J. Symbolic Computation (1999) **27**, 351–365
Article No. jsco.1998.0256
Available online at http://www.idealibrary.com on IDEAL

Computing Toric Ideals [†]

ANNA MARIA BIGATTI[‡¶], ROBERTOLA SCALA[§‖],
LORENZO ROBBIANO[‡]

[‡]*Dipartimento di Matematica, Università di Genova, dia Dodecaneso 35, I-16146 Genova, Italy*
[§]*Dipartimento di Matematica, Università di Bari, via E. Orabona 4, I-70125 Bari, Italy*

Toric ideals are binomial ideals which represent the algebraic relations of sets of power products. They appear in many problems arising from different branches of mathematics. In this paper, we develop new theories which allow us to devise a parallel algorithm and an efficient elimination algorithm. In many respects they improve existing algorithms for the computation of toric ideals.

1. Introduction

There is a problem in mathematical literature which has recently received considerable attention. It is the problem of computing the algebraic relations of a set of power products. The reason for this attention is that the problem is related to many fundamental questions arising from several branches of mathematics, such as integer programming, statistics, combinatorics, and it is also the basic step of any procedure which "computes" SAGBI bases (see Robbiano and Sweedler, 1988). For a nice introduction to the subject see Sturmfels (1996) and Eisenbud and Sturmfels (1996). There are many algorithms which solve the problem, but here the issue is efficiency, because in the applications one has to compute relations of huge numbers of power products in a huge number of indeterminates.

We start by explaining what is known with the help of a very easy problem, which we take as our guide. Let us consider the following example: we want to compute a set of generators of the toric ideal $\mathcal{I}$, which describes the algebraic relations of power products $\{st,\ s^3t^2,\ st^3,\ s^5t^2\}$. This means that we wish to compute the kernel of the k-algebra homomorphism $\pi : k[X,Y,Z,W] \to k[s,t]$ given by $X \mapsto st,\ Y \mapsto s^3t^2,\ Z \mapsto st^3,\ W \mapsto s^5t^2$. If we consider the ideal J of $k[s,t,X,Y,Z,W]$ generated by $\{X - st,\ Y - s^3t^2,\ Z - st^3,\ W - s^5t^2\}$, the solution to our problem is $J \cap k[X,Y,Z,W]$, which can be obtained by performing (in CoCoA) `Elim(s..t,J)`. This means that we compute a Gröbner basis $\mathcal{G}$ of J with a suitable elimination order and then take $\mathcal{G} \cap k[X,Y,Z,W]$. This remark already shows that $\mathcal{I}$ is generated by *binomials* (i.e. differences of power products) and indeed, if we denote by T_1, T_2 power products in X,Y,Z,W, then $\mathcal{I}$ is generated by $\{T_1 - T_2 \mid \pi(T_1) = \pi(T_2)\}$ (see Sturmfels, 1996, Lemma 4.1, p. 31 for a direct proof).

[†]Partially supported by the Consiglio Nazionale delle Ricerche (CNR).
[¶]E-mail: bigatti,robbiano@dima.unige.it
[‖]E-mail: lascala@dm.uniba.it

0747–7171/99/040351 + 15 $30.00/0

In our case, the Gröbner basis from which we compute `Elim(s..t, J)` is

$$\begin{aligned}\mathcal{G} := \{&-st+X, -t^2X+Z, -tX^2+sZ, s^2Z-X^3, -sX^2+Y, tY-X^3,\\ &-sYZ+X^5, X^7-Y^2Z, -s^2Y+W, -X^3Y+ZW, -sXY+tW, tZW\\ &-X^6, tXW-Y^2, -X^4W+Y^3, -sZW+XY^2, sY^2\\ &-X^2W, t^2W-X^2Y, Y^4-XZW^2\},\end{aligned}$$

hence, the solution is the ideal $\mathcal{I}$ generated by $\{X^7-Y^2Z,\ -X^3Y+ZW,\ -X^4W+Y^3,\ Y^4-XZW^2\}$.

We observe that $\mathcal{I}$ is *homogeneous*. Namely, if we give weight 1 to s and t, we obtain $\deg(X)=2$, $\deg(Y)=5$, $\deg(Z)=4$, $\deg(W)=7$. More precisely, the fact that we have power products in two indeterminates s, t implies that $\mathcal{I}$ is *bihomogeneous*, but in the paper we are not going to use this fact. This implies (Nakayama's Lemma) that the minimal sets of generators of $\mathcal{I}$ have the same number of elements; in our case we obtain $\{X^7-Y^2Z,\ X^3Y-ZW,\ X^4W-Y^3\}$ as a minimal set of generators of the ideal $\mathcal{I}$.

This could be the end of the story, but this way is, in general, (certainly not in our simple example) *too expensive* from the computational point of view.

