A MULTIPLICATION TECHNIQUE FOR THE FACTORIZATION OF BIVARIATE QUATERNIONIC POLYNOMIALS

JOHANNA LERCHER AND HANS-PETER SCHRÖCKER

Abstract. We consider bivariate polynomials over the skew field of quaternions, where the indeterminates commute with all coefficients and with each other. We analyze existence of univariate factorizations, that is, factorizations with univariate linear factors. A necessary condition for existence of univariate factorizations is factorization of the norm polynomial into a product of univariate polynomials. This condition is, however, not sufficient. Our central result states that univariate factorizations exist after multiplication with a suitable univariate real polynomial as long as the necessary factorization condition is fulfilled. We present an algorithm for computing this real polynomial and a corresponding univariate factorization. If a univariate factorization of the original polynomial exists, a suitable input of the algorithm produces a constant multiplication factor, thus giving an a posteriori condition for existence of univariate factorizations. Some factorizations obtained in this way are of interest in mechanism science. We present an example of a curious closed-loop mechanism with eight revolute joints.

1. Introduction

By \((\mathbb{H}, +, \cdot)\) we denote the skew field of real quaternions with the usual addition and non-commutative multiplication. Let \(\mathbb{H}[t]\) be the ring of polynomials in the indeterminate \(t\) with multiplication defined by the convention that \(t\) commutes with all coefficients. A fundamental theorem of algebra also holds true for polynomials in \(\mathbb{H}[t]\): Each non-constant univariate quaternionic polynomial admits a factorization with linear factors (c. f. [3, 4, 16]). Remarkably, such a factorization need not be unique. In general, there exist \(n!\) different factorizations with linear factors, where \(n\) denotes the degree of the polynomial. This ambiguity is caused by non-commutativity of quaternion multiplication.

Factorization of univariate quaternionic polynomials with linear factors is well understood. This article focuses on bivariate quaternionic polynomials with indeterminates \(t, s\) that commute with all coefficients and with each other. Denote the thus obtained polynomial ring by \(\mathbb{H}[t,s]\). In contrast to the univariate case, little is known about criteria that ensure existence of factorizations of a polynomial \(Q \in \mathbb{H}[t,s]\) and the same can be said about algorithms to compute factorizations. We briefly explain an important difference between the univariate and the bivariate...
case: Denote by $Q^*$ the conjugate polynomial, obtained by conjugating the quaternion coefficients of $Q$. A necessary factorization condition is factorizability of the norm polynomial $QQ^* \in \mathbb{R}[t,s]$ of $Q$. The reason for this is multiplicativity of the quaternion norm: $Q = Q_1Q_2$ with $Q_1, Q_2 \in \mathbb{H}[t,s]$ implies $QQ^* = (Q_1Q_1^*) (Q_2Q_2^*)$ with $Q_1Q_1^*, Q_2Q_2^* \in \mathbb{R}[t,s]$. The norm polynomial of a univariate quaternionic polynomial of degree greater than one is a product of at least two irreducible real polynomials that play an important role in the computation of factorizations. This is in contrast to the bivariate case where factorizability of the norm polynomial is exceptional and not a sufficient condition for existence of factorizations. One instance for this (that we will frequently encounter in this text) is given in [1].

There exist few factorization results for bivariate quaternionic polynomials. The most promising article in this context is [17] by Skopenkov and Krasauskas. They introduce a technique for the factorization of bivariate quaternionic polynomials of bi-degree $(n,1)$, where $n \in \mathbb{N}_0$ is an arbitrary non-negative integer. In [10], we build on their article and characterize all possible factorizations of quaternionic polynomials of bi-degree $(n,1)$ with univariate linear factors. We are not aware of further publications concerning this topic.

In this article, we broaden the ideas of [17] and state some new factorization results for bivariate quaternionic polynomials. Our contribution deals with factorizations of polynomials $Q \in \mathbb{H}[t,s]$ with univariate linear factors, that is,

$$Q = a(u_1 - h_1) \cdots (u_k - h_k)$$

with $u_i \in \{t,s\}$ and $a, h_i \in \mathbb{H}$ for $i = 1, \ldots, k$. We call these factorizations univariate since each factor of $Q$ is a univariate quaternionic polynomial in either $t$ or $s$. Univariate factorizations may only occur if $Q$ satisfies $QQ^* = PR$ with $P \in \mathbb{R}[t], R \in \mathbb{R}[s]$. We call this rather restrictive condition the necessary factorization condition. By [17], this condition is also sufficient for quaternionic polynomials of bi-degree $(n,1)$. Even this special case is interesting and we consider the results in [17] as an important contribution in the development of a factorization theory for bivariate quaternionic polynomials. The degree restrictions in [17] are quite strong but, unfortunately, necessary. The polynomial

$$B = (t^2 - i)s^2 + (2t)s + (it^2 - 1)$$

was given by Beauregard in [1]. It is an example that satisfies the necessary factorization condition $BB^* = (t^4 + 1)(s^4 + 1)$ but is irreducible in $\mathbb{H}[t,s]$ (c. f. [1, p. 68–69] for a proof over rational quaternions and [17, Proof of Example 1.5] for a proof over real quaternions).

We have, however,

$$(t^2 + 1)B = \left( t + \frac{-k - j}{\sqrt{2}} \right) \left( s + \frac{1 - i}{\sqrt{2}} \right) \left( t + \frac{1 + k}{\sqrt{2}} \right) \left( t + \frac{-1 + k}{\sqrt{2}} \right) \left( s + \frac{-1 + i}{\sqrt{2}} \right) \left( t + \frac{j - k}{\sqrt{2}} \right),$$

an identity that was called surprising by Skopenkov and Krasauskas [17, Example 2.11]. In the present paper we show that similar identities not only hold for the Beauregard polynomial (1) but are generally true: For any polynomial $Q \in \mathbb{H}[t,s]$ satisfying the necessary factorization condition there exists a real polynomial $K \in \mathbb{R}[t]$ (or $K \in \mathbb{R}[s]$) such that $KQ$ admits a univariate factorization. The real polynomial $K$ depends on an ordering of the irreducible real quadratic factors.
of $R$ (or $P$, respectively), where $QQ^* = PR$ with $P \in \mathbb{R}[t]$ and $R \in \mathbb{R}[s]$. For this reason, we can find up to $m! + n!$ univariate factorizations of real multiples of $Q$, where $(m, n)$ denotes the bi-degree of $Q$. If $Q$ admits a univariate factorization, a suitable ordering of irreducible real quadratic factors indeed yields $K = 1$. We provide a sharp upper bound on the total number of possible univariate factorizations of $Q$ and show how to find all of them.

Factorizability of quaternionic polynomials is an interesting research topic in its own right. However, polynomials over the quaternions and in particular over the dual quaternions (Section 5) received recent attention because of their relation to kinematics and mechanism science: Univariate (dual) quaternionic polynomials can be used to represent one-parametric rational motions [5] and factorizations correspond to decompositions of the respective motion into simpler motions. In particular, factorizations with linear factors yield decompositions into rotations and translations. In [2,5,6,12,13], this fact has been used to construct mechanisms following a given motion or curve. From different factorizations mechanical “legs” with revolute (or prismatic) joints are constructed that fully constrain a mechanism with prescribed rational end-effector motion or trajectory.

The findings of this article allow the extension of this concept to two-parametric motions. A first example will be outlined in the concluding Section 5. In this context,

(i) univariate factorizations are of particular interest as each univariate linear factor can be realized by a revolute/translational joint and
(ii) multiplication with a real polynomial factor is admissible as it does not change the underlying rational motion.

The paper is structured as follows: In Section 2, we settle our notation and recall some known facts concerning factorization theory of univariate and bivariate quaternionic polynomials. In Section 3, we formulate and prove the central result on existence of $K \in \mathbb{R}[t]$ (or $K \in \mathbb{R}[s]$, respectively) such that $KQ$ admits a univariate factorization. The proof is constructive and can be cast into an algorithm for finding $K$ and a univariate factorization of $KQ$. In Section 4 we consider the case that the original polynomial $Q$ admits a univariate factorization. In Section 5 we present applications to mechanism science and an outlook to future research.

