Computing restrictions of ideals in finitely generated $k$-algebras by means of Buchberger’s algorithm✩

Thomas Beth, Jörn Müller-Quade, Rainer Steinwandt*

Institut für Algorithmen und Kognitive Systeme, Fakultät für Informatik, Am Fasanengarten 5, Universität Karlsruhe, 76128 Karlsruhe, Germany

Available online 2 November 2005

Abstract

Gröbner bases can be used to solve various algorithmic problems in the context of finitely generated field extensions. One key idea is the computation of a certain kind of restriction of an ideal to a subring. With this restricted ideal many problems concerning function fields reduce to ideal theoretic problems which can be solved by means of Buchberger’s algorithm. In this contribution this approach is generalized to allow the computation of the restriction of an arbitrary ideal to a subring.

© 2005 Elsevier Ltd. All rights reserved.

Keywords: Gröbner bases; Finitely generated function fields

1. Introduction

Buchberger’s algorithm allows in particular for a constructive theory of ideals in polynomial rings, that led to a multitude of applications, one of which will be presented in this contribution. Many computational problems, especially concerning finitely generated field extensions, can be solved by the restriction of specific ideals to rings defined over a subfield. This paper presents a novel algorithm which allows one to restrict an arbitrary ideal $\mathcal{J} = \langle f_1, \ldots, f_s \rangle$ in a residue ring.
class ring $k(\vec{x})[Z_1, \ldots, Z_m]/\langle \vec{q} \rangle$ to a subring $k(\vec{g})[Z_1, \ldots, Z_m]/\langle \vec{q} \rangle$ defined over a subfield $k(\vec{g})$ of $k(\vec{x}) = k(x_1, \ldots, x_n)$, where $\vec{q} \in k(\vec{g})[Z_1, \ldots, Z_m]$. So for the special case $\vec{q} = 0$ we are dealing with a question on subalgebras of the polynomial ring $k(\vec{x})[Z_1, \ldots, Z_m]$. However, in contrast to Kapur and Madlener (1989), Robbiano and Sweedler (1990), for instance, here we do not focus on $k(\vec{x})$-subalgebras of the form $k(\vec{x})[a_1, \ldots, a_r]$ with $a_1, \ldots, a_r \in k(\vec{x})[Z_1, \ldots, Z_m]$; instead we are interested in $k$-subalgebras $k(\vec{g})[Z_1, \ldots, Z_m]$ that are obtained by restricting the field of coefficients $k(\vec{x})$.

Given finitely many generators $f_1, \ldots, f_s$ for an ideal $\mathcal{I} \subseteq k(\vec{x})[Z_1, \ldots, Z_m]/\langle \vec{q} \rangle$, our algorithm computes generators for the ideal $\mathcal{I} \cap k(\vec{g})[Z_1, \ldots, Z_m]/\langle \vec{q} \rangle$; here we identify $k(\vec{g})[Z_1, \ldots, Z_m]/\langle \vec{q} \rangle$ with its image under the natural embedding of $k(\vec{g})[Z_1, \ldots, Z_m]/\langle \vec{q} \rangle$ into $k(\vec{x})[Z_1, \ldots, Z_m]/\langle \vec{q} \rangle$.

An instructive example is minimal polynomials: if one restricts the ideal $\langle Z - \alpha \rangle \subseteq k(\alpha)[Z]$ to $k[Z]$ then $\langle Z - \alpha \rangle \cap k[Z]$ is a principal ideal and a monic generator of this ideal is the minimal polynomial of $\alpha$ over $k$.

This work is motivated by the implications of Buchberger’s algorithm to finitely generated field extensions. Apart from the so-called tag variable approach (Kemper, 1993; Sweedler, 1993), many problems concerning field extensions can be solved by means of ideal restriction. One can employ a correspondence between the lattice of subfields $k(\vec{g})$ of a finitely generated field $k(\vec{x})$ and a lattice of restricted ideals $\mathfrak{P}(\vec{x})/k(\vec{g}) := \langle Z_1 - x_1, \ldots, Z_n - x_n \rangle \cap k(\vec{g})[Z_1, \ldots, Z_n]$. This correspondence allows one to solve many problems concerning field extensions by means of constructive ideal theory and Buchberger’s algorithm (Müller-Quade and Steinwandt, 1999, 2000). Many characteristic properties of subfields directly translate to properties of the restricted ideals. For example, the transcendence degree of the extension $k(\vec{g}) \leq k(\vec{x})$ equals the dimension of the ideal $\mathfrak{P}(\vec{x})/k(\vec{g})$, the polynomial $n(Z_1, \ldots, Z_n) - n(\vec{g})d(Z_1, \ldots, Z_n)$ reduces to zero modulo a Gröbner basis of $\mathfrak{P}(\vec{x})/k(\vec{g})$ iff $\frac{n(\vec{g})}{d(\vec{x})}$ is contained in $k(\vec{g})$, field extensions correspond to ideal inclusions, and the coefficients of a reduced Gröbner basis of $\mathfrak{P}(\vec{x})/k(\vec{g})$ yield a canonical generating set of the field $k(\vec{g})$.

