Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 32 (2021) 797–812

indagationes mathematicae

www.elsevier.com/locate/indag

Factorizations of tropical and sign polynomials[☆]

Alexander Agudelo[a], Oliver Lorscheid[b,*]

[a] *Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, Brazil*
[b] *Rijksuniversiteit Groningen, Groningen, The Netherlands*

Received 18 October 2020; received in revised form 13 April 2021; accepted 16 April 2021

Communicated by D. Gijswijt

Abstract

In this text, we study factorizations of polynomials over the tropical hyperfield and the sign hyperfield, which we call *tropical polynomials* and *sign polynomials*, respectively. We classify all irreducible polynomials in either case. We show that tropical polynomials factor uniquely into irreducible factors, but that unique factorization fails for sign polynomials. We describe division algorithms for tropical and sign polynomials by linear terms that correspond to roots of the polynomials.

Keywords: Hyperfields; Factorization into irreducible elements; Division algorithm for polynomials

0. Introduction

Hyperfields were introduced by Marc Krasner in 1956 in his paper [5] as a generalization of fields by allowing the addition to be multi-valued. Since then a considerable amount of literature on hyperfields has built up, but, still, the notion of a hyperfield stayed largely in the shadow of mainstream mathematics until around a decade ago when the works [7] of Viro and [3] of Connes and Consani showed the potential of hyperfields for tropical and arithmetic geometry. More recently, Baker and Bowler have demonstrated in [1] the relevance of hyperfields for matroid theory.

The joint paper [2] of Baker and the second author of this text provides additional evidence for the usefulness of this concept: a study of roots of polynomials, and their multiplicities,

[☆] The authors thank the Max Planck Institute for Mathematics in Bonn that has hosted them during the time of writing this manuscript.

[*] Corresponding author.
E-mail addresses: alagudel@gmail.com (A. Agudelo), oliver@impa.br (O. Lorscheid).

https://doi.org/10.1016/j.indag.2021.04.005
0019-3577/

over hyperfields leads to a simultaneous proof of Newton's polygon rule and Descartes' rule of signs. The hyperfields that underlie these rules are the tropical hyperfield $\mathbb{T}$ and the sign hyperfield $\mathbb{S}$, respectively.

In this paper, we complement the theory from [2] by some results on the factorization of polynomials over $\mathbb{T}$ and $\mathbb{S}$, which we call *tropical polynomials* and *sign polynomials*, respectively. Before we turn to a description of our findings, we introduce the two main actors of our text.

The tropical and the sign hyperfield

Hyperfields generalize fields in the sense that the *hypersum* of elements is a subset rather than an element. The tropical hyperfield $\mathbb{T}$ is the set $\mathbb{R}_{\geqslant 0}$ of non-negative real numbers together with the usual multiplication and with the hyperaddition given as follows: for $a_1, \dots, a_n \in \mathbb{R}_{\geqslant 0}$ and i such that $a_i = \max\{a_1, \dots, a_n\}$, we have

$$a_1 \boxplus \cdots \boxplus a_n \;=\; \begin{cases} \big\{ \max\{a_i\}\big\} & \text{if } a_j < a_i \text{ for all } i \neq j; \\ [0, a_i] & \text{if } a_k \leqslant a_i = a_j \text{ for some } i \neq j \text{ and all } k. \end{cases}$$

The *sign hyperfield* $\mathbb{S}$ is the set $\{0, 1, -1\}$ together with the obvious multiplication and with the following hyperaddition: for $a_1, \dots, a_n \in \mathbb{S}$, we have

$$a_1 \boxplus \cdots \boxplus a_n \;=\; \begin{cases} \{0\} & \text{if } a_1 = \ldots = a_n = 0; \\ \{1\} & \text{if } 1 \in \{a_1, \dots, a_n\} \subset \{0, 1\}; \\ \{-1\} & \text{if } -1 \in \{a_1, \dots, a_n\} \subset \{0, -1\}; \\ \mathbb{S} & \text{if } \{1, -1\} \subset \{a_1, \dots, a_n\}. \end{cases}$$

Factorization of polynomials

Let F be a hyperfield—the reader might want to think of F as one of $\mathbb{T}$ or $\mathbb{S}$. A polynomial (of degree n) over F is an expression $p = c_nT^n + \ldots + c_1T + c_0$ with $c_i \in F$ and $c_n \neq 0$ unless $n = 0$. Given two polynomials $p = \sum c_iT^i$ and $q = \sum d_iT^i$ over F, we define their hyperproduct as the set

$$p \boxdot q \;=\; \Big\{ \sum e_iT^i \,\Big|\, e_i \in \mathop{\boxplus}_{k+l=i} c_kd_l \Big\}$$

of polynomials over F. We define recursively the hyperproduct of n polynomials $q_1, \dots, q_n$ over F as

$$\mathop{\boxdot}_{i=1}^{n} q_i \;=\; \bigcup_{p \in \boxdot_{i=1}^{n-1} q_i} p \boxdot q_n.$$

A polynomial p is *irreducible* if its degree is positive and if for all polynomials q_1 and q_2 such that $p \in q_1 \boxdot q_2$ either q_1 or q_2 is of degree 0. A *quotient of p by q* is a polynomial q' such that $p \in q \boxdot q'$.

A polynomial p has a *unique factorization into irreducibles* if there are irreducible polynomials $q_1, \dots, q_n$ that are unique up to a permutation and up to multiplication by a constant polynomial such that $p \in c \boxdot \boxdot_{i=1}^{n} q_i$ for $c \in F$.

Unique factorization for tropical polynomials and its failure for sign polynomials

Our first result is a classification of all irreducible tropical polynomials and the unique factorization over $\mathbb{T}$. The following is Theorem 3.2.

Theorem A. *The irreducible tropical polynomials are precisely the linear tropical polynomials, and every tropical polynomial has a unique factorization into irreducibles.*

The list of irreducible sign polynomials is as follows, which is Theorem 4.1.

Theorem B. *Up to multiplication by* -1*, the irreducible sign polynomials are* T*,* $T-1$*,* $T+1$ *and* T^2+1*.*

In contrast to tropical polynomials, sign polynomials fail to have unique factorizations in general. For example the sign polynomial T^3+T^2+T+1 is contained in both products

$$(T+1)\boxdot(T+1)\boxdot(T+1) \qquad \text{and} \qquad (T+1)\boxdot(T^2+1);$$

cf. Section 4.2 for more details.

Division algorithms

A fundamental fact that enters the definition of the multiplicity of a root is that if a polynomial p over a hyperfield F has a root $a \in F$, then p is divisible by $T-a$ (cf. [2, Lemma A]). In the case of usual fields, this follows directly from the division algorithm for polynomials. There is a generalization to hyperfields (cf. [4, Thm. 3.4]), but this generalization does not provide an algorithm to compute a quotient of p by $T-a$ due to the ambiguity of the multi-valued addition of the hyperfield. In particular, it happens that there are several such quotients.

In this text, we describe algorithms for the division of tropical and sign polynomials by linear polynomials. These algorithms might be useful for explicit calculations of multiplicities of tropical and sign polynomials, which is of interest for their link to Newton polygons and Descartes' rule of signs.

