8-2010

On Conjectures Concerning Nonassociate Factorizations

Jason A Laska
laska@utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Jason A Laska entitled "On Conjectures Concerning Nonassociate Factorizations." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

David F. Anderson, Major Professor

We have read this dissertation and recommend its acceptance:

Shashikant Mulay, Pavlos Tzermias, Chauncey J. Mellor

Accepted for the Council:

Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:

I am submitting herewith a dissertation written by Jason Allen Laska entitled "On Conjectures Concerning Nonassociate Factorizations". I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

David F. Anderson

Major Professor

We have read this dissertation
and recommend its acceptance:

Shashikant Mulay

Pavlos Tzermias

Chauncey J. Mellor

Accepted for the Council:

Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with offical student records.)

On Conjectures Concerning Nonassociate Factorizations

A Dissertation

Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Jason Allen Laska

August 2010

Dedication

To friends and family near and far.

Acknowledgments

I would like to express my sincerest gratitude to my advisor, David F. Anderson. Without his initial push into the pool, I would have never realized how nice the water could be. I would also like acknowledge the advice, energy, and time of the entire dissertation committee: Shashikant Mulay, Pavlos Tzermias, and Jeff Mellor. Additionally, Adalbert Kerber and Carl Wagner graciously pointed me to valuable references and resources.

Abstract

We consider and solve some open conjectures on the asymptotic behavior of the number of different numbers of the nonassociate factorizations of prescribed minimal length for specific finite factorization domains. The asymptotic behavior will be classified for Cohen-Kaplansky domains in Chapter 1 and for domains of the form R=K+XF[X] for finite fields K and F in Chapter 2. A corollary of the main result in Chapter 3 will determine the asymptotic behavior for Krull domains with finite divisor class group.

Contents

1 Introduction **1**

2 Cohen-Kaplansky domains **5**

3 Domains of the form $R = K + XF[X]$ **17**

4 Krull Domains with finite class group **48**

5 Summary and Future Directions **68**

Bibliography **70**

Appendices **74**

A The First Appendix **75**

Vita **81**

Chapter 1

Introduction

This dissertation concerns commutative rings with a focus on multiplicative ideal theory and factorization. In general, the goal of research in this area is to classify to what extent the factorizations in an integral domain R behave like the factorizations in a unique factorization domain (UFD). Standard examples of UFDs include $\mathbb{Z}$ and $F[X]$ for a field F. An integral domain is called *atomic* provided that each nonzero, nonunit element is a finite product of irreducible elements. An atomic integral domain is called a *UFD* if whenever there exist irreducible elements α_i and β_j in R so that $x = \alpha_1\alpha_2\cdots\alpha_k = \beta_1\beta_2\cdots\beta_s$, then

1. $s = k$, and

2. up to reordering, each α_i is associated to β_i.

An atomic domain that is not a UFD is $R = \mathbb{Z}[\sqrt{-3}]$. Using a norm argument, it can be shown that $1 - \sqrt{-3}$, $1 + \sqrt{-3}$, and 2 are irreducible elements in R and that 1 and -1 are the only units of R. Moreover, 2 is not associated to $1 - \sqrt{-3}$ in R, and $4 = (1-\sqrt{-3})(1+\sqrt{-3}) = 2^2$. Thus $R = \mathbb{Z}[\sqrt{-3}]$ does not satisfy condition (2) above. It is shown in [31] that R satisfies condition (1) above. An atomic integral domain that satisfies condition (1) is called a *half factorial domain* (HFD). Carlitz demonstrated that the ring of integers in an algebraic number field with class number 2 is an HFD [11].

Let F be a field. Then $F[X^2, X^3]$ is an atomic domain that is not an HFD since $X^6 = (X^2)^3 = (X^3)^2$ and X^2 and X^3 are both irreducible elements. One way of measuring the degree to which an atomic domain is not an HFD is to describe restrictions on how an irreducible factorization of one length can be transfered to an irreducible factorization of another length. Formally, the *elasticity* of an atomic domain R is $\rho(R) = \sup\{\frac{m}{n} \mid \alpha_1\alpha_2\cdots\alpha_m = \beta_1\beta_2\cdots\beta_n$ for irreducible elements α_i and β_j in R $\}$ [1]. Then $1 \leq \rho(R) \leq \infty$, and $\rho(R) = 1 \iff R$ is an HFD. Valenza introduced the term elasticity in [29].

Some other articles concerning elasticity are listed below for throughness.

1. Elasticity of factorizations in integral domains [1].

2. Elasticity of factorizations in integral domains II [2].

3. Rational elasticity of factorizations in Krull domains [3].

4. Nonunique Factorization [17].

5. An inequality concerning the elasticity of Krull monoids with divisor class group $\mathbb{Z}_p$ [13].

Results on the elasticity of an atomic domain provide bounds for connections between lengths of factorizations, but fail to describe how the factorizations are distributed across the available lengths of factorizations. To address this question, we first collect some definitions for an atomic domain R. When the risk of confusion is low, the subscript R will be suppressed for ease of reading.

- $\eta_R(x)$ is the number of nonassociated irreducible factorizations of a nonzero, nonunit $x \in R$.

- $l_R(x) = \min\{j \mid x = s_1 s_2 \cdots s_j$ with each s_i an irreducible element of R $\}$ for a nonzero, nonunit $x \in R$. If $x \in R$ is a unit, let $l_R(x) = 0$.

- $\gamma_R(n) = \{x \mid x \in R$ with $l_R(x) = n\}$, where $n = 1, 2, 3, \ldots$.

- $\mu(R, n) = \{\eta_R(x) \mid x \in \gamma_R(n)\}$.

- $\Lambda(R, n) = |\mu(R, n)|$.

- $\overline{\Lambda}(R) = \lim_{n\to\infty} \frac{\Lambda(R,n)}{n}$.

For an atomic domain R, $\Lambda(R,n)$ describes the number of different numbers of nonassociate factorizations with minimum length n. If $\Lambda(R,n) = \infty$ for some n, then we define $\overline{\Lambda}(R) = \infty$. As such, we are interested in $\overline{\Lambda}(R)$ for the class of domains where $\eta(x) < \infty$ for all nonzero, nonunit elements $x \in R$. Such a domain is called a *finite factorization domain* (FFD) [4]. It is not yet known whether the limit $\overline{\Lambda}(R)$ always exists. This dissertation is focused on answering some questions about $\overline{\Lambda}(R) = \lim_{n\to\infty} \frac{\Lambda(R,n)}{n}$.

If R is a UFD, then $\overline{\Lambda}(R) = 0$ since by condition (2) in the definition of UFD , $\eta(x) = 1$ for every nonzero, nonunit $x \in R$. The quantity $\overline{\Lambda}(R)$ was defined by S.T. Chapman. The above preliminary results were published in [8], and investigation of similar problems in the monoid case has been done in [21] and [17]. For thoroughness, we collect information known about the quantity $\overline{\Lambda}(R)$.

1. [8, Theorem 18.2.3] Let $R = K + XF[[X]]$, where $K \subset F$ is a proper extension of fields. Then R is an HFD, but not a UFD. If F is finite, then $\overline{\Lambda}(R) = 0$. If F is infinite, then $\overline{\Lambda}(R) = \infty$.

2. [8, Theorem 18.2.7] Let R be a Krull domain with $Cl(R)$ finite. Then $\overline{\Lambda}(R) = 0$ if and only if R is a UFD.

3. [8, Theorem 18.3.1] Let R be an atomic integral domain and $S \subset R$ a multiplicative set generated by prime elements of R. Then $\overline{\Lambda}(R_S) \leq \overline{\Lambda}(R)$. Moreover, if S does not contain all the prime elements of R, then $\overline{\Lambda}(R_S) = \overline{\Lambda}(R)$.

4. [26, Lemma 4.4], [8] Let $R = \mathbb{F}_2 + X\mathbb{F}_4[X]$. Then $\overline{\Lambda}(R) = \frac{4}{3}$.

5. [26, Conjecture 4.8] Let $R = K + XF[X]$, where $K \subset F$ is a proper extension of finite fields such that $|F^*/K^*| = t$. Then $\overline{\Lambda}(R) = \frac{\sigma(t)}{t}$, where $\sigma(t)$ denotes the sum of the positive divisors of t.

6. [12] For Krull monoids with divisor class group $\mathbb{Z}_2$, an algorithm is described to determine $\eta(x)$.

This dissertation expands on the previous knowledge in the following ways.

1. In Chapter one, we demonstrate that if R has only finitely many irreducible elements up to associates (a Cohen-Kaplansky domain, or CK domain for short), then $\overline{\Lambda}(R) = 0$. This result expands on [8, Theorem 18.2.3] and [8, Example 18.2.5]. As a corollary to the techniques involved, some estimation results for the number of nonassociate irreducible elements in a CK domain will be computed.

2. In Chapter two, we verify [26, Conjecture 4.8]. The proof will deviate from the proof of a special case provided in [26] and the analogous recursive summation approach presented in [12]. Both of the previous approaches consider the connections between $\overline{\Lambda}(R)$ and integer partitions. The general case was tackled by recontexualizing the question in terms of generating functions of the q-binomial coefficients and a discrete Fourier Transform.

3. In Chapter three, we expand on the result [8, Theorem 18.2.7] and answer a conjecture in [8] that if R is a Krull domain with finite divisor class group, then either R is a UFD and $\overline{\Lambda}(R) = 0$, or R is not a UFD and $\overline{\Lambda}(R) = \infty$.

Unless otherwise noted, let the following definitions and conventions extend throughout the rest of the document. Let R denote an integral domain with $U(R)$ its group of units and R^* the collection of nonzero elements of R. Let $A(R)$ be the collection of irreducible elements (atoms) of R. Let $\mathbb{Z}^+$ and $\mathbb{N}$ denote the collection of positive integers and nonnegative integers respectively. When R is said to be a local domain, it will be intended that R is both local and Noetherian. Let $Max(R)$ denote the collection of maximal ideals of R. Let $\sigma(t)$ denote the sum of the divisors of the positive integer t, and let $\tau(t)$ denote the number of distinct positive divisors of t. Let $[R : \overline{R}] = \{x \in K \mid x\overline{R} \subseteq R\}$, where K is the quotient field of R and $\overline{R}$ is the integral closure of R . Let $\mathbb{F}_q$ be the finite field with q elements.

Chapter 2

Cohen-Kaplansky domains

Intuitively, if we are interested in the number of different numbers of nonassociate factorizations of an element with prescribed length, we ought to examine some cases where the number of nonassociate irreducible elements is small.

Recall [8, Example 18.2.5] that for the ring $R = \mathbb{F}_2[[X^2, X^3]]$, it is shown that $\overline{\Lambda}(R) = 0$. The proof involves using the order of the elements of R to construct a bound on the number of nonassociate factorizations that is independent of the length of the factorization. For the above R, it is known that there are only finitely many nonassociate irreducible elements. Indeed $\{x^2, x^2 + x^3, x^3, x^3 + x^4\}$ is a complete list of all nonassociate irreducible elements in R.

This example has only finitely many nonassociate irreducible elements and $\overline{\Lambda}(R) = 0$. The balance of this chapter will focus on atomic integral domains with only a finite number of nonassociate irreducible elements; such domains are called *Cohen-Kaplansky domains* (CK domains). These domains were introduced in [14] and elaborated upon in [6].

Indeed, we will prove the following theorem

Theorem. *Let R be a CK domain. Then $\overline{\Lambda}(R) = 0$.*

The main tool that drives the observations in this section is the idea of universality introduced in [6]. We provide the definition for emphasis.

Definition 2.0.1. Let R be an atomic domain. A subset S of R is called *universal* if each element of S is divisible by each atom of R.

Since $\overline{\Lambda}(R)$ is only an interesting topic in the context of finite factorization domains [8], the consideration of universality is restricted to the CK domain case. Indeed, if R is not a CK domain and if $S \subseteq R$ is universal, then infinitely many nonassociate irreducible atoms divide each element in S, and thus R is not a FFD. It is discussed in [6] that $R = \mathbb{R}+X\mathbb{C}[[X]]$ is an example of a local atomic domain such that $Max(R)^2$ is universal, but R is not a FFD.

Recall some results concerning CK domains.

Theorem. *[6] The following conditions are equivalent for an integral domain R.*

1. *R is a CK domain.*
2. *R is a one-dimensional semilocal domain and for each nonprincipal maximal ideal M of R, R/M is finite and R_M is analytically irreducible.*
3. *R is a one-dimensional semilocal domain with R/M finite for each nonprincipal maximal ideal M of R, $\overline{R}$ is a finitely generated R-module, and $|Max(R)| = \left|Max(\overline{R})\right|$.*
4. *$\overline{R}$ is a semilocal PID, $|Max(R)| = \left|Max(\overline{R})\right|$, and if M is a nonprincipal maximal ideal of R, then R/M is finite.*

In particular, if R is a local CK domain, then $\overline{R}$ is a DVR (i.e., a local PID). Let v denote the valuation associated with the DVR $\overline{R}$, and let $Max(\overline{R}) = \{(p)\}$. Since $M \subseteq M\overline{R} \subseteq (p)$, the valuation on $\overline{R}$ is well-defined on elements of M. Most of the proofs in this chapter will combine information obtained by the valuation with information concerning the universal set S.

Let us recall some previous results about universality and CK domains found in [14] and [6].

1. [14, Theorem 3] If the maximal ideal M in a local CK domain R has n irreducible elements ($n > 1$), then every element of M^{n-1} is divisible by every irreducible element of M.

2. [14, Corollary to Theorem 11] If a local CK domain has exactly a prime number of irreducible elements, then M^2 is universal.

3. [6, Theorem 5.5] Let (R, M) be a local CK domain with integral closure $(\overline{R}, (p))$. Suppose that $M\overline{R} = p^l\overline{R}$ and $[R : \overline{R}] = p^c\overline{R}$. Let u be the least positive integer $\geq \frac{3c-1}{l}$. Then M^u is universal.

4. [6, Corollary 5.6] If $[R : \overline{R}] = p^c\overline{R} = M$, then M^3 is universal and the number of nonassociate atoms of R is $c\left|U(\overline{R})/U(R)\right|$.

We aim to show that the spirit of the last two quoted results can be expanded to tackle the task of classifying $\overline{\Lambda}(R)$ in the CK domain case. We begin with a result that provides an upper bound on the number of nonassociate irreducible elements of a local CK domain R. Let $\widetilde{A}(R)$ denote a collection of nonassociate irreducible elements of R.

Proposition 2.0.2. *Let (R, M) be a local CK domain with M^u universal, $m := \left|\frac{U(\overline{R})}{U(R)}\right|$, and $t := \min\{v(x) \mid x \in A(R)\}$. Then $|\widetilde{A}(R)| \leq m[(u-2)t+1]$. Moreover if $u \geq 3$, then $|\widetilde{A}(R)| < m[(u-2)t+1]$.*

Proof. Suppose that $x \in A(R)$ satisfies $v(x)$ is minimal, for concreteness let $x = wp^t$ for $w \in U(\overline{R})$. Because M^u is universal by assumption, x^u is divisible by every irreducible of R. Let $z \in A(R)$ be arbitrary. Then $t \leq v(z) \leq ut - t$. There are at most $[(u-2)t+1]$ possible different valuations for irreducible elements of R. Moreover, there are at most m nonassociate irreducible elements in R with the same valuation [6, Corollary 5.6]. Indeed, if w_1 and w_2 are representatives of the same equivalence class of $\frac{U(\overline{R})}{U(R)}$, then w_1p^n and w_2p^n are associates in R. Thus $|\widetilde{A}(R)| \leq m[(u-2)t+1]$.

If $u - 1 \geq 2$, then there cannot be an irreducible of the form $y = w_{u-1}p^{(u-1)t}$, where $w_{u-1}U(R) = w^{u-1}U(R)$. If $w_{u-1}U(R) = w^{u-1}U(R)$, then $w_{u-1}^{-1}w^{u-1} \in U(R)$ and

$$w_{u-1}^{-1}w^{u-1}y = w_{u-1}^{-1}w^{u-1}w_{u-1}p^{(u-1)t} = w^{u-1}p^{(u-1)t} = (wp^t)^{(u-1)} = x^{u-1}.$$

Up to associates the irreducible y has a factorization into $u-1$ irreducible elements. Thus for $u \geq 3$, $|\widetilde{A}(R)| < m[(u-2)t+1]$. □

The above result demonstrates the general flavor of the results to come. We prove a converse of Corollary 5.6 in [6].

Corollary 2.0.3. *Let (R, M) be a local CK domain with M^3 universal, and let $|\widetilde{A}(R)| = cm$. Then $[R : \overline{R}] = p^c\overline{R} = M$.*

Proof. By Proposition 2.0.2, $|\widetilde{A}(R)| < m(t+1)$ since $u = 3$. By construction, $t \leq c$. Thus $tm \leq cm$. Therefore $tm \leq cm < m(t+1)$; so $t \leq c < t+1$. Thus $t = c$. Each irreducible of R is in the conductor, and hence $[R : \overline{R}] = p^c\overline{R} = M$. □

It is already known [6, Theorem 6.2] that if (R, M) is a local CK domain with M^2 universal, then R is an HFD. However, a proof of this result can be obtained as an easy consequence of the above estimate.

Corollary 2.0.4. *If (R, M) is a local CK domain with M^2 is universal, then R is an HFD.*

Proof. If $z \in A(R)$ is arbitrary and $t = \min\{\upsilon(x) \mid x \in A(R)\}$, then $t \leq \upsilon(z) \leq 2t - t$. Suppose that $s = x_1x_2\cdots x_n = y_1y_2\cdots y_m$ are irreducible factorizations of the nonzero, nonunit element $s \in R$. Then

$$\begin{aligned} tn &= t + t + \cdots + t \\ &= \upsilon(x_1) + \upsilon(x_2) + \cdots + \upsilon(x_n) \\ &= \upsilon(x_1x_2\cdots x_n) \\ &= \upsilon(y_1y_2\cdots y_m) \\ &= \upsilon(y_1) + \upsilon(y_2) + \cdots + \upsilon(y_m) \\ &= t + t + \cdots + t = tm. \end{aligned}$$

□

Recall the following result from [6, Theorem 6.2].

Theorem. *If (R, M) is a quasilocal atomic domain with M^2 universal, then R is an HFD.*

It is exactly the observations made in Corollary 2.0.4 that lead to the development of the estimation in the first place. The previous results focused on the special case where the CK domains under consideration were local. Proposition 2.0.2 can be extended to the nonlocal case.

Proposition 2.0.5. *Suppose that R is a CK domain with maximal ideals $\{M_1, \ldots, M_n\}$ and that for each $1 \leq i \leq n$, $m_i := \left|\frac{U(\overline{R_{M_i}})}{U(R_{M_i})}\right|$, $t_i := \min\{\upsilon(x) \mid x \in A(R_{M_i})\}$, and ${M_i}_{M_i}^{u_i}$ is universal. Then $|\widetilde{A}(R)| \leq \sum_{i=1}^{n} m_i[(u_i - 2)t_i + 1]$.*

Proof. By [14, Theorem 7], the localization of a CK domain at a maximal ideal M is a CK domain, and the irreducibles in the localization are the localizations of the irreducibles of R contained in M. Thus $\widetilde{A}(R) = \bigcup_{i=1}^{n} \widetilde{A}(R_{M_i})$. Recall [14, Theorem 1] that two maximal ideals of R cannot have an irreducible element in common. Thus the union is disjoint, and hence

$$|\widetilde{A}(R)| = \sum_{i=1}^{n} |\widetilde{A}(R_{M_i})| \leq \sum_{i=1}^{n} m_i[(u_i - 2)t_i + 1],$$

by Proposition 2.0.2. □

Remark 2.0.6. A more relaxed and informal bound can be obtained for a local domain R by stating that the number of nonassociate irreducible elements in $R \leq$ than the number of admissible valuations for the irreducible elements multiplied by the maximum number of irreducible elements per valuation. Let $V := \{\upsilon(\alpha) \mid \text{ for } \alpha \in A(R)\}$. Then $|\widetilde{A}(R)| \leq |V||U(\overline{R})/U(R)|$.

Instead of appealing to universality to create a bound on the number of permissible valuations for the irreducible elements of R, we may instead use properties of rings to force nice bounds. It was shown in [6] that

Proposition 2.0.7. *Suppose that (R, M) is a one-dimensional analytically irreducible local domain with R/M finite. Then R is a CK domain.*

Using Proposition 2.0.2 we show

Proposition 2.0.8. *A one-dimensional analytically irreducible local FFD is a CK domain.*

Proof. We show $|\widetilde{A}(R)| < \infty$ using 2 steps.