For the specific ideals used in the above correspondence the restriction problem was solved in Müller-Quade and Steinwandt (1999, 2000). But the more general question of restricting an arbitrary ideal $\mathcal{I}$ to a finitely generated subfield was posed in Müller-Quade and Beth (1998a).

In Müller-Quade and Beth (1998a) an algorithm to compute a generating set for the intersection of finitely generated extension fields has been sketched. Here we give a (counter-) example which shows that this algorithm does not work in general. In this approach to solve the field intersection problem the constructive restriction of more general ideals was introduced and used as a subroutine.

The purpose of the present paper (see Steinwandt and Müller-Quade (2000) and Beth et al. (2002) for preliminary versions) is twofold. First we will solve the general ideal restriction problem and second we will show that the algorithm of Müller-Quade and Beth (1998a) cannot in all cases calculate the intersection of two finitely generated fields.

Even though the general ideal restriction problem can be solved by Gröbner basis techniques, including computing the field of definition of an ideal, ideal saturation, primary decomposition, and ideal membership, the general field intersection problem remains an interesting open problem to solve.

2. Restricting ideals in finitely generated $k$-algebras

To avoid ambiguities, we start by summarizing the notation that we use in what follows.
For $K$ a field we write $K[\tilde{Z}] := K[Z_1, \ldots, Z_m]$ for the polynomial ring in the indeterminates $Z_1, \ldots, Z_m$ over the field (of coefficients) $K$.

For $K$ a field, $\mathfrak{I} \subseteq K[\tilde{Z}]$ an ideal, and $q \in K[\tilde{Z}]$ we denote by $\mathfrak{I} : q^\infty$ the saturation of $\mathfrak{I}$ w.r.t. $q$, i.e.,

$$\mathfrak{I} : q^\infty = \{ p \in K[\tilde{Z}] : q^\mu \cdot p \in \mathfrak{I} \text{ for some } \mu \in \mathbb{N} \}.$$ 

For indeterminates $X_1, \ldots, X_u$ we denote by $T(\tilde{X})$ the set of terms in $\tilde{X}$, i.e., the set of all products $\prod_{i=1}^u X_i^{v_i}$ with $v_1, \ldots, v_u \in \mathbb{N}_0$.

$k(\bar{x}) := k(x_1, \ldots, x_n)$ denotes a finitely generated (not necessarily algebraic) extension field of some ground field $k$. We assume computations in $k(\bar{x})$ to be effective and that $k(\bar{x})$ is represented as the quotient field of $k[X_1, \ldots, X_n]/(b_1, \ldots, b_t)$ where $b$ is a finite system of generators of the ‘ideal of relations’

$$\Psi(\bar{x})/k := \{ a(\bar{x}) \in k[\tilde{X}] : a(\bar{x}) = 0 \}.$$ 

$k(\bar{g}) := (g_1, \ldots, g_r)$ denotes a subfield of $k(\bar{x})$ generated over the ground field $k$ by $g_1, \ldots, g_r \in k(\bar{x})$. Note that the $g_i$’s can in general not be expressed as polynomials in $\bar{x}$, and fractions are needed.

For an ideal $\mathfrak{I} \subseteq k(\bar{x})[\bar{Z}]$ we denote by $k_\mathfrak{I}$ the minimal field of definition of $\mathfrak{I}$. In other words, $k_\mathfrak{I}$ is the field generated over the prime field of $k$ by the coefficients occurring in a reduced Gröbner basis of $\mathfrak{I}$ (cf. Müller-Quade and Rötteler, 1998; Robbiano and Sweedler, 1998).

$\Omega := \langle q_1, \ldots, q_v \rangle \subseteq k(\bar{x})[\bar{Z}]$ denotes an arbitrary ideal whose minimal field of definition $k_\Omega$ is contained in $k(\bar{g})$. By computing a reduced Gröbner basis of $\Omega$ a generating set $B \subseteq k_\Omega[\bar{Z}]$ of $\Omega$ can be derived, we assume w.l.o.g. $q_1, \ldots, q_v \in k(\bar{x})[\bar{Z}] \subseteq k(\bar{g})[\bar{Z}]$.

