Minimal Primary Decomposition and Factorized Gröbner Bases[*]

Hans-Gert Gräbe
Institut für Informatik, Universität Leipzig, Germany

Revised version, May 23, 1996

Abstract

This paper continues our study of applications of factorized Gröbner basis computations in [8] and [9].

We describe a way to interweave factorized Gröbner bases and the ideas in [5] that leads to a significant speed up in the computation of *isolated primes* for well splitting examples.

Based on that observation we generalize the algorithm presented in [22] to the computation of *primary decompositions* for modules. It rests on an ideal separation argument.

We also discuss the practically important question how to extract a *minimal primary decomposition*, neither addressed in [5] nor in [17]. For that purpose we outline a method to detect necessary embedded primes in the output collection of our algorithm, similar to [22, cor. 2.22].

The algorithms are partly implemented in version 2.2.1 of our REDUCE package CALI [7].

1 Introduction

The computation of primary decompositions is a central goal and has attracted the attention of specialists in constructive commutative algebra for a long time. It was a popular topic illustrating and bringing together very different techniques and various approaches in "pre computer" times, see e.g. [16].

A first thorough constructive approach to primary decomposition, collecting also the ideas and observations on this topic known in the community before, is contained in the fundamental work of A. Seidenberg in the 70's and 80's, see [18], [19], [20]. It heavily influenced the first algorithmic attempts to compute primary decompositions using modern methods as e.g. Gröbner bases in [13]. These attempts culminated in the fundamental paper [5] that collected known pieces together, filled up the gaps and altogether presented the first general primary decomposition algorithm, that could be (and was) implemented in a computer algebra system.

Several papers, published almost at the same time, proposed similar ideas or improvements to the original algorithm as e.g. [14] or [11]. There are also papers generalizing the ideas of [5] to a more general context as e.g. [23], [1] or [10]. The primary decomposition algorithm of [5], originally formulated for ideals, may be extended also to (relative) submodules of a

[*] Appeared in *J. AAECC* **8** (1997), 265 - 278.

finitely generated free module, as explained in [17]. The only completely different approach to primary decomposition, that may be applied to general examples, was presented in [4].

Regardless of the wide attention that this theoretical work attracted in the community, up to now there are only a few implementations of the algorithm: As far as we know, the AXIOM implementation of the authors of [5], an implementation in MAS by H. Kredel for zero dimensional ideals, our implementation in the REDUCE package CALI [7] and the implementation in the computer algebra system Risa/Asir [15] by the authors of [22]. Only CALI offers primary decomposition also for modules.

It was the aim of this paper to collect the experience obtained during our implementation of the above algorithm and to describe some new algorithmic ideas proved to be useful especially for the computation of primary decompositions under the assumption that we know already a list of isolated primes. During the preparation of this paper we became aware of analogous considerations in [22], allowing several shortcuts compared to an earlier version of this paper. Different from [22], where the authors consider only primary decomposition of ideals, results are explained here in general for pairs of submodules $N \subset M$ of a finitely generated free module F.

After some preliminary work we first discuss, how factorization may be involved in an early stage of the computation of isolated primes. It turns out empirically, that the same advantage, observed for the factorized Gröbner basis algorithm in contrast to the ordinary one solving polynomial systems of equations in [8] and [9] for well splitting examples, holds also for the computation of isolated primes. Of course, this reflects the general observation, that usually geometric properties of ideals (here: the computation of isolated primes) are computationally more handy than algebraic ones (here: the computation of primary decompositions).

To extract finally the primary components we use as in [22] ideal separators with respect to a list of isolated primes, computed in advance. We generalize this approach to a (relative) module situation, too, i.e. separate the module N inside M into (almost) primary pieces. In contrast to the original algorithm in [5] this and the extraction of the true primary pieces needs no change to normal position.

In a third part we discuss the practically important question how to extract a *minimal primary decomposition*, addressed neither in [5] nor in [17]. First [22] contains a method to detect irrelevant primary components in a general primary decomposition. Their argument uses a careful examination of the interdependencies between different branches of the decomposition tree. We outline a “local” method, that allows to decide for a given prime in a list of primes, containing all associated primes, whether it is associated or not.

We don’t repeat here a comparison between the old and new methods at CPU time level but refer the reader to [22] for such a comparison but conclude with some examples to demonstrate the proposed new method “at work”.

2 Preliminaries and Notations

2.1 Notations

Let k be a field, $S = k[x_1, \ldots, x_n]$ the polynomial ring over k in the variables $(x_1, \ldots, x_n)$ and $N \subset M$ two submodules of a finitely generated free S-module F. For practical applications M is usually the free S-module itself and N its submodule, but the theory and also the algorithms developed below work in this more general situation as well. A special role is played by ideals as submodules of S itself, for which the primary decomposition theorems are surely better known than in the general situation.

We assume S to be equipped with a Noetherian term order as defined e.g. in [2, 5.3]. For F we fix a free basis $\mathbf{e} = (e_1, \ldots, e_k)$ and assume N and M to be given by sets of generators in their representation wrt. $\mathbf{e}$ as vectors with polynomial entries. For practical applications we collect these vectors into a matrix, such that the rows of that matrix generate the corresponding submodule of F. In this setting we assume F to be equipped with a compatible module term order as defined in [3, 15.2] (We do not restrict ourselves to the special module term orders considered in [17]). Moreover we assume the reader to be familiar with the ideas of Gröbner bases for ideals and also for submodules of free modules; see the same monographs. We will use the corresponding notions without further explanation.

