Nonunique Factorization in the Ring of Integer-Valued Polynomials

Paul Baginski

Fairfield University

March 22, 2019

2016 Fairfield University REU project.

- Gregory Knapp, Case Western Reserve University
- Jad Salem, Oberlin College
- Gabrielle Scullard, University of Rochester

The **ring of integer-valued polynomials** is

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid \forall n \in \mathbb{Z}\ f(n) \in \mathbb{Z}\}$$

The **ring of integer-valued polynomials** is

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid \forall n \in \mathbb{Z}\ f(n) \in \mathbb{Z}\}$$

$\mathbb{Z}[x] \subsetneq \mathrm{Int}(\mathbb{Z}) \subsetneq \mathbb{Q}[x]$ because

$$\frac{x}{2} \notin \mathrm{Int}(\mathbb{Z})$$

$$\text{but} \qquad \frac{x(x-1)}{2} \in \mathrm{Int}(\mathbb{Z})$$

and

The **ring of integer-valued polynomials** is

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid \forall n \in \mathbb{Z}\ f(n) \in \mathbb{Z}\}$$

$\mathbb{Z}[x] \subsetneq \mathrm{Int}(\mathbb{Z}) \subsetneq \mathbb{Q}[x]$ because

$$\frac{x}{2} \notin \mathrm{Int}(\mathbb{Z})$$

$$\text{but} \qquad \frac{x(x-1)}{2} \in \mathrm{Int}(\mathbb{Z})$$

$$\text{and} \qquad \binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-(n-1))}{n!} \in \mathrm{Int}(\mathbb{Z})$$

$\mathrm{Int}(\mathbb{Z})$ is non-Noetherian.

Irreducible elements:

- primes $p \in \mathbb{Z}$;
- linear polynomials $ax + b$ in $\mathbb{Z}[x]$ with $a \neq 0$ and $\gcd(a, b) = 1$;
- binomial polynomials $\binom{x}{n}$;
- many other polynomials.

$\mathrm{Int}(\mathbb{Z})$ is non-Noetherian.

Irreducible elements:

- primes $p \in \mathbb{Z}$;
- linear polynomials $ax + b$ in $\mathbb{Z}[x]$ with $a \neq 0$ and $\gcd(a, b) = 1$;
- binomial polynomials $\binom{x}{n}$;
- many other polynomials.

$\mathrm{Int}(\mathbb{Z})$ also has nonunique factorization:

$$x(x-1)(x-2)(x-3)(x-4) = \binom{x}{5} \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$$
$$= \frac{x(x-2)(x-4)}{3}(x-1)(x-3) \cdot 3$$

If $f \in \mathrm{Int}(\mathbb{Z})$, the **set of factorizations** is

$$Z(f) = \{f = g_1 \cdots g_k \mid k \in \mathbb{N},\ g_i \in \mathrm{Int}(\mathbb{Z}) \text{ irreducible}\}$$

which can be graded into factorizations of length k

$$Z_k(f) = \{f = g_1 \cdots g_k \mid g_i \in \mathrm{Int}(\mathbb{Z}) \text{ irreducible}\}$$

The **multiplicity** of a length k is $|Z_k(f)|$, the number of factorizations of f of that length k.

The **set of lengths** for f is

$$\begin{aligned} \mathsf{L}(f) &= \{k \in \mathbb{N} \,|\, f = g_1 g_2 \cdots g_k,\ g_i \in \mathsf{Int}(\mathbb{Z}) \text{ irreducible}\} \\ &= \{k \in \mathbb{N} \,|\, Z_k(f) \neq \emptyset\} \end{aligned}$$

Since

$$\begin{aligned} x(x-1)(x-2)(x-3)(x-4) &= \binom{x}{5} * 2 * 2 * 2 * 3 * 5 \\ &= \frac{x(x-2)(x-4)}{3}(x-1)(x-3) * 3 \end{aligned}$$

we have $\{4, 5, 6\} \subseteq \mathsf{L}(x(x-1)(x-2)(x-3)(x-4))$.

