Elimination for Coefficients of Special Characteristic Polynomials

W. Plesken and D. Robertz

CONTENTS

2000 AMS Subject Classification: Primary 14Q20, 68W30, 20C40, 13P10; Secondary 14A05

Keywords: Characteristic polynomial, Kronecker product, elimination, Janet bases

Computing the relations for the coefficients satisfied by the characteristic polynomial of the Kronecker product of a general $n\times n$ matrix by a general $m \times m$ matrix leads to an elimination problem that is already difficult for small values of n and m. In this article we focus on the problems for $(n, m) \in \{(2, 3), (2, 4), (3, 3)\}$ and use these problems for developing and testing a new elimination technique called elimination by degree steering.

1. INTRODUCTION

Elimination has a long tradition in commutative algebra and algebraic geometry, starting from the classical resultant methods (see, for example, [van der Waerden 31, Chapter 11]), nowadays being partially replaced by Gröbner-basis techniques using elimination orders; see [Cox et al. 98] for a comparison of the two methods. The problem we wanted to treat came up in the context of the recognition problem for matrix groups over finite fields in [Leedham-Green and O'Brien 97]: Decide whether a polynomial of degree nm is the characteristic polynomial of a Kronecker product of two matrices of degrees $n, m \geq 2$. As C. Leedham-Green pointed out, eliminating the coefficients of the polynomials of degrees n and m from the expressions of the coefficients for the polynomial of degree nm in terms of these for the case $n = m = 2$ can be done by a short hand calculation. The next case, $6 = 2 \cdot 3$, has been solved by heavy machine calculations in [Schwingel 99] using Magma [Bosma et al. 97]. It was noted there that no package at that time could deal with the problem as it stands. Although, for instance, Singular [Greuel et al. 05] can now just about tackle the problem, it still has to give up on the next one, $8 = 2 \cdot 4$, although the equations can be written out in a few lines; see Section 5.

The purpose of this paper is twofold. Firstly, it develops a general elimination method, called elimination by degree steering. Secondly, it applies this method to the

1058-6458/2008 $ 0.50 per page

above problem for degrees $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, and partially for $9 = 3 \cdot 3$; see Section 2 for the formulation and main results, and Section 6 for the derivation and further details. The method was found and tested in the context of Janet bases. It certainly can also be used in the context of general Gröbner bases. For our computations we use the package Involutive [Blinkov et al. 03], where a powerful implementation of Janet's algorithm in C++ is available; see also [Blinkov et al. 07]. Theoretical details on this algorithm can be found in [Plesken and Robertz 05].

For the concrete problem, an essential step in the derivation is the investigation of the determinant-one case as described in Section 5. Both the computations and the results try to teach us something by their complexity: They do not seem to be adequate for the original problem. We therefore comment on the original problem of [Leedham-Green and O'Brien 97] in the last section. Nevertheless, the challenge is a really good one to give a new impulse to develop new elimination techniques.

Concerning the general algorithmic aspect, our main point is to demonstrate how the lexicographic term ordering can be avoided for the purpose of elimination. This ordering has its merits in short descriptions of elimination algorithms in the context of Gröbner bases, but in our experience, it is not so convincing for hard problems, at least not for Janet bases, which are special Gröbner bases. The algorithmic idea of this paper is to approximate the lexicographic term ordering using gradings, but only to the point that it performs the elimination and not any further. A simple but effective lemma shows when one has reached the aim; see Section 4. The same section also gives some probabilistic tools for judging the difficulty of an elimination problem beforehand. The preceding section gives some generalities on Janet bases, in particular pointing out their advantages for the sort of calculations performed in the present paper.

General files and Maple worksheets providing the results of Sections 2 and 6 are available on an associated web page for this paper: http://wwwb.math.rwth-aachen.de/charpoly.

2. RESULTS ON THE CHARACTERISTIC POLYNOMIALS

The characteristic polynomials that come up will be written in the form

$$p_{n,a} := t^n + \sum_{i=1}^{n} (-1)^i \, a_i t^{n-i},$$

with indeterminates a_i over the field $K := \mathbb{Q}$ or over $K := \mathbb{Z}$. The following elimination problem is considered: Given two polynomials $p_{n,a}$ and $p_{m,b}$, let $p_{nm,c}$ be the characteristic polynomial of the Kronecker product of their companion matrices. The set of relations obtained in this way will be called $K_{(n,m)}$:

$$K_{(n,m)} = \{c_1 - a_1 b_1,\ c_2 - a_1^2 b_2 - a_2 b_1^2 + 2a_2 b_2, \ldots, \\ c_{nm-1} - a_n^{m-1} a_{n-1} b_m^{n-1} b_{m-1},\ c_{nm} - a_n^m b_m^n\}.$$

The problem is to eliminate $a_1, \ldots, a_n, b_1, \ldots, b_m$ from $K_{(n,m)}$. Let

$$I_{(n,m)} := \langle K_{(n,m)} \rangle \cap K[c_1, \ldots, c_{nm}] \trianglelefteq K[c_1, \ldots, c_{nm}]$$

denote the elimination ideal. It is clearly prime. Assigning degree i to c_i turns $I_{(n,m)}$ into a homogeneous ideal and $R_{(n,m)} := K[c_1, \ldots, c_{nm}]/I_{(n,m)}$ into a graded K-algebra with field of fractions $Q_{(n,m)}$ of transcendence degree $n + m - 1$ over K. The image of c_i in $R_{(n,m)}$ or in $Q_{(n,m)}$ will also be denoted by c_i.

In the sequel we shall mainly give the Hilbert series of $R_{(n,m)}$ and the minimal number of homogeneous generators of $I_{(n,m)}$ according to their degrees. The latter will be written also as a generating function. For a graded ideal I in a $\mathbb{Z}_{\geq 0}$-graded finitely generated K-algebra A,

$$\epsilon(I) := \sum_i d_i t^i$$

will be called the *minimal basis number*, where d_i is the number of elements of degree i in any minimal set of homogeneous generators of I.

2.1 The Ideal $I_{(2,2)}$

Let $K := \mathbb{Z}$. The ideal $I_{(2,2)}$ is generated by $c_3^2 - c_1^2 c_4$, which has degree 6. In particular, the minimal basis number is $\epsilon(I_{(2,2)}) = t^6$. The Hilbert series for $R_{(2,2)}$ for $K := \mathbb{Q}$ is

$$\frac{1 + t^3}{(1 - t)\,(1 - t^2)\,(1 - t^4)}.$$

This is well known and can be computed by hand. Obviously, $R_{(2,2)}$ is Cohen–Macaulay.

2.2 The Ideal $I_{(2,3)}$

In [Schwingel 99], a minimal set of generators for $I_{(2,3)}$ in the case $K = \mathbb{Q}$ is claimed to have 16 elements of degrees between 19 and 30. We confirm this. However, the generators are too long to be listed, the first and shortest one $c_1^8 c_5 c_6 + \cdots + c_4 c_5^3$ having 53 monomials (rather than 28 as claimed in [Schwingel 99]). A complete list even for the more difficult case $K = \mathbb{Z}$ appears on the associated web page.

