ARTICLE IN PRESS

Journal of Symbolic Computation ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Computing minimal associated primes in polynomial rings over the integers

Sebastian Jambor [1]

Lehrstuhl B für Mathematik, RWTH Aachen University, Templergraben 64, D–52062 Aachen, Germany

ARTICLE INFO

Article history:
Received 6 November 2010
Accepted 12 May 2011
Available online xxxx

Keywords:
Minimal associated primes
Primary decomposition

ABSTRACT

An algorithm is presented to compute the minimal associated primes of an ideal in a polynomial ring over the integers. It differs from the known algorithms insofar as it avoids having to compute Gröbner bases over the integers until the very end, thereby eliminating one of the bottlenecks of those algorithms.

1. Introduction

This paper presents an algorithm to compute the minimal associated primes of an ideal in a polynomial ring over the integers, based on an algorithm by Fabiańska (Fabiańska, 2009).

Efficient algorithms to compute the primary decomposition of ideals over fields have been known for quite a while (see (Decker et al., 1999) for an overview), and they have been implemented in most computer algebra systems for commutative algebra (for example, Magma (Bosma et al., 1997), Singular (Decker et al., 2010), and Macaulay2 (Grayson and Stillman, 2010)). The idea in Fabiańska's algorithm is to use these algorithms to compute the minimal associated primes over the rationals and over various finite fields, and combine these results to get the minimal associated primes over the integers. Of course, one has to know over which finite fields the computations have to be done, or, in other words, one has to know which primes can occur in some minimal associated prime ideal. The first step in the algorithm is therefore to compute a Gröbner basis over the integers to get a sufficient list of those primes. Unfortunately, this initial computation is often the bottleneck of the whole algorithm, since a Gröbner basis calculation over the integers can be several orders of magnitude slower than a Gröbner basis calculation over a field. It is therefore desirable to find a way to

E-mail address: sebastian@momo.math.rwth-aachen.de.
[1] Tel.: +49 241 80 93508; fax: +49 241 80 92502.

0747-7171/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2011.05.010

Please cite this article in press as: Jambor, S., Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation (2011), doi:10.1016/j.jsc.2011.05.010

compute the necessary primes which avoids calculations over the integers. This is done in this paper, where the computation over the integers is replaced by several computations over the rationals and over finite fields, which is usually still much faster than a computation over the integers.

The need for an efficient algorithm to compute the minimal associated primes over the integers arose in computations with the L_2-quotient algorithm (see (Plesken and Fabiańska, 2009; Fabiańska, 2009)) and the L_3-U_3-quotient algorithm (presented in a forthcoming paper). In the last section, I will present several examples of ideals which came up in this context, and also from other sources, together with timings taken with and without this new method.

Note that recently an algorithm was developed to compute a primary decomposition over the integers (see (Pfister et al., 2011)), which is implemented in Singular.

2. The algorithm

In this whole section, I is an ideal of the ring $\mathbb{Z}[\underline{x}] = \mathbb{Z}[x_1, \ldots, x_n]$, and $p \in \mathbb{Z}$ is some prime number. Furthermore, $\nu_p\colon \mathbb{Z}_{\langle p\rangle}[\underline{x}] \to \mathbb{F}_p[\underline{x}]$ is the canonical epimorphism, where $\mathbb{Z}_{\langle p\rangle} = \{\frac{f}{g} \mid f, g \in \mathbb{Z}, p \nmid g\}$; we also write $\overline{f}$ instead of $\nu_p(f)$ for $f \in \mathbb{Z}_{\langle p\rangle}[\underline{x}]$, and $\overline{X}$ instead of $\nu_p(X)$ for subsets $X \subseteq \mathbb{Z}_{\langle p\rangle}[\underline{x}]$. Furthermore, we set $\mathbb{Q}I := I \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\operatorname{minAss}(I)$ denotes the set of minimal associated primes of I.