2. Preliminaries

Let us consider the Clifford algebra $\mathcal{C}(3,0,1)$. The index $(3,0,1)$ indicates existence of four basis elements $e_1, e_2, e_3, e_4$, where the first 3 basis elements square to 1 ($e_1^2 = e_2^2 = e_3^2 = 1$) and the last basis element squares to 0 ($e_4^2 = 0$). By the defining conditions for Clifford algebras, the basis elements also satisfy

$$e_ie_j + e_je_i = 0 \quad \text{for} \quad i \neq j.$$  

We use the notation $e_{12..k} := e_1e_2\cdots e_k$, $0 \leq k \leq 4$, for products of consecutive basis elements. Let us consider the subalgebra $\mathbb{H}$ of quaternions which is generated by the elements $e_0, e_{23}, e_{31}, e_{12}$ which are, in that order, identified with 1, i, j and k. An element $h \in \mathbb{H}$ can be written as

$$h = h_0 + h_1i + h_2j + h_3k \quad \text{with} \quad h_0, h_1, h_2, h_3 \in \mathbb{R}.$$  

\footnote{We use a Clifford algebra that is larger than actually needed for defining quaternions because we will later (in Section 5) also consider dual quaternions.}
The basis elements satisfy the multiplication rules

\[ i^2 = j^2 = k^2 = ijk = -1. \]

Multiplication of quaternions is not commutative but \( \mathbb{H} \) forms at least a division ring. The conjugate of \( h \) is \( h^* = h_0 - h_1i - h_2j - h_3k \), its norm is the real number \( hh^* = h_0^2 + h_1^2 + h_2^2 + h_3^2 \) and the inverse of \( h \in \mathbb{H} \setminus \{0\} \) is given by \( h^{-1} = h^*/hh^* \).

By \( \mathbb{H}[t] \) and \( \mathbb{H}[t, s] \) we denote the set of univariate and bivariate quaternionic polynomials, respectively. Addition and scalar multiplication of quaternionic polynomials are defined in the common way. For multiplication we additionally assume that the indeterminates commute with the coefficients and with each other. The conjugate \( Q^* \) of a quaternionic polynomial \( Q \) is defined by conjugating its coefficients. Its norm polynomial is the real polynomial given by \( QQ^* \). We use the following notations: Let us fix \( m, n \in \mathbb{N}_0 \). By \( \mathbb{H}_{mn} \) we denote the set of quaternionic polynomials in \( \mathbb{H}[t, s] \) of degree at most \( m \) in \( t \) and at most \( n \) in \( s \). By replacing \( m \) or \( n \) with the symbol \( * \), we denote the set of polynomials with arbitrary degree in the respective variable. For instance, the set of polynomials of bi-degree \( (n, 1) \) with arbitrary \( n \in \mathbb{N}_0 \) is denoted by \( \mathbb{H}_{*1} \). This notation is taken from [17].

In this article, we repeatedly refer to known factorization results for univariate and bivariate polynomials. In particular, we use some crucial results from [17]. Therefore, we would like to briefly recapitulate the most important univariate and bivariate factorization results. The respective algorithms are taken from [5, univariate case] and [17, bivariate case] and adapted to our setting. To be able to highlight the similarities between the univariate and bivariate results, our explanations may sometimes slightly differ from the original papers.

### 2.1. Univariate Polynomials

Each non-constant univariate quaternionic polynomial \( Q \in \mathbb{H}[t] \) admits a factorization with linear factors which can be found as follows: At first, we assume that \( Q \) does not possess a real polynomial factor of positive degree. By [7, Theorem 2.3], this can be done without loss of generality since non-constant univariate real polynomials always admit factorizations with linear factors over \( \mathbb{R} \). For later reference, we state this as a proposition:

**Proposition 2.1.** A non-constant univariate real polynomial \( F \in \mathbb{R}[t] \) admits a factorization with linear factors over \( \mathbb{H} \).

The norm polynomial \( QQ^* \) is a real polynomial and it can be decomposed into irreducible factors over \( \mathbb{R} \). If \( M \in \mathbb{R}[t] \) is a monic irreducible factor of \( QQ^* \), one can apply division with remainder \(^2\) and obtains

\[
Q = TM + S \quad \text{with} \quad T, S \in \mathbb{H}[t], \deg(S) < 2.
\]

If \( S = 0 \), we have \( Q = TM \) and \( Q \) possesses a real polynomial factor of positive degree, a case which we already excluded. Therefore, we just have to consider the case \( S \neq 0 \): The norm polynomial \( SS^* \) of the remainder \( S \) satisfies the important

\(^2\)Division with remainder is applicable for polynomials in any polynomial ring \( R[t] \), where \( R \) is an arbitrary ring, if the leading coefficient of the divisor polynomial is invertible (for instance, c. f. [11]). If \( R \) is not commutative, we have to distinguish between left-division and right-division with remainder. However, \( M \in \mathbb{R}[t] \) is in the center of \( \mathbb{H}[t] \), hence this distinction is not necessary in our case and the notation division with remainder is justified.
identity \( SS^* = cM \) with \( c \in \mathbb{R} \setminus \{0\} \); indeed, the polynomial \( M \) is an irreducible factor of \( QQ^* \) and
\[
(4) \quad SS^* = (Q - TM)(Q - TM)^* = QQ^* - QT^*M - TQ^*M + TT^*M^2.
\]

Since each term on the right-hand side of Equation (4) is divisible by \( M \), the same is true for \( SS^* \). If \( \deg(S) = 0 \), the polynomial \( M \) would not divide \( SS^* \in \mathbb{R} \setminus \{0\} \) and we conclude \( \deg(S) = 1 \), \( \deg(M) = 2 \) and also \( SS^* = cM \) with \( c \in \mathbb{R} \setminus \{0\} \).

Writing \( S = a(t-h) \) with \( a, h \in \mathbb{H} \) and \( c = a^*a \), \( M = (t-h)^*(t-h) \), we conclude that \( t-h \) is a right factor of both \( S \) and \( M \) and hence, by (3), also a right factor of \( Q \). Using polynomial division we find \( Q' \in \mathbb{H}[t] \) such that \( Q = Q'(t-h) \). By proceeding inductively with \( Q' \) instead of \( Q \), we obtain the desired factorization with linear factors.

**Remark 2.2.** Let us close this section with some important observations:

(i) If \( Q \) has no real polynomial factor of positive degree, the above arguments show that a monic irreducible factor \( M \) of \( QQ^* \) is of degree two.

(ii) The right factor \( t-h \) of \( Q \) depends on the irreducible polynomial \( M \in \mathbb{R}[t] \) of \( QQ^* \). By choosing different irreducible factors of the norm polynomial, we obtain different right factors of \( Q \). In general, there exist \( \deg Q! \) different factorizations with linear factors.

(iii) Following above ideas, one successively separates linear right factors until one obtains the desired factorization of \( Q \). It is equally possible to split off left factors, for example by computing right factors of the conjugate polynomial \( Q^* \).

(iv) Unless \( Q \) is divisible by \( M \), the right factor \( t-h \) with \( (t-h)(t-h)^* = M \) is uniquely determined [5, Lemma 3]. A similar statement is true for the left factors of \( Q \).

We conclude this section with a word of warning on some algorithmic assumptions made throughout this paper. The presented iterative factorization algorithm for univariate quaternionic polynomials requires in each step as input a real quadratic factor \( M \) of the norm polynomial \( QQ^* \). In general, the computation of \( M \) is only possible numerically which poses the (yet unsolved) question for a robust numeric version of the factorization algorithm. Similar concerns apply to all factorization algorithms we encounter in this article. This should be kept in mind when reading phrases like “we can compute all factorizations” or, “this algorithm yields a factorization of a type xyz if it exists” in the remainder of this paper.

### 2.2. Bivariate Polynomials.

Let us now consider univariate factorizations of bivariate quaternionic polynomials, that is, factorizations with only univariate linear factors. Any univariate factorization of a bivariate polynomial \( Q \in \mathbb{H}[t, s] \) can be represented by a univariate factorization with monic linear factors
\[
(5) \quad Q = a(u_1 - h_1) \cdots (u_k - h_k),
\]
where \( u_i \in \{t, s\} \) and \( a, h_i \in \mathbb{H} \) for \( i = 1, \ldots, k \). We usually consider univariate factorizations of the form (5).

Univariate factorizations may only occur if the norm polynomial factors as \( QQ^* = PR \) with \( P \in \mathbb{R}[t] \) and \( R \in \mathbb{R}[s] \). In order to see this, compute
\[
QQ^* = a(u_1 - h_1) \cdots (u_k - h_k)(u_k - h_k)^* \cdots (u_1 - h_1)^* a^*.
\]
Factors of the form \((u_i - h_i)(u_i - h_i)^*\) are real univariate polynomials in \(t\) or \(s\) and hence part of the center of \(\mathbb{H}[t, s]\). Using this fact we obtain
\[
QQ^* = aa^*(u_1 - h_1)(u_1 - h_1)^* \cdots (u_k - h_k)(u_k - h_k)^* ,
\]
and \(QQ^*\) turns out to be a product of univariate real polynomials.

**Definition 2.3** (NFC). Let \(Q \in \mathbb{H}[t, s]\) be a bivariate quaternionic polynomial. We say that \(Q\) satisfies the necessary factorization condition (NFC) if \(QQ^* = PR\) with \(P \in \mathbb{R}[t]\) and \(R \in \mathbb{R}[s]\).