Proposition 2.1. *For $K = \mathbb{Q}$, the minimal basis number for $I_{(2,3)}$ is*

$$\epsilon(I_{(2,3)}) = t^{19} + t^{20} + 2t^{21} + 2t^{22} + 3t^{23} + 2t^{24} + t^{25} + t^{26} + t^{27} + t^{28} + t^{30}$$

and the Hilbert series for $R_{(2,3)}$ is

$$\frac{p-q}{(1-t)(1-t^2)(1-t^3)(1-t^4)}$$

with

$$\begin{aligned} p &= 1 + t^5 + t^6 + t^{10} + t^{11} + t^{12} + t^{15} + t^{16} + t^{17} + t^{18} \\ &\quad + t^{26} + t^{27} + t^{29}, \\ q &= t^{19}(1 + t^2 + t^3 + 2t^4 + t^6 + t^{11}). \end{aligned}$$

Corollary 2.2. *The algebra $R_{(2,3)}$ is not Cohen–Macaulay.*

Proof: In the above representation of the Hilbert series H as a rational function, numerator and denominator are relatively prime. If $R_{(2,3)}$ were Cohen–Macaulay, then one would have homogeneous elements e_1, e_2, e_3, e_4 in $R_{(2,3)}$ generating a polynomial algebra over K such that $R_{(2,3)}$ is free over $K[e_1, e_2, e_3, e_4]$ with a basis of homogeneous elements. Hence, if $a(i)$ denotes the degree of e_i, one would have

$$H = \frac{r}{(1-t^{a(1)})(1-t^{a(2)})(1-t^{a(3)})(1-t^{a(4)})}$$

with $r \in \mathbb{Z}[t]$ with all coefficients nonnegative. However, equating both sides, one sees that $(a(1), a(2), a(3), a(4))$ is bound to be obtainable from one of $(1, 2, 3, 4)$, $(1, 1, 6, 4)$, $(1, 1, 2, 12)$ by taking (possibly different) multiples in each slot after permuting the $a(i)$, because the denominator $(1-t^{a(1)})(1-t^{a(2)})(1-t^{a(3)})(1-t^{a(4)})$ must be divisible by

$$(1-t)(1-t^2)(1-t^3)(1-t^4) = \mu_1^4 \mu_2^2 \mu_3 \mu_4,$$

where μ_i denotes the ith cyclotomic polynomial. That is, one of the $a(i)$ must be divisible by 3, one by 4, and two by 2, leaving the described possibilities. In all three cases, the leading coefficient of

$$\frac{(1-t^{a(1)})(1-t^{a(2)})(1-t^{a(3)})(1-t^{a(4)})}{(1-t)(1-t^2)(1-t^3)(1-t^4)} \in \mathbb{Z}[t]$$

is positive, contradicting the fact that the leading coefficient of $p - q$ is negative. So, for instance, if the slots of $(a(1), a(2), a(3), a(4))$ are multiples of the slots of $(1, 1, 2, 12)$, then

$$\begin{aligned} \frac{1-t^{a(1)}}{1-t} &= 1 + t + \cdots + t^{a(4)-1}, \\ &\ldots, \\ \frac{1-t^{a(4)}}{1-t^{12}} &= 1 + t^{a(4)/12} + \cdots + t^{a(4)-a(4)/12}. \end{aligned}$$

□

The computation of the singular locus of $R_{(2,3)}$ is already a highly nontrivial affair with the present possibilities; we leave it as a challenge to the reader. Here are some data that are cheaper to obtain even before computing the presentation of $R_{(2,3)}$ (cf. Sections 4 and 6) and give at least some idea about the ordinary degrees of some of the relations and the structure of $R_{(2,3)}$:

Proposition 2.3. *Any four of the c_i are algebraically independent over K, and the degrees $[Q_{(2,3)} : K(c_{i(1)}, c_{i(2)}, c_{i(3)}, c_{i(4)})]$ with $1 \leq i(1) < i(2) < i(3) < i(4) \leq 6$ are in increasing order:* $3, 3, 4, 5, 5, 5, 6, 7, 7, 7, 7, 9, 9, 12, 18$.

2.3 The Ideal $I_{(2,4)}$

For $I_{(2,4)}$ we find a minimal set of generators consisting of 122 elements of degrees 28 to 40, the first $c_1^8 c_4 c_8^2 + \cdots + c_4 c_5^2 c_7^2$ having 125 terms. Complete listings are on the associated web page.

Proposition 2.4. *Let $K := \mathbb{Q}$. The minimal basis number for $I_{(2,4)}$ is*

$$\epsilon(I_{(2,4)}) = t^{28} + 11t^{30} + 9t^{31} + 36t^{32} + 20t^{33} + 22t^{34} + 10t^{35} + 8t^{36} + 3t^{37} + t^{39} + t^{40},$$

and the Hilbert series for $R_{(2,4)}$ is

$$\frac{p-q}{(1-t)(1-t^2)(1-t^3)(1-t^4)(1-t^6)}$$

with

$$\begin{aligned} p &= 1 + t^5 + t^7 + t^8 + t^{10} + t^{12} + t^{13} + t^{14} + 2t^{15} + t^{16} \\ &\quad + t^{17} + t^{18} + t^{19} + 2t^{20} + 2t^{21} + 2t^{22} + 2t^{23} + 2t^{24} \\ &\quad + 2t^{25} + 2t^{26} + 2t^{27} + 2t^{28} + 3t^{29} + 4t^{35} + 20t^{36} \\ &\quad + 19t^{37} + 34t^{38} + 8t^{39} + 5t^{40} + 7t^{45} + 3t^{46} + 3t^{47}, \\ q &= 8t^{30} + 6t^{31} + 33t^{32} + 17t^{33} + 12t^{34} + 13t^{41} + 18t^{42} \\ &\quad + 14t^{43} + 5t^{44}. \end{aligned}$$

The leading coefficient in the numerator $p - q$ is this time positive, so that the reasoning of the proof of Corollary 2.2 has to be modified, and it gets complicated. But it looks likely that $R_{(2,4)}$ is not Cohen–Macaulay. Again, the following information is much easier to obtain:

Proposition 2.5. *Any five of the c_i are algebraically independent over K, and the degrees $[Q_{(2,4)} : K(c_{i(1)}, \dots, c_{i(5)})]$ with $1 \leq i(1) < \cdots < i(5) \leq 8$ in increasing order with the numbers of instances in parentheses in case they are not equal to* 1 *are* 2(2)*,* 6(7)*,* 7*,* 9(3)*,* 10(2)*,* 11*,* 12(10)*,* 14(9)*,* 16(5)*,* 18*,* 20(2)*,* 22(2)*,* 24(2)*,* 25*,* 29*,* 32*,* 35(2)*,* 42(2)*,* 48(2)*.*

2.4 The Ideal $I_{(3,3)}$

Let $K := \mathbb{Q}$. In this case we have not computed a minimal generating set. However, we have obtained some information that demonstrates the size of the problem: The minimal basis number for $I_{(3,3)}$ is

$$\epsilon(I_{(3,3)}) = 19t^{30} + 60t^{31} + \text{higher-order terms}.$$

The Krull dimension of $R_{(3,3)}$ is still 5, any five of the c_i are algebraically independent over K, and the degrees $[Q_{(3,3)} : K(c_{i(1)}, \dots, c_{i(5)})]$ with $1 \leq i(1) < \cdots < i(5) \leq 9$ in increasing order with the numbers of instances in parentheses in case they are not equal to 1 are 6, 9, 10, 11(2), 12(13), 13(2), 14, 15(3), 16, 17(2), 18(6), 19(3), 20(3), 21(2), 24(8), 25, 26, 28, 29, 30(8), 31, 32(2), 35, 36(8), 37, 38(2), 39, 40, 42(6), 43, 44(2), 45(2), 48(10), 50(2), 51, 52, 53, 54(3), 66(2), 72(2), 78(3), 90(3), 108(4), 126(5).

