A construction of integer-valued polynomials with prescribed sets of lengths of factorizations

Sophie Frisch

Received: 2 June 2012 / Accepted: 24 April 2013 / Published online: 22 May 2013
© The Author(s) 2013. This article is published with open access at Springerlink.com

Abstract For an arbitrary finite non-empty set \( S \) of natural numbers greater 1, we construct \( f \in \text{Int}(\mathbb{Z}) = \{ g \in \mathbb{Q}[x] \mid g(\mathbb{Z}) \subseteq \mathbb{Z} \} \) such that \( S \) is the set of lengths of \( f \), i.e., the set of all \( n \) such that \( f \) has a factorization as a product of \( n \) irreducibles in \( \text{Int}(\mathbb{Z}) \). More generally, we can realize any finite non-empty multi-set of natural numbers greater 1 as the multi-set of lengths of the essentially different factorizations of \( f \).

Mathematics Subject Classification (2000) Primary 13A05; Secondary 13B25 · 13F20 · 20M13 · 11C08

1 Introduction

Non-unique factorization has long been studied in rings of integers of number fields, see the monograph of Geroldinger and Halter-Koch [5]. More recently, non-unique factorization in rings of polynomials has attracted attention, for instance in \( \mathbb{Z}_p[x] \), cf. [4], and in the ring of integer-valued polynomials \( \text{Int}(\mathbb{Z}) = \{ g \in \mathbb{Q}[x] \mid g(\mathbb{Z}) \subseteq \mathbb{Z} \} \) (and its generalizations) [1,3].

We show that every finite set of natural numbers greater 1 occurs as the set of lengths of factorizations of an element of \( \text{Int}(\mathbb{Z}) \) (Theorem 9 in Sect. 4).

Our proof is constructive, and allows multiplicities of lengths of factorizations to be specified. For example, given the multiset \( \{2,2,2,5,5\} \), we construct a polynomial that has three different factorizations into 2 irreducibles and two different factorizations into...
5 irreducibles, and no other factorizations. Perhaps a quick review of the vocabulary of factorizations is in order:

**Notation and Conventions**  \( R \) denotes a commutative ring with identity. An element \( r \in R \) is called **irreducible** in \( R \) if \( r \) is a non-zero non-unit such that \( r = ab \) with \( a, b \in R \) implies that \( a \) or \( b \) is a unit. A **factorization** of \( r \) in \( R \) is an expression \( r = s_1 \ldots s_n \) of \( r \) as a product of irreducible elements in \( R \). The number \( n \) of irreducible factors is called the **length** of the factorization. The **set of lengths** \( L(r) \) of \( r \in R \) is the set of all natural numbers \( n \) such that \( r \) has a factorization of length \( n \) in \( R \).

\( R \) is called **atomic** if every non-zero non-unit of \( R \) has a factorization in \( R \).

If \( R \) is atomic, then for every non-zero non-unit \( r \in R \) the **elasticity of** \( r \) is defined as

\[
\rho(r) = \sup \left\{ \frac{m}{n} \mid m, n \in L(r) \right\}
\]

and the elasticity of \( R \) is \( \rho(R) = \sup_{r \in R'}(\rho(r)) \), where \( R' \) is the set of non-zero non-units of \( R \). An atomic domain \( R \) is called **fully elastic** if every rational number greater than 1 occurs as \( \rho(r) \) for some non-zero non-unit \( r \in R \).

Two elements \( r, s \in R \) are called **associated** in \( R \) if there exists a unit \( u \in R \) such that \( r = us \). Two factorizations of the same element \( r = r_1 \cdots r_m = s_1 \cdots s_n \) are called **essentially the same** if \( m = n \) and, after re-indexing the \( s_i, r_j \) is associated to \( s_j \) for \( 1 \leq j \leq m \). Otherwise, the factorizations are called **essentially different**.

### 2 Review of factorization of integer-valued polynomials

In this section we recall some elementary properties of \( \text{Int}(\mathbb{Z}) \) and the fixed divisor \( d(f) \), to be found in [1–3]. The reader familiar with integer-valued polynomials is encouraged to skip to Sect. 3.