In order to state results on existence of univariate factorizations, we proceed similarly to Section 2.1 and neglect real polynomial factors of positive degree: We endow the polynomial ring \(\mathbb{H}[t, s]\) with the graded lexicographic order. For a polynomial \(Q = Q_0 + iQ_1 + jQ_2 + kQ_3 \in \mathbb{H}[t, s]\) we define \(\text{mrpf}(Q)\) to be the monic greatest common divisor of the polynomials \(Q_0, Q_1, Q_2, Q_3 \in \mathbb{R}[t, s]\).\(^3\) We then find a polynomial \(Q' \in \mathbb{H}[t, s]\) such that \(Q = \text{mrpf}(Q)Q'\). Obviously, the polynomial \(Q'\) does not possess a real divisor of positive degree. If \(Q\) satisfies the NFC, the real polynomial \(\text{mrpf}(Q)\) is a product of univariate real polynomials as well. These polynomials admit factorizations over \(\mathbb{H}\) according to Proposition 2.1. Therefore, it is sufficient to consider polynomials \(Q \in \mathbb{H}[t, s]\) with \(\text{mrpf}(Q) = 1\).

The NFC turns out to be sufficient if we consider polynomials \(Q \in \mathbb{H}_{11}\). This immediately follows from \([17]\) and we will briefly explain how to find a factorization:

Consider a non-constant polynomial \(Q \in \mathbb{H}_{11}\) with \(\text{mrpf}(Q) = 1\) satisfying the NFC \(QQ^* = PR\) with \(P \in \mathbb{R}[t]\) and \(R \in \mathbb{R}[s]\). If \(\deg(P) = 0\), \(Q\) is a linear polynomial in \(\mathbb{H}[s]\), hence there is nothing to show. Otherwise, we choose a monic irreducible factor \(M \in \mathbb{R}[t]\) of the univariate \(t\)-factor \(P\) in the norm polynomial. Let \(T, S \in \mathbb{H}[t, s]\) be polynomials with
\[
Q = TM + S \quad \text{and} \quad S \in \mathbb{H}_{11} .
\]
Representation (6) can be found by writing \(Q = Q_0 + sQ_1\) with \(Q_0, Q_1 \in \mathbb{H}[t]\) and dividing both, \(Q_0\) and \(Q_1\), with remainder by \(M\).\(^4\) If \(S = 0\), we have \(Q = TM\), whence \(Q\) has a real polynomial factor of positive degree. This contradicts our assumption \(\text{mrpf}(Q) = 1\). Therefore, \(S \neq 0\), and we repeat the computations made in Equation (4) and conclude that \(M\) divides \(SS^*\). Similar to the univariate case, this is only possible if \(\deg(M) = 2\) and \(SS^* = HM\) for an appropriate polynomial \(H \in \mathbb{R}[s]\). Note that \(H\) is indeed univariate since \(S \in \mathbb{H}_{11}\). Hence \(S\) satisfies the NFC. (We would like to emphasize the resemblance of the univariate and bivariate ideas; in the univariate case we obtained \(SS^* = cM\) with \(c \in \mathbb{R} \setminus \{0\}\).)

The remainder polynomial \(S\) possesses a very low bi-degree and, therefore, is easy to handle. Indeed, in the simple case of polynomials in \(\mathbb{H}_{11}\) satisfying the NFC, the direct computation of a univariate factorization via the Splitting Lemma by Skopenkov and Krasauskas (c. f. \([17, \text{Splitting Lemma 2.6}]\)) is possible. Using

---

\(^3\)The acronym \(\text{mrpf}\) was introduced in \([14]\) and stands for “monic real polynomial factor” of maximal degree.

\(^4\)If we view \(Q\) and \(M\) to be univariate polynomials in \(t\) having coefficients in \(\mathbb{H}[s]\), the polynomial \(S \in \mathbb{H}_{11}\) is the unique remainder after division with remainder of \(Q\) by \(M\). Note that, in this setting, the leading coefficient of \(M\) is 1, thus invertible, and division is possible. The decomposition \(Q = Q_0 + sQ_1\) was used to highlight the fact \(S \in \mathbb{H}_{11}\).
their result, one obtains

*Case 1:* \( S = (t - h)A \) or

*Case 2:* \( S = A(t - h) \),

with \( A \in \mathbb{H}[s] \), \((t-h)(t-h)^* = M, AA^* = H\). Now, one can either separate the factor \( t - h \) on the left or the right of \( Q \). Indeed, if *Case 1* is satisfied, \( t - h \) is a left factor of both \( S \) and \( M \) and, by (6), also of \( Q \). (Note that \( TM = MT \) since \( M \in \mathbb{R}[t] \) is a real polynomial.) Otherwise, \( t - h \) is a right factor of \( S \) and \( M \) and hence, again by (6), also a right factor of \( Q \). Choosing the next irreducible factor of \( P \) and proceeding inductively yields a decomposition with univariate linear factors.

**Remark 2.4.**

(i) The fact \( mrpf(Q) = 1 \) implies that the monic irreducible factor \( M \) of \( P \) is of degree two. It is not unique and a different choice for \( M \) will, in general, also yield a different left or right factor \( t - h \).

(ii) Similar to the univariate case, we may conclude that the univariate right factors with norm polynomial \( M \) are, in general, unique. Indeed, let \( t - h \) be a linear right factor of \( Q \) and let \( M := (t - h)(t - h)^* \). If \( Q \) is not divisible by \( M \), we claim that \( h \) is uniquely determined. The fact \( M \nmid Q \) implies that there exists at least one coefficient of \( Q \), viewed as an element of \( \mathbb{H}[t][s] \), that is not divisible by \( M \). This coefficient is a univariate polynomial in \( \mathbb{H}[t] \) with right factor \( t - h \). Hence \( t - h \) is uniquely determined by Remark 2.2, Item iv.

The same argument can be applied to left factors of \( Q \). This statement is not only true for \( Q \in \mathbb{H}_{s+1} \) but also for \( Q \in \mathbb{H}[t, s] \). Moreover, the arguments remain true for linear \( s \)-factors of \( Q \).

For the sake of completeness and the reader’s convenience we describe the factorization technique for polynomials in \( \mathbb{H}_{s+1} \) in Algorithm 1. The algorithm relies on the factorization technique of [17] and in particular on their crucial Splitting Lemma. Unlike [17], our slightly modified version forces the linear factors in \( t \) to be monic as described in the current section. It takes as input a tuple of quadratic factors of \( P \) rather than \( P \) itself in order to account for the ambiguity mentioned in Remark 2.4, Item i. Moreover, we assume \( mrpf(Q) = 1 \). The adaptation of Algorithm 1 to the case \( mrpf(Q) \neq 1 \) is straightforward (c. f. Proposition 2.1). Since \( \mathbb{H}[t] \subseteq \mathbb{H}_{s+1} \), the algorithm also works for univariate polynomials in \( \mathbb{H}[t] \) (c. f. lines 9-11).

Implementation of Algorithm 1 and also the later Algorithm 2 only requires a few standard ingredients: Factorization of real polynomials, quaternion algebra, and division with remainder over polynomial rings. Our examples were computed using a self written library for the computer algebra system Maple [15].

### 3. A Multiplication Technique

As outlined in Section 2.2, existence of univariate factorizations of bivariate quaternionic polynomials is exceptional. They may only occur if the – rather restrictive – NFC is satisfied. However, the Beauregard polynomial (1) is irreducible in \( \mathbb{H}[t, s] \) even though it satisfies the NFC. Nevertheless, a real multiple of \( B \) admits the desired decomposition with univariate linear factors (2). Motivated by this example, we introduce a *multiplication technique*. We consider bivariate quaternionic polynomials satisfying the NFC and show that suitable real polynomial multiples of these polynomials admit a univariate factorization.
A non-constant polynomial with \( mrpf(Q) = 1 \), satisfying the NFC \( QQ^* = PR \), where \( P \in \mathbb{R}[t] \), \( R \in \mathbb{R}[s] \).

Input: A tuple \((M_1, \ldots, M_n)\) of monic irreducible polynomials in \( \mathbb{R}[t] \) such that \( P = \text{lcm}(P) \cdot M_1 \cdots M_n \), where \( \text{lcm}(P) \) is the leading coefficient of \( P \).

Output: Tuples \( F_i = (L_1, \ldots, L_k) \), \( F_r = (R_1, \ldots, R_p) \) of univariate, linear, monic polynomials in \( \mathbb{H}[t] \) and a linear polynomial \( U \in \mathbb{H}[s] \) such that \( Q = L_1 \cdots L_k \cdot U \cdot R_1 \cdots R_p \).

