On the decomposition of rational functions

Mohamed Ayad\textsuperscript{a,1}, Peter Fleischmann\textsuperscript{b}

\textsuperscript{a} Université du Littoral, Mathematics, 46 Rue Ferdinand Buisson, 62228 Calais, France
\textsuperscript{b} Institute of Mathematics and Statistics, University of Kent, Canterbury CT2 7NF, UK

Received 2 April 2007; accepted 12 October 2007
Available online 1 November 2007

Abstract

Let \( f := p/q \in \mathbb{K}(x) \) be a rational function in one variable. By Lüroth’s theorem, the collection of intermediate fields \( \mathbb{K}(f) \subseteq L \subseteq \mathbb{K}(x) \) is in bijection with inequivalent proper decompositions \( f = g \circ h \), with \( g, h \in \mathbb{K}(x) \) of degrees \( \geq 2 \). In [Alonso, Cesar, Gutierrez, Jaime, Recio, Tomas, 1995. A rational function decomposition algorithm by near-separated polynomials. J. Symbolic Comput. 19, 527–544] an algorithm is presented to calculate such a function decomposition. In this paper we describe a simplification of this algorithm, avoiding expensive solutions of linear equations. A MAGMA implementation shows the efficiency of our method. We also prove some indecomposability criteria for rational functions, which were motivated by computational experiments.

\( \odot \) 2007 Elsevier Ltd. All rights reserved.

Keywords: Rational function decomposition; Indecomposable rational function; Normal form of a rational function

Introduction

Let \( f := p/q \in \mathbb{K}(x) \) be a rational function in one variable. By Lüroth’s theorem, the collection of intermediate fields \( \mathbb{K}(f) \subseteq L \subseteq \mathbb{K}(x) \) is in bijection with inequivalent proper decompositions \( f = g \circ h \), with \( g, h \in \mathbb{K}(x) \) of degrees \( \geq 2 \). The problem of explicitly finding all these proper decompositions algorithmically has been investigated by many authors such as Barton and Zippel (1985), von zur Gathen and Weiss (1995), Gutierrez et al. (2002) and Zippel (1991). The related problem of polynomial decompositions has been investigated in Barton and Zippel (1985), Kozen and Landau (1989, 1990) and Ayad (2006). In Alonso et al. (1995) an
algorithm is presented to calculate all function decompositions. In this paper we describe a
simplification of this algorithm, avoiding expensive solutions of linear equations. A MAGMA
implementation confirms the efficiency of our method. We also prove some indecomposability
criteria for rational functions, which were motivated by computational experiments.

1. Basic definitions and known results

Let $\mathbb{K}$ be an arbitrary field and $\mathbb{K}(x)$ the field of rational functions over $\mathbb{K}$. It is well known
by Lüroth’s theorem that every intermediate field $\mathbb{L}$ with $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(x)$ is of the form
$\mathbb{K}(f)$ for some $f \in \mathbb{K}(x)$ (see Schinzel (2000)). If $f := \frac{f_2}{f_d} \in \mathbb{K}(x) \setminus \mathbb{K}$ is a non-constant
function with $f_n, f_d \in \mathbb{K}[x]$ coprime, then since $f$ is transcendent over $\mathbb{K}$, the polynomial
$m(y) := f_n(y) - f_d(y)f \in \mathbb{K}(f)[y]$ is irreducible with $x$ as a zero. Hence

$$[\mathbb{K}(x) : \mathbb{K}(f)] = \max(\deg(f_n), \deg(f_d)) := \deg(f),$$

which one calls the degree of $f$ and denotes by $\deg(f)$.

Let $S := \mathbb{K}(x) \setminus \mathbb{K}$ be the set of non-constant functions. Then $S$ is equipped with a structure
of a monoid, given by the composition $(f \circ g)(x) := f(g(x))$ for $f, g \in S$. This monoid has a
right action on $\mathbb{K}(x)$ given by composition, i.e. for $f, g \in \mathbb{K}(x)$, $h, h' \in S$ we have:

(a) $(f + g) \circ h = f \circ h + g \circ h$;
(b) $(f \cdot g) \circ h = (f \circ h) \cdot (g \circ h)$;
(c) $f \circ (h \cdot h') = (f \circ h) \cdot h'$; and
(d) $x$, the neutral element in $S$, acts as identity operator.

Lemma 1.1. For $g, h \in S$ one has

$$\deg(g \circ h) = \deg(g) \cdot \deg(h).$$

In particular $\circ$ is right-cancellable, i.e. for $f_1, f_2 \in S$, $f_1 \circ h = f_2 \circ h$ implies $f_1 = f_2$.

Proof. The fields $\mathbb{K}(h)$ and $\mathbb{K}(x)$ are isomorphic; hence $[\mathbb{K}(h) : \mathbb{K}(g(h))] = [\mathbb{K}(x) : \mathbb{K}(g(x))]$ and we get

$$[\mathbb{K}(x) : \mathbb{K}(h)] \cdot [\mathbb{K}(x) : \mathbb{K}(g)] = [\mathbb{K}(x) : \mathbb{K}(h)] \cdot [\mathbb{K}(h) : \mathbb{K}(g(h))] = [\mathbb{K}(x) : \mathbb{K}(g \circ h)].$$

If $f_1 \circ h = f_2 \circ h$, then $(f_1 - f_2) \circ h = 0$ and a degree-argument shows that $f_1 - f_2$ is constant,
and hence zero. $\Diamond$

From this it follows easily that the group of units with respect to composition is given by

$$\mathbb{U}_o := \left\{ \frac{ax + b}{cx + d} \middle| \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \right\}.$$ 

Moreover the map

$$\varphi : \text{GL}_2(\mathbb{K}) \to S, \quad \mathcal{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{ax + b}{cx + d}$$

is easily seen to be a homomorphism of monoids and therefore it induces an isomorphism

$$\text{PGL}_2(\mathbb{K}) \cong \mathbb{U}_o.$$
It follows that there is a natural right action of \( GL_2(\mathbb{K}) \) on \( \mathbb{K}(x) \) via field automorphisms over \( \mathbb{K} \), given by \( f^M := f \circ \varphi(M) \). Let \( A := \text{Aut}_\mathbb{K}(\mathbb{K}(x)) \) denote the full group of \( \mathbb{K} \)-automorphisms of \( \mathbb{K}(x) \) and \( \alpha \in \text{Aut}_\mathbb{K}(\mathbb{K}(x)) \) with \( x^\alpha = p(x)/q(x) \) in reduced form. Then \( 1 = \deg(x) = \deg(\alpha(x)) \); hence \( p(x) = ax + b \) and \( q(x) = cx + d \) with \( \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \) and \( f^\alpha(x) = f\left(\frac{ax+b}{cx+d}\right) \) for an arbitrary \( f \in \mathbb{K}(x) \). So the right action of \( G := GL_2(\mathbb{K}) \) on \( \mathbb{K}(x) \) induces canonical isomorphisms

\[
\text{Aut}_\mathbb{K}(\mathbb{K}(x)) \cong \text{PGL}_2(\mathbb{K}) \cong \mathbb{U}_o.
\]

There is also a natural left action of \( GL_2(\mathbb{K}) \) on \( \mathbb{S} \) given by

\[
M \cdot f := \varphi(M) \circ f.
\]

It follows from right-cancellability of \( \circ \) that this action is **fixed-point free**, i.e. \( M \cdot f = f \) for some \( f \in \mathbb{S} \) implies that \( M \) is a scalar matrix in the centre of \( GL_2 \) and therefore acting trivially on \( \mathbb{S} \).

