \equiv 0 \bmod [m]_\pm$. Thus Corollary 4.2.2 (2) implies $x^m + 1$ divides $M_{de}(x)$. □

Our next result further allows us to reduce to the case when d is squarefree.

Definition 4.2.11. If $f(x) \in \mathbb{Z}[x]$ is a polynomial, then we say a cyclotomic factor $\Phi_m(x)$ of $f(x^e)$ is **induced** from $f(x)$ if $\Phi_n(x)$ divides $f(x)$ for some $n \geq 1$ and $\Phi_m(x)$ divides $\Phi_n(x^e)$.

Proposition 4.2.12. *If c is the squarefree part of d, then all cyclotomic factors of $M_d(x)$ are induced from cyclotomic factors of $M_c(x)$.*

Proof. Let $f(x)$ be a polynomial. We claim that all cyclotomic factors of $f(x^m)$ are induced from $f(x)$. If $\Phi_m(x)$ divides $f(x^e)$ and ζ_m is a primitive mth root of unity, then $f(\zeta_m^e) = 0$. Hence ζ_m^e is a root of $f(x)$. Suppose that ζ_m^e is a primitive nth root of unity, then $\Phi_n(x)$ divides $f(x)$. Furthermore $\Phi_m(x)$ divides $\Phi_n(x^e)$.

If c is the squarefree part of d, which is to say that c is the product of the distinct prime factors of d, then Proposition 4.2.5 implies that

$$\varphi[d] = \prod_{p|d} [p^{e_p}] - [p^{e_p-1}] = \prod_{p|d} [p^{e_p-1}]([p] - [1]) = [d/c]\varphi[c].$$

Hence $S_d(x) = [d/c]S_c(x) = S_c(x^{d/c})$. It follows that all cyclotomic factors of $M_d(x) = \frac{1}{d}S_d(x)$ are induced from cyclotomic factors of $M_c(x)$. □

Proposition 4.2.14 shows that $x^m - 1$ factors of $M_d(x)$ only depend on the prime factors of d up to congruence modulo m.

Definition 4.2.13. Say positive integers d and e are **primewise congruent modulo** m if

$$d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \qquad e = q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$$

for some $k \geq 1$ and primes p_i, q_i such that

1. $p_i \equiv q_i \bmod m$ for each i,
2. $p_i \neq p_j$ and $q_i \neq q_j$ for each $i \neq j$.

Proposition 4.2.14. *Let $m, d, e \geq 1$. If d is primewise congruent to e modulo m, then*

$$S_d(x) \equiv S_e(x) \bmod x^m - 1.$$

Proof. If d and e are primewise congruent modulo m, then $\varphi[d] \equiv \varphi[e] \bmod [m]$. It follows from $\varphi[d] = [S_d]$ and Proposition 4.2.1 that $S_d(x) \equiv S_e(x) \bmod x^m - 1$. □

Example 4.2.15. If d and e are primewise congruent modulo m, then $d \equiv e \bmod m$, but primewise congruence is strictly stronger. Theorem 4.2.14 requires primewise congruence.

For example, if $m = 6$ then $7 \equiv 25 \bmod 6$ but $S_7(x) \equiv x^7 - x \equiv 0 \bmod x^6 - 1$ while

$$S_{25}(x) \equiv x^{25} - x^5 \equiv x - x^5 \not\equiv 0 \bmod x^6 - 1.$$

Remark 4.2.16. Suppose p is a prime and d_k is a sequence of natural numbers such that d_k is primewise congruent to d_{k+1} modulo p^k for all $k \geq 1$. Then Theorem 4.2.14 implies that the sequence $S_{d_k}(x)$ converges in the projective limit $\varprojlim \mathbb{Z}[x]/(x^{p^k} - 1)$. This limit can be interpreted as an "analytic function on pth power roots of unity," (see Habiro [41].) We save the study of these limits for future work.

The next result gives a simple necessary condition for $x^m - 1$ to divide $M_d(x)$.

Proposition 4.2.17. *If $x^m - 1$ divides $M_d(x)$, then m divides $\varphi(d)$.*

Proof. Consider the $\mathbb{Z}$-module map $\Psi[m] \to \mathbb{Z}/(m)$ determined by $[a] \mapsto a$ for all $a \in \mathbb{N}$. Proposition 4.2.5 implies that $\varphi[d] \mapsto \varphi(d)$ under this map. Since $x^m - 1$ dividing $M_d(x)$ is equivalent to $\varphi[d] \equiv 0 \bmod [m]$, it follows that $\varphi(d) \equiv 0 \bmod m$ is a necessary condition. □

Example 4.2.18. Let $d = 15$ and $m = 8$. Then $\varphi(15) = 8$, but

$$S_{15}(x) = x^{15} - x^5 - x^3 + x \equiv x^7 - x^5 - x^3 + x \not\equiv 0 \bmod x^8 - 1.$$

Hence m dividing $\varphi(d)$ is not a sufficient condition.

4.2.3 Minimal cyclotomic factors

Proposition 4.2.10 implies that cyclotomic factors of $M_d(x)$ are inherited by $M_{de}(x)$. We say that $x^m \pm 1$ **minimally divides** $M_d(x)$ if it divides $M_d(x)$ but not $M_e(x)$ for any e dividing d. In this section we initiate the study of minimal cyclotomic factors. The first case to consider is when $d = p$ is prime.

Proposition 4.2.19. *Let $m, d \geq 1$.*

1. *If d has a prime factor p such that $p \equiv 1 \bmod m$, then $x^m - 1$ divides $M_d(x)$.*
2. *$x^m - 1$ minimally divides $M_p(x)$ for a prime p if and only if $p \equiv 1 \bmod m$.*

Proof. 1. If $p \equiv 1 \bmod m$, then $[p] \equiv [1] \bmod [m]$ and thus $\varphi[d] \equiv 0 \bmod [m]$ by Proposition 4.2.5.

2. Since $S_p(x) = x^p - x = x(x^{p-1} - 1)$ we see that $x^m - 1$ divides $S_p(x)$ if and only if m divides $p - 1$, which is to say that $p \equiv 1 \bmod m$. □

Example 4.2.20. If $d = 35 = 5 \cdot 7$, then Proposition 4.2.19 implies that $M_{35}(x)$ is divisible by

$$x^4 - 1 = \Phi_4(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \quad \text{and} \quad x^6 - 1 = \Phi_6(x) \cdot \Phi_3(x) \cdot \Phi_2(x) \cdot \Phi_1(x).$$

In fact we have

$$M_{35}(x) = f(x) \cdot \Phi_6(x) \cdot \Phi_4(x) \cdot \Phi_3(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \cdot x,$$

where $f(x) \in \frac{1}{35}\mathbb{Z}[x]$ is an irreducible, non-cyclotomic polynomial of degree 26.

Proposition 4.2.21. *Let $m \geq 2$.*

1. *If p and q are distinct primes, then there are no m for which $x^m - 1$ minimally divides $M_{pq}(x)$.*
2. *If p and q are distinct primes and $x^m + 1$ minimally divides $M_{pq}(x)$, then $p, q \not\equiv 1 \bmod 2m$ and*

$$pq \equiv 1 + m \bmod 2m$$
$$p \equiv q + m \bmod 2m$$

   For example, if $p = m - 1$ and $q = 2m - 1$ are prime then they satisfy the above congruences.
3. *If p, q, r are distinct primes such that*

$$p^2 \equiv q^2 \equiv r^2 \equiv 1 \bmod m$$
$$pqr \equiv 1 \bmod m$$
$$p, q, r \not\equiv 1 \bmod m,$$

then $x^m - 1$ minimally divides $M_{pqr}(x)$.

Proof. 1. If $x^m - 1$ divides $M_{pq}(x)$, then $\varphi[d] = [pq] - [p] - [q] + [1] \equiv 0 \bmod [m]$. By considering the signs of the coefficients of $\varphi[d]$ we see that either p or q must be congruent to 1 mod m. If $p \equiv 1 \bmod m$, then $x^m - 1$ divides $M_p(x)$, similarly for q, and thus in either case $x^m - 1$ does not minimally divide $M_{pq}(x)$.

2. If $x^m + 1$ minimally divides $M_{pq}(x)$, then $\varphi[d] = [pq] - [p] - [q] + [1] \equiv 0 \bmod [m]_{\pm}$. If p or q were congruent to 1 mod $2m$, then $x^m + 1$ is not a minimal divisor. Therefore, the only way for $\varphi[d] \equiv 0 \bmod [m]_{\pm}$ is for $pq \equiv 1 + m \bmod 2m$ so that $[pq] + [1] \equiv 0 \bmod [m]_{\pm}$, and for $p \equiv q + m \bmod 2m$ so that $[p] + [q] \equiv 0 \bmod [m]_{\pm}$.

3. Similar to the analysis in the previous two cases one can check that these congruences do imply that $\varphi[d] \equiv 0 \bmod [m]$ and force $x^m - 1$ to be minimal. □

Remark 4.2.22. For a fixed m, Dirichlet's theorem on primes in arithmetic progressions [57, Pg. 167] implies that if we can find classes in $\mathbb{Z}/(m)^\times$ which satisfy the congruences in Proposition 4.2.21, then there will be infinitely many primes in those residue classes. Hence, in general, classifying the d which are a product of k distinct primes such that $x^m \pm 1$ minimally divides $M_d(x)$ reduces to solving a single congruence equations in $\mathbb{Z}/(m)^\times$.

Example 4.2.23. If $m = 3$, then for any prime $p \equiv 5 \bmod 6$ the primes 2 and p satisfy the congruences of Proposition 4.2.21 (2). Hence if $p = 5$, it follows that $x^3 + 1 = \Phi_6(x) \cdot \Phi_2(x)$ minimally divides $M_{10}(x)$. In fact

$$M_{10}(x) = \tfrac{1}{10}(x^3 + x^2 - 1) \cdot \Phi_6(x) \cdot \Phi_4(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \cdot x.$$

Example 4.2.24. Let $m = 15$. Then $4, 11, 14 \in \mathbb{Z}/(15)^\times$ satisfy the congruence conditions in Proposition 4.2.21 (3). The primes $11, 19, 29$ fall into these congruence classes, hence $x^{15} - 1$ minimally divides $M_d(x)$ when $6061 = 11 \cdot 19 \cdot 29$.

Example 4.2.25. Proposition 4.2.21 provides the first families of examples of minimal cyclotomic factors but is far from exhaustive. If $m = 10$ and $p, q, r = 3, 13, 19$, then these primes do not satisfy the congruences of Proposition 4.2.21 (3) but one can check that $x^{10} + 1$ minimally divides $M_d(x)$ where $d = 741 = 3 \cdot 13 \cdot 19$.

In would be interesting to know the extent to which all minimal cyclotomic factors can be classified into families defined by congruences as in Proposition 4.2.21. We leave this for future work.

4.2.4 Local cyclotomic factors of necklace polynomials

The product formula for $\varphi[d]$ allows us to determine when $x^m - 1$ divides $S_d(x)$ modulo a prime ℓ. Note that this is equivalent to ℓ dividing $S_d(x)$ modulo $x^m - 1$.

