Factorization Properties of Integer-Valued Polynomials

Gabrielle Scullard;
Based on joint work with Paul Baginski, Greg Knapp, Jad Salem

May 10, 2018

Abstract

This paper summarizes results of the REU project "Factorization Properties of Integer-Valued Polynomials" completed at Fairfield University in summer 2016, under the advisment of Professor Paul Baginski, and in a group with Greg Knapp and Jad Salem. We studied nonunique factorization in the ring of integer-valued polynomials by examining the elasticity and the catenary degree of polynomials. We were able to bound catenary degree and elasticity of a polynomial in terms of its polynomial degree. Furthermore, given a valid polynomial degree and a valid catenary degree or elasticity, we were able to construct a polynomial which satisfied the desired criteria.

1 Background

We define the ring of integer-valued polynomials, $\text{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$. This is the set of polynomials with rational coefficients which maps the set of integers into itself, and is easily verified to be a ring. This paper is primarily concerned with certain combinatorial measures of nonunique factorization in $\text{Int}(\mathbb{Z})$. Although the precise questions that we examine have not been extensively studied, this ring and its interesting algebraic and analytic properties are well-known. We give a historical background, provide proof of basic factorization properties of $\text{Int}(\mathbb{Z})$, and give definitions of catenary degree and elasticity.

1.1 Historical Background

This section is based very heavily on the historical and mathematical introduction of *Integer-Valued Polynomials* by Paul-Jean Cahen and Jean-Luc Chabert. As indicated above, we are primarily interested in factorization properties of $\text{Int}(\mathbb{Z})$, but the history of the study of $\text{Int}(\mathbb{Z})$ outside of the scope of factorization is interesting.

The polynomials $\binom{x}{n} = \frac{(x)(x-1)\cdots(x-(n-2))(x-(n-1))}{n!}$, which we call binomial polynomials, are special integer-valued polynomials which appear first in the seventeenth century and were primarily interesting to mathematicians for their use in interpolation formulas, to approximate values of functions [1, page xiv]

Although the binomial polynomials are only some elements of $\text{Int}(\mathbb{Z})$, they form a basis for $\text{Int}(\mathbb{Z})$ as a $\mathbb{Z}$-module. Cahen and Chabert provide a quick proof, which we will reproduce here:

Proof [1, Proposition I.1.1]: First, note that any $\mathbb{Z}$-linear combination of the binomial polynomials is clearly integer-valued as each of the polynomials is integer-valued. Conversely, note that the binomial polynomials form a basis for $\mathbb{Q}[x]$ as a vector space over $\mathbb{Q}$, and write $f \in \text{Int}(\mathbb{Z})$ as $f = \sum_{k=1}^{n} \alpha_k \binom{x}{k}$ for $\alpha_k \in \mathbb{Q}$. Then $\alpha_0 = f(0) \in \mathbb{Z}$ because f is integer-valued. Proceeding inductively, if $\alpha_i \in \mathbb{Z}$ for all $i \leq k$ then $f - \sum_{i=1}^{k} \alpha_i \binom{x}{i} = \sum_{i=k+1}^{n} \alpha_i \binom{x}{i}$ is integer-valued. Plug in $x = k+1$ to find that α_{k+1} must be an integer. □

It was not until the twentieth century that mathematicians became interested in the ring of integer-valued polynomials apart from the binomial polynomials. The term "integer-valued polynomial" first appeared in a 1915 paper by Georg Polya, which focused mostly on entire functions which are integer-valued when restricted to $\mathbb{Z}$ or to $\mathbb{N}$. One example of a property that Polya proved is that if g is entire and satisfies that $|g(z)| \leq Ce^{k|z|}$ for constants k and C, for all $z \in \mathbb{C}$, then g is a polynomial which is integer-valued on $\mathbb{N}$ if $k < \log(2)$ and on $\mathbb{Z}$ if $k < \log(\frac{3+5}{\sqrt{2}}$. [1, page 5]

In 1919, Polya and Alexander Ostrowski independently published papers called *On integer-valued polynomials in algebraic number fields.* They considered a more generalized version of Int($\mathbb{Z}$): For a given number field K and its ring of integers $\mathcal{O}_K$, they considered the set of polynomials in $K[x]$ mapping $\mathcal{O}_K$ into itself. Polya was particularly interested in finding a "regular basis" for this set as a $\mathcal{O}_K$-module (that is, they wanted to find a set of polynomials $\{f_k\}$ such that $\deg(f_k) = k$ and each polynomial could be written as an $\mathcal{O}_K$-linear combination of $\{f_k\}$, in the same way that the binomial polynomials are for Int($\mathbb{Z}$)). He showed that there exists a regular basis if and only if the products of prime ideals in $\mathcal{O}_K$ over any given norm are principal ideals. [1, page xv]

Other generalizations have also been studied. For D an integral domain, K its quotient field, and S a subset of D, define $\text{Int}(S, D) = \{f \in K[x] \mid f(S) \subseteq D\}$. In this notation, Int($\mathbb{Z}$) is Int($\mathbb{Z}, \mathbb{Z}$). The propositions in Section 1.3, proven by Chapman and McClain, apply to this general case when S is infinite and D is a unique factorization domain. In the search for a regular basis in this case, Cahen and Chabert introduce the notion of a Polya-Ostrowski group, which is a subgroup of the class group of a Dedekind domain D, which they describe as the obstacle keeping Int(D) from having a regular basis. [1, Definition II.3.8]

As a final note which may be of interest, Int($\mathbb{Z}$) is not a Noetherian ring. This is a reproduction of the proof given by Cahen and Chabert [2, Proposition 3]. Let $I = \{f \in \text{Int}(\mathbb{Z}) \mid f(0) \equiv 0 \bmod 2\}$. (This is clearly an ideal.) Suppose I is generated by $f_1, f_2, \ldots, f_n$. Then $\{f_i\}$ have a common denominator, $2^k m$ where m is odd, meaning $f_i = \frac{g_i}{2^k m}$ where $g_i \in \mathbb{Z}[x]$ (but is not necessarily primitive). $f_i(0) \equiv 0 \bmod 2^{k+1}$ for every i by definition of I. f_i have integer coefficients, so $f_i(2^{k+1})$ must also be divisible by 2^{k+1}. (If this is not clear, a proof is presented in Section 2.5, as Lemma 2.) Then every element g of I must have $g(2^{k+1})$ divisible by 2^{k+1}, but this is a contradiction because $\binom{x}{2^{k+1}}$ is an element of I as $\binom{0}{2^{k+1}} = 0$; however, $\binom{2^{k+1}}{2^{k+1}} = 1$.

That Int($\mathbb{Z}$) is not Noetherian is generally interesting because if D is a commutative Noetherian domains, then D is a factorization domain. Int($\mathbb{Z}$) is an example that shows the converse does not hold. (It is also interesting because it is a "naturally" occurring example of a non-Noetherian ring.)

1.2 Factorization Definitions

We start with some basic definitions. Let A be an integral domain. We say that a non-unit element $x \in A$ is irreducible in A if whenever $x = yz$ (for $y, z \in A$) one of y or z is a unit. We call two elements $x, y \in A$ associates if there is a unit $u \in A$ such that $x = uy$. We say that A is atomic or a factorization domain if every element in A can be written as a product of irreducible elements.

A factorization of an element $s \in A$ is the expression $s = p_1 p_2 \cdots p_n$ where p_i are irreducibles. If z is the factorization $p_1 p_2 \cdots p_n$ and z' is the factorization $q_1 q_2 \cdots q_m$, then we say z and z' are "essentially the same" if $n = m$ and we can reorder p_j in such a way that q_j and p_j are associates for each j. We say that A has unique factorization if for all $s \in A$ every factorization of s is essentially the same, and in this case A is a unique factorization domain.

In the case that factorization is not unique, we call y a factor or divisor of x if y is irreducible and appears in any factorization of x.

There are many ways to quantify "nonuniqueness" of factorization in an integral domain. The results in this paper focus on two measures of nonunique factorization: elasticity and catenary degree.

Let $z = p_1 p_2 \cdots p_n$ be a factorization. Then the length of z, denoted $|z|$, is n. The length set of x, $\mathscr{L}(x)$, is the set $\{|z| \mid z \text{ is a factorization of } x \text{ in } A\}$. If this set is finite for every $x \in A$, then A is called a "bounded factorization domain." (We prove that Int($\mathbb{Z}$) is bounded factorization domain in Section 1.3) For x an element of a bounded factorization domain A, define $\ell(x) = \min(\mathscr{L}(x))$ and $L(x) = \max(\mathscr{L}(x))$. Then the elasticity $\rho(x) = \frac{L(x)}{\ell(x)}$. We also define the elasticity of A to be $\rho(A) = \sup\{\rho(x) \mid x \in A\}$.

Remark: In 1960, Leonard Carlitz proved that the class number of an algebraic number field is at most 2 if and only if the elasticity is 1. [2]

Remark: It useful to note here that much is known about the elasticity of Int($\mathbb{Z}$). Cahen and Chabert prove that the binomial polynomials $\binom{x}{n}$ are irreducible for all $n > 0$, and using this fact, show that the polynomial

$$f_n = n\binom{x}{n} = (x - n + 1)\binom{x}{n-1}$$

can be chosen to have arbitrarily large elasticity. The expression on the right side is a factorization into two irreducibles, as binomial polynomials and linear polynomials are irreducible in Int($\mathbb{Z}$).

On the left side, we can choose n to have as many prime divisors as we desire, say N. Then $\rho(f_n) \geq \frac{N+1}{2}$. Thus, $\rho(\text{Int}(\mathbb{Z}))$ is infinite. [1, Theorem VI.3.6]

Chapman and McClain show in fact that $\text{Int}(\mathbb{Z})$ has full elasticity, that is, every rational number $\frac{m}{n} > 1$ can be attained as the elasticity of some polynomial in $\text{Int}(\mathbb{Z})$. [3, Theorem 4.5]

Because elasticity only gives information about how the most extreme factorizations compare to each other, it is useful to consider the catenary degree, which gives information about how all the factorizations differ from each other. To do so, we must define a distance between factorizations of an element.

Let $z_1 = a_1a_2 \cdots a_rp_1p_2 \cdots p_n$ and $z_2 = a_1a_2 \cdots a_rq_1q_2 \cdots q_m$ be factorizations of x such that a_i are irreducible elements appearing in z_1 and in z_2, and $p_i \neq q_j$ for any i, j. A is an integral domain, so we can cancel each of the a_i to get factorizations $z_1' = p_1p_2 \cdots p_n$ and $z_2' = q_1q_2 \cdots q_m$ which have no terms in common and are both factorizations of the same $x' \in A$. We define the distance $d(z_1, z_2)$ to be $\max(n, m)$.

We say that a sequence of factorizations (of a particular, fixed element) $z_1, z_2, \ldots, z_n$ is a w-chain for an integer $w > 0$ if $d(z_i, z_{i+1}) \leq w$ whenever $1 \leq i \leq n-1$. The catenary degree of an element x, denoted $\text{cat}(x)$, is the least integer w such that for any two factorizations z, z' of x, there exists a w-chain $z_0 = z, z_1, z_2, \ldots, z_n = z'$. As with elasticity, we define the catenary degree of a factorization domain A to be $\text{cat}(A) = \sup\{\text{cat}(x) \mid x \in A\}$.

We have two other definitions which become useful in computing distances and catenary degrees. Let n be an integer. Then $\Omega(n)$ is the number of prime divisors with multiplicity dividing n. For p prime, $v_p(n)$ is the highest power of p dividing n. (Note that this is the p-adic valuation and hence has interesting algebraic properties, but we use it in a strictly combinatorial/number theoretic sense.)

1.3 Factorization Properties

Chapman and McClain prove some basic lemmas about factorization in $\text{Int}(S, D)$, for D a unique factorization domain and S an infinite subset of D. (Recall that this is $\{f \in K[x] \mid f(S) \subseteq D\}$ for K the quotient field of D, and that $\text{Int}(\mathbb{Z})$ is the case that $S = D = \mathbb{Z}$). We present the ones that we found the most useful here.

Definition: First, we define the fixed divisor of $f \in\text{Int}(S, D)$, $d(S, f) = \gcd\{f(s) \mid s \in S\}$. When $d(S, f) = 1$ we say that f is image primitive over S. When the context is clear, we can omit S and write the fixed divisor as $d(f)$.