By $\pi_g : k(\bar{g})[\bar{Z}]/(\bar{q}) \longrightarrow k(\bar{g})[\bar{Z}]/(\bar{q})$ and $\pi_x : k(\bar{x})[\bar{Z}] \longrightarrow k(\bar{x})[\bar{Z}]/(\bar{q})$ we denote the canonical residue class epimorphisms.

$\iota : \langle k(\bar{g})[\bar{Z}]/(\bar{q}) \rightarrow k(\bar{x})[\bar{Z}]/(\bar{q})$ denotes the natural $k(\bar{g})$-algebra monomorphism that maps $\pi_g(Z_i)$ to $\pi_x(Z_i)$ ($i = 1, \ldots, m$). In particular, we can identify $k(\bar{g})[\bar{Z}]/(\bar{q})$ with the subring $\iota(k(\bar{g})[\bar{Z}]/(\bar{q}))$ of $k(\bar{x})[\bar{Z}]/(\bar{q})$.

With this notation we can summarize the computational task to be solved in this section as follows.

Given a finite basis $f_1, \ldots, f_s$ of an ideal $\mathfrak{I} = \langle f_1, \ldots, f_s \rangle \subseteq k(\bar{x})[\bar{Z}]/(\bar{q})$, compute a finite generating set of the restricted ideal $\mathfrak{I} \cap \iota(k(\bar{g})[\bar{Z}]/(\bar{q}))$.

To compute this restriction, in a first step we determine a finite basis $\bar{p} \subseteq k(\bar{g})[\bar{X}]$ of the ideal

$$\Psi(\bar{x})/k(\bar{g}) := \{ a(\bar{X}) \in k(\bar{g})[\bar{X}] : a(\bar{x}) = 0 \} = \langle X_1 - x_1, \ldots, X_n - x_n \rangle \cap k(\bar{g})[\bar{X}]$$

This ideal will be a tool to compute the restriction of an ideal $\mathfrak{I}$; to this end we need the ideal $\Psi(\bar{x})/k(\bar{g})$ in the $\bar{X}$ variables. In the introduction this ideal was formulated in the $\bar{X}$ variables, as it was used as an example for a restriction.

The ideal $\Psi(\bar{x})/k(\bar{g})$ will be important later, because modulo $\Psi(\bar{x})/k(\bar{g})$ a polynomial $c(\bar{X})$ reduces to $c(\bar{x})$ iff $c(\bar{x})$ is contained in $k(\bar{g})$. We will later define an ideal $\tilde{\mathfrak{I}}$ which contains all “denominator free” elements of $\mathfrak{I}$ where the field elements $\bar{x}$ are replaced by variables $\bar{X}$. This ideal $\tilde{\mathfrak{I}}$ will also contain $\Psi(\bar{x})/k(\bar{g})$ and we can, by computations within the ideal $\tilde{\mathfrak{I}}$, “replace” coefficients $c(\bar{X})$ by $c(\bar{x})$ without leaving the ideal iff $c(\bar{x})$ is contained in $k(\bar{g})$. Exactly the elements of $\tilde{\mathfrak{I}}$ which correspond to elements outside of the restriction to be computed still contain coefficients in the variables $\bar{X}$ and can be removed from $\tilde{\mathfrak{I}}$ by a simple variable elimination.
The ideal \( \mathfrak{P}_{(\tilde{g})}/k(\tilde{g}) \) can be computed by means of the following result (see Müller-Quade et al., 1998, Proposition 1).

**Lemma 2.1.** With the above notation let \( g_i = n_i(\tilde{x})/d_i(\tilde{x}) \) with \( n_i, d_i \in \mathbb{K}[\tilde{x}] \) and \( d_i(\tilde{x}) \neq 0 \) (\( 1 \leq i \leq r \)). Then

\[
\mathfrak{P}_{(\tilde{g})}/k(\tilde{g}) = \langle n_1(\tilde{x}) - g_1 \cdot d_1(\tilde{x}), \ldots, n_r(\tilde{x}) - g_r \cdot d_r(\tilde{x}), b_1, \ldots, b_l \rangle : \left( \prod_{i=1}^r d_i(\tilde{x}) \right)^{\infty}.
\]