In Section 6, the determinant-one case, where the additional relations $a_3 = b_3 = c_9 = 1$ are assumed, is fully treated and a possibility to get from there to generators of $I_{(3,3)}$ is outlined.

3. THE USE OF THE JANET ALGORITHM

Most of the computations for the cases $I_{(2,4)}$ and $I_{(3,3)}$ are on the verge of the present possibilities. Therefore it was important to use one of the most powerful Gröbner-basis packages available to us; we had access to the code to modify it according to our needs, which was the `ginv` package [Blinkov et al. 07]. In fact, we used the problems of this paper to test and improve this software. It works with Janet bases or—slightly more generally—involutive bases, which form a special case of Gröbner bases; cf. [Blinkov et al. 03, Blinkov et al. 01, Gerdt 05].

Apart from its good performance, the Janet algorithm provides a Janet basis, which has various other advantages. For instance, it immediately yields an explicit vector-space basis for the ideal as well as for the residue class ring, which among other things allows one to read off the Hilbert series in the homogeneous case, as given, for example, in Propositions 2.1 and 2.4; cf. [Plesken and Robertz 05]. (Note that in [Schwingel 99], a Gröbner basis for $I_{(2,3)}$ was computed, but not the Hilbert series.) Homogenizing the elements in the Janet basis with respect to a degree-compatible term ordering yields a Janet basis of the homogenized ideal; see Section 6 for details.

Since minimal generating sets of homogeneous elements came up in the previous section, we take the opportunity to demonstrate the usefulness of the concept of Janet bases in this context as well. See [Greuel et al. 05] for corresponding algorithms using general Gröbner bases. Our point is that within the philosophy of Janet bases with its multiplicative and nonmultiplicative variables, these computations come rather naturally.

Algorithm 3.1. (Minimal generating set for homogeneous ideals.)

Input: A degree $d \in \mathbb{N}$, a grading on the polynomial algebra $K[x_1, \dots, x_n]$ with x_i homogeneous, and the Janet basis J with respect to degree-reverse lexicographic ordering of a homogeneous ideal in $K[x_1, \dots, x_n]$, where K is a field.

Output: The subset M_d of J of those elements of degree d in J that form the degree-d elements in a minimal generating set of $\langle J \rangle$ of homogeneous elements.

Step 1: Compute the set N_d of unprocessed omission precandidates as follows:

$$N_d := \{x_i p \mid p \in J, x_i \text{ nonmultiplicative for } p, \\ \deg(x_i p) = d\}.$$

Step 2: Start with $J' := \{p \in J \mid \deg(p) < d\}$ with assignment of multiplicative variables taken from J and perform involutive reduction of the elements of N_d with respect to J'. An element of N_d that reduces to zero is omitted from N_d. An element $a \in N_d$ that reduces to a nonzero element a' is also removed from N_d, but a' is appended to J' (and is potentially an involutive divisor for further reductions in degree d). This process ends when N_d is empty.

Step 3: M_d consists of all those elements of degree d in $J_d := \{p \in J \mid \deg(p) = d\}$ whose leading monomial does not occur among the leading monomials of degree d in J'.

To validate this algorithm, define

$$L_d := \{mp \mid p \in J, \deg(p) < d, m \text{ a monomial in the multiplicative variables of } p, \deg(mp) = d\},$$

so that $J_d \uplus L_d$ is a K-vector-space basis of the homogeneous component $\langle J\rangle_d$ of the ideal generated by J. We are interested in $\langle J\rangle_d / \langle N_d, L_d\rangle_K$, which is dealt with in Step 2.

There is also an alternative to the above algorithm: The Janet basis J'' for the ideal generated by $J' := \{p \in J \mid \deg(p) < d\}$ is computed accurately up to degree d, so that involutive reduction can be performed properly on homogeneous elements of degree d with respect to J''. Then the difference of the t^d-coefficients of the two Hilbert series of $\langle J\rangle$ and $\langle J''\rangle$ gives the number of elements of M_d. If one wants to compute not just the number but the set of degree-d elements in some minimal generating set for the homogeneous ideal, then involutive reduction is performed on the elements of J of degree d, and similarly as in Step 2 above, J'' gets enlarged by the elements that do not reduce to 0. In the end, the elements of degree d in J'' can be taken to form the subset of elements of degree d in a minimal homogeneous generating set for the homogeneous ideal. The principles of the techniques developed here will also be essential for passing from $I^{(1,1)}_{(3,3)}$ to $I_{(3,3)}$ in Section 6.

4. ELIMINATION BY DEGREE STEERING

Here we give an elimination algorithm that uses the philosophy of the lexicographic or elimination-term ordering on the monomials without using these orderings themselves. Since our inspiration came from Janet bases and we have tested the ideas only on Janet bases, we formulate the criterion and the algorithm only for Janet bases, though it is clear that it works also for general Gröbner bases, as the referee pointed out. The approach also profits from the idea of a Gröbner walk.

Lemma 4.1. *Let $J \subseteq K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ be a Janet basis with respect to some term ordering. For any $0 \neq p \in K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ let $\lambda(p)$ be its leading monomial. If*

$$J \cap K[Y_1, \dots, Y_m] = \{p \in J \mid \lambda(p) \in K[Y_1, \dots, Y_m]\},$$

then $J \cap K[Y_1, \dots, Y_m]$ generates $\langle J\rangle \cap K[Y_1, \dots, Y_m]$.

Proof: The case $J \cap K[Y_1, \dots, Y_m] = \varnothing$ is trivial. Let $q \in \langle J\rangle \cap K[Y_1, \dots, Y_m]$ be nonzero. Since there is no X_i involved in q, it can be reduced by some element $p \in J$ with $\lambda(p)$ not divisible by any X_i. By hypothesis, $p \in K[Y_1, \dots, Y_m]$, so that the first step of involutive reduction replaces q by an element in $\langle J\rangle$, again without X_i's and with smaller leading monomial with respect to the given term ordering. So induction yields the result. □

Note that the last lemma does not claim that $J \cap K[Y_1, \dots, Y_m]$ is a Janet basis for $\langle J\rangle \cap K[Y_1, \dots, Y_m]$, which of course might sometimes happen. By the way, the lemma immediately implies that the lexicographic and the elimination-term orderings eliminate, because these term orderings enforce the hypothesis of Lemma 4.1. The point of the following algorithm is that one gradually reaches the state in which the hypothesis is satisfied by choosing different gradings for the polynomial ring.

Algorithm 4.2. (Degree steering.)

Input: A nonempty finite subset

$$N \subseteq K[X_1, \dots, X_n, Y_1, \dots, Y_m].$$

Output: A subset $M \subseteq K[Y_1, \dots, Y_m]$ generating

$$\langle N\rangle \cap K[Y_1, \dots, Y_m].$$

Algorithm: Run Janet's algorithm for N over K with respect to some term ordering that respects the grading. Keep replacing N by this Janet basis and changing the term ordering by increasing the degrees of all the X_i until the criterion of Lemma 4.1 is satisfied. Then take the intersection of the Janet basis with $K[Y_1, \dots, Y_m]$ to obtain M.

Of course, for serious problems one will not eliminate all X_i in one go with this algorithm, but rather one by one. Successful degree steering needs some experience with the problem. For hard problems it is important not to increase the degree of the variable that one wants to eliminate too fast. If one increases the degrees of the X_i too fast, one is well advised to complement Janet's algorithm by the following global strategy for steering the run of Janet's algorithm.