The **set of lengths** for f is

$$\begin{aligned} \mathsf{L}(f) &= \{k \in \mathbb{N} \,|\, f = g_1 g_2 \cdots g_k,\ g_i \in \mathsf{Int}(\mathbb{Z}) \text{ irreducible}\} \\ &= \{k \in \mathbb{N} \,|\, Z_k(f) \neq \emptyset\} \end{aligned}$$

For $f = x(x-1)(x-2)(x-3)(x-4)$, we have

$$\begin{aligned} L(f) &= \{4, 5, 6\} \\ |Z_4(f)| &= \\ |Z_5(f)| &= \\ |Z_6(f)| &= 1 \\ &= \end{aligned}$$

The **set of lengths** for f is

$$\begin{aligned} \mathsf{L}(f) &= \{k \in \mathbb{N} \,|\, f = g_1 g_2 \cdots g_k,\ g_i \in \mathsf{Int}(\mathbb{Z}) \text{ irreducible}\} \\ &= \{k \in \mathbb{N} \,|\, Z_k(f) \neq \emptyset\} \end{aligned}$$

For $f = x(x-1)(x-2)(x-3)(x-4)$, we have

$$\begin{aligned} L(f) &= \{4, 5, 6\} \\ |Z_4(f)| &= 3 \\ |Z_5(f)| &= \\ |Z_6(f)| &= 1 \\ &= \end{aligned}$$

The **set of lengths** for f is

$$\begin{aligned} \mathsf{L}(f) &= \{k \in \mathbb{N} \,|\, f = g_1 g_2 \cdots g_k,\ g_i \in \mathsf{Int}(\mathbb{Z}) \text{ irreducible}\} \\ &= \{k \in \mathbb{N} \,|\, Z_k(f) \neq \emptyset\} \end{aligned}$$

For $f = x(x-1)(x-2)(x-3)(x-4)$, we have

$$\begin{aligned} L(f) &= \{4, 5, 6\} \\ |Z_4(f)| &= 3 \\ |Z_5(f)| &= 18 \\ |Z_6(f)| &= 1 \\ |Z(f)| &= 22 \end{aligned}$$

Theorem (Frisch 2013)

For any finite nonempty subset $L \subseteq \mathbb{N}_{\geq 2}$ *and any function* $\mu : L \to \mathbb{N}_{\geq 1}$, *there exists* $f \in \mathsf{Int}(\mathbb{Z})$ *with*

$$\mathsf{L}(f) = L \qquad and \qquad \forall k \in \mathsf{L}(f)\ \ \mu(k) = |Z_k(f)|$$

Theorem (Frisch 2013)

For any finite nonempty subset $L \subseteq \mathbb{N}_{\geq 2}$ and any function $\mu : L \to \mathbb{N}_{\geq 1}$, there exists $f \in \mathrm{Int}(\mathbb{Z})$ with

$$\mathrm{L}(f) = L \qquad and \qquad \forall k \in \mathrm{L}(f)\ \ \mu(k) = |Z_k(f)|$$

Recursive construction and the degree of the polynomials grows quickly.

Question: How bad is factorization if we restrict the polynomial degree n?

Used two measures:

1. **Elasticity** $\rho(f) = \frac{\max \mathsf{L}(f)}{\min \mathsf{L}(f)}$
2. **Catenary degree** $\mathrm{cat}(f)$, measures globally how similar factorizations are, paying attention to individual factors.

For $f = x(x-1)(x-2)(x-3)(x-4)$, we have

$$\begin{aligned} L(f) &= \{4, 5, 6\} \\ |Z_4(f)| &= 3 \\ |Z_5(f)| &= 18 \\ |Z_6(f)| &= 1 \end{aligned}$$

Catenary degree asks: can we run through these 22 factorizations using just a few swaps?