1. Show
$$|V := \{v(\alpha) \mid \text{ for } \alpha \in A(R)\}| < \infty.$$

2. Show that for each valuation in V, there exists only finitely many nonassociate irreducible elements with that valuation by verifying that $\left|U(\overline{R})/U(R)\right| < \infty$.

Since R is a one-dimensional, analytically irreducible, local (Noetherian) domain, $\overline{R}$ is a DVR, and $\overline{R}$ is a finitely generated R-module [27], [6]. Furthermore, since R is a one-dimensional local domain, R is analytically irreducible if and only if $V := \{v(\alpha) \mid \alpha \in A(R)\}$ is a bounded set; therefore $|V| < \infty$. By [6, Corollary 5.6], to each of these valuations there exists at most $|U(\overline{R})/U(R)|$ nonassociate factorizations of $x \in R$. The result is proved if $|U(\overline{R})/U(R)| < \infty$.

Suppose not and $\beta_i = w_i p^s$ are infinitely many nonassociate irreducible elements in R with valuation s, where p is the irreducible element in $\overline{R}$, and w_i are distinct coset representatives of $U(\overline{R})/U(R)$. Since $\overline{R}$ is a DVR with irreducible element p, $[R : \overline{R}] = p^l\overline{R}$ for some non-negative integer l. Consider the following possible factorizations of the element $y = (w_1 p^s)(p^l)$ in R.

Now to each $i \in \mathbb{Z}^+$,

$$y = (w_1 p^s)(p^l) = (w_i p^s)(w_1 w_i^{-1} p^l)$$

is an irreducible factorization of $y \in R$. Since the $w_i p^s$ terms were taken to be nonassociate, these factorizations are associate in R precisely when $w_1 w_i^{-1} \in U(R)$. If m is not finite, then $y = (u_1 p^s)(p^l)$ is divisible by an infinite collection of nonassociate irreducible elements, hence R is a not a FFD.

Thus $|V| < \infty$ and $|\frac{U(\overline{R})}{U(R)}| < \infty$. By the weakening of Proposition 2.0.2 , $|\widetilde{A}(R)| \leq |V| \left|U(\overline{R})/U(R)\right|$. Therefore R is a CK domain. $\square$

The above result could have been obtained by leaning more heavily on past results in the following manner.

Proposition 2.0.9. *A one-dimensional analytically irreducible local FFD is a CK domain.*

Proof. By [1, Theorem 2.12], if R is a one-dimensional, analytically irreducible, local domain, then V is a finite set. By [7, Corollary 3] and [20, Theorem 7], if R is Noetherian domain with $\overline{R}$ a finitely generated R module, then R is an FFD $\iff \frac{U(\overline{R})}{U(R)}$ is finite.

By the Proposition 2.0.2, $|\widetilde{A}(R)| \leq |V| \left|U(\overline{R})/U(R)\right|$, and hence R is a CK domain. □

The above estimates have been focused on the irreducible elements of R. We now focus on $\overline{\Lambda}(R)$.

Lemma 2.0.10. *Let (R, M) be a local CK domain, where $V := \{v(x) \mid x \in A(R)\}$, $\alpha :=$ $\max(V)$, $\beta := \min(V)$, and M^u is universal. Then if $l(y) = n \geq u$, $(n-(u-1))\alpha+(u-1)\beta \leq$ $v(y)$.*

Proof. By reordering, we can assume that $v(x_1) = \beta$ and $v(x_s) = \alpha$. Suppose that there exists a $z \in R$ with $l(z) = u$. Since $l(z) = u$ and M^u is universal, z is divisible by x_s, and $v(z) = \alpha + \sum_{n=1}^{u-1} a_i$, where each a_i satisfies $\beta \leq a_i \leq \alpha$. Thus if $l(z) = u$, then $v(z) \geq \alpha + (u-1)\beta$.

For $l(y) = n \geq u$, $v(y) = \sum_{j=1}^{n} b_j$, where $\beta \leq b_j \leq \alpha$. Below we collect u terms of the sum into brackets and reproduce the above argument. For each $1 \leq i \leq n-(u-1)$, there exists $b_{j,i}$ satisfying $\beta \leq b_{j,i} \leq \alpha$. Thus

$$
\begin{aligned}
\upsilon(y) &= \sum_{j=1}^{n} b_j = \left[\sum_{j=1}^{u} b_j\right] + \sum_{j=u+1}^{n} b_j \\
&= \left[\alpha + \sum_{j=1}^{u-1} b_{j,1}\right] + \sum_{j=u+1}^{n} b_j \\
&= \alpha + \left[\sum_{j=1}^{u-1} b_{j,1} + b_{u+1}\right] + \sum_{j=u+2}^{n} b_j \\
&= \alpha + \left[\alpha + \sum_{j=1}^{u-1} b_{j,2}\right] + \sum_{j=u+2}^{n} b_j \\
&= \cdots \\
&= (n-(u-1))\alpha + \sum_{j=1}^{u-1} b_{j,n-(u-1)} \geq (n-(u-1))\alpha + (u-1)\beta.
\end{aligned}
$$

□

Proposition 2.0.11. *If R be a local CK domain, then $\overline{\Lambda}(R) = 0$.*

Proof. Let y be an arbitrary element of R such that $l_R(y) = n$. Then $\upsilon(y) \leq n\alpha$. By [14, Theorem 3], there always exists $u \in \mathbb{Z}^+$ so that M^u is universal. Since we are considering the case where the minimal length of factorizations as n becomes arbitrarily large, we focus on the situation where $n > u$.

By the previous lemma, $|V_n := \{x \mid l(x) = n\}| \leq n\alpha - (n-(u-1))\alpha - (u-1)\beta + 1 = (u-1)(\alpha-\beta)+1$. By [6, Theorem 3.4], $\left|\frac{U(\overline{R})}{U(R)}\right| = m$. Thus admitting possible overcounting,

$$
\Lambda(R,n) = |\mu(R,n)| \leq |V_n| \left|\frac{U(\overline{R})}{U(R)}\right| \leq m((u-1)(\alpha-\beta)+1),
$$

and hence $\frac{\Lambda(R)}{n} \leq \frac{m((u-1)(\alpha-\beta)+1)}{n}$ for each $n \in \mathbb{Z}^+$. Thus

$$
\overline{\Lambda}(R) \leq \lim_{n\to\infty} \frac{m((u-1)(\alpha-\beta)+1)}{n} = 0.
$$

□

Theorem. *[10] Let R be a CK domain with $Max(R) = \{M_1, \ldots, M_s\}$. Define $\eta_i(z)$ to be the number of of nonassociate factorization into atoms of R_{M_i} of a nonzero $z \in R_{M_i}$. Then $\eta(x) = \prod_{i=1}^{s} \eta_i(x/1)$ for a nonzero $x \in R$.*

We can generalize the above result to nonlocal domains.

Theorem 2.0.12. *Let R be a CK domain. Then $\overline{\Lambda}(R) = 0$.*

Proof. As in the generalization of the local approximation result, the proof follows from the following 3 results.

1. [6] R is semilocal.

2. [14, Theorem 7] If R is a CK domain with maximal ideal M, then R_M is a CK domain and the atoms of R_M are the atoms of R contained in M .

3. [14, Theorem 1] Two maximal ideals of R cannot have an irreducible element in common.

Suppose that R is a CK domain with $Max(R) = \{M_1, \ldots, M_s\}$ and for each $1 \leq i \leq s$, $m_i := \left| \frac{U(\overline{R_{M_i}})}{U(R_{M_i})} \right|$, $V_i := \{v(\alpha) \mid \text{ for } \alpha \in A(R_{M_i})\} \,|$, $\alpha_i := \max(V_i)$, $\beta_i := \min(V_i)$, and $M_i{}^{u_i}_{M_i}$ is universal.

For a fixed $1 \leq i \leq s$, R_{M_i} is a CK domain. If $l_i \geq u_i$, then $\Lambda(R_{M_i}, l_i) \leq m_i((u_i - 1)(\alpha_i - \beta_i) + 1)$, by Theorem 2.0.12. If $l_i < u_i$, then $\Lambda(R_{M_i}, l_i) \leq m_i l_i(\alpha_i - \beta_i + 1)$. In both cases, $\Lambda(R_{M_i}, l_i) \leq m_i u_i(\alpha_i - \beta_i + 1)$. The overcount on $\Lambda(R_{M_i}, l_i)$ does not depend on l_i.

By

$$\begin{aligned}\Lambda(R, n) &\leq \prod_{i=1}^{s} \Lambda(R_{M_i}, n)\\ &\leq \prod_{i=1}^{s} m_i u_i(\alpha_i - \beta_i + 1) \text{ by Proposition \textbf{??}.}\end{aligned}$$

Thus

$$\overline{\Lambda}(R) \leq \lim_{n\to\infty} \frac{1}{n} \prod_{i=1}^{s} m_i u_i(\alpha_i - \beta_i + 1) = 0.$$

□

Corollary 2.0.13. *Let (R, M) be a one-dimensional analytically irreducible local FFD. Then* $\overline{\Lambda}(R) = 0$

Example 2.0.14. ([8] Example 18.2.5, recontextualized) Consider $R = \mathbb{F}_2[[X^2, X^3]]$.

R is a CK domain with $\overline{R} = \mathbb{F}_2[[X]]$. By [6, Theorem 7.1], M^3 is universal. Note that $(X^3 + X^4)^2 = X^6 + X^8 = X^6(1 + X^2)$ is associated to $(X^2)^3$ in R. It can be shown that $\widetilde{A}(R) = \{X^2, X^2 + X^3, X^3, X^3 + X^4\}$. We can factor these elements in $\overline{R}$ as X^2, $X^2(1 + X)$, X^3, and $X^3(1 + X)$, where $(1 + X)$ is a nonzero coset representative in $\frac{U(\overline{R})}{U(R)}$. Using the notation above, $V = \{2, 3\}$, $\beta = 2$, and $\alpha = 3$. Now, $V_n = \{3n - 2, 3n - 1, 3n\}$. These valuations are precisely given by $3(n-2)+4 \leq v(y) \leq 3n$. Since there are at most $\left|\frac{U(\overline{R})}{U(R)}\right| = 2$ different elements per valuation, $\Lambda(R, n) \leq 3(2) = 6$.

In the above results, we construct a bound on $|V_n|$. How much of an overestimate is this bound?

Example 2.0.15. Let $R = F_2[[X^2, X^5]]$. Then R is a CK domain with M^5 universal. Moreover, $V = \{2, 5\}$. By Theorem 2.0.12, $|V_n| \leq 4(5 - 2) + 1 = 13$. However, $|V_n| = 5$.

- $2 + 2 + 2 + 2 + \sum_{i=1}^{n-4} 5$
- $2 + 2 + 2 + \sum_{i=1}^{n-3} 5$
- $2 + 2 + \sum_{i=1}^{n-2} 5$
- $2 + \sum_{i=1}^{n-1} 5$
- $\sum_{i=1}^{n} 5$

There can be at most 4 irreducible elements with valuation 2 in the factorization of an element with minimal length n since M^5 is universal.

Example 2.0.16. Consider the collection of CK domains $R_k = F_2[[X^2, X^k]]$ where k is an odd integer greater than 3. Then $V = \{2, k\}$. By Proposition **??**, $|V_n| \leq (k - 1)(k - 2) + 1$.

However, $|V_n| = k$. In the event there are k or more copies of an irreducible with valuation 2, the element has a shorter factorization since M^k is universal.

Thus for the chosen collection of CK domains, the estimation can be 'arbitrarily bad' in the sense that $\lim_{k\to\infty} \frac{(k-1)(k-2)+1}{k} = \infty$.

Philosophically interesting in the proofs of Theorem 2.0.12 and Theorem 2 is the connection between elasticity of factorizations and the number of possible nonassociate factorizations. It is known in [1, Theorem 2.12] that V is a finite set $\iff$ R satisfies $\rho(R) < \infty$. An example of a Dedekind HFD with $\overline{\Lambda}(R) = \infty$ is given in [8, Example 18.2.9].

We give another example of a Dedekind HFD with $\overline{\Lambda}(R) = \infty$. The strategy in both examples is to manipulate the groupings of height-one primes to obtain nonassociate factorizations.

Definition 2.0.17. If $\beta = \sum_{i=1}^{k} b_i$ and $\alpha = \sum_{i=1}^{h} a_i$ are integer partitions of n written in weakly decreasing order of their parts, then β is said to *dominate* α ($\alpha \trianglelefteq \beta$) if and only if $\sum_{i=1}^{s} b_i \geq \sum_{i=1}^{s} a_i$ for all $1 \leq s \leq h$.

Example 2.0.18. Let R be a Dedekind domain with class group $\mathbb{Z}$ such that -1 and 1 are the only height-one prime classes with height-one primes in them. Then $\overline{\Lambda}(R) = \infty$

Proof. Denote height one-primes in the class of -1 and 1 by P_i and Q_j, respectively. If x is an nonprime, irreducible element of R, then the ideal factorization consists of exactly 2 ideals. Suppose that $l(y) = n$. Then in general $yR = P_1P_2\cdots P_nQ_1Q_2\cdots Q_n$. Now assume that each of the P_i's are distinct. For β an integer partition of n, denote y_β an element of R such that the multiset of Q's is given by the partition β in the standard way. We compute the varying numbers of nonassociate factorizations of the element y_β.

$$\begin{aligned} y_{3+2+1}R &= P_1Q_1P_2Q_1P_3Q_1P_4Q_2P_5Q_2P_6Q_3 \\ &= P_1Q_3P_2Q_1P_3Q_1P_4Q_2P_5Q_2P_6Q_1 \end{aligned}$$

Since each of the P_i terms were taken to be distinct we can instead view these factorizations as multiset permutations in the following way. To be more explicit, a height-one prime Q_i in the jth position from the left is associated with height one prime P_j.

$$\begin{aligned} y_{3+2+1}R &= P_1Q_1P_2Q_1P_3Q_1P_4Q_2P_5Q_2P_6Q_3 \rightsquigarrow Q_1Q_1Q_1Q_2Q_2Q_3 \\ &= P_1Q_3P_2Q_1P_3Q_1P_4Q_2P_5Q_2P_6Q_1 \rightsquigarrow Q_3Q_1Q_1Q_2Q_2Q_1 \end{aligned}$$

Since there are $\binom{n}{b_1,\, b_2,\, \ldots, b_k}$ many multiset permutations of the multiset β, $\eta(y_\beta) = \binom{n}{\beta} := \binom{n}{b_1,\, b_2,\, \ldots, b_k}$. If β dominates α, then $\binom{n}{\beta} \le \binom{n}{\alpha}$. Moreover, if $\alpha \lhd \beta$ is strict, then $\binom{n}{\beta} < \binom{n}{\alpha}$. In this way, there is an injective order reversing correspondence between the length of a maximal chain in the partition lattice of n ordered by domination and $\Lambda(R,n)$ Explicitly, $\Lambda(R,n) \ge$ the length of a maximal chain in the partitions of n ordered by domination. The length of a maximal chain in $P(n)$ ordered by domination is known to be asymptotically equal to $\frac{(2n)^{\frac{3}{2}}}{3}$ [19], [28]. Thus for large n, $\Lambda(R,n) \ge \frac{(2n)^{\frac{3}{2}}}{3}$.

$$\overline{\Lambda}(R) = \lim_{n\to\infty} \frac{\Lambda(R,n)}{n} \ge \lim_{n\to\infty} \frac{(2n)^{\frac{3}{2}}}{3n} = \infty.$$

□

The above examples is useful to keep in mind to show how drastically elasticity and $\overline{\Lambda}(R)$ can differ. Indeed, R is an HFD with $\overline{\Lambda}(R) = \infty$. This idea of an order reversing injective correspondence will be revisited in Chapter 3.

Chapter 3

Domains of the form $R = K + XF[X]$

In this chapter, we address [26, Conjecture 4.8], [8]. For this chapter, let $R = K + XF[X]$, where $K \subset F$ is a proper extension of fields of finite fields such that $t = \left|\frac{F^*}{K^*}\right|$. We will compute $\eta_R(x)$ for a nonzero, nonunit $x \in R$. It is known that R is a FFD and a HFD [4]. Please be mindful of changes in notation between the [26] and [8]. There are some superficial changes like $\overline{\Lambda}(R)$ is denoted $\Lambda^*(R)$ and some possibly confusing changes like $\eta(x)$ is denoted $\nu(x)$.

We reproduce the collection of relevant definitions from the introduction.

- $\eta_R(x)$ is the number of nonassociated irreducible factorizations of a nonzero, nonunit x.
- $l_R(x) = \min\{j \mid j = s_1 s_2 \dots s_j \text{ for each } s_i \in A(R).\}$
- $\gamma_R(n) = \{x \mid x \in R \text{ with } l_R(x) = n\}$ where $n \in \mathbb{Z}^+$.
- $\mu(R, n) = \{\eta_R(x) \mid x \in \gamma_R(n)\}$.
- $\Lambda(R, n) = |\mu(R, n)|$.
- $\overline{\Lambda}(R) = \lim_{n\to\infty} \frac{\Lambda(R,n)}{n}$.

To address to what extent the proof of the general case agrees with the proof of the specific case, we give a brief overview of the proof of [26, Lemma 4.4].

1. Show that for a fixed $f \in R$, $\eta(f) = \eta(\alpha^i X^s)$, where $l, s \in \mathbb{N}$ depend on f.

2. Grind some data.

3. Guess a recurrence for $\eta(\alpha^i X^n)$ for each $0 \le i \le 2$ and each residue of $n \pmod 3$.

4. Use induction and facts about integer partitions to prove recurrences in many subcases.

5. Claim that the factorizations inside $\eta(X^n)$ and $\eta(\alpha^i X^k)$ are distinct for all i and for all $k < n$.

6. Add up factorizations across different residues mod n.

To generalize the previous technique, a systematic method for determining $\eta(\alpha^i X^n)$ needed to be constructed. Overview of proof.

1. Show that for a fixed $f \in R$, $\eta(f) = \eta(\alpha^l X^s)$, where $l, s \in \mathbb{N}$ depend on f.

2. Directly compute $\eta(\alpha^i X^n)$ for each $0 \le i \le t-1$ and each residue of $n \pmod t$.

3. Prove that the factorizations inside $\eta(X^n)$ and $\eta(\alpha^i X^k)$ are distinct for all $0 \le i \le t-1$ and for all $k < n$.

4. Add up factorizations across different residues mod n.

In [5, Theorem 2.9] and proof, it is shown that an arbitrary element $f \in K + XF[X]$ can be written as $f(X) = aX^r(1 + Xh(X))$, where $a \in F$, $h(X) \in F[X]$, $r \in \mathbb{N}$ and $1 + Xh(X)$ is a product of prime elements of R. Suppose that $f \in R$ satisfies $l_R(f) = n$. Then $f = \alpha^i X^k g_{n-k}(X)$, where g_{n-k} is a degree $n - k$ polynomial that is the product of prime elements of R. Since g_{n-k} is a product of prime elements $\eta(f) = \eta(\alpha^i X^k)$. Thus

$$\begin{aligned}\gamma(n) &= \left\{ f \mid f \in R \text{ with } l(f) = n, \text{ where } n \in \mathbb{Z}^+ \right\} \\ &= \bigcup_{k=0}^{n} \bigcup_{i=0}^{t-1} \left\{ \alpha^i X^k g_{n-k}(X) \right\}.\end{aligned}$$

$$\begin{aligned}\mu(R,n) &= \{\eta(f) \mid x \in \gamma(n)\} \\ &= \bigcup_{k=0}^{n}\bigcup_{i=0}^{t-1}\left\{\eta(\alpha^i X^k g_{n-k}(X))\right\} \\ &= \bigcup_{k=0}^{n}\bigcup_{i=0}^{t-1}\left\{\eta(\alpha^i X^k)\right\}.\end{aligned}$$

Thus

$$\Lambda(R,n) = |\mu(R,n)| = \left|\left\{\bigcup_{k=0}^{n}\bigcup_{i=0}^{t-1}\eta(\alpha^i X^k)\right\}\right|.$$

We show in Theorem 3.0.46 that the collections of factorizations are distinct across different powers of k. Thus

$$\Lambda(R,n) = \sum_{k=0}^{n}\left|\bigcup_{i=0}^{t-1}\left\{\eta(\alpha^i X^k)\right\}\right|.$$

Using Proposition 3.0.33, for a fixed k and a fixed t,

$$\Lambda(R,n) = \sum_{k=0}^{n}\left|\bigcup_{i=0}^{t-1}\left\{\eta(\alpha^i X^k)\right\}\right| = \sum_{k=0}^{n}\tau(gcd(t,k)).$$

Now it is known (and proved in the appendix) that

$$\sum_{k=0}^{t}\tau(gcd(t,k)) = \sum_{d|t}\phi\left(\frac{t}{d}\right)\tau(d) = \sigma(t),$$

where ϕ is the euler phi function. If $n = tm + l$ for $0 \leq l \leq t-1$, then

$$\begin{aligned}\Lambda(R,n) &= m * \sum_{s=0}^{t-1}\tau(gcd(t,s)) + \sum_{s=0}^{l}\tau(gcd(t,s)) \\ &= m * \sum_{d|t}\phi\left(\frac{t}{d}\right)\tau(d) + \sum_{s=0}^{l}\tau(gcd(t,s)) \\ &= m\sigma(t) + \sum_{s=0}^{l}\tau(gcd(t,s)).\end{aligned}$$

The remainder of the chapter is dedicated to justifying the above claims. First we motivate our next result with an example.