**Definition 1.1.** Let \( f \in \mathbb{S} \). Then we define the following subsets of \( \mathbb{S} \):

\[
R_f := \{h \in \mathbb{S} \mid \exists g \in \mathbb{S} \text{ with } f = g \circ h\};
\]

\[
L_f := \{g \in \mathbb{S} \mid \exists h \in \mathbb{S} \text{ with } f = g \circ h\}.
\]

Note that for \( f = g \circ h \) and \( \alpha \in \mathbb{U}_o \) we have \( f = g \circ \alpha \circ \alpha^{-1} \circ h \), so there is a right action of \( G \) or \( \mathbb{U}_o \) on \( L_f \) and a left action on \( R_f \). The following result shows the significance of these actions:

**Theorem 1.2.** Let \( \mathbb{L}_i = \mathbb{K}(f_i) \) with \( f_i \in \mathbb{S} \) for \( i = 1, 2 \) be two intermediate fields with \( \mathbb{K} \subseteq \mathbb{L}_i \subseteq \mathbb{K}(x) \). Then

(a) \( \mathbb{L}_1 \subseteq \mathbb{L}_2 \) if and only if \( f_2 \in R_{f_1} \).

(b) \( \mathbb{L}_2 = \mathbb{L}_1 \) if and only if \( f_2 = \alpha f_1 \) for some \( \alpha \in G \).

(c) The \( \mathbb{L}_i \) are conjugate over \( \mathbb{K} \), i.e. \( \mathbb{L}_2 = \mathbb{L}_1^\alpha \) for \( \alpha \in \text{Aut}_\mathbb{K}(\mathbb{K}(x)) \) if and only if \( f_2 = u \circ f_1 \circ v \) for some \( u, v \in \mathbb{U}_o \).

(d) Let \( f \in \mathbb{S} \) and let \( R_f / G \) denote the set of left \( G \)-orbits on the set of right factors \( R_f \). The mapping \( G \cdot h \mapsto \mathbb{K}(h) \) is a bijection between \( R_f / G \) and the set of intermediate fields \( \mathbb{K}(f) \subseteq \mathbb{L} \subseteq \mathbb{K}(x) \).

**Proof.** If \( \mathbb{K}(f_1) \subseteq \mathbb{K}(f_2) \) then clearly \( f_1 = g \circ f_2 \) for some \( g \in \mathbb{S} \) which is uniquely determined by the \( f_i \). If \( \mathbb{L}_1 = \mathbb{L}_2 \), then \( g \) is of degree 1. On the other hand, if \( f_1 = g \circ f_2 \) with \( g \in \mathbb{U}_o \), then clearly \( \mathbb{L}_1 = \mathbb{L}_2 \). Now the rest is clear. \( \diamond \)

In dealing with functional decompositions, we will often come across homogenization of functions.

**Definition 1.2.** For \( F \in \mathbb{K}[x] \) define its **homogenization** to be

\[
\mathcal{H}_F(x, y) := y^{\deg(F)} F(x/y) \in \mathbb{K}[x, y].
\]

We will need the following lemma:

**Lemma 1.3.** Let \( R, S, P, Q \in \mathbb{K}[x] \) with \( \gcd(R, S) = \gcd(P, Q) = 1 \). Then the polynomials \( Q, \mathcal{H}_R(P, Q) \) and \( \mathcal{H}_S(P, Q) \) are pairwise coprime.

**Proof.** See Schinzel (2000), p. 18. \( \diamond \)
2. A normal form for subfield generators

Let $\mathbb{L} = \mathbb{K}(f)$ be an intermediate field. Since the generators $f \in \mathbb{S}$ are only determined up to (left) $G$-conjugacy, it may be useful to have a unique normal form for such a generator. This is provided by the next definition and proposition. As a matter of notation $Gf$ will denote the left $G$-orbit of $f$ in $\mathbb{S}$.

**Definition 2.1.** A function $f = \frac{p}{q} \in \mathbb{S}$ is called in normal form or normalized if $p, q \in \mathbb{K}[x]$ are monic and coprime, $p(0) = 0$ and either $\deg(p) > \deg(q)$ or $m := \deg(p) < \deg(q) =: n$ with $q = x^n + q_{n-1}x^{n-1} + \cdots + q_0$ and $q_m = 0$.

The set of all functions in normal form will be denoted by $\mathcal{N}$ or $\mathcal{N}_\mathbb{K}$.

If $f = \frac{p}{q} \in \mathbb{S}$ is in normal form, then the polynomials $p$ and $q$ are coprime and both monic; hence they are uniquely determined.

For example $\frac{x^2}{x+1}$ is a generator in normal form of the field $\mathbb{K}(\frac{x^2}{x+1})$ and $\frac{x}{x^2+1}$ is a generator in normal form of the field $\mathbb{K}(\frac{x}{x^2+1})$. If $f := f_nx^n + \cdots + f_1x + f_0 \in \mathbb{K}[x]$ is of degree $n$, then $\hat{f} := (1/f_0)(f - f_0)$ is a generator in normal form of $\mathbb{K}(f)$.

**Proposition 2.1.** For every $f \in \mathbb{S}$ there is a unique $\hat{f} = p/q$ of normal form inside $Gf$. The polynomials $p$ and $q$ are uniquely determined by $f$ and the properties in the Definition 2.1.

**Proof.** We first show the existence of $\hat{f}$ in $G \cdot f$. So let $f = p/q = \frac{p_{m}x^{m} + \cdots + p_0}{q_nx^n + \cdots + q_0}$ with $\deg(p) = m$, $\deg(q) = n$ and $\gcd(p, q) = 1$. Note that

$$
\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \cdot f = \frac{ap + bq}{cp + dq} 
$$

with $\mathcal{H}_{ax+b}(p, q) = ap + bq$ and $\mathcal{H}_{cx+d}(p, q) = cp + dq$ being coprime, by Lemma 1.3. Firstly assume that $p_0 \neq 0$. Then we can apply a matrix to make $p_0 = 0$: indeed, if $q_0 = 0$ we apply $T := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and if $p_0q_0 \neq 0$ we apply $\begin{pmatrix} -q_0/p_0 & 1 \\ 0 & 1 \end{pmatrix}$. If now the degrees of the numerator and denominator coincide we can use another matrix to cancel the leading term of the denominator. In other words we can assume that $p_0 = 0$, $m \neq n$ and after applying a matrix of the form $\begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$ we will have that $p, q$ are monic, coprime and of different degree. If now $m > n$ we have achieved the normal form and if $m < n$ the function $\begin{pmatrix} 1 \\ -q_m \\ 0 \\ 1 \end{pmatrix} \cdot f = \frac{p}{q - q_mp}$ will be in normal form.

Now we show the uniqueness. Let $f = p/q$ and $\hat{f} := \frac{ap + bq}{cp + dq} = p'/q'$ with

$$
\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 
$$

and suppose that $f$ and $\hat{f}$ are both in normal form. We will show that this implies $b = c = 0 = a - d$, and hence $f = \hat{f}$.

If $d = 0$, then $(ap + bq)q' = p'pc$, so $bq_0q'_0 = 0$ and $b = 0$, a contradiction. Hence $d \neq 0$ and $\hat{f}(0) = bq_0/dq_0 = 0$ implies $b = 0$. We get the equation $apq' = p'(cp + dq)$, which implies $p \mid p'$ $| p$ and therefore $p = p'$, since these are monic polynomials; so $aq' = cp + dq$. Assume $\deg(p) = m > n = \deg(q)$. If $c \neq 0$, then $\deg(q') = \deg(p) = \deg(p')$, a contradiction. Hence...
$c = 0$ and $a = d$. If $\deg(p) = m < n = \deg(q)$, a comparison of coefficients at $x^m$ shows $a \cdot 0 = c + 0$ and again we conclude $c = 0 = a - d$.

If $\hat{f} = p/q$ is the normal form of $f$, then it is clear from the above that the monic polynomials $p$ and $q$ are uniquely determined by $f$. \hfill \diamond

Now Theorem 1.2 and Proposition 2.1 yield:

**Corollary 2.2.** The function $f \mapsto \mathbb{K}(f)$ induces a bijection between the set of non-constant intermediate fields $\mathbb{K} < \mathbb{L} \subseteq \mathbb{K}(x)$ and the set $\mathcal{N}_\mathbb{K}$ of normalized rational functions. If $\mathbb{L} = \mathbb{K}(f)$ with $f \in \mathcal{N}_\mathbb{K}$, we call $f$ the (unique) normalized generator of $\mathbb{L}$.