The division algorithms for tropical polynomials is as follows. Let $p=\sum c_iT^i$ be a tropical polynomial of degree n. By Theorem A, p factors into a unique product $c_n\prod(T+a_i)$ of linear polynomials $T+a_i$ where we assume that $a_1 \leqslant \cdots \leqslant a_n$. It follows from the fundamental theorem for the tropical hyperfield (cf. [2, Theorem 4.1]) that $\{a_1,\dots,a_n\}$ are the roots of p, and that the multiplicity m of a root a of p coincides with the number of a_i's that are equal to a, i.e.

$$a \;=\; a_k \;=\; \dots \;=\; a_{k+m-1}$$

for some $k \in \{1\dots,n-m+1\}$ and $a_{k-1} < a_k$ if $k-1 \geqslant 1$ as well as $a_{k+m-1} < a_{k+m}$ if $k+m \leqslant n$. Since the case $a=0$ is trivial, let us assume that a is not zero. The following is Theorem 3.4.

Theorem C. *Define the tropical numbers* $d_0,\dots,d_{n-1}$ *by the following algorithm.*

(1) *If* $k \leqslant n-m$*, then let* $d_{n-1}=c_n$*. For* $i=n-2,\dots,k+m-1$*, we define (in decreasing order)*

$$d_i \;=\; \max\{c_{i+1},\; ad_{i+1}\}.$$

(2) *If* $k \geqslant 2$, *then let* $d_0 = a^{-1}c_0$. *For* $i = 1, \dots, k-2$, *we define (in increasing order)*

$$d_i \ = \ \max\{a^{-1}c_i,\ a^{-1}d_{i-1}\}.$$

(3) *For* $i = k-1, \dots, k+m-2$, *we define*

$$d_i \ = \ a_{i+2}\cdots a_n c_n.$$

Then the polynomial $q = \sum d_i T^i$ *is a divisor of* p *by* $T + a$.

The division algorithm for sign polynomials can be described more compactly as follows, which is Theorem 4.2.

Theorem D. *Let* $p = \sum c_i T^i$ *be a sign polynomial of degree* n *where* $c_0, \dots, c_n \in \mathbb{S}$. *Let* $a \in \{\pm 1\}$ *be a root of* p. *Define*

$$l \ = \ \min\{\, i \in \mathbb{N} \,|\, c_i \neq 0 \,\} \qquad \text{and} \qquad k \ = \ \min\{\, i \in \mathbb{N} \,|\, c_{i+1} = -a^{i+1-l}c_l \,\}.$$

Define recursively for $i = n-1, \dots, 0$ *(in decreasing order)*

$$\begin{array}{llll} (1) & d_i = c_{i+1} & & \text{if } c_{i+1} \neq 0 \text{ and } i > k; \\ (2) & d_i = a d_{i+1} & & \text{if } c_{i+1} = 0 \text{ and } i > k; \\ (3) & d_i = -a^{i+l-1}c_l & & \text{if } l \leqslant i \leqslant k; \\ (4) & d_i = 0 & & \text{if } 0 \leqslant i < l. \end{array}$$

Then $q = \sum d_i T^i$ *is a quotient of* p *by* $T - a$.

1. Hyperfields

A *hyperfield* is a set F together with a multiplication, i.e. a map $\cdot : F \times F \to F$, and with a *hyperaddition*, which is a map $\boxplus : F \times F \to \mathcal{P}(F)$ where $\mathcal{P}(F)$ is the power set of F, that satisfies the following axioms:

(HF1) There are unique elements 0 and 1 of F such that $(F, \cdot, 1)$ is a commutative monoid and such that $F^\times = F - \{0\}$ is a group with respect to $\cdot$.
(HF2) For all $a, b, c \in F$, we have $a \cdot b \boxplus a \cdot c = \{a \cdot d | d \in b \boxplus c\}$. *(distributive)*
(HF3) $(F \boxplus, 0)$ is a commutative hypergroup, i.e. we have for all $a, b, c \in F$ that

(HG1) $a \boxplus b$ is not empty; *(non-empty sums)*
(HG2) $a \boxplus b = b \boxplus a$; *(commutative)*
(HG3) $a \boxplus 0 = \{a\}$; *(neutral element)*
(HG4) there is a unique $d \in F$ such that $0 \in a \boxplus d$; *(additive inverse)*
(HG5) $\bigcup\{a \boxplus d | d \in b \boxplus c\} = \bigcup\{d \boxplus c | d \in a \boxplus b\}$. *(associative)*

In the following, we write ab for $a \cdot b$ and $-a$ for the additive inverse of a, i.e. $0 \in a \boxplus (-a)$. For $n \geqslant 3$ and $a_1, \dots, a_n \in F$, we define recursively the subset

$$\mathop{\boxplus}_{i=1}^{n} a_i \ = \ \bigcup_{b \in \boxplus_{i=1}^{n-1} a_i} b \boxplus a_n,$$

of F, which does not depend on the order of the a_i thanks to associativity and commutativity.

The axioms of a hyperfield imply that $0 \cdot a = 0$ for all $a \in F$ and that

(HG6) $a \in b \boxplus c$ if and only if $-b \in (-a) \boxplus c$ *(reversibility)*

for all $a, b, c \in F$.

1.1. Examples

A primary example of hyperfields are fields. Namely, given a field K, we can define a hyperaddition $\boxplus$ on K by the rule $a \boxplus b = \{a+b\}$, which turns K into a hyperfield.

To give some examples of hyperfields that do not come from fields, let us introduce the two main characters of our story: the tropical hyperfield $\mathbb{T}$ and the sign hyperfield $\mathbb{S}$.

The *tropical hyperfield* $\mathbb{T}$ is the set $\mathbb{R}_{\geqslant 0}$ of nonnegative real numbers together with their usual multiplication and the hyperaddition defined by the rule

$$a \boxplus b \;=\; \begin{cases} \big\{ \max\{a,b\} \big\} & \text{if } a \neq b; \\ [0,a] & \text{if } a = b. \end{cases}$$

In other words, we have $c \in a \boxplus b$ if and only if the maximum among a, b and c appears twice. Note that $-a = a$ for every $a \in \mathbb{T}$.

The *sign hyperfield* $\mathbb{S}$ is the set $\{0, 1, -1\}$ together with the obvious multiplication and with the hyperaddition given by the table

$\boxplus$	0	1	−1
0	{0}	{1}	{−1}
1	{1}	{1}	{0, 1, −1}
−1	{−1}	{0, 1, −1}	{−1}

1.2. Morphisms of hyperfields

A *morphism between hyperfields* F_1 *and* F_2 is a map $f : F_1 \to F_2$ such that $f(0) = 0$, $f(1) = 1$, $f(ab) = f(a)f(b)$ and $f(a \boxplus b) \subset f(a) \boxplus f(b)$ for all $a, b \in F_1$. Note that the latter property is equivalent with requiring that whenever $b \in \boxplus a_i$ in F_1, then $f(b) \in \boxplus f(a_i)$ in F_2.

Let us describe the two examples of morphisms of hyperfields that are of interest for our purpose. The first example is that of the sign map sign : $\mathbb{R} \to \mathbb{S}$ that associates with a nonzero real number $a \in \mathbb{R}$ its sign $\operatorname{sign}(a) = a/|a|$ and that maps 0 to 0.

The second example is based on a general fact observed by Viro in [7]. Namely, by identifying a field K with its associated hyperfield and the nonnegative real numbers $\mathbb{R}_{\geqslant 0}$ with the tropical hyperfield $\mathbb{T}$ as sets, a nonarchimedean absolute value $v : K \to \mathbb{R}_{\geqslant 0}$ is the same as a morphism of hyperfields $v : K \to \mathbb{T}$.