2.2 Primes and Primary Components

Lets repeat for convenience the definitions and existence statements on primary decomposition of submodules as given e.g. in [21, ch. 9]: N is said to be a *primary submodule of* M precisely when $M/N \neq 0$ and every zero divisor of M/N is already nilpotent. In this case the ideal $P := Rad(Ann_S(M/N))$, the radical of the annihilator of M/N in S, is a prime ideal and we say that N is a P-primary submodule of M. If $N_1, \ldots, N_m$ are P-primary submodules of M, then so is $\cap_{i=1}^m N_i$. Hence P-primary submodules can be collected together.

For an arbitrary submodule a *primary decomposition of* N *in* M is a representation of N as an intersection of finitely many primary submodules of M. Such a primary decomposition

$$N = N_1 \cap N_2 \cap \ldots \cap N_m$$

with P_i-primary modules $N_i \subset M$ $(i = 1, \ldots, m)$ is said to be *minimal* precisely when

(a) $P_1, \ldots, P_m$ are pairwise distinct, and

(b) for all $j = 1, \ldots, m$ we have

$$N_j \not\supset \bigcap_{i \neq j} N_i.$$

The first uniqueness theorem states that for such a minimal primary decomposition the set of primes $\{P_1, \ldots, P_m\}$ is uniquely defined. These primes are called the *associated primes of* M/N. We denote this set by $Ass(M/N)$. Their union is exactly the set of zero divisors of M/N. The *support* $Supp(M/N) := \{P \in Spec\ S : (M/N)_P \neq 0\}$ consists of all primes containing one of the associated primes. The dimension $dim(M/N)$ is the maximal possible length of an ascending chain of primes in $Supp(M/N)$.

The prime ideals in $Ass(M/N)$ that are minimal with respect to inclusion are called the *isolated primes of* M/N, the remaining associated prime ideals are the *embedded primes of* M/N. Geometrically, the isolated primes correspond to the different components of $Supp(M/N)$ as a subset of the affine scheme $Spec\ S$. The embedded components are not visible from the geometric point of view but represent more delicate algebraic properties and cause the most trouble in applications.

The second uniqueness theorem states that not only the primes but also the primary components corresponding to isolated primes, the *isolated components of* N *in* M, are uniquely defined. The other primary components, the *embedded components of N in M*, need not be defined uniquely.

In [5] the authors propose a recursive approach to find a (not necessarily minimal) primary decomposition: In each step they compute some of the isolated components (of highest dimension) and a certain "remainder" to be decomposed recursively. It is this remainder that introduces non-uniqueness for the shape of embedded components and that may produce components not necessary for a *minimal* primary decomposition. Computationally it is not advisable to use the above definition to detect them. Until CALI v. 2.2. we used a mutual inclusion test instead. Testing different primary decomposition packages Kazuhiro Yokoyama and Shimoyama Takeshi pointed out to me, that there must be something wrong. Indeed, this shortcut is clearly incorrect. Below we present a test to decide for a given prime P whether it is in $Ass(M/N)$. Since embedded *primes* are defined uniquely, this allows us to filter out superfluous components in a primary decomposition.

2.3 Quotient Computations and Primary Decomposition

Let $N \subset M$ be two S-modules as before. Below we use various quotient computations to separate primary components of N in M. Here we collect the necessary technical prerequisites.

Let $J = (f_1, \ldots, f_k) \subset S$ be the ideal generated by $f_1, \ldots, f_k \in S$. We write

$$N :_M J := \{m \in M \, : \, J \cdot m \subset N\} \qquad \text{and}$$

$$N :_M J^\infty := \{m \in M \, : \, \exists\, k > 0 \;\; J^k \cdot m \subset N\}$$

for the *quotient* resp. *stable quotient* of N by J (in M).

Lemma 1 *Let N be a P-primary submodule of M and $f \in S$. Then*

1. $N :_M (f)^\infty = M$ *if* $f \in P$.
2. $N :_M (f)^\infty = N$ *if* $f \notin P$.

More generally, for an arbitrary submodule $N \subset M$ and its primary decomposition $N = \cap N_i$ into P_i-primary modules N_i we get

$$N :_M (f)^\infty = \bigcap \{N_i \, : \, f \notin P_i\}$$

and for the ideal $J \subset S$

$$N :_M J^\infty = \bigcap \{N_i \, : \, J \not\subset P_i\}$$

Proof : The first assertion follows immediately from the fact, that the multiplication map by f on M/N is either nilpotent (for $f \in P$) or injective (for $f \notin P$).

The other statements are easy consequences of the first one and general quotient properties. □

Lemma 2 *For S-modules $N \subset M$ the inclusions*

$$Ass(N) \subset Ass(M) \subset Ass(N) \cup Ass(M/N)$$

hold. In particular, for a polynomial $s \in S$ we get $Ass(M/(N :_M (s))) \subset Ass(M/N)$, i.e. if N is P-primary in M, then either $N :_M (s) = M$ or $N :_M (s)$ is P-primary in M, too.