For $q \in \mathbb{Z}$ a prime or zero, define $\operatorname{minAss}_q(I) := \{P \in \operatorname{minAss}(I) \mid P \cap \mathbb{Z} = \langle q\rangle_{\mathbb{Z}}\}$. Then it is well known that $\operatorname{minAss}_0(I) = \{P' \cap \mathbb{Z}[\underline{x}] \mid P' \in \operatorname{minAss}(\mathbb{Q}I)\}$ (see, for example, (Atiyah and Macdonald, 1969)). Prime ideals containing an integer are handled as follows.

Proposition 1 (*Fabiańska, 2009, Lemma 1.3.11*)**.** *For any prime p, we have*

$$\operatorname{minAss}_p(I) = \{\nu_p^{-1}(\widetilde{P}) \mid \widetilde{P} \in \operatorname{minAss}(\nu_p(I)) \text{ with } \nu_p^{-1}(\widetilde{P}) \not\supseteq P' \text{ for all } P' \in \operatorname{minAss}_0(I)\}.$$

Proof. Let $P_1, \ldots, P_r$ be the minimal associated primes of I, and $\widetilde{P}_1, \ldots, \widetilde{P}_s$ the minimal associated primes of $\overline{I}$. Then, for any $i \in \{1, \ldots, s\}$, we have

$$P_1 \cap \cdots \cap P_r = \sqrt{I} \subseteq \nu_p^{-1}\left(\sqrt{\overline{I}}\right) \subseteq \nu_p^{-1}(\widetilde{P}_i),$$

so $\nu_p^{-1}(\widetilde{P}_i)$ contains some minimal associated prime of I.

Now let $j \in \{1, \ldots, r\}$ such that $p \in P_j$. Then $\widetilde{P}_1 \cap \cdots \cap \widetilde{P}_s \subseteq \nu_p(P_j)$, so $\widetilde{P}_i \subseteq \nu_p(P_j)$ for some i, and hence $\nu_p^{-1}(\widetilde{P}_i) \subseteq P_j$. But we proved above that $P_k \subseteq \nu_p^{-1}(\widetilde{P}_i)$ for some k, and hence $P_k = \nu_p^{-1}(\widetilde{P}_i) = P_j$, by the minimality of P_j. □

Obviously, $\operatorname{minAss}(I) = \operatorname{minAss}_0(I) \cup \bigcup_{p \text{ prime}} \operatorname{minAss}_p(I)$. Thus, instead of doing the computation over the integers, we can do (almost) all calculations over the rationals and over finite fields.

Example 2. Let $I = \langle 2x^2 + 3x + 1, x^2 + 3x + 2\rangle \trianglelefteq \mathbb{Z}[x]$; set $p := 3$. Then $\operatorname{minAss}_0(I) = \{\langle x + 1\rangle\}$ and $\operatorname{minAss}(\overline{I}) = \{\langle \overline{x + 1}\rangle, \langle \overline{x + 2}\rangle\}$. Using Proposition 1, it follows that $\langle 3, x + 2\rangle$ is a minimal associated prime of I, but $\langle 3, x + 1\rangle$ is not.

For $p = 2$, we get $\operatorname{minAss}(\overline{I}) = \{\langle \overline{x + 1}\rangle\}$, so $\operatorname{minAss}_2(I) = \emptyset$.

It remains to find the primes p for which $\operatorname{minAss}_p(I)$ is non-empty.

One way to do this is the following (used in (Fabiańska, 2009)). There exists a multiplicatively closed subset $S \subseteq \mathbb{Z}$ generated by finitely many primes such that $\mathbb{Q}I \cap \mathbb{Z}[\underline{x}] = S^{-1}I \cap \mathbb{Z}[\underline{x}]$. Then every prime contained in an associated prime of I is contained in S (Atiyah and Macdonald, 1969, Proposition 4.9). To determine such S one can use Gröbner bases over $\mathbb{Z}$.

Proposition 3 (*Adams and Loustaunau, 1994, Proposition 4.4.4*)**.** *Let G be a Gröbner basis of I, and let S be generated by the prime factors of leading coefficients of G. Then $\mathbb{Q}I \cap \mathbb{Z}[\underline{x}] = S^{-1}I \cap \mathbb{Z}[\underline{x}]$.*

Unfortunately, Gröbner basis computations over the integers can be very expensive and several orders of magnitudes slower than a calculation over $\mathbb{Q}$ or over a finite field. We would therefore like to have another criterion which is less expensive.