Theorem 4.2.26. *Let $m \geq 1$ and suppose that $a \bmod m$ has multiplicative order dividing ℓ^k for some prime ℓ and $k \geq 1$. If d has at least $j\ell^k$ distinct prime factors p such that $p \equiv a \bmod m$, then ℓ^j divides $S_d(x) \bmod x^m - 1$.*

Proof. Proposition 4.2.5 gives the factorization

$$\varphi[d] = \prod_{p|d} [p^{e_p - 1}]([p] - [1]).$$

Our assumption on the divisors of d implies that $\varphi[d]$ has a factor of $([a] - [1])^{j\ell^k}$ modulo $[m]$. Reducing coefficients modulo ℓ we see that

$$([a] - [1])^{\ell^k} \equiv [a^{\ell^k}] - [1] \equiv 0 \bmod \ell.$$

Hence $([a] - [1])^{\ell^k}$ is divisible by ℓ in $\Psi[m]$. Therefore $S_d(x) = \varphi[d]x$ is divisible by ℓ^j modulo $x^m - 1$ by Corollary 4.2.2 (1). □

Example 4.2.27. Let $m = 3$ and $\ell = 2$. Consider $d = 2 \cdot 5 \cdot 11 \cdot 17 \cdot 23 \cdot 29 = 1247290$. All six of the prime factors of d are congruent to 2 mod 3 which has multiplicative order 2. Hence, in the notation of Theorem 4.2.26, $j = 3$ and it follows that 2^3 divides $S_d(x) \bmod x^3 - 1$. If ω is a primitive 3rd root of unity, then we can also conclude that $S_d(\omega)$ is divisible by 8 in $\mathbb{Z}[\omega]$. The divisibility of Theorem 4.2.26 is not sharp; for example,

$$S_d(x) \equiv 2^5(x - x^2) \bmod x^3 - 1.$$

Recall that

$$\Phi_d(x) = \prod_{e|d} (x^{d/e} - 1)^{\mu(e)}.$$

Taking logarithms we get

$$\log \Phi_d(x) = \varphi[d] \log \Phi_1(x) = \varphi[d] \log(x - 1). \tag{4.7}$$

Proposition 4.2.8 shows that cyclotomic factors of $M_d(x)$ imply cyclotomic factors of $\varphi[d]f(x)$. This result does not directly apply to $\log \Phi_d(x) = \varphi[d] \log(x-1)$ since $\log(x-1)$ is not a polynomial; convergence issues arise when trying to define the quotient of the power series ring by $x^m - 1$. Nevertheless, we recover the following result.

Proposition 4.2.28. *Suppose that $m, d > 1$ and $x^m - 1$ divides $M_d(x)$, then $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$.*

Proof. If c is the squarefree part of d, then $\Phi_d(x) = \Phi_c(x^{d/c})$ and it follows that all cyclotomic factors of $\Phi_d(x) - 1$ are induced (in the sense of Definition 4.2.11) from cyclotomic factors of $\Phi_c(x) - 1$. Therefore, by Proposition 4.2.12, it suffices to prove the result for d squarefree.

Proposition 4.2.1 implies that $x^m - 1$ dividing $M_d(x)$ is equivalent to $\varphi[d] \equiv 0 \bmod [m]$. Thus

$$0 \equiv \sum_{e|d} \mu(e)[d/e] \equiv \sum_{0 \le a < m} n_a[a] \bmod [m],$$

where

$$n_a = \sum_{\substack{e|d \\ d/e \equiv a \bmod m}} \mu(e).$$

Therefore $n_a = 0$ for each $0 \le a < m$. Note that if $a \equiv b \bmod m$, then

$$\frac{x^a - 1}{x - 1} \equiv \frac{x^b - 1}{x - 1} \bmod \frac{x^m - 1}{x - 1}.$$

Consider the product formula for $\Phi_d(x)$ with $d > 1$,

$$\Phi_d(x) = \prod_{e|d} (x^{d/e} - 1)^{\mu(e)} = \prod_{e|d} \left(\frac{x^{d/e} - 1}{x - 1} \right)^{\mu(e)},$$

where the last equality follows from $\sum_{e|d} \mu(e) = 0$ whenever $d > 1$. Reducing modulo $\frac{x^m-1}{x-1}$ we have

$$\Phi_d(x) \equiv \prod_{0 \le a < m} \prod_{\substack{e|d \\ d/e \equiv a \bmod m}} \left(\frac{x^a - 1}{x - 1} \right)^{\mu(e)} \equiv \prod_{0 \le a < m} \left(\frac{x^a - 1}{x - 1} \right)^{n_a} \equiv 1 \bmod \frac{x^m - 1}{x - 1}. \qquad \square$$

Example 4.2.29. In Example 4.2.24 we showed that $x^{15} - 1$ divides $M_{6061}(x)$. Theorem 4.2.28 implies that $\frac{x^{15}-1}{x-1}$ divides $\Phi_{6061}(x) - 1$.

Example 4.2.30. Since $\log(x - 1)$ is not an odd power series we should not expect factors of $M_d(x)$ of the form $x^m + 1$ to correspond to factors of $\Phi_d(x) - 1$. For example, in Example 4.2.23 we showed that $x^3 + 1$ divides $M_{10}(x)$, while $\Phi_{10}(x) - 1$ factors as

$$\Phi_{10}(x) - 1 = (x^2 + 1)(x - 1)x.$$

Theorem 4.2.28 may be interpreted as giving explicit relations between algebraic units in cyclotomic extensions. If $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$, then

$$\prod_{a \in (\mathbb{Z}/(d))^\times} (\zeta_m - \zeta_d^a) = 1,$$

where ζ_m and ζ_d are primitive m and dth roots of unity respectively. For more on cyclotomic units and their relations see Washington [94, Chp. 8] and Sinnott [83].

4.2.5 Trace of $M_d(\zeta_m)$

We conclude this section with a computation of the trace of $M_d(\zeta_m)$, where ζ_m is a primitive mth root of unity. Let $\mathrm{Tr}_m : \mathbb{Q}(\zeta_m) \to \mathbb{Q}$ be the $\mathbb{Q}$-linear trace function defined by

$\mathrm{Tr}_m(\alpha) := \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} \sigma(\alpha)$. Then we define $T(d, m)$ for positive integers $d, m \geq 1$ by

$$T(d, m) := \mathrm{Tr}_m(M_d(\zeta_m)) \in \mathbb{Q}.$$

Note that $T(d, m)$ is independent of the choice of primitive mth root of unity ζ_m since the trace is invariant under the action of Galois, which is transitive on primitive mth roots of unity.

Theorem 4.2.31. *For all $m, d \geq 1$ we have*

$$T(d, m) := \mathrm{Tr}_m(M_d(\zeta_m)) = \begin{cases} \mu(m/d) & \text{when } d \text{ divides } m \\ 0 & \text{otherwise.,} \end{cases}$$

where μ is the standard Möbius function.

Our proof of Theorem 4.2.31 uses results stated in Section 4.4.

Proof. The cyclotomic identity (see Theorem 4.4.3) is the following product formula for formal power series with coefficients in $\mathbb{Q}[x]$,

$$\frac{1}{1 - xt} = \prod_{d \geq 1} \left(\frac{1}{1 - t^d} \right)^{M_d(x)}.$$

Substituting $x = \zeta_m^k$ for each k gives

$$\frac{1}{1 - t^m} = \prod_{0 \leq k < m} \frac{1}{1 - \zeta_m^k t} = \prod_{0 \leq k < m} \prod_{d \geq 1} \left(\frac{1}{1 - t^d} \right)^{M_d(\zeta_m^k)}.$$

Switching the order of the product we have

$$\begin{aligned}\frac{1}{1-t^m} &= \prod_{d\geq 1}\left(\frac{1}{1-t^d}\right)^{\sum_{0\leq k<m} M_d(\zeta_m^k)} \\ &= \prod_{d\geq 1}\left(\frac{1}{1-t^d}\right)^{\sum_{e|m} \mathrm{Tr}_e(M_d(\zeta_e))} \\ &= \prod_{d\geq 1}\left(\frac{1}{1-t^d}\right)^{\sum_{e|m} T(d,e)}.\end{aligned}$$

Lemma 4.4.2 allows us to compare exponents on both sides of this equation to conclude that

$$\sum_{e|m} T(d,e) = \delta_{d,m},$$

where $\delta_{d,m} = 1$ if and only if $d = m$ and 0 otherwise. Applying Möbius inversion gives our conclusion,

$$T(d,m) = \sum_{e|m} \mu(m/e)\delta_{d,e} = \begin{cases}\mu(m/d) & \text{when } d \text{ divides } m \\ 0 & \text{otherwise.}\end{cases}$$ □

Since $M_d(x)$ is defined over $\mathbb{Q}$, if $M_d(\zeta_m) = 0$ for some primitive mth root of unity ζ_m, then $M_d(x)$ must vanish at all primitive nth roots of unity. Thus, if $\mathrm{Tr}_m(M_d(\zeta_m)) \neq 0$ it follows that $M_d(\zeta_m) \neq 0$. This provides a minor obstruction for cyclotomic factors of necklace polynomials.

Corollary 4.2.32. *If d is a divisor of m such that m/d is squarefree, then $M_d(\zeta_m) \neq 0$, or equivalently $\Phi_m(x)$ does not divide $M_d(x)$.*

Proof. If m/d is squarefree, then

$$\mathrm{Tr}_m(M_d(\zeta_m)) = \mu(m/d) \neq 0.$$

Therefore $M_d(\zeta_m) \neq 0$. □

Theorem 4.2.31 shows that $M_d(\zeta_m)$ approximately vanishes for all but finitely many d

where it presents an obstruction. Corollary 4.2.33 gives a simple vanishing criterion from Theorem 4.2.31.

Corollary 4.2.33. *If d does not divide m and $M_d(\zeta_m)$ is rational, then $M_d(\zeta_m) = 0$.*

Proof. If $M_d(\zeta_m)$ were rational, then $\mathrm{Tr}_m(M_d(\zeta_m)) = \varphi(m)M_d(\zeta_m)$. On the other hand, Theorem 4.2.31 implies that $\mathrm{Tr}_m(M_d(\zeta_m)) = 0$. Hence $M_d(\zeta_m) = 0$. □

In particular when $m = 1, 2$ the values of $M_d(\pm 1)$ are necessarily rational. Theorem 4.2.31 specializes in that case to give the following computation.

Corollary 4.2.34. *Let $M_d(x)$ be the dth necklace polynomial. Then,*

$$M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & d > 1. \end{cases} \qquad M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2. \end{cases}$$

We compute the evaluations $M_d(\pm 1)$ in two other ways as Corollary 4.4.4 and Corollary 4.6.8. It is, of course, easy to compute $M_d(\pm 1)$ directly from the explicit formula for $M_d(x)$ (see Lagarias [55, Lem. 2.2] where this evaluation is used in his construction of the z-splitting measure.) These alternative computations of $M_d(\pm 1)$ each offer a new perspective, and in the case of Corollary 4.6.8 a surprising geometric interpretation.