Exact definition of catenary degree

For factorizations z, z' of f with $\gcd(z, z') = z''$, the **distance** is

$$\mathrm{d}(z, z') = \max\{|z/z''|, |z'/z''|\}$$

An N-**chain** from z to z' are factorizations $z = z_0, z_1, \ldots, z_k = z'$, such that for all $0 \leq i \leq k-1$, $\mathrm{d}(z_i, z_{i+1}) \leq N$.

The **catenary degree** of f is

$$\mathrm{cat}(f) = \min\{N \in \mathbb{N} \,|\, \forall z, z' \in Z(f) \\ z \text{ and } z' \text{ can be connected by an } N\text{-chain}\}$$

Problem: Fix $n \in \mathbb{N}$. Consider all $f \in \mathrm{Int}(\mathbb{Z})$ with $\deg(f) = n$. What possible values do we get for $\rho(f)$ and $\mathrm{cat}(f)$?

Problem: Fix $n \in \mathbb{N}$. Consider all $f \in \mathrm{Int}(\mathbb{Z})$ with $\deg(f) = n$. What possible values do we get for $\rho(f)$ and $\mathrm{cat}(f)$?

Results involve $\Omega(k) =$ number of prime factors of $k \in \mathbb{Z}$, counting multiplicity. E.g. $\Omega(20) = \Omega(2 * 2 * 5) = 3$.

Problem: Fix $n \in \mathbb{N}$. Consider all $f \in \mathrm{Int}(\mathbb{Z})$ with $\deg(f) = n$. What possible values do we get for $\rho(f)$ and $\mathrm{cat}(f)$?

Results involve $\Omega(k) =$ number of prime factors of $k \in \mathbb{Z}$, counting multiplicity. E.g. $\Omega(20) = \Omega(2 * 2 * 5) = 3$.

For $n = 0$ or $n = 1$, get $\rho(f) = 1$ and $\mathrm{cat}(f) = 0$ for all f because we have unique factorization. So let $n \geq 2$.

Slight simplification:

Lemma. Each $f \in \mathrm{Int}(\mathbb{Z})$ can be written uniquely as $f = af^*/b$, where $a, b \in \mathbb{N}$ and $f^* \in \mathbb{Z}[x]$ is primitive (i.e., gcd of its coefficients is 1). Furthermore, we have

$$Z(f) = Z_{\mathbb{Z}}(a) + Z(f^*/b)$$

Elasticity:

Theorem

If $f = af^*/b \in \mathrm{Int}(\mathbb{Z})$ *and* $\deg(f) = n \geq 2$, *then*

1. $\max \mathrm{L}(f^*/b) \leq \Omega(n!) + 1$
2. $0 \leq \max \mathrm{L}(f) - \min \mathrm{L}(f) \leq \Omega(n!) - 1$
3. *If* $\max \mathrm{L}(f) \neq \min \mathrm{L}(f)$ *then*

$$1 < \rho(f) \leq \frac{\Omega(n!) + 1}{2}$$

Elasticity:

Theorem

If $f = af^*/b \in \mathrm{Int}(\mathbb{Z})$ *and* $\deg(f) = n \geq 2$, *then*

1. $\max \mathrm{L}(f^*/b) \leq \Omega(n!) + 1$
2. $0 \leq \max \mathrm{L}(f) - \min \mathrm{L}(f) \leq \Omega(n!) - 1$
3. *If* $\max \mathrm{L}(f) \neq \min \mathrm{L}(f)$ *then*

$$1 < \rho(f) \leq \frac{\Omega(n!) + 1}{2}$$

Conversely, given

$$1 < \frac{r}{s} \leq \frac{\Omega(n!) + 1}{2} \ \textit{with}\ 1 \leq r - s \leq \Omega(n!) - 1$$

$\exists f \in \mathrm{Int}(\mathbb{Z})$ *with* $\deg(f) = n$ *and* $\rho(f) = r/s$.