2. Polynomials over hyperfields

A *polynomial over a hyperfield* F is an expression of the form $p = c_n T^n + \cdots + c_1 T + c_0$ with $c_0, \ldots, c_n \in F$, or, more formally, a sequence $(c_i)_{i \in \mathbb{N}}$ of elements $c_i \in F$ for which $\{i \in \mathbb{N} | c_i \neq 0\}$ is finite. We denote the set of all polynomials over F by $\operatorname{Poly}(F)$.

Note that for a field K, $\operatorname{Poly}(K)$ is equal to the usual polynomial algebra $K[T]$. For reasons explained in [2, Appendix A], we refrain from the notation $F[T]$ for the set $\operatorname{Poly}(F)$ of polynomials over a hyperfield F.

We will identify elements a of F with the constant polynomial $p = a$ over F. In particular, we write 0 for the zero polynomial $p = 0$ and 1 for the constant polynomial $p = 1$.

2.1. Hyperproducts

The multiplication and hyperaddition of a hyperfield F endows the set $\mathrm{Poly}(F)$ of polynomials over F with an additive and a multiplicative structure. The additive structure is the hyperaddition on $\mathrm{Poly}(F)$ that results from the hyperaddition of coefficients, which might not come as a surprise. Since the hyperaddition of polynomials is not of interest for our present purpose, we omit a discussion, but refer the reader to [2, Appendix A] for details.

The multiplicative structure of $\mathrm{Poly}(F)$ is the *hypermultiplication*

$$\boxdot \; : \; \mathrm{Poly}(F) \times \mathrm{Poly}(F) \quad \longrightarrow \quad \mathcal{P}\big(\mathrm{Poly}(F)\big)$$

that maps a pair of polynomials $p = \sum c_i T^i$ and $q = \sum d_i T^i$ to the subset

$$p \boxdot q \;=\; \Big\{ \sum e_i T^i \,\Big|\, e_i \in \mathop{\boxplus}_{k+l=i} c_k d_l \Big\}$$

of $\mathrm{Poly}(F)$. Note that in the case of a hyperfield coming from a field F, $p \boxdot q = \{pq\}$ is the singleton containing the usual product of p and q.

It is easily verified that this hypermultiplication satisfies the following properties in analogy to that of a hyperaddition (cf. (HG1)–(HG3) in Section 1): for all $p, q \in \mathrm{Poly}(F)$, we have

(HM1) $p \boxdot q$ is not empty; *(non-empty sums)*
(HM2) $p \boxdot q = q \boxdot p$; *(commutative)*
(HM3) $p \boxdot 1 = \{p\}$. *(neutral element)*

Similar as for the hyperaddition of a hyperfield, we extend $\boxdot$ recursively to n-fold products by the rule

$$\mathop{\boxdot}_{i=1}^{n} q_i \;=\; \bigcup_{p \in \boxdot_{i=1}^{n-1} q_i} p \boxdot q_n.$$

Note that the definition of the n-fold product depends on the order of the factors in general since, in contrast to the situation over a field, $\boxdot$ fails to be associative for some hyperfields. This is, in particular, the case for $\mathrm{Poly}(\mathbb{T})$ and $\mathrm{Poly}(\mathbb{S})$, as shown in [6].

2.2. The degree

The *degree* of a polynomial $p = c_n T^n + \cdots + c_0$ over a hyperfield F is the largest $k \in \mathbb{N}$ such that $c_k \neq 0$, which we denote by $\deg p$.

For n polynomials $q_1, \dots, q_n$, we have $\deg p = \sum \deg q_i$ for every $p \in \boxdot q_i$. In so far, $1 \in p \boxdot q$ implies that $\deg p = \deg q = 0$ and thus $p = a$ and $q = a^{-1}$ for some $a \in F^\times$. For every $p = \sum c_n T^i$, we have $p \boxdot a T^k = \big\{\sum a c_i T^{i+k}\big\}$ and, in particular, $p \boxdot 0 = \{0\}$. We write $-p$ for the unique element $\sum (-c_n) T^n$ in $(-1) \boxdot p$.

2.3. Factorizations

We say that p and q are *associated*, and write $p \sim q$, if $p \in a \boxdot q$ for some $a \in F^\times$. Note that $\sim$ is an equivalence relation. A polynomial p is *monic* if $c_{\deg p} = 1$. We conclude that for every nonzero polynomial p there is a unique monic polynomial q with $p \sim q$.

Let $p, q_1, \dots, q_n \in \mathrm{Poly}(F)$ be polynomials over F. We say that *p factors into the product of $q_1, \dots, q_n$* if $p \in \boxdot q_i$.

We can extend a morphism $f : F_1 \to F_2$ to a map $f : \mathrm{Poly}(F_1) \to \mathrm{Poly}(F_2)$ between polynomials: given a polynomial $p = \sum c_i T^i$ over F_1, we define $f(p) = \sum f(c_i)T^i$.

Lemma 2.1. *Let $f : F_1 \to F_2$ be a morphism of hyperfields, $n \geqslant 2$ and $p, q_1, \dots, q_n \in \mathrm{Poly}(F_1)$ such that $p \in \boxdot\, q_i$. Then $f(p) \in \boxdot\, f(q_i)$.*

Proof. Let $p = \sum c_j T^j$ and $q_i = \sum d_{i,j} T^j$. We prove the claim by induction on $n \geqslant 2$.

If $n = 2$, then $p \in q_1 \boxdot q_2$ means that $c_i \in \boxplus_{k+l=i} d_{1,k} d_{2,l}$ in F_1. Since f is a morphism of hyperfields, we have $f(c_i) \in \boxplus_{k+l=i} f(d_{1,k}) f(d_{2,l})$ in F_2, and thus $f(p) \in f(q_1) \boxdot f(q_2)$ as claimed.

If $n > 2$, then $r \in \boxdot_{i=1}^{n-1} q_i$ and the inductive hypothesis imply that $f(r) \in \boxdot_{i=1}^{n-1} f(q_i)$. This and the case $n = 2$ show that $p \in \boxdot\, q_i$ implies that

$$f(p) \in f\Big(\bigcup_{r\in \boxdot_{i=1}^{n-1} q_i} r \boxdot q_n\Big) = \bigcup_{r\in \boxdot_{i=1}^{n-1} q_i} f\big(r \boxdot q_n\big) \subset \bigcup_{f(r)\in \boxdot_{i=1}^{n-1} f(q_i)} f(r) \boxdot f(q_n),$$

which establishes the claim of the lemma. □

2.4. Irreducible polynomials

We say that a polynomial $p = \sum c_i T^i$ over a hyperfield F is *irreducible* if $\deg p \geqslant 1$ and if for every factorization $p \in q_1 \boxdot q_2$, we have $p \sim q_1$ or $p \sim q_2$. Note that if $p \sim q$, then p is irreducible if and only if q is irreducible.

Since $p \in q_1 \boxdot q_2$ implies $\deg p = \deg q_1 + \deg q_2$, we have $p \sim q_1$ if and only if $\deg p = \deg q_1$, or if, equivalently, $q_2 = c_0 \in F^\times$ is a constant nonzero polynomial. It follows that every linear polynomial $p = c_1 T + c_0$ (with $c_1 \neq 0$) is irreducible. In Lemma 2.6, we give an irreducibility criterion for quadratic and cubic polynomials.