It is well known that the intermediate field $\mathbb{L}$ contains a non-constant polynomial if and only if it has a polynomial generator. This easily follows from the above, and it turns out, as might be expected, that the unique normalised generator is a polynomial:

**Corollary 2.3.** Let $\mathbb{L} = \mathbb{K}(\hat{f})$ with $\hat{f}$ in normal form. Then $\mathbb{L}$ contains a non-constant polynomial if and only if $\hat{f} \in \mathbb{K}[x]$.

**Proof.** Let $h \in \mathbb{K}[x] \cap \mathbb{L}\backslash \mathbb{K}$ and $\hat{f} = p/q$ in normal form. Then $h = g \circ \hat{f}$ for some $g = u/v$ with coprime polynomials $u$ and $v$. Then $h = \frac{\mathcal{H}_u(p,q) \cdot q^{-\deg(u)}}{\mathcal{H}_v(p,q) \cdot q^{-\deg(v)}}$ and $h q^{\deg(u)} \mathcal{H}_v(p,q) = q^{\deg(v)} \mathcal{H}_u(p,q)$. Now by Lemma 1.3 $\mathcal{H}_v(p,q)$ must be a constant. In general this does not imply that $v \in \mathbb{K}$, but in our situation this follows: let $v = v_s x^s + \cdots + v_0$ with $v_s \neq 0$; then $\mathcal{H}_v(p,q) = v_s p^s + v_{s-1} p^{s-1} q + \cdots + v_0 q^s$. Then $\mathcal{H}_v(p,q) = \mathcal{H}_v(p,q)(0) = v_0 q_0^s$. If $v_0 = 0$, then $v_s p^s \equiv 0 \mod(q)$, in contradiction to $v_s \neq 0$. So $\mathcal{H}_v(p,q) = v_0 q_0^s \neq 0$. If $\deg(p) < \deg(q)$, then

$$0 = \deg(\mathcal{H}_v(p,q)) = \deg(v_0 q_0^s) = \deg(q) \Rightarrow s = 0$$

and if $\deg(p) > \deg(q)$, then

$$0 = \deg(\mathcal{H}_v(p,q)) = \deg(v_s p^s) = \deg(p) \Rightarrow s = 0.$$ 

Hence $v \in \mathbb{K}$. Now it follows that

$$h q^{\deg(u)} v_0 = \mathcal{H}_u(p,q).$$

Since $h \notin \mathbb{K}$, we have that $u \notin \mathbb{K}$, so $\deg(u) > 0$ and Lemma 1.3 yields $q \in \mathbb{K}$, so $q = 1$. \hfill \diamond

3. An indecomposability criterion

Let $f = p/q$ be in the normal form of Definition 2.1. Then $p = x^\ell \tilde{p}$ with $\ell > 0$ and $\tilde{p}, q \in \mathbb{K}[x]$ are monic with non-vanishing constant term. In this section we investigate the possible decompositions of $f$. It turns out that $f$ is indecomposable, whenever $\tilde{p}$ and $q$ are irreducible with $\gcd(\ell, \deg(q)) = 1 = \gcd(\deg(\tilde{p}), \deg(q))$ (see Proposition 3.4). If $\tilde{p}$ and $q \in \mathbb{K}[x]$ satisfy $\tilde{p}(x) = \tilde{p}(x^k)$ and $q = \tilde{q}(x^k)$ for some $1 < k \mid \ell \in \mathbb{N}$ and $\max\{\deg(\tilde{p}), \deg(\tilde{q})\} > 1$, then clearly $f = x^\ell \tilde{p} = x^{\ell/k} \tilde{p} = x^{\ell/k} \tilde{q}(x^k)$ is decomposable. If $\tilde{p}$ and $q$ are both irreducible with $\deg(q) < \deg(p)$, this is the only possibility for $f$ being decomposable (see Proposition 3.4).

**Definition 3.1.** Two polynomials $p, q \in \mathbb{K}[x]$ will be called $\ell$-related, if $p(x) = \tilde{p}(x^k)$ and $q(x) = \tilde{q}(x^k)$ for $\tilde{p}, \tilde{q} \in \mathbb{K}[x]$ and $1 < k \mid \ell$. For $p, q \in \mathbb{K}[x]$, the symbol $p \sim q$ will denote that $p$ and $q$ are associated, i.e. $q = \lambda p$ for some $0 \neq \lambda \in \mathbb{K}$. 

---

We conclude that Proposition 3.1. Let \( \tilde{p} \in \mathbb{K}[x] \) be irreducible and not associated with \( x \); let \( f = \frac{p}{q} \in \mathbb{K}(x) \) with \( p = x^{\ell} \cdot \tilde{p}, \ell > 0, \deg(p) \neq \deg(q), \gcd(p, q) = 1 \); \( f \) is not necessarily in normal form. Assume that \( f = g \circ h \) is a proper decomposition. Then up to equivalence, \( h = r/s \) with \( r = x^k, k \mid \ell \) and \( s(0) \neq 0 \). Moreover \( g := u/v \) with \( u := u_{\mu}x^{\mu} + \cdots + u_{i_0}x^{i_0}, \mu := \deg(u), i_0 := \min(i \mid u_i \neq 0) > 0, v := v_{\nu}x^{\nu} + \cdots + v_0, v := \deg(v), v_0 \neq 0 \), and one of the following holds:

**I.** \( s = \tilde{p}, k\mu = \ell, u = u_{\mu} \cdot x^{\mu}, v = \mu + 1 \) and 
\[
q \sim \mathcal{H}_v(x^k, \tilde{p}) = v_{\mu+1}x^{k(\mu+1)} + \cdots + v_0\tilde{p}^{\mu+1},
\]
\[
\deg(p) < \deg(q) = \begin{cases} (\mu + 1)k = \ell + k & \text{if } k > \deg(\tilde{p}) \\ (\mu + 1)\deg(\tilde{p}) & \text{if } k < \deg(\tilde{p}). \end{cases}
\]

**II.** \( p \sim \mathcal{H}_u(x^k, s), q \sim s^{\mu-\nu}\mathcal{H}_v(x^k, s), \ell = ki_0, v \leq \mu, \) 
\[
\tilde{p} = u_{\mu}x^{k(\mu-i_0)} + u_{\mu-1}x^{k(\mu-i_0-1)}s + \cdots + u_{i_0}s^{\mu-i_0};
\]
\[
q = s^{\mu-\nu} \cdot (v_{\nu}x^{kv} + v_{\nu-1}x^{k(v-1)s} + \cdots + v_0s^{\nu}).
\]

Moreover we have in case II:
\[
\deg(s) < \deg(r) = k \iff \deg(q) < \deg(p) = k\mu \text{ with } \mu > \nu;
\]
\[
\deg(s) > \deg(r) = k \iff \deg(q) = \mu \cdot \deg(s) > \deg(p)
\]

with \( \deg(\tilde{p}) = \deg(s)(\mu - i_0). \)

**Proof.** Assume that \( f = g \circ h \) is a proper decomposition. We can assume that \( g = u/v \) with \( u, v \) coprime and \( h = r/s \) is in normal form so \( r(0) = 0, s(0) \neq 0 \). Using the notation of Definition 1.2 and Lemma 1.3 we have 
\[
p \cdot \mathcal{H}_v(r, s)s^{\mu} = q \cdot \mathcal{H}_u(r, s)s^{\nu},
\]
with \( s, \mathcal{H}_v(r, s), \mathcal{H}_u(r, s) \) pairwise coprime. Hence
\[
\mathcal{H}_u(r, s) \mid p \mid \mathcal{H}_u(r, s)s^{\nu} \text{ and } \mathcal{H}_v(r, s) \mid q \mid \mathcal{H}_v(r, s)s^{\mu}.
\]
Since \( x \) does not divide \( s, x^{\ell} \) must be the exact \( x \)-power dividing \( \mathcal{H}_u(r, s) \); hence \( 0 < i_0 \) and \( r \mid \mathcal{H}_u(r, s) \mid p \).