4.3 G-Necklace Polynomials

For any finite group G there is a polynomial $M_G(x)$ called the **G-necklace polynomial** such that if $G = C_d$ is the cyclic group of order d, then $M_{C_d}(x) = M_d(x)$ is the classic necklace polynomial. In this section we show that the cyclotomic factor phenomenon studied in Section 4.2 for $M_d(x)$ extends to $M_G(x)$ for all solvable groups G. Our main result is Theorem 4.3.2 stated below.

4.3.1 Constructing $M_G(x)$

Let X be a finite set and let X^G be the set of functions from G to X, or equivalently **X-colorings of G**. The group G acts on $f \in X^G$ by $(g \cdot f)(a) := f(g^{-1}a)$. For each

subgroup $K \subseteq G$ we define $S_{G,K}(X) \subseteq X^G$ to be the set of colorings with stabilizer K. If K is a subgroup of G, then the subset of all X-colorings of G with stabilizer containing K correspond naturally to X-colorings of the right cosets $K\backslash G$. Thus we have the decomposition G-sets,

$$X^{K\backslash G} \cong \bigsqcup_{K \subseteq H \subseteq G} S_{G,H}(X).$$

If X has x elements, then Möbius inversion with respect to the subgroup lattice of G [86, Prop. 3.7.1] implies that $|S_{G,K}(X)|$ is a polynomial in $x = |X|$ which we denote $S_{G,K}(x)$,

$$S_{G,K}(x) := \sum_{K \subseteq H \subseteq G} \mu(K, H) x^{[G:H]}, \tag{4.8}$$

where μ is the Möbius function of the subgroup lattice of G. When $K = 1$ is the trivial subgroup we write $S_G(X) := S_{G,1}(X)$ and

$$S_G(x) := S_{G,1}(x) = \sum_{H \subseteq G} \mu(H) x^{[G:H]}, \tag{4.9}$$

where $\mu(H) := \mu(1, H)$. Let $M_G(X)$ denote the set of G-orbits of elements in $S_G(X)$. The elements of $M_G(X)$ are called **primitive G-necklaces**. Then by the orbit-stabilizer theorem,

$$M_G(x) := |M_G(X)| = \frac{1}{|G|} S_G(x).$$

$M_G(x)$ is called the **G-necklace polynomial**. When $G = C_d$ is the cyclic group of order d, (4.9) specializes to the formula for $M_d(x)$

$$M_{C_d}(x) = \frac{1}{|C_d|} \sum_{H \subseteq C_d} \mu(H) x^{[C_d:H]} = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e} = M_d(x).$$

Hence the G-necklace polynomials generalize the classic necklace polynomials and $S_G(x) = |G| M_G(x)$ generalizes $S_d(x) = d M_d(x)$.

Dress and Siebeneicher [24] introduced the G-necklace polynomials in the course of constructing an isomorphism between the G-necklace algebra and the G-Burnside-Witt ring. In their work G is allowed to be any profinite group, but for simplicity we restrict

to finite groups. Oh [71] studied the G-necklace polynomials in depth, generalizing the functional identities (Theorem 4.2.7) established by Metropolis and Rota [63] for the classic necklace polynomials $M_d(x)$ to the G-necklace polynomials $M_G(x)$.

Example 4.3.1. Let $G = S_3$ be the 3rd symmetric group. If we divide an equilateral triangle into six regions by connecting each edge to the opposite vertex, then S_3 acts freely and transitively by reflections on the regions. Hence an X-coloring of the regions gives an element of X^{S_3}. The figure below illustrates 2-colorings of S_3 with stabilizers $H = 1, \langle(12)\rangle, \langle(123)\rangle$ respectively. Recall that the Möbius function of a poset P is defined

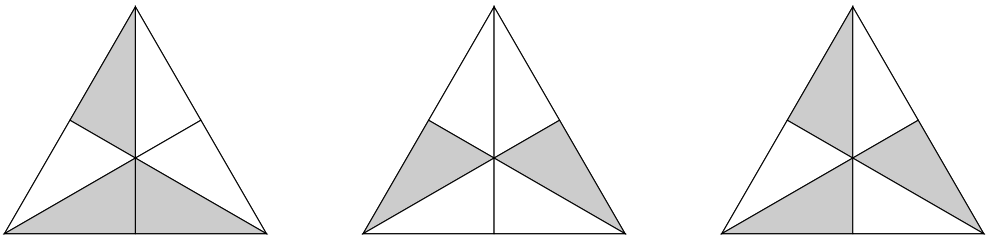


Figure 4.1: Primitive 2-colorings of S_3.

so that for each interval $[a, c]$ in P we have $\sum_{a\leq b\leq c} \mu(a, b) = 0$ unless $a = c$ in which case $\mu(a, a) = 1$. These conditions uniquely determine μ if P has finite intervals. Using (4.9) we compute

$$M_{S_3}(x) = \frac{1}{6}(x^6 - 3x^3 - x^2 + 3x).$$

Therefore there are $7 = M_{S_3}(2)$ primitive 2-colorings of S_3. Representatives of these colorings are depicted below.

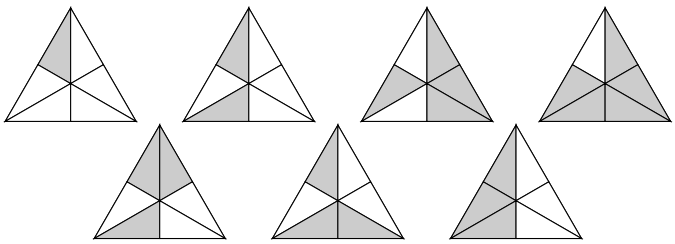


Figure 4.2: All primitive 2-colorings of S_3.

4.3.2 Cyclotomic factors of $M_G(x)$

Recall the Mahler algebra Ψ defined in Section 4.2.1 as the $\mathbb{Z}$-algebra generated by $[m]$ for $m \in \mathbb{N}$ such that $[m][n] = [mn]$. Theorem 4.3.2 shows how an expression of G as a solvable extension of a subgroup K corresponds to a factorization of $[S_G]$ in Ψ and hence to a functional equation relating $S_G(x)$ and $S_K(x)$.

Theorem 4.3.2. *Suppose G is a finite group with subgroup K and a chain of subgroups*

$$K = N_0 \triangleleft N_1 \triangleleft \dots N_k \triangleleft N_{k+1} = G$$

such that N_{i+1}/N_i is cyclic of prime order p_i. Let c_i be the number of non-trivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$.

1. *Let $S_G(x)$ be the polynomial defined in* (4.9)*, then*

$$S_G(x) = \Big(\prod_{i=0}^{k} [p_i] - c_i[1] \Big) S_K(x).$$

2. *If $c_i = 1$ for some i, then $x^{p_i - 1} - 1$ divides $S_G(x)$. If G is solvable and $K = 1$, then $c_0 = 1$ and this implies that $S_G(x)$ has cyclotomic factors.*

We first prove Lemma 4.3.3. This result, due to Oh [71, Thm. 3.6], generalizes an identity for $M_d(x)$ first proved by Metropolis and Rota [63, Thm. 3].

Lemma 4.3.3. *If $K \subseteq G$ is a subgroup, then*

$$S_K(x^{[G:K]}) = \sum_{K \cap H = 1} S_{G,H}(x).$$

Proof. The result follows by counting the elements of the restriction $\mathrm{Res}^G_K(X^G)$ with trivial stabilizer in two ways.

First note that as a left K-set G decomposes into $[G : K]$ copies of K corresponding to the right cosets $K\backslash G$. Hence we have the K-set isomorphisms,

$$\mathrm{Res}^G_K(X^G) \cong (X^K)^{[G:K]} \cong (X^{[G:K]})^K.$$

Therefore the number of elements of $\mathrm{Res}^G_K(X^G) \cong (X^{[G:K]})^K$ with trivial stabilizer is, by definition, $S_K(x^{[G:K]})$.

On the other hand, if f is an element of X^G with stabilizer H, then the stabilizer of f in $\mathrm{Res}^G_K(X^G)$ is $K \cap H$. Thus

$$S_K(x^{[G:K]}) = \sum_{K \cap H = 1} S_{G,H}(x). \qquad \square$$

Proof of Theorem 4.3.2. 1. Applying Lemma 4.3.3 to $G = N_{i+1}$ with subgroup $K = N_i$ we have

$$S_{N_i}(x^{p_i}) = \sum_{N_i \cap H = 1} S_{N_{i+1},H}(x),$$

hence

$$S_{N_{i+1}}(x) = S_{N_i}(x^{p_i}) - \sum_{\substack{N_i \cap H = 1 \\ H \neq 1}} S_{N_{i+1},H}(x). \tag{4.10}$$

Since $N_i \triangleleft N_{i+1}$ is a normal subgroup with cyclic quotient of prime order, any nontrivial subgroup $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$ must be cyclic of order p_i. By (4.8) we have

$$S_{N_{i+1},H}(x) = \sum_{H \subseteq J \subseteq N_{i+1}} \mu(H, J) x^{[N_{i+1}:J]}.$$

The second isomorphism theorem for groups [57, Pg. 17] implies that the interval of subgroups between H and N_{i+1} is isomorphic as a lattice to the subgroups of N_i and that $[N_{i+1} : J] = [N_i, N_i \cap J]$. Hence

$$S_{N_{i+1},H}(x) = \sum_{1 \subseteq J \subseteq N_i} \mu(J) x^{[N_i:J]} = S_{N_i}(x).$$

If c_i is the number of nontrivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$, then (4.10) simplifies to

$$S_{N_{i+1}}(x) = S_{N_i}(x^{p_i}) - c_i S_{N_i}(x) = ([p_i] - c_i[1]) S_{N_i}(x),$$

where $[p_i] - c_i[1] \in \Psi$ is an element of the Mahler algebra. The product formula then follows by induction on i.

2. If $c_i = 1$, then the factor $[p_i] - c_i[1]$ in the product formula for $S_G(x)$ vanishes in $\Psi[p_i - 1]$. Hence by Corollary 4.2.2 (1) it follows that $x^{p_i-1} - 1$ divides $S_G(x)$. If G is solvable and $K = N_0 = 1$, then N_1 is the only nontrivial subgroup of N_1 and $N_0 \cap N_1 = 1$. Hence $c_0 = 1$ and $S_G(x)$ is divisible by $x^{p_i-1} - 1$.

(3) This follows from (2) after reducing the coefficients in Ψ modulo $c_i - 1$. □

Example 4.3.4. If $G = C_{p^e}$ is cyclic of order p^e with $e > 1$ and $1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_e = C_{p^e}$ is a composition series, then each $p_i = p$ and $c_i = 0$ for all i except $c_0 = 1$. In this case Theorem 4.3.2 (1) simplifies to Proposition 4.2.5,

$$S_{C_{p^e}}(x) = ([p^e] - [p^{e-1}])x = \varphi[p^e]x.$$

Example 4.3.5. If $G = D_{2d}$ is the dihedral group of order $2d$, then the cyclic group $C_d \triangleleft D_{2d}$ is a normal subgroup of index 2. There are d elements of order 2 in D_{2d} not contained in C_d, hence Theorem 4.3.2 (1) implies that

$$S_{D_{2d}}(x) = ([2] - d[1])S_d(x) = S_d(x^2) - dS_d(x) = \sum_{e|d} \mu(e)(x^{2d/e} - dx^{d/e}).$$

Corollary 4.2.2 (1) implies that $x^m - 1$ divides $S_{D_{2d}}(x)$ whenever $x^m - 1$ divides $S_d(x)$. This does not hold for factors of $S_d(x)$ of the form $x^m + 1$ since 2 is even. For instance, in Example 4.2.23 we saw that $x^3 + 1$ divides $S_{10}(x)$, but

$$S_{D_{20}}(x) = x^{20} - 11x^{10} + 10x^5 - x^4 + 11x^2 - 10x = f(x)(x^2 + 1)(x + 1)(x - 1)x,$$

where $f(x)$ is an irreducible, non-cyclotomic polynomial of degree 15; hence $S_{D_{20}}(x)$ is not divisible by $x^3 + 1$.