Example 3.0.19. Let $R = \mathbb{F}_3 + X\mathbb{F}_9[X]$. We compute $\eta(X^3)$ Here $t = \frac{\mathbb{F}_9^*}{\mathbb{F}_3^*} = \frac{9-1}{3-1} = \frac{8}{2} = 4$. Denote as α a generator of $\mathbb{F}_9^*/\mathbb{F}_3^*$.

$$\begin{aligned} X^3 &= X \cdot X \cdot X \\ &= X \cdot \alpha X \cdot \alpha^3 X \\ &= \alpha X \cdot \alpha X \cdot \alpha^2 X \\ &= X \cdot \alpha^2 X \cdot \alpha^2 X \\ &= \alpha^2 X \cdot \alpha^3 X \cdot \alpha^3 X \end{aligned}$$

Now if $\alpha^0 := 1$, we can recontextualize the previous calculation.

$$\begin{aligned} (0,0,0) &= (0,0,0) \\ &= (3,1,0) \\ &= (2,1,1) \\ &= (2,2,0) \\ &= (3,3,2). \end{aligned}$$

The number of nonassociate irreducible factorizations of X^3 are given by the number of partitions of 0, 4, and 8 with at most 3 parts and each part is less than or equal to 3. If we denote the number of partitions of n with at most A parts each part less than or equal to B as $p(n, A, B)$, then $\eta_R(X^3) = p(0,3,3) + p(4,3,3) + p(8,3,3)$.

Proposition 3.0.20. *Let $R = K + XF[X]$ with $t = |F^*/K^*|$. Then*

$$\eta(\alpha^i X^n) = \sum_{k \equiv i \pmod t} p(k, n, t-1).$$

Proof. Using a degree argument, the irreducible elements dividing $\alpha^i X^n$ will have the form $\alpha^s X$, where $0 \leq s \leq t-1$. Let $\lambda \vdash \bigcup_{k \equiv i \pmod t} P(k, n, t-1)$, where $\lambda = \sum_{i=1}^{n} \lambda_i$ is written in weakly decreasing order. Then $\alpha^i X^n = \alpha^{\lambda_1} X \alpha^{\lambda_2} X \ldots \alpha^{\lambda_n} X$ is a factorization of $\alpha^i X^n$ in R.

Suppose that $\beta \neq \lambda \vdash \bigcup_{k \equiv i \pmod t} P(k, n, t-1)$, each written in weakly decreasing order. Then $\alpha^{\lambda_1} X \alpha^{\lambda_2} X \ldots \alpha^{\lambda_n} X$ and $\alpha^{\beta_1} X \alpha^{\beta_2} X \ldots \alpha^{\beta_n} X$ are nonassociated factorizations of $\alpha^i X^n$ in R. Since $0 \leq \lambda_i \leq t-1$ and $0 \leq \beta_i \leq t-1$, no $u \in k = U(R)$, satisfies $u\alpha^{\lambda_i} = \alpha^{\beta_i}$ for $\lambda_i \neq \beta_i$. Informally, for any $u \in K$, t is the smallest power of α that divides u in $U(R)$. □

By rewriting the partitions in terms of a weakly decreasing sequence of integers, we recover the notation used in the special cases considered in [26].

Remark 3.0.21. In $R = K + XF[X]$,

$$\eta(\alpha^i X^n) = |\{(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n \text{ and } 0 \leq a_1 \leq a_2 \leq \cdots \leq a_n \leq t-1 \ | $$

$$\sum_{i=1}^{n} a_i \equiv i \pmod t\}.$$

Next we compute $\eta(\alpha^i X^n) = \sum_{k \equiv i \pmod t} p(k, n, t-1)$ with the help of generating functions. The q-binomial coefficient $\binom{n+t-1}{t-1}_q$ is the generating function of $p(k, n, t-1)$ by [9, pg 39]. Namely the coefficient of q^k of $\binom{n+t-1}{t-1}_q$ is $p(k, n, t-1)$ where

$$\binom{n+t-1}{t-1}_q = \frac{(1-q^{n+t-1})(1-q^{n+t-2})\cdots(1-q^{n+2})(1-q^{n+1})}{(1-q^{t-1})(1-q^{t-2})\cdots(1-q^2)(1-q^1)}.$$

For notational convenience, let $A_i := \eta(\alpha^i X^n)$, $x := e^{\frac{2\pi i}{t}}$ a primitive t-th root of unity, and

$$B_k := \binom{n+t-1}{t-1}_{q=x^k} := \lim_{q\to x^k} \binom{n+t-1}{t-1}_q.$$

This construction of B_k is well defined because the q-binomial coefficient is a polynomial in q by [9, pg. 35]. With the adopted notation above, for $0 \le k \le t-1$

$$B_k = \binom{n+t-1}{t-1}_{q=x^k} = \sum_{i=0}^{t-1} A_i x^{ki}.$$

Remark 3.0.22. The A_i's and B_i's create a discrete Fourier transformation in that the A_i terms can be recovered from the B_i terms.

$$B_k = \sum_{i=0}^{t-1} A_i x^{ki} \iff A_i = \frac{1}{t}\sum_{k=0}^{t-1} B_k x^{-ki}.$$

To directly compute the value $A_i = \eta(\alpha^i X^n)$, we first compute some facts about the B_k terms.

Lemma 3.0.23. *[9, pg. 35]* $B_0 = \binom{n+t-1}{t-1}$.

Proof. $B_0 = \binom{n+t-1}{t-1}_{q=x^0} = \binom{n+t-1}{t-1}_{q=1} = \binom{n+t-1}{t-1}$. □

Lemma 3.0.24. $B_1 = \begin{cases} 1 & \textit{if } t \mid n \\ 0 & \textit{if } t \nmid n \end{cases}.$

Proof.

$$\begin{aligned} B_1 &= \binom{n+t-1}{t-1}_{q=x} \\ &= \frac{(1-x^{n+t-1})(1-x^{n+t-2})\cdots(1-x^{n+2})(1-x^{n+1})}{(1-x^{t-1})(1-x^{t-2})\cdots(1-x^{2})(1-x^{1})} \end{aligned}$$

The collection of exponents of x in the denominator form a transversal of the nonzero residues $\pmod t$. If $t \nmid n$, then the collection of exponents of x in the numerator is not a transversal of the nonzero residues $\pmod t$. There exists an l, where $1 \le l \le t-1$, such that $t \mid (n+l)$. Hence the factor $1 - x^{n+l} = 0$ occurs in the numerator; therefore $B_1 = 0$.

Otherwise, if $t \mid n$, the set of exponents of the numerator is also a transversal of all nonzero representatives $\pmod t$, and $B_1 = 1$. $\square$

To utilize the fact that

$$B_k = \sum_{i=0}^{t-1} A_i x^{ki} \iff A_i = \frac{1}{t}\sum_{k=0}^{t-1} B_k x^{-ki},$$

our next results determine values of B_k for all $0 \le k \le t-1$.

Proposition 3.0.25. *Suppose $t = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ and d is a positive divisor of t. Then*

$$B_d = \begin{cases} 0 & \text{if } \frac{t}{d} \nmid n \\ \displaystyle\prod_{f=1}^{d-1} \frac{tf + dn}{tf} & \text{if } \dfrac{t}{d} \mid n \end{cases}.$$

Proof. Let us manipulate the q-binomial before we evaluate at $q = x^d$. If $\frac{t}{d} \mid n$, then $n = \frac{tk}{d}$ for some $k \in \mathbb{Z}^+$. We reorganize the numerator and denominator in order to collect the terms whose exponent is divisible by $\frac{t}{d}$. We separate those exponents not divisible by $\frac{t}{d}$ on the left and those divisible by $\frac{t}{d}$ on the right. Let S_1 and S_2 denote the exponents in the numerator and denominator, respectively, not divisible by $\frac{t}{d}$.

$$\begin{aligned} \binom{n+t-1}{t-1}_q &= \frac{(1-q^{n+t-1})(1-q^{n+t-2})\cdots(1-q^{n+2})(1-q^{n+1})}{(1-q^{t-1})(1-q^{t-2})\cdots(1-q^2)(1-q^1)} \\ &= \prod_{s_1 \in S_1} (1-q^{s_1}) \prod_{s_2 \in S_2} \left(\frac{1}{1-q^{s_2}}\right) \prod_{f=1}^{d-1} \left(\frac{1-q^{\frac{t}{d}(f+k)}}{1-q^{\frac{t}{d}(f)}}\right). \end{aligned}$$

There are $t-d$ factors in each of the products on the left, and $d-1$ factors in the product on the right. We focus more explicitly on a factor in the right product.

$$\frac{1-q^{\frac{t}{d}(k+f)}}{1-q^{\frac{t}{d}(f)}} = \frac{(1-q^{\frac{t}{d}})(1+q^{\frac{t}{d}}+q^{2\frac{t}{d}}+\cdots+q^{\frac{t}{d}(k+f-1)})}{(1-q^{\frac{t}{d}})(1+q^{\frac{t}{d}}+q^{2\frac{t}{d}}+\cdots+q^{\frac{t}{d}(f-1)})}$$
$$= \frac{1+q^{\frac{t}{d}}+q^{2\frac{t}{d}}+\cdots+q^{\frac{t}{d}(k+f-1)}}{1+q^{\frac{t}{d}}+q^{2\frac{t}{d}}+\cdots+q^{\frac{t}{d}(f-1)}}.$$

Thus we may rewrite the q-binomial coefficient,

$$\binom{n+t-1}{t-1}_q = \prod_{s_1\in S_1}(1-q^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-q^{s_2}}\right)\prod_{f=1}^{d-1}\left(\frac{1-q^{\frac{t}{d}(f+k)}}{1-q^{\frac{t}{d}(f)}}\right)$$
$$= \prod_{s_1\in S_1}(1-q^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-q^{s_2}}\right)\prod_{f=1}^{d-1}\left(\frac{1+q^{\frac{t}{d}}+q^{\frac{t}{d}2}+\cdots+q^{\frac{t}{d}(k+f-1)}}{1+q^{\frac{t}{d}}+q^{2\frac{t}{d}}+\cdots+q^{\frac{t}{d}(f-1)}}\right).$$

For notational convince, let $y := x^d$. We compute B_d.

$$B_d = \prod_{s_1\in S_1}(1-y^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-y^{s_2}}\right)\prod_{f=1}^{d-1}\left(\frac{1+y^{\frac{t}{d}}+y^{2\frac{t}{d}}+\cdots+y^{\frac{t}{d}(k+f-1)}}{1+y^{\frac{t}{d}}+y^{2\frac{t}{d}}+\cdots+y^{\frac{t}{d}(f-1)}}\right).$$

Since d is a divisor of t, $y = x^d$ is a $\frac{t}{d}$-th root of unity [22, Lemma 7.10]. Moreover, the $t-d$ terms in each of the left products are split into d transversals of the nonzero residues (mod $\frac{t}{d}$). Thus

$$\prod_{s_1\in S_1}(1-y^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-y^{s_2}}\right) = 1.$$

Moreover,

$$\frac{1+y^{\frac{t}{d}}+y^{2\frac{t}{d}}+\cdots+y^{\frac{t}{d}(k+f-1)}}{1+y^{\frac{t}{d}}+y^{2\frac{t}{d}}+\cdots+y^{\frac{t}{d}(f-1)}} = \frac{1+x^t+x^{2t}+\ldots x^{t(k+f-1)}}{1+x^t+x^{2t}+\cdots+x^{t(f-1)}}$$
$$= \frac{f+k}{f}.$$

Thus

$$
\begin{aligned}
B_d &= \prod_{s_1\in S_1}(1-y^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-y^{s_2}}\right)\prod_{f=1}^{d-1}\left(\frac{1+y^{\frac{t}{d}}+y^{\frac{t}{d}2}+\cdots+y^{\frac{t}{d}(k+f-1)}}{1+y^{\frac{t}{d}}+y^{\frac{t}{d}2}+\cdots+y^{\frac{t}{d}(f-1)}}\right)\\
&=\prod_{f=1}^{d-1}\left(\frac{1+y^{\frac{t}{d}}+y^{\frac{t}{d}2}+\cdots+y^{\frac{t}{d}(k+f-1)}}{1+y^{\frac{t}{d}}+y^{\frac{t}{d}2}+\cdots+y^{\frac{t}{d}(f-1)}}\right)\\
&=\prod_{f=1}^{d-1}\left(\frac{f+k}{f}\right)\\
&=\prod_{f=1}^{d-1}\left(\frac{\frac{tf}{d}+\frac{tk}{d}}{\frac{tf}{d}}\right)=\prod_{f=1}^{d-1}\left(\frac{tf+dn}{tf}\right).
\end{aligned}
$$

Otherwise, if $\frac{t}{d}\nmid n$, then there exists an $1\le l\le \frac{t}{d}-1$ such that $\frac{t}{d}\mid n+l$. We reorganize the q-binomial coefficient depending on divisibility by $\frac{t}{d}$. In this case, there are d terms in the numerator that are divisible by $\frac{t}{d}$ and only $d-1$ terms divisible by $\frac{t}{d}$ in the denominator.

$$
\begin{aligned}
\binom{n+t-1}{t-1}_q &= \frac{(1-q^{n+t-1})(1-q^{n+t-2})\cdots(1-q^{n+2})(1-q^{n+1})}{(1-q^{t-1})(1-q^{t-2})\cdots(1-q^{2})(1-q^{1})}\\
&=(1-q^{n+l})\prod_{s_1\in S_1}(1-q^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-q^{s_2}}\right)\prod_{f=1}^{d-1}\left(\frac{1-q^{\frac{ft}{d}+n+l}}{1-q^{\frac{t}{d}(f)}}\right).
\end{aligned}
$$

Simplifying as in the previous case,

$$
\begin{aligned}
\binom{n+t-1}{t-1}_q &= \prod_{s_1\in S_1}(1-q^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-q^{s_2}}\right)(1-q^{n+l})\prod_{f=1}^{d-1}\left(\frac{1-q^{\frac{ft}{d}+n+l}}{1-q^{\frac{t}{d}(f)}}\right)\\
&=(1-q^{n+l})\prod_{s_1\in S_1}(1-q^{s_1})\prod_{s_2\in S_2}\left(\frac{1}{1-q^{s_s}}\right)\\
&\qquad\prod_{f=1}^{d-1}\frac{1+q^{\frac{t}{d}}+q^{2\frac{t}{d}}+\cdots+q^{\frac{t}{d}(f-1)+n+l}}{1+q^{\frac{t}{d}}+q^{2\frac{t}{d}}+\cdots+q^{\frac{t}{d}(f-1)}}.
\end{aligned}
$$

To compute B_d, we evaluate the above equation at $q=x^d$. Reading left to right, the first term is zero since $\frac{t}{d}\mid n+l$ and x^d is a $\frac{t}{d}$-th root of unity. The rest of the terms are nonzero. Thus if $\frac{t}{d}\nmid n$, then $B_d=0$. □

Remark 3.0.26. Notice that B_d can be given as a binomial coefficient for $\frac{t}{d} \mid n$

$$B_d = \prod_{f=1}^{d-1} \binom{tf + dn}{tf} = \binom{\frac{td-t+dn}{t}}{\frac{td-t}{t}} = \binom{d - 1 + \frac{dn}{t}}{d-1}.$$

Remark 3.0.27. With the usual convention that empty products are 1, the proof for the B_1 case is a special case of Proposition 3.0.25.

Remark 3.0.28. Since x was chosen to be a t-th root of unity,

$$B_0 = B_t = \prod_{f=1}^{t-1} \binom{f + n}{f} = \binom{n + t - 1}{t - 1}.$$

Example 3.0.29. Let $t = 6$ and $n = 12$, then $B_0 = \binom{12+5}{5} = 6188$, $B_1 = 1$, $B_2 = \frac{6(1)+2(12)}{6(1)} = 5$, and $B_3 = \prod_{f=1}^{2} \binom{6f+3(12)}{6f} = \binom{6+3(12)}{6}\binom{2(6)+3(12)}{6(2)} = 28$.

Example 3.0.30. Let $t = 8$ and $n = 16$, then $B_0 = \binom{16+7}{7}$, $B_1 = 1$, and $B_2 = \frac{(8)+2(16)}{8} = 5$.

$$B_4 = \prod_{f=1}^{3} \binom{8f + 4(16)}{8f} = \binom{1+8}{1}\binom{2+8}{2}\binom{3+8}{3} = 165.$$

Note in the first example that $B_1 < B_2 < B_3$, and in the second example $B_1 < B_2 < B_4$. This behavior generalizes to the general case in the following manner.

Lemma 3.0.31. *Let $d_1 < d_2$ be nonzero divisors of t, where $B_{d_1} \neq 0$, and $B_{d_2} \neq 0$. Then $B_{d_1} < B_{d_2}$.*

Proof.

$$B_{d_1} = \prod_{f=1}^{d_1-1}\left(\frac{f+\frac{d_1 n}{t}}{f}\right) = \frac{\left(1+\frac{d_1 n}{t}\right)\left(2+\frac{d_1 n}{t}\right)\ldots\left(d_1-1+\frac{d_1 n}{t}\right)}{(d_1-1)!}.$$

$$\begin{aligned} B_{d_2} &= \prod_{f=1}^{d_2-1}\left(\frac{f+\frac{d_2 n}{t}}{f}\right) \\ &= \frac{\left(1+\frac{d_2 n}{t}\right)\left(2+\frac{d_2 n}{t}\right)\ldots\left(d_2-1+\frac{d_2 n}{t}\right)}{(d_2-1)!} \\ &= \underbrace{\frac{\left(1+\frac{d_2 n}{t}\right)\left(2+\frac{d_2 n}{t}\right)\ldots\left(d_1-1+\frac{d_2 n}{t}\right)}{(d_1-1)!}}_{>B_{d_1}} \underbrace{\frac{\left(d_1+\frac{d_2 n}{t}\right)\left(d_1+1+\frac{d_2 n}{t}\right)\ldots\left(d_2-1+\frac{d_2 n}{t}\right)}{(d_1)(d_1+1)\ldots(d_2-2)(d_2-1)}}_{>1} \end{aligned}$$

□

Since $x^t = x^0 = 1$, the nonzero condition of Lemma 3.0.31 cannot be relaxed. If $d_1 \mid d_2$, $d_2 := d_1 h$, the above bound can be made more explicit.

Lemma 3.0.32. *Let $d_1 \mid d_2$ be nonzero divisors of t satisfying $\frac{t}{d_1} \mid n$, $\frac{t}{d_2} \mid n$. Then* $B_{d_2} > B_{d_1}(1 + d_2)$

Proof.

$$\begin{aligned} B_{d_1} &= \prod_{f=1}^{d_1-1}\left(\frac{f+\frac{d_1 n}{t}}{f}\right) = \frac{\left(1+\frac{d_1 n}{t}\right)\left(2+\frac{d_1 n}{t}\right)\ldots\left(d_1-1+\frac{d_1 n}{t}\right)}{(d_1-1)!}. \\ B_{d_2} &= \prod_{f=1}^{d_2-1}\left(\frac{f+\frac{d_2 n}{t}}{f}\right) \\ &= B_{d_1} \prod_{\substack{f=1,2,\ldots d_2-1 \\ \text{where } h\nmid f}}\left(\frac{f+\frac{d_2 n}{t}}{f}\right) \\ &> B_{d_1}\left(1+\frac{d_2 n}{t}\right). \end{aligned}$$

□

Recall the Discrete Fourier Transform at the heart of our consideration,

$$B_k = \sum_{i=0}^{t-1} A_i x^{ki} \iff A_i = \frac{1}{t}\sum_{k=0}^{t-1} B_k x^{-ki}.$$

We extend the definition of the B_k terms beyond just those k that are divisors of t.