1: \( i \leftarrow 1, F_i \leftarrow ( ) \), \( F_r \leftarrow ( ) \) (empty tuples)
2: \( U \leftarrow Q \)
3: while \( i \leq n \) do
4: \( T \leftarrow \text{quotient of division with remainder of } U \text{ by } M_i \text{ in } \mathbb{H}[s][t]. \)
5: \( S \leftarrow \text{remainder of division with remainder of } U \text{ by } M_i \text{ in } \mathbb{H}[s][t]. \)
6: \( S_0 \leftarrow \text{coeff}(S, s, 0), \ S_1 \leftarrow \text{coeff}(S, s, 1) \)
7: \( S_{00} \leftarrow \text{coeff}(S_0, t, 0), S_{10} \leftarrow \text{coeff}(S_0, t, 1) \)
8: \( S_{01} \leftarrow \text{coeff}(S_1, t, 0), S_{11} \leftarrow \text{coeff}(S_1, t, 1) \)
9: if \( S_1 = 0 \) then
10: \( F_r \leftarrow \text{concat}(t + S_{10}^{-1}S_{00}, F_r) \) (concatenation of tuples)
11: \( U \leftarrow T(t + S_{10}^{-1}S_{00}) + S_{10} \)
12: else (Splitting Lemma of [17])
13: \( q \leftarrow -S_{10}S_{11}^{-1} \)
14: \( p \leftarrow S_{00} - S_{10}S_{11}^{-1}S_{01} \)
15: if \( p = 0 \) then
16: \( F_r \leftarrow \text{concat}(t + S_{11}^{-1}S_{01}, F_r) \)
17: \( U \leftarrow T(t + S_{11}^{-1}S_{01}) + (s - q)S_{11} \)
18: else
19: \( F_i \leftarrow \text{concat}(F_i, t + S_{01}S_{11}^{-1}) \)
20: \( U \leftarrow (t + S_{01}S_{11}^{-1})^* T + S_{11}(s - (p^{-1}q)^*) \)
21: end if
22: end if
23: \( i \leftarrow i + 1 \)
24: end while
25: return \( F_i, U, F_r \)

We state our results for monic polynomials with respect to the graded lexicographic order. This can be done without loss of generality: If \( Q \in \mathbb{H}[t, s] \) is not monic, we write \( Q = \text{lcm}(Q)Q' \), where \( \text{lcm}(Q) \in \mathbb{H} \) is the leading coefficient of \( Q \), and apply our results to the monic polynomial \( Q' \in \mathbb{H}[t, s] \). If a monic polynomial satisfies the NFC \( QQ^* = PR \) with \( P \in \mathbb{R}[t] \) and \( R \in \mathbb{R}[s] \), we may assume that \( P \) and \( R \) are monic as well. Moreover, if a monic polynomial admits a factorization of the form (5), we may always conclude \( a = 1 \).

**Theorem 3.1.** Let \( Q \in \mathbb{H}[t, s] \) be a non-constant monic bivariate quaternionic polynomial with \( mrpf(Q) = 1 \) satisfying the NFC \( QQ^* = PR \) for \( P \in \mathbb{R}[t], R \in \mathbb{R}[s] \). There exists \( K \in \mathbb{R}[t] \) such that \( KQ \) decomposes into monic univariate linear factors, that is,

\[
KQ = (u_1 - h_1) \cdots (u_k - h_k)
\]

with \( k \in \mathbb{N}, u_i \in \{t, s\} \) and \( h_i \in \mathbb{H} \) for \( i = 1, \ldots, k \).
Proof. For $m, n \in \mathbb{N}_0$ let $(m, n)$ be the bi-degree of $Q$, where $m + n = k$. We prove the statement via induction over $n$. For $n \in \{0, 1\}$ there is nothing to show. Indeed, if $n = 0$, the polynomial $Q$ is an element of $\mathbb{H}[t]$ and we can apply the univariate factorization results stated in Section 2.1. If $n = 1$, it holds that $Q \in \mathbb{H}_1$ and we find a factorization according to Section 2.2. In both cases we obtain the desired result by choosing $K = 1$.

Let us now assume $n \geq 2$. We choose a monic irreducible factor $M \in \mathbb{R}[s]$ of the univariate $s$-factor $R$ in the norm polynomial. We apply division with remainder and obtain polynomials $T, S \in \mathbb{H}[t, s]$ such that
\begin{equation}
Q = TM + S,
\end{equation}
where $S \in \mathbb{H}_1$. If $S = 0$, we have $Q = TM$, a contradiction to $\text{mrpf}(Q) = 1$. Hence $S \neq 0$, and we repeat the computations applied in Section 2.1 and Section 2.2:
\begin{equation}
SS^* = (Q - TM)(Q - TM)^* = QQ^* - QT^*M - TQ^*M + TT^*M^2.
\end{equation}
Since $M$ is a factor of $QQ^*$, each term on the right-hand side of Equation (8) is divisible by $M$. This is only possible if $\deg(M) = 2$ and $SS^* = HM$ for an appropriate univariate polynomial $H \in \mathbb{R}[t]$. Hence the remainder polynomial $S$ satisfies the NFC. We apply Algorithm 1 to $S/\text{mrpf}(S)$ and inductively produce linear $t$-factors on the left-hand side and on the right-hand side of the $s$-factor:
\[
\frac{S}{\text{mrpf}(S)} = (t - h_1) \cdots (t - h_l)(as + b)(t - k_1) \cdots (t - k_r)
\]
with $l, r \in \mathbb{N}_0$ and appropriate quaternions $h_1, \ldots, h_l, a, b, k_1, \ldots, k_r \in \mathbb{H}$. For better readability, we use the following abbreviation: We set $h := -ba^{-1}$ and $G := a(t - k_1) \cdots (t - k_r) \cdot \text{mrpf}(S) \in \mathbb{H}[t]$. We then obtain
\[
S = (t - h_1) \cdots (t - h_l)(s - h)G.
\]
Note that $M = (s - h)(s - h)^*$. Define
\[
K_1^t := (t - h_1) \cdots (t - h_l) \in \mathbb{H}[t] \quad \text{and} \quad K_1 := K_1^t K_1^t\in \mathbb{R}[t].
\]
Then
\[
K_1Q = K_1^tK_1^t(TM + S) = K_1^tMK_1^tT + SK_1^tK_1^t
= (t - h_1) \cdots (t - h_l)(s - h)((s - h)^*K_1^tT + GK_1^tK_1^t)
= Q'.
\]
The polynomial $Q' \in \mathbb{H}_{*(n-1)}$ still satisfies the NFC because the norm polynomial $QQ'^*$ divides $K_1^tQQ^* = K_1^tPR$ with $K_1^tP \in \mathbb{R}[t], R \in \mathbb{R}[s]$.

By induction hypothesis, there exists $K_2 \in \mathbb{R}[t]$ such that $K_2Q'$ admits a univariate factorization. (This is true even if $Q'$ has a non-trivial real polynomial factor, a case which is formally not covered by the induction hypothesis. This factor is negligible by Proposition 2.1.)

---

5. We view divident $Q$ and divisor $M$ as univariate polynomials in $s$, having coefficients in $\mathbb{H}[t]$. The leading coefficient 1 of $M$ is invertible so that division is possible.

6. The polynomial $S/\text{mrpf}(S)$ need not possess any $t$-factor on the left- or right-hand side of the $s$-factor. In this case, $l = 0$ or $r = 0$ and we appeal to the convention that the empty product equals 1.
Define $K := K_2K_1 \in \mathbb{R}[t]$. Then
\[
KQ = K_2(K_1Q) = K_2((t-h_1)\cdots(t-h_l)(s-h)Q')
= (t-h_1)\cdots(t-h_l)(s-h)K_2Q',
\]
which proves the claim. \hfill \square

Remark 3.2. In above proof, we computed a factorization of the remainder polynomial $S = (t-h_1)\cdots(t-h_l)(s-h)G$, where $G \in \mathbb{H}[t]$, and then forced the factor $(t-h_1)\cdots(t-h_l)(s-h)$ to be a left factor of a suitable real multiple of $Q$. Obviously, one may also compute a factorization of the form $S = F(s-k)(t-k_1)\cdots(t-k_r)$, where $F \in \mathbb{H}[t]$, and find a real polynomial multiple of $Q$ admitting a univariate factorization with right factor $(s-k)(t-k_1)\cdots(t-k_r)$.