Catenary degree:

Theorem

If $f = af^*/b \in \mathrm{Int}(\mathbb{Z})$ *and* $\deg(f) = n \geq 2$, *then*

$$\mathrm{cat}(f) = 0 \quad \textit{or} \quad 2 \leq \textit{cat}(f) \leq \Omega(n!) + 1$$

Catenary degree:

Theorem

If $f = af^*/b \in \mathrm{Int}(\mathbb{Z})$ *and* $\deg(f) = n \geq 2$, *then*

$$\mathrm{cat}(f) = 0 \quad or \quad 2 \leq cat(f) \leq \Omega(n!) + 1$$

Conversely, given

$$c = 0 \quad or \quad 2 \leq c \leq \Omega(n!) + 1$$

$\exists f \in \mathrm{Int}(\mathbb{Z})$ *with* $\deg(f) = n$ *and* $\mathrm{cat}(f) = c$.

Both together:

Theorem. Fix $n \geq 0$ and set
$A = \{(\rho(f), \mathrm{cat}(f)) \mid f \in \mathrm{Int}(\mathbb{Z}),\ \deg(f) = n\}$.

- If $n = 0$ or $n = 1$, then $A = \{(1, 0)\}$;
- If $n = 2$ then $A = \{(1, 0), (1, 2)\}$;
- If $n \geq 3$, then

$$A \subseteq \{(1,0),(1,2)\} \cup \left\{ \left(\frac{s+k}{t+k},\ c \right) \,\middle|\, c \in [3, \Omega(n!)+1],\ k \geq 0,\ s \in [c, \Omega(n!)+1],\ t \in [2, s] \right\}$$

$$A \supseteq \{(1,0),(1,2)\} \cup \left\{ \left(\frac{u+k}{k},\ c \right) \,\middle|\, c \in [3, \Omega(n!)+1], k \geq 2, \text{ and } u | c-2 \right\}$$

Previous theorems use high-degree irreducibles of $\mathbb{Z}[x]$ in constructions. By contrast:

Previous theorems use high-degree irreducibles of $\mathbb{Z}[x]$ in constructions. By contrast:

Theorem

If $f \in \mathbb{Z}[x]$ has degree $n \geq 2$ and f factors in $\mathbb{Z}[x]$ as a product of linear polynomials and constants, i.e.

$$f = c_1 c_2 \dots c_k (a_1 x - b_1) \cdots (a_n x - b_n)$$

then f considered in $\mathrm{Int}(\mathbb{Z})$ will satisfy

$$\max \mathrm{L}(f) \leq k + \Omega(n!) + 1$$

$$1 \leq \rho(f) \leq \frac{k + \Omega(n!) + 1}{k + 2}$$

$$\mathrm{cat}(f) \leq \Omega(n!) + 1$$

Previous theorems use high-degree irreducibles of $\mathbb{Z}[x]$ in constructions. By contrast:

Theorem

If $f \in \mathbb{Z}[x]$ has degree $n \geq 2$ and f factors in $\mathbb{Z}[x]$ as a product of linear polynomials and constants, i.e.

$$f = c_1 c_2 \dots c_k (a_1 x - b_1) \cdots (a_n x - b_n)$$

then f considered in $\mathrm{Int}(\mathbb{Z})$ will satisfy

$$\max \mathsf{L}(f) \leq k + \Omega(n!) + 1$$

$$1 \leq \rho(f) \leq \frac{k + \Omega(n!) + 1}{k + 2}$$

$$\mathrm{cat}(f) \leq n$$

Thank you.

References

- P. Baginski, G. Knapp, J. Salem, G. Scullard, *Elasticity and catenary degree in the ring of integer-valued polynomials*, in preparation.
- S. Frisch, *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations* Monatsh. Math. (2013) **171** 341–350.
- P.-J. Cahen, J.-L. Chabert, *What you should know about integer-valued polynomials*, Amer. Math. Monthly (2016) **123**, no. 4, 311–337.