For effectively computing the saturation in Lemma 2.1 we can apply Becker and Weispfenning (1993, Proposition 6.37), for instance. Next, we fix for each generator \( f_i \) of the ideal \( \mathfrak{I} \) a representative \( f_i(\tilde{x}, \tilde{Z}) \in \mathbb{K}(\tilde{x})[\tilde{Z}] \), i.e., for \( i = 1, \ldots, s \) we have \( f_i = \pi_x(f_i(\tilde{x}, \tilde{Z})) \). By “clearing denominators” we may select polynomials \( \tilde{d}_i(\tilde{x}) \in \mathbb{K}[\tilde{x}] \) such that for \( i = 1, \ldots, s \) both \( \tilde{d}_i(\tilde{x}) \neq 0 \) and

\[
F_i = F_i(\tilde{x}, \tilde{Z}) := \tilde{d}_i(\tilde{x}) \cdot f_i(\tilde{x}, \tilde{Z}) \in \mathbb{K}[\tilde{x}, \tilde{Z}]
\]

hold. Now the essential tool we will use both for characterizing and for computing the restricted ideal \( \mathfrak{I} \cap \iota(\mathbb{K}(\tilde{Z})/(\tilde{g})) \) is the ideal

\[
\mathfrak{H} := \sum_{h \in \mathbb{K}[\tilde{x}]/\mathfrak{P}_{(\tilde{g})}} \left( (\tilde{F}, \tilde{p}, \tilde{q}) : h^\infty \right) \subseteq \mathbb{K}(\tilde{x}, \tilde{Z}).
\]

The ideal \( \mathfrak{H} \) is tailored such that for all “denominator free” elements \( f(\tilde{x}, \tilde{Z}) \) of \( \langle \tilde{g} \rangle \) the polynomial \( f(\tilde{x}, \tilde{Z}) \) is contained in \( \mathfrak{H} \). Furthermore, due to \( \mathfrak{P}_{(\tilde{g})}/k(\tilde{g}) \) being contained in \( \mathfrak{H} \) a coefficient \( c(\tilde{x}) \) for which \( c(\tilde{x}) \) is contained in \( k(\tilde{g}) \) can be “replaced by” \( c(\tilde{x}) \) without leaving the ideal. Hence, all elements of \( \mathfrak{I} \cap \iota(\mathbb{K}(\tilde{Z})/(\tilde{g})) \) are contained in \( \mathfrak{H} \) and all other elements of \( \mathfrak{H} \) contain coefficients in \( \tilde{x} \). By eliminating the variables \( \tilde{x} \) we obtain \( \mathfrak{I} \cap \iota(\mathbb{K}(\tilde{Z})/(\tilde{g})) \) from \( \mathfrak{H} \), see Lemma 2.2.

The ideal \( \mathfrak{H} \) can in fact be written as a simple saturation. Exploiting the fact that \( k(\tilde{g})[\tilde{x}, \tilde{Z}] \) is noetherian we obtain the following.

**Remark.** With the above notation, there is a polynomial \( h_0 \in k(\tilde{g})[\tilde{x}] \setminus \mathfrak{P}_{(\tilde{g})}/k(\tilde{g}) \) such that \( \mathfrak{H} = \langle \tilde{F}, \tilde{p}, \tilde{q} \rangle : h_0^\infty \).

**Proof.** As \( k(\tilde{g})[\tilde{x}, \tilde{Z}] \) is noetherian, there is a finite subset \( \mathcal{P} \subseteq k(\tilde{g})[\tilde{x}] \) with \( \mathfrak{H} = \sum_{h \in \mathcal{P}} \left( (\tilde{F}, \tilde{p}, \tilde{q}) : h^\infty \right) \). For a finite sum one easily checks the inclusion

\[
\sum_{h \in \mathcal{P}} \left( (\tilde{F}, \tilde{p}, \tilde{q}) : h^\infty \right) \subseteq \langle \tilde{F}, \tilde{p}, \tilde{q} \rangle : \left( \prod_{h \in \mathcal{P}} h \right)^{\infty}.
\]

(1)

Thus, setting \( h_0 := \prod_{h \in \mathcal{P}} h \in k(\tilde{g})[\tilde{x}] \), we have \( h_0 \notin \mathfrak{P}_{(\tilde{g})}/k(\tilde{g}) \), because of the latter being a prime ideal. Moreover, from Eq. (1), we also know that \( \mathfrak{H} \subseteq \langle \tilde{F}, \tilde{p}, \tilde{q} \rangle : h_0^\infty \). Equality follows from \( h_0 \in k(\tilde{g})[\tilde{x}] \setminus \mathfrak{P}_{(\tilde{g})}/k(\tilde{g}) \), i.e., \( h_0 \) is one of the summands occurring in the defining sum of \( \mathfrak{H} \).