Example 4.3.6. If $G = Q_8$ is the quaternion group, then Q_8 has a cyclic normal subgroup N of order 4 such that there are no nontrivial subgroups of Q_8 which intersect N trivially.

Thus Theorem 4.3.2 (1) and Proposition 4.2.5 imply that

$$S_{Q_8}(x) = [2]S_4(x) = x^8 - x^4 = x^4(x^2+1)(x+1)(x-1).$$

Example 4.3.7. If G is a finite abelian group, then G is a direct product of cyclic groups [58, Thm. 8.2],

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}.$$

Combining Theorem 4.3.2 (1) and Proposition 4.2.5 we find that

$$S_G(x) = \varphi[d_1]\varphi[d_2]\cdots\varphi[d_k]x,$$

hence if $x^m - 1$ divides $S_{d_i}(x)$ for some i, then $x^m - 1$ divides $S_G(x)$ by Corollary 4.2.2.

4.3.3 Möbius function of a solvable extension

Combining the explicit formula for $S_G(x)$ in (4.9) with the functional equations in Theorem 4.3.2 (1) we derive a relation between the value of the Möbius function of a group K and of a solvable extension G of K. An essentially equivalent version of this formula appears in Hawkes, Isaacs, Özaydin [47, Cor. 3.4]. They attribute this formula to Gaschütz [36], however we were unable to find a reference to it in his paper.

Theorem 4.3.8. *If G is a group with normal subgroup K such that G/K is solvable with composition series*

$$1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_{k+1} = G/K,$$

such that $[N_{i+1} : N_i] = p_i$ is prime with c_i non-trivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$, then

$$\mu(G) = (-1)^{k+1} c_0 c_1 \cdots c_k \mu(K).$$

Proof. Recall the formula (4.9) for $S_G(x)$,

$$S_G(x) = \sum_{H \subseteq G} \mu(H) x^{[G:H]}.$$

The coefficient of the linear term of $S_G(x)$ is $\mu(G)$. On the other hand Theorem 4.3.2 (1) gives the relation

$$S_G(x) = \Big(\prod_{i=0}^{k} [p_i] - c_i[1] \Big) S_K(x).$$

Comparing linear terms on each side of this equation we get

$$\mu(G) = (-1)^{k+1} c_0 c_1 \cdots c_k \mu(K). \qquad \square$$

When G is solvable and $K = 1$ Theorem 4.3.8 simplifies to

$$\mu(G) = (-1)^{k+1} c_0 c_1 \cdots c_k,$$

which appears in [47, Cor. 3.4].

4.4 Combinatorial Euler Products

Our main tool for the results in Sections 4.5 and 4.6 is a product formula for unital formal power series which we call the **combinatorial Euler product**. In this section we review the existence and uniqueness of combinatorial Euler products (Lemma 4.4.2); discuss their relation to number theory, combinatorics, and Witt vectors; and apply them to the evaluation of necklace polynomials (Corollary 4.4.4.)

4.4.1 Existence and uniqueness

Definition 4.4.1. A commutative ring R is called a **binomial ring** if

1. R is torsion free as an abelian group ($ma = 0$ with $m \in \mathbb{Z}$ and $a \in A$ implies $m = 0$ or $a = 0$,) and
2. For each $a \in R$ and $n \geq 0$, $\binom{a}{n} = \frac{1}{n!} a(a-1)(a-2)\cdots(a-n+1) \in R$.

Binomial rings were defined by Philip Hall [42] in his study of nilpotent groups. See Elliott [25] for an overview and further references on binomial rings. Examples of binomial rings include any localization of $\mathbb{Z}$, any $\mathbb{Q}$-algebra, and the ring of integer valued polynomials in $\mathbb{Q}[x]$.

Let

$$\left(\!\!\binom{x}{n}\!\!\right) := \frac{1}{n!}x(x+1)(x+2)\cdots(x+n-1) = \binom{x+n-1}{n}.$$

Recall that $\left(\!\!\binom{x}{n}\!\!\right)$ counts the number of subsets of size n chosen from a set of size x with repetition. The second condition of a binomial ring is equivalent to $\left(\!\!\binom{a}{n}\!\!\right) \in R$ for each $a \in R$ and $n \geq 0$ by the **combinatorial reciprocity identity** (see Stanley [85],)

$$\left(\!\!\binom{x}{n}\!\!\right) = (-1)^n \binom{-x}{n}. \tag{4.11}$$

Let R be a binomial ring and let $\Lambda(R) := 1 + tR[\![t]\!]$ be the set of unital formal power series with coefficients in R. We use $\left(\!\!\binom{x}{n}\!\!\right)$ to define an exponential action of R on certain elements of $\Lambda(R)$. In particular,

$$\left(\frac{1}{1-t}\right)^a := \sum_{n\geq 0} \left(\!\!\binom{a}{n}\!\!\right) t^n.$$

By (4.11) this identity is equivalent to the binomial theorem.

Lemma 4.4.2 is well-known in the context of formal power series, symmetric functions, and the theory of Witt vectors but is typically not stated in the generality which we technically require.[1] We prove it here for completeness.

Lemma 4.4.2. *For any binomial ring R and any sequence $a_d \in R$ for $d \geq 0$ such that $a_0 = 1$ there exists a unique sequence $b_j \in R$ for $j \geq 1$ such that the following identity holds in $\Lambda(R)$.*

$$\sum_{d\geq 0} a_d t^d = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right)^{b_j}. \tag{4.12}$$

Furthermore (4.12) *is equivalent to*

$$a_d = \sum_{\lambda \vdash d} b_\lambda$$

[1] Metropolis and Rota [63, Sec. 6, Prop. 1] mistakenly state this result for an arbitrary commutative ring; the correct version in terms of binomial rings appears in Elliott [25, Prop. 10.1].

where for a partition $\lambda = (1^{m_1}2^{m_2}\cdots)$

$$b_\lambda := \prod_{j\geq 1} \left(\!\!\binom{b_j}{m_j}\!\!\right). \tag{4.13}$$

Proof. The right hand side of (4.12) expands as

$$\prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{b_j} = \prod_{j\geq 1}\sum_{m\geq 0}\left(\!\!\binom{b_j}{m}\!\!\right)t^{mj} = \sum_{d\geq 0}\sum_{\lambda\vdash d} b_\lambda t^d.$$

We show by induction on d that there exists a uniquely determined sequence b_j such that for all $d \geq 1$,

$$a_d = \sum_{\lambda\vdash d} b_\lambda.$$

For $d = 1$ there is only partition λ and thus $a_1 = b_1$. Now suppose that $d > 1$ and that we have shown b_j is uniquely determined for $j < d$. Then

$$b_d = a_d - \sum_{\substack{\lambda\vdash d\\ \lambda\neq(d)}} b_\lambda.$$

If $\lambda \neq (d)$, then all parts of λ have size $j < d$ hence b_d is uniquely determined by our induction hypothesis. □

We call (4.12) the **combinatorial Euler product** factorization of the series $f(t) = \sum_{d\geq 0} a_d t^d$. This terminology was chosen to highlight a useful analogy which we discuss below.

4.4.2 Combinatorial Euler products in number theory

Classically an Euler product refers to a factorization of a Dirichlet series associated to prime ideals in a ring of integers. The essential example is the Euler product for the Riemann zeta function,

$$\zeta(s) := \sum_{n\geq 1}\frac{1}{n^s} = \prod_p \frac{1}{1-\frac{1}{p^s}}.$$

If V is a variety defined over a finite field $\mathbb{F}_q$, then the Hasse-Weil zeta function $\zeta_V(t) \in \Lambda(\mathbb{Z})$ associated to V is defined by

$$\zeta_V(t) := \exp\left(\sum_{d\geq 1} |V(\mathbb{F}_{q^d})| \frac{t^d}{d}\right) = \sum_{d\geq 0} |\mathrm{Sym}^d(V)(\mathbb{F}_q)| t^d,$$

where $\mathrm{Sym}^d(V)$ is the dth symmetric power of V. The Euler product for $\zeta_V(t)$ takes the form

$$\zeta_V(t) = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right)^{M_j(V)},$$

where $M_j(V)$ is the number of transitive Frobenius orbits on $V(\overline{\mathbb{F}}_q)$ with size j. This Euler product is an example of a combinatorial Euler product and is our motivation for the name.

4.4.3 Combinatorial Euler products in combinatorics

The combinatorial aspect of the combinatorial Euler product relates in part to an analogy between integers and partitions discussed in the paper [39] by Granville and further elaborated in the book [3] by Arratia, Barbour, and Tavaré: Just as every integer has a unique prime factorization, every partition has a unique "factorization" as $\lambda = (1^{m_1} 2^{m_2} \cdots)$. The "primes" in this setting are the natural numbers $j \geq 1$. The analog of the Riemann zeta function is the partition generating function; its combinatorial Euler product decomposition is the well-known identity

$$\sum_{d\geq 0} p(d) t^d = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right),$$

where $p(d)$ is the number of partitions of d.

4.4.4 Necklace rings and Witt vectors

For any commutative ring R Grothendieck [40] defined a ring structure on the unital formal power series $\Lambda(R)$. The addition in $\Lambda(R)$ is multiplication $f(t) \oplus g(t) := f(t)g(t)$ and the

product is uniquely determined by

$$\frac{1}{1-at} \otimes \frac{1}{1-bt} := \frac{1}{1-abt},$$

where $a, b \in R$. The ring $\Lambda(R)$ is isomorphic to the ring of big Witt vectors $W(R)$. See the unpublished notes of Lenstra [59] for a nice proof that $\Lambda(R)$ forms a ring with these operations and that $\Lambda(R)$ is canonically isomorphic to $W(R)$ as it is classically defined.