The following fact was pointed out to us by Trevor Gunn.

Lemma 2.2. *Let $p \in \mathrm{Poly}(F)$ be irreducible, $n \geqslant 2$ and $p \in \boxdot_{i=1}^{n} q_i$ a factorization. Then there is an $i \in \{1, \dots, n\}$ such that $p \sim q_i$.*

Proof. We prove the claim by induction on n. The case $n = 2$ follows by the definition of irreducibility.

Assume that $n > 2$. By the definition of $\boxdot_{i=1}^{n} q_i$, there is an r in $\boxdot_{i=1}^{n-1} q_i$ such that $p \in r \boxdot q_n$. Since p is irreducible, we have $p \sim r$ or $p \sim q_n$. If $p \sim q_n$, then there is nothing to prove. If $p \sim r$, then r is also irreducible. By the inductive hypothesis, applied to r, we have $p \sim r \sim q_i$ for some $i \in \{1, \dots, n-1\}$, which completes the proof of the lemma. □

We say that $\mathrm{Poly}(F)$ *has the unique factorization property* if for any two factorizations $p \in q_1 \boxdot \cdots \boxdot q_n$ and $p \in q'_1 \boxdot \cdots \boxdot q'_m$ into irreducible factors $q_1, \dots, q_n, q'_1, \dots, q'_m$, we have $n = m$ and $q_i \sim q'_{\sigma(i)}$ for some permutation σ of $\{1, \dots, n\}$.

We conclude with the following implication of unique factorization on a weakened form of associativity. By definition, we have $p \boxdot q \boxdot r = (p \boxdot q) \boxdot r$. In contrast, $p \boxdot (q \boxdot r)$ must be read as $\bigcup\{p \boxdot s | s \in q \boxdot r\}$.

Lemma 2.3. *If $\mathrm{Poly}(F)$ has the unique factorization property, then $(p \boxdot q) \boxdot r = p \boxdot (q \boxdot r)$ for all irreducible $p, q, r \in \mathrm{Poly}(F)$.*

Proof. Let $p, q, r \in \mathrm{Poly}(F)$ irreducible polynomials. Since $\mathrm{Poly}(F)$ has the unique factorization property, we have $s \in (p \boxdot q) \boxdot r$ if and only if $s \in (q \boxdot r) \boxdot p$. Using the commutativity of $\boxdot$, we find the desired equality $(p \boxdot q) \boxdot r = (q \boxdot r) \boxdot p = p \boxdot (q \boxdot r)$. □

2.5. Roots

Let $a \in F$ and $p = \sum c_i T^i$ be a polynomial over a hyperfield F. We say that *a is a root of p*, and write $0 \in p(a)$, if $0 \in \boxplus c_i a^i$. Alternatively, we can characterize roots in terms of the following fact, which is Lemma A in [2].

Lemma 2.4. *Let $a \in F$ and $p \in \mathrm{Poly}(F)$. Then $0 \in p(a)$ if and only if there exists a $q \in \mathrm{Poly}(F)$ such that $p \in (T - a) \boxdot q$.*

Note that if $p = \sum c_i T^i$ and $q = \sum d_i T^i$, then the relation $p \in (T - a) \boxdot q$ is equivalent with $n = \deg p = 1 + \deg q$ and the relations

$$c_0 = -ad_0, \quad c_i \in (-ad_i) \boxplus d_{i-1} \quad \text{for } i = 1, \dots, n-1, \quad \text{and} \quad c_n = d_{n-1}.$$

Example 2.5. In the case of a field K, we have $0 \in p(a)$ in the hyperfield sense if and only if $0 = p(a)$ in the usual sense, and we have $p \in (T - a) \boxdot q$ in the hyperfield sense if and only if $p = (T - a)q$ in the usual sense.

As an immediate consequence of Lemma 2.4, we see that an irreducible polynomial of degree at least 2 cannot have any roots. For quadratic and cubic polynomials, this implication can be reversed.

Lemma 2.6. *Let p be a polynomial over F of degree 2 or 3. Then p is irreducible if and only if p does not have a root in F.*

Proof. As noted before, if p is irreducible, it cannot have any roots. If p is not irreducible, then $p \in q_1 \boxdot q_2$ for a linear polynomial q_1 and polynomial q_2 of degree 1 or 2. After multiplying q_2 with the leading coefficient d_1 of q_1, and q_1 by its inverse d_1^{-1}, we can assume that q_1 is of the form $T - a$. Thus we have $p \in (T - a) \boxdot q_2$, i.e. a is a root of p by Lemma 2.4. □

2.6. A non-deterministic division algorithm

As explained in [4, Thm. 3.4], polynomials over hyperfields admit an Euclidean algorithm that is based on non-deterministic choices in each step. In this section, we include an independent treatment of this algorithm in the case of the division of a polynomial p by a linear term. We will improve on this in the cases of the tropical hyperfield and the sign hyperfield in Sections 3 and 4, respectively, which allow for deterministic choices.

Let F be a hyperfield, $a \in F$ and $p = \sum c_i T^i$ a polynomial of degree n. Define $D_n = \{0\}$ and for decreasing $i = n-1, \dots, -1$, the subsets $D_i = c_{i+1} \boxplus aD_{i+1}$.

Lemma 2.7. *For every $i \in \{-1, \dots, n\}$, we have*

$$D_i = \boxplus_{k=i+1}^{n} c_k a^{k-i-1}.$$

Proof. We prove this by induction on $i = n, \dots, -1$. The result follows for $i = n$ by the definition of the empty hypersum as $\{0\}$. If $i < n$, then we have

$$\begin{aligned} D_i &= c_{i+1} \boxplus aD_{i+1} \\ &= c_{i+1} \boxplus a \cdot \mathop{\boxplus}\limits_{k=i+2}^{n} c_k a^{k-(i+1)-1} \\ &= c_{i+1} a^{i+1-i-1} \boxplus \mathop{\boxplus}\limits_{k=i+2}^{n} c_k a^{k-i-1} = \mathop{\boxplus}\limits_{k=i+1}^{n} c_k a^{k-i-1}, \end{aligned}$$

as claimed. □

Corollary 2.8. *The element a is a root of p if and only if $0 \in D_{-1}$.*

Proof. By Lemma 2.7, we have $D_{-1} = \boxplus_{k=0}^{n} c_k a^{k-(-1)-1} = p(a)$, and thus $0 \in D_{-1} = p(a)$ if and only if a is a root of p. □

Proposition 2.9. *Let $a \in F$ be a root of $p = \sum c_i T^i$ and let $D_{-1}, \dots, D_n$ be as before. Then for every $i = -1, \dots, n-2$ and every $d_i \in D_i$, there is a $d_{i+1} \in D_{i+1}$ such that $c_{i+1} \in d_i \boxplus (-ad_{i+1})$. Moreover, if $d_{-1} = 0$, then $d_0 = -a^{-1} c_0$ and $p \in (T-a)q$ for $q = \sum_{i=0}^{n-1} d_i T^i$.*

Proof. By the definition of D_i as $c_{i+1} \boxplus aD_{i+1}$, there is for every $d_i \in D_i$ a $d_{i+1} \in D_{i+1}$ such that $d_i \in c_{i+1} \boxplus ad_{i+1}$, or, equivalently, $c_{i+1} \in d_i \boxplus (-ad_{i+1})$, which proves the first assertion.