By means of the ideal \( \mathfrak{H} \), the restricted ideal \( \mathfrak{I} \cap \iota(\mathbb{K}(\tilde{Z})/(\tilde{g})) \) can now be characterized as follows.
Lemma 2.2. With the above notation we have

\[ \mathcal{I} \cap \iota(k(\bar{g})[\bar{Z}]/\langle \bar{q}\rangle) = (\iota \circ \pi_\mathcal{I})(\mathfrak{J} \cap k(\bar{g})[\bar{Z}]). \]

Proof. \( \geq \): From the above remark we know that there exists a polynomial \( h_0 \in k(\bar{g})[\bar{X}] \setminus \mathfrak{P}(\bar{x}/k(\bar{g})) \) with \( \mathfrak{J} = \langle \bar{F}, \bar{p}, \bar{q} \rangle : h_0 = 0 \).

Now let \( a \in (\iota \circ \pi_\mathcal{I})(\mathfrak{J} \cap k(\bar{g})[\bar{Z}]) \) and \( a(\bar{Z}) \in (\iota \circ \pi_\mathcal{I})^{-1}(a) \), i.e., for a suitable \( \mu \in \mathbb{N} \) we have \( h_0^\mu \cdot a(\bar{Z}) \in \langle \bar{F}, \bar{p}, \bar{q} \rangle \subseteq k(\bar{g})[\bar{X}, \bar{Z}] \). Then, as \( h_0 \notin \mathfrak{P}(\bar{x}/k(\bar{g})) \), by specializing \( X_i \mapsto x_i \) we obtain \( a(\bar{Z}) \in \langle \bar{f}(\bar{x}, \bar{Z}), \bar{q} \rangle \subseteq k(\bar{x})(\bar{Z}) \) resp.

\[ \pi_x(a(\bar{Z})) \in (\bar{f}) \subseteq k(\bar{x})[\bar{Z}]/\langle \bar{q} \rangle. \]

From \( a(\bar{Z}) \in k(\bar{g})[\bar{Z}] \) we conclude \( a = (\iota \circ \pi_\mathcal{I})(a(\bar{Z})) = \pi_x(a(\bar{Z})) \in (\bar{f}) = \mathcal{I} \). By assumption \( a \) is contained in \( (\iota \circ \pi_\mathcal{I})(k(\bar{g})[\bar{Z}]) \), so we have \( a \in \mathcal{I} \cap k(\bar{g})[\bar{Z}]/\langle \bar{q} \rangle \) as required.

\( \subseteq \): Let \( b \in \mathcal{I} \cap \iota(k(\bar{g})[\bar{Z}]/\langle \bar{q}\rangle) \), and fix a representation \( b(\bar{x}, \bar{Z}) \in k(\bar{x})[\bar{Z}] \) of \( b = (\iota \circ \pi_\mathcal{I})(b(\bar{x}, \bar{Z})) \). In particular, \( b(\bar{x}, \bar{Z}) - b(\bar{x}, \bar{Z}) \) is contained in the kernel of the specialization \( X_i \mapsto x_i \), and because of \( T(\bar{Z}) \setminus \{1\} \) being linearly independent over \( k(\bar{x}) \), there is a polynomial \( s(\bar{x}) \in k[\bar{x}] \) with \( s(\bar{x}) \neq 0 \) and

\[ s(\bar{x}) \cdot (b(\bar{x}, \bar{Z}) - b(\bar{x}, \bar{Z})) \in (\bar{p}) \cdot k(\bar{g})[\bar{X}, \bar{Z}] \subseteq \mathfrak{J}. \]

As \( b \) is contained in the ideal \( \mathcal{I} \), there are \( a_i \in k(\bar{x})[\bar{Z}]/\langle \bar{q} \rangle \) such that \( b = \sum a_i f_i \), and by passing to representatives we can conclude

\[ b(\bar{x}, \bar{Z}) = \sum a_i(\bar{x}, \bar{Z}) \cdot f_i(\bar{x}, \bar{Z}) + p_0 \]

for some \( p_0 \in \langle \bar{p} \rangle \cdot k(\bar{x})[\bar{Z}] \) and \( a_i(\bar{x}, \bar{Z}) \in k(\bar{x})[\bar{Z}] \). Writing \( p_0 = \sum_{j=1}^v c_j(\bar{x}, \bar{Z})q_j \) with \( c_j(\bar{x}, \bar{Z}) \in k(\bar{x}, \bar{Z}) \) and choosing \( t(\bar{x}) \in k[\bar{x}] \setminus \mathfrak{P}(\bar{x}/k) \) appropriately we obtain

\[ t(\bar{x}) \cdot \left( b(\bar{x}, \bar{Z}) - \left( \sum a_i(\bar{x}, \bar{Z})f_i + \sum c_j(\bar{x}, \bar{Z})q_j \right) \right) \in \mathfrak{P}(\bar{x}/k(\bar{g})) \cdot k(\bar{g})[\bar{X}, \bar{Z}]. \]