Assume first that \( r \) is not associated with a power of \( x \). Then \( \tilde{p} \notin \mathbb{K} \) and \( r = x^k \cdot \tilde{p} \) for some \( 0 \leq k \leq \ell \). It follows that 
\[
\mathcal{H}_u(r, s) = u_{\mu} \cdot r^{\mu} + \cdots + u_{i_0} \cdot r_{i_0}^{i_0} s^{\mu-i_0},
\]
with \( \tilde{p}^{i_0} \mid p, \) so \( i_0 = 1 \); hence \( k = \ell \) and \( r = p \sim \mathcal{H}_u(r, s) \). Now Eq. (6) reads \( \mathcal{H}_v(r, s)s^{\mu} \sim qs^{\nu} \); hence \( v \leq \mu \). If \( \deg(r) > \deg(s) \), then \( \mu \cdot \deg(r) = \deg(p) = \deg(r) \), so \( \mu = 1 \geq v \), a contradiction. If \( \deg(r) < \deg(s) \), then \( \deg(r) = \deg(p) = \deg(r) + (\mu - 1)\deg(s) \) and again we get the contradiction \( \mu = 1 \geq v \). 2 We conclude that \( r = x^k \) with \( k \leq \ell \).

Now we assume that \( \mathcal{H}_u(r, s) \) is not associated with \( p \). Then \( \tilde{p} \notin \mathbb{K} \) and
\[
x^k \sim \mathcal{H}_u(r, s) = x^{ki_0} \cdot \varphi
\]

2 Here and in the following note that since \( \deg(r) \neq \deg(s) \), the summands in the \( \mathcal{H}_u(r, s) \) have pairwise different degrees, so \( \deg(\mathcal{H}_u(r, s)) = \mu \cdot \deg(r) \) if \( \deg(r) > \deg(s) \) and \( i_0 \deg(r) + (\mu - i_0)\deg(s) \) if \( \deg(s) > \deg(r) \).
with \( \varphi = u_\mu x^{k(\mu - i_0)} + \cdots + u_{i_0} s^{\mu - i_0} \). But \( x \nmid \varphi \) so \( \varphi \in \mathbb{K} \) and since \( \deg(r) \neq \deg(s) \), we conclude that \( \mu = i_0 \) and \( u = u_\mu x^\mu \) with \( k\mu = \ell \). Now Eq. (6) reads \( \tilde{p} \mathcal{H}_v(r, s)^{s_\mu} \sim q s^v \); hence \( \tilde{p} \mid s \) and \( v > \mu \). But \( s^{\nu - \mu} \nmid \tilde{p} \); hence \( \tilde{p} = s, v = \mu + 1 \) and \( \deg(\tilde{p}) \neq k \). It follows that \( q = \mathcal{H}_v(x^k, \tilde{p}) \) with \( \deg(q) = (\mu + 1)k = \ell + k > \deg(p) \) if \( k > \deg(\tilde{p}) \) and
\[
\deg(q) = (\mu + 1)\deg(\tilde{p}) \text{ if } k < \deg(\tilde{p}).
\]
Note that
\[
k < \deg(\tilde{p}) \iff \ell < \deg(\tilde{p})\mu \iff \ell + \deg(\tilde{p}) < (\mu + 1)\deg(\tilde{p}),
\]
and hence \( \deg(q) > \deg(p) \) in both cases. Now we assume that \( p \sim \mathcal{H}_u(r, s) = u_\mu \cdot x^{k\mu} + \cdots + u_{i_0} \cdot x^{k i_0} s^{\mu - i_0} \) with \( \ell = i_0k \) and
\[
\tilde{p} \sim u_\mu \cdot x^{k(\mu - i_0)} + \cdots + u_{i_0} \cdot s^{\mu - i_0}.
\]
Then Eq. (6) implies that \( v \leq \mu \) and
\[
q \sim \mathcal{H}_v(r, s)^{s^{\mu - v}} = s^{\mu - v}(v_\nu \cdot x^{k\nu} + \cdots + v_0 \cdot s^\nu)
\]
with \( v_0 \sim q(0) \neq 0 \). If \( k > \deg(s) \), then \( \deg(q) = k\nu + \deg(s)(\mu - \nu) < k\mu = \deg(p) \) and \( \mu > v \). If \( k < \deg(s) \), then
\[
\deg(q) = \mu \cdot \deg(s) > \mu \cdot \deg(s) + i_0(k - \deg(s)) = \deg(s)(\mu - i_0) + i_0k = \deg(p),
\]
and \( \deg(\tilde{p}) = \deg(s)(\mu - i_0) \). \( \diamond \)

**Remark 3.2.** It is straightforward to construct decomposable examples for each of the situations described in Proposition 3.1:

I. : This case can be realized for any given irreducible polynomial \( \tilde{p} \in \mathbb{K}[x] \). Indeed, \( s = \tilde{p} \) is already determined. Now let \( k \in \mathbb{N} \) be any positive integer different from \( \deg(\tilde{p}) \) and set \( r := x^k \) to determine \( h := r/s \), define \( \ell := k \cdot \mu \) for some \( \mu \in \mathbb{N} \) and set \( u := u_\mu x^\mu \). For any \( v := \nu_\mu x^{\mu + 1} + \cdots + v_0 \in \mathbb{K}[x] \) with \( v_\mu \nu_\mu v_0 \neq 0, v_\mu + 1 = 1 \) if \( k > \deg(\tilde{p}) \) and \( v_0 = 1 \) otherwise, the polynomial
\[
q := \mathcal{H}_v(x^k, \tilde{p}) = u_\mu + 1 x^{k(\mu + 1)} + \cdots + v_0 \tilde{p}^{\mu + 1}
\]
is coprime to \( p := x^\ell \tilde{p} \), monic and of degree strictly larger that \( \deg(p) \). Hence the rational functions \( f := \frac{x^\ell \tilde{p}}{q}, h = \frac{x^\ell}{p} \) are reduced and satisfy \( f = g \circ h \) with \( g = \frac{u_\mu x^\mu}{v_\mu} \), where \( u_\mu \) is a suitable scalar.

II. : The occurrence of these cases depends on special properties of \( \tilde{p} \). A necessary condition is that there are positive integers \( k, z \), a polynomial \( s \in \mathbb{K}[x] \) of degree different from \( k \) and scalars \( a_0, a_1, \ldots, a_z \in \mathbb{K} \) such that \( a_0 \cdot a_z \neq 0 \) and \( \tilde{p} \) can be written in the form
\[
\tilde{p} = \sum_{j=0}^{z} a_j \cdot s^j x^{k(z-j)}.
\]
If this is possible, we set \( h := \frac{z^k}{z} \). Now let \( \ell := k \cdot i_0 \) be any multiple of \( k \); set \( \mu := z + i_0 \) and \( p := x^\ell \tilde{p} \). If \( \deg(s) < k \), define \( u := \sum_{j=0}^{z} a_j x^{\mu - j} \) and choose \( \nu < \mu \); if \( \deg(s) > k \) then define \( u := \sum_{j=i_0}^{\mu} a_{\mu - j} x^{\mu - j} \) and choose \( \nu \leq \mu \).

Now search for \( v := \sum_{m=0}^{\nu} v_m x^m \in \mathbb{K}[x] \) with \( v_\nu \neq 0 \neq v_0 \) such that the polynomial
\[
q := \mathcal{H}_v(x^k, s) = s^{\mu - v}(v_\nu x^{k\nu} + v_{\nu - 1} x^{k(\nu - 1)} s + \cdots + v_0 s^v)
\]
is coprime to \( \tilde{p} \). Then \( f = g \circ h \) with \( g := u/v \).
Example 3.3. Let $\mathbb{K} = \mathbb{F}_2$, $\overline{p} := x^3 + x + 1$, $s_1 := x + 1$, $k_1 := 3$, $z := 1$, $a_1 := 1 =: a_0$, $u := x^{i_0}(x + 1)$, $p_1 = x^3i_0(x^3 + x + 1)$, $v := 4 \leq 1 + i_0 = \mu$. Let $v := x^4 + x^3 + x^2 + x + 1$ and

$$q_1 := (x + 1)^{i_0+4}(x^{12} + x^9(x+1) + x^6(x^2 + 1) + x^3(x+1)^3 + x^4 + 1)$$

$$= (x + 1)^{i_0-3}(x^{12} + x^{10} + x^9 + x^8 + x^5 + x^3 + 1).$$

Then $\gcd(q_1, p_1) = 1$ and $f_1 = p_1/q_1 = (u/v) \circ (x^3/(x + 1))$. Let $s_2 = x^3 + 1$, $k_2 := 1$, $\ell = i_0 > 3$, $p_2 := x^{i_0}(x^3 + x + 1)$. Note that $v = 4 < \mu_2 = 1 + i_0$. For $q_2 := (x^3 + 1)^{i_0-3}(x^4 + x^3(x^3 + 1) + x^2(x^6 + 1) + x(x^3+1)+ (x^3+1)^4) =$

$$(x^3 + 1)^{i_0-3}(x^{12} + x^{10} + x^8 + x^7 + x^6 + x^3 + x^2 + x + 1)$$

we have $\gcd(q_2, p_2) = 1$ and $f_2 := p_2/q_2 = g \circ h_2$ with $h_2 = x/(x^3 + 1)$.