If $d_{-1} = 0$, then $c_0 \in 0 \boxplus (-ad_0)$ if and only if $d_0 = -a^{-1}c_0$. By definition, we have $D_{n-1} = c_n \boxplus aD_n = \{c_n\}$ and thus $d_{n-1} = c_n$. Summing up, these relations show that $q = \sum d_i T^i$ divides p, i.e. $p \in (T-a)q$. □

3. Factorizations of tropical polynomials

A *tropical polynomial* is a polynomial over the tropical hyperfield $\mathbb{T}$. In this section, we use the fundamental theorem for the tropical hyperfield to establish the unique factorization of tropical polynomials into linear polynomials, and we describe a division algorithm.

3.1. Unique factorization for tropical polynomials

The fact that every polynomial function on the tropical line is piecewise linear can be expressed by saying that every polynomial function over the tropical numbers factors uniquely into linear functions. This is sometimes called the *fundamental theorem of tropical algebra.*

This result is reflected by the following variant for the tropical hyperfield, which we call the *fundamental theorem for the tropical hyperfield.*

Let $p = \sum c_i T^i$ be a monic polynomial of degree n over $\mathbb{T}$ and let $a_1, \dots, a_n \in \mathbb{T}$. Then we have

$$p \in \mathop{\boxdot}\limits_{i=1}^{n} (T + a_i) \quad \text{if and only if} \quad c_i \in \mathop{\boxplus}\limits_{e_{i+1} < \cdots < e_n} a_{e_{i+1}} \cdots a_{e_n} \quad \text{for all } i = 0, \dots, n-1.$$

If $a_1 \leqslant \cdots \leqslant a_n$, then this is equivalent to the conditions that $c_i \leqslant a_{i+1} \cdots a_n$ for all $i = 0, \dots, n-1$, with equality holding if $a_i < a_{i+1}$. The following is Theorem 4.1 in [2].

Theorem 3.1 (*Fundamental Theorem for the Tropical Hyperfield*)**.** *Let $p = \sum_{i=0}^{n} c_i T^i$ be a monic polynomial of degree n over $\mathbb{T}$. Then there is a unique sequence $a_1, \dots, a_n \in \mathbb{T}$ with $a_1 \leqslant \cdots \leqslant a_n$ such that $p \in \boxdot\,(T+a_i)$, and $a \in \mathbb{T}$ is a root of p if and only if $a \in \{a_1, \dots, a_n\}$.*

In addition, [2, Thm. 4.1] provides an effective way to compute the tropical numbers $a_1, \dots, a_n$: they correspond to the slopes of the linear segments of the Newton polygon of p; cf. Section 3.3 for an example. This allows us to formulate a division algorithm for tropical polynomials in Section 3.2.

A direct consequence of Theorem 3.1 is the unique factorization of tropical polynomials.

Theorem 3.2. *The irreducible tropical polynomials are precisely the linear tropical polynomials, and* Poly($\mathbb{T}$) *has the unique factorization property.*

Remark 3.3. Using the methods of this text, we find the following short argument to prove the fact that every irreducible tropical polynomial is linear. Namely, consider a surjective morphism $v : K \to \mathbb{T}$ from an algebraically closed field K to $\mathbb{T}$. For example, we could take the (exponential) valuation $v_p : \mathbb{C}\{T\} \to \mathbb{T}$ of the field of Puiseux series $K = \mathbb{C}\{T\}$ over $\mathbb{C}$ with real exponents.

For an irreducible tropical polynomial $p = \sum c_i T^i$, we choose elements $\hat{c}_i \in K$ with $v(\hat{c}_i) = c_i$. By Lemma 2.1, the polynomial $\hat{p} = \sum \hat{c}_i T^i$ is irreducible over K. Since K is algebraically closed, $\hat{p}$ is linear, and so is $p = v(\hat{p})$.

3.2. A division algorithm for tropical polynomials

While it is a direct calculation to verify whether $0 \in p(a)$ for an element a of $\mathbb{T}$ and a tropical polynomial p, it is not so clear how to find a $q \in \text{Poly}(F)$ that satisfies $p \in (T-a) \boxdot q$, which exists by Lemma 2.4. In the case of a field K, this can be done using the usual division algorithm for polynomials over K. For the tropical hyperfield, there is a similar, but slightly more involved, algorithm, which we describe in the following.

Let $p = \sum c_i T^i$ be a polynomial of degree n over $\mathbb{T}$. By Theorem 3.1, there is a unique sequence $a_1 \leqslant \cdots \leqslant a_n$ of tropical numbers such that $c_n^{-1} p \in \boxdot\,(T + a_i)$. Since the roots of $c_n^{-1} p$ are the same as the roots of p, we conclude that the roots of p are $a_1, \dots, a_n$, counted with multiplicities. Fix a root $a \in \{a_1, \dots, a_n\}$ of multiplicity m, i.e.

$$a \;=\; a_k \;=\; \dots \;=\; a_{k+m-1}$$

for some $k \in \{1 \dots, n-m+1\}$ and $a_{k-1} < a_k$ if $k \geqslant 2$ as well as $a_{k+m-1} < a_{k+m}$ if $k \leqslant n-m$. If $a = 0$, then $c_0 = 0$ and $q = \sum_{i=0}^{n-1} c_{i+1} T^i$ is the unique polynomial such that $p \in (T-0) \boxdot q$.

Thus let us assume from here on that a is not zero. We can determine a polynomial $q = \sum d_i T^i$ of degree $n-1$ with $p \in (T+a) \boxdot q$ by the following recursive definition.

(1) If $k \leqslant n-m$, then let $d_{n-1} = c_n$. For $i = n-2, \dots, k+m-1$, we define (in decreasing order)

$$d_i \;=\; \max\{c_{i+1},\, a d_{i+1}\}.$$

(2) If $k \geqslant 2$, then let $d_0 = a^{-1} c_0$. For $i = 1, \dots, k-2$, we define (in increasing order)

$$d_i \;=\; \max\{a^{-1} c_i,\, a^{-1} d_{i-1}\}.$$

(3) For $i = k-1, \dots, k+m-2$, we define

$$d_i \;=\; a_{i+2} \cdots a_n c_n.$$

Theorem 3.4. *If $a \neq 0$ is a root of p, then the polynomial $q = \sum d_i T^i$ as defined above satisfies $p \in (T+a) \boxdot q$, i.e.*

$$c_n = d_{n-1}, \qquad c_0 = ad_0 \qquad \text{and} \qquad c_i \in (ad_i) \boxplus d_{i-1} \qquad \text{for} \qquad i = 1, \dots, n-1.$$

Remark 3.5. The recursion in step (1) stays in a direct analogy to the division algorithm for polynomials over a field, which is given by the formulas $d_{n-1} = c_n$ and $d_i = c_{i+1} + ad_{i+1}$ where i decreases from $n-2$ to 0. In the tropical setting, step (1) of the algorithm fails in general to provide the required result if used to define all coefficients of q, cf. Section 3.3. To achieve $p \in (T+a) \boxdot q$, one needs to define the coefficients d_i for smaller i in terms of step (2).