Proof : For the first statement see e.g. [21, ex. 9.42]. The latter statement follows from the exact sequence

$$0 \longrightarrow M/(N :_M (s)) \longrightarrow M/N,$$

induced by the multiplication by s. □

2.4 Factorized Gröbner Bases

In addition to the notation introduced so far let $\bar{k}$ be the algebraic closure of k and $B := \{f_1, \ldots, f_m\} \subset S$ a set of polynomials.

$$Z(B) := \{a \in \bar{k}^n : f(a) = 0 \text{ for all } f \in B\ \}$$

denotes the *set of zeroes* of B over $\bar{k}$.

The Gröbner algorithm with factorization is a powerful tool to decompose the zero set of a well splitting polynomial system into smaller components. It invokes factorization of reduced S-polynomials during the calculation of Gröbner bases and splits the computation into as many branches as (different) factors occur. Since the algorithm is part of almost all general purpose Computer Algebra Systems, we will not describe it here and refer the reader to [8] and [9] instead, where we discussed this algorithm in great detail and employed it successfully to decompose a given set of polynomials into triangular systems.

For our considerations below let's fix only its input/output specification:

The Algorithm FGB(B) :
Input : A set of polynomials $B \subset S$.
Output: A list of Gröbner bases $\{B_i : i = 1, \ldots, m\}$ with $Z(B) = \cup Z(B_i)$.

It turned out that in practical examples often, especially with respect to the lexicographic term order, the list of bases produced by the Gröbner factorizer consists already of primes and hence presents a decomposition of (B) into isolated primes. Of course, this cannot be guaranteed. Below we use it in a first step and complete the computation in a second step along the lines of [5].

2.5 Reduction to dimension zero

A general tool, used in several places of our algorithm, is the base change trick proposed in [5]: Consider some of the variables as parameters to reduce the general problem to a zero dimensional one. A systematic study of consequences that can be derived this way is contained in [12]. Here we generalize these ideas to submodules of a finitely generated free S-module F, extending the results of [17] into a more computational direction.

Recall first the notion of independent sets: For a given ideal $I \subset S$ the set of variables $(x_v, v \in V)$ is an *independent set* iff $I \cap k[x_v, v \in V] = (0)$. See [2] for the definition and also a guideline to the history of this notion. [6] contains another explanation of this notion, its connection to strongly independent sets, and discusses algorithms for an effective computation of strongly independent sets.

[6] generalizes this notion also to submodules of F. Here we need a further generalization to a relative situation. Let $N \subset M$ be as above. We say that $(x_v, v \in V)$ is a *relative independent set* for $N \subset M$ iff it is an independent set for $I = Ann_S(M/N)$.

Let $(x_v, v \in V)$ be a maximal (wrt. inclusion) relative independent set for $N \subset M$. Denote by $\tilde{S} := k(x_v, v \in V)[x_v, v \notin V]$ the extension ring of S that we obtain localizing at $\sigma := k[x_v, v \in V] \setminus \{0\}$, and by $\tilde{F}, \tilde{M}, \tilde{N}$, and $\tilde{I}$ the extension modules and the extension ideal obtained from F, M, N, and I by the flat base change $S \longrightarrow \tilde{S}$. Since localization commutes with taking annihilators we get $\tilde{I} = Ann_{\tilde{S}}(\tilde{M}/\tilde{N})$ and thus $dim\ \tilde{M}/\tilde{N} = dim\ \tilde{S}/\tilde{I} = 0$.

Since S is an integral domain, there are natural embeddings $S \subset \tilde{S}$ and $F \subset \tilde{F}$ and we can define retractions $\tilde{I} \cap S$, $\tilde{M} \cap F$, $\tilde{N} \cap M$ etc.

Lemma 3 *Let N be an P-primary submodule of $M \subset F$. Then one of the following two alternatives holds:*

1. *If $P \cap \sigma = \emptyset$ then $\tilde{N}$ is a $\tilde{P}$-primary submodule of $\tilde{M}$ and $\tilde{N} \cap M = N$.*

2. *If $P \cap \sigma \neq \emptyset$ then $\tilde{N} \cap M = M$.*

Proof : Since primarity commutes with localization we have only to prove the assertions about the recontractions.

For the first part assume $\frac{n}{s} = m \in \tilde{N} \cap M$ with $n \in N, s \in \sigma, m \in M$. Hence $n = m \cdot s$ and $m \in N :_M (s) = N$ since $s \notin P$ is a non zero divisor on M/N.

For the second part take $s \in \sigma \cap P$. Since s is nilpotent on M/N there is a power $e \gg 0$ such that $s^e\, M \subset N$ and every $m \in M$ may be represented as $\frac{n}{s^e}$ for an appropriate $n \in N$. □

For arbitrary submodules N of F there is a close connection between N and $\tilde{N}$. With respect to a special module term order on F, one can even read off a Gröbner basis of $\tilde{N}$ from a Gröbner basis of N. For this purpose we define an *inverse module term block order wrt. V* on F in the following way: Let $<_1$ be an inverse block order wrt. V on S as defined in [2, p. 390]. Then module terms $m\, e_i$ and $n\, e_j$ are compared by the rule

$$m\, e_i < n\, e_j \quad :\Leftrightarrow \quad \begin{array}{c} m <_1 n \quad \text{or} \\ m = n \text{ and } i < j \end{array}$$

(i.e. in the sense of [17] $<$ is the TOP module term order on F induced by $<_1$). Wrt. such a module term order the extension of a Gröbner basis B of N to $\tilde{F}$ is a Gröbner basis of $\tilde{N}$ and a *minimal* Gröbner basis of $\tilde{N}$ can be obtained picking up the elements with leading terms, that are minimal with respect to the (module) division order on $\tilde{F}$. This generalizes well known properties of ideals, see [5] or [2].