Example: Let $f(x) = x(x-1)$ and $S = \mathbb{Z}$. Then we note that for every integer, x or $x - 1$ is even, so $2 \mid d(f)$. Moreover, $d(f) \mid f(2) = 2$, so $d(f) = 2$.

Proposition 1.3.1 [3, Lemma 2.2] Let $f = f_1f_2 \ldots f_n$ for $f_i \in\text{Int}(S, D)$. Then

1. $d(S, f_1)d(S, f_2) \cdots d(S, f_n) \mid d(S, f)$.

2. If $f_1 = f_2 = \ldots = f_n$ then $d(S, f) = (d(S, f_1))^n$.

Proof: (1) Let $m = d(S, f_1)d(S, f_2) \cdots d(S, f_n)$. By hypothesis, for every $x \in S$, $f(x) = f_1(x)f_2(x) \cdots f_n(x)$. Then $d(S, f_i) \mid f_i(x)$ for each i, so $m \mid f(x)$. Thus $m \mid d(S, f)$.

(2) Let $d = d(S, f) = d(S, f_1^n)$ and let $m = d(S, f_1)$. By (1) $m^n \mid d$. Write $d = rm^n$. Then r is the greatest common divisor of $\{\frac{f(x)}{m^n} \mid x \in S\} = \{\frac{f_1(x)}{m})^n \mid x \in S\}$. r must be an $n-th$ power (as for every prime p dividing $(\frac{f_1(x)}{m})^n$ we have $p \mid (\frac{f_1(x)}{m})$, so $p^n \mid (\frac{f_1(x)}{m})^n)$, say $r = b^n$; and $b \mid \frac{f_1(x)}{m}$ for every $x \in S$. But then $bm \mid f_1(x)$ for every $x \in S$, and by definition of m we have $b = 1$, so $r = 1$ and $d = m^n$. $\square$

Note that $d(S, f_1)d(S, f_2) \cdots d(S, f_n)$ may be a proper divisor of $d(f)$. For example, let $S = \mathbb{Z}$, $f_1(x) = x$, $f_2(x) = x - 1$, and $f(x) = f_1f_2$. We have already shown that $d(f) = 2$, but it is clear that $d(f_1) = d(f_2) = 1$ (as $f_1(1) = f_2(2) = 1$).

Proposition 1.3.2 [3, Lemma 2.4]

1. (1) If f is irreducible in $\text{Int}(S, D)$ then f is image primitive.

2. (2) If f is image primitive over S and $f = f_1f_2 \cdots f_n$ (with $f_i \in\text{Int}(S, D)$), then each $f_i(x)$ is image primitive over S.

Proof: (1) $\frac{f(x)}{d(f)}$ is an element of Int(S, D), so we can write $f(x) = d(f) \cdot \frac{f(x)}{d(f)}$. If f is irreducible, then $d(f)$ must be a unit (which is one of ± 1), so f is image primitive.

(2) Follows from Proposition 1.3.1 (1). □

Proposition 1.3.3 [3, Theorem 2.6] Let f be primitive in $D[x]$. f is irreducible in Int(S, D) if and only if $f(x)$ is irreducible and image primitive in $D[x]$.

Proof: If f is irreducible in Int(S, D) then by Proposition 1.3.2 (1), f is image primitive. If $f(x) = g(x)h(x)$ for $g, h \in D[x]$ then $g, h \in$Int(S, D), so either g is a unit or h is a unit in Int(S, D). The only units in Int(S, D) are units in D, so f is irreducible in Int(S, D).

Conversely, assume f is image primitive and irreducible in $D[x]$. If $f = gh$ for $g, h \in$Int(S, D), then g and h are image primitive by Proposition 1.3.2 (2). Write $g = \frac{g^*}{d(g^*)}$ and $h = \frac{h^*}{d(h^*)}$, so $d(g^*)d(h^*)f = gh$. This is a factorization in $D[x]$ which is a UFD, so g, h are primitive imply that $d(g^*) = d(h^*) = 1$. Then $g, h \in D[x]$, so this is a factorization in $D[x]$. f is irreducible, so one of g or h is a unit in $D[x]$, which is a unit in Int(S, D), so f is irreducible in Int(S, D). □

Proposition 1.3.4 [3, Lemma 2.7] Let $f(x)$ be image primitive in $Int(S, D)$. Then there is a unique primitive polynomial $f^* \in D[x]$ and a unique (up to associates) $n \in D$ such that $f(x) = \frac{f^*(x)}{n}$.

Proof: We can always write $f(x) = \frac{h(x)}{n}$ for some $n \in D$ and $h(x) \in D[x]$. If h is not primitive, write $f(x) = \frac{c(h)h_1(x)}{m}$ where $c(h)$ is the greatest common divisor in D of coefficients of h, and h_1 is image primitive. f is image primitive, so $d(c(h)h_1) = n$. But $d(c(h)h_1) = c(h)d(h_1) = n$ so $f(x) = \frac{c(h)h_1(x)}{c(h)d(h_1)} = \frac{h_1(x)}{d(h_1)}$. Set $f^* = h_1$, which is primitive, and $n = d(h_1) = d(f^*)$. □

Note that the proof tells us that $n = d(f^*)$.

Note also that if $f \in$ Int$(\mathbb{Z})$ then any factorization of f is of the form $p_1 p_2 \cdots p_n \frac{f_1^*}{d(f_1^*)} \cdots \frac{f_m^*}{d(f_m^*)}$ (because nonconstant irreducible factors are image primitive). Multiplying both sides by denominators gives $cf = p_1 \cdots p_n f_1^* \cdots f_m^* \in \mathbb{Z}[x]$. Using the fact that $\mathbb{Z}[x]$ has unique factorization, we find that there are only finitely many possibilities for f_i^*, so there are only finitely many possible irreducible factors of f, which says that there are only finitely many combinations of nonconstant irreducible factors (in such a way that their degrees add to the degree of f) and hence only finitely many factorizations of f.

Proposition 1.3.5 [4, Remark 3(iii)] Let f be primitive in $\mathbb{Z}[x]$ of degree n. Then $d(f) \mid n!$.

Proof: Use that $\frac{f}{d(f)} \in$ Int$(\mathbb{Z})$ is a $\mathbb{Z}$-linear combination of $\binom{x}{k}$ for $k \leq \deg(f)$. Then $n!\frac{f}{d(f)}$ is an element of $\mathbb{Z}[x]$. As f is primitive, $\frac{n!}{d(f)}f$ is an element of $\mathbb{Z}[x]$ if and only if $d(f) \mid n!$. □

2 Results

Our REU produced a few significant results regarding catenary degree and elasticity in Int$(\mathbb{Z})$, which we present below. First, the catenary degree of Int$(\mathbb{Z})$ is unbounded, and in fact for every $n \geq 2$ there exists a polynomial of catenary degree n. When we restrict to polynomials of degree n, the catenary degree and elasticity is bounded in terms of n, and the bounds we produce are sharp. When we restrict f to be a product of n linear polynomials, then the catenary degree upper bound drops drastically. We also show that we can construct polynomials of desired polynomial degree and valid catenary degree, or of desired polynomial degree and valid elasticity.

2.1 Catenary degree of Int(Z) is unbounded.

We give two proofs that cat(Int$(\mathbb{Z})$) $= \infty$. The first relies on a construction of Chapman and McClain and is computational in nature. The proof is a straightforward computation of catenary degree for a certain class of polynomials.

Proposition 2.1.1 [3, Proposition 3.4] Let p be prime. Then there is a sequence of integers $i_1, \ldots, i_t$ such that the polynomial $\frac{(x-i_1)\cdots(x-i_t)}{p}$, which we denote f_p, is irreducible in Int$(S, \mathbb{Z})$.

We do not reproduce the full proof here, but we give a general sketch. Chapman and McClain choose the integers $i_1, i_2, \ldots, i_t$ to form *a complete set of residues of* p *with respect to* S (and to lack such a set of residues of any other prime q). Chapman and McClain define these terms as follows. If m is an integer, the set of residues of m with respect to S is $R_S(m) = \{n \mid 0 \leq n \leq m-1, \exists s \in S \text{ such that } s \equiv n \text{mod} m\}$. A set of integers $\{i_1, i_2, \ldots, i_t\}$ where $t = |R_S(m)|$ forms a complete set of residues of m with respect to S if for every j there is some n in $R_S(m)$ such that $i_j \equiv n \text{mod} m$, and $i_j \equiv i_k \text{mod} m$ only if $j = k$. It is said to lack a set of residues for some m if no subset forms a complete set of residues of m. As we are focused on the case that $S = \mathbb{Z}$, we can assume $t = p$.

So, the integers i_j are chosen to form a complete set of residues of p in S and to lack a set of residues for every prime $q \neq p$. A finite set of integers can only form a complete set of residues for finitely many primes, so we just have to choose i_j in such a way that it lacks a set of residues for finitely many primes. We may do so using the Chinese Remainder Theorem. Then the only prime dividing the fixed divisor of $(x-i_1)\cdots(x-i_t)$ is p (because if $\{i_j\}$ lacks a residue of a prime q, then that residue has a representative s in S, such that $s - i_j$ is not divisible by q for any j). Furthermore, in the case of $\text{Int}(\mathbb{Z})$, the fixed divisor is not divisible by p^2 by Proposition 1.3.5. (Note that Chapman and McClain do not use this argument and instead construct an element $s \in S$ such that $(s-i_1)\cdots(s-i_t)$ is not divisible by p^2.)

Thus, the fixed divisor is exactly p, and since any irreducible factors of smaller degree are would have to be of the form $\frac{\prod_{j\in\mathcal{I}}(x-i_j)}{d}$ where d is the fixed divisor of the polynomial in the numerator by image primitivity of irreducibles, we find that $d = 1$ since there is no prime dividing the fixed divisor of a proper subset of the $\{i_j\}$ by construction, so all potential irreducible factors are irreducible in $\mathbb{Z}[x]$. However, f_p is not in $\mathbb{Z}[x]$, so it cannot factor into elements in $\mathbb{Z}[x]$, hence it must be irreducible.

We give an example to illustrate the construction in $\text{Int}(\mathbb{Z})$.

Example Let $p_n > 2$ be the n-th prime, and let $P = \prod_{k=1}^{n-1}$. Then $\{0, P, P^2, \ldots, P^{p_n-1}\}$ forms a complete set of residues mod p_n (as P is not divisible by p_n, hence is a unit in the ring $\mathbb{Z}/p_n\mathbb{Z}$ so it generates representatives of all nonzero congruence classes of p_n) and for no other prime (as every integer chosen is divisible by every prime smaller than p_n). The proposition tells us that $f_{p_n} = \frac{x(\prod_{i=1}^{p_n-1}(x-(P^i))}{p_n}$ is irreducible in $\text{Int}(\mathbb{Z})$.

We also make use of this lemma.

Proposition 2.1.2 [3, Lemma 4.2] Let f_p as above, and let $h_p(x) = p \cdot f_p = (x-i_1)(x-i_2)\cdots(x-i_t)$. Let s and k be positive integers. Then the only irreducible factors in $\text{Int}(\mathbb{Z})$ of the polynomial $f(x) = f_p^s h_p^k$ are f_p and the linear polynomials $(x - i_j)$.

Proof: Every irreducible factor of f is image primitive, by Proposition 1.3.2. By Proposition 1.3.4, this factor is of the form $\frac{f^*(x)}{d(f^*)}$ where f^* divides $\prod_{j=1}^{p}(x-i_j)^{s+k}$. Also, $d(f^*) \mid d(h_p^{s+k}) = p^{s+k}$ by Proposition 1.3.2. Then for some integers $0 \leq n_j \leq s+k$, we have $f^*(x) = \prod_{j=1}^{p}(x-i_j)^{n_j}$. If any $n_j = 0$ then $p \nmid d(f^*)$, so $d(f^*) = 1$. By irreducibility, f^* must be one of $(x - i_j)$. Otherwise, $n_j \geq 1$ so by construction of $\{i_j\}$ we have $p \mid d(f^*)$, so that $f_p \mid \frac{f^*}{d(f^*)}$. But $\frac{f^*}{d(f^*)}$ is irreducible, so it must be f_p. □

It may be interesting to note that Chapman and McClain use the polynomials f_p and $h_p(x)$ in their proof that $\text{Int}(\mathbb{Z})$ has full elasticity. In particular, they show that for any rational number $\frac{t}{u}$ such that $t > u \geq 2$, in lowest terms, they can choose a prime p such that $s = up - 2t \geq 0$. For this s and $k = t - u \geq 1$, they show that $f(x) = f_p^s h_p^k$ has elasticity $\frac{t}{u}$. [3, Theorem 4.5] We use the same polynomial here to show that catenary degree is unbounded in $\text{Int}(\mathbb{Z})$.