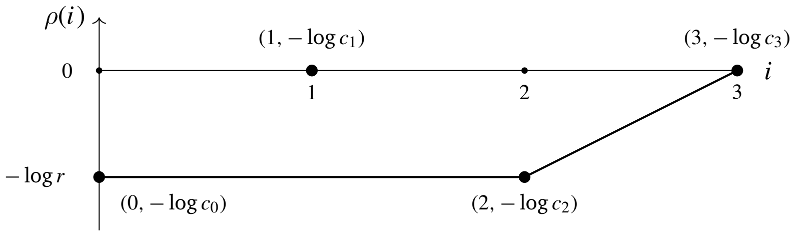
In contrast, the coefficients d_i occurring in step (3) could also be defined by the recursions (1) or (2)—all three definitions yield the same result in this case. We opted for the definition as it is because it is explicit and therefore useful for calculation, and it is this form that we use in the proof of Theorem 3.4.

Another facility in calculating the coefficients of q is that whenever $a_i < a_{i+1}$, then $c_i = a_{i+1} \cdots a_n c_n$. In the course of the proof of Theorem 3.4, we show that $ad_i \leqslant a_{i+1} \cdots a_n c_n$ for $k+m-1 \leqslant i \leqslant n-1$ and $d_i \leqslant a_{i+2} \cdots a_n c_n$ for $0 \leqslant i \leqslant k-2$. Thus we have $d_i = c_{i+1}$ if $k+m-1 \leqslant i \leqslant n-2$ and $a_{i+1} < a_{i+2}$, and we have $d_i = a^{-1} c_i$ if $1 \leqslant i \leqslant k-2$ and $a_i < a_{i+1}$. This means that the recursive definitions in steps (1) and (2) are only needed if multiple zeros other than a occur. In particular, q can be defined explicitly and is unique if all zeros of p are simple.

If multiple zeros occur, then $q = \sum d_i T^i$ is in general not the unique divisor of p by $T+a$, but it is maximal among all such divisors in the following sense: if $p \in (T+a) \boxdot q'$ for another polynomial $q' = \sum d_i' T^i$, then $d_i' \leqslant d_i$. This additional statement is easily derived from the proof of Theorem 3.4, but we will forgo to spell out the details.

3.3. An example

As an illustration of the division algorithm and of some observations from Remark 3.5, we consider the tropical polynomial $p = T^3 + rT^2 + T + r$ and $a = r$ where $r > 1$. The roots of p can be determined from the Newton polygon of p, which is the maximal convex function $\rho : [0,3] \to \mathbb{R}$ with $\rho(i) \leqslant -\log c_i$ for $i = 0, \dots, 3$. Its graph looks as follows:



The roots of p can be calculated from ρ by the formula $a_i = \exp\bigl(\rho(i) - \rho(i-1)\bigr)$; cf. [2, Thm. 4.1] for details. This yields the roots $a_1 = a_2 = 1$ and $a_3 = r$ of p. We encourage the reader to convince herself or himself that indeed $p \in (T+1) \boxdot (T+1) \boxdot (T+r)$.

Thus we see that $a = r = a_3$ is a root of p of multiplicity 1. We are prepared to execute the algorithm to determine $q = \sum d_i T^i$. In our example, we have $k = 3$ and $m = 1$. Thus only steps (2) (for $i = 0, 1$) and (3) (for $i = 2$) of the algorithm apply to determine the coefficients d_i of q. We calculate for increasing $i = 0, \dots, 2$:

$$d_0 = a^{-1} c_0 = 1, \quad d_1 = \max\{a^{-1} c_1, \, a^{-1} d_0\} = r^{-1}, \quad d_2 = c_3 = 1.$$

Thus we find that $q = T^2 + r^{-1}T + 1$ is a divisor of p by $T + r$. Once again, we encourage the reader to verify that indeed $p \in (T + r) \boxdot q$.

In order to exhibit some of the earlier mentioned effects that occur in the tropical setting and differ from the situation of polynomials over a field, we analyse this example in more detail. To begin with, we determine all polynomials $q' = \sum d'_i T^i$ that satisfy $p \in (T + a) \boxdot q'$, i.e.

$$c_3 \;=\; d'_2, \quad c_2 \;\in\; ad'_2 \boxplus d'_1, \quad c_1 \;\in\; ad'_1 \boxplus d'_0, \quad c_0 \;=\; ad'_0.$$

The first and last condition imply that $d'_2 = c_3 = 1$ and $d'_0 = a^{-1}c_0 = 1$, respectively. Using reversibility (HG6), the two middle conditions can be rewritten as

$$d'_1 \;\in\; (ad'_2) \boxplus c_2 \;=\; [0, r] \quad \text{and} \quad d'_1 \;\in\; (a^{-1}d'_0) \boxplus (a^{-1}c_1) \;=\; [0, r^{-1}],$$

which are simultaneous satisfied if and only if $d'_1 \in [0, r^{-1}]$. Thus the divisors of p by $T + a$ are precisely the polynomials of the form $q_s = T^2 + sT + 1$ with $s \in [0, r^{-1}]$.

This shows that there are several divisors q_s of p by $T + r$. Note that $q = q_{r^{-1}}$ is maximal among all divisors. It also shows that the naive attempt to find a divisor $\tilde{q} = \sum \tilde{d}_i T^i$ in terms of elementary symmetric polynomials $\tilde{d}_i = \sigma_{2-i}(a_1, a_2)$, i.e.

$$\tilde{q} \;=\; T^2 + \max\{a_1, a_2\}T + a_1a_2 \;=\; T^2 + T + 1$$

fails to provide a divisor of p by $T + r$, in contrast to the situation over a field.

This example also shows that we cannot replace step (2) of the division algorithm neither by (1) nor by (3). To wit, step (1) produces the coefficients

$$d_2 = c_3 = 1, \quad d_1 = \max\{c_2, ad_2\} = r, \quad d_0 = \max\{c_1, ad_1\} = r^2,$$

and step (3) produces the coefficients

$$d_2 = c_3 = 1, \quad d_1 = a_3c_3 = r, \quad d_0 = a_2a_3c_3 = r,$$

which both fail to provide a divisor $q = \sum d_i T^i$ of p by $T + ar$.

An example where step (2) fails to provide a divisor of p by $T + a$ is the polynomial $p = T^3 + rT^2 + T + r$ with $r \in (0, 1)$ and the root $a = r$. To wit, the roots of p are $a_1 = r$ and $a_2 = a_3 = 1$. We have $p \in (T + r) \boxdot q$ if and only if $q = T^2 + sT + 1$ with $s \in [0, r]$. But the steps in (2) produce the polynomial $r^{-2}T^2 + r^{-1}T + 1$, which is not a divisor of p by $T + r$.

3.4. The proof of Theorem 3.4

Let $a, a_1, \dots, a_n \in \mathbb{T}$ and the polynomials $p = \sum c_i T^i$ and $q = \sum d_i T^i$ be as in Theorem 3.4, i.e. $c_n^{-1}p \in \boxdot(T + a_i)$ is the unique factorization into linear terms with $a_1 \leqslant \cdots \leqslant a_n$, the nonzero element a is a root of p and the d_i are defined by the algorithmic steps (1)–(3). In this section, we prove Theorem 3.4, i.e.

$$c_n \;=\; d_{n-1}, \qquad c_0 \;=\; ad_0 \qquad \text{and} \qquad c_i \in (ad_i) \boxplus d_{i-1} \qquad \text{for} \qquad i = 1, \dots, n-1.$$

If $k \leqslant n - m$, then $c_n = d_{n-1}$ follows immediately from the definition in step (1). If $k = n - m + 1$, then d_{i-1}

The relation $c_n = d_{n-1}$ follows immediately from the definition in step (1) if $k \leqslant n - m$ and the definition in step (1) if $k = n - m + 1$. The relation $c_0 = ad_0$ follows immediately from the definition in step (2) if $k \geqslant 2$. If $k = 1$, then $a = a_1$ and according to the definition in step (3),

$$ad_0 \;=\; aa_2 \cdots a_n c_n \;=\; a_1 \cdots a_n c_n \;=\; c_0,$$

as desired.