Metropolis and Rota [63, Sec. 6, Prop. 1] use the combinatorial Euler product formula to give an isomorphism between $\Lambda(\mathbb{Z})$ with Grothendieck's ring structure and the **necklace ring** $\mathrm{Nr}(\mathbb{Z})$. Dress and Siebeneicher [24] give a combinatorial construction of the necklace ring $\mathrm{Nr}(\mathbb{Z})$ as the Burnside ring of almost finite C-sets $\widehat{\Omega}(C)$, where C is the infinite cyclic group. A set X with an action of C is called an **almost finite C-set** if for each subgroup C^j of C, the set $M_j(X)$ of orbits with stabilizer C^j is finite. Then the Burnside ring of almost finite C-sets is the complete topological ring generated by classes $[X]$ for each isomorphism class of almost finite C-set X with relations

$$[X \sqcup Y] = [X] + [Y] \qquad [X \times Y] = [X][Y]$$

when X and Y are almost finite C-sets. If $[j] \in \widehat{\Omega}(\mathbb{Z})$ represents the class of the transitive C-set with j elements, then each $[X] \in \widehat{\Omega}(\mathbb{Z})$ has a unique expression as

$$[X] = \sum_{j \geq 1} |M_j(X)|[j].$$

The isomorphism between $\widehat{\Omega}(C)$ and $\Lambda(\mathbb{Z})$ is given by

$$[X] \longmapsto \prod_{j \geq 1} \left(\frac{1}{1-t^j}\right)^{|M_j(X)|}, \tag{4.14}$$

bringing us again to a combinatorial Euler product.

There is a close connection between this interpretation and the Euler product formula for the Hasse-Weil zeta function: if V is a variety over $\mathbb{F}_q$, then $V(\overline{\mathbb{F}}_q)$ is an almost finite C-set, where the cyclic action is given by the Frobenius automorphism of V. Hence

$[V(\overline{\mathbb{F}}_q)] \in \widehat{\Omega}(\mathbb{Z})$ and the map (4.14) sends $[V(\overline{\mathbb{F}}_q)]$ to $\zeta_V(t)$.

4.4.5 Cyclotomic identity

The necklace polynomials $M_d(x)$ arise in relation to an important combinatorial Euler product formula known as the **cyclotomic identity**.

Theorem 4.4.3 (Cyclotomic identity)**.** *The following identity holds in* $\Lambda(\mathbb{Q}[x])$*,*

$$\frac{1}{1-xt} = \prod_{j \geq 1} \left(\frac{1}{1-t^j} \right)^{M_j(x)}.$$

When $x = q$ is a prime power, Theorem 4.4.3 reduces to the Euler product formula for Hasse-Weil zeta function of $\mathbb{A}^1$ over $\mathbb{F}_q$. One may interpret this formula as an expression of the unique factorization of polynomials in $\mathbb{F}_q[x]$ into irreducibles. There are many proofs of the cyclotomic identity from different perspectives including number theory [78, Pg. 13], combinatorics [63, Sec. 5], and Lie theory [77, Lem. 3.2].

We close this section by applying the uniqueness of combinatorial Euler products (Lemma 4.4.2) to give a second computation of the values $M_d(\pm 1)$ for all $d \geq 1$.

Corollary 4.4.4. *Let* $M_d(x)$ *be the dth necklace polynomial. Then,*

$$M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & \textit{otherwise,} \end{cases} \qquad M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. 1. Evaluating the cyclotomic identity at $x = 1$ we have

$$\frac{1}{1-t} = \prod_{j \geq 1} \left(\frac{1}{1-t^j} \right)^{M_j(1)}.$$

On the other hand, by Lemma 4.4.2 we can compare exponents on both sides of this

equation to see that

$$M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & d > 1. \end{cases}$$

2. Evaluating the cyclotomic identity at $x = -1$ we have

$$\frac{1}{1+t} = \prod_{j \geq 1} \left(\frac{1}{1-t^j} \right)^{M_j(-1)}.$$

The left hand side can also be written

$$\frac{1}{1+t} = \frac{1-t}{1-t^2} = \left(\frac{1}{1-t} \right)^{-1} \left(\frac{1}{1-t^2} \right).$$

Comparing exponents with Lemma 4.4.2 we conclude

$$M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & \text{otherwise.} \end{cases}$$

□

In Section 4.5 we generalize the cyclotomic identity to a one parameter family of identities associated to the **higher necklace polynomials** $M_{d,n}(x)$. Our proof of Corollary 4.4.4 generalizes to the evaluation of higher necklace polynomials at certain roots of unity, including ± 1 (see Theorem 4.5.6.)

4.5 Higher Necklace Polynomials

Let K be a field and consider the polynomial ring $K[x_1, x_2, \ldots, x_n]$ in n variables.

Definition 4.5.1. A **monic polynomial** is a $K^\times$-orbit of non-zero polynomials in $K[x_1, x_2, \ldots, x_n]$. Let $\mathrm{Poly}_{d,n}(K)$ be the space of total degree d monic polynomials in $K[x_1, x_2, \ldots, x_n]$. Let $\mathrm{Irr}_{d,n}(K) \subseteq \mathrm{Poly}_{d,n}(K)$ be the subspace of K-irreducible polynomials.

In this section we study $\mathrm{Poly}_{d,n}(K)$ and $\mathrm{Irr}_{d,n}(K)$ when $K = \mathbb{F}_q$ is a finite field. Section

4.6 considers these spaces when $K = \mathbb{R}$ or $\mathbb{C}$. To keep track of the subscripts d and n note that d stands for the **d**egree of the polynomials and n stands for the **n**umber of variables.

If $K = \mathbb{F}_q$ is a finite field, then $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ is a finite set. In Chapter 3 we showed that the cardinality of $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ is a polynomial in q with rational coefficients. Note that $n = 1$ corresponds to the space of univariate polynomials and in that case $|\mathrm{Irr}_{d,1}(\mathbb{F}_q)| = M_d(q)$.

Definition 4.5.2. Suppose that $d, n \geq 1$.

1. Let $P_{d,n}(x) \in \mathbb{Q}[x]$ be the polynomial such that for any prime power q

$$P_{d,n}(q) = |\mathrm{Poly}_{d,n}(\mathbb{F}_q)|.$$

2. The **higher necklace polynomial** $M_{d,n}(x)$ is the polynomial with rational coefficients such that for any prime power q,

$$M_{d,n}(q) = |\mathrm{Irr}_{d,n}(\mathbb{F}_q)|.$$

The polynomial $P_{d,n}(x)$ is given explicitly by

$$P_{d,n}(x) := \frac{x^{\binom{d+n}{n}} - x^{\binom{d+n-1}{n}}}{x-1}, \tag{4.15}$$

(see Lemma 3.2.1.) When the number of variables is $n = 1$ the higher necklace polynomials specialize to the classic necklace polynomials

$$M_{d,1}(x) = M_d(x) = \frac{1}{d}\sum_{e|d} \mu(e) x^{d/e}. \tag{4.16}$$

When $n > 1$ there is no known explicit formula for $M_{d,n}(x)$ analogous to (4.16). This makes it challenging to study the higher necklace polynomials directly. Instead we approach $M_{d,n}(x)$ indirectly using the following family of combinatorial Euler products.

Theorem 4.5.3. *For each $n \geq 1$ the following identity holds in $\Lambda(\mathbb{Q}[x]) := 1 + t\mathbb{Q}[x][\![t]\!]$,*

$$\sum_{d\geq 0} P_{d,n}(x) t^d = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right)^{M_{j,n}(x)}. \tag{4.17}$$

Proof. This identity is equivalent to $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ having unique factorization. More explicitly, for each partition $\lambda = (1^{m_1}2^{m_2}\cdots)$ of d define $P_{\lambda,n}(x)$ by

$$P_{\lambda,n}(x) := \prod_{j\geq 1} \left(\!\!\binom{M_{j,n}(x)}{m_j}\!\!\right).$$

The degrees of the $\mathbb{F}_q$-irreducible factors of a polynomial $f \in \mathrm{Poly}_{d,n}(\mathbb{F}_q)$ form a partition $\lambda \vdash d$ which we call the **factorization type** of f. Thus $P_{\lambda,n}(q)$ is the number of elements of $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ with factorization type λ. Since every element of $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ factors uniquely into $\mathbb{F}_q$-irreducibles, we have for each prime power q

$$P_{d,n}(q) = \sum_{\lambda\vdash d} P_{\lambda,n}(q). \tag{4.18}$$

Lemma 4.4.2 shows that (4.18) is equivalent to

$$\sum_{d\geq 0} P_{d,n}(q)t^d = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_{j,n}(q)}.$$

Finally, since this holds for all prime powers q the identity must hold as polynomials in x. □

Theorem 4.5.3 appears in the proof of Theorem 3.2.3 where we used it to study the x-adic convergence of $M_{d,n}(x)$ for d fixed as $n \to \infty$. The advantage of Theorem 4.5.3 is that it allows us to study the implicitly defined polynomial sequence $M_{d,n}(x)$ by way of the explicitly known polynomial sequence $P_{d,n}(x)$. When $n = 1$, $P_{d,n}(x) = x^d$ and Theorem 4.5.3 specializes to the classic cyclotomic identity (Theorem 4.4.3.)

The cyclotomic factor phenomenon studied for $M_d(x)$ in Section 4.2 extends, in part, to the entire family $M_{d,n}(x)$ of higher necklace polynomials. When $n > 1$ the polynomials $M_{d,n}(x)$ do not appear to satisfy functional equations similar to those satisfied by $M_d(x)$ and $M_G(x)$. This is reflected in the fact that for each fixed $n > 1$ we see fewer distinct cyclotomic factors as d varies. Our main result for this section is Theorem 4.5.6.

Definition 4.5.4. Let $b \geq 2$ and $n \geq 1$ be integers. A **balanced base b expansion of n** is

an expression

$$n = b^{k_1} - b^{k_2} + b^{k_3} - \ldots + b^{k_{i-1}} - b^{k_i},$$

where i is even and $k_1 > k_2 > k_3 > \ldots > k_i \geq 0$ is a decreasing sequence of integers and the coefficients on the right hand side alternate between ± 1 with an equal number of each sign. Equivalently, n has a balanced base b expansion if all of the base b digits of n are 0 or $b-1$,

$$n = (b-1)b^{\ell_1} + (b-1)b^{\ell_2} + \ldots + (b-1)b^{\ell_j}.$$

In that case, the balanced base b expansion of n is gotten by expanding each $(b-1)b^k = b^{k+1} - b^k$ and collecting coefficients. Not every $n \geq 1$ has a balanced base b expansion, but when they do exist they are unique.

Example 4.5.5. Every positive integer has a balanced base 2 expansion. For example the balanced base 2 expansion of $n = 13$ is

$$13 = 2^4 - 2^2 + 2^1 - 1.$$

Theorem 4.5.6. *Let p be a prime and let $n \geq 1$ be an integer such that*

$$n = \sum_{k \geq 0} a_k p^k$$

is the balanced base p expansion of n. If ζ_p is a primitive pth root of unity, then

$$M_{d,n}(\zeta_p) = \begin{cases} a_k & \text{if } d = p^k \\ 0 & \text{otherwise.} \end{cases}$$

Thus it follows that $\Phi_p(x)$ divides $M_{d,n}(x)$ for all but finitely many $d \geq 1$ whenever n has a balanced base p expansion.