Remark 4.3. Let t be a certain step during the run of Janet's algorithm. In step t the algorithm has an intermediate Janet basis $J(t)$. Some of the elements of $J(t)$

might stay in the final Janet basis $J = J(t_f)$, while others might get thrown out before the algorithm finishes. Call $\rho(t)$ the number of times up to step t that some element got thrown out of some intermediate Janet basis $J(s)$ with $s \leq t$. Also at step t, one has a list of submodule elements that still have to be tested to reduce to zero or to lead to new elements in an intermediate Janet basis $J(s)$ for some $s > t$. Denote the length of this list in step t by $\theta(t)$.

1. A run of Janet's algorithm will be considered smooth if $\rho(t_f) = 0$.
2. If $\rho(t)$ grows beyond a certain bound and $\theta(t)$ is still big, then it might well be worthwhile to add $J(t)$ to the original input and start a new run of Janet's algorithm rather than finishing the present run.

Similar to the spirit of this remark, we mention that in our experience, it is very helpful to add to the input any approximation of the Janet basis in the Y_j that is already available.

To have a rough measure of the difficulty of a problem, the computation of various field degrees can be helpful. Here is a setup that is more special than the general setup for degree steering but general enough to cover the problems treated in this paper. Given a field K and n variables $x_1, \dots, x_n$ and polynomials

$$y_i = p_i(x_1, \dots, x_n) \in K[x_1, \dots, x_n], \quad i = 1, \dots, m, \tag{4–1}$$

the aim is to find a presentation for the subring $K[y] := K[y_1, \dots, y_m]$ of $K[x] := K[x_1, \dots, x_n]$.

Lemma 4.4. *Let K be infinite and assume that $y_1, \dots, y_n$ in (4–1) are algebraically independent over K. Then there exist infinitely many $(a_1, \dots, a_n) \in K^n$ such that the degree $[K(x_1, \dots, x_n) : K(y_1, \dots, y_n)]$ is equal to the K-vector-space dimension of*

$$K[X_1, \dots, X_n]/\langle a_i - p_i(X_1, \dots, X_n) \mid i = 1, \dots, n\rangle.$$

Proof: Apply Janet's algorithm to $\{Y_i - p_i(X_1, \dots, X_n) \mid i = 1, \dots, n\}$ over $K(Y_1, \dots, Y_n)$. During this run, only finitely many polynomials $q(Y_1, \dots, Y_n) \in K[Y_1, \dots, Y_n]$ occur in the denominators or are chosen for dividing all coefficients of an intermediate Janet-basis element. Obviously there are infinitely many choices for $(a_1, \dots, a_n) \in K^n$ such that $q(a_1, \dots, a_n) \neq 0$ for all these q. For each such $(a_1, \dots, a_n)$, the Janet basis for the ideal $\langle a_i - p_i(X_1, \dots, X_n) \mid i = 1, \dots, n\rangle$ over K can be obtained from the Janet basis for $\langle Y_i - p_i(X_1, \dots, X_n) \mid i = 1, \dots, n\rangle$ over $K(Y_1, \dots, Y_n)$ by substituting the a_j for the Y_j. In particular, the dimension claim follows. □

If the field K is big enough and suitable for quick computations, this lemma allows quick and rather reliable guesses for the degrees $[K(x) : K(y_i \mid i \in S)]$ for the maximal subsets $S \subseteq \{1, \dots, m\}$ such that $\{y_i \mid i \in S\}$ is algebraically independent over K. For small degrees and small $|S|$ one might be able to verify the result by actually computing over the field $K(y_i \mid i \in S)$.

5. THE PROBLEMS AND THEIR SPECIAL STRUCTURE

Returning to the elimination problem for characteristic polynomials, we keep the notation of Section 2. Table 1 gives some examples of $K_{(n,m)}$ for small values of n, m.

Remark 5.1. We note the following:

1. If one assigns degree i to a_i and b_i and $2j$ to c_j, the relations are homogeneous [Glasby 01].
2. A scaling of the a_i by a factor f^i with $f \in K^*$ can be compensated by a scaling of the b_j by the factor f^{-j} without changing the c_k. Therefore, one may assume $b_m = 1$. As a result, the rational function field $K(a_1, \dots, a_n, b_1, \dots, b_{m-1})$ is finite over $K(c_1, \dots, c_{nm})$.
3. More generally, a scaling of the a_i by a factor f^i with $f \in K^*$ and a scaling of the b_j by a factor g^{-j} with $g \in K^*$ results in a scaling of the c_k by the factor $(fg)^k$.
4. If all determinants are equal to 1, i.e., if $a_n := 1$ and $b_m := 1$, then $c_{nm} = 1$ and the resulting system allows the automorphism
$$a_i \mapsto a_{n-i}, \quad b_j \mapsto b_{m-j}, \quad c_k \mapsto c_{nm-k}$$
for $1 \leq i < n$, $1 \leq j < m$, and $1 \leq k < mn$.

Item 3 above suggests that we should proceed as follows: Assume first that $a_1 = b_1 = 1$. Then we have $c_1 = 1$. We do the elimination there and recover the relations from those in $c_2, \dots, c_{nm}$ by making them homogeneous (with respect to the grading defined in item 1). For instance, in the case $n = m = 2$, one obtains $-2a_2b_2 + a_2 + b_2 - c_2$, $a_2b_2 - c_3$, ${a_2}^2{b_2}^2 - c_4$ and hence $c_3^2 - c_4$ as an inhomogeneous relation and $c_3^2 - c_4c_1^2$ as the

$\boldsymbol{K_{(n,m)}}$	**Examples**
$K_{(2,3)}$	$a_1b_1 - c_1, -2a_2b_2 + {b_1}^2a_2 + {a_1}^2b_2 - c_2, 3a_1a_2b_3 - b_1a_2a_1b_2 - {a_1}^3b_3 + c_3, -2{a_2}^2b_3b_1 + a_2b_1{a_1}^2b_3 + {a_2}^2{b_2}^2 - c_4, -{a_2}^2b_3a_1b_2 + c_5, {a_2}^3{b_3}^2 - c_6$
$K_{(2,4)}$	$a_1b_1 - c_1, -2a_2b_2 + {b_1}^2a_2 + {a_1}^2b_2 - c_2, 3a_1a_2b_3 - b_1a_2a_1b_2 - {a_1}^3b_3 + c_3, 2{a_2}^2b_4 - 2{a_2}^2b_3b_1 - 4{a_1}^2a_2b_4 + a_2b_1{a_1}^2b_3 + {a_1}^4b_4 + {a_2}^2{b_2}^2 - c_4, {a_2}^2b_3a_1b_2 - 3{a_2}^2a_1b_4b_1 + a_2b_1{a_1}^3b_4 - c_5, -2{a_2}^3b_2b_4 + {a_2}^3{b_3}^2 + {a_2}^2{a_1}^2b_4b_2 - c_6, {a_2}^3a_1b_3b_4 - c_7, {a_2}^4{b_4}^2 - c_8$
$K_{(3,3)}$	$a_1b_1 - c_1, -2a_2b_2 + {b_1}^2a_2 + {a_1}^2b_2 - c_2, -3a_3b_3 + 3b_2a_3b_1 + 3a_1a_2b_3 - {b_1}^3a_3 - b_1a_2a_1b_2 - {a_1}^3b_3 + c_3, -2{b_2}^2a_3a_1 - 2{a_2}^2b_3b_1 - a_1b_3a_3b_1 + {b_1}^2a_3a_1b_2 + a_2b_1{a_1}^2b_3 + {a_2}^2{b_2}^2 - c_4, 2a_3b_2{a_1}^2b_3 - {a_2}^2b_3a_1b_2 - a_3{b_2}^2a_2b_1 + b_2a_3a_2b_3 + 2a_2b_3{b_1}^2a_3 - a_3{b_1}^2{a_1}^2b_3 + c_5, {a_2}^3{b_3}^2 + 3{a_3}^2{b_3}^2 - 3b_2{a_3}^2b_3b_1 - 3a_1{b_3}^2a_3a_2 + {a_3}^2{b_2}^3 + a_3b_2a_1b_3a_2b_1 - c_6, 2a_1{b_3}^2{a_3}^2b_1 - {a_3}^2{b_2}^2b_3a_1 - {a_2}^2{b_3}^2a_3b_1 + c_7, b_2{a_3}^2{b_3}^2a_2 - c_8, {a_3}^3{b_3}^3 - c_9$