**Definition**  For \( f \in \mathbb{Z}[x] \),

(i) the **content** \( c(f) \) is the ideal of \( \mathbb{Z} \) generated by the coefficients of \( f \),

(ii) the **fixed divisor** \( d(f) \) is the ideal of \( \mathbb{Z} \) generated by the image \( f(\mathbb{Z}) \).

By abuse of notation we will identify the principal ideals \( c(f) \) and \( d(f) \) with their non-negative generators. Thus, for \( f = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x] \),

\[
c(f) = \gcd(a_k \mid k = 0, \ldots, n) \quad \text{and} \quad d(f) = \gcd(f(c) \mid c \in \mathbb{Z}).
\]

A polynomial \( f \in \mathbb{Z}[x] \) is called **primitive** if \( c(f) = 1 \).

Recall that a primitive polynomial \( f \in \mathbb{Z}[x] \) is irreducible in \( \mathbb{Z}[x] \) if and only if it is irreducible in \( \mathbb{Q}[x] \). Similarly, \( f \in \mathbb{Z}[x] \) with \( d(f) = 1 \) is irreducible in \( \mathbb{Z}[x] \) if and only if it is irreducible in \( \text{Int}(\mathbb{Z}) \).

We denote \( p \)-adic valuation by \( v_p \). Almost everything that we need to know about the fixed divisor follows immediately from the fact that

\[
v_p(d(f)) = \min_{c \in \mathbb{Z}}(v_p(f(c))).
\]
In particular, it is easy to deduce that for any \( f, g \in \mathbb{Z}[x] \),

\[
\text{d}(f)\text{d}(g) \mid \text{d}(fg).
\]

Unlike \( c(f) \), which satisfies \( c(f)c(g) = c(fg) \), \( \text{d}(f) \) is not multiplicative: \( \text{d}(f)\text{d}(g) \) is in general a proper divisor of \( \text{d}(fg) \).

**Remark 1**

(i) Every non-zero polynomial \( f \in \mathbb{Q}[x] \) can be written in a unique way as

\[
f(x) = \frac{a g(x)}{b} \quad \text{with} \quad g \in \mathbb{Z}[x], \ c(g) = 1, \ a, b \in \mathbb{N}, \ \gcd(a, b) = 1.
\]

(ii) When expressed as in (i), \( f \) is in \( \text{Int}(\mathbb{Z}) \) if and only if \( b \) divides \( \text{d}(g) \).

(iii) For non-constant \( f \in \text{Int}(\mathbb{Z}) \) expressed as in (i) to be irreducible in \( \text{Int}(\mathbb{Z}) \) it is necessary that \( a = 1 \) and \( b = \text{d}(g) \).

**Proof**

(i) and (ii) are easy. Ad (iii). Note that the only units in \( \text{Int}(\mathbb{Z}) \) are \( \pm 1 \). By (ii), \( b \) divides \( \text{d}(g) \). Let \( \text{d}(g) = bc \). Then \( f \) factors as \( a \cdot c \cdot (g/bc) \), where \( (g/bc) \) is non-constant and \( ac \) is a unit only if \( a = c = 1 \).

**Remark 2**

(i) Every non-zero polynomial \( f \in \mathbb{Q}[x] \) can be written in a unique way up to the sign of \( a \) and the signs and indexing of the \( g_i \) as

\[
f(x) = \frac{a}{b} \prod_{i \in I} g_i(x),
\]

with \( g_i \) primitive and irreducible in \( \mathbb{Z}[x] \) for \( i \in I \) (a finite set) and \( a \in \mathbb{Z}, b \in \mathbb{N} \) with \( \gcd(a, b) = 1 \).