For retractions the situation is slightly more difficult. If $P \subset S$ is prime then either $\tilde{P} \cap S = P$ (if $P \cap \sigma = \emptyset$) or $\tilde{P} \cap S = S$ (otherwise). In general retractions can be found by a stable quotient computation from a Gröbner basis over $\tilde{S}$. For this purpose define a *denominator-free basis* B of the module $J \subset \tilde{F}$ as a set of polynomial vectors in F such that they generate J regarded as elements of $\tilde{F}$. Such a basis can be constructed from an arbitrary basis of J clearing denominators. Denote by (B) the module generated by B in F.

Lemma 4 *Let B be a denominator-free Gröbner basis of $J \subset \tilde{F}$ and $c \in S$ the product of the leading coefficients of the elements of B regarded as polynomial vectors in $\tilde{F}$. Then*

$$J \cap F = (B) :_F (c)^\infty.$$

PROOF : As explained e.g. in [9] one can compute denominator-free in $\tilde{F}$ using the well known pseudo normal form algorithm **PNF(p,B)**. For $p \in F$ it returns a denominator-free pseudo $\tilde{S}$-normal form $p' \in F \subset \tilde{F}$ with respect to B, i.e. satisfying $z \cdot p \equiv p' \ (mod\ J)$ for a certain unit $z \in \tilde{S}$ that can be chosen to be a product of leading coefficients of the elements in B.

Since c is invertible in $\tilde{S}$ we have only to show, that $J \cap F \subset (B) :_F (c)^\infty$. But since B is a Gröbner basis of J over $\tilde{S}$, for a (denominator-free) element $p \in J \cap F$ we get $PNF(p, B) = 0$ and hence $p \in (B) :_F (c)^\infty$. □

For ideals this is a slight modification of [5, 3.8.] or [22, A.8], where c is the product of all leading coefficients in a Gröbner basis over S instead of $\tilde{S}$, and was first proved in this form in [12, 1.3]. See also [2, 8.94] or [9].

3 Isolated Primes

For the computation of isolated primes we follow the original ideas explained in [5] with modifications proposed in [11], see also [2, ch. 8.7] for details. Since these sources are easy accessible, below we restrict ourselves to outline modifications (and non-modifications) caused by FGB.

Let $I \subset S$ be an ideal (e.g. $I = Ann_S(M/N)$ from above). To compute its isolated primes in [5] the authors propose the following rough scheme:

1. Find a maximal independent set $(x_v : v \in V)$ of I, e.g. from a Gröbner basis of I.

2. (Re)compute a Gröbner basis B of I with respect to an inverse block order wrt. V.

3. Change to $\tilde{S}$, extract the minimal denominator-free Gröbner basis $B' \subset B$ and the product of their leading coefficients $c \in S$.

4. Compute the zero dimensional isolated primes of $\tilde{I}$ and their retractions to S. This yields a list of primes $P_1, \ldots, P_m$ such that

$$Z(I) = \bigcup_{i=1}^{m} Z(P_i) \bigcup Z(I + (c))$$

5. Compute the isolated primes of the (in most cases lower dimensional) ideal $I + (c)$ recursively and pick only those not containing one of the P_i's.

By our experience, for practical applications it is better not to change to dimension zero in one step, but to "slice the problem" descending the dimension in each step by one as in (the final version of) [5]. Since such a variant rests on exactly the same ideas as above, we do not enter into details here.

How may FGB be invoked ? In the first step one can compute factorized Gröbner bases to split the problem in advance into possibly more handy pieces. This is at the same time the most important invocation of FGB, since afterwards pieces tend to be almost prime, thus seldom allowing a deeper splitting. In the second step (Gröbner basis recomputation with respect to an inverse block order) FGB cannot be applied, since for the result V must remain independent. This is not guaranteed for ideals strongly containing I. In step 4, by lemma 4 the retract may be computed as a stable quotient. Done as described in [2, 6.38] FGB might be invoked during the elimination step, but this is of limited use since the result is known to be prime in this case.

It remains to discuss the zero dimensional part of the above algorithm. So assume $I \subset S$ is a zero dimensional ideal. Following the rules of [5] or [2, ch. 8.6] we would proceed as follows:

1. Compute, e.g. by Buchberger's approach (cf. [2, 9.6]), the monic generators of $I \cap k[x_i]$ for $i = 1, \ldots, n$. Adding their square-free parts to the set of generators of I we get a basis for the radical $\sqrt{I}$.

2. Make a generic (or moderate, as suggested in [11]) change of coordinates to put $\sqrt{I}$ into normal position with respect to x_1 ([2, 8.67]) and decompose the monic generator of $\sqrt{I} \cap k[x_1]$ into (pairwise non-associated) factors $p_1, \ldots, p_m$. Then $\{\sqrt{I} + (p_1), \ldots, \sqrt{I} + (p_m)\}$ are the isolated primes of I.