Before proving Theorem 4.5.6 we prove two lemmas. If $m \geq 0$ is an integer, let

$$[m]_x := \frac{x^m - 1}{x - 1} = x^{m-1} + x^{m-2} + \ldots + x + 1.$$

Lemma 4.5.7. *If ζ is a non-trivial nth root of unity, then $[m]_\zeta$ depends only on m modulo n.*

Proof. If ζ is a nontrivial nth root of unity, then

$$[n]_\zeta = \zeta^{n-1} + \zeta^{n-2} + \ldots + \zeta + 1 = 0.$$

If $m = an + b$, then

$$\begin{aligned}
[m]_x &= \frac{x^{an+b} - 1}{x - 1} \\
&= x^b \cdot \frac{x^{an} - 1}{x - 1} + \frac{x^b - 1}{x - 1} \\
&= x^b \cdot \frac{x^{an} - 1}{x^n - 1} \cdot \frac{x^n - 1}{x - 1} + \frac{x^b - 1}{x - 1} \\
&= x^b [a]_{x^n} [n]_x + [b]_x.
\end{aligned}$$

Evaluating at $x = \zeta$ gives

$$[m]_\zeta = [b]_\zeta.$$

□

Lemma 4.5.8 is known as Lucas' congruence, due to Èdouard Lucas [61]. See Fine [32] for a quick proof.

Lemma 4.5.8. *If p is a prime and*

$$\begin{aligned}
m &= a_k p^k + a_{k-1} p^{k-1} + \ldots + a_1 p + a_0 \\
n &= b_k p^k + b_{k-1} p^{k-1} + \ldots + b_1 p + b_0
\end{aligned}$$

are the base p expansions of the natural numbers m and n (without assuming the leading coefficients are non-zero), then

$$\binom{m}{n} \equiv \binom{a_k}{b_k}\binom{a_{k-1}}{b_{k-1}} \cdots \binom{a_1}{b_1}\binom{a_0}{b_0} \bmod p.$$

We now prove Theorem 4.5.6.

Proof of Theorem 4.5.6. The polynomial $P_{d,n}(x)$ may be expressed as

$$P_{d,n}(x) = \frac{x^{\binom{d+n}{n}} - x^{\binom{d+n-1}{n}}}{x-1} = \left[\binom{d+n}{n}\right]_x - \left[\binom{d+n-1}{n}\right]_x. \tag{4.19}$$

Suppose that n has a balanced base p expansion and let ζ be a non-trivial pth root of unity. Then by Theorem 4.5.3,

$$\sum_{d\geq 0} P_{d,n}(\zeta)t^d = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_{j,n}(\zeta)}. \tag{4.20}$$

We evaluate $M_{d,n}(\zeta)$ by expressing the left hand side of (4.20) as a combinatorial Euler product in another way and then using the uniqueness of Lemma 4.4.2. Towards that end, let $Q(t) \in \Lambda(\mathbb{Q}(\zeta))$ be defined by

$$Q(t) := \sum_{d\geq 0}\left[\binom{d+n}{n}\right]_\zeta t^d.$$

Then by (4.19)

$$\begin{aligned}
\sum_{d\geq 0} P_{d,n}(\zeta)t^d &= \sum_{d\geq 0}\left(\left[\binom{d+n}{n}\right]_\zeta - \left[\binom{d+n-1}{n}\right]_\zeta\right)t^d \\
&= \sum_{d\geq 0}\left[\binom{d+n}{n}\right]_\zeta t^d - t\sum_{d\geq 1}\left[\binom{d+n-1}{n}\right]_\zeta t^{d-1} \\
&= Q(t) - tQ(t) \\
&= (1-t)Q(t).
\end{aligned}$$

Next we determine the coefficients of $Q(t)$. Say positive integers d and n are *p-complementary* if there is no p^k with a non-zero coefficient in the base p expansions of both d and n. If d and n are not p-complementary, suppose p^k is the smallest power of p common to the base p expansions of d and n. Then the coefficient of p^k in $d+n$ is 0 since

1. The coefficient of p^k in n is $p-1$ by our assumption that n has a balanced base p expansion.

2. The coefficient of p^k in d is at least 1.

3. The minimality of k implies there are no carries for smaller power p in the sum.

Thus Lucas' congruence (Lemma 4.5.8) implies that if d and n are not p-complementary, then

$$\binom{d+n}{n} \equiv 0 \bmod p$$

since the factor corresponding to p^k will be 0. Therefore, if d and n are not p-complementary, then by Lemma 4.5.7 we have

$$\left[\binom{d+n}{n}\right]_\zeta = 0.$$

Suppose d and n are p-complementary. Then for each k, the coefficient of p^k in the base p expansion of n is either 0 or $p-1$ by the assumption that n has a balanced base p expansion. In the first case the factor corresponding to p^k in Lucas' congruence is $\binom{d_k}{0} = 1$ where d_k is the coefficient of p^k in the base p expansion of d. In the latter case, note that if $0 \leq a < p$, then

$$\binom{a}{p-1} = \begin{cases} 0 & \text{if } a < p-1 \\ 1 & \text{if } a = p-1 \end{cases}. \tag{4.21}$$

Then Lucas' congruence and (4.21) imply that when d and n are p-complementary,

$$\binom{d+n}{n} \equiv 1 \bmod p.$$

Hence by Lemma 4.5.7,

$$\left[\binom{d+n}{n}\right]_\zeta = 1.$$

Combining these calculations we have

$$Q(t) = \sum_{d \geq 0} \left[\binom{d+n}{n}\right]_\zeta t^d = \sum_{\substack{d \text{ is } p\text{-comp.} \\ \text{to } n}} t^d.$$

The existence and uniqueness of base p expansions of natural numbers is equivalent to the

following product formula,

$$\frac{1}{1-t} = \sum_{d\geq 0} t^d = \prod_{k\geq 1} \sum_{a=0}^{p-1} t^{ap^k} = \prod_{k\geq 1} \frac{1-t^{p^{k+1}}}{1-t^{p^k}},$$

where the factor of $\frac{1-t^{p^{k+1}}}{1-t^{p^k}}$ contributes to the coefficient of t^d precisely when d is not p-complementary to p^k. If $n = (p-1)p^{k_1} + (p-1)p^{k_2} + \ldots + (p-1)p^{k_s}$ is the base p expansion of n, then

$$Q(t) = \sum_{\substack{d \text{ is } p\text{-comp.} \\ \text{to } n}} t^d = \frac{1}{1-t} \prod_{i=1}^{s} \frac{1-t^{p^{k_i}}}{1-t^{p^{k_i+1}}}.$$

Therefore

$$\sum_{d\geq 0} P_{d,n}(\zeta)t^d = (1-t)Q(t) = \prod_{i=1}^{s} \frac{1-t^{p^{k_i}}}{1-t^{p^{k_i+1}}} = \prod_{j\geq 1} \left(\frac{1}{1-t^{p^k}}\right)^{a_k},$$

where $n = a_\ell p^\ell + a_{\ell-1}p^{\ell-1} + \ldots + a_1 p + a_0$ is the balanced base p expansion of n. The uniqueness of combinatorial Euler products (Lemma 4.4.2) implies that $M_{p^k,n}(\zeta) = a_k$ and $M_{d,n}(\zeta) = 0$ when d is not a power of p. □

For a fixed n there are finitely many primes p for which n has a balanced base p expansion. Theorem 4.5.6 tells us that for each such prime p there are only finitely many d such that $M_{d,n}(\zeta_p) \neq 0$ for ζ_p a primitive pth root of unity. The only prime p for which $n = 1$ has a balanced base p expansion is $p = 2$ and this reflects the fact that $M_{d,1}(\zeta_p) = 0$ for all but finitely many d if and only if $p = 2$ (Corollary 4.4.4.)

For any integer $m \geq 1$ we have $[m]_0 = 1$. Thus (4.19) implies $P_{d,n}(0) = 0$ for all $d, n \geq 1$, hence $M_{d,n}(0) = 0$. Setting $x = 1$ gives $[m]_1 = m$, hence by (4.19)

$$P_{d,n}(1) = \binom{d+n}{n} - \binom{d+n-1}{n} = \binom{d+n-1}{d} = \left(\!\!\binom{n}{d}\!\!\right).$$

Therefore

$$\sum_{d\geq 0} P_{d,n}(1)t^d = \sum_{d\geq 0} \left(\!\!\binom{n}{d}\!\!\right) t^d = \left(\frac{1}{1-t}\right)^n.$$

Thus $M_{1,n}(1) = n$ and $M_{d,n}(1) = 0$ for $d > 1$. We record these computations in Proposition 4.5.9. In Section 4.6 we interpret the values of $M_{d,n}(\pm 1)$ as Euler characteristics.

Proposition 4.5.9. *For all $d, n \geq 1$, $M_{d,n}(0) = 0$ and*

$$M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We finish this section with a result on the family of formal power series

$$Z_n(x,t) := \sum_{d\geq 0} P_{d,n}(x)t^d$$

appearing in the generalized cyclotomic identity.

Theorem 4.5.10. *If $n \geq 1$, then the formal power series*

$$Z_n(x,t) = \sum_{d\geq 0} P_{d,n}(x)t^d$$

is a rational function in t with coefficients in $\mathbb{Q}[x]$ if and only if $n = 1$. However, for every root of unity ζ, $Z(\zeta, t)$ is a rational function in t with coefficients in $\mathbb{Q}(\zeta)$.

Proof. When $n = 1$ the series $Z_n(x,t)$ specializes to

$$Z_1(x,t) = \frac{1}{1-xt}.$$

If $n > 1$ and $Z_n(x,t)$ were a rational function in t with coefficients in $\mathbb{Q}[x]$, then the coefficient of t^d in $Z_n(x,t)$ would have leading term x^{cd} for some constant c. However, (4.15) shows that $P_{d,n}(x)$ has leading term of the form x^{cd^n} which for $n > 1$ implies that $Z_n(x,t)$ is not rational.

If $x = \zeta$ is an mth root of unity, then

$$P_{d,n}(\zeta) = \left[\binom{d+n}{n}\right]_\zeta - \left[\binom{d+n-1}{n}\right]_\zeta,$$

and by Lemma 4.5.7 the values of $P_{d,n}(\zeta)$ only depend on $\binom{d+n}{n}$ and $\binom{d+n-1}{n}$ modulo m. Hence the values of $P_{d,n}(\zeta)$ are periodic as functions of d. All formal power series with periodic coefficients are rational. □

4.6 Necklace values as Euler characteristics

Recall from Definition 4.5.1 the space $\mathrm{Poly}_{d,n}(K)$ of all total degree d monic polynomials in $K[x_1, x_2, \ldots, x_n]$ and the subspace $\mathrm{Irr}_{d,n}(K)$ of K-irreducible polynomials. When $K = \mathbb{R}$ or $\mathbb{C}$ the space $\mathrm{Poly}_{d,n}(K)$ has a natural topology inherited from the ambient projective space of all monic polynomials in $K[x_1, x_2, \ldots, x_n]$ with degree at most d, and thus $\mathrm{Irr}_{d,n}(K) \subseteq \mathrm{Poly}_{d,n}(K)$ inherits a subspace topology.