Proposition 3.0.33. *If $gcd(t,k) = a$, then $B_k = B_a$.*

Proof.

$$\begin{aligned}
B_k &= \binom{n+t-1}{t-1}_{q=x^k} \\
&= \frac{(1-(x^k)^{n+t-1})(1-(x^k)^{n+t-2})\cdots(1-(x^k)^{n+2})(1-(x^k)^{n+1})}{(1-(x^k)^{t-1})(1-(x^k)^{t-2})\cdots(1-(x^k)^{2})(1-(x^k)^{1})} \\
&= \frac{(1-(e^{\frac{2\pi ik}{t}})^{n+t-1})(1-(e^{\frac{2\pi ik}{t}})^{n+t-2})\cdots(1-(e^{\frac{2\pi ik}{t}})^{n+2})(1-(e^{\frac{2\pi ik}{t}})^{n+1})}{(1-(e^{\frac{2\pi ik}{t}})^{t-1})(1-(e^{\frac{2\pi ik}{t}})^{t-2})\cdots(1-(e^{\frac{2\pi ik}{t}})^{2})(1-(e^{\frac{2\pi ik}{t}})^{1})}.
\end{aligned}$$

Proceed according to the definition of q-binomial coefficient. Then we use the fact that $x = e^{\frac{2\pi i}{t}}$ is a primitive t-th root of unity. If $t = ac$ and $k = ab$ where $gcd(b,c) = 1$ are relatively prime, then $x^k = (e^{\frac{2\pi i}{t}})^k = (e^{\frac{2\pi i}{ac}})^{ab} = (e^{\frac{2\pi i}{c}})^b$. Now $e^{\frac{2\pi i}{c}}$ is a primitive c-th root of unity, and thus $(e^{\frac{2\pi i}{c}})^b$ is also a primitive c-th root of unity since $gcd(b,c) = 1$.

$$\begin{aligned}
&= \frac{(1-(e^{\frac{2\pi ib}{c}})^{n+t-1})(1-(e^{\frac{2\pi ib}{c}})^{n+t-2})\cdots(1-(e^{\frac{2\pi ib}{c}})^{n+2})(1-(e^{\frac{2\pi ib}{c}})^{n+1})}{(1-(e^{\frac{2\pi ib}{c}})^{t-1})(1-(e^{\frac{2\pi ib}{c}})^{t-2})\cdots(1-(e^{\frac{2\pi ib}{c}})^{2})(1-(e^{\frac{2\pi ib}{c}})^{1})} \\
&= \frac{(1-(e^{\frac{2\pi i}{c}})^{n+t-1})(1-(e^{\frac{2\pi i}{c}})^{n+t-2})\cdots(1-(e^{\frac{2\pi i}{c}})^{n+2})(1-(e^{\frac{2\pi i}{c}})^{n+1})}{(1-(e^{\frac{2\pi i}{c}})^{t-1})(1-(e^{\frac{2\pi i}{c}})^{t-2})\cdots(1-(e^{\frac{2\pi i}{c}})^{2})(1-(e^{\frac{2\pi i}{c}})^{1})} \\
&= \frac{(1-(x^a)^{n+t-1})(1-(x^a)^{n+t-2})\cdots(1-(x^a)^{n+2})(1-(x^a)^{n+1})}{(1-(x^a)^{t-1})(1-(x^a)^{t-2})\cdots(1-(x^a)^{2})(1-(x^a)^{1})} \\
&= \binom{n+t-1}{t-1}_{q=x^a} = B_a.
\end{aligned}$$

□

Corollary 3.0.34. *Suppose that p_1 is the minimal prime number in the prime factorization of t and d a nonzero divisor of t. Then $B_d \leq B_{\frac{t}{p_1}}$ provided each is nonzero.*

Corollary 3.0.34 follows directly from the straight forward combination of Lemma 3.0.31, Lemma 3.0.32, and Proposition 3.0.33.

Combining Proposition 3.0.33 and Lemma 3.0.34 we obtain the following result.

Theorem 3.0.35.

$$|\{B_k \mid 0 \leq k \leq t-1\}| = \tau(gcd(n,t)).$$

Proof. Consider the map $\{0 \leq k \leq t-1\} \to \{B_k \mid 0 \leq k \leq t-1\}$ given by $f : k \mapsto B_k$. By Proposition 3.0.33, $im(f) \subseteq \{B_d \mid d \mid t\}$. By Proposition 3.0.25, $|f^{-1}(0)| = |\left\{k \mid \frac{t}{k} \mid n\right\}|$. The cardinality of the preimage of 0 is the number of divisors of t that are not divisors of n. Suppose that $k_1 < k_2$ are divisors of both t and n. Then, by Lemma 3.0.31, $B_{k_1} \neq B_{k_2}$. □

Since the discrete Fourier Transform connecting the A and B terms is invertible, we have

$$|\{B_k \mid 0 \leq k \leq t-1\}| = |\{A_i \mid 0 \leq i \leq t-1\}|.$$

For a fixed n, we restate the result in the varied notation employed.

Proposition 3.0.36.

- $|\{A_i \mid 0 \leq i \leq t-1\}| = \tau(gcd(n,t))$.
- $|\left\{\eta_R(\alpha^i X^n) \mid 0 \leq i \leq t-1\right\}| = \tau(gcd(n,t))$.
- *The number of different number of factorizations of* $\alpha^i X^n$ *for* $0 \leq i \leq t-1$ *and* n *fixed is is* $\tau(gcd(n,t))$.

We are now well equipped to tackle [26, Conjecture 3.7].

Proposition 3.0.37. *If* $|F^*/K^*| = t$ *and* $gcd(n,t) = 1$*, then* $\eta(\alpha^i X^n) = \eta(\alpha^j X^n)$ *for* $i \neq j$*. Thus* $|\left\{\eta(\alpha^i X^n)| \text{ for } i = 0,1,2,\ldots,t-1\right\}| = 1$ *and* $A_i = \eta(X^n) = \frac{1}{t}\binom{n+t-1}{t-1}$.

Proof. Using Proposition 3.0.25 , Lemma 3.0.33, and $gcd(n,t) = 1$,

$$B_k = \begin{cases} \binom{n+t-1}{t-1} & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases}.$$

Now for $0 \leq i \leq t-1$,

$$\eta(\alpha^i X^n) = A_i = \frac{1}{t}\left(B_0 + \sum_{k=1}^{t-1} B_k x^{-ki}\right) = \frac{1}{t}B_0 = \frac{1}{t}\binom{n+t-1}{t-1}.$$

□

Example 3.0.38. Using the chart provided in [26], if $t = 16$ and $n = 19 = 16 + 3$, then there are 1159997970 nonassociate factorizations of X^{19}. By the above fact, $\eta(\alpha^i X^{19}) = \frac{1}{16}\binom{19+15}{15} = 1159997970$ for all $0 \leq i \leq t-1$.

Our next objective is to determine $\eta(\alpha^i X^n)$ when $gcd(n,t) \neq 1$.

Remark 3.0.39. Recall that if x is a primitive t-th root of unity, then the sum of the primitive t-th roots of unity is $\mu(t)$, where μ is the Möbius function. Explicitly, for $x = e^{\frac{2\pi i}{t}}$

$$\sum_{gcd(s,t)=1} x^s = \mu(t).$$

Recall the relationship

$$B_k = \sum_{i=0}^{t-1} A_i x^{ki} \iff A_i = \frac{1}{t}\sum_{k=0}^{t-1} B_k x^{-ki}.$$

Thus,

$$tA_i = \sum_{k=0}^{t-1} B_k x^{-ki} = \sum_{0 \neq d|t}\left[B_d \sum_{gcd(k,t)=d} x^{-ki}\right].$$

Now x is a primitive t-th root of unity, and x^{-k} is a primitive $\frac{t}{d}$-th root of unity since $gcd(k,t) = d$. For a fixed value of i and d, compute $f_d = gcd(\frac{t}{d}, i)$. Then x^{-ki} is a primitive $\frac{t}{df_d}$-th root of unity.

x	$\rightarrow$	x^{-k}	$\rightarrow$	x^{-ki}
primitive t-th root	$\rightarrow$	primitive $\frac{t}{d}$-th root	$\rightarrow$	primitive $\frac{t}{df_d}$-th root

For a fixed d and a fixed i, there are $\phi(\frac{t}{d})$ members of the sum $\sum_{gcd(k,t)=d} x^{-ki}$. These summands are split into $\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})}$ copies of the sum of primitive $\frac{t}{df_d}$-th roots of unity. Thus

$$\begin{aligned}
tA_i &= \sum_{k=0}^{t-1} B_k x^{-ki} \\
&= \sum_{0 \neq d | t} \left[B_d \sum_{gcd(k,t)=d} x^{-ki} \right] \\
&= \sum_{0 \neq d | t} \left[B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})} \sum_{gcd(ki, \frac{t}{df_d})=1} x^{-ki} \right] \\
&= \sum_{0 \neq d | t} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})} \mu \left(\frac{t}{df_d} \right).
\end{aligned}$$

Example 3.0.40. For $t = 36$ and $gcd(i,t) = 6$, compute tA_6.

Proof. Using the notation above,

$$tA_6 = \sum_{k=0}^{35} B_k x^{-k6} = \sum_{0 \neq d | 36} \frac{\phi(\frac{36}{d})}{\phi(\frac{36}{df_d})} B_d \mu \left(\frac{36}{df_d} \right).$$

Recall that $f_d := gcd(\frac{36}{d}, 6)$.

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	6	6	6	3	6	2	3	2	1
resulting root of unity	$\frac{t}{df_d}$	6	3	2	3	1	2	1	1	1

Focus on just the term of the sum determined by $d = 4$. Then $\frac{t}{d} = 9$, and $f_4 = 3$. The term contributed to the sum by $d = 4$ is $B_4 \frac{\phi(9)}{\phi(3)} \mu(3) = -3B_4$. Let $y := x^4$, $z := y^3$, and write $i = 3s$, where $gcd(s, \frac{36}{4(3)}) = 1$. Then

$$
\begin{aligned}
B_4 \sum_{gcd(k,36)=4} x^{-ki} &= B_4 \left\{ x^{-4i} + x^{-8i} + x^{-16i} + x^{-20i} + x^{-28i} + x^{-32i} \right\} \\
&= B_4 \left\{ y^{-i} + y^{-2i} + y^{-4i} + x^{-5i} + y^{-7i} + y^{-8i} \right\} \\
&= B_4 \left\{ y^{i} + y^{2i} + y^{4i} + y^{5i} + y^{7i} + y^{8i} \right\} \\
&= B_4 \left\{ z^{s} + z^{2s} + z^{4s} + z^{5s} + z^{7s} + z^{8s} \right\} \\
&= 3B_4 \left\{ z^{s} + z^{2s} \right\} = 3B_4\mu(3) = -3B_4.
\end{aligned}
$$

Applying this procedure to each of the divisors of 36, it is true that

$$
\begin{aligned}
tA_6 &= \sum_{k=0}^{t-1} B_k x^{-k6} \\
&= \sum_{0 \neq d | 36} \frac{\phi(\frac{36}{d})}{\phi(\frac{36}{df_d})} B_d \mu\left(\frac{36}{df_d}\right) \\
&= B_0(1) + B_1 \frac{\phi(36)}{\phi(6)}\mu(6) + B_2 \frac{\phi(18)}{\phi(3)}\mu(3) + B_3 \frac{\phi(12)}{\phi(2)}\mu(2) + \\
&\qquad B_4 \frac{\phi(9)}{\phi(3)}\mu(3) + B_6\phi(6) + B_9 \frac{\phi(4)}{\phi(2)}\mu(2) + B_{12}\phi(3) + B_{18}\phi(2) \\
tA_6 &= B_0 + B_1 \frac{\phi(36)}{\phi(6)} - B_2 \frac{\phi(18)}{\phi(6)} - B_3 \frac{\phi(12)}{\phi(6)} - \\
&\qquad B_4 \frac{\phi(9)}{\phi(3)} + B_6\phi(6) - B_9 \frac{\phi(4)}{\phi(2)} + B_{12}\phi(3) + B_{18}\phi(2).
\end{aligned}
$$

□

We introduce some vocabulary to assist in the arrangement of the next result. For a fixed i the members of the sum $\sum_{0 \neq d|t} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})}\mu\left(\frac{t}{df_d}\right)$ are split into three groups depending on f_d.

- For a fixed d and i, we say that d undergoes *complete reduction* or d determines a *complete reduction term* if $f_d = \frac{t}{d}$.

- For a fixed d and i, we say that d undergoes *no reduction* or d determines a *no* *reduction term* if $f_d = 1$.

- Otherwise, we say that d undergoes *partial reduction* or d determines a *partial reduction term.*

This choice of vocabulary describes the behavior of the $\frac{t}{d}$-th roots of unity after being raised to the i-th power. Note in the above example, the full reduction terms are $d = 36, d = 18, d = 12$, and $d = 6$. Therefore the number of full reduction terms is $4 = \tau(6) = \tau(gcd(i,t))$.

We motivate the next result by another example.

Example 3.0.41. Consider the situation where $t = 36$ and $i = 2$.

As before, we separate the divisors of 36 according to f_d.

$$tA_2 = \sum_{\substack{0 \neq d | t \\ f_d = 2}} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{d2})} \mu\left(\frac{t}{d2}\right) + \sum_{\substack{0 \neq d | t \\ f_d = 1}} B_d \mu\left(\frac{t}{d}\right)$$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	2	2	2	1	2	2	1	2	1
resulting root of unity	$\frac{t}{df_d}$	18	9	6	9	3	2	3	1	1

- The complete reduction terms are $d = 36$, and $d = 18$.
- The no reduction terms are $d = 12$, $d = 4$.
- Te partial reduction terms are $d = 9$, $d = 6$, $d = 3$, $d = 2$, and $d = 1$.

Assuming that $t \mid n$, we show $A_2 - A_1 > 0$. Informally we show that the complete reduction terms from A_2 will be larger than the partial reduction terms of A_2 along with the remaining complete reduction terms from A_1.

$$
\begin{aligned}
t(A_2 - A_1) &= \sum_{\substack{0\neq d|t \\ f_d=2}} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{d2})}\mu\left(\frac{t}{d2}\right) + \sum_{\substack{0\neq d|t \\ f_d=1}} B_d\mu\left(\frac{t}{d}\right) - \sum_{0\neq d|t} B_d\mu\left(\frac{t}{d}\right) \\
&= \sum_{\substack{0\neq d|t \\ f_d=2}} B_d \left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{d2})}\mu\left(\frac{t}{2d}\right) - \mu\left(\frac{t}{d}\right)\right] \\
&= (\phi(2) - \mu(2))B_{18} + \left(\frac{\phi(4)}{\phi(2)}\mu\left(2\right) - \mu\left(4\right)\right) B_9 + \left(\frac{\phi(6)}{\phi(3)}\mu\left(3\right) - \mu\left(6\right)\right) B_6 \\
&\quad + \left(\frac{\phi(12)}{\phi(6)}\mu\left(6\right) - \mu\left(12\right)\right) B_3 + \left(\frac{\phi(18)}{\phi(9)}\mu\left(9\right) - \mu\left(18\right)\right) B_2 \\
&\quad + \left(\frac{\phi(36)}{\phi(18)}\mu\left(18\right) - \mu\left(36\right)\right) B_1.
\end{aligned}
$$

Now we reduce the right hand side in two ways. The first way is to choose the value of the Möbius function to ensure that the coefficients for the partial reduction terms and no reduction terms are negative. The second way is to approximate the $\phi(\frac{t}{d})/\phi(\frac{t}{2d})$ term using well known facts concerning the totient function.

Remark 3.0.42. Let p a prime number. Then since

$$
\phi\left(\frac{t}{pd}\right)\phi(p) \leq \phi\left(\frac{t}{d}\right) \leq p\phi\left(\frac{t}{pd}\right)
$$

it is true that

$$
\phi(p) \leq \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{pd})} \leq p.
$$

Thus

$$\begin{aligned}
t(A_2 - A_1) = (\phi(2) - \mu(2))B_{18} &+ \left(\frac{\phi(4)}{\phi(2)}\mu\left(2\right) - \mu\left(4\right)\right) B_9 + \left(\frac{\phi(6)}{\phi(3)}\mu\left(3\right) - \mu\left(6\right)\right) B_6 \\
&+ \left(\frac{\phi(12)}{\phi(6)}\mu\left(6\right) - \mu\left(12\right)\right) B_3 + \left(\frac{\phi(18)}{\phi(9)}\mu\left(9\right) - \mu\left(18\right)\right) B_2 \\
&+ \left(\frac{\phi(36)}{\phi(18)}\mu\left(18\right) - \mu\left(36\right)\right) B_1 \\
\geq 2B_{18} &+ (-2-1)B_9 + (-2-1)B_6 \text{ by Remark 3.0.42} \\
&+ (-2-1)B_3 + (-2-1)B_2 \\
&+ (-2-1)B_1.
\end{aligned}$$

We further reduce the right hand side by using Lemma 3.0.31 and Corollary 3.0.34. The assumption $t \mid n$ ensures that $B_d \neq 0$ for all d, and the amount subtracted is as large as possible.

$$\begin{aligned}
t(A_2 - A_1) &> 2B_{18} + -3(5)B_9 && \text{using Lemma 3.0.31} \\
&> 2(1+18)B_9 - 3(5)B_9 && \text{using Lemma 3.0.32} \\
&> 23B_9 > 0.
\end{aligned}$$

Theorem 3.0.43.

- $\max\left\{\eta(\alpha^i X^n) i = 0, 1, \ldots, t-1\right\} = \eta(X^n)$.
- $\min\{\eta(\alpha^i X^n) i = 0, 1, \ldots, t-1\} = \eta(\alpha X^n)$.

Proof. Given that $gcd(i,t) = t$, then $f_d = \frac{t}{d}$ for all d. Every divisor of t is a complete reduction term, equivalently each of the $\frac{t}{d}$ roots of unity are fully reduced to 1. Thus,

$$\begin{aligned}
tA_i &= \sum_{0 \neq d \mid t} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})} \mu\left(\frac{t}{df_d}\right) \\
&= \sum_{0 \neq d \mid t} B_d \phi\left(\frac{t}{d}\right).
\end{aligned}$$

Otherwise, if $gcd(i_1, t) < t$, then there exists a d_1 such that $f_{d_1} < \frac{t}{d_1}$ or a root that is not fully reduced. Then

$$\phi\left(\frac{t}{d}\right) > \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})}\mu\left(\frac{t}{df_d}\right)$$

for each of the not fully reduced terms. So, each of the constituent terms in the sum A_i is greater than or equal to the corresponding term in A_{i_1}. Thus

$$\max\left\{\eta(\alpha^i X^n) i = 0, 1, \ldots, t-1\right\} = \eta(X^n).$$

This proves the first assertion.

Given that $gcd(i, t) = 1$, then $f_d = 1$ for all d. Thus

$$\begin{aligned} tA_i &= \sum_{0 \neq d \mid t} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})}\mu\left(\frac{t}{df_d}\right) \\ &= \sum_{0 \neq d \mid t} B_d \mu\left(\frac{t}{d}\right). \end{aligned}$$

Each term except $d = t$ is a no reduction term. The main idea is that for an i satisfying $gcd(i, t) \neq 1$, the complete reduction term(s) in A_i dominate the contribution of the partial reduction terms. By Theorem 3.0.35, we focus on the situation where $t \mid n$. First specialize to the situation where $i = p$ for a prime dividing t. We aim to show $t\left(A_p - A_1\right) \geq 0$.

$$tA_1 = \sum_{0 \neq d \mid t} B_d \mu\left(\frac{t}{d}\right).$$

Since p is prime, $f_d = 1$ or $f_d = p$. So, we split up the divisors of t according to the value of f_d.

$$tA_p = \sum_{0 \neq d \mid t} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{df_d})}\mu\left(\frac{t}{df_d}\right) = \sum_{\substack{0 \neq d \mid t \\ f_d = p}} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{dp})}\mu\left(\frac{t}{dp}\right) + \sum_{\substack{0 \neq d \mid t \\ f_d = 1}} B_d \mu\left(\frac{t}{d}\right).$$

$$\begin{aligned}
t\left(A_p - A_1\right) &= \sum_{\substack{0\neq d|t\\ f_d=p}} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{dp})}\mu\left(\frac{t}{dp}\right) + \sum_{\substack{0\neq d|t\\ f_d=1}} B_d\mu\left(\frac{t}{d}\right) - \sum_{0\neq d|t} B_d\mu\left(\frac{t}{d}\right)\\
&= \sum_{\substack{0\neq d|t\\ f_d=p}} B_d\left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{dp})}\mu\left(\frac{t}{dp}\right) - \mu\left(\frac{t}{d}\right)\right]\\
&= (\phi(p)-\mu(p))B_{\frac{t}{p}} + \sum_{\substack{0\neq d\neq \frac{t}{p}\\ f_d=p}} B_d\left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{dp})}\mu\left(\frac{t}{dp}\right) - \mu\left(\frac{t}{d}\right)\right].
\end{aligned}$$

The right hand side has exactly $\tau\left(\frac{t}{p}\right)$ terms. The term $(\phi(p)-\mu(p))B_{\frac{t}{p}}$ is the only complete reduction term, and the other $\tau\left(\frac{t}{p}\right)-1$ terms are partial reduction terms.

$$\begin{aligned}
t\left(A_p - A_1\right) &\geq (\phi(p)-\mu(p))B_{\frac{t}{p}} + \sum_{\substack{0\neq d\neq \frac{t}{p}\\ f_d=p}} B_d\left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{dp})}(-1) - 1\right]\\
&\geq (\phi(p)-\mu(p))B_{\frac{t}{p}} - \sum_{\substack{0\neq d\neq \frac{t}{p}\\ f_d=p}} B_d\left[p+1\right] \text{ by Remark 3.0.42}
\end{aligned}$$

Let q be the smallest prime dividing $\frac{t}{p}$. (If no such prime exists, then $t = p$ and $\tau\left(\frac{t}{p}\right) - 1 = 0$.)

$$\begin{aligned}
t\left(A_p - A_1\right) &\geq (\phi(p)-\mu(p))B_{\frac{t}{p}} - \left(\tau\left(\frac{t}{p}\right)-1\right)\left[p+1\right]B_{\frac{t}{pq}} \text{ by Lemma 3.0.34}\\
&\geq pB_{\frac{t}{p}} - \left(\tau\left(\frac{t}{p}\right)-1\right)\left[p+1\right]B_{\frac{t}{pq}}\\
&\geq p\left(1+\frac{t}{p}\right)B_{\frac{t}{pq}} - \left(\tau\left(\frac{t}{p}\right)-1\right)\left[p+1\right]B_{\frac{t}{pq}} \text{ by Lemma 3.0.32}\\
&\geq \left[p\left(1+\frac{t}{p}\right) - \left(\tau\left(\frac{t}{p}\right)-1\right)\left[p+1\right]\right]B_{\frac{t}{pq}}
\end{aligned}$$

Thus if $p\left(1+\frac{t}{p}\right) > \left(\tau\left(\frac{t}{p}\right)-1\right)\left[p+1\right]$, then $t\left(A_p - A_1\right) > 0$.