Since $c_i \in (ad_i) \boxplus d_{i-1}$ if and only if the minimum among c_i, ad_i and d_{i-1} occurs twice, the relation $c_i \in (ad_i) \boxplus d_{i-1}$ is satisfied for $i = k+m, \dots, n-1$ and $i = 1, \dots, k-2$ by the very definition of d_{i-1} in (1) and d_i in (2), respectively.

Since $a = a_{i+1}$ for $i = k-1, \dots, k+m-2$, we have that

$$ad_i \;=\; aa_{i+2} \cdots a_n \;=\; d_{i-1}$$

for $i = k, \dots, k+m-2$, and thus $ad_i \boxplus d_{i-1} = [0, d_{i-1}]$. The relation $p \in \boxdot(T + a_i)$ means that

$$c_i \;\leqslant\; a_{i+1} \cdots a_n c_n \;=\; d_{i-1},$$

and thus $c_i \in ad_i \boxplus d_{i-1}$ for $i = k, \dots, k+m-2$, as desired.

We are left with $i = k-1$ and $i = k+m-1$, which are the critical cases that exhibit the compatibility between the different steps in the division algorithm.

We begin with the case $i = k-1$. Since $a_{k-1} < a_k$, we have $c_{k-1} = a_k \cdots a_n c_n$. By the definition in step (3) and since $a = a_k$, we have

$$ad_{k-1} \;=\; a_k a_{k+1} \cdots a_n c_n \;=\; c_{k-1}.$$

If we can show that $d_{k-2} \leqslant a_k \cdots a_n c_n$, then we obtain $c_{k-1} \in ad_{k-1} \boxplus d_{k-2}$ as desired.

We claim that $d_j \leqslant a_{j+2} \cdots a_n c_n$ for $j = 0, \dots, k-2$, which we will prove by induction on j. The case $j = k-2$ is the missing inequality to conclude the proof of the case $i = k-1$. For $j = 0$, we have indeed that $d_0 = a^{-1} c_0 \leqslant a_2 \cdots a_n c_n$ since $a_1 \leqslant a$. For $j = 1, \dots k-2$, we have $a_{j+1} \leqslant a_k = a$ and thus $a^{-1} a_{j+1} \cdots a_n c_n \leqslant a_{j+2} \cdots a_n c_n$. Since $c_j \leqslant a_{j+1} \cdots a_n c_n$ by our assumptions and $d_{j-1} \leqslant a_{j+1} \cdots a_n c_n$ by the inductive hypothesis, we get

$$d_j \;=\; \max\{a^{-1} c_j,\, a^{-1} d_{j-1}\} \;\leqslant\; a^{-1} a_{j+1} \cdots a_n c_n \leqslant a_{j+2} \cdots a_n c_n,$$

which verifies our claim and concludes the proof of the case $i = k$.

We turn to the case $i = k+m-1$. By the definition in step (3), $d_{k+m-2} = a_{k+m} \cdots a_n c_n$. Since $a_{k+m-1} < a_{k+m}$, we have $c_{k+m-1} = a_{k+m} \cdots a_n c_n = d_{k+m-2}$. If we can show that $ad_{k+m-1} \leqslant a_{k+m} \cdots a_n c_n$, then we obtain the desired relation $c_{k+m-1} \in ad_{k+m-1} \boxplus d_{k+m-2}$.

We claim that $ad_j \leqslant a_{j+1} \dots a_n c_n$ for $j = n-1, \dots, k+m-1$, which we will prove by induction on j (in decreasing order). The case $j = k+m-1$ is the missing inequality to conclude the proof of the case $i = k+m-1$. For $j = n-1$, we have $d_{n-1} = c_n$ and $a \leqslant a_n$. Thus $ad_{n-1} \leqslant a_n c_n$, as claimed. For $l = n-2, \dots, k+m-1$, we have $a \leqslant a_{j+1}$. Since $c_{j+1} \leqslant a_{j+2} \cdots a_n c_n$ by our assumptions and $ad_{j+1} \leqslant a_{j+2} \dots a_n c_n$ by the inductive hypothesis, we get

$$ad_j \;=\; a \cdot \max\{c_{j+1},\, ad_{j+1}\} \;\leqslant\; a_{j+1} a_{j+2} \cdots a_n c_n,$$

as claimed. This concludes the proof of Theorem 3.4. □

4. Factorizations of sign polynomials

A *sign polynomial* is a polynomial over the sign hyperfield $\mathbb{S}$. In this section, we classify all irreducible sign polynomials and show that the sign hyperfield fails to have the unique factorization property. Still it admits a division algorithm for the division of sign polynomials by linear terms, in analogy to the division algorithm for tropical polynomials.

4.1. Classification of the irreducible polynomials

Since a sign polynomial p is irreducible if and only if ap is irreducible for any $a \in \mathbb{S}^\times$, we can restrict our attention to monic irreducible sign polynomials.

Theorem 4.1. *The monic irreducible sign polynomials are T, $T-1$, $T+1$ and T^2+1.*

Proof. It is clear that every linear polynomial is irreducible, cf. Section 2.3. Thus T, $T-1$ and $T+1$ are precisely the monic irreducible polynomials of degree 1.

Given a monic irreducible sign polynomial $p = \sum c_i T^i$, let $\hat{c}_i \in \mathbb{R}$ be real numbers with $\operatorname{sign}(\hat{c}_i) = c_i$. By Lemma 2.1, the monic real polynomial $\hat{p} = \sum \hat{c}_i T^i$ is irreducible as well. We know that the monic irreducible real polynomials are either linear or quadratic with positive constant term $\hat{c}_0 > 0$. Thus if p is not linear then it must be of the form $T^2 + aT + 1$ for some $a \in \mathbb{S}$.

By Lemma 2.6, a quadratic polynomial is irreducible if and only if it does not have a root. We can verify this for all polynomials of the form $T^2 + aT + 1$: while $T^2 + T + 1$ has -1 as a root and $T^2 - T + 1$ has 1 as a root, $T^2 + 1$ is the only quadratic polynomial of this shape that does not have a root. This completes our classification of the monic irreducible sign polynomials. □

4.2. The failure of unique factorization

It is easy to see that the unique factorization property holds for sign polynomials of degree $\leqslant 2$. The following example shows that this property fails from degree 3 on.