(ii) A non-constant polynomial \( f \in \text{Int}(\mathbb{Z}) \) expressed as in (i) is irreducible in \( \text{Int}(\mathbb{Z}) \) if and only if \( a = \pm 1, b = \text{d}(\prod_{i \in I} g_i), \) and there do not exist \( \emptyset \neq J \subseteq I \) and \( b_1, b_2 \in \mathbb{N} \) with \( b_1 b_2 = b \) and \( b_1 = \text{d}(\prod_{i \in J} g_i), b_2 = \text{d}(\prod_{i \in I \setminus J} g_i) \).

(iii) \( \text{Int}(\mathbb{Z}) \) is atomic.

(iv) Every non-zero non-unit \( f \in \text{Int}(\mathbb{Z}) \) has only finitely many factorizations into irreducibles in \( \text{Int}(\mathbb{Z}) \).

**Proof**

Ad (ii). If \( f \) is irreducible, the conditions on \( f \) follow from Remark 1 (ii) and (iii). Conversely, if the conditions hold, what chance does \( f \) have to be reducible? By Remark 1 (ii), we cannot factor out a non-unit constant, because no proper multiple of \( b \) divides \( \text{d}(\prod_{i \in I} g_i) \). Any non-constant irreducible factor would, by Remark 1 (iii), be of the kind \( (\prod_{i \in J} g_i)/b_1 \) with \( b_1 = \text{d}(\prod_{i \in I \setminus J} g_i) \), and its co-factor would be \( (\prod_{i \in I \setminus J} g_i)/b_2 \) with \( b_1 b_2 = b \) and \( b_2 = \text{d}(\prod_{i \in I \setminus J} g_i) \). Also, \( b_2 \) could not be a proper divisor of \( \text{d}(\prod_{i \in I \setminus J} g_i) \), because otherwise \( b_1 b_2 = b \) would be a proper divisor of \( \prod_{i \in I} g_i \). So, the existence of a non-constant irreducible factor would imply the existence of \( J \) and \( b_1, b_2 \) of the kind we have excluded.

Ad (iii). With \( f(x) = a g(x)/b, g = \prod_{i \in I} g_i \) as in (i), \( \text{d}(g) = cb \) for some \( c \in \mathbb{N} \), and \( f(x) = ac g(x)/d(g) \) with \( g(x)/d(g) \in \text{Int}(\mathbb{Z}) \). We can factor \( ac \) into irreducibles in \( \mathbb{Z} \), which are also irreducible in \( \text{Int}(\mathbb{Z}) \). Either \( g(x)/d(g) \) is irreducible, or (ii) gives
an expression as a product of two non-constant factors of smaller degree. By iteration we arrive at a factorization of \( g(x)/d(g) \) into irreducibles.

Ad (iv). Let \( f \in \text{Int}(\mathbb{Z}) = (a(g(x))/b) \) with \( g = \prod_{i \in I} g_i \) as in (i). Then all factorizations of \( f \) are of the form, for some \( c \in \mathbb{N} \) such that \( bc \) divides \( d(g) \),

\[
f = a_1 \ldots a_n c_1 \ldots c_m \prod_{j=1}^{k} \frac{\prod_{i \in I_j} g_i}{d_j},
\]

where \( a = a_1 \ldots a_n \) and \( c = c_1 \ldots c_m \) are factorizations into primes in \( \mathbb{Z} \), \( I = I_1 \cup \ldots \cup I_k \) is a partition of \( I \) into non-empty sets, \( d_1 \ldots d_k = bc \), \( d_j = d(\prod_{i \in I_j} g_i) \). There are only finitely many such expressions. \( \square \)

Remark 3 (i) The binomial polynomials

\[
\binom{x}{n} = \frac{x(x-1)\ldots(x-n+1)}{n!} \quad \text{for } n \geq 0
\]

are a basis of \( \text{Int}(\mathbb{Z}) \) as a free \( \mathbb{Z} \)-module.

(ii) \( n! f \in \mathbb{Z}[x] \) for every \( f \in \text{Int}(\mathbb{Z}) \) of degree at most \( n \).