TABLE 1. Some examples of $K_{(n,m)}$ for small values of n, m.

final homogeneous relation. However, the computations in the other cases turn out to be rather hard. It appeared to be much better to treat the case $c_{nm} = 1$ first, which is of independent interest, because we are talking about the determinant being one.

Proposition 5.2.

1. *The affine variety* $V := V(K_{(n,m)})$ *is irreducible of dimension* $n + m$*, and the Zariski closure* $V_c := V(I_{(n,m)})$ *of its projection onto the c-components is therefore also irreducible;* V_c *has dimension* $n+m-1$.
2. *Let* $d := \gcd(n, m)$*. The variety* $V^1 := V(K_{(n,m)} \cup \{c_{nm} - 1\})$ *decomposes into the subvarieties*
$$V^{(1,\omega)} := V\left(K_{(n,m)} \cup \left\{c_{nm} - 1, a_n^{m/d} b_m^{n/d} - \omega\right\}\right),$$
where ω *runs through the dth roots of unity in* K*. All these varieties have dimension* $n + m - 2$*. They are permuted transitively by multiplication of the* a_i *by* f^i *and the* b_j *by* g^j*, where* $f, g \in K^*$ *satisfy* $(fg)^{nm} = 1$*. On projection onto the c-components, the Zariski closures* $V_c^{(1,\omega)}$ *of the images of the* $V^{(1,\omega)}$ *stay disjoint and have the corresponding properties.*
3. *The codimension-one subvariety*
$$V(K_{(n,m)} \cup \{c_{nm} - 1, a_n - 1, b_m - 1\}) \subseteq V^{(1,1)}$$
projects onto a dense subset of $V_c^{(1,1)}$.

Proof: The claims follow from the previous remark and from $c_{nm} - a_n^m b_m^n \in K_{(n,m)}$, which factors on setting $c_{nm} = 1$ in

$$1 - (a_n^{m/d} b_m^{n/d})^d = \prod_{\omega^d=1} (\omega - a_n^{m/d} b_m^{n/d}).$$

□

We introduce the following notation:

$$I_{(n,m)}^{(\alpha,\beta)} := \langle K_{(n,m)} \cup \{c_{nm} - 1, a_n - \alpha, b_m - \beta\}\rangle \\ \cap K[c_1, \ldots, c_{nm}],$$

where $\alpha^{m/d}\beta^{n/d}$ is a dth root of unity in K as in the previous proposition.

As a pleasant feature, one should note that the computation of the vanishing ideal of one of the $V_c^{(1,\omega)}$, for example of $V_c^{(1,1)}$, easily yields the others and that any two of them are relatively prime because of the pairwise disjointness of the $V_c^{(1,\omega)}$. In particular, their intersection is equal to their product. After having taken the intersection, one can again pass to the homogeneous relations without difficulty, whereas one still has to perform an (in general unpleasant) elimination of some variable s against the relation $s^d - c_{nm}$. For instance, the case $n = m = 2$ gives with $c_4 = a_2 = b_2 = 1$ almost immediately the polynomial $c_3 - c_1$ for $V_c^{(1,1)}$. This easily yields $c_3 + c_1$ for $V_c^{(1,-1)}$ and hence $c_3^2 - c_1^2$ for the projection V_c^1 of V^1 onto the c-components, which immediately yields $c_3^2 - c_1^2 c_4$ as its homogenization generating the ideal $I_{(2,2)}$ for V_c. Of course, the same result can be obtained by eliminating the element s of degree 2 from $c_3 - c_1 s$ and $s^2 - c_4$.

6. THE COMPUTATION AND FURTHER RESULTS

In this section we describe how the actual computations for finding generators of the elimination ideal $I_{(n,m)}$, where $(n, m) \in \{(2, 3), (2, 4), (3, 3)\}$, are carried out, or in the last case, could be carried out. In each case, first generators for $I_{(n,m)}^{(1,1)}$ will be computed, where the Krull dimension is one less and the result interesting in itself. By homogenizing a Janet basis for $I_{(2,3)}^{(1,1)}$, one immediately gets generators for $I_{(2,3)}$, because 2, 3 are relatively prime. In the other two cases one has more work to do, as explained in Section 5.

6.1 The System $K_{(2,3)}$

The following derivation of generators of $I_{(2,3)}$ seems to be different from that given in [Schwingel 99] and has the advantage of being reproducible.

We compute a Janet basis of $I_{(2,3)}^{(1,1)}$ as follows:

(a) Set $a_2 = b_3 = c_6 = 1$ in $K_{(2,3)}$ to obtain $K_{(2,3)}^{\mathrm{det}=1}$.

(b) Compute a Janet basis from $K_{(2,3)}^{\mathrm{det}=1}$ using the degree-reverse lexicographic ordering defined by $c_5 > c_4 > \cdots > c_1 > b_2 > b_1 > a_1$ with degrees $2i$ for c_i and i for b_i and for a_i.

(c) Eliminate a_1 by degree steering (cf. Algorithm 4.2), that is, by increasing the degree of a_1 up to 9.

(d) Eliminate b_1 by degree steering, that is, by increasing the degree of b_1 up to 21.

(e) Eliminate b_2 by degree steering, that is, by increasing the degree of b_2 up to 19.

(f) Redefine the degrees of c_i to be i and end up with a Janet basis for $I_{(2,3)}^{(1,1)}$ consisting of 21 elements of degrees 19 to 31.

We compute information about $I_{(2,3)}$ as follows:

(a) Use the degree-reverse lexicographic ordering defined by $c_6 > c_5 > c_4 > \cdots > c_1$ with degrees i for c_i and obtain a generating set of $I_{(2,3)}$ by homogenizing the elements of the Janet basis for $I_{(2,3)}^{(1,1)}$.

(b) Compute a Janet basis from the generating set of (a). It consists of 42 elements of degrees 19 to 41. Immediately obtain the Hilbert series for the residue class ring $R_{(2,3)}$ listed in Proposition 2.1.

(c) Compute a minimal set of homogeneous generators for $I_{(2,3)}$ from the set of generators in (a) and the Janet basis in (b) by applying the methods of Section 3.

Remark 6.1. We note the following:

1. Homogenizing a polynomial in $c_1, \ldots, c_5$ works as follows: One substitutes c_i/t^i for c_i, takes the numerator of the resulting expression, and substitutes c_6 for t^6. Because of the special situation that $m = 2$ and $n = 3$ are relatively prime, by Section 5, the result will not contain any t's, and because of the special properties of Janet bases (cf. Section 3), this process applied to a Janet basis will give a generating set for the homogeneous situation.