Proposition 3.4. Let $\overline{p} \in \mathbb{K}[x]$ be irreducible. Moreover let $\ell > 0$ and $f := p/q = x^{i\overline{p}}/\overline{q}$ be a rational function as in Proposition 3.1, or in normal form. Then $f$ is indecomposable in each of the following cases:

(a) $\deg(q) < \deg(p)$ and $\gcd(\ell, \deg(\overline{p})) = 1$.
(b) $\deg(q) < \deg(p)$, $q$ is irreducible and $\overline{p}$ and $q$ are not $\ell$-related.
(c) $\deg(q) > \deg(p)$, $\gcd(\ell, \deg(q)) \leq \deg(\overline{p})$ and $\gcd(\deg(q), \deg(\overline{p})) = 1$.
(d) $q$ is irreducible of prime degree and $\overline{p}$ and $q$ are not $\ell$-related.
(e) $q$ is irreducible with $\gcd(\ell, \deg(q)) = \gcd(\deg(p), \deg(q)) = 1$.

Proof. Assume $f$ is decomposable. In case (a), Proposition 3.1 shows that we are in situation II with $\deg(s) < k | \gcd(\deg(\overline{p}), \ell) = 1$, which is a contradiction. Assume (b) holds. Again we are in situation II with $\deg(s) < k$; then $\mu > v$ and $s$ divides $q$. If $s \sim 1$, then $1 < k$ and the Eqs. (2) and (3) show that $\overline{p}$ and $q$ are $\ell$-related. Hence $q \sim s \not\in \mathbb{K}$, $\mu = v + 1$ and $kv = 0$, which gives the contradiction $v = 0$ and $\mu = 1$. Assume (c) holds. Then we are in situation I or in situation II with $\deg(s) > k$. Assume I: if $k > \deg(\overline{p})$, then we get the contradiction $k | \gcd(\ell, \deg(q)) \leq \deg(\overline{p})$. Hence

$$k < \deg(s) = \deg(\overline{p}) = \gcd(\deg(q), \deg(\overline{p})) = 1,$$

again a contradiction. So we are in situation II with

$$k < \deg(s) | \gcd(\deg(q), \deg(\overline{p})) = 1.$$

Assume (d) holds. Since $\deg(f) = \max(\deg(p), \deg(q))$, decomposability of $f$ requires $\deg(q) < \deg(p)$ and (b) gives a contradiction. Assume (e) holds. Then $\overline{p}$ and $q$ are not $\ell$-related and by (b) we have $\deg(q) > \deg(p) \geq 1$. This and (c) give the contradiction $0 < \deg(\overline{p}) < 1$. 

Corollary 3.5. Let $x \not\sim \overline{p} \in \mathbb{K}[x]$ be irreducible, $\ell > 0$ and $f := x^{\ell \overline{p}}(x^k)$ with $\overline{p} \in \mathbb{K}[x]$ and $1 < k | \ell$.

Proof. The given condition is equivalent to $\overline{p}$ and $q := 1$ not being $\ell$-related. So the claim follows from Proposition 3.4. 

4. A simplified decomposition algorithm

From Theorem 1.2 it is clear that in order to describe the set of intermediate fields containing a given subfield \( \mathbb{L} := \mathbb{K}(f) \), one has to know the set \( R_f \) of right factors of \( f \). Assume we are given \( \mathbb{L} \subseteq \mathbb{T} := \mathbb{K}(h) \) with \( h \in R_f \). In order to express elements of \( \mathbb{L} \) explicitly as functions of \( h \), we also need to know the left factor \( g \in \mathbb{K}(x) \) with \( f = g \circ h \). Recall that \( g \) is uniquely determined by \( f \) and \( h \).

In Alonso et al. (1995) the authors describe algorithms for explicitly calculating this functional decomposition. We will briefly revisit these here with the aim of some simplifications. First we need the following easy lemma, which is also used in constructive proofs of Lüroth’s theorem:

**Lemma 4.1.** Let \( u(x), v(x), F(x) \in \mathbb{K}[x], v(x) \neq 0 \) with \( u(x) \neq \lambda v(x) \) for any \( \lambda \in \mathbb{K} \) and let \( t \) be a new variable, algebraically independent of \( x \). Then \( F \) is not divisible by \( u(x) - tv(x) \) in the polynomial ring \( \mathbb{K}(t)[x] \).

**Proof.** Assume otherwise; then

\[
\varphi(t) \cdot F(x) = A(t, x) \cdot (u(x) - tv(x))
\]

with polynomials \( \varphi \in \mathbb{K}[t] \) and \( A \in \mathbb{K}[t, x] \). Let \( c(x) | \gcd(F, u(x) - tv(x)) \) and assume that \( c(x) \) has positive degree. Then \( u(\eta) = tv(\eta) \) for some root \( \eta \in \overline{\mathbb{K}} \) of \( c \); hence \( t \) is algebraic over \( \mathbb{K} \). This contradiction shows that \( \gcd(F, u(x) - tv(x)) = 1 \). Considering roots of \( \varphi \) and the fact that \( u \) and \( v \) are linearly independent over \( \mathbb{K} \) (and hence over \( \overline{\mathbb{K}} \)), we can also see that \( \gcd(\varphi, u(x) - tv(x)) = 1 \). This contradiction proves the lemma. \( \diamond \)

We will use the following definition of Alonso et al. (1995):

**Definition 4.1.** A bivariate polynomial \( a(y, x) \in \mathbb{K}[y, x] \) is called **near-separate** if it is of the form

\[
a(y, x) = \nabla_{p, q}(y, x) = p(y)q(x) - p(x)q(y) \quad (8)
\]

with coprime polynomials \( p(x), q(x) \in \mathbb{K}[x] \).

The following remarkable theorem has been proved in Alonso et al. (1995).

**Theorem 4.2.** Let \( f = p/q, h = r/s \in \mathbb{S} \) with \( 1 = \gcd(p, q) = \gcd(r, s) \); then the following are equivalent:

1. \( f = g \circ h \) for some \( g \in \mathbb{K}(x) \).
2. \( \nabla_{r,s}(y, x) \) divides \( \nabla_{p,q}(y, x) \) in \( \mathbb{K}[y, x] \).

It remains to find the right factor \( h \). In Alonso et al. (1995) it is proposed to first factorize \( \nabla_{p,q} \) in \( \mathbb{K}[y, x] \) and then check proper factors of the form \( (y - x) \cdot a(y, x) \) for being near-separate, by solving certain linear systems of equations. We will now show that these linear systems can be completely replaced by a short and simple calculation. This is based on the following elementary observation:

**Proposition 4.3.** Let \( a(y, x) = \nabla_{u,v}(y, x) \) for \( u(x), v(x) \in \mathbb{K}[x] \). Then the following identities hold in \( \mathbb{K}[w, x, y, z] \):

\[
a(x, y) = -a(y, x) \quad (9)
a(w, x)a(y, z) + a(w, y)a(z, x) + a(w, z)a(x, y) = 0. \quad (10)
\]
Conversely, assume that \( a(y, x) \in \mathbb{K}[y, x] \) satisfies the identities (9) and (10); then
\[
a(y, x) = \nabla_{u,v}(y, x) \quad \text{with} \quad u(x) := a(x, \alpha) \quad \text{and} \quad v(x) := \frac{a(x, \beta)}{a(\alpha, \beta)} \in \mathbb{K}[x]
\]
for every \( \alpha, \beta \in \mathbb{K} \) with \( a(\alpha, \beta) \neq 0 \).