(iii) Let \( f \in \mathbb{Z}[x] \) primitive, \( \deg f = n \) and \( p \) prime. Then

\[
v_p(d(f)) \leq \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = v_p(n!).
\]

In particular, if \( p \) divides \( d(f) \) then \( p \leq \deg f \).

Proof Ad (i). The binomial polynomials are in \( \text{Int}(\mathbb{Z}) \) and they form a \( \mathbb{Q} \)-basis of \( \mathbb{Q}[x] \). If a polynomial in \( \text{Int}(\mathbb{Z}) \) is written as a \( \mathbb{Q} \)-linear combination of binomial polynomials then an easy induction shows that the coefficients must be integers. (ii) follows from (i).

Ad (iii). Let \( g = f/d(f) \). Then \( g \in \text{Int}(\mathbb{Z}) \) and \( d(f)\mathbb{Z} = (\mathbb{Z}[x] : \mathbb{Z} g) \). Since \( n! \in (\mathbb{Z}[x] : \mathbb{Z} g) \) by (ii), \( d(f) \) divides \( n! \) \( \square \)

3 Useful Lemmata

Lemma 4 Let \( p \) be a prime, \( I \neq \emptyset \) a finite set and for \( i \in I \), \( f_i \in \mathbb{Z}[x] \) primitive and irreducible in \( \mathbb{Z}[x] \) such that \( d(\prod_{i \in I} f_i) = p \). Let

\[
g(x) = \frac{\prod_{i \in I} f_i}{p}.
\]

Then every factorization of \( g \) in \( \text{Int}(\mathbb{Z}) \) is essentially the same as one of the following:

\[
g(x) = \frac{\prod_{j \in J} f_j}{p} \cdot \prod_{i \in I \setminus J} f_i,
\]

where \( J \subseteq I \) is minimal such that \( d(\prod_{i \in J} f_j) = p \).
Proof Follows from Remark 1 (iii) and the fact that \( d(f) d(h) \) divides \( d(fh) \) for all \( f, h \in \mathbb{Z}[x] \).

The following two easy lemmata are constructive, since the Euclidean algorithm makes the Chinese Remainder Theorem in \( \mathbb{Z} \) effective.

**Lemma 5** For every prime \( p \in \mathbb{Z} \), we can construct a complete system of residues mod \( p \) that does not contain a complete system of residues modulo any other prime.

**Proof** By the Chinese Remainder Theorem we solve, for each \( k = 1, \ldots, p \) the system of congruences \( s_k \equiv k \pmod{p} \) and \( s_k \equiv 1 \pmod{q} \) for every prime \( q < p \).

**Lemma 6** Given finitely many non-constant monic polynomials \( f_i \in \mathbb{Z}[x], i \in I \), we can construct monic irreducible polynomials \( F_i \in \mathbb{Z}[x] \), pairwise non-associated in \( \mathbb{Q}[x] \), with \( \deg F_i = \deg f_i \), and with the following property:

Whenever we replace some of the \( f_i \) by the corresponding \( F_i \), setting \( g_i = F_i \) for \( i \in J \) (\( J \) an arbitrary subset of \( I \)) and \( g_i = f_i \) for \( i \in I \setminus J \), then for all \( K \subseteq I \),

\[
\text{d}\left( \prod_{i \in K} g_i \right) = \text{d}\left( \prod_{i \in K} f_i \right).
\]

**Proof** Let \( n = \sum_{i \in I} \deg f_i \). Let \( p_1, \ldots, p_s \) be all the primes with \( p_i \leq n \), and set \( \alpha_i = v_{p_i}(n!) \). Let \( q > n \) be a prime. For each \( i \in I \), we find by the Chinese Remainder Theorem the coefficients of a polynomial \( \varphi_i \in (\prod_{k=1}^s p_k^{\alpha_k})\mathbb{Z}[x] \) of smaller degree than \( f_i \), such that \( F_i = f_i + \varphi_i \) satisfies Eisenstein’s irreducibility criterion with respect to the prime \( q \). Then, with respect to some linear ordering of \( I \), if \( F_i \) happens to be associated in \( \mathbb{Q}[x] \) to any \( F_j \) of smaller index, we add a suitable non-zero integer divisible by \( q^2 \prod_{k=1}^s p_k^{\alpha_k} \) to \( F_i \), to make \( F_i \) non-associated in \( \mathbb{Q}[x] \) to all \( F_j \) of smaller index.