Lemma 3.0.44. $p\left(1+\frac{t}{p}\right) > \left(\tau\left(\frac{t}{p}\right)-1\right)[p+1]$.

Proof. We split the proof of this lemma into two cases.

Let $\frac{t}{p} > 16$. Then $2\sqrt{\frac{t}{p}} \leq \frac{t}{2p}$. Since $\tau\left(\frac{t}{p}\right) < 2\sqrt{\frac{t}{p}}$,

$$(p+1)\tau\left(\frac{t}{p}\right) < (p+1)\frac{t}{2p} = \frac{t}{2} + \frac{t}{2p} < t < t+2p+1.$$

If $\frac{t}{d} \leq 16$, then case by case exhaustion observations contained in the appendix verifies the result. □

We have now shown that $A_1 \leq A_p$ for all primes p dividing t. A straight forward variation of the above proof on the factors of i will prove the more general result that $A_1 \leq A_i$ for all i where $gcd(i,t) \neq 1$.

□

We demonstrate the modifications needed in a special case.

Example 3.0.45. Consider the situation where $t = 36$ and $gcd(i,t) = 6$. We show that $(A_6 - A_1) \geq 0$.

Proof.

$$tA_6 = \sum_{\substack{0\neq d|t \\ f_d=6}} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{6d})}\mu\left(\frac{t}{6d}\right) + \sum_{\substack{0\neq d|t \\ f_d=3}} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{3d})}\mu\left(\frac{t}{3d}\right)$$
$$+ \sum_{\substack{0\neq d|t \\ f_d=2}} B_d \frac{\phi(\frac{t}{d})}{\phi(\frac{t}{2d})}\mu\left(\frac{t}{2d}\right) + \sum_{\substack{0\neq d|t \\ f_d=1}} B_d \mu\left(\frac{t}{d}\right).$$

Thus

$$t(A_6 - A_1) = \sum_{\substack{0\neq d|t \\ f_d=6}} B_d \left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{6d})}\mu\left(\frac{t}{6d}\right) - \mu\left(\frac{t}{d}\right)\right] + \sum_{\substack{0\neq d|t \\ f_d=3}} B_d \left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{3d})}\mu\left(\frac{t}{3d}\right) - \mu\left(\frac{t}{d}\right)\right]$$
$$+ \sum_{\substack{0\neq d|t \\ f_d=2}} B_d \left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{2d})}\mu\left(\frac{t}{2d}\right) - \mu\left(\frac{t}{d}\right)\right] + \sum_{\substack{0\neq d|t \\ f_d=1}} B_d \left[\frac{\phi(\frac{t}{d})}{\phi(\frac{t}{1d})}\mu\left(\frac{t}{1d}\right) - \mu\left(\frac{t}{d}\right)\right].$$

The last summand consists of the no reduction terms canceling with the corresponding terms in A_1. To each of the above sums, we split off its corresponding complete reduction term.

$$\begin{aligned}
t(A_6 - A_1) = {} & [\phi(6) - \mu(6)]\, B_6 + \left[\frac{\phi(36)}{\phi(6)}\mu\,(6) - \mu\,(36)\right] B_1 \text{ terms reduced by 6} \\
& + \left[\frac{\phi(18)}{\phi(3)}\mu\,(3) - \mu\,(18)\right] B_2 + \left[\frac{\phi(12)}{\phi(2)}\mu\,(2) - \mu\,(12)\right] B_3 \\
& + [\phi(3) - \mu(3)]\, B_{12} + \left[\frac{\phi(9)}{\phi(3)}\mu\,(3) - \mu\,(9)\right] B_4 \text{ terms reduced by 3} \\
& + [\phi(2) - \mu(2)]\, B_{18} + \left[\frac{\phi(4)}{\phi(2)}\mu\,(2) - \mu\,(4)\right] B_9 \text{ terms reduced by 2} \\
> {} & [\phi(6) - \mu(6)]\, B_6 - 7B_1 - 7B_2 - 7B_3 \text{ terms reduced by 6} \\
& + 3B_{12} - 4B_4 \text{ terms reduced by 3} \\
& + 2B_{18} - 3B_9 \text{ terms reduced by 2} \\
> {} & [\phi(6) - \mu(6)]\, B_6 - 7B_1 - 7B_2 - 7B_3 \\
& + 2(1 + 18)B_9 - 3B_9 \\
& + 3(1 + 12)B_4 - 4B_4
\end{aligned}$$

□

Theorem 3.0.46. *For $n_1 \neq n_2$, $\{\eta(\alpha^i X^{n_1}) \mid 0 \leq i \leq t-1\}$ and $\{\eta(\alpha^i X^{n_2}) \mid 0 \leq i \leq t-1\}$ are disjoint.*

This result was assumed in [26].

Proof. It suffices to show for a fixed n,

$$\max\{\eta(\alpha^i X^n) \mid i = 0, 1, \ldots, t-1\} < \min\{\eta(\alpha^i X^{n+1}) \mid i = 0, 1, \ldots, t-1\}.$$

By Theorem 3.0.43, it is sufficient to show $\eta(X^n) < \eta(\alpha X^{n+1})$. Now

$$t\eta(X^n) = tA_0 = \sum_{d|t} B_d \phi\left(\frac{t}{d}\right).$$

Suppose p_1 is the smallest prime dividing our fixed value of n and t. Then for all B_d, $B_{\frac{t}{p_1}} \geq B_d$, by Corollary 3.0.34.

$$\begin{aligned} t\eta(X^n) &= B_0 + \sum_{\substack{d|t \\ d<t}} B_d \phi\left(\frac{t}{d}\right) \\ &< B_0 + \sum_{\substack{d|t \\ d<t}} B_{\frac{t}{p_1}} \phi\left(\frac{t}{d}\right) \\ &= B_0 + B_{\frac{t}{p_1}} \sum_{\substack{d|t \\ d<t}} \phi\left(\frac{t}{d}\right) \\ &< B_0 + B_{\frac{t}{p_1}} t. \end{aligned}$$

To distinguish between the A and B terms for n and $n+1$, we denote with a bar those terms associated with $n+1$. Thus

$$t\eta(\alpha X^{n+1}) = t\overline{A}_1 = \sum_{d|t} \overline{B_d} \mu\left(\frac{t}{d}\right).$$

We reindex and split the sum according to the values of μ,

$$\sum_{d|t} \overline{B_d} \mu\left(\frac{t}{d}\right) = \sum_{d|t} \overline{B_{\frac{t}{d}}} \mu(d)$$

where d_1, d_2, and d_3 are divisors of t such that $\mu(d_1) = 1$, $\mu(d_2) = -1$, $\mu(d_3) = 0$. Thus

$$\sum_{d|t} \overline{B_{\frac{t}{d}}} \mu(d) = \sum_{d_1|t} \overline{B_{\frac{t}{d_1}}} \mu(d_1) + \sum_{d_2|t} \overline{B_{\frac{t}{d_2}}} \mu(d_2) + \sum_{d_3|t} \overline{B_{\frac{t}{d_3}}} \mu(d_3)$$
$$\sum_{d|t} \overline{B_{\frac{t}{d}}} \mu(d) = \sum_{d_1|t} \overline{B_{\frac{t}{d_1}}} + \sum_{d_2|t} \overline{B_{\frac{t}{d_2}}} (-1).$$

Define H to be the number of (possibly zero) summands in $\sum_{d_2|t} \overline{B_{\frac{t}{d_2}}}(-1)$. Equivalently, H is the number of nonunit, squarefree divisors of $n+1$ with an odd number of distinct primes in its prime factorization. Additionally, let p_2 denote the smallest prime in the prime factorization of $gcd(n+1,t)$. Then

$$\begin{aligned} t\eta(\alpha X^{n+1}) &= \overline{B_0} + \sum_{\substack{d_1|t \\ d_1\neq 1}} \overline{B_{\frac{t}{d_1}}} - \sum_{d_2|t} \overline{B_{\frac{t}{d_2}}} \\ &> \overline{B_0} - \sum_{d_2|t} \overline{B_{\frac{t}{d_2}}} \\ &> \overline{B_0} - \overline{B_{\frac{t}{p_2}}} \sum_{d_2|t} \text{ by Corollary 3.0.34} \\ &= \overline{B_0} - H\overline{B_{\frac{t}{p_2}}}. \end{aligned}$$

To show $\eta(X^n) < \eta(\alpha X^{n+1})$, we show $B_0 + B_{\frac{t}{p_1}} t < \overline{B_0} - H\overline{B_{\frac{t}{p_2}}}$. We considered p_1 and p_2, which are the smallest primes dividing $gcd(n,t)$ and $gcd(n+1,t)$, respectively. So, we examine cases where these terms are not available.

Cases of p_1,p_2

1. Suppose $gcd(n,t) = gcd(n+1,t) = 1$.

   By Proposition 3.0.36, $|\{A_i \mid 0 \leq i \leq t-1\}| = 1$, and $\left|\{\overline{A}_i \mid 0 \leq i \leq t-1\}\right| = 1$. Moreover, $t\eta(X^n) = B_0$ and $t\eta(\alpha X^{n+1}) = \overline{B_0}$. It suffices to show $B_0 < \overline{B_0}$, which is clear by definition.

2. Suppose $gcd(n+1,t) = 1$ and $gcd(n,t) \neq 1$.

   As above, $t\eta(\alpha X^{n+1}) = \overline{B_0}$. It is sufficient to show that $(B_0 + B_{\frac{t}{p_1}} t) < \overline{B_0}$. Since $n > 0$,

$$\begin{gathered} t \leq n+t-1 \Rightarrow \\ t \prod_{f=1}^{\frac{t}{p_1}-1} \left(\frac{p_1 f + n}{p_1 f}\right) < (n+t-1) \prod_{f=2}^{t-2} \left(\frac{n+f}{f}\right) \Rightarrow \\ tB_{\frac{t}{p_1}} < \frac{t-1}{n+1} B_0 \Rightarrow \\ B_0 + tB_{\frac{t}{p_1}} < B_0 + \frac{t-1}{n+1} B_0 = \overline{B_0}. \end{gathered}$$

3. Suppose $gcd(n,t) = 1$ and $gcd(n+1,t) \neq 1$.

Then $t\eta(X^n) = B_0$, and $t\eta(\alpha X^{n+1}) > \overline{B_0} - H\overline{B_{\frac{t}{p_2}}}$. It is sufficient to show that $B_0 < \overline{B_0} - H\overline{B_{\frac{t}{p_2}}}$.

Lemma 3.0.47. *$H \leq n - 1$ for $2 \leq n$.*

Proof. Suppose that $n + 1 = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$ is the factorization of $n + 1$ into distinct primes p_i for $1 \leq i \leq s$. Recall that H is the number of nonunit, squarefree divisors of $n + 1$ with an odd number of distinct primes in its prime factorization. Thus $H = 2^{s-1}$.

(a) If $s = 1$, then $H = 1$. Thus $1 \leq n - 1$ for $2 \leq n$.

(b) If $s \neq 1$, then $2^{s-1} + 2 \leq (3)2^{s-1} \leq n + 1$ since the above p_i's are pairwise distinct.

□

Thus

$$H \leq n + t - 1 \Rightarrow$$
$$H \prod_{f=1}^{\frac{t}{p_2}-1} \left(\frac{p_2 f + n + 1}{p_2 f} \right) < (n + t - 1) \prod_{f=2}^{t-2} \left(\frac{n + f}{f} \right) \Rightarrow$$
$$H\overline{B_{\frac{t}{p_2}}} < \frac{t-1}{n+1} B_0 \Rightarrow$$
$$B_0 + H\overline{B_{\frac{t}{p_2}}} < B_0 + \frac{t-1}{n+1} B_0 = \overline{B_0} \Rightarrow$$
$$B_0 < \overline{B_0} - H\overline{B_{\frac{t}{p_2}}}.$$

4. If $gcd(n,t) \neq 1$ and $gcd(n + 1, t) \neq 1$, then it suffices to show $B_0 + tB_{\frac{t}{p_1}} < \overline{B_0} - H\overline{B_{\frac{t}{p_2}}}$.

Lemma 3.0.48. *Let $B := \max\left(B_{\frac{t}{p_1}}, \overline{B_{\frac{t}{p_2}}}\right)$. Then $B < \prod_{f=2}^{t-2} \left(\frac{n+f}{f}\right)$.*

The proof is contained in the appendix. Thus

$$\begin{aligned}
H &\leq n-1 \Rightarrow && \text{by Lemma 3.0.47}\\
t+H &\leq t+n-1 \Rightarrow && \\
(t+H)\,B &< (n+t-1)\prod_{f=2}^{t-2}\left(\frac{n+f}{f}\right) \Rightarrow && \text{by Lemma 3.0.48}\\
(t+H)\,B &< \frac{t-1}{n+1}B_0 \Rightarrow && \\
tB_{\frac{t}{p_1}} \leq tB &< \frac{t-1}{n+1}B_0 - HB \leq \frac{t-1}{n+1}B_0 - H\overline{B_{\frac{t}{p_2}}} \Rightarrow && \text{by Lemma 3.0.48}\\
B_0 + tB_{\frac{t}{p_1}} &< \overline{B_0} - H\overline{B_{\frac{t}{p_2}}}. &&
\end{aligned}$$

We have thus exhausted all of the cases. Therefore for a fixed n,

$$\max\{\eta(\alpha^i X^n) \mid i = 0, 1, \ldots, t-1\} < \min\{\eta(\alpha^i X^{n+1}) \mid i = 0, 1, \ldots, t-1\}.$$

□

Recall

$$\begin{aligned}
\mu(R,n) &= \{\eta_R(x) \mid x \in \gamma_R(n)\}\\
&= \bigcup_{k=0}^{n}\bigcup_{i=0}^{t-1}\left\{\eta(\alpha^i X^k g_{n-k}(X))\right\}\\
&= \bigcup_{k=0}^{n}\bigcup_{i=0}^{t-1}\left\{\eta(\alpha^i X^k)\right\}.
\end{aligned}$$

Thus

$$\Lambda(R,n) = \left|\bigcup_{k=0}^{n}\bigcup_{i=0}^{t-1}\left\{\eta_R(\alpha^i X^k)\right\}\right|.$$

By Theorem 3.0.46, the collections of factorizations are distinct across different powers k, and

$$\Lambda(R,n) = \sum_{k=0}^{n}\left|\bigcup_{i=0}^{t-1}\left\{\eta_R(\alpha^i X^k)\right\}\right|.$$

To count the total number of different numbers of factorizations, it is sufficient to count the number of different factorizations for each fixed value up to n and add them. Recall from Theorem 3.0.35 that the number of different numbers of irreducible factorizations in R for a fixed value of n and t is $\tau(gcd(t,k))$. Hence,

$$\left|\bigcup_{i=0}^{t-1}\left\{\eta_R(\alpha^i X^k)\right\}\right| = \tau(gcd(t,k)).$$

Thus

$$\Lambda(R,n) = \sum_{k=0}^{n} \tau(gcd(t,k)).$$

We rely on the following result from elementary number theory contained in the appendix.

Remark 3.0.49.

$$\sum_{k=0}^{t} \tau(gcd(t,k)) = \sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d) = \sigma(t).$$

Theorem 3.0.50. *Let $R = K + XF[X]$, where $K \subset F$ is a proper extension of fields of finite fields such that $t = \left|\frac{F^*}{K^*}\right|$. Then $\overline{\Lambda}(R) = \frac{\sigma(t)}{t}$.*

Proof. If $n = tm + l$ for $0 \le l \le t-1$, then

$$\begin{aligned}\Lambda(R,n) &= \sum_{k=0}^{n} \tau(gcd(t,k)) \\ &= \left[m * \sum_{k=0}^{t} \tau(gcd(t,k)) + \sum_{s=0}^{l} \tau(gcd(t,s))\right] \\ &= \left[m * \sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d) + \sum_{s=0}^{l} \tau(gcd(t,s)).\right]\end{aligned}$$

Thus,

$$\begin{aligned}
\overline{\Lambda}(R) = \lim_{n\to\infty} \frac{\Lambda(R,n)}{n} &= \lim_{n\to\infty} \frac{1}{n}\left[m * \sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d) + \sum_{s=0}^{l} \tau(gcd(t,s))\right] \\
&= \lim_{m\to\infty} \frac{m * \sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d) + \sum_{s=0}^{l} \tau(gcd(t,s))}{tm+l} \\
&= \lim_{m\to\infty} \frac{m * \sigma(t) + \sum_{s=0}^{l} \tau(gcd(t,s))}{tm+l} \\
&= \lim_{m\to\infty} \left[\frac{\sigma(t)}{t} + \frac{\sum_{s=0}^{l} \tau(gcd(t,s)) - \frac{\sigma(t)s}{t}}{tm+l}\right] \\
&= \frac{\sigma(t)}{t}.
\end{aligned}$$

□

This settles Conjecture 4.6 in [26].

This is quite satisfying. The previously known values of $\overline{\Lambda}(R)$ were 0, 4/3 , and ∞.

We informally discuss the following example.

Example 3.0.51. Let $t = 27 = 3^3$, $\overline{\Lambda}(R) = \frac{\sigma(27)}{27} = 40/27$.

Let $x := e^{\frac{2\pi\imath}{27}}$. $A_i := \eta(\alpha^i X^n)$ and $t\eta(\alpha^i X^n) = \sum_{k=0}^{t-1} B_k x^{-ki}$. Using the fact that if $gcd(27,k) = a$, then $B_k = B_a$ we group together the sum on the right hand side according the divisors of 27.

$$\eta(\alpha^i X^n) = \frac{1}{t}\left[B_0 + B_1 \sum_{ord_3(k)=0} x^{-ik} + B_3 \sum_{ord_3(k)=1} x^{-ik} + B_9 \sum_{ord_3(k)=2} x^{-ik}\right].$$

We continue simplifying the sum on the right hand side depending on the values of i. Informally, we have split the sum in the following manner.

$$\begin{aligned}
27\eta(\alpha^i X^n) = B_0 + B_1&(\text{sum of i-th powers of the primitive 27th roots}) \\
&+B_3(\text{sum of i-th powers of primitive 9th roots}) \\
&+B_9(\text{sum of i-th powers of primitive 3rd roots}).
\end{aligned}$$

Cases of i

1. If $gcd(t, i) = 1$, then

$$27\eta(\alpha^i X^n) = B_0 + B_1\mu(27) + B_3\mu(9) + B_9\mu(3) = B_0 - B_9.$$

2. If $gcd(t, i) = 3$, then

$$27\eta(\alpha^i X^n) = B_0 + B_1\frac{\phi(3^3)}{\phi(3^2)}\mu(9) + \frac{\phi(3^2)}{\phi(3^1)}B_3\mu(3) + B_9\phi(3).$$

3. If $gcd(t, i) = 9$, then

$$27\eta(\alpha^i X^n) = B_0 + B_1\frac{\phi(3^3)}{\phi(3^1)}\mu(3) + B_3\phi(3^2) + B_9\phi(3).$$

4. If $i = 0$, then

$$27\eta(\alpha^i X^n) = B_0 + B_1\phi(3^3) + B_3\phi(3^2) + B_9\phi(3).$$

Now, the quantities B_1, B_3, B_9 all depend on n.