**Proof.** Eq. (9) is obvious. Eq. (10) is of the form
\[
= A \cdot 0 + D \cdot 0 = 0.
\]
The rest is clear. \( \diamond \)

If \( 0 \neq a(y, x) \) is a divisor of \( \nabla_{p,q} \) with \( f = p/q \), then in order to decide whether \( a(y, x) \) is near-separate, we simply have to check the identities of Lemma 4.3. If they are satisfied and \( a(y, x) \) does not vanish on \( \mathbb{K} \) (e.g. whenever \( \mathbb{K} \) is infinite), then Lemma 4.3 also provides polynomials \( r(x), \, s(x) \in \mathbb{K}[x] \) with \( a(y, x) = \nabla_{r,s} \). However, if \( \mathbb{K} \) is a finite field, it can happen that \( 0 \neq a(y, x) \) is zero on \( \mathbb{K} \). If the identities of Lemma 4.3 hold, we can find \( a(\alpha, \beta) \neq 0 \) with \( \alpha, \beta \in \mathbb{K} \) and solve \( a(y, x) = \nabla_{r,s} \), with \( r, s \in \mathbb{K}[x] \). But it is slightly more subtle to check and construct solutions over the ground field \( \mathbb{K} \) (see Lemma 4.4 and Eq. (15)). For this analysis the following observation is useful:

Let \( \mathbb{K}[y, x]/\mathbb{K}^* \) denote the set of bivariate polynomials modulo constants. Then the function \( \nabla : \mathbb{S} \rightarrow \mathbb{K}[y, x]/\mathbb{K}^* \), mapping the reduced expression \( f = p/q \) to the class \( [\nabla_{p,q}] \), is constant on left \( G \)-orbits: indeed for \( M = \begin{pmatrix}a & b \\ c & d \end{pmatrix} \in \text{GL}_2 \) we have \( M \circ f = \frac{ap+bq}{cp+dq} \) with
\[
\nabla_{ap+bq,cp+dq} = \text{det}(M) \cdot \nabla_{p,q}.
\]

**Theorem 4.4.** Let \( 0 \neq a(y, x) \in \mathbb{K}[y, x] \) with no univariate factors. Then the following are equivalent:

1. \( a(y, x) = \nabla_{u,v} \) for two polynomials \( u(x), \, v(x) \in \mathbb{K}[x] \).
2. There are \( \alpha, \beta \in \mathbb{K} \) such that \( a(0, \alpha) \neq 0 \) and \( a(y, x) = \nabla_{r,s_{\alpha,\beta}} \) with \( r(x) := a(x, 0) \) and \( s_{\alpha,\beta}(x) := \frac{a(\alpha, x)}{a(\alpha, 0)} + \beta \cdot r(x) \in \mathbb{K}[x] \).

Assume that 1 or 2 holds and let \( r, s \in \mathbb{K}[x] \) with
\[
a(y, x) = \nabla_{r,s}.
\]

Then the total set of solutions \( s' \in \mathbb{K}[x] \) of Eq. (13) with fixed \( r \) consists of all polynomials of the form \( s'(x) = s(x) + c \cdot r(x) \) with \( c \in \mathbb{K} \).

For any two pairs of solutions \( (u(x), \, v(x)), \, (w(x), \, t(x)) \) of Eq. (13), the corresponding functions \( h := u/v \) and \( h' := w/t \) are equivalent, i.e. \( h' = M \circ h \) with \( M \in \text{GL}_2(\mathbb{K}) \).

**Proof.** 2 \( \Rightarrow 1 \) is obvious.

\( 1 \Rightarrow 2 \): By the assumption on \( a(y, x) \), the polynomials \( u, v \) must be coprime. Hence the vector \( (u(0), v(0))^{tr} \) is non-zero. Since \( \text{SL}_2 \) acts transitively on non-zero vectors, we can find \( M \in \text{SL}_2(\mathbb{L}) \) such that \( M \cdot (u(0), v(0))^{tr} = (0, 1)^{tr} \). Now Eq. (12) shows that \( a(y, x) = \nabla_{r,s} \) with \( r(0) = 0, \, s(0) = 1 \) and \( r/s = M \circ u/v \). It follows that \( r(x) = a(x, 0) \neq 0 \) and we can choose \( \alpha \) as above. Now \( a(\alpha, x) = a(\alpha, 0) s(x) - r(x) s(\alpha) \); hence \( s(x) = \frac{a(\alpha, x)}{a(\alpha, 0)} + \beta r(x) \) with \( \beta := \frac{s(\alpha)}{a(\alpha, 0)} \).
Assume now that 1 and 2 hold. The operator $\nabla_{u,v}$ is bilinear in both arguments and $\nabla_{r,r} = 0$. It follows that for fixed $r$, any solution $s$ and $c \in K$, the combination $s + cr$ is again a solution of Eq. (13). On the other hand, if $\nabla_{r,s_0} = 0$ with $s_0 \in K[x]$, then $s_0(x) = c \cdot r(x)$ for $c = s_0(\gamma) / r(\gamma)$ with suitable $\gamma \in K$. Hence $c \in K \cap K(x) = K$. So the set of all solutions with fixed numerator $r$ is as described above.

Let $(u,v), (w,r)$ be arbitrary solutions with corresponding functions $h$ and $h'$. As in the beginning of this proof we can find elements $M, M' \in \text{SL}_2(K)$ with $M \circ h = \frac{\xi}{r}, M' \circ h' = \frac{\xi'}{r}$ and $r(x) = a(x, 0), s, s' \in K[x]$ with $s(0) = s'(0)$. From the above we know that $s' = s + c \cdot r$ for suitable $c \in K$; hence $r/s'$ and $r/s$ are equivalent and so are $h'$ and $h$.

Now we assume that $K = \mathbb{F}_q$, a finite field of size $q = p^s$. Let $0 \neq a(y, x) \in K[y, x]$ have no univariate factors and suppose it satisfies the identities of Lemma 4.3, but vanishes on $K^2$. If $a(y, x)$ is a divisor of $\nabla_{p,q}$ with normalized $f = p(x)/q(x) \in K(x)$, then this implies that $p(x)$ and, hence, $f$ vanish on $K$, e.g. $f = \frac{x^2 + q}{x^3 + x + 1} \in \mathbb{F}_3(x)$.

Assume $a(\alpha, 0) \neq 0$ with $\alpha \in \overline{K}$, then $r := a(x, 0)$ and $s_\alpha := \frac{a(\alpha, x)}{a(\alpha, 0)}$ are solutions of Eq. (13). Clearly $r \in K[x]$, but $s_\alpha \in \overline{K}[x]$. By Lemma 4.4, there is a solution $s \in K[x]$ if and only if we can find $\beta \in K$ such that

$$s_\alpha(x) + \beta \cdot r(x) \in \mathbb{F}_q[x].$$

Let $s_\alpha(x) = a_{m}x^m + \cdots + a_1x + 1$, with $a_i \in \mathbb{F}_q$ and $r(x) = a_mx^m + \cdots + a_1x$ with $a_i \in \mathbb{F}_q$ and $m \geq \text{max}$ the maximum of both degrees. Such an element $\beta$ satisfying Eq. (14) exists if and only if $a_i + \beta \cdot a_i \in \mathbb{F}_q$, for all $i = 1, \ldots, m$. This is equivalent to

$$\beta^q - \beta = \frac{a_i - a_i^q}{a_i} =: \gamma \quad \text{for all } i \text{ with } a_i \neq 0 \text{ and } a_i \in \mathbb{F}_q, \quad \text{for all } i \text{ with } a_i = 0.$$  

These conditions are easily verifiable and, if they are met, we can take $\beta$ to be a root of $x^q - x - \gamma$.