Proposition 2.1.3 Fix a prime p. Let $i_1, i_2, \ldots, i_p$ be as in the previous construction, so that $\{i_j\}$ form a complete set of residues mod p in $\mathbb{Z}$, and let $f_p = \frac{\prod_{j=1}^{p}(x-i_j)}{p}$ and $h_p = p \cdot f_p$. Let $f(x) = f_p^s h_p^k$ for some positive integers s and k. We claim that $\text{cat}(f) = p$.

Proof: The only irreducible nonconstant factors of f are f_p and $(x - i_r)$ for $1 \leq r \leq p$, by Lemma 2.1.2. Note that the only constant irreducible factor is p, as the product of the nonconstant factors in a factorization has a denominator p^r. f has denominator p^s, so p must appear in the factorization exactly $t = s - r$ times.

If p appears j times in the factorization, then f_p appears exactly $s + j$ times, as f_p is the only factor with a nontrivial denominator, p, and f has denominator p^s. If f_p appears exactly $s + j$

times, then each $(x - i_r)$ for $1 \leq r \leq p$ must appear exactly $k - j$ times, by Proposition 1.6.

So, every factorization of f is of the following form, and for every $0 \leq j \leq k$ this is a factorization of f.

$$z_j = p^j f_p^{s+j}(x - i_1)^{k-j}(x - i_2)^{k-j} \cdots (x - i_p)^{k-j}$$

We compute the distance between any two factorizations z_j and z_{j+m}.

$$z_j = p^j f_p^{s+j}(x - i_1)^{k-j}(x - i_2)^{k-j} \cdots (x - i_p)^{k-j}$$

$$z_{j+m} = p^{j+m} f_p^{s+j+m}(x - i_1)^{k-j-m}(x - i_2)^{k-j-m} \cdots (x - i_p)^{k-j-m}$$

The common factors are p^j, f_p^{s+j}, and $(x - i_r)^{k-j-m}$ for each $0 \leq r \leq p$. We cancel by the common factors to get z'_j and z'_{j+m}:

$$z'_j = (x - i_1)^m (x - i_2)^m \ldots (x - i_p)^m$$

$$z'_{j+m} = p^m f_p^m$$

Thus z'_j has length pm and z'_{j+m} has length $2m$. Thus the distance $d(z_j, z_{j+m}) = pm \geq p$, so any sequence of factorizations of f has consecutive distances at least p, so $\text{cat}(f) \geq p$. However, for any two factorizations we can construct a sequence $z_j, z_{j+1}, \ldots, z_{j+m-1}, z_{j+m}$ such that the consecutive distances are exactly p. Thus, $\text{cat}(f) \geq p$.

Therefore the catenary degree of f is p. □

Corollary 2.1.4 $\text{cat}(\text{Int}(\mathbb{Z})) = \infty$, and for every prime p there exists a polynomial $f \in \text{Int}(\mathbb{Z})$ such that $cat(f) = p$.

A stronger result with less computational proof can be shown as a corollary of Frisch's Theorem.

First, we state and prove the following fact, which we will use not only in this section but as a guiding principle in our constructions.

Proposition 2.1.5 If a polynomial f has two distinct factorizations, z and z', and $|z| = 2$, then z and z' share no common factors and $d(z, z') = |z'|$. Furthermore, if these are the only two factorizations, then $\text{cat}(f) = d(z, z') = |z'|$.

Proof: Let $n = |z'|$, and notice that if f is not irreducible then $n \geq 2$. If the factorizations share any common terms, say $z_1 = a \cdot a_1$ and $z_2 = a \cdot b_1 \cdots b_{n-1}$, then by cancelling, we obtain a factorization of a_1 into non-units if $n > 2$, which means a_1 is not irreducible, or that $a_1 = b_1$ if $n = 2$ (implying that z_1 and z_2 are not essentially different factorizations). In both cases, we have a contradiction, so the factorizations share no common terms. Thus the distance between them is n. If these are the only two factorizations, then $\text{cat}(f) = d(z, z') = n$. □

We state and do not prove Frisch's theorem below, except to note that it makes use of a lemma which we will state and use in the construction of polynomials of valid catenary degree and elasticity.

Theorem 2.1.6 (Frisch's Theorem) [4, Theorem 2.4] Given integers m_i such that $1 \leq m_1 \leq m_2 \leq \ldots \leq m_n$, there is a polynomial $f \in \text{Int}(\mathbb{Z})$ such that f has exactly n essentially different factorizations, with lengths $m_1 + 1, m_2 + 1, \ldots, m_n + 1$.

An immediate corollary for those who are interested in catenary degree is what follows:

Corollary 2.1.7 $\text{cat}(\text{Int}(\mathbb{Z})) = \infty$, and for every $n \geq 2$ there exists a polynomial with catenary degree n.

Proof: By Frisch, given any $n \geq 2$, we can construct a polynomial with exactly 2 factorizations, of lengths n and 2. By Corollary, the catenary degree is exactly n. □

2.2 Catenary degree and polynomial degree

In the previous section, we found that every integer can be attained as the catenary degree of some polynomial. However, it is intuitively clear that a polynomial of fixed degree should have a bounded catenary degree.

Our main result is that a polynomial f of degree n has $\text{cat}(f) \leq \Omega(n!) + 1$, where $\Omega(n)$ is defined to be the number of prime divisors, with multiplicity, of an integer n.

Note that the following lemmas and main theorem were proven during the REU, primarily by Greg Knapp.

Lemma 2.2.1 For all $n, m \in \mathbb{N}$, with $n, m \geq 1$, we have $\Omega((n+m)!) > \Omega(n!m!)$.

Proof: Bu definition of Ω, this is equivalent to showing that $n!m!$ is a proper divisor of $(n+m)!$. $(n+m)! = (n+m)(n+m-1)(n+m-2)\cdots(n+1)n!$. Any product of m consecutive integers is divisible by $m!$, and as $n+k > k$ for all $1 \leq k \leq m$, we have that $(n+m)(n+m-1)(n+m-2)\cdots(n+1) > m!$. Thus, $n!m!$ is a proper divisor of $(n+m)!$, so $\Omega((n+m)!) > \Omega(n!m!)$. □

Corollary 2.2.2 For $x_1, x_2, \ldots, x_n \in \mathbb{N}$, with $x_i \geq 1$ and $n \geq 2$, we have $\Omega((\sum_{i=1}^{n} x_i)!) > \Omega(\prod_{i=1}^{n}(x_i!)) + n - 2$.

Proof: The case $n = 2$ is exactly Lemma 2.2.1. We proceed by induction. Assume we have the result for $n = k-1$. Let $x_1, \ldots, x_k$ satisfy the above hypotheses. Let $y = \sum_{i=1}^{k-1} x_i$. Let $\ell = \prod_{j=1}^{x_1}(y+j)$. This is a product of x_1 consecutive integers hence is divisible be $x_1!$, and as $y > 0$ we have that $x_1!$ is a proper divisor of ℓ, so that $\Omega(\ell) > \Omega(x_1!)$. By inductive hypothesis, as y is a sum of $k-1$ integers, we have $\Omega(y!) > \Omega(\prod_{i=2}^{k}(x_i!)) + k - 3$. Then $\Omega((\sum_{i=1}^{n} x_i)!) = \Omega((x_1+y)!) = \Omega(\ell \cdot y!) = \Omega(\ell) + \Omega(y!) > \Omega(x_1!) + \Omega(\prod_{i=2}^{k}(x_i!)) + (k-3) + 1$ (by pigeonhole principle). Thus, $\Omega((\sum_{i=1}^{n} x_i)!) > \Omega(\prod_{i=1}^{k}(x_i!)) + k - 2$. □

Lemma 2.2.3 Let $g \in \mathbb{Z}[x]$ be primitive of degree n, and let $d(g) = \frac{n!}{p_1 p_2 \cdot p_k}$ for (not necessarily distinct) primes $p_1, \ldots, p_k$. Then $L(\frac{g}{d(g)}) \leq k+1$.

Proof: $\frac{g}{d(g)}$ has no constant irreducible factors. Write $\frac{g}{d(g)} = g_1 g_2 g_3 \ldots g_m$ where each g_i is irreducible and nonconstant. By Proposition 1.3.4, we can write each $g_i = \frac{g_i^*}{d(g_i^*}$ where each $g_i^* \in \mathbb{Z}[x]$ and is primitive. Using unique factorization in $\mathbb{Z}[x]$ we find that $g = \prod_{i=1}^{m} g_i^*$ and $d(g) = \prod_{i=1}^{m} d(g_i^*)$.

Set $x_i = deg(g_i^*)$. Then $n = \sum_{i=1}^{m} x_i$, hence $\frac{n!}{p_1 p_2 \ldots p_k} = \frac{(\sum_{i=1}^{m} x_i)!}{p_1 p_2 \ldots p_k} = d(g) = \prod_{i=1}^{m} d(g_i^*)$. By proposition, $d(g_i^*) \mid deg(g_i^*)! = x_i!$, so $\prod_{i=1}^{m} d(g_i^*) \mid \prod_{i=1}^{m}(x_i!)$. So $\frac{(\sum_{i=1}^{m} x_i)!}{p_1 p_2 \ldots p_k} \mid \prod_{i=1}^{m}(x_i!)$. Equivalently, $\Omega(\frac{(\sum_{i=1}^{m} x_i)!}{p_1 p_2 \ldots p_k}) \leq \Omega(\prod_{i=1}^{m}(x_i!))$. Equivalently, $\Omega((\sum_{i=1}^{m} x_i)!) - \Omega(p_1 p_2 \ldots p_k) \leq \Omega(\prod_{i=1}^{m}(x_i!))$. By definition, $\Omega(p_1 \ldots p_k) = k$, so we have $\Omega((\sum_{i=1}^{m} x_i)!) \leq \Omega(\prod_{i=1}^{m}(x_i!)) + k$. By Corollary 3.2, we have that $\Omega(\prod_{i=1}^{m}(x_i!)) + m - 2 < \Omega((\sum_{i=1}^{m} x_i)!) \leq \Omega(\prod_{i=1}^{m}(x_i!)) + k$. Therefore, $m - 2 \leq k - 1$, or equivalently, $m \leq k+1$.

m is exactly the number of irreducible factors of $\frac{g}{d(g)}$, so $m = L(\frac{g}{d(g)}) \leq k+1$, which is what we wanted to show. □

Corollary 2.2.4 Let g satisfy the hypotheses of Lemma 2.2.3, that is, g is primitive in $\mathbb{Z}[x]$. Then $L(\frac{g}{d(g)}) \leq \Omega(n!) - \Omega(d(g)) + 1$.

Proof: In the lemma, we have $n! = d(f) \cdot p_1 p_2 \cdots p_k$, so $\Omega(n!) = \Omega(d(f)) + k$ and thus $L(\frac{g}{d(g)} \leq \Omega(n!) - \Omega(d(g)) + 1$. □

Lemma 2.2.5 Let $n \in \mathbb{N}$, $n \geq 1$. Then $n \leq \Omega(n!)$.

Proof: This is trivial if $n = 1$. We proceed by induction. Assume $n - 1 \leq \Omega((n-1)!)$. Then $\Omega(n!) = \Omega((n-1)!) + \Omega(n)$. By induction hypothesis, this is $\geq n - 1 + \Omega(n)$. But n is not a unit, hence has at least one prime divisor. Thus $\Omega(n) \geq 1$, so $\Omega(n!) \geq n$. □

Lemma 2.2.6 Let $f \in \text{Int}(\mathbb{Z})$ of degree n, and suppose f is prime minimal for some primitive $f^* \in \mathbb{Z}[x]$. Let z be a factorization of f of the form $w(\frac{d(f^*)}{b})w(\frac{f^*}{d(f^*)})$, where $w(g)$ denotes some factorization of g. Then for any other factorization of f, z', we have $d(z, z') \leq \Omega(n!) + 1$.