Again, the first step strongly suggests that factorization should be invoked. A modification of FGB for the monic generators mentioned above thus will do some of the work of step 2 in advance and split the ideal already *before* changing coordinates. For many practical applications this reduces the computational amount in the second step to its necessary minimum.

Note that, due to a reduction argument for the embedding dimension, we may moreover restrict ourselves in the first step to those variables not contained among the generators of the initial ideal of I. This is especially useful for pure lexicographic term orders, since on the one hand factorized Gröbner bases of zero dimensional ideals tend to be in Shape Lemma form (cf. [2, 8.77] and our observations in [8]) and on the other hand monic generators for such variables are usually hard to compute.

4 Primary Decomposition

Starting from a set of isolated primes one can use ideal separation to compute the corresponding primary decomposition. Let's illustrate this approach at first for modules without embedded primes.

Proposition 1 *Let $N \subset M$ be as above and assume that $Ass(M/N) = \{P_1, \ldots, P_m\}$ contains no embedded primes. For $i, j = 1, \ldots, m$ take $f_i \in S$ such that $f_i \in P_j$ if $i \neq j$, but $f_i \notin P_i$. Then*

$$N = \bigcap (N :_M (f_i)^\infty)$$

is a (minimal) primary decomposition of N in M.

This is an immediate consequence of lemma 1.

Note that the construction of f_i is easy: Lacking embedded primes we find for each $j \neq i$ a (base) polynomial p_{ij} in P_j not contained in P_i. Then $f_i := \prod_{j \neq i} p_{ij}$ has the desired property. We say that f_i *separates* $\{P_j : j \neq i\}$ *from* P_i.

Since zero dimensional ideals are unmixed, this applies especially to the situation, when $dim\ M/N = 0$ and allows the computation of a primary decomposition for modules of (relative) dimension zero without a coordinate change to normal position (at least in that phase of the computation).

In general we can do the same construction for the *isolated* primes of M/N, but neither $N :_M (f_i)^\infty$ must be primary nor the above equality must hold. Thm. 2.7 in [22] contains the necessary improvements for ideals, that generalize to modules in the following way:

Proposition 2 *Let $N \subset M$ be two S-modules and assume that $L := \{P_1, \ldots, P_k\}$ are the isolated primes of M/N. Take as in the previous proposition $f_i \in S$ separating $L \setminus \{P_i\}$ from P_i, $N_i := N :_M (f_i)^\infty$ and integers e_i such that $f_i^{e_i} N_i \subset N$.*

Then

1. *N_i is a* quasi P_i-primary module *in M, i.e. has a unique isolated prime P_i (and possibly embedded components).*
2. *The sets $A_i := Ass(M/N_i) = \{P \in Ass(M/N) \,:\, f_i \notin P\}$ are pairwise disjoint.*
3. *For $J := (f_1^{e_1}, \ldots, f_k^{e_k})$ we have*

$$N = (\cap N_i) \bigcap (N + J \cdot M).$$

This is a decomposition of N into quasi primary components N_i and a component $N' := N + J \cdot M \subset M$ of lower (relative) dimension.

Proof : By definition, f_i vanishes on all associated primes of M/N not embedded in or equal to P_i (and may vanish on some of the remaining primes different from P_i). Since by lemma 1 a stable quotient with respect to f_i cuts off all such components, this verifies the first assertion.

By construction $P \in Ass(M/N)$ may not contain at most one of the separators. This verifies also the second assertion.

Since $N \subset N' \subset M$ and $(M/N')_P = 0$ for all $P \in L$ we conclude also immediately $dim(M/N') < dim(M/N)$.

The remaining assertion follows as in [22]: First notice, that $N_i :_M (f_j^{e_j}) = M$ for each $j \neq i$. Indeed, since

$$N_i :_M (f_j^{e_j}) \supset N :_M (f_j^{e_j}) = N_j \qquad \text{and} \qquad N_i :_M (f_j^{e_j}) \supset N_i$$

we conclude by lemma 2 $Ass(M/(N_i :_M (f_j^{e_j}))) \subset A_i \cap A_j = \emptyset$.

Now, if $n + \sum f_j^{e_j} m_j \in \cap N_i$ with $n \in N, m_j \in M$, we conclude $f_j^{e_j} m_j \in N_i$ for $j \neq i$ and thus also $f_i^{e_i} m_i \in N_i = N :_M (f_i^{e_i})$. Hence $f_i^{2e_i} m_i \in N, m_i \in N :_M (f_i)^\infty = N :_M (f_i^{e_i})$ and finally $f_i^{e_i} m_i \in N$. □

It remains to decompose the quasi primary components N_i. Here we apply reduction to dimension zero once more. So lets assume that M/N has a unique isolated prime P. Choose a maximal relative independent set $(x_v, v \in V)$ for $N \subset M$ and let $\tilde{N}, \tilde{M}$ etc. be as in section 2.5 the extension modules of N, M etc. to $\tilde{S} := k(x_v, v \in V)[x_v, v \notin V]$.

Lemma 5 *Assume moreover that B is a Gröbner basis of N wrt. an inverse module term block order wrt. V on F, $B' \subset B$ a denominator-free Gröbner basis for $\tilde{N}$ and $c \in S$ the product of the leading coefficients of the elements of B' regarded as polynomial vectors in $\tilde{F}$. Then*

$$N' := \tilde{N} \cap M = N :_M (c)^\infty$$

is the (uniquely determined) P-primary component of N in M.