From \( \mathfrak{P}(\bar{x}/k(\bar{g})) \cdot k(\bar{g})[\bar{X}, \bar{Z}] \) being prime and \( t(\bar{x}) \neq 0 \) we may conclude that

\[ b(\bar{x}, \bar{Z}) - \left( \sum a_i(\bar{x}, \bar{Z}) \cdot f_i + \sum c_j(\bar{x}, \bar{Z}) \cdot q_j \right) \in \mathfrak{P}(\bar{x}/k(\bar{g})) \cdot k(\bar{g})[\bar{X}, \bar{Z}] \subseteq \mathfrak{J}. \]

Because of \( \bar{F}, \bar{q} \) being contained in \( \mathfrak{J} \), now also \( b(\bar{x}, \bar{Z}) \in \mathfrak{J} \) must hold.

From (2) we therefore obtain \( s(\bar{x}) \cdot b(\bar{x}, \bar{Z}) \in \mathfrak{J} \), and as \( \mathfrak{J} \) is saturated w.r.t. all polynomials in \( k(\bar{g})[\bar{X}] \setminus \mathfrak{P}(\bar{x}/k(\bar{g})) \), we have \( b(\bar{x}, \bar{Z}) \in \mathfrak{J} \). Since \( b(\bar{x}, \bar{Z}) \in k(\bar{g})[\bar{Z}] \) this yields

\[ b = (\iota \circ \pi_\mathcal{I})(b(\bar{x}, \bar{Z})) \in (\iota \circ \pi_\mathcal{I})(\mathfrak{J} \cap k(\bar{g})[\bar{Z}]) \]

as required. □

From a computational point of view the characterization of \( \mathcal{I} \cap \iota(k(\bar{g})[\bar{Z}]/\langle \bar{q}\rangle) \) in Lemma 2.2 is not really satisfying, as it does not give a hint on how to determine a basis of the ideal \( \mathfrak{J} \). For computing such a finite set of generators for \( \mathfrak{J} \), we can make use of the following remark.
Remark. We keep the notation from Lemma 2.2. Let \( \langle \vec{F}, \vec{p}, \vec{q} \rangle = \cap_{i=1}^{w} \Omega_i \) be an irredundant primary decomposition. Then

\[
\mathcal{H} = \bigcap_{1 \leq i \leq w} \Omega_i.
\]

Proof. According to Eisenbud (1995, Exercise 2.3) we have

\[
\mathcal{H} = k(\vec{g})[\vec{X}, \vec{Z}] \cap \left( \langle \vec{F}, \vec{p}, \vec{q} \rangle \cdot k(\vec{g})[\vec{X}, \vec{Z}] \rangle_{k(\vec{g})[\vec{X}] \setminus \mathfrak{P}(\vec{X})} \right)
\]

where as usual \( k(\vec{g})[\vec{X}, \vec{Z}] \rangle_{k(\vec{g})[\vec{X}] \setminus \mathfrak{P}(\vec{X})} \) denotes the localization of \( k(\vec{g})[\vec{X}, \vec{Z}] \) at \( k(\vec{g})[\vec{X}] \setminus \mathfrak{P}(\vec{X}) \). So the claim follows from Zariski and Samuel (1979, Chapter IV, Theorem 17).

The condition \( \Omega_i \cap k(\vec{g})[\vec{X}] \subseteq \mathfrak{P}(\vec{X})/k(\vec{g}) \) in the previous remark can be verified effectively by means of standard Gröbner basis techniques (cf., e.g., Buchberger, 1965, 1985; Trinks, 1978 and Becker and Weispfenning, 1993, Propositions 5.38 and 6.15). Moreover, if the required computations in \( k(\vec{g})[\vec{X}, \vec{Z}] \) can be performed effectively then an irredundant primary decomposition of \( \langle \vec{F}, \vec{p}, \vec{q} \rangle \) can be computed by means of the techniques described in Decker et al. (1999), Gianni et al. (1988), Seidenberg (1974) for instance. Finally, computing the elimination ideal \( \mathcal{H} \cap k(\vec{g})[\vec{Z}] \) in Lemma 2.2 is a standard application of Gröbner basis techniques again, and as applying \( \iota \circ \pi_\mathcal{I} \), which is essentially a change of the interpretation of the data computed, does not provide any difficulties, in summary we have the following.