Proof: Write $z' = p_1 p_2 \cdots p_k \frac{f_1^*}{d(f_1^*)} \frac{f_2^*}{d(f_2^*)} \cdots \frac{f_m^*}{d(f_m^*)}$. This is a factorization of f, so $\frac{p_1 p_2 \cdots p_k}{d(f_1^*) d(f_2^*) \cdots d(f_m^*)} = \frac{1}{b}$. Multiply both sides by $d(f_1^*) d(f_2^*) \cdots d(f_m^*)$ to get $p_1 p_2 \cdots p_k = \frac{d(f_1^*) d(f_2^*) \cdots d(f_m^*)}{b}$. Note that by Proposition $\prod_{i=1}^{m} d(f_i^*) \mid d(f^*)$, so $p_1 p_2 \cdots p_k \mid \frac{d(f^*)}{b}$ and by unique factorization in integers, each p_j must appear in any factorization of $\frac{d(f)^*}{b}$, hence must appear in the factorization z. So, after cancelling common factors, we have $d(z', z) \leq \max(m, \Omega(\frac{d(f^*)}{bp_1p_2\cdots p_k}) + L(\frac{f^*}{d(f^*)}))$.

m is the number of nonconstant irreducible factors appearing in z', hence $m \leq n \leq \Omega(n!) + 1$ by Lemma 2.2.5. By Corollary 2.2.4, $\Omega(\frac{d(f^*)}{bp_1p_2\cdots p_k}) + L(\frac{f^*}{d(f^*)})) \leq \Omega(d(f^*)) + \Omega(n!) - \Omega(d(f^*)) + 1 = \Omega(n!) + 1$. Thus $d(z', z) \leq \Omega(n!) + 1$. □

Theorem 2.2.7: Let $f \in \mathrm{Int}(\mathbb{Z})$ with degree n. Then $\mathrm{cat}(f) \leq \Omega(n!) + 1$

Proof:

Case 1: f is image primitive. Then by Proposition, f has no constant divisors, hence the length of any factorization is at most n, so the distance between any two factorizations is at most n, so the $\mathrm{cat}(f) \leq n \leq \Omega(n!) + 1$.

Case 2: f is not image primitive. Then let z_1 and z_2 be two distinct factorizations of f, say $z_1 = p_1p_2\cdots p_k \cdots \frac{f_1^*}{d(f_1^*)}\frac{f_2^*}{d(f_2^*)}\cdots\frac{f_m^*}{d(f_m^*)}$ and $z_2 = q_1q_2\cdots q_r \cdots \frac{g_1^*}{d(g_1^*)}\frac{g_2^*}{d(g_2^*)}\cdots\frac{g_t^*}{d(g_t^*)}$. Let $c = \gcd(p_1p_2\cdots p_k, q_1q_2\cdots q_t)$ and consider the polynomial $\frac{f}{c}$. This is an element of $\mathrm{Int}(\mathbb{Z})$ with two factorizations which share no common constant divisors. Thus $\frac{f}{c}$ has form $\frac{f^*}{b}$ for some primitive f^* in $\mathbb{Z}[x]$. Let z_1' and z_2' denote the factorizations of $\frac{f}{c}$ gotten by dividing z_1 and z_2 (respectively) by factors of c. By Lemma 3.6, there is a factorization z' of $\frac{d(f^*)}{b}\frac{f^*}{d(f^*)}$, such that $d(z_1', z') \leq \Omega(n!) + 1$ and $d(z', z_2') \leq \Omega(n!) + 1$.

By multiplying z' by the unique factorization of c into primes, we obtain a factorization z of f, whose distance from z_1 is $d(z, z_1) = d(z', z_1')$ and from z_2 is $d(z, z_2) = d(z', z_2')$, as each of the three factorizations z, z_1, z_2 contains a prime factorization of c as common factors. We chose z' such that each of these distances is $\leq \Omega(n!) + 1$, so we have shown that there is an $(\Omega(n!) + 1) - \mathit{chain}$ between any two factorizations of f, which shows that $\mathrm{cat}(f) \leq \Omega(n!) + 1$. □

2.3 Elasticity

We notice that the proof in the previous section relied on results about lengths of factorizations. With a little more work, we find bounds for elasticity as well. These lemmas and results are due primarily to Greg Knapp.

Lemma 2.3.1: Suppose $f \in \mathrm{Int}(\mathbb{Z})$. Write $f = \frac{a \cdot f^*}{b}$ for integers a, b such that $(a, b) = 1$ and $f^* \in \mathbb{Z}[x]$ is primitive. Then the product of constant factors in any factorization of f is divisible by a.

Proof: Let

$$p_1p_2\cdots p_k \frac{f_1^*}{d(f_1^*)} \cdots \frac{f_n^*}{d(f_n^*)}$$

be a factorization of f into irreducible elements, such that f_i^* are primitive. Then $f^* = f_1^* f_2^* f_3^* \cdots f_n^*$ and $\frac{a}{b} = \frac{p_1p_2\cdots p_k}{d(f_1^*)\cdots d(f_n^*)}$. Then $a \cdot d(f_1^*)d(f_2^*)\cdots d(f_n^*) = b \cdot p_1p_2\cdots p_k$. These are all integers, so a divides $b \cdot p_1p_2\cdots p_k$ but by hypothesis, a and b are relatively prime, so $a \mid p_1\cdots p_k$. □

Lemma 2.3.2: Let $f \in \mathrm{Int}(\mathbb{Z})$ and write $f = \frac{af^*}{b}$ for some primitive f^* in $\mathbb{Z}[x]$ and $\gcd(a, b) = 1$, $a, b \in \mathbb{Z}$. Then every factorization of f is of the form $a \cdot z'$ for a factorization z' of $\frac{f^*}{b}$ (and where a is factored). f has unique factoriation if and only if $\frac{f^*}{b}$ has unique factorization.

Proof: By Lemma 2.3.1, the unique factorization of a appears in every factorization of f. Let z be a factorization of f, say $z = p_1\cdots p_k f_1 f_2\cdots f_n$. If we reindex so that $p_1\cdots p_r = a$, then $p_{r+1}\cdots p_k f_1 f_2\cdots f_n$ forms a factorization of $\frac{f^*}{b}$. Also note that for every factorization of $\frac{f^*}{b}$, we can get a factorization of f by multiplying by $p_1\cdots p_r$. That is, there is a one to one correspondence between factorizations of f and of $\frac{f^*}{b}$, so f has unique factorization if and only if $\frac{f^*}{b}$ has unique factorization. □

Lemma 2.3.3 Let $f \in \mathrm{Int}(\mathbb{Z})$. Write $f = \frac{af^*}{b}$ for a primitive $f^* \in \mathbb{Z}[x]$. Then $\mathcal{L}(f) \leq \Omega(n!) + \Omega(a) - \Omega(b) + 1$ and $\ell(f) = \Omega(a) + \ell(\frac{f^*}{b})$.

Proof: Let

$$p_1p_2\cdots p_k \frac{f_1^*}{d(f_1^*)} \cdots \frac{f_n^*}{d(f_n^*)}$$

be a factorization of f into irreducible elements. By Lemma we can reorder $p_i's$ if necessary to get $a = p_1 \cdots p_r$ for $r = \Omega(a)$. Then the product

$$z = p_{r+1}p_{r+2} \dots p_k \frac{f_1^*}{d(f_1^*)} \cdots \frac{f_n^*}{d(f_n^*)}$$

is a factorization of $\frac{f^*}{b}$. As every factorization of f can therefore be written as the product of a (unique) factorization of a and of $\frac{f^*}{d(f^*)}$, we have $\mathcal{L}(f) = \Omega(a)+(L)(\frac{f^*}{d(f^*)}$ and $\ell(f) = \Omega(a)+\ell(\frac{f^*}{d(f^*)})$.

By Lemma 2.2.4 $\mathcal{L}(\frac{f^*}{n}) \leq \Omega(n!) - \Omega(b) + 1$. This is maximized if $b = 1$. The smallest length of any factorization of non-irreducible elements is 2. Together, this gives the result. □

Theorem 2.3.4 Let $f \in \text{Int}(\mathbb{Z})$ be of degree n and with nonunique factorization. Write $f = \frac{a \cdot f^*}{b}$ for a primitive f^* in $\mathbb{Z}[x]$. Then $\rho(f) \leq \frac{\Omega(n!)+\Omega(a)-\Omega(b)+1}{\Omega(a)+\ell(\frac{f^*}{b})} \leq \frac{\Omega(n!)+1}{2}$

Proof This follows from Lemma and because whenever $t \geq 0$ and $u \leq s$, we have $\frac{s+t}{u+t} \leq \frac{s}{u}$. (This inequality holds if and only if $u(s+t) \leq s(u+t)$ which is true if and only if $ut \leq st$ which is true if and only if $u \leq s$.) So $\rho(f) \leq \frac{\Omega(n!)+\Omega(a)-\Omega(b)+1}{\Omega(a)+\ell(\frac{f^*}{b})} \leq \frac{\Omega(n!)-\Omega(b)+1}{\ell(\frac{f^*}{b})}$. The numerator is maximized in the case that $b = 1$ and the denominator is minimized in the case that $\frac{f^*}{b}$ has a factorization of length 2, so $\rho(f) \leq \frac{\Omega(n!)-\Omega(b)+1}{\ell(\frac{f^*}{b})} \leq \frac{\Omega(n!)+1}{2}$. □

Theorem 2.3.5 Given $n \in \mathbb{N}$ which is ≥ 2, and rational number $1 < \frac{r}{s} \leq \frac{\Omega(n!)+1}{2}$ in lowest terms, there exists a polynomial $f \in \text{Int}(\mathbb{Z})$ of elasticity $\frac{r}{s}$ if and only if $r - s \leq \Omega(n!) - 1$.

We will construct the polynomial in the next section, but we will show one direction here: Suppose $f \in \text{Int}(\mathbb{Z})$ of degree n and $\rho(f) = \frac{r}{s}$ in lowest terms. We show that $r - s \leq \Omega(n!) - 1$.

Half Proof: Note that $r = \mathcal{L}(f)t$ and $s = \ell(f)t$ for some $t \in \mathbb{N}$. Then $r - s = t(\mathcal{L}(f) - \ell(f))$. We write $f = \frac{a \cdot f^*}{b}$ for $(a, b) = 1$ and f^* primitive. By Proposition, $\mathcal{L}(f) \leq \Omega(n!) + 1 + \Omega(a)$ and $\ell(f) = \Omega(a) + \ell(\frac{f^*}{b})$, so $r - s \leq t(\Omega(n!) + 1 - \ell(\frac{f^*}{b})) \leq t(\Omega(n!) - 1) \leq \Omega(n!) - 1$. □

2.4 Constructions

The previous two sections show that for a polynomial of degree n, the catenary degree is bounded between 2 and $\Omega(n!)+1$, and the elasticity is between 1 and $\frac{\Omega(n!)+1}{2}$. The purpose of this section is to not only show that these are "good bounds," but that this is a "good range," in the sense that for any integer in the allowed range, we can construct a polynomial of degree n with the desired catenary degree, and we can construct a polynomial of degree n with the desired elasticity.

The general principle for catenary degree constructions is as follows. For an n-degree polynomial which is primitive and an element of $\mathbb{Z}[x]$, its fixed divisor divides $n!$. If f is primitive in $\mathbb{Z}[x]$ and $\frac{f}{d(f)}$ is irreducible, then there is a factorization of length $\Omega(d(f)) + 1$ (given by a factorization of $d(f)$ in integers, multiplied by $\frac{f}{d(f)}$). If f has exactly one other factorization of length 2, then we can conclude that the catenary degree is exactly $\Omega(d(f)) + 1$.

This is a specific application of Proposition 2.1.5. We prove a general version of this result below. Note that this result was proven during the REU by Professor Baginski.

Proposition 2.4.1 (Bagisnki) Let f be primitive in $\mathbb{Z}[x]$, and let $f_1, \dots, f_n$ be irreducible in $\mathbb{Z}[x]$ such that $f = f_1 \cdots f_n$, for $n \geq 2$. If for every proper nonempty subset I of $\{1, \dots, n\}$, we have $d(\prod_{i \in I} f_i) = 1$, and if $d(f) \neq 1$, then f has exactly two factorizations, of lengths $\Omega(d(f)) + 1$ and n. Then $\text{cat}(f) = \max(d(f) + 1, n)$.