The statement about the fixed divisor follows, because for every \( c \in \mathbb{Z} \) and every prime \( p_i \) that could conceivably divide the fixed divisor,

\[
\prod_{i \in K} (g_i(c)) \equiv \prod_{i \in K} (f_i(c)) \pmod{p_i^{\alpha_i}},
\]

where \( p_i^{\alpha_i} \) is the highest power of \( p_i \) that can divide the fixed divisor of any monic polynomial of degree at most \( n \).

**4 Constructing polynomials with prescribed sets of lengths**

We precede the general construction by two illustrative examples of special cases, corresponding to previous results by Cahen, Chabert, Chapman and McClain.

**Example 7** For every \( n \geq 0 \), we can construct \( H \in \text{Int}(\mathbb{Z}) \) such that \( H \) has exactly two essentially different factorizations in \( \text{Int}(\mathbb{Z}) \), one of length 2 and one of length \( n + 2 \).
Proof Let $p > n + 1$, $p$ prime. By Lemma 5 we construct a complete set $a_1, \ldots, a_p$ of residues mod $p$ in $\mathbb{Z}$ that does not contain a complete set of residues mod any prime $q < p$. Let

$$f(x) = (x - a_2)(x - a_3) \ldots (x - a_p) \quad \text{and} \quad g(x) = (x - a_{n + 2})(x - a_{n + 3}) \ldots (x - a_p).$$

By Lemma 6, we construct monic irreducible polynomials $F, G \in \mathbb{Z}[x]$, not associated in $\mathbb{Q}[x]$, with $\deg F = \deg f$, $\deg G = \deg g$, such that any product of a selection of polynomials from $(x - a_1), \ldots, (x - a_{n + 1})$. $f(x), g(x)$ has the same fixed divisor as the corresponding product with $f$ replaced by $F$ and $g$ by $G$.

Let

$$H(x) = \frac{F(x)(x - a_1) \ldots (x - a_{n + 1})G(x)}{p}.$$ 

By Lemma 4, $H$ factors into two irreducible polynomials in $\text{Int}(\mathbb{Z})$

$$H(x) = F(x) \cdot \frac{(x - a_1) \ldots (x - a_{n + 1})G(x)}{p}$$

or into $n + 2$ irreducible polynomials in $\text{Int}(\mathbb{Z})$

$$H(x) = \frac{F(x)(x - a_1)}{p} \cdot (x - a_2)(x - a_3) \ldots (x - a_{n + 1})G(x).$$

\[\Box\]

Corollary (Cahen and Chabert [1]) $\rho(\text{Int}(\mathbb{Z})) = \infty$.

Example 8 For $1 \leq m \leq n$, we can construct a polynomial $H \in \text{Int}(\mathbb{Z})$ that has in $\text{Int}(\mathbb{Z})$ a factorization into $m + 1$ irreducibles and an essentially different factorization into $n + 1$ irreducibles, and no other essentially different factorization.

Proof Let $p > mn$ be prime, $s = p - mn$. By Lemma 5 we construct a complete system of residues $R$ mod $p$ that does not contain a complete system of residues for any prime $q < p$. We index $R$ as follows:

$$R = \{r(i, j) \mid 1 \leq i \leq m, 1 \leq j \leq n\} \cup \{b_1, \ldots, b_s\}.$$ 

Let $b(x) = \prod_{k=1}^{s}(x - b_k)$. For $1 \leq i \leq m$ let $f_i(x) = \prod_{k=1}^{n}(x - r(i, k))$ and for $1 \leq j \leq n$ let $g_j(x) = \prod_{k=1}^{m}(x - r(k, j))$.