Cases of n

1. If $gcd(t, n) = 1$, then $B_1 = B_3 = B_9 = 0$, and

$$\left|\{\eta(\alpha^i X^n) \mid i = 0, 1 \cdots, 26\}\right| = 1.$$

2. If $gcd(t, n) = 3$, then $B_1 = B_3 = 0, B_9 \neq 0$, and

$$\left|\{\eta(\alpha^i X^n) \mid i = 0, 1 \cdots, 26\}\right| = 2.$$

3. If $gcd(t, n) = 9$, then $B_1 = 0$ and B_3 and B_9 are distinct and nonzero, and

$$\left|\{\eta(\alpha^i X^n) \mid i = 0, 1 \cdots, 26\}\right| = 3.$$

4. If $n = 0 \pmod{27}$, then B_1,B_3, B_9 are all distinct and nonzero, and

$$\left|\{\eta(\alpha^i X^n) \mid i = 0, 1 \cdots, 26\}\right| = 4.$$

Now $\gamma_R(n) = \bigcup_{k=0}^{n}\{\alpha^i X^k g_{n-k}(X) \mid i = 0, 1, \ldots, t-1\}$, where $g_{n-k}(X)$ is a product of primes in R of degree $n-k$. Write $n = tm + l$, where $0 \leq l \leq t-1$. By Theorem 3.0.46, different values of l create disjoint sets of the number of factorizations of X^{27m+l}, we can add up the number of distinct factorizations per equivalence class of t.

For a fixed value of $m > 0$,

$$\begin{aligned}\sum_{s=0}^{t-1} \Big| \bigcup_{i=0}^{26} \eta(\alpha^i X^{27m+s})\Big| &= \tau(27) + \phi(27)\tau(1) + \phi(9)\tau(3) + \phi(3)\tau(9) \\ &= 4 + 18 + 12 + 6 = 40 = \sigma(27).\end{aligned}$$

Since different values of l create disjoint sets of the number of factorizations of X^{27m+l},

$$\Lambda(R, n) = m * \sum_{s=0}^{t-1}\left|\bigcup_{i=0}^{t-1}\{\eta(\alpha^i X^{27m+s})\}\right| + \sum_{s=0}^{l}\left|\bigcup_{i=0}^{t-1}\eta(\alpha^i X^s)\right|.$$

Finally,

$$\begin{aligned}\lim_{n\to\infty}\frac{\Lambda(R, n)}{n} &= \lim_{m\to\infty}\frac{\sigma(27) * m + \sum_{s=0}^{l}\left|\bigcup_{i=0}^{t-1}\eta(\alpha^i X^s)\right|}{27m + l} \\ &= \lim_{m\to\infty}\left[\frac{\sigma(27)}{27} + \frac{\sum_{s=0}^{l}\left|\bigcup_{i=0}^{t-1}\eta(\alpha^i X^s)\right| - \frac{\sigma(27)s}{27}}{27m + s}\right] \\ &= \frac{\sigma(27)}{27} = \frac{40}{27}.\end{aligned}$$

Chapter 4

Krull Domains with finite class group

In this section, we attack the invariant $\overline{\Lambda}(R)$ using more combinatorial reasoning. The following results from [8] will be generalized.

Theorem. *Let R be a Krull domain such the Cl(R) has an element of finite order with infinitely many height-one prime ideals in the divisor class. Then $\overline{\Lambda}(R) = 0$ if and only if R is a UFD.*

Theorem. *Let R be a Krull domain with Cl(R) finite. Then $\overline{\Lambda}(R) = 0$ if and only if R is a UFD.*

The main proof idea is to manipulate the different groupings of height-one primes to manufacture differing numbers of numbers of nonassociate factorizations.

The preliminary observations can be split into 2 main sections. A combinatorial section focusing on results concerning group actions and Young Tableau, and an algebraic section concerning distributions of height-one primes in the divisor class group of a Krull domain. Some general resources for Krull domains are [16] and [18]. Some general resources for combinatorics in this section are [28] and [24].

We will require a slight modification of the next two results.

1. [23, Theorem 60] A semilocal Dedekind domain is a PID.

2. [16, Lemma 13.9] If R is a Dedekind domain and all but finitely many of its height-one primes are principal, then R is a PID.

A straight forward modification of the proof of Lemma 13.9 results in a proof of

Remark 4.0.52. If R is a Krull domain and all but finitely many of its height one primes are principal, then R is a UFD.

Proof. Let $P_1, \dots P_k$ be the non-principal height-one primes of R. Let Q_i denote the principal height one primes and $\alpha_i R = Q_i$. Let υ_{P_i}, and υ_{Q_i} denote the valuations of R_{P_i} and R_{Q_i}, respectively. By the Krull Approximation theorem, we can find to each $1 \leq j \leq k$ a $x_j \in R$ satisfying $\upsilon_{P_j}(x_j) = 1$ and $\upsilon_{P_j}(x_i) = 0$ for $i \neq j$ and $\upsilon_{Q_i} \geq 0$ for all i. So, $\upsilon_{Q_i}(x_1) \geq 0$ for infinitely many principal height one primes, but since R satisfies finite character we know that there exists a finite collection so that $\upsilon_{Q_{i_1}}(x_1) > 0$.

Thus translating the comments concerning valuations to v-factorizations

$$\begin{aligned} x_1 R &= \left(P_1 Q_{i_1}^{n_1} Q_{i_2}^{n_2} \dots Q_{i_k}^{n_k} \right)_v \\ &= \alpha_1^{n_1} \alpha_2^{n_2} \dots \alpha_k^{n_k} P_1 \end{aligned}$$

Each of the α_i's are prime elements of R, so there exists an $\overline{x}_1$ satisfying $x_1 = \overline{x}_1 \alpha_1^{n_1} \alpha_2^{n_2} \dots \alpha_k^{n_k}$. Thus $\upsilon_{P_1}(\overline{x}_1) = 1$, and $\upsilon_{P_j}(\overline{x}_1) = 0$ for $j \neq i$, and $\upsilon_{Q_i}(\overline{x}_1) = 0$. Hence R is a UFD by [16, Result 43.14]. □

It is known that

Theorem. *[8, Lemma 18.2.6] Let R be a Krull domain such that $Cl(R)$ has an element of finite order with infinitely many height-one prime ideals in that divisor class. Then $\overline{\Lambda}(R) = 0$ if and only if R is a UFD.*

Suppose that R is a Krull domain such that some nonzero divisor class g with finite order $k \geq 2$ contains infinitely many height-one prime ideals of R. Choose distinct height-one prime ideals $\{P_n \mid 1 \leq n < \infty\}$ in the class of g. For each n and each partition $\beta \vdash nk$

where $\beta = \sum_{i=1}^{j} \beta_i$ is written in weakly decreasing order, we define nonzero, nonunits of R $x_{n,\beta}$ such that there are β_i copies of the height-one prime P_i in the v-factorization. This is a specialization of the idea that the multiset of P_i's is given by the partition β in the standard way.

We demonstrate how to characterize differing factorizations using functions.

Example 4.0.53. Let $1980 \in \mathbb{Z}$. Then $1980 = (2^2)(3^2)(5)11$, and $l_{\mathbb{Z}}(1980) = 6$. We may associate to any factorization of 1980 a function $f : \{1,2,3,4,5,6\} \mapsto \{2,3,5,11\}$ by $f(i) = j$ if the prime j sits in i-th 'position' of the factorization. Any such function will satisfy $f^{-1}(2) = f^{-1}(3) = 2$, and $f^{-1}(5) = f^{-1}(11) = 1$. Any 2 such functions represent associated factorizations of 1980 in $\mathbb{Z}$.

Example 4.0.54. Let $x_{4,4+4} \in R$ have 4 copies of the height-one prime P_1 and 4 copies of the height-one prime P_2 in its v-factorization, and P_1 and P_2 both have order 2 in $Cl(R)$.

We may associate to a factorization of $x_{4,4+4}$ a function $f : \{1,2,3,4,5,6,7,8\} \mapsto \{P_1, P_2\}$ by $f(i) = P_j$ if the height-one prime P_j sits in i-th 'position' of the factorization.

$$\begin{aligned} x_{4,4+4}R &= ((P_1P_1)_v(P_1P_1)_v(P_2P_2)_v(P_2P_2)_v)_v \\ &= ((P_1P_1)_v(P_1P_2)_v(P_1P_2)_v(P_2P_2)_v)_v \\ &= ((P_1P_2)_v(P_1P_2)_v(P_1P_2)_v(P_1P_2)_v)_v . \end{aligned}$$

The main idea of this section involves viewing nonassociate factorizations in R as equivalent functions up to a suitable group action. As in the proofs of [8, Lemma 18.2.6, Example 18.2.9], we manipulate groupings of height one primes in order to create nonassociate factorizations. However, we formalize this manipulation with group actions.

Definition 4.0.55. The *content* of the function, $f : \{1,2,\ldots,nk\} \to \{1,2,\ldots,nk\}$, denoted $c(f)$, is the following sequence

$$c(f) := (\lambda_1, \lambda_2, \ldots), \text{ where } \lambda_i := \left| f^{-1}(i) \right| .$$

In Example 4.0.53, if f and g satisfy $c(f) = c(g)$, then the factorizations associated to f and g are associates in R. In Example 4.0.54, if f and g satisfy $c(f) = c(g)$, then the factorizations associated to f and g may not be associates in R.

Example 4.0.56. Consider the following elements.

$$x_{4,4+4}R = ((P_1P_1)_v(P_1P_1)_v(P_2P_2)_v(P_2P_2)_v)_v$$

$$\overline{x}_{4,4+4}R = ((P_3P_3)_v(P_3P_3)_v(P_4P_4)_v(P_4P_4)_v)_v$$

Here are facts concerning the two factorizations.

1. $x_{4,4+4}$ has content $(4,4)$, and $\overline{x}_{4,4+4}$ has content $(0,0,4,4)$. $x_{4,4+4}$ has 4 copies each of the height-one primes P_1 and P_2. $\overline{x}_{4,4+4}$ has 4 copies each of the height-one primes P_3 and P_4.

2. $x_{4,4+4}$ and $\overline{x}_{4,4+4}$ are not associates in R.

3. $\eta(x_{4,4+4}) = \eta(\overline{x}_{4,4+4}) = 3$.

Example 4.0.57. Consider the following elements of R.

$$x_{4,4+2+2}R = ((P_1P_1)_v(P_1P_1)_v(P_2P_2)_v(P_3P_3)_v)_v$$

$$\overline{x}_{4,4+2+2}R = ((P_2P_2)_v(P_2P_2)_v(P_1P_1)_v(P_4P_4)_v)_v$$

1. $c(x_{4,4+2+2}) = (4,2,2)$, and $c(\overline{x}_{4,4+2+2}) = (2,4,0,2)$.

2. $x_{4,4+2+2}$ and $\overline{x}_{4,4+2+2}$ are not associates in R.

3. $\eta(x_{4,4+2+2}) = \eta(\overline{x}_{4,4+2+2}) = 7$.

It is precisely members of the sequence of the content, not their order, that stores the crucial information concerning the number of nonassociate factorizations (orbits). The above example motivates the underlying assumption for the rest of the treatment. We restrict our attention to terms $x_{n,\beta}$ so that if $\beta = \sum_{i=1}^{n} k\beta_i$, then $c(x_{n,\beta}) = (\beta_1, \beta_2, \ldots, \beta_k)$.

The practice of considering content as an integer partition instead of strictly as a sequence follows the treatment of [**?**]kerber, and [25].

Example 4.0.58. Consider the situation where $k = 2$, $n = 4$ and varying β's.

$$\begin{aligned} x_{4,6+2}R &= ((P_1P_1)_v(P_1P_1)_v(P_1P_1)_v(P_2P_2)_v)_v \\ &= ((P_1P_1)_v(P_1P_1)_v(P_1P_2)_v(P_1P_2)_v)_v. \end{aligned}$$

$$\begin{aligned} x_{4,4+4}R &= ((P_1P_1)_v(P_1P_1)_v(P_2P_2)_v(P_2P_2)_v)_v \\ &= ((P_1P_1)_v(P_1P_2)_v(P_1P_2)_v(P_2P_2)_v)_v \\ &= ((P_1P_2)_v(P_1P_2)_v(P_1P_2)_v(P_1P_2)_v)_v \,. \end{aligned}$$

$$\begin{aligned} x_{4,4+2+2}R &= ((P_1P_1)_v(P_1P_1)_v(P_2P_2)_v(P_3P_3)_v)_v \\ &= ((P_1P_1)_v(P_1P_2)_v(P_1P_2)_v(P_3P_3)_v)_v \\ &= ((P_1P_1)_v(P_1P_3)_v(P_1P_3)_v(P_2P_2)_v)_v \\ &= ((P_1P_1)_v(P_1P_1)_v(P_2P_3)_v(P_2P_3)_v)_v \\ &= ((P_1P_2)_v(P_1P_2)_v(P_1P_3)_v(P_1P_3)_v)_v \\ &= ((P_1P_1)_v(P_1P_2)_v(P_1P_3)_v(P_2P_3)_v)_v. \end{aligned}$$

Remark 4.0.59. By choice of $x_{n,\beta} \in R$, $l_R(x_{n,\beta}) = n$ for all $\beta \vdash nk$.

Definition 4.0.60. If $\beta = \sum_{i=1}^{k} \beta_i$ and $\alpha = \sum_{i=1}^{h} \alpha_i$ are integer partitions of n written in weakly decreasing order of their parts, then β is said to *dominate* α (denoted $\alpha \trianglelefteq \beta$) if and only if $\sum_{i=1}^{s} \beta_i \geq \sum_{i=1}^{s} \alpha_i$ for all $1 \leq s \leq h$.

The previously chosen 3 partitions of 8 give an indication that the number of number of factorizations and the dominance order of partitions may be connected.

β	$\eta(x_{n,\beta})$
8	1
$6+2$	2
$4+4$	3
$4+2+2$	6
$2+2+2+2$	17

The above list demonstrates a stronger possible connection between partitions of a certain type and number of different numbers of factorizations of carefully chosen elements of length 4 in R. The remainder of this chapter will demonstrate a injective order reversing correspondence between elements in the partition lattice ordered by domination and the number of different number of factorizations in R. The motivation for this recharacterization of the problem is the following theorem in [24, Theorem 7.4.4] and an analogous theorem [25, Theorem 2].

Theorem 4.0.61. *If $\lambda, \mu \vdash n$ and $\lambda \trianglelefteq \mu$, then the number of G-classes of content λ on $Hom(X, Y)$ is greater than or equal to the number of G-classes of content μ. In particular, each sequence of numbers of G-classes of $Hom(X, Y)$ by content is monotone as soon as the partitions corresponding to the contents form a chain.*

Instead of directly enumerating some base cases through exhaustive techniques, we will enumerate $\eta(x_{n,\beta})$ using a group action on the collection of nk height-one prime ideals. This group G will need to take into account 2 facts.

F1 Commutativity of height-one primes within the factorization of a single irreducible element, i.e., the following ideal factorizations represent the principal ideal generated by the same irreducible element

$$(P_1P_3P_2P_4\dots P_k)_v = (P_1P_2P_3\dots P_k)_v\,.$$

F2 Commutativity of irreducible elements in a factorization. Using the notation above

$$\begin{aligned} x_{4,4+4}R &= ((P_1P_1)_v(P_1P_2)_v(P_1P_2)_v(P_2P_2)_v)_v \\ &= ((P_2P_2)_v(P_1P_2)_v(P_1P_2)_v(P_1P_1)_v)_v \,. \end{aligned}$$

Instead of viewing a specific v-factorization of $x_{n,\beta}R$ as a sequence of nk height-one primes, we may view it as a $n \times k$ matrix using the following rubric. The first β_1 entries of the matrix are given by (reading first left to right and then top to bottom) with the first β_1 height-one primes in the v-factorization of $x_{n,\beta}$. The next β_2 entries of the matrix are given by the next β_2 height-one primes in the v-factorization of $x_{n,\beta}$. Exhaustively distribute all height-one primes in an ideal factorization of $x_{n,\beta}R$ continuing in this fashion.

Remark 4.0.62. The v-product of the elements of row i for $1 \leq i \leq n$ is the height-one prime factorization of an irreducible element dividing $x_{n,\beta}$.

Example 4.0.63. Let $n = 5$, $k = 3$, and $\beta = 9 + 6$.

To

$$x_{5,9+6} = (P_1P_1P_1P_1P_1P_1P_1P_1P_2P_1P_2P_2P_2P_2P_2)_v$$

we associate the following matrix,

$$\begin{bmatrix} P_1 & P_1 & P_1 \\ P_1 & P_1 & P_1 \\ P_1 & P_1 & P_2 \\ P_1 & P_2 & P_2 \\ P_2 & P_2 & P_2 \end{bmatrix}.$$

Since we are interested in the number of different number of *nonassociate* factorizations of an element, we would like for this association to preserve associate factorizations in the domain R.

Remark 4.0.64. 1. Condition F1 above, the commutativity of height one primes inside the v-factorization of an irreducible element, is achieved by acting on the elements of a row of this matrix with S_k.

2. Condition F2 above, the commutativity of irreducible elements in a factorization, is achieved by acting on the collection of rows with S_n.

Example 4.0.65. Let $n = 5$, $k = 3$, and $\beta = 9 + 6$. Then the following matrices represent associate factorizations of the element $x_{5,9+6}$.

$$\begin{bmatrix} P_1 & P_1 & P_1 \\ P_1 & P_1 & P_1 \\ P_1 & P_1 & P_2 \\ P_1 & P_2 & P_2 \\ P_2 & P_2 & P_2 \end{bmatrix} \qquad \begin{bmatrix} P_2 & P_2 & P_2 \\ P_1 & P_1 & P_1 \\ P_1 & P_2 & P_1 \\ P_2 & P_1 & P_2 \\ P_1 & P_1 & P_1 \end{bmatrix}$$

Proof. Indeed, by reordering the entries in each row so that the indicies of the height one primes are weakly increasing and interchanging rows one and five of the right matrix one obtains the left matrix. Concretely let $y_1R := (P_1P_1P_1)_v$, $y_2R := (P_1P_1P_2)_v$, $y_3R := (P_1P_2P_2)_v$, and $y_4R := (P_2P_2P_2)_v$.

Starting at the left matrix we can directly rewrite the v-factorization resulting in the v-factorization represented by the right matrix.

$$\begin{aligned} x_{5,9+6}R &= ((P_1P_1P_1)_v(P_1P_1P_1)_v(P_1P_1P_2)_v(P_1P_2P_2)_v(P_2P_2P_2)_v)_v \\ &= (y_1y_1y_2y_3y_4)R \\ &= (y_4y_1y_2y_3y_1)R \text{ by F1} \\ &= ((P_2P_2P_2)_v(P_1P_1P_1)_v(P_1P_1P_2)_v(P_1P_2P_2)_v(P_1P_1P_1)_v)_v \\ &= ((P_2P_2P_2)_v(P_1P_1P_1)_v(P_1P_2P_1)_v(P_2P_1P_2)_v(P_1P_1P_1)_v)_v \text{ by F2.} \end{aligned}$$

□

Example 4.0.66. Let $n = 5$, $k = 3$, and $\beta = 9 + 6$. Then the following matrices represent nonassociate factorizations of the element $x_{5,9+6}$.

$$\begin{bmatrix} P_1 & P_1 & P_1 \\ P_1 & P_1 & P_1 \\ P_1 & P_1 & P_2 \\ P_1 & P_2 & P_2 \\ P_2 & P_2 & P_2 \end{bmatrix} \qquad \begin{bmatrix} P_1 & P_1 & P_2 \\ P_1 & P_1 & P_2 \\ P_1 & P_1 & P_2 \\ P_1 & P_1 & P_1 \\ P_2 & P_2 & P_2 \end{bmatrix}$$

Proof. Consider directly rewriting the v-factorization of both matrices using the notation $y_1R = (P_1P_1P_1)_v$, $y_2R = (P_1P_1P_2)_v$, $y_3R = (P_1P_2P_2)_v$, and $y_4R = (P_2P_2P_2)_v$.

$$\begin{aligned} x_{5,9+6}R &= ((P_1P_1P_1)_v(P_1P_1P_1)_v(P_1P_1P_2)_v(P_1P_2P_2)_v(P_2P_2P_2)_v)_v \\ &= (y_1y_1y_2y_3y_4)R. \end{aligned}$$

$$\begin{aligned} x_{5,9+6}R &= ((P_1P_1P_2)_v(P_1P_1P_2)_v(P_1P_1P_2)_v(P_1P_1P_1)_v(P_2P_2P_2)_v)_v \\ &= (y_3y_3y_2y_1y_4)R. \end{aligned}$$

By the uniqueness of the v-product, the two factorizations are nonassociate. $\square$

The group satisfying F1 (permuting elements in a row) and F2 (permuting the collection of rows) is known to be the wreath product $S_k \wr S_n$ (See comment number 5 below). Recall some facts about the wreath product $S_k \wr S_n$ [24, 1.3.1].