It is an elementary fact that p occurs in an associated prime of I if and only if $(I : p) \neq I$. This gives a criterion to decide for a single prime p whether we should bother to compute $\operatorname{minAss}_p(I)$, but this decision still has to be made for every single prime. Thus, as a first step, the set of primes one has to consider is reduced to a finite set.

Please cite this article in press as: Jambor, S., Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation (2011), doi:10.1016/j.jsc.2011.05.010

Proposition 4. *Let G be a reduced Gröbner basis of $\mathbb{Q}I$ (we always assume that a reduced Gröbner basis consists of monic elements). Let $S \subseteq \mathbb{Z}$ be the multiplicatively closed subset generated by all prime divisors of denominators which occurred during Buchberger's algorithm applied to any generating set of I, and $T \subseteq S$ the multiplicatively closed subset generated by all prime divisors of denominators of G. Then:*

1. *For any prime $p \in \mathbb{Z}-S$ we have $(I : p) = I$. In particular, the prime numbers which occur in associated primes of I are contained in S.*
2. *Assume that T is generated by $p_1, \ldots, p_\ell$, and that S is generated by $p_1, \ldots, p_m$. Then*

$$T^{-1}(I : (p_{\ell+1} \cdots p_m)^\infty) = \langle G \rangle_{T^{-1}\mathbb{Z}[\underline{x}]}.$$

Proof. Let $I = \langle f_1, \ldots, f_r \rangle$. Then any $g \in G$ can be written as $g = \sum_{i=1}^{r} \frac{z_i}{s_i} f_i$ with $z_i \in \mathbb{Z}[\underline{x}]$ and $s_i \in S$, for all i.

1. Let $f \in (I : p) \subseteq \mathbb{Q}I$. Then $f \in \mathbb{Q}I \cap \mathbb{Z}[\underline{x}]$, so $f = \sum_{g \in G} \lambda_g g$ with $\lambda_g \in T^{-1}\mathbb{Z}[\underline{x}]$, since all $g \in G$ are monic; thus $sf \in I$ for a suitable $s \in S$. But $pf \in I$, and p and s are coprime; hence $f \in I$.
2. By the first statement, we have $\mathbb{Q}I \cap \mathbb{Z}[\underline{x}] = S^{-1}I \cap \mathbb{Z}[\underline{x}] = (I : (p_1 \cdots p_m)^\infty)$, so localizing gives

$$T^{-1}(I : (p_{\ell+1} \cdots p_m)^\infty) = T^{-1}(\mathbb{Q}I \cap \mathbb{Z}[\underline{x}]) = \mathbb{Q}I \cap T^{-1}\mathbb{Z}[\underline{x}].$$

But G is a Gröbner basis of $\mathbb{Q}I \cap T^{-1}\mathbb{Z}[\underline{x}] \trianglelefteq T^{-1}\mathbb{Z}[\underline{x}]$, which gives the result. □

Example 5. Let $I = \langle 2x^2 + 3x + 1, x^2 + 3x + 2 \rangle \trianglelefteq \mathbb{Z}[x]$ be as in Example 2. Depending on the order in which the two generators are processed, S is generated either by 2, or by 2 and 3. In both cases, Example 2 proves that $\operatorname{minAss}(I) = \{\langle x + 1 \rangle, \langle 3, x + 2 \rangle\}$.

Note that this proposition is independent of the monomial order used in the computation of the Gröbner basis. In particular, we only have to consider those primes which occur as denominators in *any* Gröbner basis calculation of $\mathbb{Q}I$. This can be used to our advantage in two ways. First, by computing a new reduced Gröbner basis, one can try to reduce the number of primes we have to consider. Second, and perhaps even more importantly, it can help to determine the primes in the first place. The problem is that during the computation the denominators can get very big, often the size of several hundred decimal digits, so there is no efficient way to compute the prime factors of this number. Let d be such a denominator. The solution is to compute another reduced Gröbner basis and collect the denominators D of the computation. Then, instead of keeping d, only the greatest common divisors of d with all elements of D are necessary.