**Theorem 2.1.** We keep the above notation. Moreover, assume that an irredundant primary decomposition of \( \langle \vec{F}, \vec{p}, \vec{q} \rangle \subseteq k(\vec{g})[\vec{X}, \vec{Z}] \) can be computed effectively. Then a finite generating set of \( \mathcal{H} \cap (k(\vec{g})[\vec{Z}] / \langle \vec{q} \rangle) \) can be computed effectively.

We want to illustrate the method just described through two simple examples.

**Example.** Let \( x \) be transcendental over \( \mathbb{Q} \), and consider the principal ideal

\[
\mathfrak{I} := \langle Z^3 + Z^2 - x^3 - x^2 \rangle \subseteq \mathbb{Q}(x)[Z].
\]

We want to compute the restriction \( \mathfrak{I} \cap \mathbb{Q}(x^2)[Z] \). For this we first have to determine a basis of the ideal \( \mathfrak{P}(x)/\mathbb{Q}(x^2) \); obviously the minimal polynomial \( p := Z^2 - x^2 \) of \( x \) over \( \mathbb{Q}(x^2) \) can be used here. Denoting the given generator of \( \mathfrak{I} \) by \( f_1 \), the corresponding polynomial \( F_1 \) computes to \( Z^3 + Z^2 - X^3 - X^2 \). As we are dealing with a polynomial ring we have \( \Omega = \langle 0 \rangle \), and so in our example the ideal \( \langle \vec{F}, \vec{p}, \vec{q} \rangle \) is generated by

\[
\{ Z^3 + Z^2 - X^3 - X^2, X^2 - x^2 \}.
\]

For example, by means of a computer algebra system like MAGMA (see Bosma et al., 1997) one can determine the following irredundant primary decomposition of \( \langle \vec{F}, \vec{p}, \vec{q} \rangle \subseteq \mathbb{Q}(x^2)[Z] \):

\[
\langle \vec{F}, \vec{p}, \vec{q} \rangle = \langle Z - X, X^2 - x^2 \rangle \cap \langle Z^2 + ZX + Z + x^2, X^2 - x^2 \rangle
\]

\[
=: \Omega_1 \cap \Omega_2
\]

By looking at the corresponding lexicographical Gröbner basis with \( Z > X \) we see that \( \Omega_i \cap \mathbb{Q}(x^2)[X] \subseteq \mathfrak{P}(x)/\mathbb{Q}(x^2) \) holds for \( i = 1, 2 \). So in our example we have \( \mathcal{H} = \Omega_1 \cap \Omega_2 \), namely
\( \mathfrak{H} = \langle F_1, p \rangle \). Computing the elimination ideal \( \mathfrak{H} \cap \mathbb{Q}(x^2)[Z] \) with a lexicographic Gröbner basis provides no further difficulties and yields

\[
\mathcal{I} \cap \mathbb{Q}(x^2)[Z] = (Z^6 + 2 \cdot Z^5 + Z^4 - 2x^2 \cdot Z^3 - 2x^2 \cdot Z^2 - x^6 + x^4).
\]

**Example.** Let \( x_1, x_2 \) be algebraically independent over \( \mathbb{Q} \), and consider the ideal

\[
\mathfrak{J} := (x_1 \cdot Z_1 - Z_2, x_2 \cdot Z_2 - Z_3, Z_3^2) \subseteq \mathbb{Q}(x_1, x_2)[Z_1, Z_2, Z_3].
\]

We want to compute the restriction \( \mathfrak{J} \cap \mathbb{Q}[Z_1, Z_2, Z_3] \). The ideal \( \mathfrak{P}_{(x_1, x_2)/\mathbb{Q}} \) is the zero ideal, and the polynomials \( \tilde{F} \) compute to

\[
\begin{align*}
F_1 &= X_1 \cdot Z_1 - Z_2, \\
F_2 &= X_2 \cdot Z_2 - Z_3, \\
F_3 &= Z_3^2.
\end{align*}
\]