2. The computations can also be carried out over $\mathbb{Z}$ instead of over $\mathbb{Q}$. In this case one gets slightly different generators. On the web page we list a minimal set of homogeneous generators over $\mathbb{Z}$, which turns out also to be minimal over the rationals. (A set of generators for $I_{(2,3)}^{(1,1)}$ is obtained from this list by simply substituting 1 for c_6.)

3. Prior to the above computations one can get very reliable guesses of various degrees of field extensions involved by applying Lemma 4.4, starting from $K_{(2,3)}$ with $b_3 = 1$ as additional relation. These degrees can be checked afterward. For instance, the degree of $K(a_1, a_2, b_1, b_2, b_3 = 1)$ over $K(c_1, \ldots, c_6)$ is 1. It turns out that any four of the c_i are algebraically independent over K. Here are the degrees for $[K(c_1, \ldots, c_6) : K(c_i \mid i \in S)]$ followed by the four-element subsets S of $\{1, \ldots, 6\}$ corresponding to the minimal subsets of the c_i where this degree is finite:

3:	$\{1,2,5,6\},\ \{1,4,5,6\},$
4:	$\{1,3,5,6\},$
5:	$\{1,2,3,4\},\ \{1,2,3,5\},\ \{1,3,4,5\},$
6:	$\{1,2,4,5\},$
7:	$\{1,2,3,6\},\ \{1,3,4,6\},\ \{2,3,5,6\}, \{3,4,5,6\},$
9:	$\{1,2,4,6\},\ \{2,4,5,6\},$
12:	$\{2,3,4,5\},$
18:	$\{2,3,4,6\}$

This list not only says something about the general degree of difficulty in computing a Janet basis for $I_{(2,3)}$ but also gives some specific information about certain elements. For example, any polynomial in c_1, c_2, c_3, c_4, c_5 contained in $I_{(2,3)}$ is a multiple of a minimal relation of degrees 12, 5, 6, 5, 5 in c_1, c_2, c_3, c_4, c_5. Actually, one should more carefully say "of degrees dividing these numbers," but they always turn out to be equal.

6.2 The System $K_{(2,4)}$

We compute a Janet basis of $I_{(2,4)}^{(1,1)}$ as follows:

(a) Set $a_2 = b_4 = c_8 = 1$ in $K_{(2,4)}$ to obtain $K_{(2,4)}^{\mathrm{det}=1}$.

(b) Compute a Janet basis from $K_{(2,4)}^{\mathrm{det}=1}$ using the degree-reverse lexicographic ordering defined by $c_7 > c_6 >$

$\cdots > c_1 > b_2 > b_1 > a_1$ with degrees $2i$ for c_i and i for b_i and for a_i.

(c) Eliminate a_1 by degree steering (cf. Algorithm 4.2), that is, by increasing the degree of a_1 up to 15.

(d) Eliminate b_1 by degree steering, that is, by increasing the degree of b_1 up to 24.

(e) Eliminate b_2 by degree steering, that is, by increasing the degree of b_2 up to 40.

(f) Eliminate b_3 by degree steering, that is, by increasing the degree of b_3 up to 18.

(g) Redefine the degrees of c_i to be i and end up with a Janet basis for $I_{(2,4)}^{(1,1)}$ consisting of 131 elements of degrees 16 to 41, listed on the associated web page.

We compute information about $I_{(2,4)}$ as follows:

(a) Use the degree-reverse lexicographic ordering defined by $z_4 > c_8 > c_7 > \cdots > c_1$ with degrees i for c_i and 4 for z_4, homogenize the elements of the Janet basis for $I_{(2,4)}^{(1,1)}$ (see below), and add the relation $z_4^2 - c_8$.

(b) Compute a Janet basis from the generating set of (a). Use degree steering to eliminate z_4 by increasing the degree of z_4.

(c) End up with a Janet basis for $I_{(2,4)}$. It consists of 233 elements of degrees 28 to 55. Immediately obtain the Hilbert series for the residue class ring $R_{(2,4)}$ listed in Proposition 2.4.

(d) Compute a minimal set of homogeneous generators for $I_{(2,4)}$ from the Janet basis in (c) by applying the methods of Section 3; see the associated web page.

Remark 6.2. We note the following:

1. Homogenizing a polynomial in $c_1, \dots, c_7$ works as follows: One substitutes c_i/t^i for c_i, takes the numerator of the resulting expression, and substitutes c_8 for t^8. This time, since $m = 2$ and $n = 4$ have greatest common divisor 2, the results of Section 5 imply that the resulting polynomials will also depend on t, more precisely on t^4, which is replaced by the new variable z_4, and because of the special properties of Janet bases (cf. Section 3), this process applied to a Janet basis will give a generating set for the homogeneous situation.

2. The intermediate variable z_4 can be avoided by homogenizing a Janet basis for the intersection $I_{(2,4)}^{(1,1)} \cap I_{(2,4)}^{(1,-1)}$. As pointed out in Section 5, a Janet basis of $I_{(2,4)}^{(1,-1)}$ can be obtained from an easy substitution into the Janet basis of $I_{(2,4)}^{(1,1)}$. However, taking the intersection of the two ideals turns out to be much more time-consuming than proceeding as described above via elimination of z_4. From the minimal generating set of $I_{(2,4)}$, one can, of course, also obtain generators for $I_{(2,4)}^{(1,1)} \cap I_{(2,4)}^{(1,-1)}$ by specializing c_8 to 1.

3. Again, prior to the computation one can compute reliable guesses for various degrees of field extensions and check them afterward. One obtains, for instance,

$$[K(a_1, a_2, b_1, b_2, b_3, b_4 = 1) : K(c_1, \dots, c_8)] = 2,$$

and that any five of the $c_1, \dots, c_8$ are algebraically independent over K. The occurrences of the various degrees of the $[K(c_1, \dots, c_8) : K(c_i \mid i \in S)]$ are listed in Proposition 2.5 for the 56 subsets S of $\{1, \dots, 8\}$ with five elements. The explicit assignment of the subsets to the degrees are as follows:

Degrees[1] where S contains 8:

2:	$\{1,2,6,7,8\}, \{1,3,5,7,8\}$
6:	$\{1,2,3,7,8\}, \{1,2,5,7,8\}, \{1,3,4,7,8\},$
	$\{1,3,6,7,8\}, \{1,4,5,7,8\}, \{1,5,6,7,8\}$
12:	$\{1,2,3,5,8\}, \{1,2,4,7,8\}, \{1,2,5,6,8\},$
	$\{1,4,6,7,8\}, \{2,3,6,7,8\}, \{3,5,6,7,8\}$
14:	$\{1,2,3,4,8\}, \{1,2,3,6,8\}, \{1,2,4,5,8\},$
	$\{1,3,4,5,8\}, \{2,3,5,6,8\}, \{2,5,6,7,8\},$
	$\{3,4,5,7,8\}, \{3,4,6,7,8\}, \{4,5,6,7,8\}$
16:	$\{1,3,5,6,8\}, \{2,3,5,7,8\}$
20:	$\{1,4,5,6,8\}, \{2,3,4,7,8\}$
22:	$\{1,3,4,6,8\}, \{2,4,5,7,8\}$
24:	$\{1,2,4,6,8\}, \{2,4,6,7,8\}$
42:	$\{2,3,4,5,8\}, \{3,4,5,6,8\}$
48:	$\{2,3,4,6,8\}, \{2,4,5,6,8\}$

[1] The subfield of $K(c_1, \dots, c_8)$ generated by $c_1, \dots, c_7$ is not isomorphic to the field $K(c_1, \dots, c_7)$ for the case $K_{(2,4)}^{\det=1}$, but is isomorphic to an extension of degree 2 of it. Therefore the degree $[K(c_1, \dots, c_7) : K(c_i \mid i \in S)]$ for the case $K_{(2,4)}^{\det=1}$, where S is a 4-element subset of $\{1, \dots, 7\}$ corresponding to a minimal subset of $\{c_1, \dots, c_7\}$ for which the above degree is finite, equals $[K(c_1, \dots, c_8) : K(c_i \mid i \in S')]$ divided by 2, where $S' = S \cup \{8\}$.