While the proposition above reduces the number of primes to consider to a finite set, this set can still be very big, and computing the minimal associated primes of I modulo all these primes can be expensive. So remember again the criterion $(I : p) \neq I$ to decide if p is necessary. Of course, this could be decided using several Gröbner basis calculations over the integers, but this should be avoided. However, the equivalent inequation $(I : p^\infty) \neq I$ can be decided with a calculation over the field $\mathbb{F}_p$:

Lemma 6. *We have $(I : p^\infty) \supsetneq I$ if and only if $\overline{(I : p^\infty)} \supsetneq \overline{I}$.*

Proof. Assume that $(I : p^\infty) \supsetneq I$, and let $\ell \in \mathbb{N}$ be minimal with $(I : p^\ell) = (I : p^\infty)$. Choose $f \in (I : p^\ell) - (I : p^{\ell-1})$, and suppose that $\overline{f} \in \overline{I}$. Then $\overline{f} = \overline{g}$ for some $g \in I$, so $p | (f - g)$; in particular, $\frac{f-g}{p} \in (I : p^\infty)$. But $p^\ell \frac{f-g}{p} = p^{\ell-1}f - p^{\ell-1}g \notin I$, by the choice of f, which is a contradiction. □

Proposition 7. *Let G, S, and T be as in Proposition 4, and let p be a prime not contained in T. Then p is contained in an associated prime of I if and only if $\langle \overline{G} \rangle_{\mathbb{F}_p[\underline{x}]} \supsetneq \overline{I}$.*

Proof. We may assume that $p \in S$. Then $\langle \overline{G} \rangle_{\mathbb{F}_p[\underline{x}]} = \overline{\langle G \rangle_{T^{-1}\mathbb{Z}[\underline{x}]}} = \overline{(I : p^\infty)}$, by the second statement of Proposition 4. The claim now follows by the lemma. □

Now the algorithm can be formulated; it is presented as Algorithm 1.

Note that the only time a Gröbner basis calculation over $\mathbb{Z}$ is necessary is in line 2. The decision in line 5 whether D cannot be factored, or if $|S|$ is too big, is a matter of experimentation. The current implementation tries in lines 5–9 only to factor integers of size less than 2^{150} and to get the size of S below 20. If after five Gröbner basis computations over the rationals this cannot be established, it

Please cite this article in press as: Jambor, S., Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation (2011), doi:10.1016/j.jsc.2011.05.010

Algorithm 1 Compute the minimal associated primes of an ideal

Input: An ideal $I \lhd \mathbb{Z}[\underline{x}]$.
Output: The set $\{P_1, \ldots, P_k\}$ of minimal associated prime ideals of I.

1: Compute the minimal associated primes $\{P'_1, \ldots, P'_r\}$ of $\mathbb{Q}I$ (using one of the well-known algorithms).
2: Compute $\text{minAss}_0(I) = \{P'_i \cap \mathbb{Z}[\underline{x}] \mid i = 1, \ldots, r\}$.
3: Compute a reduced Gröbner basis G of $\mathbb{Q}I$, consisting of monic polynomials. Let D be the set of denominators occurring in the Gröbner basis computation, and T the set of denominators of elements of G.
4: Try to compute the set S of prime factors of D.
5: **while** entries in D cannot be factored or $|S|$ is too big **do**
6: Compute another reduced Gröbner basis with respect to some other monomial order, and let D' be the set of denominators occurring in this computation.
7: Replace D by $\{\gcd(d, d') \mid d \in D, d' \in D'\}$.
8: Try to compute the set S of prime factors of D.
9: **end while**
10: **for** $p \in S$ **do**
11: **if** p divides an element of T or $\langle \overline{G} \rangle \supsetneq \overline{I}$ **then**
12: Compute the minimal associated primes $\{\widetilde{P}_1, \ldots, \widetilde{P}_s\}$ of $\overline{I}$ (using one of the well-known algorithms).
13: Compute $\text{minAss}_p(I) = \{\nu_p^{-1}(\widetilde{P}_i) \mid i \in \{1, \ldots, s\} \text{ and } \nu_p^{-1}(\widetilde{P}_i) \not\supseteq P' \text{ for all } P' \in \text{minAss}_0(I)\}$.
14: **end if**
15: **end for**
16: **return** $\bigcup_{q \in \mathcal{P} \cup \{0\}} \text{minAss}_q(I)$.

tries to factor arbitrary numbers and accepts any size of S. With this approach, for any ideal for which a Gröbner basis over the rationals could be computed, the algorithm was able to compute a set S of necessary primes.