Proof: We show that the only nonconstant irreducible factors of f are each f_i and $\frac{f}{d(f)}$. Every nonconstant irreducible factor of f is of the form $\frac{\prod_{i \in I} f_i}{d(\prod_{i \in I} f_i)}$ for some subset I of $\{1, 2, 3, \dots, n\}$, because f_i are irreducible. If I is a proper subset, then the denominator is 1, and $\prod_{i \in I} f_i$ is irreducible in $\text{Int}(\mathbb{Z})$ if and only if I consists of a single element. Otherwise, I is nonproper and this element is $\frac{f}{d(f)}$. $d(f) \neq d(\prod_{i \in J} f_j) = 1$ for any proper subset J, so this element is irreducible in $\text{Int}(\mathbb{Z})$.

Thus any factorization of f either contains the irreducible element $\frac{f}{d(f)}$, in which case the factorization must be $z = p_1 p_2 \cdots p_k \frac{f}{d(f)}$ where $p_1 \cdots p_k = d(f)$, or it contains each f_i, in which case the factorization is exactly $z' = f_1 f_2 \cdots f_n$. These are all cases and hence all factorizations. $|z| = \Omega(d(f)) + 1$ and $|z'| = n$. Then the $\text{cat}(f) = \max(d(f) + 1, n)$. $\square$

We use this lemma particularly in the case that $n = 2$. Our strategy is as follows. We want to determine whether or not, given any c between 2 and $\Omega(n!) + 1$, we can construct a primitive polynomial f of degree n in $\mathbb{Z}[X]$ whose fixed divisor is $c - 1$, with the additional property that $\frac{f}{d(f)}$ is irreducible and has exactly one other factorization of length 2. By Proposition 2.4.1, our catenary degree in this case is exactly $c \geq 2$. Incredibly, the answer is (almost) yes.

When $c = 2$, it is impossible to construct such a polynomial in the described way, as if the fixed divisor of f is $c - 1 = 1$, then $\frac{f}{d(f)}$ is in $\mathbb{Z}[x]$–that is, every factorization of f, if constructed as above, is a factorization in $\mathbb{Z}[x]$ and hence is unique, so catenary degree is not 2.

However, we can still always construct a polynomial of catenary degree 2 and polynomial degree $n \geq 2$ by different means.

Proposition 2.4.2 Given $n \in \mathbb{N}, n \geq 2$ we can construct a polynomial f such that $deg(f) = n$ and $cat(f) = 2$.

Proof: Let $k = n - 1$. Let $f(x) = (X^k + 2)(X + 1)$. This is a polynomial of degree n. Note that $d(f) = 2$ as $2 \mid d(f)$ because $x^k + 2$ is always the same parity as x, and $x + 1$ is always of the opposite parity, and $d(f) \mid f(0) = 2$. Then $\frac{f}{d(f)}$ is irreducible because $x^k + 2$ has fixed divisor 1 (the fixed divisor must divide $0^k + 2 = 2$ and $1^k + 2 = 3$, which are relatively prime) and $x + 1$ has fixed divisor 1 (which is true of all primitive linear polynomials). By Proposition *** $\frac{f}{d(f)}$ must be irreducible.

There is a factorization of f which is the unique factorization of f in $\mathbb{Z}[x]$, say z, and there is a factorization of f which is $d(f)\frac{f}{d(f)}$ (where $d(f)$ is factored in $\mathbb{Z}$). The factorization in $\mathbb{Z}[x]$ is exactly $(x^k + 2)(x + 1)$, as $(x^k + 2)$ is irreducible by Eisenstein, and primitive linear polynomials are irreducible in $\text{Int}(\mathbb{Z})$. $|z| = 2$ and $|z'| = 2$, so the distance $d(z, z') = 2$, and as these are the only factorizations $\text{cat}(f) = 2$. $\square$

Now, we prove the main result of this section. We first show that we can construct polynomials with desired fixed divisor and degree. The following results were proven primarily by Jad Salem during the REU.

Lemma 2.4.3 Let $f(x) = n!\binom{x}{n}$ and let $p_i \mid n!$. We can construct monic polynomials $g_i, h_i \in \mathbb{Z}[x]$ such that $f(x) = g_i(x)h_i(x)$, $p_i \nmid d(g_i), d(h_i)$, and g_i has degree $\lceil \frac{n}{2} \rceil$ and h_i has degree $\lfloor \frac{n}{2} \rfloor$.

Proof: The idea is to partition the linear factors $x(x-1)(x-2)\cdots(x-n+1)$ between g_i and h_i, in such a way that we can guarantee that the fixed divisor is not divisible by the prime we chose. Write $g'_i = \prod_{p_i | i, 0 \leq i \leq n-1}(x - i)$ and $h'_i = \prod_{i \equiv 1 \bmod p_i, 0 \leq i \leq n-1}(x - i)$. The degree of g'_i is exactly $\lceil \frac{n-1}{p_i} \rceil$ and the degree of h'_i is $\lfloor \frac{n-1}{p_i} \rfloor$, so we are done if $p_i = 2$ and we can set $g_i = g'_i$ and $h_i = h'_i$. Otherwise, choose (arbitrarily) $\lceil \frac{n}{2} \rceil - \lceil \frac{n-1}{p_i} \rceil$ distinct factors from $x(x-1)(x-2)\cdots(x-n+1)$, which were not already chosen as divisors of g'_i and h'_i, and call their product g_i”. Let $g_i = g'_i \cdot g_i$”. Let h_i” denote the product of the unused factors, and let $h_i = h'_i \cdot h_i$”. Then if x is divisible by p_i, by construction $p_i \nmid h_i(x)$, and if $x + 1$ is divisible by p_i then $p_i \nmid g_i(x)$. By the way we chose factors, we have that the degree condition is satisfied and that $g_i h_i = f$. $\square$

Example: Let $n = 9$ and let $p_i = 5$. Then $g'_i = x(x - 5)$ and $h'_i = (x - 1)(x - 6)$. Picking from the remaining choices arbitrarily, we can construct $g_i = x(x - 5)(x - 2)(x - 3)(x - 4)$ and $h_i = (x - 1)(x - 6)(x - 7)(x - 8)$.

Before we prove the theorem, we state and do not prove an extremely useful result of Frisch, which she uses in the proof that a polynomial can be constructed with any given multiset of natural numbers greater than 2 as its set of lengths of factorizations.

Lemma 2.4.4 (Frisch's Lemma) [4, Lemma 6] Given finitely many nonconstant monic polynomials $f_i \in \mathbb{Z}[x]$ we can construct monic irreducible polynomials F_i which are pairwise non-associated in $\mathbb{Q}[x]$, with $deg(F_i) = deg(f_i)$, and with the additional property that if J is a subset of the set of indices of f_i, I, then $d(\prod_{i \in J} F_i = d(\prod_{i \in J} f_i)$.

In our strategy of finding two irreducible polynomials in $\mathbb{Z}[x]$ with fixed divisor 1 and whose product has some desired fixed divisor, Frisch's Lemma tells us that it suffices to find monic polynomials in $\mathbb{Z}[x]$ with the correct fixed divisor and degree properties.

Proposition 2.4.5 Let $2 \le c \le \Omega(n!)+1$, and $n \ge 4$. Let $P \mid n!$ such that $\Omega(P) = \Omega(n!)+1-c$. Then there are polynomials $g, h \in \mathbb{Z}[x]$ satisfying the following properties.

1. $\deg(g) = \lceil \frac{n}{2} \rceil$ and $\deg(h) = \lfloor \frac{n}{2} \rfloor$
2. $d(g) = d(h) = 1$
3. $d(gh) = \frac{n!}{P}$
4. g and h are irreducible in $\mathbb{Z}[x]$

Proof: It is clear that we can choose P in such a way as long as $\Omega(n!) + 1 - c \ge 0$. Write $n! = q_1^{e_1} \cdots q_m^{e_m}$ for primes q_i and $e_i > 0$. Then there are nonnegative integers r_i and j_i such that $r_i + j_i = e_i$, $P = \prod_{i=1}^m q_i^{r_i}$ and $\frac{n!}{P} = \prod_{i=1}^m q_i^{j_i}$. Let $I = \{i \mid q_i \nmid \frac{n!}{P}\}$ and $J = \{i \mid q_i \mid \frac{n!}{P}\}$

Define
$$g^*(x) = \frac{n!}{P} + \sum_{q_i \in J} [u_i \frac{n!}{q_i^{j_i} P} g_i(x))]$$

where g_i are the polynomials defined in Lemma corresponding to q_i, and u_i are chosen such that $\sum_{i \in J} u_i \frac{n!}{q_i^{j_i} P} = 1$. (We can do this because for any prime q_i dividing $\frac{n!}{P}$, the term $\frac{n!}{q_i^{j_i} P}$ is not divisible by q_i, so each of these terms are relatively prime integers.) Note that this implies that g^* is monic.

We define h^* similarly but with some added conditions.

First let
$$h'(x) = \sum_{i \in J} u_j \frac{n!}{q_i^{j_i} P} h_i(x)$$

where h_i is as defined in the lemma and u_j are as defined above.

Let ℓ_i be integers defined for every $q_i \in I$, as follows:

- If $q_i = 2$ let $\ell_i = 1$
- Otherwise, if $h'(0) - 1$ is not divisible by q_i, pick ℓ_i such that $\ell_i \cdot \frac{n!}{P} \equiv h'(0) - 1 \mathrm{mod} q_i$.
- Otherwise, choose ℓ_i such that $\ell_i \cdot \frac{n!}{P} \equiv h'(0) - 2 \mathrm{mod} q_i$

We only have finitely many primes to consider. By Chinese Remainder Theorem, there is an integer s such that $s \equiv \ell_i \mathrm{mod} q_i$ for every $q_i \in I$.

Now define
$$h^*(x) = \frac{sn!}{P} + \sum_{i \in J} u_j \frac{n!}{q_i^{j_i} P} h_i(x)$$

We first show that the fixed divisor of each of these polynomials is 1. $g^*(0) = \frac{n!}{P}$ so $d(g^*) \mid \frac{n!}{P}$. By construction, for every prime q_i dividing $\frac{n!}{P}$, at most one of the summands $u_i \frac{n!}{q_i^{j_i}} g_i$ is not divisible by q_i. u_i is not divisible by q_i because if it were, then the sum $\sum_{i \in J} u_i \frac{n!}{q_i^{j_i} P}$ would necessarily be divisible by q_i and also be equal to 1, which is a contradiction. By construction, the fixed divisor of g_i is not divisible by q_i. Hence, $d(g^*)$ is not divisible by q_i for any $q^i \mid g^*(0)$, so $d(g^*) = 1$.

$h^*(0) = \frac{sn!}{P}$. By the same argument, $q_i \nmid d(h^*)$ for any $i \in J$. Thus the only possible divisors are divisors of $d(h^*)$ are divisors of s, which we chose to not be divisible by any q_i for $i \in I$. As these are all the divisors of $n!$ and the fixed divisor of h^* must divide $n!$ (as h^* is monic hence primitive), $d(h^*) = 1$ as well.

We show next that $d(g^* h^*) = \frac{n!}{P}$. Recall that $g_j(0)$ for each j, so $g^*(0) = \frac{n!}{P}$. s was constructed so that for any prime $q_i \ne 2$ either $h^*(0) \equiv 1$ or $h^*(0) \equiv 2$ mod q_i, for each prime q_i which does not divide $\frac{n!}{P}$, giving $d(g^* h^*) \equiv \frac{n!}{P} \mathrm{mod} q_i$, or $\equiv 2\frac{n!}{P}$. In either case, q_i does not divide the fixed divisor for these primes.

If $q_i = 2 \nmid \frac{n!}{P}$, we show that by controlling our choice of h_j, we can ensure $2 \nmid d(h^*)$. For any h_j, let q_j be the divisor of $\frac{n!}{P}$ which does not divide the fixed divisor of h_j. q_j is an odd prime, so if $q_j + 1 \le n - 1$, we have that $(x-1)(x - q_j + 1) \mid h_j$ has fixed divisor divisible by 2. Otherwise, the only fixed choice we made for h_j was that h_j is divisible by $x - 1$ and that the degree be $\lfloor \frac{n}{2} \rfloor \le 2$.

(Note that here we use the assumption that the degree is at least 4.) So, as 2 is not divisible by q_j, we construct h_j such that $(x-1)(x-2)$ divides h_j, and in particular, $2 \mid d(h_j)$. So $h^*(x) \equiv \frac{sn!}{P}$ mod 2 but by construction of s and because $2 \nmid \frac{n!}{P}$, we find that in fact h^* is never divisible by 2. As $g^*(0)$ is not divisible by 2, we get that $d(g^*h^*)$ is not divisible by any prime not dividing $\frac{n!}{P}$.