Consider the sign polynomial $p = T^3 + T^2 + T + 1$. Then -1 is a root of p, i.e. $0 \in p(-1)$. Thus there is a polynomial $q = d_2T^2 + d_1T + d_0$ such that $p \in (T+1) \boxdot q$, which is equivalent to

$$d_0 = 1, \quad d_2 = 1 \quad \text{and} \quad 1 \in 1 \boxplus d_1.$$

The equation $1 \in 1 \boxplus d_1$ is true for all $d_1 \in \mathbb{S}$, which means that p is an element of all the three hyperproducts

$$(T+1) \boxdot (T^2+1), \quad (T+1) \boxdot (T^2+T+1) \quad \text{and} \quad (T+1) \boxdot (T^2-T+1).$$

The factors $T^2 \pm T + 1$ factorize into $T^2 + T + 1 \in (T+1) \boxdot (T+1)$ and $T^2 - T + 1 \in (T-1) \boxdot (T-1)$, respectively. The factor T^2+1 is irreducible. Thus we find the three different factorizations

$$(T+1) \boxdot (T^2+1), \quad (T+1) \boxdot (T+1) \boxdot (T+1) \quad \text{and} \quad (T+1) \boxdot \Big((T-1) \boxdot (T-1) \Big)$$

of $T^3 + T^2 + T + 1$.

In fact, this example shows that sign polynomials cannot have the unique factorization property with respect to any concept of factorization that is preserved under morphisms, in the sense of Lemma 2.1. Indeed, the sign map $\operatorname{sign} : \mathbb{R} \to \mathbb{S}$ maps both real polynomials $T^3 + T^2 + T + 1 = (T+1)(T^2+1)$ and $T^3 + 3T^2 + 3T + 1 = (T+1)^3$ to p.

4.3. A division algorithm

In spite of the failure of unique factorization, there is still an algorithmic way to determine a divisor of a sign polynomial by a linear term. Such a division algorithm was already exhibited in the proof of Theorem 3.1 in [2] for a restricted class of sign polynomials. In the following, we describe an extension of this division algorithm that applies to all sign polynomials.

As a preliminary consideration, we observe that if $a = 0$ is a root of a sign polynomial $p = \sum c_i T^i$, then $c_0 = 0$ and $q = \sum c_{i+1} T^i$ is the unique sign polynomial such that $p \in T \boxdot q$. Thus it suffices to describe the division algorithm for nonzero roots $a \in \mathbb{S}^\times = \{\pm 1\}$ only.

Theorem 4.2. *Let $p = \sum c_i T^i$ be a sign polynomial of degree n with root $a \in \{\pm 1\}$. Define*

$$l \; = \; \min\big\{ i \in \mathbb{N} \,\big|\, c_i \neq 0 \big\} \qquad \textit{and} \qquad k \; = \; \min\big\{ i \in \mathbb{N} \,\big|\, c_{i+1} = -a^{i+1-l} c_l \big\}.$$

Define recursively for $i = n-1, \dots, 0$ (in decreasing order)

$$d_i \; = \; c_{i+1} \qquad \textit{if } c_{i+1} \neq 0 \textit{ and } i > k; \tag{1}$$

$$d_i \; = \; a d_{i+1} \qquad \textit{if } c_{i+1} = 0 \textit{ and } i > k; \tag{2}$$

$$d_i \; = \; -a^{i+l-1} c_l \qquad \textit{if } l \leqslant i \leqslant k; \tag{3}$$

$$d_i \; = \; 0 \qquad \textit{if } 0 \leqslant i < l. \tag{4}$$

Then $p \in (T - a) \boxdot q$ for $q = \sum d_i T^i$.

Proof. Once we have proven the theorem for the root $a = 1$ of $p = \sum c_i T^i$, we can derive the division algorithm for the root -1 by applying the division algorithm for $a = 1$ to $p(-T) = \sum (-1)^i c_i T^i$ and using that $p \in \big(T - (-1)\big) \boxdot q$ if and only if $p(-T) \in -(T-1) \boxdot q(-T)$. Thus the case $a = -1$ follows by a straight forward calculation from the case $a = 1$.

We proceed with the proof for $a = 1$. Recall that $p \in (T - 1) \boxdot q$ if and only if

$$c_n \; = \; d_{n-1}, \qquad c_0 \; = \; -d_0 \qquad \text{and} \qquad c_i \in (-d_i) \boxplus d_{i-1} \qquad \text{for} \qquad i = 1, \dots, n-1.$$

We begin with $c_n = d_{n-1}$. If $k < n-1$, then $d_{n-1} = c_n$ by (1) since $c_n \neq 0$. If $k = n-1$, then $c_n = -c_l$ by the definition of k and thus $d_{n-1} = -c_l = c_n$ by (3). Thus $c_n = d_{n-1}$, as desired.

We proceed with $c_0 = -d_0$. If $l = 0$, then $d_0 = -c_0$ by (3). If $l > 0$, then $c_0 = 0$ and $d_0 = 0 = c_0$ by (4). Thus $c_0 = -d_0$, as desired.

We proceed with $c_i \in (-d_i) \boxplus d_{i-1}$ for $1 \leqslant i \leqslant n-1$. If $1 \leqslant i < l$, then $c_i = 0$ and $d_{i-1} = d_i = 0$ by (4). Thus $c_i \in (-d_i) \boxplus d_{i-1}$, as desired.

If $i = l$, then $c_l \neq 0$, $d_l = -c_l$ by (3) and $d_{l-1} = 0$ by (4). Thus $c_i \in (-d_i) \boxplus d_{i-1}$, as desired.

If $l < i \leqslant k$, then $d_{i-1} = d_i = -c_l \neq 0$ by (3) and the definition of l. Thus $c_i \in (-d_i) \boxplus d_{i-1}$, as desired.

If $i = k+1$, then $c_{k+1} = -c_l \neq 0$ by the definitions of k and l. Thus $d_k = -c_l \neq 0$ by (3), and $c_i \in (-d_i) \boxplus d_{i-1}$, as desired.

If $k+1 < i \leqslant n-1$ and $c_i \neq 0$, then $d_{i-1} = c_i \neq 0$ by (1). If $k+1 < i \leqslant n-1$ and $c_i = 0$, then $d_{i-1} = d_i$ by (2). Thus in both cases $c_i \in (-d_i) \boxplus d_{i-1}$, as desired. This concludes the proof of the theorem. □

Acknowledgments

The authors thank Matt Baker for helpful discussions that led to the results of this paper. We thank Gunn Trevor and Liu Ziqi for correcting some wrong statements of an early draft of this text. We thank an anonymous referee for pointing out the existence of a (non-deterministic) division algorithm for polynomials over an arbitrary hyperfield.

References

[1] Matthew Baker, Nathan Bowler, Matroids over partial hyperstructures, Adv. Math. 343 (2019) 821–863.

[2] Matthew Baker, Oliver Lorscheid, Descartes' rule of signs, Newton polygons, and polynomials over hyperfields, J. Algebra 569 (2021) 416–441.

[3] Alain Connes, Caterina Consani, The hyperring of adèle classes, J. Number Theory 131 (2) (2011) 159–194.

[4] B. Davvaz, T. Musavi, Codes over hyperrings, Mat. Vesnik 68 (1) (2016) 26–38.

[5] Marc Krasner, Approximation des corps valués complets de caractéristique $p \neq 0$ par ceux de caractéristique 0, in: Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956, in: Centre Belge de Recherches Mathématiques, Établissements Ceuterick, Librairie Gauthier-Villars, Louvain, Paris, 1957, pp. 129–206.

[6] Ziqi Liu, A few results on associativity of hypermultiplications in polynomial hyperstructures over hyperfields, 2019, Preprint, arxiv:1911.09263.

[7] Oleg Ya. Viro, On basic concepts of tropical geometry, Proc. Steklov Inst. Math. 273 (1) (2011) 252–282.