Definition 4.6.1. Say a topological space X is **tame** if the compactly supported singular cohomology $H_c^k(X, \mathbb{Q})$ (see Hatcher [46, Pg. 243]) is defined for all $k \geq 0$ and vanishes for all but finitely many k. If X is tame, then the **compactly supported Euler characteristic** $\chi_c(X)$ is

$$\chi_c(X) := \sum_{k \geq 0} (-1)^k \dim_{\mathbb{Q}} H_c^k(X, \mathbb{Q}).$$

When $K = \mathbb{R}$ or $\mathbb{C}$, the space $\mathrm{Irr}_{d,n}(K)$ may be constructed from projective spaces by cut-and-paste relations and is therefore tame. The main result of this section is Theorem 4.6.2 which shows that $\chi_c(\mathrm{Irr}_{d,n}(K))$ when $K = \mathbb{R}$ or $\mathbb{C}$ is given by $M_{d,n}(\pm 1)$.

Theorem 4.6.2. *Let $d, n \geq 1$ and let $M_{d,n}(x)$ be the higher necklace polynomial as defined in Definition 4.5.2. Then*

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad \chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1) = \begin{cases} a_k & \text{if } d = 2^k \\ 0 & \text{otherwise.} \end{cases}$$

where $n = \sum_{k \geq 0} a_k 2^k$ is the balanced binary expansion of n (see Definition 4.5.4.)

Remark 4.6.3. When one has a space V which can be defined over any field K such that the size of $V(\mathbb{F}_q)$ is given by a polynomial $F(x)$ evaluated at $x = q$, one hopes that the compactly supported Euler characteristic of $V(K)$ when $K = \mathbb{R}$ or $\mathbb{C}$ should be given by evaluating $F(x)$ at $x = \pm 1$. If V is a variety defined over $\mathbb{Z}$ this heuristic can be made precise by working with the Grothendieck ring of varieties (see Farb, Wolfson [29, 30, 31] or Vakil's notes [90].) Theorem 4.6.2 shows that this is the case for the space $\mathrm{Irr}_{d,n}$, although $\mathrm{Irr}_{d,n}$ is not a variety or even constructible in the Zariski topology, which presents a technical difficulty.

We first prove several lemmas. Lemma 4.6.4 describes the geometry of the space $\mathrm{Poly}_{d,n}(K)$.

Lemma 4.6.4. *Let K be a field. Then for all $d, n \geq 1$,*

1. *If $\mathrm{Poly}_{\leq d,n}(K)$ is the space of all non-zero monic polynomials in $K[x_1, x_2, \ldots, x_n]$ with degree at most d, then $\mathrm{Poly}_{\leq d,n}(K) \cong \mathbb{P}^{\binom{d+n}{n}-1}(K)$. The space $\mathrm{Poly}_{\leq d-1,n}(K)$ sits naturally inside of $\mathrm{Poly}_{\leq d,n}(K)$ and $\mathrm{Poly}_{d,n}(K)$ is the complement,*

$$\mathrm{Poly}_{d,n}(K) = \mathbb{P}^{\binom{d+n}{n}-1}(K) \setminus \mathbb{P}^{\binom{d+n-1}{n}-1}(K).$$

2. *If λ is a partition, let $m_j(\lambda)$ denote the number of parts of λ of size j. Unique factorization of polynomials over a field gives the decomposition*

$$\mathrm{Poly}_{d,n}(K) = \bigsqcup_{\lambda \vdash d} \prod_{j \geq 1} \mathrm{Sym}^{m_j(\lambda)}(\mathrm{Irr}_{j,n}(K)).$$

Proof. 1. Consider the K-vector space spanned by all monomials in n variables of degree at most d. By the classic stars-and-bars counting argument this space has dimension $\binom{d+n}{n}$. The projectivization of this vector space is, by definition, the space of all non-zero monic polynomials of degree at most d in $K[x_1, x_2, \ldots, x_n]$. Hence $\mathrm{Poly}_{\leq d,n}(K) \cong \mathbb{P}^{\binom{d+n}{n}-1}(K)$.

2. This follows immediately from the fact that any finitely generated polynomial ring over a field has unique factorization. □

Remark 4.6.5. Some caution is needed when interpreting the symmetric powers in Lemma

4.6.4 (2). That is, $\mathrm{Sym}^m(\mathrm{Irr}_{d,n}(K))$ should not be interpreted as $(\mathrm{Sym}^m \mathrm{Irr}_{d,n})(K)$ in the sense of scheme theory. For example, the irreducible degree one polynomials over K correspond to points on the affine line $\mathrm{Irr}_{1,1}(K) \cong \mathbb{A}^1(K)$; on one hand $\mathrm{Sym}^2 \mathbb{A}^1$ is a scheme defined over $\mathbb{Z}$ and as such is isomorphic to $\mathbb{A}^2$, hence $(\mathrm{Sym}^2 \mathrm{Irr}_{1,1})(\mathbb{R}) = \mathbb{A}^2(\mathbb{R})$ is the space of all degree 2 monic polynomials over $\mathbb{R}$. However $\mathrm{Sym}^2(\mathrm{Irr}_{1,1}(\mathbb{R}))$ is the collection all reducible quadratic polynomials of the form $(x-a)(x-b)$ with $a, b \in \mathbb{R}$.

Theorem 4.6.6, due to MacDonald [62], allows us to compute the Euler characteristic of a symmetric power of a space X in terms of the Euler characteristic of X. See Vakil's notes [90, Thm. 2.3] for a nice one line proof.

Theorem 4.6.6 (MacDonald)**.** *If X is a tame space, then so is $\mathrm{Sym}^m X$ and*

$$\chi_c(\mathrm{Sym}^m X) = \left(\!\!\binom{\chi_c(X)}{m}\!\!\right).$$

Equivalently, in $\Lambda(\mathbb{Z})$ we have

$$\sum_{d \geq 0} \chi_c(\mathrm{Sym}^d X) t^d = \left(\frac{1}{1-t}\right)^{\chi_c(X)}.$$

Finally Lemma 4.6.7 recalls some important well-known properties of the compactly supported Euler characteristic (see [90].) Note that property (2) fails for the non-compactly supported Euler characteristic.

Lemma 4.6.7. *Suppose that X and Y are tame spaces. Then*

1. $\chi_c(X \sqcup Y) = \chi_c(X) + \chi_c(Y)$,
2. $\chi_c(X \times Y) = \chi_c(X)\chi_c(Y)$,
3. $\chi_c(\mathbb{R}) = -1$ *and* $\chi_c(\mathbb{C}) = 1$,
4. *If $K = \mathbb{R}$ or $\mathbb{C}$, then $\chi_c(\mathbb{P}^{n-1}(K)) = [n]_{\chi_c(K)}$.*

Proof. The first three properties are well-known. To compute the Euler characteristic of

projective space we use

$$\mathbb{P}^{n-1}(K) = K^{n-1} \sqcup K^{n-2} \sqcup \ldots \sqcup K \sqcup 1,$$

where $1 = K^0$ is the one point space. Taking χ_c when $K = \mathbb{R}$ or $\mathbb{C}$ we have

$$\chi_c(\mathbb{P}^{n-1}(K)) = \chi_c(K)^{n-1} + \chi_c(K)^{n-2} + \ldots + \chi_c(K) + 1 = [n]_{\chi_c(K)}. \qquad \square$$

We now prove Theorem 4.6.2.

Proof of Theorem 4.6.2. Let $K = \mathbb{R}$ or $\mathbb{C}$. Then by Lemma 4.6.4 (2), Lemma 4.6.7, and MacDonald's Theorem 4.6.6 we have

$$\begin{aligned}\chi_c(\mathrm{Poly}_{d,n}(K)) &= \sum_{\lambda \vdash d} \prod_{j \geq 1} \chi_c(\mathrm{Sym}^{m_j}(\mathrm{Irr}_{j,n}(K))) \\ &= \sum_{\lambda \vdash d} \prod_{j \geq 1} \left(\!\!\binom{\chi_c(\mathrm{Irr}_{j,n}(K))}{m_j}\!\!\right).\end{aligned}$$

Lemma 4.4.2 implies that this is equivalent to

$$\sum_{d \geq 0} \chi_c(\mathrm{Poly}_{d,n}(K)) t^d = \prod_{j \geq 1} \left(\frac{1}{1-t^j}\right)^{\chi_c(\mathrm{Irr}_{j,n}(K))}.$$

On the other hand, Lemma 4.6.4 (1) and Lemma 4.6.4 show that

$$\begin{aligned}\chi_c(\mathrm{Poly}_{d,n}(K)) &= \chi_c(\mathbb{P}^{\binom{n+d}{n}-1}(K)) - \chi_c(\mathbb{P}^{\binom{n+d-1}{n}-1}(K)) \\ &= \left[\binom{n+d}{n}\right]_{\chi_c(K)} - \left[\binom{n+d-1}{n}\right]_{\chi_c(K)} \\ &= P_{d,n}(\chi_c(K)).\end{aligned}$$

The generalized cyclotomic identity (Theorem 4.5.3) gives

$$\sum_{d \geq 0} P_{d,n}(\chi_c(K)) t^d = \prod_{j \geq 1} \left(\frac{1}{1-t^j}\right)^{M_{j,n}(\chi_c(K))}.$$

Hence by the uniqueness of combinatorial Euler products we conclude that for all $d, n \geq 1$,

$$\chi_c(\mathrm{Irr}_{d,n}(K)) = M_{d,n}(\chi_c(K)).$$

Our result then follows from Lemma 4.6.7 (3), Proposition 4.5.9, and Theorem 4.5.6. □

4.6.1 Geometric computations of necklace values

Theorem 4.6.2 gives a geometric interpretation of $M_{d,n}(\pm 1)$. When $n = 1$ this leads to a "geometric computation" of $M_d(\pm 1)$.

Corollary 4.6.8. *Let $M_d(x)$ be the dth necklace polynomial. Then,*

$$M_d(1) = \begin{cases} 1 & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad M_d(-1) = \begin{cases} -1 & \text{if } d = 1 \\ 1 & \text{if } d = 2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. 1. Theorem 4.6.2 implies that $M_d(1) = \chi_c(\mathrm{Irr}_{d,1}(\mathbb{C}))$. Since $\mathbb{C}$ is algebraically closed, there are no $\mathbb{C}$-irreducible polynomials of degree $d > 1$. Hence $M_d(1) = 0$ for $d > 1$. On the other hand, every degree one polynomial is irreducible and thus $\mathrm{Irr}_{1,1}(\mathbb{C}) \cong \mathbb{C}$. Therefore $M_1(1) = \chi_c(\mathbb{C}) = 1$.

2. Theorem 4.6.2 implies that $M_d(-1) = \chi_c(\mathrm{Irr}_{d,1}(\mathbb{R}))$. Since $\mathbb{C}/\mathbb{R}$ is a degree 2 extension and $\mathbb{C}$ is algebraically closed, it follows that there are no $\mathbb{R}$-irreducible polynomials of degree $d > 2$. Thus $M_d(-1) = \chi_c(\mathrm{Irr}_{d,1}(\mathbb{R})) = 0$ for $d > 2$. As noted above, $\mathrm{Irr}_{1,1}(\mathbb{R}) \cong \mathbb{R}$ and thus $M_1(-1) = \chi_c(\mathbb{R}) = -1$.