By Lemma 6, we construct monic irreducible polynomials $F_i, G_j \in \mathbb{Z}[x]$, pairwise non-associated in $\mathbb{Q}[x]$, such that the product of any selection of the polynomials $(x - b_1), \ldots, (x - b_s), f_1, \ldots, f_m, g_1, \ldots, g_n$ has the same fixed divisor as the corresponding product in which $f_i$ has been replaced by $F_i$ and $g_j$ by $G_j$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. Let

$$H(x) = \frac{1}{p} b(x) \prod_{i=1}^{m} F_i(x) \prod_{j=1}^{n} G_j(x).$$
then, by Lemma 4, $H$ has a factorization into $m + 1$ irreducibles

$$H(x) = F_1(x) \cdot \ldots \cdot F_m(x) \cdot \frac{b(x)G_1(x) \cdot \ldots \cdot G_n(x)}{p}$$

and an essentially different factorization into $n + 1$ irreducibles

$$H(x) = \frac{b(x)F_1(x) \cdot \ldots \cdot F_m(x)}{p} \cdot G_1(x) \cdot \ldots \cdot G_n(x)$$

and no other essentially different factorization.

\[ \square \]

**Corollary** (Chapman and McClain [3]) $\text{Int}(\mathbb{Z})$ is fully elastic.

**Theorem 9** Given natural numbers $1 \leq m_1 \leq \ldots \leq m_n$, we can construct a polynomial $H \in \text{Int}(\mathbb{Z})$ that has exactly $n$ essentially different factorizations into irreducibles in $\text{Int}(\mathbb{Z})$, the lengths of these factorizations being $m_1 + 1, \ldots, m_n + 1$.

**Proof** Let $N = \left( \sum_{i=1}^{n} m_i \right)^2 - \sum_{i=1}^{n} m_i^2$, and $p > N$ prime, $s = p - N$. By Lemma 5, we construct a complete system of residues $R \mod p$ that does not contain a complete system of residues for any prime $q < p$. We partition $R$ into disjoint sets $R = R_0 \cup \{t_1, \ldots, t_s\}$ with $|R_0| = N$. The elements of $R_0$ are indexed as follows:

$$R_0 = \{r(k, h, i, j) \mid 1 \leq k \leq n, 1 \leq h \leq m_k, 1 \leq i \leq n, 1 \leq j \leq m_i; i \neq k\},$$

meaning we arrange the elements of $R_0$ in an $m \times m$ matrix with $m = m_1 + \ldots + m_n$, whose rows and columns are partitioned into $n$ blocks of sizes $m_1, \ldots, m_n$. Now $r(k, h, i, j)$ designates the entry in the $h$-th row of the $k$-th block of rows and the $j$-th column of the $i$-th block of columns. Positions in the matrix whose row and column are each in block $i$ are left empty: there are no elements $r(k, h, i, j)$ with $i = k$.

For $1 \leq k \leq n, 1 \leq h \leq m_k$, let $S_{k,h}$ be the set of entries in the $(k, h)$-th row:

$$S_{k,h} = \{r(k, h, i, j) \mid 1 \leq i \leq n, i \neq k, 1 \leq j \leq m_i\}.$$

For $1 \leq i \leq n, 1 \leq j \leq m_i$, let $T_{i,j}$ be the set of elements in the $(i, j)$-th column:

$$T_{i,j} = \{r(k, h, i, j) \mid 1 \leq k \leq n, k \neq i, 1 \leq h \leq m_k\}.$$

For $1 \leq k \leq n, 1 \leq h \leq m_k$, set

$$f_{h}^{(k)}(x) = \prod_{r \in S_{k,h}} (x - r) \cdot \prod_{r \in T_{k,h}} (x - r).$$

Also, let $b(x) = \prod_{i=1}^{s} (x - t_i)$.