Example 3.3. Let us precisely investigate the Beauregard polynomial (1) of [1]:
\[
B = (t^2 - i)s^2 + (2jt)s + (i^2 - 1) \in \mathbb{H}_{22} \text{ with } BB^* = (t^4 + 1)(s^4 + 1)
\]
Following the proof of Theorem 3.1, we choose an irreducible factor $M := s^2 + \sqrt{2}s + 1 \in \mathbb{R}[s]$ of $s^4 + 1$. Division with remainder yields a remainder $S \in \mathbb{H}_{s1}$ of the form
\[
S = (\sqrt{2}i + 2jt - \sqrt{2}t^2)s + i(t^2 + 1) - 1 - t^2,
\]
which satisfies the NFC. We compute the following factorization of $S$ via Algorithm 1:
\[
S = \left(t + \frac{-k-j}{\sqrt{2}}\right)\left(s + \frac{1 - i}{\sqrt{2}}\right)\left(j - k - \sqrt{2}t\right).
\]
Define
\[
K' := \left(t + \frac{-k-j}{\sqrt{2}}\right) \quad \text{and} \quad K := K'K'^* = (t^2 + 1).
\]
Then
\[
KB = \left(t + \frac{-k-j}{\sqrt{2}}\right)\left(s + \frac{1 - i}{\sqrt{2}}\right)B'
\]
with $B' \in \mathbb{H}_{s1}$ satisfying the NFC. Algorithm 1 yields one factorization of the form
\[
B' = \left(t + \frac{1+k}{\sqrt{2}}\right)\left(t + \frac{-1+k}{\sqrt{2}}\right)\left(s + \frac{-1+i}{\sqrt{2}}\right)\left(t + \frac{j-k}{\sqrt{2}}\right),
\]
which shows that factorization (2) can be found by means of the multiplication technique of Theorem 3.1.

Remark 3.4. Even though our multiplication technique actually yields a factorization of a real polynomial multiple $KQ$ of $Q$, it is sometimes possible to simplify the real polynomial $K \in \mathbb{R}[t]$. In the first step of the proof of Theorem 3.1, we computed polynomials $K_1 \in \mathbb{R}[t]$ and $Q' \in \mathbb{H}[t,s]$ such that $K_1Q = (t-h_1)\cdots(t-h_l)(s-h)Q'$. It may happen that the polynomials $K_1$ and $Q'$ share a real polynomial factor of positive degree. One may therefore replace both $K_1$ and $Q'$ by $K_1/\gcd(K_1, \operatorname{mrpf}(Q'))$ and $Q'/\gcd(K_1, \operatorname{mrpf}(Q'))$, respectively. By applying this idea in each step of the algorithm, it might be possible to significantly reduce the degree of $K$. This is illustrated in the next example.
Example 3.5. Consider
\[
Q := (i(-3t + 1) + t^2 - t - 2)s^2 \\
+ (i(-t^2 + t + 2) + j(-2t^2 - 2t) + k(2 + 2t) - 3t + 1)s \\
+ i(2t^2 - 2t + 4) + j(-t^2 + 2t - 1) + k(-t^2 - 3) - 2t - 2.
\]
The polynomial satisfies the NFC
\[
QQ' = (t^2 + 1)(t^2 - 2t + 5)(s^2 + 2)(s^2 + 3).
\]
We choose an irreducible factor
\[
s^2 + 3 \in \mathbb{R}[s],
\]
apply division with remainder and find a remainder \(S \in \mathbb{H}_1\) that admits the following factorization:
\[
S = (t - i)
\left(t - \frac{2i}{5} - \frac{4j}{5} + \frac{4k}{5} + \frac{3}{5}\right)
\left(s - \frac{i}{5} - \frac{7j}{5} + k\right)(-i - 2j).
\]
We define
\[
K := (t^2 + 1)\left(t^2 + \frac{6}{5}t + \frac{9}{5}\right)
\]
and obtain
\[
KQ = (t - i)
\left(t - \frac{2i}{5} - \frac{4j}{5} + \frac{4k}{5} + \frac{3}{5}\right)
\left(s - \frac{i}{5} - \frac{7j}{5} + k\right)Q'
\]
for an appropriate polynomial \(Q' \in \mathbb{H}_1\). It turns out that the factor \(t^2 + 1\) is also a factor of \(Q'\), whence multiplication with this factor is redundant and we just have to consider the polynomial
\[
\frac{K}{t^2 + 1} = t^2 + \frac{6}{5}t + \frac{9}{5}.
\]
According to Section 2.2 we find a univariate factorization of \(\frac{Q'}{t^2 + 1}\). Ultimately, we obtain
\[
(9) \quad \left(t^2 + \frac{6}{5}t + \frac{9}{5}\right)Q = (t - i)
\left(t - \frac{2i}{5} - \frac{4j}{5} + \frac{4k}{5} + \frac{3}{5}\right)
\left(s - \frac{i}{5} - \frac{7j}{5} + k\right)
\left(t - \frac{6i}{5} - \frac{8j}{5} - 1\right)
\left(s - \frac{4i}{5} - \frac{3j}{5} - k\right)
\left(t - \frac{2i}{5} - \frac{4j}{5} - \frac{4k}{5} + \frac{3}{5}\right).
\]

The proof of Theorem 3.1 is constructive. This fact enables us an algorithmic formulation of the multiplication technique (Algorithm 2). It relies on the factorization technique of [17] for polynomials in \(\mathbb{H}_1\), which is described in Algorithm 1.

Remark 3.6. Let us continue with a few remarks on Algorithm 2:

(i) Algorithm 2 depends on a tuple \((M_1, \ldots, M_n)\) of irreducible real factors of \(R\). This tuple is unique up to permutation. By choosing different orders of the irreducible factors, we obtain, similar to Remark 2.4, Item i, different real multiples of \(Q\) that admit univariate factorizations. In general, if the polynomials \(M_1, \ldots, M_n\) are pairwise different, we find \(n!\) different univariate factorizations of real multiples of \(Q\).
**Algorithm 2** Factorization by Multiplication with Real Polynomial

**Require:** A non-constant monic polynomial $Q \in \mathbb{R}[t,s]$ with $\text{mrpf}(Q) = 1$, satisfying the NFC $QQ^* = PR$, where $P \in \mathbb{R}[t]$, $R \in \mathbb{R}[s]$.

**Input:** A tuple $(M_1, \ldots, M_n)$ of irreducible polynomials in $\mathbb{R}[s]$ such that $R = M_1 \cdots M_n$.

**Output:** A real polynomial $K \in \mathbb{R}[t]$ and a tuple of univariate linear polynomials $L = (L_1, \ldots, L_k)$ such that $KQ = L_1 \cdots L_k$.

1. $i \leftarrow 1$, $K \leftarrow 1$, $L \leftarrow ()$ (empty tuple)
2. $U \leftarrow Q$
3. while $i < n$ do
4. \hspace{1em} $T \leftarrow$ quotient of division with remainder of $U$ by $M_i$ in $\mathbb{R}[t][s]$
5. \hspace{1em} $S \leftarrow$ remainder of division with remainder of $U$ by $M_i$ in $\mathbb{R}[t][s]$
6. \hspace{1em} Compute a factorization $\frac{S}{\text{mrpf}(S)} = (t-h_{i_1}) \cdots (t-h_{i_t})(s-h_i)(as+b)(t-k_{i_1}) \cdots (t-k_{i_t})$ via Algorithm 1.
7. \hspace{1em} $h_i \leftarrow ba^{-1}$, $G \leftarrow a(t-k_{i_1}) \cdots (t-k_{i_t}) \cdot \text{mrpf}(S)$
8. \hspace{1em} $K_i \leftarrow (t-h_{i_1}) \cdots (t-h_{i_t})(t-h_{i_1})^* \cdots (t-h_{i_t})^*$
9. \hspace{1em} $U \leftarrow (s-h_i)^*(t-h_{i_1})^* \cdots (t-h_{i_t})^*T + GK_i$
10. \hspace{1em} $D \leftarrow \gcd(K_i, \text{mrpf}(U))$
11. \hspace{1em} $K_i \leftarrow K_i/D$, $U \leftarrow U/D$
12. \hspace{1em} $L \leftarrow \text{concat}(L, t-h_{i_1}, \ldots, t-h_{i_t}, s-h_i)$
13. \hspace{1em} $K \leftarrow K_1 \cdot K$
14. \hspace{1em} $i \leftarrow i + 1$
5. end while
16. Compute a factorization $U = (t-h_{n_1}) \cdots (t-h_{n_t})(s-h_n)(t-k_{n_1}) \cdots (t-k_{n_r})$
17. \hspace{1em} via Algorithm 1.
18. return $K, L$

(ii) Obviously, our ideas also work for irreducible $t$-factors of $QQ^*$. We then obtain a polynomial $K \in \mathbb{R}[s]$ such that $KQ$ admits a univariate factorization. If $P = N_1 \cdots N_m$ is a decomposition of the $t$-factor $P$ in the norm polynomial with irreducible factors and if $N_1, \ldots, N_m$ are different in pairs, the algorithm yields $m!$ different univariate factorizations.