Degrees where S does not contain 8:

6:	$\{1,2,3,5,6\}$
7:	$\{1,2,3,4,5\}$
9:	$\{1,2,3,4,6\},\{1,2,3,5,7\},\{1,2,5,6,7\}$
10:	$\{1,2,3,4,7\},\{1,2,3,6,7\}$
11:	$\{1,3,4,5,7\}$
12:	$\{1,2,4,5,6\},\{1,2,4,5,7\},\{1,3,4,5,6\},$ $\{1,3,5,6,7\}$
16:	$\{1,3,4,6,7\},\{1,4,5,6,7\},\{2,3,5,6,7\}$
18:	$\{1,2,4,6,7\}$
25:	$\{2,3,4,5,6\}$
29:	$\{3,4,5,6,7\}$
32:	$\{2,3,4,5,7\}$
35:	$\{2,3,4,6,7\},\{2,4,5,6,7\}$

6.3 The System $K_{(3,3)}$

We compute a Janet basis of $I^{(1,1)}_{(3,3)}$ as follows:

(a) Set $a_3 = b_3 = c_9 = 1$ in $K_{(3,3)}$ to obtain $K^{\text{det}=1}_{(3,3)}$.

(b) Compute a Janet basis from $K^{\text{det}=1}_{(3,3)}$ using the degree-reverse lexicographic ordering defined by $c_8 > c_7 > \cdots > c_1 > b_2 > b_1 > a_2 > a_1$ with degrees $2i$ for c_i and i for b_i and for a_i.

(c) Eliminate a_1 by degree steering (cf. Algorithm 4.2), that is, by increasing the degree of a_1 up to 15.

(d) Eliminate b_1 by degree steering, that is, by increasing the degree of b_1 up to 21.

(e) Eliminate a_2 by degree steering, that is, by increasing the degree of b_2 up to 21. Here things are speeded up by assigning new degrees, namely 2, 3, 4, 5, 4, 3, 2, 1 for c_8, c_7, …, c_1 and 2, 2 for a_2, b_2. The degree of a_2 needs to be increased only up to 4.

(f) Eliminate b_2 by degree steering. Things are speeded up tremendously by keeping the degrees for the c_i from (e). Then the degree of b_2 has to be raised only up to 3.

(g) Raise the degrees of c_i to i for $i = 6$, 7, 8 in this order and compute the Janet basis for $I^{(1,1)}_{(3,3)}$ in each step (in the spirit of degree steering), until one has a Janet basis for $I^{(1,1)}_{(3,3)}$ with respect to the ordering $c_8 > c_7 > \cdots > c_1$ with degrees i for c_i. This Janet basis consists of 171 elements of degrees 15 to 41; see the associated web page.

Remark 6.3. We note the following:

1. Step (e) gets a bit hard and step (f) very hard if one does not lower the degrees of c_8, c_7, c_6. The price one has to pay is in step (g), which provides the necessary starting Janet basis for the homogenization. Somehow, the problem does not like its natural degrees: When all the c_i apart from c_8 have degree i and c_8 still has degree 2, the Janet basis has only 36 elements instead of the final 171 elements.

2. Here are some additional data for $K^{\text{det}=1}_{(3,3)}$. From Lemma 4.4 or by checking explicitly one gets (after setting $b_3 = a_3 = c_9 = 1$)

$$[K(a_1, a_2, b_1, b_2) : K(c_1, \ldots, c_8)] = 6$$

and the following list of degrees for $[K(c_1, \ldots, c_8) : K(c_i \mid i \in S)]$ followed by the four-element subsets S of $\{1, \ldots, 8\}$ corresponding to the minimal subsets of $\{c_1, \ldots, c_8\}$ for which these degrees are finite:

2:	$\{1,2,3,8\},\{1,2,4,8\},\{1,2,5,8\},$ $\{1,2,7,8\},\{1,4,7,8\},\{1,5,7,8\},$ $\{1,6,7,8\}$
3:	$\{1,3,5,8\},\{1,4,5,8\},\{1,4,6,8\}$
4:	$\{1,2,3,7\},\{1,2,5,7\},\{1,2,6,8\},$ $\{1,3,4,8\},\{1,3,7,8\},\{1,5,6,8\},$ $\{2,4,7,8\},\{2,6,7,8\}$
5:	$\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,7\},$ $\{1,2,6,7\},\{2,3,7,8\},\{2,5,7,8\},$ $\{4,6,7,8\},\{5,6,7,8\}$
6:	$\{1,2,4,5\},\{1,3,6,8\},\{1,4,6,7\},$ $\{1,5,6,7\},\{2,3,4,8\},\{2,3,5,8\},$ $\{4,5,7,8\}$
7:	$\{1,2,3,6\},\{1,2,5,6\},\{1,4,5,7\},$ $\{2,4,5,8\},\{3,4,7,8\},\{3,6,7,8\}$
8:	$\{1,3,4,5\},\{1,3,4,7\},\{1,3,5,7\},$ $\{1,3,6,7\},\{1,4,5,6\},\{2,3,6,8\},$ $\{2,4,6,8\},\{2,5,6,8\},\{3,4,5,8\},$ $\{4,5,6,8\}$
9:	$\{1,2,4,6\},\{3,5,7,8\}$
11:	$\{1,3,5,6\},\{3,4,6,8\}$
12:	$\{1,3,4,6\},\{3,5,6,8\}$
13:	$\{2,3,4,7\},\{2,4,5,7\},\{2,5,6,7\}$
15:	$\{2,3,5,7\},\{2,3,6,7\},\{2,4,6,7\}$
18:	$\{2,3,4,5\},\{2,3,5,6\},\{3,4,6,7\},$ $\{4,5,6,7\}$
21:	$\{2,3,4,6\},\{2,4,5,6\},\{3,4,5,6\},$ $\{3,4,5,7\},\{3,5,6,7\}$

We compute information about $I_{(3,3)}$ as follows:

(a) Use the degree-reverse lexicographic ordering defined by $z_3 > c_9 > c_8 > c_7 > \cdots > c_1$ with degrees i for c_i and 3 for z_3, homogenize the elements of the Janet basis for $I^{(1,1)}_{(3,3)}$ (see below), and add the relation $z_3^3 - c_9$. Denote by $I_{(3,3,z)}$ the ideal generated by this set in $K[c_1, \ldots, c_9, z_3]$. After this, one could in principle proceed as in the case $I_{(2,4)}$:

(b) Compute a Janet basis from the generating set of (a). Use degree steering to eliminate z_3 by increasing the degree of z_3.

(c) End up with a Janet basis for $I_{(3,3)}$. Immediately obtain the Hilbert series for the residue class ring $R_{(3,3)}$.

(d) Compute a minimal set of homogeneous generators for $I_{(3,3)}$ from the Janet basis in (c) by applying the methods of Section 3.