But by construction, for every prime q_i dividing $\frac{n!}{P}$, $g^*(x) \equiv u_i \frac{n!}{q_i^{j_i}P} g_i(x) \mathrm{mod} q_i$ and $h^*(x) \equiv u_i \frac{n!}{q_i^{j_i}P} h_i(x)$. By construction of the g_i and h_i, this is exactly $u_i^2 (\frac{n!}{q_i^{j_i}P})^2 x(x-1)\cdots(x-n+1)$, which has fixed divisor divisible by $q_i^{j_i}$ as $x(x-1)\cdots(x-n+1)$ has fixed divisor $n!$. We need to show that j_i is the highest power of q_i dividing gh.

Assume j_i is not the highest power of q_i dividing $n!$ (otherwise the statements is trivial because the fixed divisor must divide $n!$).

Evaluate $g^*(0)h^*(0)$. This is $\frac{n!}{P}h^*(0)$ as $g_j(0) = 0$ by construction. $h^(0)$ is not divisible by q_i because every term except for $u_i \frac{n!}{q_i^{j_i}P} h_i(0)$ is divisible by q_i, j_i is the highest power of q_i dividing $d(g^*h^*)$ for every prime $q_i \mid \frac{n!}{P}$.

In summary, we have that (1) $\deg(g^*) = \lceil \frac{n}{2} \rceil$, (2) $d(g^*) = d(h^*) = 1$, and (3) $d(g^*h^*) = \frac{n!}{P}$.

Now we have checked that g^* and h^* satisfy properties 1, 2, 3. g^* and h^* as constructed may not be irreducible. However, by Frisch's Lemma, we may replace g^* and h^*–which are monic elements of $\mathbb{Z}[x]$–with polynomials g and h such that $d(g) = d(g^*) = 1$, $d(h) = d(h^*) = 1$, $d(gh) = d(g^*h^*) = \frac{n!}{P}$, and g and h are irreducible–that is, g and h are polynomials satisfying all four properties and the proposition is proved. □

Note that the above construction does not work when the polynomial degree is 2 or 3. By the proposition and because catenary degree is at most $\Omega(n!)+1$ for any polynomial degree n, the only missing case is a polynomial of degree 3 and catenary degree 3. The following is a construction of a polynomial of degree at least 3, which has catenary degree 3.

Proposition 2.4.6 Given $n \in \mathbb{N}, n \geq 3$ we can construct a polynomial f such that $deg(f) = n$ and $\mathrm{cat}(f) = 3$.

Proof: Let $k = n-2$. Let $f = (X^2+2)(X^k+3)$.

(X^2+2) and (X^k+3) are both irreducible in $\mathbb{Z}[X]$ by Eisenstein Criterion, and both are image primitive because $d((X^2+2)) \mid \gcd(2,3) = 1$ and $d((X^k+3)) \mid \gcd(0^k+3, 1^k+3) = 1$. Thus, these are both irreducible in $Int(\mathbb{Z})$.

Furthermore, when $y \equiv 0(\mathrm{mod} 2)$, we have that $2 \mid (y^2+2)$, and when $y \equiv 1(\mathrm{mod} 2)$, we have that $2 \mid (y^k+3)$; and when $y \equiv 1, 2(\mathrm{mod} 3)$, we have that $3 \mid (y^2+2)$, and when $y \equiv 0(\mathrm{mod} 3)$, we have that $3 \mid (y^k+3)$. That is, $d(f) \mid 6$, and since $f(0) = 6$, we get that $6 \mid d(f)$, and thus, $d(f) = 6$.

By Proposition 2.4.1 this is a polynomial with exactly 2 factorizations, $(X^2+2)(X^k+3)$ and $\frac{(X^2+2)(X^k+3)}{6} \cdot 2 \cdot 3$, and catenary degree 3.

So, f is a polynomial of degree $k+2 = n$ with $cat(f) = 3$. □

All together, we have proven the following.

Theorem 2.4.7 Given an integer $n \geq 2$ and c such that $2 \leq c \leq Omega(n!)+1$, there exists a polynomial $f \in \mathrm{Int}(\mathbb{Z})$ of degree n and catenary degree c. In particular, there exists such a polynomial with the property that $f \in \mathbb{Z}[x]$, and f has exactly two factorizations–one of length 2 and one of length c.

Once we have constructed polynomials of given catenary degree and polynomial degree, we can construct polynomials of desired elasticity and polynomial degree.

Theorem 2.3.5 Given $n \in \mathbb{N}$ which is ≥ 2, and rational number $1 < \frac{r}{s} \leq \frac{\Omega(n!)+1}{2}$ in lowest terms, there exists a polynomial $f \in \mathrm{Int}(\mathbb{Z})$ of elasticity $\frac{r}{s}$ if and only $r - s \leq \Omega(n!) - 1$.

Half-Proof We showed one direction in Section 2.3. Note that $2 \geq r - s + 2 \leq \Omega(n!) + 1$. The construction gives us a polynomial f with exactly two factorizations, of length $r - s + 2$ and 2.

In the case that $s \geq 2$, so $g = 2^{s-2}f \in \mathrm{Int}(\mathbb{Z})$. Then $\mathcal{L}(g) = (s-2) + (r-s+2) = r$ and $\ell(g) = (s-2) + 2 = s$. Thus, $\rho(g) = \frac{r}{s}$.

Otherwise, $s = 1$, and we want to construct a polynomial of elasticity $r \leq \frac{\Omega(n!)+1}{2}$ which implies $2r \leq \Omega(n!) + 1$ and we can construct a polynomial f of degree n with exactly two factorizations, of lengths $2r$ and 2. Then $\rho(f) = r$ as desired.

2.5 Catenary degree and polynomial degree

This section presents a proof that when f is restricted to be a product of n linear polynomials in $\mathbb{Z}[x]$, then $\text{cat}(f) \leq n$. While it is a less "full" result than those presented in the previous sections, it suggests that it may be interesting to examine the growth of $\text{cat}(f)$ if we restrict f to be a product of polynomials in $\mathbb{Z}[x]$ of degree at most k.

The first two lemmas are basic number theoretic properties of polynomials in $\mathbb{Z}[x]$.

Lemma 2.5.1: Let $\gcd(a, b) = 1$ and let p be prime. Then

1. $\exists x \in \mathbb{Z}$ such that $p \mid ax - b$ if and only if $p \nmid a$.
2. Let $x, y \in \mathbb{Z}$. If $p \nmid a$, then $ax - b \equiv ay - b(\text{mod}p^k)$ if and only if $x \equiv y(\text{mod}p^k)$.

Proof:

1.
   - Suppose $p \nmid a$. Then $a^{-1}(\text{mod}p)$ exists. Then, when $x = a^{-1} \cdot b$, we have $ax - b = a(a^{-1} \cdot b) - b \equiv 0(\text{mod}p)$.
   - Assume $\exists x \in \mathbb{Z}$ such that $p \mid ax - b$, and suppose that $p \mid a$. Then $ax \equiv b(\text{mod}p)$, and since $a \equiv 0(\text{mod}p)$, we have that $b \equiv ax \equiv 0(\text{mod}p)$. Then $p \mid b$ and $p \mid a$, so $p \mid \gcd(a, b)$. But $\gcd(a, b) = 1$. This is a contradiction, so $p \nmid a$.
2.
   - Suppose $ax - b \equiv ay - b(\text{mod}p)$. Then $ax \equiv ay(\text{mod}p)$, and since $p \nmid a$, we have that $a^{-1}(\text{mod}p)$ exists. Then $x \equiv a^{-1} \cdot ay(\text{mod}p) \equiv y(\text{mod}p)$
   - Suppose $x \equiv y(\text{mod}p^k)$, say $x = y + mp^k$. Then $ax - b = a(y + mp^k) - b = ay - b + amp^k \equiv ay - b(\text{mod}p^k)$. □

Lemma 2.5.2: Let $f \in \mathbb{Z}[X]$, and let $x \equiv y(\text{mod}m)$. Then $f(x) \equiv f(y)(\text{mod}m)$.
Proof: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, and let $y = x + km$. Then $f(y) = a_n(x + km)^n + a_{n-1}(x + km)^{n-1} + \ldots + a_0$. Then $\forall 0 \leq s \leq n$ we have $a_s(x + km)^s = a_s \sum_{i=0}^{s} \binom{s}{i} x^i (km)^{s-i} \equiv a_s x^s(\text{mod}m)$. Thus, $f(y) \equiv a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0(\text{mod}m) \equiv f(x)(\text{mod}m)$. □

The rest of the lemmas rely on the following definition:

Definition: Fix a polynomial $f = g_1 \cdots g_n \in Int(\mathbb{Z})$ and a prime number p. Let $x \in \mathbb{Z}$ and m a positive integer. Define $I_{x,m} = \{i \mid 1 \leq i \leq n, g_i(x) \equiv 0(\text{mod}p^m)\}$.

It is also useful to recall that $v_p(n)$ for an integer n is defined to be the highest power of p dividing n.

We want to use the sets defined above to count the prime divisors of f, in such a way that we can keep track of the contribution of each factor g_i to the prime divisor. The eventual goal is to prove that $v_p(d(f)) - v_p(d(f'))$ is bounded for f a product of linear polynomials and f' the product of $n - 1$ of those polynomials, which would allow us to use an inductive proof to find a bound for the catenary degree.

Lemma 2.5.3: Suppose $f = g_1 \cdots g_n$, with $g_i \in \text{Int}(\mathbb{Z})$, and let $x \in \mathbb{Z}$. Let p be prime. Let $r \in \mathbb{Z}$ such that $\forall 1 \leq i \leq n$, $p^{r+1} \nmid g_i(x)$. Then $v_p(f(x)) = \sum_{m=1}^{r} |I_{x,m}|$.

Proof: $\sum_{m=1}^{r} |I_{x_m}| = \sum_{i=1}^{n} |\{m \mid 1 \leq m \leq r, i \in I_{x,m}\}| = \sum_{i=1}^{n} v_p(g_i(x)) = v_p(f(x))$ □

Lemma 2.5.4: Let $f = g_1 \cdots g_n$, with $g_i \in \mathbb{Z}[X], \forall 1 \leq i \leq n$. Let $x \equiv y(\text{mod}p^r)$ and $x \not\equiv y(\text{mod}p^{r+1})$. Then $\forall 1 \leq m \leq r$, we have $I_{x,m} = I_{y,m}$. Furthermore, when $1 \leq i \leq n$, $g_i(x) = a_i x - b_i$ with $\gcd(a_i, b_i) = 1$ and $m > r$, we have that $I_{x,m} \cap I_{y,m} = \emptyset$.

Proof: Let $m \leq r$, and let $i \in I_{x,m}$. Then $x \equiv y(\text{mod}p^m)$, and $g_i(x) \equiv 0(\text{mod}p^m)$. By Lemma 2.5.2, $g_i(y) \equiv g_i(x)(\text{mod}p^m)$, so $g_i(y) \equiv 0(\text{mod}p^m)$. Thus, $i \in I_{y,m}$. Therefore, $I_{x,m} = I_{y,m}$.

Now, let $m > r$, and suppose $\forall 1 \leq i \leq n$, $g_i(x) = a_i x - b_i$ with $\gcd(a_i, b_i) = 1$. Let $i \in I_{x,m}$. Then $x \not\equiv y(\text{mod}p^m)$. Note also that since $i \in I_{x,m}$, we know that $g_i(x) \equiv 0(\text{mod}p)$, so $p \nmid a_i$. Thus, by Lemma 2.5.1, $g_i(x) \not\equiv g_i(y)(\text{mod}p^m)$, so $g_i(y) \not\equiv 0(\text{mod}p^m)$ and $i \notin I_{y,m}$. Thus, $I_{x,m} \cap I_{y,m} = \emptyset$. $\square$

Lemma 2.5.5: Let $f = g_1 \cdots g_n$, where $g_i \in \mathbb{Z}[X]$. Let $y \in \mathbb{Z}$, let p prime, and for some m and $\forall 0 \leq r \leq p-1$, let $y_r \equiv y + rp^{m-1}$. Then $\forall 0 \leq r \leq p-1$, $I_{y_r,m} \subseteq I_{y,m-1}$. If $\forall 1 \leq i \leq n$, $g_i = a_i x - b_i$ with $\gcd(a_i, b_i) = 1$, then $I_{y,m-1} = \dot{\bigcup}_{r=0}^{p-1} I_{y_r,m}$ and $|I_{y,m-1}| = \sum_{r=0}^{p-1} |I_{y_r,m}|$.