(iii) For a polynomial $Q \in \mathbb{H}_{m,n}$ with $\text{mrpf}(Q) = 1$ we find up to $m! + n!$ different univariate factorizations of real multiples of $Q$.

**Example 3.7.** Let us again consider the Beauregard polynomial (1) from [1]. It is of bi-degree $(2,2)$. The multiplication technique yields $2! + 2! = 4$ factorizations of real multiples of the polynomial $B$:

$$(t^2 + 1)B = \left(t + \frac{-k - j}{\sqrt{2}}\right) \left(s + \frac{1 - i}{\sqrt{2}}\right) \left(t + \frac{1 + k}{\sqrt{2}}\right) \left(t + \frac{-1 + k}{\sqrt{2}}\right) \left(s + \frac{-1 + 1}{\sqrt{2}}\right) \left(t + \frac{j - k}{\sqrt{2}}\right).$$
\[(t^2 + 1)B = \left( t + \frac{j + k}{\sqrt{2}} \right) \left( s + \frac{1 + i}{\sqrt{2}} \right) \left( t + \frac{1 - k}{\sqrt{2}} \right) \left( s + \frac{-1 - i}{\sqrt{2}} \right) \left( t + \frac{k - j}{\sqrt{2}} \right)
\]
\[(s^2 + 1)B = \left( s + \frac{-k}{\sqrt{2}} \right) \left( t + \frac{-1 - i}{\sqrt{2}} \right) \left( s + \frac{1 + k}{\sqrt{2}} \right) \left( s + \frac{-1 + k}{\sqrt{2}} \right) \left( t + \frac{1 + i}{\sqrt{2}} \right) \left( s + \frac{j + k}{\sqrt{2}} \right)
\]

4. An A Posteriori Condition for Existence of Factorizations

So far we have just considered univariate factorizations of real multiples of \( Q \), where \( Q \) satisfies the NFC \( QQ^* = PR \) with \( P \in \mathbb{R}[t] \) and \( R \in \mathbb{R}[s] \). We did not yet take the possibility into account that \( Q \) itself admits a univariate factorization. If this is the case, multiplication with a real polynomial is not necessary. An a priori condition for existence of a univariate factorization of \( Q \) is yet unknown. Moreover, if a univariate factorization exists, we do not know how to find it. At least the second issue can be tackled by means of our multiplication technique: According to Remark 3.4, it may sometimes happen that the real polynomial \( K \in \mathbb{R}[t] \) cancels out. We will show that, if a univariate factorization exists, there is a suitable permutation \( (M_1, \ldots, M_n) \) of irreducible \( s \)-factors of \( R \) such that Algorithm 2 yields \( K = 1 \) and a factorization that is equivalent to the given factorization in a sense to be specified.

We proceed by introducing a sensible concept of equivalence of factorizations that will allow us to formulate our statements in a clear and simple way. It identifies factorizations that arise from ambiguities of factorizations of univariate polynomials (c.f. Remark 2.2, Item ??) and from commutation of adjacent \( t \)- and \( s \)-factors:

**Example 4.1.** Because of \((t + i + j)(t - i) = (t + i)(t - i + j)\), the polynomial
\[Q = (s - i)(t + i + j)(t - i)(s - 2i + k)\]
obviously allows a second factorization:
\[Q = (s - i)(t + i)(t - i + j)(s - 2i + k)\]
Moreover, in this special example, we may even write
\[Q = (t + i)(s - i)(t - i + j)(s - 2i + k)\]
since \((t + i)\) and \((s - i)\) commute. We will view all of these factorizations of \( Q \) as equivalent.

**Definition 4.2.** Given a univariate factorization \( Q = (u_1 - h_1) \cdots (u_k - h_k) \) of a monic polynomial \( Q \in \mathbb{H}[t, s] \) with \( u_i \in \{t, s\} \) and \( h_i \in \mathbb{H} \) for \( i = 1, \ldots, k \), we define two elementary operations that again yield a univariate factorization of \( Q \):

(i) Interchange \( u_l - h_l \) and \( u_{l+1} - h_{l+1} \), provided these factors commute.
(ii) Replace the product \((u_l - h_l)(u_{l+1} - h_{l+1})\) by \((u_l - k_l)(u_{l+1} - k_{l+1})\) where \(u_l = u_{l+1}\) and \((u_l - h_l)(u_{l+1} - h_{l+1}) = (u_l - k_l)(u_{l+1} - k_{l+1})\).

Two univariate factorizations of a monic polynomial \(Q \in \mathbb{H}[t, s]\) are called equivalent\(^7\) if they correspond in a sequence of elementary operations.

The second elementary operation replaces a quadratic \(s-\) or \(t\)-factor by its second factorization according to Remark 2.2, Item ii. In \([14, \text{Definition 4}]\) this is called a “Bennett flip” and the explicit formula

\[
k_{l+1} = -(h_l^* - h_{l+1})^{-1}(h_l h_{l+1} - h_l^*), \quad k_l = h_l + h_{l+1} - k_{l+1}
\]

is provided. It is well-known that all factorizations of a univariate quaternionic polynomial can be generated by Bennett flips \([5, 14]\).

Definition 4.2 captures a natural notion for equivalence of factorizations in our context. Nonetheless, we also introduce a stricter concept of equivalence which takes into account the asymmetry of Algorithm 2 with respect to \(s\) and \(t\). Let \(Q \in \mathbb{H}[t, s]\) be a monic polynomial with \(\text{mrpf}(Q) = 1\). Assume that \(Q\) admits two factorizations with univariate linear factors. Write

\[
Q = A_0(s - h_1)A_1(s - h_2)A_3(s - h_3) \cdots A_n(s - h_n)A_n
\]

with monic \(A_i, \tilde{A}_i \in \mathbb{H}[t]\) for \(i = 0, \ldots, n\) and \(h_i, \tilde{h}_i \in \mathbb{H}\) for \(i = 1, \ldots, n\). We use this notation in order to highlight the appearance of the univariate linear \(s\)-factors. The polynomials \(A_i\) and \(\tilde{A}_i\) occur by merging consecutive linear \(t\)-factors. Some of the polynomials \(A_i\) and \(\tilde{A}_i\) may equal 1.

**Definition 4.3.** We call the two factorizations (10) \(t\)-equivalent if

\[
(s - h_i)(s - h_i^*) = (s - \tilde{h}_i)(s - \tilde{h}_i^*)
\]

for all \(i = 1, \ldots, n\). This definition is an equivalence relation on the set of all possible univariate factorizations of \(Q\). Obviously, there is an analogous concept of \(s\)-equivalence of factorizations.

**Proposition 4.4.** Let \(Q \in \mathbb{H}[t, s]\) be a monic polynomial with \(\text{mrpf}(Q) = 1\). Moreover, assume that \(Q\) admits two factorizations of the form (10) which are \(t\)-equivalent according to Definition 4.3. If \(\text{gcd}(A_0 A_0^*, \tilde{A}_0 \tilde{A}_0^*) = 1\), we obtain \(A_0(s - h_1) = (s - h_1)A_0, \tilde{A}_0(s - \tilde{h}_1) = (s - \tilde{h}_1)\tilde{A}_0,\) and \(h_1 = \tilde{h}_1\).

We prove the statement by means of the following technical lemma:

**Lemma 4.5.** Let \(Q \in \mathbb{H}[t, s]\) be a bivariate quaternionic polynomial of the form \(Q = A(s - h)B\) with \(A \in \mathbb{H}[t]\), \(B \in \mathbb{H}[t, s]\) and \(h \in \mathbb{H}\).

The remainder of having divided \(Q\) by \(M := (s - h)(s - h)^*\) equals \(R = A(s - h)C\) for an appropriate \(C \in \mathbb{H}[t]\), that is, \(Q\) and \(R\) share the common left factor \(A(s - h)\).

**Proof.** Let us divide the polynomial \((s - h)B\) with remainder by \(M\). We obtain \((s - h)B = TM + S\) with \(S \in \mathbb{H}_{n, 1}\). Obviously, \((s - h)\) is a left factor of both \(TM\) and \(S\).}

\(^7\)Formally, we consider a univariate factorization to be an \((m+n)\)-tuple of monic linear univariate polynomials, where \((m, n)\) is the bi-degree of \(Q\). The set of all possible univariate factorizations of \(Q\) can then be viewed as a subset of \((\mathbb{H}[t, s])^{m+n}\).
(s − h)B and TM = MT. For this reason, it is also a left factor of S. We write
S = (s − h)C for an appropriate polynomial C ∈ ℍ[t]. Ultimately, we obtain
(11) Q = A(s − h)B = A(TM + S) = A(TM + (s − h)C) = ATM + A(s − h)C.
Since A is a univariate polynomial in ℍ[t], the polynomial A(s − h)C is an element of ℍ_{s+1}. By Equation (11), it turns out to be the unique remainder of having divided Q by M, whence the claim follows.