If e is an integer such that $c^e \cdot N' \subset N$, then

$$N = N' \bigcap (N + c^e\, M)$$

is a decomposition of N into a P-primary component and another module of lower (relative) dimension.

Proof : The first assertion follows immediately from the fact that $dim\ \tilde{M}/\tilde{N} = 0$ and that P is the unique isolated prime of M/N. The second one may be proved as in the last proposition. □

Lets collect our considerations into the following primary decomposition algorithm:

The Algorithm PrimeDecomposeA(N,M)

Input : $N \subset M \subset F$
Output : A primary decomposition of N in M.

1. Compute $L := \{P_1, \ldots, P_k\}$, the list of isolated primes of M/N as in section 3.
2. For $i = 1, \ldots, k$ compute polynomials $f_i \in S$ separating $L \setminus \{P_i\}$ from P_i.
3. For $i = 1, \ldots, k$ compute the quasi primary components $N_i := N :_M (f_i)^\infty$ as stable quotients and integers e_i such that $f_i^{e_i} N_i \subset N$.
4. Return

   $$(\cup_i PrimeDecomposeB(N_i, M, P_i)) \bigcup PrimeDecomposeA(N' := N + (f_1^{e_1}, \ldots, f_k^{e_k})\, M, M)$$

The Algorithm PrimeDecomposeB(N,M,P)

Input : $N \subset M \subset F$, such that M/N has a unique isolated prime P.
Output : A primary decomposition of N in M.

1. Find a maximal relative independent set $(x_v, v \in V)$ for $N \subset M$.
2. Compute a Gröbner basis B of N wrt. an inverse module term block order wrt. V.
3. Change to $\tilde{S}$, extract a minimal Gröbner basis $B' \subset B$ of $\tilde{N}$ and compute $c \in S$, the product of the leading coefficients of the elements of B' regarded as polynomial vectors in $\tilde{F}$.
4. Compute $N' := N :_M (c)^\infty$ and an integer e such that $c^e N' \subset N$.
5. Return

   $$\{(N', M, P)\} \bigcup PrimeDecomposeA(N + c^e \cdot M, M)$$

To obtain a primary decomposition with pairwise different primes we may collect all components in the output collection of *PrimeDecomposeA* with the same prime P and substitute them by their intersection. Note that even such a decomposition may not be minimal.

5 Minimal Primary Decomposition

To extract a minimal primary decomposition from an arbitrary one we employ the following necessity check. Assume $N = \cap N_i$ is a primary decomposition of N in M into P_i-primary components N_i (we may assume the P_i to be pairwise distinct), but $L = \{P_1, \ldots, P_m\}$ eventually contains superfluous primes. Fix $P_i \in L$ and N_i as the corresponding primary component.

As above we find $f \in S$ that separates $\{P_j \not\subset P_i\}$ from P_i. Hence by lemma 1 the associated primes of the module

$$M_i := N :_M (f)^\infty = \bigcap_{\{P_j \subset P_i\}} N_j$$

are contained in P_i. Again by lemma 1 we conclude that another stable quotient by P_i cuts off exactly N_i. Hence we can decide whether N_i is redundant in the decomposition of N testing M_i and $M_i :_M P_i^\infty$ for equality. Altogether we proved the following

Proposition 3 *Let $\{(N_i, M, P_i) : i = 1, \ldots, m\}$ be as above a collection of P_i-primary modules $N_i \subset M$, such that $N = \cap N_i$ is an eventually redundant primary decomposition of N in M with pairwise different primes P_i.*

Let $f \in S$ separate $\{P_j \not\subset P_i\}$ from P_i and compute $M_i := N :_M (f)^\infty$.

Then $P_i \notin Ass(M/N)$ iff $M_i = M_i :_M P_i^\infty$.

This proposition is in the spirit of [22, cor. 2.22]. It gives the possibility "locally" to check primes whether they belong to $Ass(M/N)$, i.e. not referring to the corresponding primary components themselves. Hence one can do this check on the list of primes produced by $PrimeDecomposeA(N, M)$ before primary components corresponding to the same prime are collected together.

[4, thm. 1.1] proposes another way to find the associated primes of M/N: A prime $P \subset S$ of codimension e is associated to M/N iff P is an isolated prime of $Ann\ Ext^e_S(M/N, S)$.

6 Some Examples

We conclude with some easy examples to demonstrate the algorithms "at work". The following computations were done with an experimental implementation of the above algorithms based on our REDUCE package CALI [7] on an IBM RS/6000. The examples are taken from [16] and were computed wrt. the pure lexicographic term order with $x_0 > x_1 > \ldots$.

Ex. 1 ([16, 8.1.1]) : This is a monomial ideal in $S = k[x_0, x_1, x_2, x_3]$ with two isolated and one embedded component:

$$I = (x_0^2 x_1 ,\ x_0 x_2^2 ,\ x_1^2 x_2 ,\ x_2^3)$$

The isolated primes, computed by FGB, are $P_1 = (x_0 ,\ x_2)$ and $P_2 = (x_1 ,\ x_2)$. As ideal separators we can take $f_1 = x_1$ and $f_2 = x_0$. This yields

$$I_1 = I : (x_1)^\infty = (x_0^2 ,\ x_2) \text{ with } f_1^2 I_1 \subset I,$$
$$I_2 = I : (x_0)^\infty = (x_1 ,\ x_2^2) \text{ with } f_2^2 I_2 \subset I$$

and finally

$$I = I_1 \cap I_2 \cap (I\ +\ (x_0^2 ,\ x_1^2)).$$

Here

$$I_3 := I + (x_0^2\,,\ x_1^2) = (x_0\,x_2^2\,,\ x_2^3\,,\ x_0^2\,,\ x_1^2)$$

is already P_3-primary with $P_3 = (x_0\,,\ x_1\,,\ x_2)$.