**Example 4.5.** Let $K := \mathbb{F}_2$ and $f := (x^4 + x^2)/(x^2 + x + 1)$. Then we get the factorization $f := (x^2 + x) \circ \frac{x^2}{x^2 + 1}$; however the function Nearsep() needs to extend the field to $\mathbb{F}_4$ along the way (see Algorithm 2, Section 6).

## 5. Complete decompositions, intermediate fields and examples

In this section we describe a MAGMA implementation of an algorithm which determines all fields $L$ with $K(f) \subseteq L \subseteq K(x)$.

A sequence $g := (g_m, g_{m-1}, \ldots, g_1)$ of elements $g_i \in K(x)$ with $f = g_m \circ g_{m-1} \circ \cdots \circ g_1$ and $\deg(g_i) \geq 2$ is called a decomposition of $f$. Two decompositions $g := (g_m, g_{m-1}, \ldots, g_1)$ and $h := (h_n, h_{n-1}, \ldots, h_1)$ of $f$ are called equivalent if $m = n$ and there are units $\alpha_1, \ldots, \alpha_m \in \mathbb{U}_x$ such that

$$g_m = h_n \circ \alpha_{m-1}, g_{m-1} = \alpha_m \circ h_{m-1} \circ \alpha^{-1}_{m-2}, \ldots,$$

$$g_1 = \alpha_1 \circ h_1 \circ \alpha_{1-1}^{-1}, \ldots, g_1 = \alpha_1 \circ h_1.$$

The decomposition $g$ is called a full decomposition if all factors $g_i$ are indecomposable and it is called normal if all factors $g_{m-1}, \ldots, g_1$, with the possible exception of $g_m$, are in normal form. It follows from Definition 2.1 that for every decomposition $g$ of $f$ there is a unique normal one which is equivalent to $g$. 
For the decomposition $g$ of $f$ and $i = 1, \ldots, m$ define $\widetilde{g}_i := g_i \circ g_{i-1} \circ \cdots \circ g_1$ and the associated sequence of proper intermediate fields

$$S_g := (\mathbb{L}_{m-1}, \ldots, \mathbb{L}_i, \ldots, \mathbb{L}_1) \text{ with } \mathbb{K}(f) < \mathbb{L}_i := \mathbb{K}(\widetilde{g}_i) < \mathbb{K}(x).$$

It follows directly from Theorem 1.2 that for two decompositions $g, h$ of $f$ we have $S_g = S_f$ if and only if $g$ and $f$ are equivalent and that $S_g$ is a maximal sequence of proper intermediate fields if and only if $g$ is a full decomposition. In other words, the set of maximal sequences of proper intermediate fields between $\mathbb{K}(f)$ and $\mathbb{K}(x)$ is in bijection with the set of all normal, full decompositions of $f$.

For $h := u/v$ in the reduced expression define $\nabla_h$ to be the class $[\nabla_{u,v}] \in \mathbb{K}[y, x]/\mathbb{K}^*$. We define divisibility of classes $[q], [r] \in \mathbb{K}[y, x]/\mathbb{K}^*$ in the obvious way, i.e. $[q] | [r]$ iff $q \mid r$ in $\mathbb{K}[y, x]$. Then, due to Theorem 4.2 we have

$$f = g_m \circ g_{m-1} \circ \cdots \circ g_1 \iff \nabla_{\widetilde{g}_1} | \nabla_{\widetilde{g}_2} | \cdots | \nabla_{\widetilde{g}_m} = \nabla_f,$$

and $g$ is a full decomposition of $f$ if and only if for every $i = 1, \ldots, m - 1$ there are no proper near-separate divisors “between” $\nabla_{\widetilde{g}_i}$ and $\nabla_{\widetilde{g}_{i+1}}$. In other words, there is a bijection between the set of intermediate fields $\mathbb{L}_i = \mathbb{K}(\widetilde{g}_i)$ and the set of near-separate divisors $\nabla_{\widetilde{g}_i}$ of $\nabla_f$. Using the function $\text{Nearsep}()$, one can easily produce a complete list of these, once the full factorization of $\nabla_f$ is known.

Example 5.1. Let $\mathbb{K} = \mathbb{Q}$, $f := \frac{x^{16} + 2x^{12} + x^8}{x^{24} - 2x^{12} + 1}$. MAGMA produces the following list of irreducible factors with multiplicities of $\nabla_f$:

$$\langle x - y, 1 \rangle, \langle x + y, 1 \rangle, \langle x \cdot y - 1, 1 \rangle, \langle x \cdot y + 1, 1 \rangle, \langle x^2 + y^2, 1 \rangle,$$

$$\langle x^2 \cdot y^2 + 1, 1 \rangle, \langle x^8 \cdot y^4 + x^8 \cdot y^4 + x^4 \cdot y^8 + x^4 + y^4, 1 \rangle,$$

$$\langle x^8 \cdot y^8 + x^8 \cdot y^8 + x^4 \cdot y^8 + x^4 + y^4 + 1, 1 \rangle.$$

Using $\text{Nearsep}()$ we obtain the exponent vectors (in terms of the above list) of all near-separate divisors of $\nabla_f$, together with corresponding generators of intermediate fields:

$$[1, 0, 0, 0, 0, 0, 0, 0], \quad x,$$
$$[1, 1, 0, 0, 0, 0, 0, 0], \quad x^2,$$
$$[1, 0, 1, 0, 0, 0, 0, 0], \quad x/(x^2 + 1),$$
$$[1, 0, 0, 1, 0, 0, 0, 0], \quad x/(x^2 - 1),$$
$$[1, 1, 1, 1, 0, 0, 0, 0], \quad x^2/(x^4 + 1),$$
$$[1, 1, 0, 0, 1, 0, 0, 0], \quad x^4,$$
$$[1, 0, 0, 0, 1, 0, 0, 0], \quad x^2/(x^4 - 1),$$
$$[1, 1, 1, 1, 1, 0, 0, 0], \quad x^4/(x^8 + 1),$$
$$[1, 1, 0, 0, 0, 0, 1, 0], \quad (x^8 + x^4)/(x^{12} - 1),$$
$$[1, 1, 1, 1, 1, 1, 1, 1], \quad (x^{16} + 2x^{12} + x^8)/(x^{24} - 2x^{12} + 1).$$

Recall that $\mathbb{K}(f) \subseteq \mathbb{K}(h) \iff \nabla_h | \nabla_f$; hence the containment relations between subfields are reflected in the reverse “dominance order” of exponent vectors, where $v \prec w \iff v - w$ is non-negative. So $[1, 1, 1, 1, 1, 0, 0, 0] \prec [1, 1, 0, 0, 1, 0, 0, 0]$ indicates that $\mathbb{K}(\frac{x^4}{x^8 + 1}) \subseteq \mathbb{K}(x^4)$ and $[1, 1, 0, 0, 1, 0, 0, 1] \neq [1, 1, 1, 1, 1, 0, 0, 0]$ shows that $\mathbb{K}(\frac{x^4 + x^8}{x^{12} - 1})$ is not contained in $\mathbb{K}(\frac{x^2}{x^4 + 1})$.

The computation was performed in 0.470 CPU seconds on a laptop PC with a Pentium 4/2.00 GHz CPU.
In Alonso et al. (1995), Example 5.4, a non-normalized version of this example was considered. The calculation, performed with MAPLE on a Macintosh SE/30, took 202.53 s for one full decomposition. Since there is more than a decade between the paper Alonso et al. (1995) and our experiments, such comparisons have to be treated with caution. According to Wikipedia (Wikipedia, 2007), Mac Se/30 worked with Motorola 68030, 16 MHz, so the CPU speedup to 2 GHz is by a factor of 125 and our 0.470 CPU seconds should more properly be compared to 202.53/125 = 1.616 “contemporary CPU seconds” (although it should be, also, taken into consideration that the current version of MAPLE is probably more performing than the one used in 1995 by Alonso et al.)