By Lemma 6, we construct monic irreducible polynomials $F_{h}^{(k)}$, pairwise non-associated in $\mathbb{Q}[x]$, with $\deg F_{h}^{(k)} = \deg f_{h}^{(k)}$, such that any product of a selection of
polynomials from \((x - t_1), \ldots, (x - t_s)\) and \(f_h^{(k)}\) for \(1 \leq k \leq n, 1 \leq h \leq m_k\) has the same fixed divisor as the corresponding product in which the \(f_h^{(k)}\) have been replaced by the \(F_h^{(k)}\). Let

\[
H(x) = \frac{1}{p} b(x) \prod_{k=1}^{n} \prod_{h=1}^{m_k} F_h^{(k)}(x).
\]

Then \(\deg H = N + p\); and for each \(i = 1, \ldots, n\), \(H\) has a factorization into \(m_i + 1\) irreducible polynomials in \(\text{Int}(\mathbb{Z})\):

\[
H(x) = F_{1}^{(i)}(x) \cdot \ldots \cdot F_{m_i}^{(i)}(x) \cdot \frac{b(x) \prod_{k \neq i} \prod_{h=1}^{m_k} F_h^{(k)}(x)}{p}
\]

These factorizations are essentially different, since the \(F_j^{(i)}\) are pairwise non-associated in \(\mathbb{Q}[x]\) and hence in \(\text{Int}(\mathbb{Z})\).

By Lemma 4, \(H\) has no further essentially different factorizations. This is so because a minimal subset with fixed divisor \(p\) of the polynomials \((x - t_i)\) for \(1 \leq i \leq s\) and \(F_h^{(k)}\) for \(1 \leq k \leq n, 1 \leq h \leq m_k\) must consist of all the linear factors \((x - t_i)\) together with a minimal selection of \(F_h^{(k)}\) such that all \(r \in R_0\) occur as roots in the product of the corresponding \(f_h^{(k)}\). For all linear factors \((x - r)\) with \(r \in R_0\) to occur in a set of polynomials \(f_h^{(k)}\), it must contain for all but one \(k\) all \(f_h^{(k)}, h = 1, \ldots, m_k\). If, for \(i \neq k\), \(f_h^{(k)}\) and \(f_j^{(i)}\) are missing, then \(r(k, h, i, j)\) and \(r(i, j, k, h)\) do not occur among the roots of the polynomials \(f_h^{(k)}\). A set consisting of all \(f_h^{(k)}\) for \(n - 1\) different values of \(k\), however, has the property that all linear factors \((x - r)\) for \(r \in R_0\) occur.

**Corollary** Every finite subset of \(\mathbb{N} \setminus \{1\}\) occurs as the set of lengths of a polynomial \(f \in \text{Int}(\mathbb{Z})\).

### 5 No transfer homomorphism to a block-monoid

For some monoids, results like the above Corollary have been shown by means of transfer-homomorphisms to block monoids. For instance, by Kainrath [6], in the case of a Krull monoid with infinite class group such that every divisor class contains a prime divisor.

\(\text{Int}(\mathbb{Z})\), however, doesn’t admit this method: We will show a property of the multiplicative monoid of \(\text{Int}(\mathbb{Z}) \setminus \{0\}\) that excludes the existence of a transfer-homomorphism to a block monoid.

**Proposition 10** For every \(n \geq 1\) there exist irreducible elements \(H, G_1, \ldots, G_{n+1}\) in \(\text{Int}(\mathbb{Z})\) such that \(xH(x) = G_1(x) \ldots G_{n+1}(x)\).