Proof of Proposition 4.4. We apply division with remainder of Q by (s−h)(s−h)^∗ = (s−h_1)(s−h_1)^∗. According to Lemma 4.5, the remainder polynomial S ∈ ℍ_{s+1} admits two factorizations of the form
(12) S = A_0(s − h_1)B_0 = ˜A_0(s − ˜h_1) ˜B_0,
where B_0, ˜B_0 ∈ ℍ[t]. By [10, Theorem 3.21], this implies A_0(s − h_1) = (s − h_1)A_0 and ˜A_0(s − ˜h_1) = (s − ˜h_1) ˜A_0. Plugging this into (12) we obtain (s − h_1)A_0B_0 = (s − ˜h_1) ˜A_0 ˜B_0. Now h_1 = ˜h_1 by Remark 2.4, Item ii. This concludes the proof.

Proposition 4.6. Two factorizations that are t-equivalent are also equivalent in the sense of Definition 4.2.

Proof. We argue that t-equivalence of the two factorizations (10) indeed implies that they can be converted into each other by computing suitable factorizations of the polynomials A_i, ˜A_i and by commuting neighbouring s- and t-factors: As long as A_0A_0^∗ and ˜A_0 ˜A_0^∗ share common irreducible factors we choose a quadratic irreducible common factor M of A_0A_0^∗ and ˜A_0 ˜A_0^∗ and compute left factors of both A_0 and ˜A_0 with norm M according to Remark 2.2, Item iii. These factors are also left factors of Q and the fact mrpf(Q) = 1 implies M ∤ Q. According to Remark 2.4, Item ii, the respective linear factors are equal.

According to Proposition 4.4, the remaining factors B_0, ˜B_0 of A_0 and ˜A_0, respectively, commute with (s − h_1) = (s − ˜h_1). Now, we apply the same arguments to the new polynomials B_1 := B_0A_1, ˜B_1 := ˜B_0 ˜A_1 and (s − h_2), (s − ˜h_2). Inductively, the claim follows.

Example 4.7. The two factorizations

\[
\left( t - \frac{7i}{5} + \frac{k}{5} \right) \left( t - \frac{3i}{5} + \frac{4k}{5} \right) (s + 2i - 2k)(t + 2j)(s - i - 4j + k)(t + j - 2k)
\]

and

\[
(t - i)(s + 2i - 2k) \left( t - \frac{4i}{3} + \frac{2j}{3} + \frac{4k}{3} \right) (s - i - 4j + k)
\]

\[
\left( t + \frac{14i}{33} + \frac{65j}{33} - \frac{32k}{33} \right) \left( t - \frac{i}{11} + \frac{4j}{11} - \frac{15k}{11} \right)
\]

are t-equivalent and, by Proposition 4.6, also equivalent. The reader is invited to transform them into each other by using only elementary operations according to Definition 4.2.

Example 4.8. The polynomial

(13) \[ Q = (t - i)(t - j)(s - j)(s - i + j)(s - 2k)(t - 1 - j) \]
admits six univariate factorizations arising from the six different factorizations of $(s - j)(s - i + j)(s - 2k)$ according to Section 2.1. None of them are $t$-equivalent. Among these factorizations, two have the left factor $(s - j)$ which commutes with $(t - j)$. Each of them gives rise to a further $t$-equivalent factorization. All eight factorizations are equivalent, showing that the converse of Proposition 4.6 is not true. From Corollary 4.13 below it will follow that the polynomial admits no further factorizations.

The following theorem is the centerpiece of the present section:

**Theorem 4.9.** Let $Q \in \mathbb{H}[t,s]$ be a monic quaternionic polynomial satisfying the NFC $QQ^* = PR$, where $P \in \mathbb{R}[t]$, $R \in \mathbb{R}[s]$, and $\text{mrpf}(Q) = 1$. Moreover, let $R = M_1 \cdots M_n$ be a decomposition of $R$ with monic, quadratic, irreducible factors. If the polynomial $Q$ admits a univariate factorization, there exists a permutation $\sigma \in S_n$ such that Algorithm 2 with input $(M_{\sigma(1)}, \ldots, M_{\sigma(n)})$ yields $K = 1$ and a univariate factorization which is equivalent to the given factorization of $Q$.

**Proof.** By assumption, the polynomial $Q$ decomposes into univariate linear factors. We are interested in the leftmost $s$-factor of this factorization. For this reason, we write

$$Q = (t - h_1) \cdots (t - h_l)(s - h)\tilde{Q}$$

with $l \in \mathbb{N}_0$, $h_1, \ldots, h_l, h \in \mathbb{H}$ and an appropriate polynomial $\tilde{Q} \in \mathbb{H}[t,s]$. (In case $l = 0$, the empty product convention applies.) There exists $k \in \{1, \ldots, n\}$ such that

$$(s - h)(s - h)^* = M_k.$$

We set $\sigma(1) := k$ and apply the first step of Algorithm 2. By Lemma 4.5, the remainder polynomial of having divided $Q$ by $M_{\sigma(1)}$ equals

$$S = (t - h_1) \cdots (t - h_l)(s - h)C$$

for an appropriate $C \in \mathbb{H}[t]$. Following the proof of Theorem 3.1, we have to define

$$K_1 := (t - h_1) \cdots (t - h_l)(t - h_l)^* \cdots (t - h_1)^*$$

and obtain

$$K_1Q = (t - h_1) \cdots (t - h_l)(s - h)Q'$$

with $Q' \in \mathbb{H}[t,s]$. By Equation (14), $(t - h_1) \cdots (t - h_l)(s - h)$ is a left factor of $Q$. Therefore, $K_1$ is a real divisor of $Q'$ (we have $Q' = K_1\tilde{Q}$) and we get rid of this divisor according to Remark 3.4. Replacing $Q$ by $\tilde{Q}$ and proceeding inductively yields the desired factorization of $Q$. \qed

**Remark 4.10.** In contrast to Algorithm 2, our proof of Theorem 4.9 yields precisely the given factorization of $Q$. Algorithm 2 is not deterministic (for example, line 6 leaves us a choice). Hence, its output is not necessarily identical but $t$-equivalent and, by Proposition 4.6, also equivalent to the given factorization of $Q$.

Theorem 4.9 provides an *a posteriori* condition for existence of univariate factorizations. In case of existence of a univariate factorization, at least an equivalent univariate factorization can be found by application of the multiplication technique.
Example 4.11. Consider the polynomial $Q$ from Example 3.5. In Equation (9), we found a factorization of $(t^2 + \frac{5}{2}t + \frac{7}{2})Q$ with univariate linear factors by applying Algorithm 2 with input $(s^2 + 3, s^2 + 2)$. In fact, it turns out that already $Q$ admits a univariate factorization. It can be found by application of Algorithm 2 with input $(s^2 + 2, s^2 + 3)$:

$$Q = (t - i)(s - j + k)(t - 2i - 1)(s - i - j - k).$$

Example 4.12. The Beauregard polynomial $B$ does not admit a factorization with univariate linear factors since it is irreducible in $\mathbb{H}[t, s]$. Nonetheless, non-existence of a univariate factorization also follows from the fact that Algorithm 2 with inputs $(s^2 + \sqrt{2}s + 1, s^2 - \sqrt{2} + 1)$ or $(s^2 - \sqrt{2}s + 1, s^2 + \sqrt{2}s + 1)$ only yields univariate factorizations of $(t^2 + 1)B$ (c.f. Example 3.7).

Corollary 4.13. Let $Q \in \mathbb{H}[t, s]$ satisfy the assumptions of Theorem 4.9. Moreover, let $(m, n)$ with $m, n \in \mathbb{N}_0$ be the bi-degree of $Q$. The polynomial $Q$ may admit up to $k!$ non-equivalent univariate factorizations, where $k := \min(m, n)$. All of them can be found by applying the multiplication technique.

Proof. Let us consider the case $n \leq m$. By Theorem 4.9, any univariate factorization of $Q$ is equivalent to a factorization that can be found by application of Algorithm 2 with suitable input polynomials. However, there exist at most $n!$ different tuples with quadratic, irreducible, real polynomials $(M_1, \ldots, M_n)$, which can be used as input for Algorithm 2. This proves the claim. If $m \leq n$, we interchange $s$ and $t$. □

Remark 4.14. An arbitrary input tuple need not automatically yield a univariate factorization of $Q$. This is only the case if the algorithm produces $K = 1$. Moreover, it may happen that different input tuples of Algorithm 2 give rise to univariate factorizations which are not $t$-equivalent, but still equivalent. Indeed, consider the polynomial $Q$ from Example 4.8. Algorithm 2 with different input tuples yields six different univariate factorizations. All of them are equivalent, demonstrating that the upper bound of Corollary 4.13 need not be strict.