Also note that lines 3–9 can be parallelized, as well as lines 10–15.

3. Examples

The Gröbner basis algorithm used to compute the necessary primes is Ginv (Blinkov and Gerdt, 2008), an implementation of the involutive basis algorithm by Gerdt and Blinkov (Gerdt, 2005) computing Janet bases (see (Plesken and Robertz, 2005)), which has an option to collect all denominators occurring in a Janet basis computation.

The first two examples are taken from the SymbolicData Project (Gräbe, 2010).

Example 8 (*ZeroDim.example_54.xml*)**.** After the first run of the involutive basis algorithm over the rationals, the biggest denominator is of size 10^{85}, so the algorithm does not try to factor this number. After the second run, there are 35 primes left, and after another two runs, this is reduced to 18 primes, which are then tested using the criterion of Proposition 7, leaving only six primes. Apart from the minimal associated primes which occur already in a calculation over the rationals, this ideal also has a minimal associated prime ideal containing 2, and another one containing 3.

Example 9 (*Gerdt-85_1.xml*)**.** There are two calculations needed over the rationals to reduce the number of necessary primes from 60 to 13, and after the modular criterion we see that only seven primes are necessary. There are 22 minimal associated primes, and 14 of these prime ideals contain one of the prime numbers 2, 3, 5, or 7.

The next set of examples comes up in a run of the L_3-U_3-quotient algorithm (presented in a forthcoming paper).

Example 10 (L_3-U_3-*quotient Algorithm*)**.** The L_3-U_3-quotient algorithm finds all epimorphic images of a finitely presented group which are isomorphic to PSL(3, q) or to PSU(3, q) simultaneously for

Please cite this article in press as: Jambor, S., Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation (2011), doi:10.1016/j.jsc.2011.05.010

Table 1
Time (in seconds) to compute the necessary primes, the minimal associated primes of the ideal, and the Gröbner basis over $\mathbb{Z}$ of the ideal. The value ∞ means that the computation did not finish after 5 h, and OOM means that the process tried to use more than 8 GB of memory.

Example	Compute minAss(I)			Gröbner basis over $\mathbb{Z}$			
	Rational criterion	Modular criterion	Associated primes	Ginv	Macaulay2	Magma	Singular
Example 8	9.8	1.5	9.2	197.3	4.2	38.9	OOM
Example 9	0.6	0.1	3.2	5253.6	∞	∞	OOM
Example 10.1	35.9	12.4	3.2	15.8	52.4	29.5	∞
Example 10.2	4.3	2.0	0.6	16.8	OOM	26.7	∞
Example 10.3	7.8	6.3	2.6	24.5	OOM	OOM	∞
Example 10.4	7.2	2.9	0.8	175.4	OOM	12873.1	∞
Example 10.5	1.1	5.4	1.5	466.0	OOM	OOM	∞

any q. We start with the group $\langle a, b \mid a^2, b^6, (ab)^7, [a, b]^8\rangle$, and during the computation we have to compute the minimal associated primes of five ideals. The first one is an ideal in the ring $R := \mathbb{Z}[x_1, x_{-1}, x_2, x_{-2}, x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}, x_{[1,2]}]$, with a grading of the variables given by $\deg(x_i) = 2$ and $\deg(x_{i,j}) = 4$ for $i, j \in \{-2, -1, 1, 2\}$, and $\deg(x_{[1,2]}) = 8$; the other four ideals are ideals in the ring $R[\zeta]$, with $\deg(\zeta) = 1$ and the relation $\zeta^2 + \zeta + 1$.

Each ideal has at least one minimal associated prime containing a prime number.

The ideals are referred to in Table 1 as Example 10.1 to Example 10.5.

The following times are measured.