To decide whether I_3 is necessary for a *minimal* primary decomposition we compute $I : P_3^\infty = (x_1\,x_2\,,\ x_2^2\,,\ x_0^2\,x_1)$. Since $I : P_3^\infty \neq I$ we conclude that $P_3 \in Ass\ S/I$.

Ex. 2 ([16, 8.1.3]) : This is a monomial ideal in $S = k[x_0, x_1, x_2]$ with one isolated and one embedded component:

$$I = (x_1) \cdot (x_0\,,\ x_1\,,\ x_2) = (x_1^2\,,\ x_1\,x_2\,,\ x_0\,x_1).$$

The only isolated prime is $P_1 = (x_1)$. Taking $(x_0\,,\ x_2)$ as maximal independent set and $\tilde{S} = k(x_0, x_2)[x_1]$ we obtain $I_1 = \tilde{I} \cap S = I : (x_0\,x_2)^\infty = (x_1)$ and

$$I = I_1 \cap (I + (x_0\,x_2^2))$$

$J := I + (x_0\,x_2^2) = (x_1^2\,,\ x_1\,x_2\,,\ x_0\,x_1\,,\ x_0\,x_2^2)$ decomposes as the ideal in ex. 1 into

$$J = (x_1\,,\ x_2^2) \cap (x_0\,,\ x_1) \cap (J + (x_0\,,\ x_2^2)),$$

where $J + (x_0\,,\ x_2^2) = (x_1^2\,,\ x_1\,x_2\,,\ x_0\,,\ x_2^2)$ is (x_0, x_1, x_2)-primary. Altogether we obtain the (not minimal) primary decomposition

$$I = (x_1) \cap (x_1\,,\ x_2^2) \cap (x_0\,,\ x_1) \cap (x_1^2\,,\ x_1\,x_2\,,\ x_0\,,\ x_2^2).$$

To extract from the decomposition computed so far a minimal primary decomposition, we have to apply our necessity check to the primes in $L = \{(x_1\,,\ x_2), (x_0\,,\ x_1), (x_0\,, x_1\,, x_2)\}$.

For $P_2 = (x_1\,,\ x_2)$ we first separate it from $\{(x_0\,,\ x_1), (x_0\,, x_1\,, x_2)\}$ by $f = x_0$. We obtain $I' = I : (x_0)^\infty = (x_1)$, that has evidently no P_2-primary component. Hence the P_2-component in the decomposition of I may be skipped. The same applies to $P_3 = (x_0\,,\ x_1)$.

For $P_4 = (x_0\,, x_1\,, x_2)$ there is nothing to separate. Since $I : P_4^\infty = (x_1) \neq I$ we conclude that this component cannot be skipped.

Altogether we obtain the minimal primary decomposition

$$I = (x_1) \cap (x_1^2\,,\ x_1\,x_2\,,\ x_0\,,\ x_2^2).$$

Ex. 3 ([16, 8.5.2]) This is a presentation of Macaulay's curve as a set theoretic intersection of three surfaces

$$I = (x_0\,x_3 - x_1\,x_2\,,\ x_0^2\,x_2 - x_1^3\,,\ x_1\,x_3^2 - x_2^3)$$

FGB produces the only isolated prime $P_1 = I + (f)$ with $f := x_0\,x_2^2 - x_1^2\,x_3$. Since our term order is already an inverse block order for the maximal independent set $(x_2\,,\ x_3)$, we extract from the Gröbner basis

$$\begin{aligned} B = \{&x_0\,x_1\,x_2^2 - x_1^3\,x_3\,,\ x_0\,x_2^3 - x_1^2\,x_2\,x_3\,,\\ &x_0\,x_3 - x_1\,x_2\,,\ x_0^2\,x_2 - x_1^3\,,\ x_1\,x_3^2 - x_2^3\} \end{aligned}$$

of $I \subset S$ the minimal Gröbner basis $B' = \{x_0\,x_3 \,-\, x_1\,x_2\,,\ x_1\,x_3^2 \,-\, x_2^3\}$ of $\tilde{I}$ and $c = x_3 \in S$ as the (square free) product of the leading coefficients of B' regarded as polynomials in $\tilde{S}$. Since $I : (c)^\infty = P_1$ and $c\,f \in I$ we conclude

$$I = P_1 \cap (I + (c)),$$

where $J := I{+}(c) = (x_2^3\,,\ x_1\,x_2\,,\ x_3\,,\ x_0^2\,x_2 - x_1^3)$ is P_2-quasi primary with $P_2 := (x_3\,,\ x_2\,,\ x_1)$.