Proof: Let $i \in I_{y_r,m}$. Then $g_i(y_r) \equiv 0(\text{mod}p^m) \equiv 0(\text{mod}p^{m-1})$, so $i \in I_{y_r,m-1}$. By Lemma 2.5.4, since $y_r \equiv y(\text{mod}p^{m-1})$, we have $i \in I_{y,m-1}$ as well.

If $\forall 1 \leq i \leq n$, $g_i = a_i x - b_i$ with $\gcd(a_i, b_i) = 1$, then $\forall 0 \leq r, j \leq p-1, r \neq j$, we have by Lemma 2.5.4 that $I_{y_r,m-1} \cup I_{y_j,m-1} = \emptyset$. To see that $\forall i \in I_{y,m-1} \exists 0 \leq r \leq p-1$ such that $i \in I_{y_r,m}$, we let $0 \leq k \leq p-1$ such that $a_i y - b_i \equiv kp^{m-1}(\text{mod}p^m)$. Then, let $r \equiv -a^{-1}k(\text{mod}p)$ and note that $a_i(y_r) - b_i \equiv a_i(y - a^{-1}kp^{m-1}) - b_i(\text{mod}p^m) \equiv 0(\text{mod}p^m)$. That is, $i \in I_{y_r,m}$ for some r, so $I_{y,m-1} = \dot{\bigcup}_{r=0}^{p-1} I_{y_r,m}$ and $|I_{y,m-1}| = \sum_{r=0}^{p-1} |I_{y_r,m}|$. $\square$

Lemma 2.5.6: Let $f = (a_1 x - b_1) \cdots (a_n x - b_n)$, with $\gcd(a_i, b_i) = 1 \forall 1 \leq i \leq n$. Given $y \in \mathbb{Z}, m \geq 1$, $\exists y' \in \mathbb{Z}$ such that $y' \equiv y(\text{mod}p^m)$ and $|I_{y',m+1}| \leq \frac{I_{y,m}}{p}$, and $\exists y”$ such that $y” \equiv y(\text{mod}p^m)$ and $|I_{y”,m+1}| \geq \frac{|I_{y,m}|}{p}$.

Proof: $\forall 0 \leq r \leq p-1$ let $y_r \equiv y + rp^m(\text{mod}p^{m+1})$. By Lemma 2.5.4, $|I_{y,m}| = \sum_{r=0}^{p-1} |I_{y_r,m}|$. By Pigeonhole Principle, then, $\exists r$ such that $|I_{y_r,m}| \leq \frac{|I_{y,m}|}{p}$, and similarly, $\exists j$ such that $|I_{y_j,m}| \geq \frac{|I_{y,m}|}{p}$. Let $y' = y_r$, $y” = y_j$.$\square$

Corollary 2.5.7: Let $f = (a_1 x - b_1) \cdots (a_n x - b_n)$, with $\gcd(a_i, b_i) = 1 \forall 1 \leq i \leq n$. Let $y, m, t \in \mathbb{Z}$, with $m, t \geq 1$. Then $\exists y' \in \mathbb{Z}$ such that $y' \equiv y(\text{mod}p^m)$ and $\forall 1 \leq s \leq t$, we have $|I_{y',m+s}| \leq \frac{|I_{y,m}|}{p^s}$.

Proof: Induct on t. $t = 1$ is exactly Lemma 2.5.6. Assume $\exists y' \in \mathbb{Z}$ such that $y' \equiv y(\text{mod}p^m)$ and $\forall 1 \leq s \leq t-1$ we have $|I_{y',m+s}| \leq \frac{I_{y,m}}{p^s}$. By Lemma 2.5.6, we can again find $y” \in \mathbb{Z}$ such that $y” \equiv y'(\text{mod}p^{m+t-1})$ and $|I_{y”,m+t}| \leq \frac{|I_{y',m+t-1}|}{p}$. Then $y” \equiv y(\text{mod}p^m)$, and $|I_{y”,m+t}| \leq \frac{I_{y',m+t-1}}{p} \leq \frac{I_{y,m+t}}{p^t}$. Furthermore, because $y” \equiv y'(\text{mod}p^{m+t-1})$ and thus $\forall 1 \leq s \leq t-1$ we have $y” \equiv y'(\text{mod}p^{m+s})$, we know by Lemma 4 that $|I_{y”,m+s}| = |I_{y',m+s}| \leq \frac{|I_{y,m}}{p^s}$ by inductive hypothesis.

After these long, technical lemmas, we are finally able to prove the result that we want.

Lemma 2.5.8: Let $f'(x) = (a_2 x - b_2) \cdots (a_n x - b_n)$, and let $f(x) = (a_1 x - b_1) \cdot f'(x)$, where $\gcd(a_i, b_i) = 1, \forall 1 \leq i \leq n$. Let $k = v_p(d(f)) - v_p(d(f'))$. Then, $k \leq \lfloor \log_p(n) \rfloor$.

Proof: Let $l = v_p(d(f'))$. We show that $l + k \geq v_p(p^k!) = 1 + p + \ldots + p^{k-1}$.

First, note that $\exists x_0 \in \mathbb{Z}$ such that $p^{l+1} \nmid f'(x_0)$. Note also that since $p^{l+k} \mid d(f)$, we must have that $p^k \mid (a_1 x_0 - b_1)$. By Lemma 2.5.2, $\forall y \equiv x_0(\text{mod}p^{l+1})$, we have $p^{l+1} \nmid f'(y)$, and again, because $p^{l+k} \mid d(f)$, we have that $p^k \mid (a_1 y - b_1)$. By Lemma 2.5.1, $y \equiv x_0(\text{mod}p^k)$. Thus, $k - 1 \leq l$.

By Lemma 2.5.3, $l = \sum_{m=1}^{l} I_{x_0,m}$. Note that $l \leq \sum_{m=1}^{k-1} |I_{x_0,m}|$, and it suffices to show that

$\forall 1 \leq m \leq k-1, |I_{x_0,k-m}| \leq p^m - 1$. We proceed by induction on m.

$\forall 1 \leq r \leq p-1$, let $y_r \equiv x_0 + rp^{k-1} (\text{mod} p^k)$. Note that, for any r, $y_r \not\equiv x_0 (\text{mod} p^k)$ but $y_r \equiv x_0 (\text{mod} p^{k-1})$. Then by Lemma 1, $(a_1 y_r - b_1) \equiv (a_1 x_0 - b_1) \equiv 0 (\text{mod} p^{k-1})$ and $(a_1 y_r - b_1) \not\equiv (a_1 x_0 - b_1) \equiv 0 (\text{mod} p^k)$. That is, $p^k \nmid (a_1 y_r - b_1)$, so $p^{l+1} \mid f'(y_r)$. In other words, $v_p(f'(y_r)) \geq v_p(f'(x_0)) + 1$.

By Lemma 2.5.3, we can write this as

$$\sum_{i=1}^{v_p(f'(y_r))} |I_{y_r,i}| \geq (\sum_{i=1}^{l} |I_{x_0,i}|) + 1$$

. By Lemma 2.5.4, $\forall 1 \leq s \leq k-1$, $|I_{x_0,s}| = |I_{y_r,s}|$. We can subtract these terms from both sides, giving $\sum_{i=k}^{v_p(f'(y_r))} |I_{y_r,i}| \geq (\sum_{i=k}^{l} |I_{x_0,i}|) + 1$. Then $I_{y_r,k}$ must be nonempty–otherwise the left side is exactly 0–and by Lemma 2.5.5, we can write $|I_{x_0,k-1}| \geq \sum_{r=1}^{p-1} |I_{y_r,k}| \geq p-1$.

Now, assume $\forall 1 \leq t \leq m-1$ that $|I_{x_0,k-t}| \geq p^t - 1$.

Suppose for contradiction that $|I_{x_0,k-m}| < p^m - 1$. We know $\exists y \in \mathbb{Z}$ such that $y \equiv x_0 (\text{mod} p^{k-m})$, $y \not\equiv x_0 (\text{mod} p^{k-m+1})$, and $|I_{y,k-m+1}| < p^{m-1}$. If not, then $|I_{y,k-m+1}| \geq p^{m-1}$, and by inductive hypothesis, $|I_{x_0,k-m+1}| \geq p^{m-1} - 1$. So by Lemma 5, $|I_{x_0,k-m}| \geq (p-1) \cdot (p^{m-1}) + p^{m-1} - 1 = p^m - 1$, which contradicts our supposition that $|I_{x_0,k-m}| < p^m - 1$. Furthermore, by Corollary 7, $\exists y' \equiv y (\text{mod} p^{k-m+1})$ such that $\forall s \geq 1, |I_{y',k-m+1+s}| \leq \frac{|I_{y,k-m+1}|}{p^s} < p^{m-1-s}$. (Note that $I_{y',k} = \emptyset$).

Note that $y' \equiv x_0 (\text{mod} p^{k-m})$ and $y' \not\equiv x_0 (\text{mod} p^{k-m+1})$, so by Lemma 1, $p^{k-m} \mid (a_1 y' - b_1)$ but $p^{k-m+1} \nmid (a_1 y' - b_1)$. Because $p^{l+k} \mid d(f)$, we know $v_p(f'(y')) \geq l + m$. That is, $\sum_{i=1}^{k-1} |I_{y',i}| \geq (\sum_{i=1}^{l} |I_{x_0,i}|) + m \geq (\sum_{i=1}^{k-1} |I_{x_0,i}|) + m$

Since $y' \equiv x_0 (\text{mod} p^{k-m})$, we have by Lemma 2.5.4 that for $1 \leq r \leq k-m$, $I_{y',r} = I_{x_0,r}$, so we can subtract these values from each sum, leaving $\sum_{i=k-m+1}^{k-1} |I_{y',i}| \geq (\sum_{i=k-m+1}^{k-1} |I_{x_0,i}|) + m$. By inductive hypothesis, and by construction of y', we can write $\sum_{i=k-m+1}^{k-1} p^{k-i} < \sum_{i=k-m+1}^{k-1} |I_{y',i}| \geq (\sum_{i=k-m+1}^{k-1} |I_{x_0,i}|) + m \geq (\sum_{i=k-m+1}^{k-1} p^{k-i} - 1) + m = (\sum_{i=k-m+1}^{k-1} p^{k-1}) + 1$. This is a contradiction. So we must have $|I_{x_0,k-m}| \geq p^m - 1$.

By induction, we have $|I_{x_0,k-m}| \geq p^m - 1$ for all $1 \leq m \leq k-1$, so $l + k \geq \sum_{i=1}^{k} p^i$. □

The next statement gives an indication as to why this result is useful for our purposes, and why this previously encountered messiness may give a nice result.

Corollary 2.5.9: Let $f'(x) = (a_2 x - b_2) \cdots (a_n x - b_n)$, and let $f(x) = (a_1 x - b_1) \cdot f'(x)$, where $\gcd(a_i, b_i) = 1, \forall 1 \leq i \leq n$. Then $\Omega(d(f)) - \Omega(d(f')) \leq \sum_{\substack{p \leq n \\ p \text{ prime}}} \lfloor \log_p(n) \rfloor$.

Proof:

$$\Omega(d(f)) - \Omega(d(f'))$$

$$= \sum_{\substack{p \leq n \\ p \text{ prime}}} v_p(d(f)) - v_p(d(f'))$$

. By Lemma 8, this is less than or equal to

$$\sum_{\substack{p \le n \\ p \text{ prime}}} \lfloor \log_p(n) \rfloor$$

.

Lemma 2.5.10: Let $n \ge 2$. Then $\sum_{\substack{p \le n \\ p \text{ prime}}} \lfloor \log_p(n) \rfloor \le n - 1$.