1. The time to find a sufficient list of primes (Proposition 4, corresponding to lines 3–9 of Algorithm 1) using Ginv, listed in column "Rational criterion".
2. The time to reduce this list to a necessary list of primes (Proposition 7, corresponding to line 11 of Algorithm 1) using Magma, listed in column "Modular criterion".
3. The time to compute the minimal associated primes (Proposition 1, corresponding to lines 2, 12, and 13 of Algorithm 1) using Magma, listed in column "Associated primes".

For comparison, the time to compute a Gröbner basis or Janet basis over $\mathbb{Z}$ in various computer algebra systems is given. All computations were done on a Quad-Core AMD Opteron Processor 8356. Each process was given 5 h CPU time and 8 GB of RAM. The timings are recorded in Table 1. All source files for these examples are available from Jambor (2010). The program versions used are Singular 3-1-1, Magma V2.16-12, and Macaulay2 1.2. For Ginv, a current developer version was used, which is also available from Jambor (2010).

4. Another approach with fewer primes

The set S generated by the prime divisors of denominators occurring during Buchberger's algorithm is usually largely redundant. What are really necessary for the argument in Proposition 4 are the denominators of a representation of the Gröbner basis elements g in terms of the original ideal generators $f_1, \ldots, f_r$, that is, the s_i in some representation $g = \sum_{i=1}^{r} \frac{z_i}{s_i} f_i$ (see the proof of Proposition 4). As pointed out by one of the referees, the set generated by the prime divisors of those s_i can be considerably smaller than the set S considered in this paper.

While this is true, this approach is usually not an efficient alternative. There are mainly two problems. First, the standard approach to compute these representations is to do calculations in a certain submodule of $\mathbb{Q}[x]^{r+1}$ with a position over term order, so there is an additional cost for the polynomial arithmetic, which has to be done for $r + 1$ components instead of one component, which leads to increased time consumption. Second, while the polynomial generators f_i and the Gröbner basis elements are often sparse polynomials, the cofactors $\frac{z_i}{s_i}$ tend to be dense polynomials, which leads to increased memory consumption.

On the other hand, the approach presented in this paper, that is, remembering the denominators during the computation, is virtually cost free.

Please cite this article in press as: Jambor, S., Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation (2011), doi:10.1016/j.jsc.2011.05.010

There is a third problem with the standard approach to get the representations above. One is only interested in the first entry of the $r + 1$ entries, but the Gröbner basis with the position over term order will further reduce the elements where the first entry is zero. This is overcome in the Maple package Janet and its C++ counterpart Ginv (see (Blinkov et al., 2003, Section 4)), where computations are done in a submodule of $\mathbb{Q}[\underline{x}]^{r+1}$ as well, but only the first entry is considered for reductions.

Of the seven examples above, only one computation with simultaneous construction of the representations finished without exceeding 8 GB of memory (Example 8). And while in fact this alternative approach leads to fewer primes to consider (there are 37 primes in this alternative approach, while a Janet basis computation with the same monomial ordering, remembering only the denominators, produces 262 primes), the tradeoff is not acceptable. Just this one Janet basis computation takes 153.3 s with the alternative approach, while the approach presented in this paper takes 0.2 s. In fact, the whole computation of the minimal associated primes as presented here takes 20.5 s, so it finishes long before even the first Janet basis computation with the alternative approach in $\mathbb{Q}[\underline{x}]^{r+1}$ finishes.

5. Conclusion

This paper presents a method to compute the prime numbers which can occur in associated prime ideals of a given ideal $I \trianglelefteq \mathbb{Z}[\underline{x}]$ (see Section 2). In contrast to the known method, which relies on a Gröbner basis calculation over $\mathbb{Z}$, the new method relies entirely on a Gröbner basis calculation over prime fields. Together with the methods of Fabiańska's algorithm, this gives a new algorithm to compute the minimal associated prime ideals of an ideal in $\mathbb{Z}[\underline{x}]$, presented in Algorithm 1, which is often faster than the old approach.