Finally, there is a homeomorphism $\mathrm{Poly}_{2,1}(\mathbb{R}) \cong \mathbb{R}^2$ given by $x^2 + bx + c \mapsto (b, c)$ and $\mathrm{Irr}_{2,1}(\mathbb{R})$ corresponds to the open subspace $b^2 - 4c < 0$ with Euler characteristic 1. Hence $M_2(-1) = \chi_c(\mathrm{Irr}_{2,1}(\mathbb{R})) = 1$. □

As another example of this type of argument consider the space of degree 1 irreducible polynomials $\mathrm{Irr}_{1,n}(K)$. The space of monic linear polynomials is $\mathbb{P}^n$ minus a point $\mathbb{P}^0$ corresponding to the constant monic function 1. Since every degree 1 polynomial is

irreducible, we have

$$\chi_c(\mathrm{Irr}_{1,n}(\mathbb{C})) = \chi_c(\mathbb{P}^n(\mathbb{C})) - \chi_c(\mathbb{P}^0(\mathbb{C})) = (n+1) - 1 = n.$$

This agrees with Proposition 4.5.9 where we found that $M_{1,n}(1) = n$. On the other hand

$$\chi_c(\mathrm{Irr}_{1,n}(\mathbb{R})) = \chi_c(\mathbb{P}^n(\mathbb{R})) - \chi_c(\mathbb{P}^0(\mathbb{R})) = \frac{1+(-1)^n}{2} - 1 = \begin{cases} 0 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

This agrees with the evaluation of $M_{1,n}(-1)$ from Theorem 4.5.6 since the coefficient of 1 in the balanced binary expansion of n is 0 if n is even and -1 if n is odd.

Theorem 4.6.2 connects the evaluation of $M_{d,n}(x)$ at the second roots of unity to the geometry of the space $\mathrm{Irr}_{d,n}(K)$ of irreducible polynomials. When $n = 1$ our understanding of these spaces for $K = \mathbb{R}$ or $\mathbb{C}$ gives a geometric reason for cyclotomic factors $\Phi_m(x)$ of $M_d(x)$ with $m = 1, 2$. It would be interesting to know if there is some geometric or otherwise "motivic" explanation for the rest of the cyclotomic factors of $M_d(x)$.

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 $\deg(\tilde{f}_n) = \deg(f) = d_f$ 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.

For each $d \geq 1$, let $B_{f,d}$ denote the set of all maps $u : C_u \to \mathcal{D}$ with $\deg(u) = d$ where C_u is an irreducible curve such that if $u' : C'_u \to \mathcal{D}$ is the fiber product of u with f, then C'_u is irreducible of genus at most 1. 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 $u : C \to \mathcal{D}$ 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 $K(C)/K(\mathcal{D})$ is the compositum of all the conjugates of $K(C)$. The set of ramification indices over a point $p \in \mathcal{D}$ is the same in all conjugates of $K(C)$, 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 $u : C \to \mathcal{D}$ 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 $g(C_n) \leq 1$ 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 $g(C_n) \leq 1$ 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.

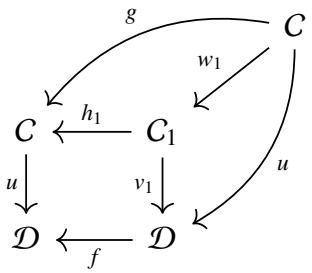
In particular, if u has irreducible fiber product with f, then u has Galois closure of genus at most 1.

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.

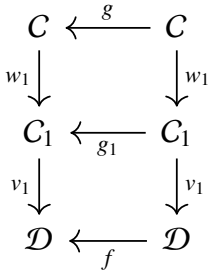
If the fiber product of u with f is reducible, then (5.7) factors through some irreducible component $v_1 : C_1 \to \mathcal{D}$ of the fiber product. It follows that $u = v_1 \circ w_1$ and $g = h_1 \circ w_1$

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 $u : C \to \mathcal{D}$ 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 $g(C_n) \leq 1$ 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 $h : C_{j+k} \to C_j$ defined over K such that $u_j \circ h = u_{j+k}$.*

Proof. Since u is f-stable with $g(C_n) \leq 1$ 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 $v : C \to \mathcal{D}$ 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 $u : \mathcal{C} \to \mathcal{D}$ and $f : \mathcal{D} \to \mathcal{D}$ be finite maps between irreducible curves defined over K. If* $\deg(f) \geq 2$ *and $p \in \mathcal{D}(K)$, then $\{n : f^n(p) \in u(\mathcal{C}(K))\}$ 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 $L = \{n : f^n(p) \in u(\mathcal{C}(K))\}$. 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 $u(\mathcal{C}(K))$ 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 $f^n(q) \in u(\mathcal{C}(K))$. It follows that the fiber product $\mathcal{C}_n$ has infinitely many K-rational points. Thus $g(\mathcal{C}_n) \leq 1$ for each $n \geq 0$ by Faltings' theorem.

Therefore u is f-stable and $g(\mathcal{C}_n) \leq 1$ 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 $p \in u_n(\mathcal{C}_n(K))$. 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 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 phenomenon 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

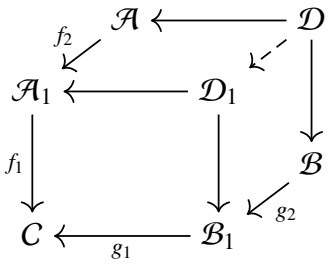
$$m' := \frac{m}{d-1} > d!^3 + \log_2(170d - 84)$$

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 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 $X \times Y$. □

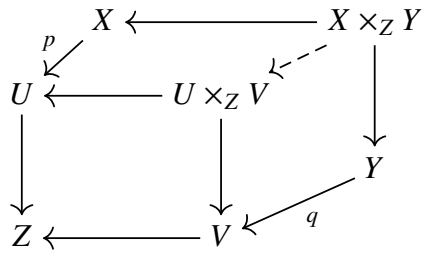
If $f : Y \to Z$ is a G-map, then for each $y \in Y$, there is an inclusion of stabilizer groups $G_y \subseteq G_{f(y)}$; we call the index $[G_{f(y)} : G_y]$ the *degree* of f at y, denoted $\deg_y(f)$. The degree depends only on the irreducible component of y. We define $\deg(f)$ to be the sum of 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

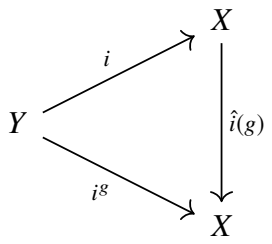
In this appendix we review first non-abelian group cohomology and its relation to twists in a general setting.

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.



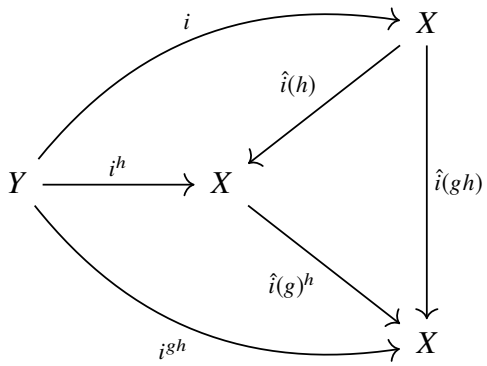
(5.8)

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

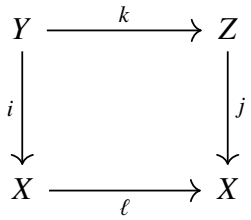
$$\hat{i}(gh) = \hat{i}(g)^h \circ \hat{i}(h) \qquad \text{(or equivalently } i^{gh-1} = i^{gh-h} \circ i^{h-1}.)$$

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

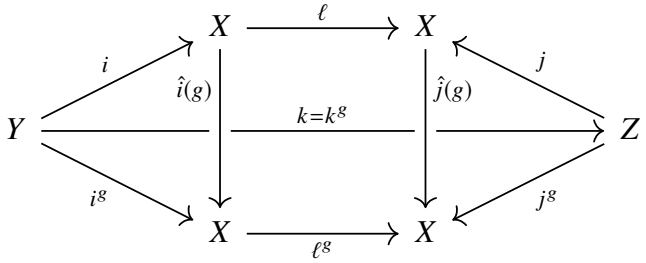
$\hat{i}(gh)$ in two ways:



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

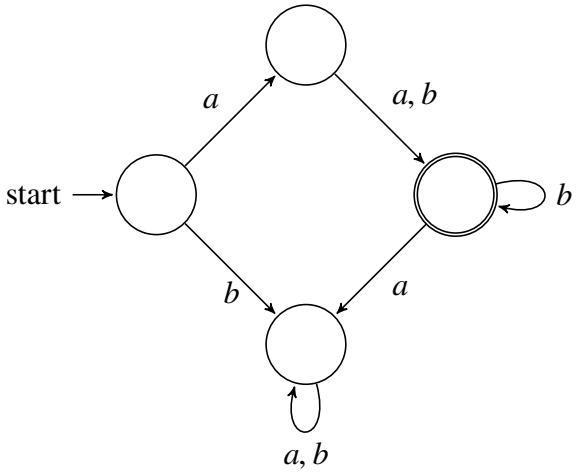
1. e is a disjunction $e = e_1|e_2$ where $e_1, e_2 \in \text{Reg}$,
2. e is a concatenation $e = e_1e_2$ where $e_1, e_2 \in \text{Reg}$, or
3. e is a *Kleene star* $e = e_1^*$ where $e_1 \in \text{Reg}$.

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 when 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 end and 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

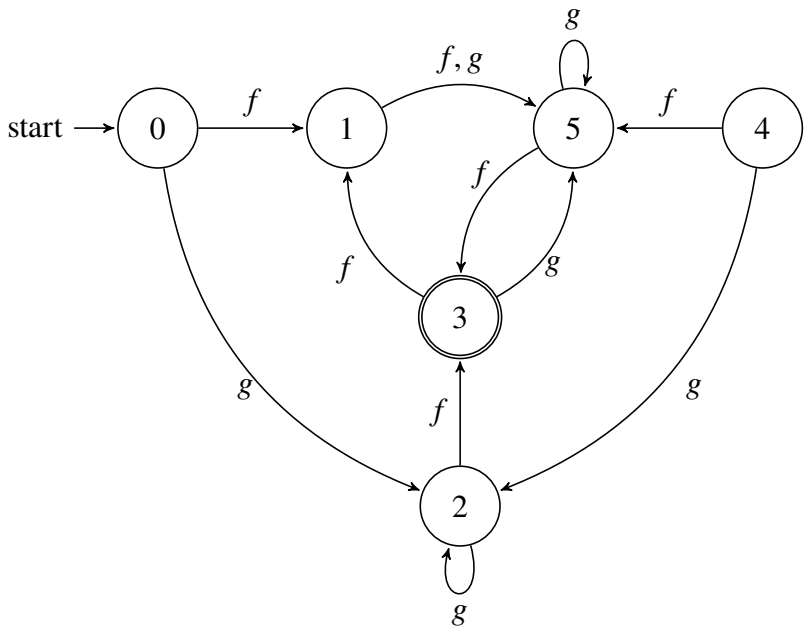
finitely generated, N is also finite. If $v : C_v \to \mathcal{D}$ represents a class in N, then $C_v(K)$ must be finite; if $C_v(K)$ were infinite, then Faltings' theorem implies that C_v has genus at most 1 and thus v would belong to M.

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, 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.