**Example 5.2.** The following example also appears in Alonso et al. (1995), Example 5.1.:

\[
 f := f_n/f_d
\]

\[
 f_n := -(4x^6 + 9x^5 - 13x^4 - 12x^3 + 29x^2 - 17x - 8)(x^3 + x^2 - 2x + 1)
 \cdot (3x^3 + 5x^2 - 8x - 3)(9x^6 + 29x^5 - 24x^4 - 90x^3 + 39x^2 + 37x + 3);
\]

\[
 f_d := 91x^{18} + 803x^{17} + 1634x^{16} - 4230x^{15} - 16526x^{14} + 5744x^{13} + 61317x^{12} + 6452x^{11} - 117349x^{10} - 23079x^9 + 111529x^8 + 27940x^7 - 34289x^6 - 36809x^5 + 5132x^4 + 11548x^3 + 1021x^2 - 929x - 167.
\]

The normalization of \( f \) is equal to \( N := N_n/N_d \) with

\[
 N_n := x^{18} + 68203/8196x^{17} + 87695/6147x^{16} - 32675/683x^{15} - 3378407/24588x^{14} + 532687/4098x^{13} + 324203/683x^{12} - 1916254/6147x^{11} - 6713321/8196x^{10} + 5584523/8196x^9 + 1543365/2732x^8 - 4842583/6147x^7 + 1155847/8196x^6 + 1528231/8196x^5 - 667808/6147x^4 - 100585/6147x^3 + 136280/6147x^2 + 12775/2732x;
\]

\[
 N_d := x^{17} + 49436/6735x^{16} + 1212/449x^{15} - 592253/6735x^{14} - 59726/449x^{13} + 889368/2245x^{12} + 5126696/6735x^{11} - 2101079/2245x^{10} - 4175731/2245x^9 + 2950617/2245x^8 + 14668796/6735x^7 - 2312663/2245x^6 - 527851/449x^5 + 2211184/6735x^4 + 1919492/6735x^3 - 146716/6735x^2 - 66477/2245x - 8196/2245.
\]

There is a unique full normalized decomposition, which is calculated by our MAGMA implementation in 0.490 s:

\[
 \left[ \begin{array}{c}
 x^3 - 3805/4098x^2 + 9125/32784x \\
 x^2 + 5/12x \\
 x^3 + 4/3x^2 - 7/3x
 \end{array} \right] \cdot \left[ \begin{array}{c}
 x^2 + 515/898x - 17075/64656 \\
 x + 4/15 \\
 x^2 - x - 3
 \end{array} \right] .
\]

(In Alonso et al. (1995) a corresponding MAPLE calculation took 249.23 \( \sim 1.994 = 249.23/125 \).)

**Example 5.3.** Let \( f := (x^4 - 8x)/(x^3 + 1) \). Over the rationals \( f \) has the unique full decomposition

\[
 [(x^2 - 2x)/(x + 1), (x^2 + 4x)/(x + 1)].
\]
The timing for this was 0.016 CPU seconds. Let $\mathbb{K} := \mathbb{Q}(\zeta)$ with $\zeta$ a primitive third root of unity. Then $f$ has the three non-equivalent full decompositions:

$$
\begin{align*}
[(x^2 - 2x)/(x + 1), (x^2 + 4x)/(x + 1)] \\
[(x^2 + (2\zeta + 2)x)/(x - \zeta - 1), (x^2 + (-4\zeta - 4)x)/(x - \zeta - 1)] \\
[(x^2 - 2\zeta x)/(x + \zeta), (x^2 + 4\zeta x)/(x + \zeta)].
\end{align*}
$$

Using the MAGMA implementation of cyclotomic fields, the timing here was 0.187 CPU seconds.

6. Concluding remarks

All algorithms in this paper have been implemented and tested in the computer algebra system MAGMA, version V2.11-6 (Cannon and Playoust, 2007). The following are three examples of functions, in MAGMA pseudo-code, taken from the implementation. A synopsis and the full software can be obtained at http://www.kent.ac.uk/ims/personal/pf10/calais/decomp_synopsis.txt and http://www.kent.ac.uk/ims/personal/pf10/calais/decomp, respectively.

Algorithm 1: Normal form algorithm

Function Normalize()

**Input:** Fct $f = p/q$; // normalized

**Output:** normalized Fct $\hat{f}$, Matrix $M$ with $\hat{f} = M \circ f$.

1. **local** Matrix $M$, $U$, Fct $\hat{f}$, Pol $p$, $q$, Int $m$, $n$;
2. $\hat{f} := f$; $p := \text{Num}(\hat{f})$; $q := \text{Denom}(\hat{f})$; $m := \text{Deg}(p)$; $n := \text{Deg}(q)$;
3. $p_0 := \text{Coeff}(p, 0)$; $q_0 := \text{Coeff}(q, 0)$;
4. if $p_0 \neq 0$ then // want $p_0 = 0$;
5. if $q_0 = 0$ then
6. $M := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $\hat{f} := M \cdot \hat{f}$;
7. else // now $p_0 \cdot q_0 \neq 0$
8. $U := \begin{pmatrix} -q_0/p_0 & 1 \\ 0 & 1 \end{pmatrix}$; $\hat{f} := U \circ \hat{f}$; $M := U \cdot M$;
9. end if;
10. end if; // from now $p_0 = 0$, $q_0 \neq 0$.
11. if $m = n$ then
12. $U := \begin{pmatrix} 1 & 0 \\ -q_0/p_m & 1 \end{pmatrix}$; $\hat{f} := U \circ \hat{f}$; $M := U \cdot M$;
13. end if; // now $p$, $q$ of different degrees.
14. $U := \begin{pmatrix} q_n/p_m & 0 \\ 0 & 1 \end{pmatrix}$; $\hat{f} := U \circ \hat{f}$; $M := U \cdot M$; // make $p, q$ monic;
15. if $m < n$ then
16. \[ U := \begin{pmatrix} 1 & 0 \\ -q_m & 1 \end{pmatrix}; \hat{f} := U \circ \hat{f}; M := U \cdot M; \quad // \text{remove } q_m; \]
17. end if;
18. return \hat{f}, M;
19. end function;

---

**Algorithm 2: Decide near-separability of a and solve** \( a = \nabla_{r,s} \)

**Function** \texttt{Nearsep()}

**Input:** BivPol \( a(y, x); \quad // \text{multiple of } y - x; \)
\( // \text{no univariate factors}; \)

**Output:** Fct \( h; \text{Int bool}; \quad // \text{right factor } h = r/s, \text{if bool} = 1; \)
\( // \text{if } \mathbb{K} \text{ is finite, } h \text{ can be defined in } \)
\( // \text{a suitable finite extension field}. \)
\( \text{bool} = 0, \text{if } a(y, x) \text{ is not near-separate}. \)

1. \texttt{local Fct h; Pol r, s; Int bool; Scalar } \alpha, m; \)
2. \( r := a(x, 0); \)
3. \texttt{find } \alpha \text{ with } r(\alpha) =: m \neq 0; \quad // \text{if } \mathbb{K} \text{ is finite, we need to search in extension fields} \)
4. \( s(x) := \frac{1}{m} a(\alpha, x); \)
5. \texttt{if } a(y, x) = \nabla_{r,s} \text{ then return } h := \frac{r}{s}, 1; \text{ end if; } \)
6. \texttt{return } h := x, 0; \quad // a \text{ is not near-separate, return } \text{function} ‘x’ \quad \text{and the boolean ‘0’}. \)
7. end function;

---

**Algorithm 3: Compute the unique left factor** \( g \) \textit{with } \( f = g \circ h \)

**Function** \texttt{Leftfactor()}

**Input:** Fct \( f = p(x)/q(x), h = r(x)/s(x); \quad // \text{reduced, } h \in R_f. \)

**Output:** Fct \( g; \quad // f = g \circ h, \)

1. \texttt{local Fct g; Pol } F, B, C \in \mathbb{K}(x)[y];
2. \( F(x, y) := r(y) - x \cdot s(y); \quad // \text{in } \mathbb{K}(x)[y]; \)
3. \( B(x, y) := p(y) \mod F; C(x, y) := q(y) \mod F; \)
4. \( g(x) := \text{LeadingCoefficient}_y(B)/\text{LeadingCoefficient}_y(D); \)
5. \texttt{return } g(x); \texttt{end function;}\)

---

**References**


Cannon, John, Playoust, Catherine, 2007. Algebraic Programming with Magma I An Introduction to the Magma