The examples in Section 3 show that, even though the Gröbner basis calculation over $\mathbb{Z}$ can take a long time to finish, the computation of the minimal associated primes can be relatively fast. Examples 8 and 9 show in particular that it can be important to compute Gröbner bases with respect to different monomial orders to keep the Gröbner basis computations over finite fields to a minimum (in Example 9, a second Gröbner basis calculation reduces the number of primes to consider from 60 to 13, thereby replacing 47 otherwise necessary Gröbner basis computations over finite fields by a single Gröbner basis calculation over $\mathbb{Q}$).

Of course, there are examples where this new approach is slower than Fabiańska's method, for instance, if the Gröbner basis computation is fast with respect to one monomial order, but slow with respect to others (at present, the new monomial order is selected randomly). Furthermore, the Gröbner basis calculation over $\mathbb{Z}$ might be fast: in Example 10.1 it takes 15.8 s to compute the necessary primes by a Janet basis calculation over $\mathbb{Z}$, and about three times as long ($35.9 + 12.4 = 48.3$ s) to compute the necessary primes via the rational and the modular criterion. However, in applications, in particular the L_3-U_3-quotient algorithm, this new approach gives an overall speedup.

Acknowledgements

I would like to thank Daniel Robertz for many fruitful discussions, and for helpful comments on an early version of the paper. I would also like to thank one of the referees for pointing out a mistake in Proposition 4.

This work was partially supported by the SPP 1388 of the German Science Foundation (DFG).

References

Adams, W. W., Loustaunau, P., 1994. An introduction to Gröbner bases. In: Graduate Studies in Mathematics, Vol. 3. American Mathematical Society, Providence, RI.

Atiyah, M.F., Macdonald, I.G., 1969. Introduction to Commutative Algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont.

Blinkov, Y.A., Cid, C.F., Gerdt, V.P., Plesken, W., Robertz, D., 2003. The MAPLE package "Janet": I. Polynomial systems. In: Proc. 6th Int. Workshop on Computer Algebra in Scientific Computing. Passau Germany, pp. 31–40.

Blinkov, Y.A., Gerdt, V.P., 2008. The specialized computer algebra system GINV. Programmirovanie (2), 67–80.

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (3–4), 235–265. Computational algebra and number theory (London, 1993). http://dx.doi.org/10.1006/jsco.1996.0125.

Please cite this article in press as: Jambor, S., Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation (2011), doi:10.1016/j.jsc.2011.05.010

Decker, W., Greuel, G.-M., Pfister, G., 1997. Primary decomposition: algorithms and comparisons. In: Algorithmic Algebra and Number Theory (Heidelberg). Springer, Berlin, pp. 187–220.

Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H., 2010. Singular 3-1-1 — a computer algebra system for polynomial computations. http://www.singular.uni-kl.de.

Fabiańska, A., 2009. Algorithmic analysis of presentations of groups and modules. Ph.D. Thesis, RWTH Aachen University.

Gerdt, V.P., 2005. Involutive algorithms for computing Gröbner bases. In: Computational Commutative and Non-commutative Algebraic Geometry. In: NATO Sci. Ser. III Comput. Syst. Sci., Vol. 196. IOS, Amsterdam, pp. 199–225.

Gräbe, H.-G., 2010. The symbolicdata project. http://www.symbolicdata.org.

Grayson, D.R., Stillman, M.E., 2010. Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

Jambor, S., 2010. Source files for all ideals. http://wwwb.math.rwth-aachen.de/~sebastian.

Pfister, G., Sadiq, A., Steidel, S., 2011. An algorithm for primary decomposition in polynomial rings over the integers. Cent. Eur. J. Math. 9 (4), 897–904.

Plesken, W., Fabiańska, A., 2009. An L_2-quotient algorithm for finitely presented groups. J. Algebra 322 (3), 914–935. http://dx.doi.org/10.1016/j.jalgebra.2009.03.026.

Plesken, W., Robertz, D., 2005. Janet's approach to presentations and resolutions for polynomials and linear PDEs. Arch. Math. (Basel) 84 (1), 22–37. http://dx.doi.org/10.1007/s00013-004-1282-x.

Please cite this article in press as: Jambor, S., Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation (2011), doi:10.1016/j.jsc.2011.05.010