Example 4.15. Consider the polynomial $Q$ from Examples 3.5 and 4.11. By Corollary 4.13, all univariate factorizations are equivalent to the factorization obtained by application of Algorithm 2 with input $(s^2 + 2, s^2 + 3)$. This is the only input tuple which yields a univariate factorization.

5. A Remarkable Example and Future Research

We conclude this article by a remarkable example which shows that the upper bound of Corollary 4.13 is sharp. It also demonstrates applicability of our factorization ideas to mechanism science which is a topic of future research.

Example 5.1. The following polynomial $Q \in \mathbb{H}[t, s]$ admits $2! = 2$ non-equivalent factorizations with univariate linear factors:

$$Q = (t + i + j + 2k)(s + k)(t - i - j)(s + i + j - k)$$

$$= (s + i + j + k)(t + i + j)(s - k)(t - i - j + 2k).$$

Both of them can be found by application of the multiplication technique. To the best of our knowledge, this is the first example of a bivariate quaternionic polynomial with non-equivalent factorizations and without a real polynomial factor of positive degree.
One of the prime applications of quaternions is kinematics. Quaternions can be used to model the special orthogonal group $SO(3)$ and linear quaternionic polynomials parametrize rotations around fixed axes [5]. Thus, the two factorizations in (15) describe, in two ways, a spherical two-parametric motion of a chain of revolute joints. Note that non-equivalence of factorizations is crucial as otherwise the two chains of revolute joints “essentially” coincide by arguments similar to [10].

Quite surprisingly, the two factorizations (15) (and all other similar examples that we know of) can be extended to dual quaternions which allows to extend the spherical chains of revolute joints to spatial mechanisms (c. f. [5]).

The dual quaternions $\mathbb{DH}$ are obtained by adjoining a new element $\varepsilon$ to $\mathbb{H}$ which commutes with everything and squares to zero: $\varepsilon^2 = 0$. The algebra of dual quaternions is isomorphic to the even subalgebra $\mathcal{C}ℓ^{+}_{(3,0,1)}$ of the Clifford algebra $\mathcal{C}ℓ_{(3,0,1)}$, which was introduced in Section 2. The generators of $\mathcal{C}ℓ^{+}_{(3,0,1)}$ are the elements $e_0, e_{12}, e_{13}, e_{14}, e_{23}, e_{24}, e_{34}$ and $e_{1234}$. The isomorphism is given by (c. f. [9, p. 184])

$$
e_0 \mapsto 1, \quad e_{23} \mapsto i, \quad e_{31} \mapsto j, \quad e_{12} \mapsto k,$$

$$-e_{1234} \mapsto \varepsilon, \quad e_{14} \mapsto i\varepsilon, \quad e_{24} \mapsto j\varepsilon, \quad e_{34} \mapsto k\varepsilon.$$

An element $h \in \mathbb{DH}$ can be uniquely written as $h = p + \varepsilon d$ with primal part $p \in \mathbb{H}$ and dual part $d \in \mathbb{H}$.

In order to extend the factorization (15) to $\mathbb{DH}$ we make the ansatz

$$C = G_1 G_2 G_3 G_4 = H_1 H_2 H_3 H_4$$

where

$$
G_1 = t + i + j + 2k + \varepsilon d_1, \quad H_1 = s + i + j + k + \varepsilon f_1, \\
G_2 = s + k + \varepsilon d_2, \quad H_2 = t + i + j + \varepsilon f_2, \\
G_3 = t - i - j + \varepsilon d_3, \quad H_3 = s - k + \varepsilon f_3, \\
G_4 = s + i + j - k + \varepsilon d_4, \quad H_4 = t - i - j + 2k + \varepsilon f_4,
$$

with yet unknown quaternions $d_\ell, f_\ell \in \mathbb{H}$. A linear polynomial $t + p + \varepsilon d \in \mathbb{DH}[t]$ parametrizes a rotation around an arbitrary axis in space if it satisfies the Study condition $pd^* + dp^* = 0$ and $d + d^* = 0$ [8]. Imposing these conditions on each linear factor and augmenting this system of equations with the conditions obtained by comparing coefficients of $s$ and $t$ on both sides of (16) yields a system of 48 linear equations for 32 unknowns. The solution space turns out to be of dimension
Figure 1. A spatial mechanism constructed from the factorizations in Equation (16)

Each of the two factorizations in (16) yields an open chain of revolute joints which can follow the motion parametrized by $C \in \mathbb{DH}[t,s]$. However, this requires synchronization of joints that share the same parameter values $t$ or $s$. In order to avoid this control problem, one can combine the two open chains to obtain a closed-loop spatial mechanism with eight revolute joints (Figure 1; axes are labeled by the factors in (16)) and remarkable properties. As any generic mechanism of this type, it has two degrees of freedom. Its configuration variety contains the motion parametrized by the polynomial $C \in \mathbb{DH}[t,s]$ in a very special way. By construction, locking any of its joints (parametrized by $t$, say) automatically locks every other joint parametrized by $t$. The remaining four joints yield, in any configuration, a closed-loop spatial structure with four revolute joints which one would expect to be rigid but which is movable (via parameter $s$) at any configuration (for any $t$). A closer investigation of this mechanism is on the agenda for future research.

Note that a similar mechanism construction from the polynomial $Q$ in (15) is possible but results in a fairly trivial spherical mechanism with five degrees of freedom whose configuration space contains an open subset of $SO(3)$. This demonstrates the need for extending our results to dual quaternions. Since the algebra of dual
quaternions contains zero divisors and non-invertible elements, factorization theory of bivariate dual quaternionic polynomials will be more involved.

References

[1] Raymond A. Beauregard, *When is $F[x,y]$ a unique factorization domain?*, Proc. Am. Math. Soc. 117 (1993), no. 1, 67–70.

[2] Matteo Gallet, Christoph Koutschan, Zijia Li, Georg Regensburger, Josef Schicho, and Nelly Villamizar, *Planar linkages following a prescribed motion*, Math. Comput. 86 (2016), no. 303, 473–506.

[3] Graziano Gentili and Caterina Stoppato, *Zeros of regular functions and polynomials of a quaternionic variable*, Michigan Math. J. 56 (2008), 655–667.

[4] Basil Gordon and Theodore S. Motzkin, *On the zeros of polynomials over division rings*, Trans. Amer. Math. Soc. 116 (1965), 218–226.

[5] Gábor Hegedűs, Josef Schicho, and Hans-Peter Schröcker, *Factorization of rational curves in the Study quadric and revolute linkages*, Mech. Mach. Theory 69 (2013), no. 1, 142–152.

[6] Gábor Hegedűs, Josef Schicho, and Hans-Peter Schröcker, *Four-pose synthesis of angle-symmetric 6R linkages*, ASME J. Mechanisms Robotics 7 (2015), no. 4.

[7] Liping Huang and Wasin So, *Quadratic formulas for quaternions*, Appl. Math. Lett. 15 (2002), no. 15, 533–540.

[8] Manfred Husty and Hans-Peter Schröcker, *Kinematics and algebraic geometry*, 21st Century Kinematics. The 2012 NSF Workshop, 2012, pp. 85–123.

[9] Daniel Klawitter, *Clifford algebras. geometric modelling and chain geometries with application in kinematics*, Springer Spektrum, 2015.

[10] Johanna Lercher, Daniel F. Scharler, Hans-Peter Schröcker, and Johannes Siegle, *Factorization of quaternionic polynomials of bi-degree $(1,1)$*, 2020.

[11] Zijia Li, Daniel F. Scharler, and Hans-Peter Schröcker, *Factorization results for left polynomials in some associative real algebras: State of the art, applications, and open questions*, J. Comput. Appl. Math. 349 (2019), 508–522.

[12] Zijia Li, Josef Schicho, and Hans-Peter Schröcker, *Spatial straight-line linkages by factorization of motion polynomials*, ASME J. Mechanisms Robotics 8 (2015), no. 2.

[13] Zijia Li, Josef Schicho, and Hans-Peter Schröcker, *Kempe’s universality theorem for rational space curves*, Found. Comput. Math. 18 (2018), no. 2, 509–536.

[14] Zijia Li, Josef Schicho, and Hans-Peter Schröcker, *Kempe’s universality theorem for rational space curves*, Found. Comput. Math. 18 (2018), no. 2, 509–536.

[15] Maplesoft, a division of Waterloo Maple Inc., Maple. Waterloo, Ontario, 2020.

[16] Ivan Niven, *Equations in quaternions*, Amer. Math. Monthly 48 (1941), no. 10, 654–661.

[17] Mikhail Skopenkov and Rimvydas Krasauskas, *Surfaces containing two circles through each point*, Math. Ann. 373 (2019), 1299–1327.