Proof: We induct on n. $\sum_{\substack{p \le 2 \\ p \text{ prime}}} \lfloor \log_p(2) \rfloor = \lfloor \log_2(2) \rfloor = 1$. Suppose $\sum_{\substack{p \le n-1 \\ p \text{ prime}}} \lfloor \log_p(n-1) \rfloor \le n - 2$. Examine $\sum_{\substack{p \le n \\ p \text{ prime}}} \lfloor \log_p(n) \rfloor$. If for any prime p, $\lfloor \log_p(n) \rfloor > \lfloor \log_p(n-1) \rfloor$, then $n \ge p^{\lfloor \log_p(n) \rfloor} > n-1$. Since $p^{\lfloor \log_p(n) \rfloor}$ is an integer, we must have $n = p^{\lfloor \log_p(n) \rfloor}$. Clearly, in this case we cannot have $n = q^{\lfloor \log_q(n) \rfloor}$ for some $q \ne p$, so for any $q \ne p$, $\lfloor \log_q(n) \rfloor = \lfloor \log_q(n-1) \rfloor$. So, there is at most one prime p such that $\lfloor \log_p(n) \rfloor > \lfloor \log_p(n-1) \rfloor$. If $\lfloor \log_p(n) \rfloor \ge \lfloor \log_p(n-1) \rfloor + 2$ then $n \ge p^{\lfloor \log_p(n) \rfloor} > p^{\lfloor \log_p(n) \rfloor - 1} > n - 1$, but there is no integer between n and $n-1$, so $\lfloor \log_p(n) \rfloor < \lfloor \log_p(n-1) \rfloor + 2$. So,

$$\sum_{\substack{p \le n-1 \\ p \text{ prime}}} \lfloor \log_p(n) \rfloor \le \sum_{\substack{p \le n-1 \\ p \text{ prime}}} \lfloor \log_p(n) \rfloor + 1$$

By inductive hypothesis, this is $\le n - 1$.

□

Finally, the grand finale of this series of lemmas is a an inductive proof that shows that the catenary degree of a product of linear polynomials is bounded by its polynomial degree. Using an inductive proof, the case that induction doesn't make trivial–the case that doesn't somehow reduce to a factorization of a smaller degree polynomial of the same form–is the case in which $\frac{f}{d(f)}$ is irreducible. In this case, we remove one of the linear factors of f and ask what might happen to the fixed divisor of the $n-1$-degree polynomial which remains. From the above corollaries, we know that the number of prime divisors decreases, and we know the maximum amount that it can decrease (which is

$$\sum_{\substack{p \le n \\ p \text{ prime}}} \lfloor \log_p(n) \rfloor$$

). This allows us to carry through the inductive step.

Theorem 2.5.12: Let $f = (a_1x - b_1) \cdots (a_nx - b_n)$ be primitive. Then $\text{cat}(f) \le n$ in $\text{Int}(\mathbb{Z})$.

Proof: First, we assume that f is primitive. If f is not primitive, then we can always reduce to the primitive case by cancelling the content between any two factorizations. Note that the content must appear (factored) in every factorization by Lemma 2.3.1, so it suffices to consider the primitive case.

Induct on n. We already know that this holds in the case that $n = 2$, as $\Omega(2!) + 1 = 2$. Assume that for all functions g with a factorization into exclusively linear terms and with $deg(g) \le n - 1$, that $cat(g) \le deg(g)$. Consider $f = (a_1x - b_1) \cdots (a_nx - b_n)$ (where $\gcd(a_i, b_i) = 1, \forall i$).

Let z be the factorization of f into linear terms. Let z' by any factorization not equal to the factorization into linear terms, say $z' = c_1 \cdots c_m$. We have two cases:

Case 1: Suppose $\forall 1 \le i \le m$, $\deg(c_i) \le n-1$. Then without loss of generality, let $c_1, c_2, \ldots, c_k$ be nonconstant polynomials. $\forall 1 \le i \le k$ we can write $c_i = \frac{c_i^*}{d(c_i^*)}$ for some $c_i^* \in \mathbb{Z}[X]$. (By unique factorization in $\mathbb{Z}[X]$, c_i^* will be a product of linear terms in z.) Since f is primitive and has a factorization in $\mathbb{Z}[X]$, we can write $z' = \frac{c_1^*}{d(c_1^*)} \cdots \frac{c_k^*}{d(c_k^*)} d(c_1^*) \cdots d(c_k^*)$ (where each $d(c_i^*)$ is factored). Let $f_1(x) = c_1 \cdots d(c_1^*)$ and $f_2(x) = c_2 \cdots c_k \cdot d(c_2^*) \cdots d(c_k^*)$, noting that $f_1(x)f_2(x) = f(x)$, $deg(f_1) \le n - 1$, and $deg(f_2) \le n - 1$.

Then $f_1 = c_1^*$, which is a product of linear terms in the factorization z. Reorder so that $c_1^* = (a_1x - b_1) \cdots (a_rx - b_r)$. Then $\frac{z'}{c_2 \cdots c_k \cdot d(c_2^*) \cdots d(c_k^*)} = c_1 \cdots d(c_1^*)$ is factorization of f_1, and

$\frac{z}{(a_{r+1}x-b_{r+1})\cdots(a_nx-b_n)} = (a_1x-b_1)\cdots(a_rx-b_r)$ is also factorization of f_1. By inductive hypothesis, we can find an $(n-1)$-chain from $\frac{z'}{c_2\cdots c_k\cdot d(c_2^*)\cdots d(c_k^*)}$ to $\frac{z}{(a_{r+1}x-b_{r+1})\cdots(a_nx-b_n)}$, say, $z_1 = \frac{z'}{c_2\cdots c_k\cdot d(c_2^*)\cdots d(c_k^*)}, z_2, \ldots, z_h = \frac{z}{(a_{r+1}x-b_{r+1})\cdots(a_nx-b_n)}$. Multiply each factorization by $c_2\cdots c_k \cdot d(c_2^*)\cdots d(c_k^*)$ to get factorizations of f, noting that $z_1 \cdot c_2\cdots c_k \cdot d(c_2^*)\cdots d(c_k^*)$ is exactly z'.

Denote $z_h \cdot c_2\cdots c_k \cdot d(c_2^*)\cdots d(c_k^*)$ as $z”$. Note that $f_2 = (a_{r+1}x-b_{r+1})\cdots(a_nx-b_n)$ and $deg(f_2) \leq n-1$, so by inductive hypothesis, we can find an (n-1)-chain between $\frac{z”}{z_h}$ and $(a_{r+1}x-b_{r+1})\cdots(a_nx-b_n) = \frac{z}{(a_1x-b_1)\cdots(a_rx-b_r)}$, say $z_1^* = \frac{z”}{z_h}, z_2^*, \ldots, z_j^* = \frac{z}{(a_1x-b_1)\cdots(a_rx-b_r)}$. Multiply by $(a_1x-b_1)\cdots(a_rx-b_r)$ to get factorizations of f, with $(a_1x-b_1)\cdots(a_rx-b_r)\cdot z_1^* = z”$ and $(a_1x-b_1)\cdots(a_rx-b_r)\cdot z_j^* = z$.

Then $z_1 \cdot (c_2\cdots c_k \cdot d(c_2^*)\cdots d(c_k^*)), z_2 \cdot (c_2\cdots c_k \cdot d(c_2^*)\cdots d(c_k^*)), \ldots, z”, ((a_1x-b_1)\cdots(a_rx-b_r))\cdot z_2^*, ((a_1x-b_1)\cdots(a_rx-b_r))\cdot z_3^*, \ldots, (a_1x-b_1)\cdots(a_rx-b_r)\cdot z_j^*$ is an (n-1)-chain between z' and z.

Case 2: Suppose for some c_i, we have $\deg(c_i) = n$. Without loss of generality, say this is c_1. Because c_1 is irreducible and nonconstant, we know $c_1 = \frac{(a_1x-b_1)\cdots(a_nx-b_n)}{d(f)}$. Since f is primitive and factors in $\mathbb{Z}[X]$, we know $c_2\cdots c_m = d(f)$.

Let

$$f'(x) = (a_2x-b_2)\cdots(a_nx-b_n)$$

, and let w be an arbitrary factorization of $\frac{f'(x)}{d(f')}$. Let

$$z” = (a_1x-b_1)\cdot w \cdot d(f')$$

(where $d(f')$ is factored). Then $d(z', z”) = max\{\Omega(d(f)) - \Omega(d(f')) + 1, |w|+1\}$. By Corollary 11, $\Omega(d(f)) - \Omega(d(f')) \leq n-1$. Since w is a factorization of an image primitive polynomial, then w is a factorization into nonconstant polynomials, so $|w| \leq n-1$. Thus, $d(z', z”) \leq n$. Note that $w \cdot d(f') = (a_2x-b_2)\cdots(a_nx-b_n)$, which is a primitive product of linear polynomials of degree $n-1$. Then there is an (n-1)-chain from $w\cdot d(f')$ to the factorization $(a_2x-b_2)\cdots(a_nx-b_n)$, say $z_1 = w\cdot d(f'), z_2, \ldots, z_r = (a_2x-b_2)\cdots(a_nx-b_n)$. Multiply each factorization by (a_1x-b_1) for factorizations of f, where $(a_1x-b_1)\cdot w\cdot d(f') = z”$ and $(a_1x-b_1)\cdots(a_nx-b_n) = z$. Then $z', z”, (a_1x-b_1)\cdot z_2, \ldots, (a_1x-b_1)\cdot z_r$ is an n-chain from z' to z.

In both cases, given any two factorizations z' and z^*, we can find an n-chain from z' to z and from z to z^*, and so $cat(f) \leq n$. □

We remark here that this bound is "good," though not in the same sense that the first bound we produced is "good." In particular, we can easily construct a polynomial of this form, whose catenary degree is equal to its polynomial degree, by using f_p as defined in section, and considering $p\cdot f_p$. $p\cdot f_p$ has precisely two factorizations, a product of p linear polynomials and the factorization $p\cdot f_p$ (as f_p is irreducible). By Proposition 2.4.1, the catenary degree is exactly p.

3 Conclusion

We gave a short history of the study of the ring of integer-valued polynomials and the study of nonunique factorization in Int($\mathbb{Z}$). In particular, we defined the elasticity and catenary degree, and using factorization properties shown by Chapman and McClain, and Frisch, we were able to show original results bounding these values in Int($\mathbb{Z}$).

We showed that the catenary degree of Int($\mathbb{Z}$) is unbounded in general. When we restrict f to be of degree n, we found that cat$(f) \leq \Omega(n!) + 1$. As a corollary, we also found bounds for elasticity of a polynomial of degree n. When we restricted f further such that f is a product of n linear polynomials, we found that cat$(f) \leq n$.

We also showed that we can construct f of given polynomial degree n and given catenary degree between 2 and $\Omega(n!) + 1$, as well as of polynomial degree n and elasticty between 1 and $\frac{\Omega(n!)+1}{2}$.

Some natural questions remain unanswered. With regards to bounds of catenary degree, the bound for f a product of linears was not particularly sharp. If the fixed divisor of f factors in a certain way, can we put stricter bounds on the catenary degree? Furthermore, the proof we gave in the general case admitted corollaries regarding elasticity–can we do this in the linear case as well?

Regarding constructions, we were able to prescribe two of three conditions at a time. Can we, under any conditions, construct a polynomial of prescribed polynomial degree, catenary degree, and elasticity? Can we prescribe elasticity and catenary degree? If we could prescribe a very small elasticity and a very large catenary degree, both of which are measures of nonunique factorization, it would be an indication of a certain independence between them, which would be surprising. At the same time, we do not have results which link elasticity to catenary degree, aside from the computation of the catenary degree of $f_p^s h_p^k$ and the remark that the integers s, k, and prime p can be chosen such that this polynomial has certain elasticity.

There are also questions about to what extent the results generalize. In particular, it would be interesting to investigate to what extent catenary degree might have algebraic implications (similar to the question Carlitz answered regarding elasticity), and what these might mean for $\text{Int}(\mathbb{Z})$.

4 Acknowledgements

I would like to acknowledge my REU group, Fairfield University, and the NSF for funding and supporting the majority of the research that was summarized in this paper. In particular, although it was a collaboration, it is certainly true that my group members Greg Knapp and Jad Salem, and advisor Paul Baginski, proved some of the deeper results in this paper (regarding most of the constructions and also the general bounds on catenary degree and elasticity with respect to polynomial degree). I would also like to acknowledge and thank the University of Rochester mathematics department, and in particular the honors committee who heard me present on this topic. Some interesting information in the background was added based on suggestions from Professor Naomi Jochnowitz (that the ring is not Noetherian and why this is interesting) and Professor Dinesh Thakur (the result relating class number to elasticity).

5 References

[1] P.J. Cahen and J-L Chabert, *Integer-Valued Polynomials*, American Mathematical Society, 1997.

[2] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. of the American Mathematical Society, 1960.

[3] S. Chapman and B. McClain, *Irreducible polynomials and full elasticity in the ring of integer-valued polynomials*, Journal of Algebra **293** (2005), 595-610

[4] S. Frisch, *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations*, Monatsh Math **171** (2013) 341-350