**Proof** Let \(p_1 < p_2 < \cdots < p_n\) be \(n\) distinct odd primes, \(P = \{p_1, p_2, \ldots, p_n\}\), and \(Q\) the set of all primes \(q \leq p_n + n\). By the Chinese remainder theorem construct
A construction of integer-valued polynomials

\[ a_1, \ldots, a_n \] with \( a_i \equiv 0 \mod p_i \) and \( a_i \equiv 1 \mod q \) for all \( q \in Q \) with \( q \neq p_i \). Similarly, construct \( b_1, \ldots, b_{pn} \) such that, firstly, for all \( p \in P \), \( b_k \equiv k \mod p \) if \( k \leq p \) and \( b_k \equiv 1 \mod q \) if \( k > p \) and, secondly, \( b_k \equiv 1 \mod q \) for all \( q \in Q \setminus P \). So, for each \( p_i \in P \), a complete set of residues mod \( p_i \) is given by \( b_1, \ldots, b_{pi} \), while all remaining \( a_j \) and \( b_k \) are congruent to 1 mod \( p_i \). Also, all \( a_j \) and \( b_k \) are congruent to 1 for all primes in \( Q \setminus P \).

Set \( f(x) = (x - b_1) \ldots (x - b_{pn}) \) and let \( F(x) \) be a monic irreducible polynomial in \( \mathbb{Z}[x] \) with \( \deg F = \deg f \) such that the fixed divisor of any product of a selection of polynomials from \( f(x), (x - a_1), \ldots, (x - a_n) \) is the same as the fixed divisor of the corresponding set of polynomials in which \( f \) has been replaced by \( F \). Such an \( F \) exists by Lemma 6.

Let

\[ H(x) = \frac{F(x)(x - a_1) \ldots (x - a_n)}{p_1 \ldots p_n} \]

Then \( H(x) \) is irreducible in \( \text{Int}(\mathbb{Z}) \), and

\[ xH(x) = \frac{xF(x)}{p_1 \ldots p_n} \cdot (x - a_1) \cdot \ldots \cdot (x - a_n), \]

where \( xF(x)/(p_1 \ldots p_n) \) and, of course, \( (x - a_1), \ldots, (x - a_n) \), are irreducible in \( \text{Int}(\mathbb{Z}) \).

**Remark 11** Thanks to Roger Wiegand for suggesting an easier proof of Proposition 10:

Using the well-known fact that the binomial polynomials \( \binom{x}{m} \) are irreducible in \( \text{Int}(\mathbb{Z}) \) for \( m > 0 \), it suffices to consider

\[ x \left( \frac{x - 1}{m - 1} \right) = m \left( \frac{x}{m} \right) \]

with \( m \) chosen to have exactly \( n \) prime factors in \( \mathbb{Z} \).

**Remark 12** Thanks to Alfred Geroldinger for pointing this out: Proposition 10 implies that there does not exist a transfer-homomorphism from the multiplicative monoid \( (\text{Int}(\mathbb{Z}) \setminus \{0\}, \cdot) \) to a block-monoid. (For the definition of block-monoid and transfer-homomorphism see [5, Def. 2.5.5 and Def. 3.2.1], respectively.)

This is so because, in a block-monoid, the length of factorizations of elements of the form \( cd \) with \( c, d \) irreducible, \( c \) fixed, is bounded by a constant depending only on \( c \), cf. [5, Lemma 6.4.4]. More generally, applying [5, Lemma 3.2.2], one sees that every monoid that admits a transfer-homomorphism to a block-monoid has this property, in marked contrast to Proposition 10.
References

1. Cahen, P.-J., Chabert, J.-L.: Elasticity for integral-valued polynomials. J. Pure Appl. Algebra 103, 303–311 (1995)
2. Cahen, P.-J., Chabert, J.-L.: Integer-valued polynomials. Mathematical Surveys and Monographs, vol. 48. American Mathematical Society, Providence (1997)
3. Chapman, S.T., McClain, B.A.: Irreducible polynomials and full elasticity in rings of integer-valued polynomials. J. Algebra 293, 595–610 (2005)
4. Frei, Ch., Frisch, S.: Non-unique factorization of polynomials over residue class rings of the integers. Commun. Algebra 39, 1482–1490 (2011)
5. Geroldinger, A., Halter-Koch, F.: Non-unique factorizations. Pure and Appl. Mathematics, vol. 278. Chapman & Hall/CRC, Boca Raton (2006)
6. Kainrath, F.: Factorization in Krull monoids with infinite class group. Colloq. Math. 80, 23–30 (1999)