1. The underlying set of the wreath product is given by

$$\begin{aligned} S_k \wr S_n :&= Hom(\{1, 2, \ldots, n\}, S_k) \times S_n \\ &= \{(\phi, g) \mid \phi : \{1, 2, \ldots n\} \to S_k, g \in S_n\} \text{ with multiplication defined by} \\ &(\phi, g)(\phi', g') := (\phi\phi'_g, gg'), \phi\phi'_g(x) := \phi(x)\phi'_g(x) := \phi(x)\phi'(g^{-1}x). \end{aligned}$$

Let us denote by i the map in $Hom(\{1, 2, \ldots, n\}, S_k)$ sending each element to 1.

2. The base group S_k^* of $S_k \wr S_n$ is defined by

$$S_k^* := \{(\phi, 1) \mid \phi \in Hom(\{1, 2, \ldots, n\}, S_k)$$

and is isomorphic to the direct product of n copies S_k.

3. The subgroup $S_n' := \{(i, g) \mid g \in S_n\} \simeq S_n$ is a complement of S_k^* in the sense that

$$S_k \wr S_n = S_k^* \cdot S_n', \qquad S_k^* \trianglelefteq S_k \wr S_n, \qquad S_k^* \cap S_n' = \{(id, 1)\}.$$

The wreath product can be viewed as a the semidirect product of the base group and the complement with respect to an injective homomorphism from $S_n \to Aut(S_k^*)$ [15, p. 187].

4. The group actions S_n acting on $\{1, 2, \ldots, n\}$ and S_k acting on $\{1, 2, \ldots, k\}$ yield the following natural action of $S_k \wr S_n$ on $Hom(\{1, 2, \ldots, n\}, \{1, 2, \ldots, k\})$:

$$S_k \wr S_n \times Hom(\{1, 2, \ldots, n\}, \{1, 2, \ldots, k\}) \to Hom(\{1, 2, \ldots, n\}, \{1, 2, \ldots, k\}),$$
$$((\phi, g), f) \mapsto \overline{f}$$

where $\overline{f}$ is defined by $\overline{f}(x) := \phi(x) f(g^{-1}x)$.

5. By [24, 2.2.1 p. 59], there is an injective homomorphism from $S_k \wr S_n$ into S_{nk} given by

$$\delta : S_k \wr S_n \to S_{nk} : (\phi, \pi) \to \begin{pmatrix} jk + i \\ \pi j \cdot k + \phi(\pi j) i \end{pmatrix}$$

for $0 \leq i \leq k - 1$ and $0 \leq j \leq n - 1$.

This injection can be visualized in the following way. For a fixed index j, the image of the j-th direct factor of the base group S_k^* acts on the collection $\{j \cdot k + 0, \ldots, j \cdot k + k - 1\}$

as S_k acts on $\{1, 2, \ldots k\}$. Additionally, the image of the complement, S_n' of the base group, acts on the set of the n subsets for $0 \leq j \leq n-1$, $\{j \cdot k, \ldots, j \cdot k + k - 1\}$ as S_n acts on $\{1, 2, \ldots, n\}$.

In terms of our matrix representation, the image of the j-th direct factor of the base group S_k^* acts on the the $j+1$th row of the matrix by permuting the elements in that row. The image of the complement, S_n' of the base group, acts on the the collection of rows of the matrix by permuting them.

Remark 4.0.67. Instead of viewing the matrix as in the above examples as fixed, we instead may view a particular configuration of the matrix as the image of a map $f : \{1, 2, \ldots, nk\} \to \{1, 2, \ldots, nk\}$ where $f(l) = j$ if P_j is in the $(\lfloor \frac{l}{k} \rfloor + 1, l - k\lfloor \frac{l}{k} \rfloor)$-th position in the matrix. In this way, we identify 2 associate factorizations with a representative of an orbit of the group $S_k \wr S_n$ acting on the collection of functions $f : \{1, 2, \ldots, nk\} \to \{1, 2, \ldots, nk\}$.

Any factorization of $x_{5,9+6}$ viewed as a function from the 5×3 matrix to the collection of height-one primes has content $9+6$ since there are 9 entries with image 1 and 6 entries with image 2. The notation for $x_{5,9+6}$ has been chosen specifically to ensure that the content is at the forefront of our minds.

Lemma 4.0.68. *$\eta(x_{n,\beta})$ is equal to the number of elements in a transversal of the symmetry classes of content β determined by action of the wreath product $S_k \wr S_n$ on the functions from $\{1, 2, \ldots, nk\}$ to $\{1, 2, \ldots, nk\}$.*

Proof. By the above matrix reformulation, 2 factorizations of $x_{n,\beta}$ are associate if and only if they lie in the same orbit of the wreath product $S_k \wr S_n$ acting on the functions from $\{1, 2, \ldots, nk\}$ to $\{1, 2, \ldots, nk\}$. □

We create a lower estimate on $\Lambda(R, n)$ by restricting our attention to a transversal of the symmetry classes of content β determined by action of the wreath product $S_k \wr S_n$ on the functions from $\{1, 2, \ldots, nk\}$ to $\{1, 2, \ldots, n\}$. Reformulating in terms of the height-one primes, we are only considering those element factorizations such that each height-one prime in the v-factorization appears a multiple of k times. Let us introduce some new notation.

Definition 4.0.69.

1. Define $P^*(nk) := \{\alpha \vdash nk \mid \alpha = \sum_{l=i}^{n} k\alpha_i$ where for all i, $0 \leq \alpha_i \leq n\}$, and $p^*(nk) := |P^*(nk)|$.
2. Let $P(n, A, B)$ denote the set of partitions of n with at most A parts each part less than or equal to B, and $p(n, A, B) := |P(n, A, B)|$.

We specialize to the situation that α is dominated by β and there is nothing properly between them in the dominance order. We follow the treatment of [24, Theorem 6.1.15].

Definition 4.0.70. $\alpha \vdash n$ is *covered* by $\beta \vdash n$, denoted $\alpha \lhd \beta$, if and only if there exist indices i and j such that $0 \leq i < j$ and

1. $\beta_j = \alpha_j - 1$ and $\beta_i = \alpha_i + 1$, while for $l \neq i$ and $l \neq j$, we have $\alpha_l = \beta_l$.
2. $i = j - 1$ or $\alpha_i = \alpha_j$.

However this above definition does not take into account the restricted partition set $P^*(nk)$.

Definition 4.0.71. For $\alpha, \beta \in P^*(nk)$, α is *covered* by β, denoted $\alpha \lhd \beta$, if and only if there exist indices i and j such that $0 \leq i < j$ and

1. $\beta_j = \alpha_j - k$ and $\beta_i = \alpha_i + k$, while for $l \neq i$ and $l \neq j$, we have $\alpha_l = \beta_l$.
2. $i = j - 1$ or $\alpha_i = \alpha_j$.

Remark 4.0.72. By the first remark in the definition of $\alpha \lhd \beta$, these two partitions differ in exactly 2 summands. Let us denote these two summands by $\alpha_i + \alpha_j$ and $\beta_i + \beta_j$, respectively. In fact, we may find $v \in \mathbb{Z}^+$ and $w \in \mathbb{N}$ so that $\alpha_i + \alpha_j = vk + (w + 1)k$, and $\beta_i + \beta_j = (v + 1)k + wk$, where $vk \geq (w + 1)k$.

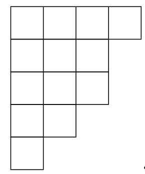
The Young diagram of a partition α is a 2-d visual representation of the partition α, and can be obtained from the summands of α using the following rubric [24, pg 183].

Definition 4.0.73. The Young Diagram ν can be considered as a subset of $\mathbb{N} \times \mathbb{N}$

$$\nu = \bigcup_k \{(i, 1), \ldots, (i, \alpha_k)\}$$

where (i, j) is the coordinate pair of the node in the i-th row and the j-th column of ν.

Example 4.0.74. The Young Diagram associated with the partition $4+3+3+2+1 \vdash 13$ is



.

Definition 4.0.75. Each mapping $T : \nu \to \{1, 2, \ldots, n\}$ given by $(i, j) \mapsto t_{ij}$ is called an ν-tableau over $\{1, 2, \ldots, n\}$.

Example 4.0.76.

1	1	2	3
2	2	3	
3	3	4	
4	5		
9			

1	1	2	2
2	3	3	
3	3	4	
4	5		
9			

3	3	2	5
2	1	1	
9	4	4	
2	3		
3			

Definition 4.0.77. The *shape* of an ν-tableau T is ν, and the *content* of the tableau T, denoted $c(T)$, is the following sequence

$$c(T) := (\lambda_1, \lambda_2, \ldots), \text{ where } \lambda_i := \left|T^{-1}(i)\right|.$$

As with our consideration of the content of a function, we restrict our attention to tableaux so that if the summands of $\beta \in P^*(nk)$ are in one-to-one correspondence with the images of the sequence $c(T)$, then $c(T) = (\beta_1, \beta_2, \ldots, \beta_k)$.

The sequence definition of content is more narrowly focused on special types of tableaux called Standard Young Tableaux and Semistandard Young Tableaux that will not be considered here. The collection of tableau T with shape ν and content ϕ will be denoted $T^\nu(\phi)$.

We say that tableau T_1 and T_2 are equivalent if T_1 and T_2 have the same shape and the functions ν_1 and ν_2 lie in the same orbit of the wreath product acting in the standard way.

Example 4.0.78.

$$T_1 := \begin{array}{cccc} 1 & 1 & 2 & 3 \\ 2 & 2 & 3 & \\ 3 & 3 & 4 & \\ 4 & 5 & & \\ 9 & & & \end{array}$$

is a tableau of shape $4+3+3+2+1$ and content $4+3+2+2+1+1$.

$$T_2 := \begin{array}{cccc} 1 & 1 & 2 & 2 \\ 2 & 3 & 3 & \\ 3 & 3 & 4 & \\ 4 & 5 & & \\ 9 & & & \end{array}$$

is a tableau of shape $4+3+3+2+1$ and content $4+3+2+2+1+1$. Moreover $T_1 \neq T_2$ since these two tableaux are not equivalent under the action of the wreath product. Informally, no permutation of the elements of any row combined with a permutation of the rows of T_1 will result in T_2.

Remark 4.0.79. The number of elements in a transversal of the equivalence classes of matrices of content β is the number of distinct tableau of shape $k^n := \underbrace{k+k+\cdots+k}_{n \text{ times}}$ and content β.

$$\eta(x_{n,\beta}) = |T^{k^n}(\beta)|.$$

Definition 4.0.80. $\lambda\backslash\nu$ is the *skew diagram* arising from deleting the sub-diagram of shape ν from the diagram of shape λ.

Example 4.0.81. Let $\lambda = 4+3+3+2+1$ and $\nu = 2+2+1$, then

$$\begin{array}{cccc} & & 2 & 3 \\ & & 3 & \\ & 3 & 4 & \\ 4 & 5 & & \\ 9 & & & \end{array}$$

is a skew tableau of shape $\lambda\backslash\nu$ and content $3+2+1+1+1$.

Lemma 4.0.82. *There is a well defined surjective map*

$$f : \{\eta(x_{n,\beta})\} \to \{\cup_{\nu\in P(\beta_j,n,k)} T^{\nu}(\beta_i + \beta_j)\}.$$

Proof. By our convention, there are β_i (respectively β_j) copies of the height one prime P_i (P_j) in the v-factorization of $x_{n,\beta}$. Using the action of the wreath product on this representative viewed as a matrix, we may left justify the height one primes associated with $\beta_i + \beta_j$ and then reorder the rows of the matrix so that the number of entries in each row containing P_i and P_j are weakly decreasing when read down the columns.

Suppose that m_1 and m_2 are two representatives of the same equivalence class in $x_{n,\beta}$. To each row there is a permutation of the elements combined with a permutation of the collection of rows of the matrix m_1 that results in the matrix m_2. Thus $f(m_1)$ and $f(m_2)$ the same actions result in equivalent tableau. Hence $f(m_1) = f(m_2)$.

Given a $T \in T^{\nu}(\beta_i + \beta_j)$, construct any skew-tableau $T_1 \in T^{k^n\backslash\nu}(\beta - (\beta_i + \beta_j)$. Now fit T and T_1 in together in a $n \times k$ matrix m. Then $f(m) = T$.

□

Proposition 4.0.83.

$$\eta(x_{n,\alpha}) = \sum_{\nu\in P(\alpha_i+\alpha_j,n,k)} |T^{\nu}(\alpha_i + \alpha_j)| \left| T^{n^k\backslash\nu}(\alpha - (\alpha_i + \alpha_j)) \right|.$$

Proof.

$$\eta(x_{n,\alpha}) = \sum_{\nu\in P(\alpha_i+\alpha_j,n,k)} |T^{\nu}(\alpha_i + \alpha_j)| \left| T^{n^k\backslash\nu}(\alpha - (\alpha_i + \alpha_j)) \right|.$$

The number of different tableaux of content β and shape k^n is enumerated in two ways. The left hand side by definition. The right hand side enumerates the quantity in disjoint subsets by first counting the number of different tableaux of a fixed shape ν and content $\beta_i + \beta_j$ which fit into the matrix, and then counting the number of skew-tableaux of shape $n^k\backslash\nu$ and content $\beta - (\beta_i + \beta_j)$ that forms the remainder of the $n \times k$ matrix. □

We will use the above proposition and the following facts concerning q-binomial coefficents to show our main result.

1. [24, Application 2.2.8-2.2.9] The orbits of $S_k \wr S_n$ on $2^{n\times k}$ are in one-to-one correspondence with the partitions of nk, where each part is at most k and the total number of parts is at most n. There is a one-to-one correspondence between the number of Young diagrams that fit into an $n \times k$ matrix and $P(nk, n, k)$.

2. This characterization can be thought of in terms of Tableau in the following manner. It is known [24, Application 2.2.8-2.2.9] that the number of distinct tableau that fit into a rectangular subtableau of size $l_i \times i$ with precisely γ_i copies of 1 is $p(\gamma_i, l_i, i)$.

3. [24, Theorem 7.4.16-7.4.17] The q-binomial coefficient is a unimodal polynomial in the sense that the coefficents weakly increase until the 'middle term' and then the coefficients weakly decrease.

4. [24, Lemma 7.4.9] The product of unimodal polynomials is unimodal.

Lemma 4.0.84. *If $\nu \in P(\alpha_i + \alpha_j, n, k)$, then*

$$|T^{\nu}(\alpha_i + \alpha_j)| \geq |T^{\nu}(\beta_i + \beta_j)| .$$

Proof. Let $\nu = 1^{l_1}2^{l_2}3^{l_3}\dots k^{l_k}$. Then

$$|T^{\nu}(\alpha_i + \alpha_j)| = \prod_{\sum_{i=1}^{l} \gamma_i = \alpha_j} P(\gamma_1, l_1, 1)P(\gamma_2, l_2, 2)\cdots P(\gamma_k, l_k, k).$$

Both sides count the number of distinct Tableau of shape ν with α_i copies of P_i and α_j copies of P_j distributed into the Tableau. The left hand side by definition, and the right side counts the collection by specifying a specific distribution of the α_j copies of the height-one prime P_j among the constituent rectangular subtableau inside the shape ν. It is known [24, Application 2.2.8-2.2.9] that the number of distinct tableau that fit into a rectangular subtableau of size $l_i \times i$ with precisely γ_i copies of 1 is $p(\gamma_i, l_i, i)$.

By [9, pg 39], the number of partitions of γ_i with at most l_i parts each of size at most i is the coefficient of q^{γ_i} in the polynomial $\binom{l_i+i}{i}_q$. Borrowing notation from [30], $p(\gamma_i, l_i, i) = [q^{\gamma_i}]\binom{l_i+i}{i}_q$.

Thus

$$\begin{aligned}
|T^\nu(\alpha_i+\alpha_j)| &= \prod_{\sum_{i=1}^l \gamma_i=\alpha_j} p(\gamma_1,l_1,1)p(\gamma_2,l_2,2)\cdots p(\gamma_k,l_k,k)\\
&= \prod_{\sum_{i=1}^l \gamma_i=\alpha_j} [q^{\gamma_1}]\binom{l_1+1}{1}_q [q^{\gamma_2}]\binom{l_2+2}{2}_q \cdots [q^{\gamma_k}]\binom{l_k+k}{k}_q\\
&= \prod_{\sum_{i=1}^l \gamma_i=\alpha_j} [q^{\sum_{i=1}^l \gamma_i}]\binom{l_1+1}{1}_q \binom{l_2+2}{2}_q \cdots \binom{l_k+k}{k}_q\\
&= [q^{\alpha_j}]\prod_{i=1}^k \binom{l_i+i}{i}_q.
\end{aligned}$$

The last of the above equalities is a product of unimodal polynomials hence the product is also a unimodal polynomial by [24, Lemma 7.4.9].

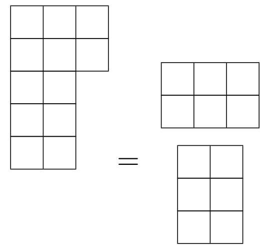
Recall Remark 4.0.72, we may write $\alpha_i+\alpha_j = wk+(v+1)k$, where $wk \geq (v+1)k$ and $\beta_i+\beta_j = (w+1)k+vk$, where $(w+1)k > vk$. By construction, the degree of the product is precisely ν. Since $wk \geq (v+1)k$, both $(v+1)k$ and vk are on the same side of the 'middle' coefficient of the unimodal polynomial. Thus

$$|T^\nu(\alpha_i+\alpha_j)| \geq |T^\nu(\beta_i+\beta_j)|.$$

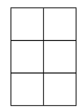
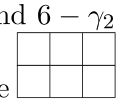
□

Example 4.0.85. Let $n = 6$, $k = 3$, $\alpha = 9+3+3+3$, $\beta = 6+6+3+3$. Thus $\beta_i+\beta_j = 9+3$, and $\alpha_i+\alpha_j = 6+6$. Suppose that $\nu = 3+3+2+2+2$ we show that $\left|T^{3+3+2+2+2}(6+6)\right| \geq \left|T^{3+3+2+2+2}(9+3)\right|$.

Now ν has exactly 2 different summands 3 and 2. Therefore the Tableau of shape $\nu = 3+3+2+2+2$ can be thought of as the justification of 2 rectangular tableaux one of shape $3+3$ and one of shape $2+2+2$.



$$\left|T^{3+3+2+2+2}(6+6)\right| = \prod_{\gamma_1+\gamma_2=6} p(\gamma_1,3,2)p(\gamma_2,2,3).$$

It is known that the number of tableaux of shape  with γ_2 copies of 1 and $6-\gamma_2$ copies of 0 inside is precisely $p(\gamma_2,2,3)$. Additionally, the number of tableau of shape  with γ_1 copies of 1 and $6-\gamma_1$ copies of 0 inside is precisely $p(\gamma_1,3,2)$.

Moreover, $p(\gamma_1,3,2) = [q^{\gamma_1}]\binom{3+2}{2}_q$ and $p(\gamma_2,2,3) = [q^{\gamma_2}]\binom{2+3}{3}_q$.

Now

$$p(\gamma_1,3,2)p(\gamma_2,2,3) = [q^{\gamma_1+\gamma_2}]\binom{3+2}{2}_q\binom{2+3}{3}_q = [q^6]\binom{3+2}{2}_q\binom{2+3}{3}_q.$$

Thus

$$\begin{aligned}\left|T^{3+3+2+2+2}(6+6)\right| &= \prod_{\gamma_1+\gamma_2=6} p(\gamma_1,3,2)p(\gamma_2,2,3)\\ &= [q^6]\binom{3+2}{2}_q\binom{2+3}{3}_q.\end{aligned}$$

$$\begin{aligned}\left|T^{3+3+2+2+2}(9+3)\right| &= \prod_{\gamma_1+\gamma_2=3} p(\gamma_1,3,2)p(\gamma_2,2,3)\\ &= [q^3]\binom{3+2}{2}_q\binom{2+3}{3}_q.\end{aligned}$$

$\binom{3+2}{2}_q\binom{2+3}{3}_q$ is the product of 2 unimodal polynomials in q, and hence is a unimodal polynomial polynomial in q. Moreover, $\deg(\binom{3+2}{2}_q\binom{2+3}{3}_q) = 12$; therefore $[q^3]\binom{3+2}{2}_q\binom{2+3}{3}_q \leq [q^6]\binom{3+2}{2}_q\binom{2+3}{3}_q$ as desired.