Dealing again with a polynomial ring, we have \( \Omega = \langle 0 \rangle \), and thus we obtain \( \langle \tilde{F}, \tilde{p}, \tilde{q} \rangle = \langle F_1, F_2, F_3 \rangle (\subseteq \mathbb{Q}[X_1, X_2, Z_1, Z_2, Z_3]) \). For example, by means of MAGMA one can determine the following irredundant primary decomposition \( \mathcal{I} = \mathcal{Q}_1 \cap \mathcal{Q}_2 \cap \mathcal{Q}_3 \) of \( \langle \tilde{F}, \tilde{p}, \tilde{q} \rangle \subseteq \mathbb{Q}[X_1, X_2, Z_1, Z_2, Z_3] \):

\[
\begin{align*}
\mathcal{Q}_1 &= (X_1^2, X_1 \cdot Z_1 - Z_2, X_1 \cdot Z_2, X_1 \cdot Z_3, X_2 \cdot Z_2 - Z_3, Z_2^2, Z_2 \cdot Z_3, Z_3^2) \\
\mathcal{Q}_2 &= (X_1 \cdot Z_1 - Z_2, X_2^2, X_2 \cdot Z_2 - Z_3, X_2 \cdot Z_3, Z_3^2) \\
\mathcal{Q}_3 &= (X_1 \cdot Z_1 - Z_2, X_2 \cdot Z_2 - Z_3, Z_1^2, Z_1 \cdot Z_2, Z_1 \cdot Z_3, Z_2^2, Z_2 \cdot Z_3, Z_3^2).
\end{align*}
\]

Only for \( i = 3 \) we have \( \mathcal{Q}_i \cap \mathbb{Q}[X_1, X_2] = \langle 0 \rangle (= \mathfrak{P}_{(x_1, x_2)/\mathbb{Q}}) \), and thus we obtain \( \mathfrak{H} = \mathcal{Q}_3 \). By intersecting \( \mathfrak{H} \) with \( \mathbb{Q}[Z_1, Z_2, Z_3] \) we get (via Lemma 2.2)

\[
\mathfrak{J} \cap \mathbb{Q}[Z_1, Z_2, Z_3] = (Z_1^2, Z_1 \cdot Z_2, Z_1 \cdot Z_3, Z_2^2, Z_2 \cdot Z_3, Z_3^2).
\]

3. **A (counter-)example: Intersecting fields**

As described in Müller-Quade and Beth (1998a), an ideal restriction can be used to compute generators of the intersection \( k(\tilde{g}) \cap k(\tilde{h}) \) of two subfields \( k(\tilde{g}), k(\tilde{h}) \subseteq k(\tilde{x}) \): it is sufficient to find a basis of the ideal

\[
\frac{\mathfrak{P}_{(\tilde{x})/k(\tilde{g})} \cap k(\tilde{h})[\tilde{X}]}{\subseteq k(\tilde{g})[\tilde{X}]} \subseteq (k(\tilde{g}) \cap k(\tilde{h}))[\tilde{X}].
\]

Unfortunately, the method discussed in the previous section does not allow the computation of the intersection (3), as in general \( k(\tilde{h}) \) is not a subfield of \( k(\tilde{g}) \). In Müller-Quade and Beth (1998a) an algorithm for accomplishing this task was proposed, but a more detailed analysis shows that it actually computes the ideal \( \mathfrak{P}_{(\tilde{x})/k(\tilde{g})} \cdot k(\tilde{x})[\tilde{X}] \cap k(\tilde{h})[X] \) which in general does not coincide with the ideal (3).

**Example.** Consider the two subfields \( k(\tilde{g}) := \mathbb{Q}(x^3 + x^2) \) and \( k(\tilde{h}) := \mathbb{Q}(x^2) \) of \( k(\tilde{x}) := \mathbb{Q}(x) \). Then we know from the first example in the previous section that

\[
\mathfrak{P}_{(\tilde{x})/k(\tilde{g})} \cdot k(\tilde{x})[\tilde{X}] \cap k(\tilde{h})[X] = (X^6 + 2 \cdot X^5 + X^4 - 2x^2 \cdot X^3 - 2x^2 \cdot X^2 - x^6 + x^4).
\]
As adjoining the coefficients of a reduced Gröbner basis of this ideal to \( \mathbb{Q} \) yields the field \( \mathbb{Q}(x^2) \), the algorithm from Müller-Quade and Beth (1998a) yields \( \mathbb{Q}(x^3 + x^2) \cap \mathbb{Q}(x^2) = \mathbb{Q}(x^2) \), which is clearly wrong.

So it remains an interesting open question whether the techniques described here can be extended in such a way that they allow the computation of a system of generators of the intersection of arbitrary finitely generated extension fields.

References