However, steps (b) to (d) were rather hard to perform with the computing facilities available to us. Instead we modestly computed some starting information, such as the list of field degrees given at the end of Section 2 based on Lemma 4.4. Further, we computed the smallest two degrees for which the components of $I_{(3,3)}$ were not trivial, by starting from the Janet basis for $I_{(3,3,z)}$ from (a). The Hilbert series for the ideal is too big to be recorded here, but the concept of multiplicative and nonmultiplicative variables for Janet bases allows us not only to enumerate vector-space bases for each homogeneous component $(I_{(3,3,z)})_k$ of degree k but also, since $z_3^3 - c_9$ is in the Janet basis with all c_i multiplicative, to enumerate vector-space bases for the subspaces $(I_{(3,3,z)})_{k,2}$ of elements of degree ≤ 2 in z_3. The generating function counting these basis vectors can be computed explicitly as a rational function. The first few terms of the expansion are

$$\begin{aligned}&2t^{15} + 3t^{16} + 7t^{17} + 21t^{18} + 37t^{19} + 64t^{20} + 117t^{21}\\ &\quad + 172t^{22} + 264t^{23} + 388t^{24} + 538t^{25} + 735t^{26}\\ &\quad + 1009t^{27} + 1311t^{28} + 1715t^{29} + 2216t^{30} + 2798t^{31}\\ &\quad + 3511t^{32} + 4400t^{33} + \cdots .\end{aligned}$$

What we want to know are vector-space bases of the subspace $(I_{(3,3,z)})_{k,0} = (I_{(3,3)})_k$ of $(I_{(3,3,z)})_{k,2}$ of elements of degree 0 in z_3, and we have computed them for $k = 29$, 30, 31 and obtained dimensions 0, 19, 79, which implies that the minimal basis number is

$$\epsilon(I_{(3,3)}) = 19t^{30} + 60t^{31} + \text{higher-order terms.}$$

If one computes these bases for the next few degrees, one can hope to give this as supporting information into a run of elimination by degree steering into the Janet basis for $I_{(3,3,z)}$ to eliminate z_3, where of course one would start with a rather high degree for z_3. But from the numbers that have been computed, it should be clear that it is not so easy to finish the calculation in a reasonable amount of time.

7. CONCLUDING REMARKS

The elimination problem turned out to be rather difficult already for the case $9 = 3 \cdot 3$. In view of the original recognition problem for matrix groups over finite fields, it will certainly be easier to decide things by direct computation: Given a polynomial $p_{nm,c}(x)$ of degree nm over a finite field F, decide whether it is the characteristic polynomial of a Kronecker product of two matrices of degrees n, m over F. The equations for this involving the coefficients of the characteristic polynomials of the two smaller matrices are readily written down, as we saw, and—with the concrete c_i given—much more easily solved or else the nonexistence of solutions checked than can be performed by the general elimination. However, there will also be a limit to this sort of computation. At that stage, one could proceed as follows: Find a splitting field F_1 for $p_{nm,c}(x)$ and see whether the nm roots $w_1, \ldots, w_{nm}$ of $p_{nm,c}(x)$ in F_1 can be distributed into an $n \times m$ matrix of rank 1 over F_1. This is a problem for which it is easy to give an algorithm based on the fact that for any w_i there must exist at least $(n-1)(m-1)$ indices j such that there are two different indices $k, l \in \{1, \ldots, nm\} - \{i, j\}$ with $w_i w_j = w_k w_l$. In this case, too, it is easier to try to compute the decomposition than to come up with any sort of invariant deciding the existence. But in any case, this remark throws an interesting light on the problem of this paper, since there one does not start with the w_i but looks for conditions expressed in terms of the elementary symmetric functions in the w_i.

ACKNOWLEDGMENTS

We are grateful to C. Leedham-Green for pointing out the problem to us, to E. O'Brien for providing us with background material, to V. Levandovskyy for trying to treat our examples using the conventional elimination methods in Singular, and to Mohamed Barakat for his support.

REFERENCES

[Blinkov et al. 01] Y. A. Blinkov, V. P. Gerdt, and D. A. Yanovich. "Construction of Janet bases, II. Polynomial Bases." In *Computer Algebra in Scientific Computing CASC 2001*, edited by V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, pp. 249–263. New York: Springer, 2001.

[Blinkov et al. 03] Y. A. Blinkov, C. F. Cid, V. P. Gerdt, W. Plesken, and D. Robertz. "The MAPLE Package 'Janet': I. Polynomial Systems." In *Proc. of Computer Algebra in Scientific Computing CASC 2003*, edited by V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, pp. 31–40. Garching, Germany: Institut für Informatik, TU München, 2003. Also available together with the package online (http://wwwb.math.rwth-aachen.de/Janet).

[Blinkov et al. 07] Y. A. Blinkov, S. Jambor, and D. Robertz. "The `ginv` Project." Available online (http://invo.jinr.ru and http://wwwb.math.rwth-aachen.de/Janet), 2007.

[Bosma et al. 97] W. Bosma, J. J. Cannon, and C. Playoust. "The Magma Algebra System I: The User Language." *J. Symbolic Computation* 24 (1997), 235–265. (http://magma.maths.usyd.edu.au/magma/MagmaInfo.html).

[Cox et al. 98] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. New York: Springer, 1998.

[Gerdt 05] V. P. Gerdt. "Involutive Algorithms for Computing Gröbner Bases." In *Computational Commutative and Non-Commutative Algebraic Geometry*, edited by S. Cojocaru, G. Pfister, and V. Ufnarovski, pp. 199–225, NATO Science Series. Amsterdam: IOS Press, 2005.

[Gerdt and Blinkov 05] V. P. Gerdt and Y. A. Blinkov. "Janet-like Gröbner Bases." In *Computer Algebra in Scientific Computing*, pp. 184–195, Lecture Notes in Comput. Sci. 3718. Berlin: Springer, 2005.

[Glasby 01] S. P. Glasby. "On the Tensor Product of Polynomials over a Ring." *J. Aust. Math. Soc.* 71 (2001), 307–324.

[Greuel et al. 05] G.-M. Greuel, G. Pfister, and H. Schönemann. "SINGULAR 3.0. A Computer Algebra System for Polynomial Computations." Available online from the Center for Computer Algebra, University of Kaiserslautern (http://www.singular.uni-kl.de), 2005.

[Leedham-Green and O'Brien 97] C. R. Leedham-Green and E. O'Brien. "Recognising Tensor Products for Matrix Groups." *Int. J. of Algebra and Computation* 7 (1997), 541–559.

[Plesken and Robertz 05] W. Plesken and D. Robertz. "Janet's Approach to Presentations and Resolutions for Polynomials and Linear PDEs." *Arch. Math.* 84:1 (2005), 22–37.

[Schwingel 99] R. Schwingel. "The Tensor Product of Polynomials." *Exp. Math.* 8 (1999), 395–397.

[van der Waerden 31] B. L. van der Waerden. *Moderne Algebra, II.* Berlin: Springer, 1931.

W. Plesken, Lehrstuhl B für Mathematik, RWTH Aachen University, Templergraben 64, 52062 Aachen, Germany (plesken@momo.math.rwth-aachen.de)

D. Robertz Lehrstuhl B für Mathematik, RWTH Aachen University, Templergraben 64, 52062 Aachen, Germany (daniel@momo.math.rwth-aachen.de)

Received May 11, 2007; accepted in revised form May 20, 2008.