Lemma 4.0.86. *If $\nu = k^{w+v+1}$, then $|T^{\nu}(\alpha_i+\alpha_j)| > |T^{\nu}(\beta_i+\beta_j)|$.*

Proof. By the fourth sentence of the previous lemma, the LHS can be identified with the number of ways to distribute α_j copies of P_j into a $w+v+1 \times k$ matrix, and therefore

$$|T^{\nu}(\alpha_i+\alpha_j)| = p(\alpha_j, w+v+1, k)| = p((v+1)k, w+v+1, k) \text{ ,and}$$
$$|T^{\nu}(\beta_i+\beta_j)| = p(\beta_j, w+v+1, k) = p(vk, w+v+1, k).$$

It suffices to show $p(vk+k, w+v+1, k) > p(vk, w+v+1, k)$ which follows directly from the known recurrence for q-binomial coefficients $p(l,n,k) = p(l-k, n-1, k) + p(l, n, k-1)$. □

Theorem 4.0.87. *Suppose that $x_{n,\alpha}$ and $x_{n,\beta}$ have been chosen so that $\alpha, \beta \in P^*(nk)$ and that β covers α namely there is no element strictly between α and β in the dominance order. Then $\eta(x_{n,\alpha}) > \eta(x_{n,\beta})$.*

Proof. Since $\alpha \lhd \beta$, we have $\beta_i+\beta_j = \alpha_i+\alpha_j$ by construction.

By Proposition 4.0.83,

$$\eta(x_{n,\alpha}) = \sum_{\nu \in P(\alpha_i+\alpha_j,n,k)} |T^{\nu}(\alpha_i+\alpha_j)| \left|T^{n^k\setminus\nu}(\alpha-(\alpha_i+\alpha_j))\right| \text{ ,and}$$

$$\eta(x_{n,\beta}) = \sum_{\nu \in P(\beta_i+\beta_j,n,k)} |T^{\nu}(\beta_i+\beta_j)| \left|T^{n^k\setminus\nu}(\beta-(\beta_i+\beta_j))\right|.$$

Now

$$\left|T^{n^k\setminus\nu}(\beta-(\beta_i+\beta_j))\right| = \left|T^{n^k\setminus\nu}(\beta-(\alpha_i+\alpha_j))\right|.$$

Thus it suffices to show

1. For a fixed $\nu \in P(\alpha_i+\alpha_j, n, k)$,

$$|T^{\nu}(\alpha_i+\alpha_j)| \geq |T^{\nu}(\beta_i+\beta_j)|.$$

2. For $\nu = k^{w+v+1}$,

$$|T^{\nu}(\alpha_i + \alpha_j)| > |T^{\nu}(\beta_i + \beta_j)| .$$

These two statements are precisely the previous 2 lemmas. □

Theorem 4.0.88. *Suppose that R is a Krull domain such that $Cl(R)$ has an element of finite order with infinitely many height-one prime ideals in that divisor class. Then R is a UFD if and only if $\overline{\Lambda}(R) = 0$. If R is not a UFD, then $\overline{\Lambda}(R) = \infty$.*

Proof. Suppose that R is not a UFD. By Remark 4.0.52 we may assume that some nonzero divisor class g with finite order $k \geq 2$ contains infinitely many height-one prime ideals of R. By Theorem 4.0.87 , there is a injective order reversing correspondence between elements in a strict chain in $P^*(nk)$ ordered by domination and the number of number of nonassociate irreducible factorizations of length n. Now $p^*(nk) = p(n)$ in the obvious way.

Explicitly, $\Lambda(R, n) \geq$ the length of a maximal chain in $P(n)$ ordered by domination. The length of a maximal chain ordered by domination in $P(n)$ is known to be asymptotically equal to $\frac{(2n)^{\frac{3}{2}}}{3}$ [19], [28].

Thus for large n, $\Lambda(R, n) \geq \frac{(2n)^{\frac{3}{2}}}{3}$.

$$\overline{\Lambda}(R) = \lim_{n\to\infty} \frac{\Lambda(R, n)}{n} \geq \lim_{n\to\infty} \frac{(2n)^{\frac{3}{2}}}{3n} = \infty.$$

□

Corollary 4.0.89. *Let R be a Krull Domain with finite divisor class group. Then $\overline{\Lambda}(R) = 0$ if and only if R is a UFD. If R is not a UFD, then $\overline{\Lambda}(R) = \infty$.*

Proof. A Krull domain with finite divisor class group that is not a UFD is guaranteed to have an element of finite order $k \geq 2$ with infinitely many height-one prime ideals in that divisor class. □

Chapter 5

Summary and Future Directions

This dissertation has directly extended the following previously known results using proof techniques from the fields of commutative algebra (Chapter 1), number theory (Chapter 2), and combinatorics (Chapter 3).

Previously known information.

1. [8, Theorem 18.2.3] Let $R = K + XF[[X]]$ and let $K \subset F$ be a proper extension of fields. Then R is an HFD, but not a UFD. If F is finite, then $\overline{\Lambda}(R) = 0$. If F is infinite, then $\overline{\Lambda}(R) = \infty$.

2. [26, Conjecture 4.8] Let $R = K + XF[X]$, where $K \subset F$ be a proper extension of finite fields such that $|F^*/K^*| = t$. Then $\overline{\Lambda}(R) = \frac{\sigma(t)}{t}$, where $\sigma(t)$ denotes the sum of the positive divisors of t.

3. [8, Theorem 18.2.7] Let R be a Krull domain with $Cl(R)$ finite. Then $\overline{\Lambda}(R) = 0$ if and only if R is a UFD.

New Results.

1. Theorem 2.0.12 Let R be a CK domain. Then $\overline{\Lambda}(R) = 0$.

2. Theorem 3.0.50 Let $R = K + XF[X]$ where $K \subset F$ is a proper extension of fields of finite fields such that $t = \left|\frac{F^*}{K^*}\right|$. Then $\overline{\Lambda}(R) = \frac{\sigma(t)}{t}$.

3. Theorem 4.0.88 Suppose that R is a Krull domain such that $Cl(R)$ has an element of finite order with infinitely many height-one prime ideals in that divisor class. R is a UFD if and only if $\overline{\Lambda}(R) = 0$. If R is not a UFD, then $\overline{\Lambda}(R) = \infty$.

The open questions remaining can be grouped into 2 categories depending on the scope of the question.

1. [8] Determine conditions on R so that $\overline{\Lambda}(R)$ exists.

2. [8] How does the theory change if we use $L_R(x) = \max\{l \mid x = s_1 s_2 \dots s_l \text{ for each } s_i \in A(R)\}$?

3. How does the theory change for $\overline{\Lambda}(M)$ for a finite factorization monoid M instead of a finite factorization domain? In particular, does the corresponding Theorem 4.0.88 hold in the monoid case?

4. For every $q \in \mathbb{Q}$ with $q \geq 1$, does there exist an atomic domain R satisfying $\overline{\Lambda}(R) = q$?

5. Can the finite condition of Theorem 4.0.88 be relaxed?

Bibliography

[1] D. D. Anderson and D. F. Anderson. Elasticity of factorizations in integral domains. *J. Pure Appl. Algebra*, 80(3):217–235, 1992.

[2] D. D. Anderson and D. F. Anderson. Elasticity of factorizations in integral domains. II. *Houston J. Math.*, 20(1):1–15, 1994.

[3] D. D. Anderson, D. F. Anderson, S. T. Chapman, and W. W. Smith. Rational elasticity of factorizations in Krull domains. *Proc. Amer. Math. Soc.*, 117(1):37–43, 1993.

[4] D. D. Anderson, D. F. Anderson, and M. Zafrullah. Factorization in integral domains. *J. Pure Appl. Algebra*, 69(1):1–19, 1990.

[5] D. D. Anderson, D. F. Anderson, and M. Zafrullah. Rings between $D[X]$ and $K[X]$. *Houston J. Math.*, 17(1):109–129, 1991.

[6] D. D. Anderson and J. L. Mott. Cohen-Kaplansky domains: integral domains with a finite number of irreducible elements. *J. Algebra*, 148(1):17–41, 1992.

[7] D. D. Anderson and B. Mullins. Finite factorization domains. *Proc. Amer. Math. Soc.*, 124(2):389–396, 1996.

[8] D. F. Anderson and E. V. Mclaughlin. How far is an HFD from a UFD? In *Abelian groups, rings, modules, and homological algebra*, volume 249 of *Lect. Notes Pure Appl. Math.*, pages 15–22. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[9] G. E. Andrews. *The theory of partitions*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1998. Reprint of the 1976 original.

[10] A. Badra and M. Picavet-L'Hermitte. Some Diophantine equations associated to seminormal Cohen-Kaplansky domains. *Int. J. Math. Game Theory Algebra*, 15(2):139–153, 2006.

[11] L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.*, 11:391–392, 1960.

[12] S. T. Chapman, J. Herr, and N. Rooney. A factorization formula for class number two. *J. Number Theory*, 79(1):58–66, 1999.

[13] S. T. Chapman and W. W. Smith. An inequality concerning the elasticity of Krull monoids with divisor class group $\mathbb{Z}_p$. *Ric. Mat.*, 56(1):107–117, 2007.

[14] I. S. Cohen and I. Kaplansky. Rings with a finite number of primes. I. *Trans. Amer. Math. Soc.*, 60:468–477, 1946.

[15] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[16] R. M. Fossum. *The divisor class group of a Krull domain*. Springer-Verlag, New York, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 74.

[17] A. Geroldinger and F. Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.

[18] R. Gilmer. *Multiplicative ideal theory*. Marcel Dekker Inc., New York, 1972. Pure and Applied Mathematics, No. 12.

[19] C. Greene and D. J. Kleitman. Longest chains in the lattice of integer partitions ordered by majorization. *European J. Combin.*, 7(1):1–10, 1986.

[20] F. Halter-Koch. Finiteness theorems for factorizations. *Semigroup Forum*, 44(1):112–117, 1992.

[21] F. Halter-Koch. On the asymptotic behaviour of the number of distinct factorizations into irreducibles. *Ark. Mat.*, 31(2):297–305, 1993.

[22] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[23] I. Kaplansky. *Commutative rings*. The University of Chicago Press, Chicago, Ill.-London, revised edition, 1974.

[24] A. Kerber. *Applied finite group actions*, volume 19 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, second edition, 1999.

[25] W. J. Martin and B. E. Sagan. A new notion of transitivity for groups and sets of permutations. *J. London Math. Soc. (2)*, 73(1):1–13, 2006.

[26] E. McLaughlin. *Numbers of Factorizations in Non-Unique Factorial Domains*. Allegheny College, Meadville, PA, 2004. Senior Comprehensive Project.

[27] M. Nagata. *Local rings*. Robert E. Krieger Publishing Co., Huntington, N.Y., 1975. Corrected reprint.

[28] R. P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

[29] R. J. Valenza. Elasticity of factorization in number fields. *J. Number Theory*, 36(2):212–218, 1990.

[30] H. S. Wilf. *generatingfunctionology*. A K Peters Ltd., Wellesley, MA, third edition, 2006.

[31] A. Zaks. Half-factorial-domains. *Israel J. Math.*, 37(4):281–302, 1980.

Appendices

Appendix A

The First Appendix

The following is a list of 9 grids that contain information useful inside Chapter 2. Recall that the setup is that $t = 36$ and we characterize below the behavior of the reduction factor for each of the divisors of 36.

for $i = 1$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	1	1	1	1	1	1	1	1	1
resulting root of unity	$\frac{t}{df_d}$	36	18	12	9	6	4	3	2	1

for $i = 2$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	2	2	2	1	2	2	1	2	1
resulting root of unity	$\frac{t}{df_d}$	18	9	6	9	3	2	3	1	1

for $i = 3$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	3	3	3	3	3	1	3	1	1
resulting root of unity	$\frac{t}{df_d}$	12	6	4	3	2	4	1	2	1

for $i = 4$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	4	2	4	1	2	4	1	2	1
resulting root of unity	$\frac{t}{df_d}$	9	9	3	9	3	1	3	1	1

for $i = 6$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	6	6	6	3	6	2	3	2	1
resulting root of unity	$\frac{t}{df_d}$	6	3	2	3	1	2	1	1	1

for $i = 9$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	9	9	3	9	3	1	3	1	1
resulting root of unity	$\frac{t}{df_d}$	4	2	4	1	2	4	1	2	1

for $i = 12$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	12	6	12	3	6	4	3	2	1
resulting root of unity	$\frac{t}{df_d}$	3	3	1	3	1	1	1	1	1

for $i = 18$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	18	18	6	9	6	2	3	2	1
resulting root of unity	$\frac{t}{df_d}$	2	1	2	1	1	2	1	1	1

for $i = 36$

term in sum	d	1	2	3	4	6	9	12	18	36
root of unity	$\frac{t}{d}$	36	18	12	9	6	4	3	2	1
reduction factor	f_d	36	18	12	9	6	4	3	2	1
resulting root of unity	$\frac{t}{df_d}$	1	1	1	1	1	1	1	1	1

There is a particularly unenlightening proof that is required in the chapter concerning the D+M construction.

Lemma A.0.90. *Let* $B := \max\left(B_{\frac{t}{p_1}}, \overline{B_{\frac{t}{p_2}}}\right)$. *Then* $B < \prod_{f=2}^{t-2}\left(\frac{n+f}{f}\right)$.

Proof. Consider the binomial expressions of the relevant terms. $\prod_{f=2}^{t-2}\left(\frac{n+f}{f}\right) = \frac{1}{n+1}\binom{t-2+n}{n}$.

$$\overline{B_{\frac{t}{p_2}}} = \binom{\frac{t}{p_2} - 1 + \frac{n+1}{p_2}}{\frac{n+1}{p_2}}.$$

Case 1. If $B = B_{\frac{t}{p_1}}$, the product that defines B is directly contained in $\prod_{f=2}^{t-2}\left(\frac{n+f}{f}\right)$ in a straightforward modification of the proof of Lemma 3.0.32.

Case 2. $B = \overline{B_{\frac{t}{p_2}}}$. The plan is to reduce the binomial coefficient $\frac{1}{n+1}\binom{t-2+n}{n}$ to $\binom{\frac{t}{p_2}-1+\frac{n+1}{p_2}}{\frac{n+1}{p_2}}$ using well established recurrence relations defined on binomial coefficients. Let $l_1 = n - \frac{n+1}{p_2}$, and $l_2 = t-2+n-(\frac{n+1}{p_2}+\frac{t}{p_2}-1)$.

$$\begin{aligned}
\binom{t-2+n}{n} &= \prod_{f=1}^{l_1}\left(\frac{t-2+f}{n-(f-1)}\right)\binom{t-2+n}{\frac{n+1}{p_2}} \\
&= \prod_{f=1}^{l_1}\left(\frac{t-2+f}{n-(f-1)}\right)\prod_{g=1}^{l_2}\left(\frac{t-2+n-(g-1)}{t-2+n-\frac{n+1}{p}-(g-1)}\right)\binom{\frac{t}{p_2}+\frac{n+1}{p_2}-1}{\frac{n+1}{p_2}} \\
&= \prod_{f=1}^{l_1}\left(\frac{t-2+f}{n-(f-1)}\right)\prod_{g=1}^{l_2}\left(\frac{t-2+n-(g-1)}{t-2+n-\frac{n+1}{p_2}-(g-1)}\right)B.
\end{aligned}$$

For this case it remains to show that

$$\prod_{f=1}^{l_1}\left(\frac{t-2+f}{n-(f-1)}\right)\prod_{g=1}^{l_2}\left(\frac{t-2+n-(g-1)}{t-2+l_1-(g-1)}\right) > n+1.$$

Please note that the last term in the left product has the same numerator as the denominator of the right product. We can reorganize the two products in the following way.

$$\begin{aligned}
&\prod_{f=1}^{l_1}\left(\frac{t-2+f}{n-(f-1)}\right)\prod_{g=1}^{l_2}\left(\frac{t-2+n-(g-1)}{t-2+l_1-(g-1)}\right) \\
&= \prod_{f=1}^{l_1}\left(\frac{1}{n-(f-1)}\right)\prod_{g=1}^{l_2}(t-2+n-(g-1))\prod_{h=1}^{l_2-l_1}\frac{1}{t-2-(h-1)} \\
&= \prod_{h=1}^{l_2-l_1}\left(\frac{t-2+n-(h-1)}{t-2-(h-1)}\right)\prod_{f=1}^{l_1}\left(\frac{n+\frac{t}{p}-1}{n-(f-1)}\right) \\
&> (l_2-l_1)\left(1+\frac{n}{t-2}\right)l_1\left(1+\frac{\frac{t}{p}-1}{n}\right) \\
&= \left[n+\frac{t}{p}-1+\frac{n+1}{p_2}+\frac{(n+1)(\frac{t}{p}-1)}{np_2}\right]\left[n-\frac{nt}{(t-2)p_2}+\frac{n}{t-2}+t-2-\frac{t}{p-2}+1\right] > n+1.
\end{aligned}$$

□

Lemma A.0.91. $p\left(1+\frac{t}{p}\right) > \left(\tau\left(\frac{t}{p}\right)-1\right)[p+1]$.

If $\frac{t}{d} \leq 16$, then simple case by case exhaustion will verify the result.

Proof. For all primes p $\left(\tau\left(\frac{t}{p}\right)-1\right)\left[\frac{3}{2}\right] \geq \left(\tau\left(\frac{t}{p}\right)-1\right)\left[1+\frac{1}{p}\right]$

Thus,

$\frac{t}{d}$	$\left(1+\frac{t}{p}\right)$	$\left(\tau\left(\frac{t}{p}\right)-1\right)\left[\frac{3}{2}\right]$
16	17	6
15	16	$\frac{9}{2}$
14	15	$\frac{9}{2}$
13	14	$\frac{3}{2}$
12	13	$\frac{15}{2}$
11	12	$\frac{3}{2}$
10	11	$\frac{9}{2}$
9	10	3
8	9	$\frac{9}{2}$
7	8	$\frac{3}{2}$
6	7	$\frac{9}{2}$
5	6	$\frac{3}{2}$
4	5	3
3	4	$\frac{3}{2}$
2	3	$\frac{3}{2}$
1	2	0

□

Here are some results concerning the totient function and the divisor function.

Lemma A.0.92. *Suppose that* $t = p^n$, *then* $\sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d) = \sigma(t)$.

Proof. $\sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d)$

$$= \sum_{i=1}^{n+1} i\phi\left(p^{n+1-i}\right)$$

$$= (1)\phi(p^n) + (2)\phi(p^{n-1}) + \cdots + (n-1)\phi(p^2) + n\phi(p) + (n+1)(1)$$

$$= 1(p^n - p^{n-1}) + 2(p^{n-1} - p^{n-2}) + \dots (n-1)(p^2 - p) + n(p-1) + (n+1)(1)$$

$$= p^n + p^{n-1} + \cdots + p^2 + p + 1 = \frac{p^{n+1}-1}{p-1} = \sigma(p^n).$$

□

Lemma A.0.93. *Suppose that* $t = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, $\sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d) = \sigma(t)$.

Proof.

$$\sum_{d|t} \phi\left(\frac{t}{d}\right)\tau(d) = \sum_{d_i|p_i^{n_i}} \phi\left(\frac{p_1^{n_1}}{d_1}\right)\tau(d_1)\phi\left(\frac{p_2^{n_2}}{d_2}\right)\tau(d_2)\dots\phi\left(\frac{p_s^{n_s}}{d_s}\right)\tau(d_s)$$

$$= \left(\sum_{d_1|p_1^{n_1}} \phi\left(\frac{p_1^{n_1}}{d_1}\right)\tau(d_1)\right)\left(\sum_{d_2|p_2^{n_2}} \phi\left(\frac{p_1^{n_2}}{d_2}\right)\tau(d_2)\right)\dots\left(\sum_{d_s|p_s^{n_s}} \phi\left(\frac{p_1^{n_1}}{d_1}\right)\tau(d_s)\right)$$

$$= \sigma(p_1^{n_1})\sigma(p_2^{n_2})\dots\sigma(p_s^{n_s}) = \sigma(p_1^{n_1}p_2^{n_2}\dots p_s^{n_s}) = \sigma(t).$$

□

Vita

Jason A. Laska was born in 1981. He graduated from Farragut High School in 1999. He has B.S. degree in Mathematics and a B.A. degree in German from the University of Tennessee. He finished his PhD in Mathematics under the direction of David F. Anderson in August 2010.