For J only (x_0) may serve as maximal independent set, so we have to compute a Gröbner basis of J wrt. an appropriate inverse block order, where x_0 is the lowest variable. As in the computation for I we obtain

$B = \{x_0^2\,x_2^2\,,\ x_2^3\,,\ x_1\,x_2\,,\ x_3\,,\ -x_0^2\,x_2 \,+\, x_1^3\}$,
$B' = \{x_0^2\,x_2^2\,,\ x_1\,x_2\,,\ x_3\,,\ -x_0^2\,x_2 \,+\, x_1^3\}$,
$c = x_0$,
$I_2 := J : (c)^\infty = (x_2^2\,,\ x_1\,x_2\,,\ x_3\,,\ -x_0^2\,x_2 \,+\, x_1^3)$
as the P_2-primary component and

$$J = I_2 \cap (J + (x_0^2)).$$

Here $K := J + (x_0^2) = (x_0^2\,,\ x_2^3\,,\ x_1\,x_2\,,\ x_3\,,\ x_1^3)$ is P_3-primary with $P_3 = (x_0\,,\ x_1\,,\ x_2\,,\ x_3)$.

Altogether we obtain the decomposition $I = P_1 \cap I_2 \cap K$, where again I_2 may be skipped. Indeed, separating $\{P_3\}$ from P_2 by a stable quotient by x_0 we get

$$\begin{aligned} I' = I : (x_0)^\infty = (&-x_0\,x_2^2 \,+\, x_1^2\,x_3\,,\ -x_0\,x_3^3 \,+\, x_2^4\,,\ -x_0\,x_3 \,+\, x_1\,x_2\,,\\ &-\, x_0^2\,x_2 \,+\, x_1^3\,,\ x_1\,x_3^2 \,-\, x_2^3) \end{aligned}$$

and $I' : P_2^\infty = I'$.

References

[1] Alonso, M.E., Mora, T., Raimondo, M.: Local decomposition algorithms. In: Proc. AAECC-6, Lect. Notes Comp. Sci. 508 (1991), 208 - 221.

[2] Becker, T., Weispfenning, V., Kredel, H. : A computational approach to commutative algebra. Springer, New York 1993.

[3] Eisenbud, D.: Commutative algebra with a view toward algebraic geometry. Springer, New York 1995.

[4] Eisenbud, D., Huneke, C., Vasconcelos, W.V.: Direct methods for primary decomposition. *Inv. Math.* **110** (1992), 207 - 235.

[5] Gianni, P., Trager, B., Zacharias, G.: Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6** (1988), 149 - 167.

[6] Gräbe, H.-G.: Two remarks on independent set. *J. Alg. Comb.* **2** (1993), 137 - 145.

[7] Gräbe, H.-G.: CALI – A REDUCE package for commutative algebra. Version 2.2.1, June 1995.
Available via WWW from `http://www.informatik.uni-leipzig.de/~graebe`.

[8] Gräbe, H.-G.: On factorized Gröbner bases. In: "Computer algebra in Science and Engineering", World Scientific, Singapore 1995, 77 - 89.

[9] Gräbe, H.-G.: Triangular systems and factorized Gröbner bases. In: Proc. AAECC-11, Lect. Notes Comp. Sci. 948 (1995), 248 - 261.

[10] Kalkbrener, M.: Prime decompositions of radicals in polynomial rings. *J. Symb. Comp.* **18** (1994), 365 - 372.

[11] Kredel, H.: Primary ideal decomposition. In: Proc. EUROCAL-87, Lect. Notes Comp. Sci. 378 (1989), 270 - 281.

[12] Krick, T., Logar, A.: An algorithm for the computation of the radical of an ideal in the ring of polynomials. In: Proc. AAECC-9, Lect. Notes Comp. Sci. 539 (1991), 195 - 205.

[13] Lazard, D.: Ideal bases and primary decomposition: case of two variables. *J. Symb. Comp.* **1** (1985), 261 - 270.

[14] Neff, C.A.: Decomposing algebraic sets using Gröbner bases. *Comp. Aided Geom. Design* **6** (1989), 249 - 263.

[15] Noro, M., Takeshima, T.: Risa/Asir – a computer algebra system. In: Proc. ISSAC'92, ACM Press, New York 1992, 387 - 396.
Available via WWW from `ftp://ftp.mm.sophia.ac.jp/Asir`.

[16] Renschuch, B.: Elementare und praktische Idealtheorie. VEB Deutscher Verlag der Wissenschaften, Berlin 1976.

[17] Rutman, E. W.: Gröbner bases and primary decomposition of modules. *J. Symb. Comp.* **14** (1992), 483 - 503.

[18] Seidenberg, A.: Constructions in algebra. *Trans. Amer. Math. Soc.* **197** (1974), 273 - 313.

[19] Seidenberg, A.: Constructions in a polynomial ring over the integers. *Amer. J. Math.* **100** (1978), 685 - 703.

[20] Seidenberg, A.: On the Lasker-Noether decomposition theorems. *Amer. J. Math.* **106** (1984), 611 - 638.

[21] Sharp, R. Y.: Steps in commutative algebra. Cambridge Univ. Press 1990.

[22] Shimoyama, T., Yokoyama, K.: Localization and primary decomposition of polynomial ideals. To appear in *J. Symb. Comp.*

[23] Yokoyama, K., Noro, M., Takeshima, T.: Solutions of systems of algebraic equations and linear maps on residue class rings. *J. Symb. Comp.* **14** (1992), 399 - 417.