Factorization Properties of Integer-Valued Polynomials

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

May 10, 2018

Abstract

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 Int(Z) has full elasticity, that is, every rational number $\frac{m}{n} > 1$ can be attained as the elasticity of some polynomial in Int(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 $z_1 = a_1 a_2 \cdots a_r p_1 p_2 \cdots p_n$ and $z_2 = a_1 a_2 \cdots a_r q_1 q_2 \cdots q_m$ be factorizations of x such that a_i are irreducible elements appearing in z_1 and in z_2, and $p_i = q_j$ for any i, j. A is an integral domain, so we can cancel each of the a_i to get factorizations $z_1 = p_1 p_2 \cdots p_n$ and $z_2 = q_1 q_2 \cdots q_m$ which have no terms in common and are both factorizations of the same $x \quad A$. 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 $\text{cat}(A) = \sup\{\text{cat}(x) \mid x \quad A\}$.

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 $\{f \quad K[x] \mid f(S) \quad D\}$ for K the quotient field of D, and that Int(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 $f \quad \text{Int}(S, D)$, $d(S, f) = \gcd\{f(s) \mid s \quad S\}$. When $d(S, f) = 1$ we say that f is image primitive over S

Proof: (1) $\frac{f(x)}{d(f)}$ is an element of $\mathrm{Int}(S, D)$, 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 127/Ty3f

Our main result is that a polynomial f of degree n has $\mathrm{cat}(f) \leq \Omega$

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 inax(

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 $r = \Omega($

(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 $\frac{n!}{P}$, $g(x) \equiv u_i \frac{n!}{q_i^{j_i} P} g_i(x)$mod

Otherwise, $s = 1$

$1 \leq m \leq k-1, |I_{x_0,k-m}| \leq p^m - 1$. We proceed by induction on m.
$1 \leq r \leq p-1$, let $y_r \equiv x_0 + rp^{k-1} (\mathrm{mod}\, p^k)$

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

□

p

$$\frac{z}{(a_{r+1}x - b_{r+1})\cdots(a_n x - b_n)} = (a_1 x - b_1)\cdots(a_r x - b_r)$$

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 Int(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