So one follows a different path. Namely, suppose that a binomial T_1-T_2 is in the kernel. Let us write $T_1 := X^{a_1}Y^{b_1}Z^{c_1}W^{d_1}$ and $T_2 := X^{a_2}Y^{b_2}Z^{c_2}W^{d_2}$. Then we obtain

$$s^{a_1+3b_1+c_1+5d_1}\cdot t^{a_1+2b_1+3c_1+2d_1} = s^{a_2+3b_2+c_2+5d_2}\cdot t^{a_2+2b_2+3c_2+2d_2}.$$

If we put $a := a_1-a_2,\ b := b_1-b_2,\ c := c_1-c_2,\ d := d_1-d_2$, we obtain $a+3b+c+5d = a+2b+3c+2d = 0$, which can be written as

$$(a\quad b\quad c\quad d)\,\mathbf{A} = (0\quad 0), \qquad \text{where} \quad \mathbf{A} := \begin{pmatrix}1 & 1\\ 3 & 2\\ 1 & 3\\ 5 & 2\end{pmatrix}.$$

We denote by $\mathrm{Ker}(\mathbf{A})$ the free $\mathbb{Z}$-module of the solutions of the homogeneous diophantine system associated to $\mathbf{A}$. To every element in $\mathrm{Ker}(\mathbf{A})$ we may associate an element in $\mathcal{I}$. For instance $(-3,-1,1,1)$ is a solution and we associate $ZW-X^3Y\in\mathcal{I}$, and we could as well say that $(3,1,-1,-1)$ is a solution and associate $X^3Y-ZW\in\mathcal{I}$.

The next fundamental step is to use the fact that the following conditions are equivalent (see Lemma 12.2 p.114 in Sturmfels, 1996):

(1) $L\subseteq \mathrm{Ker}(\mathbf{A})$ spans the lattice $\mathrm{Ker}(\mathbf{A})$,
(2) $I_L\ k[X,Y,Z,W]_{XYZW} = \mathcal{I}\ k[X,Y,Z,W]_{XYZW}$,
(3) $I_L : (XYZW)^\infty = \mathcal{I}$, ←

why?

where I_L denotes the ideal generated by the binomials associated with the vectors in L and $I_L : (XYZW)^\infty$ denotes the saturation of I_L with respect to $XYZW$.

So let us see what happens in our example. We wish to compute I_L, hence, we need to compute L, a $\mathbb{Z}$-basis of $\mathrm{Ker}(\mathbf{A})$. We know that $\#(L)=n-\rho$, where n and ρ are the number of rows and the rank of $\mathbf{A}$; in our example $\#(L)=2$. There are well-known algorithms which compute that basis in polynomial time, for instance by computing the Hermitian normal form of $\mathbf{A}$. In our example, we perform elementary operations on the rows of $\mathbf{A}$ and keep track of the corresponding operations on the identity matrix. We obtain

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -5 & 0 & 0 & 1 \end{pmatrix} \mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 0 & 2 \\ 0 & -3 \end{pmatrix} \qquad \text{hence} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -7 & 2 & 1 & 0 \\ 4 & -3 & 0 & 1 \end{pmatrix} \mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Therefore, if we let

$$E := \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -7 & 2 & 1 & 0 \\ 4 & -3 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad (a \quad b \quad c \quad d) = (a' \quad b' \quad c' \quad d')\,E,$$

we obtain

$$(a' \quad b' \quad c' \quad d') \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} = (0 \quad 0).$$

A basis of solutions with respect to a', b', c', d' is given by $\{(0,\ 0,\ 1\ ,0),\ (0,\ 0,\ 0\ ,1)\}$, which corresponds to the two solutions with respect to a, b, c, d given by the last two rows of E. In conclusion, we obtain $L = \{(-7,\ 2,\ 1\ ,0),\ (4,\ -3,\ 0\ ,1)\}$, hence $I_L = (X^7 - Y^2 Z,\ X^4 W - Y^3)$.

The final and, from the computational point of view, most demanding step is to compute the ideal $I_L : (XYZW)^\infty$. One way to proceed is to adjoin an indeterminate, say t, to our ring so that we obtain $k[t, X, Y, Z, W]$, then consider the ideal $H := I_L + (tXYZW - 1)$ and finally intersect H with $k[X, Y, Z, W]$. In other words, we have to compute `Elim(t,H)`, where $H := (-X^7 + YZ,\ X^4 W - Y^3,\ tXYZW - 1)$. The Gröbner basis from which we compute `Elim(t,H)` is $\{tXYZW - 1,\ tZ^2W^2 - X^2,\ -tY^3Z^2W + X^6,\ X^4W - Y^3,\ -X^7 + Y^2Z,\ -X^3Y + ZW,\ -Y^4 + XZW^2\}$. Hence, the solution is the ideal $\mathcal{I}$ generated by $\{X^4W - Y^3,\ -X^7 + Y^2Z,\ -X^3Y + ZW,\ -Y^4 + XZW^2\}$. As before, we minimalize and obtain again $\mathcal{I} = (X^4W - Y^3,\ X^7 - Y^2Z,\ X^3Y - ZW)$.

It is quite clear that this method of computing $\mathcal{I}$ is superior to the first one, since the computation of the Gröbner basis related to `Elim(t,H)` is simpler than the computation of the Gröbner basis related to `Elim(s..t,J)`, while the computation of L is based on polynomial time algorithms and so it can be considered as a sort of "easy preprocessing".

However, this method is not completely satisfactory yet. It is well known that computing with homogeneous ideals has many advantages and it is clear that computing with the least number of indeterminates lowers the complexity. Now with the last method we have to adjoin a new indeterminate (t in our example) and we destroy the homogeneity in the sense that we introduce the inhomogeneous polynomial $tXYZW - 1$ among homogeneous ones.

A first easy way of fixing the second problem is to change the method of computing the saturation. Because $XYZW$ is homogeneous of degree 18, we introduce a new indeterminate u with degree 18 and the *homogeneous* polynomial $XYZW - u$. Then, $I_L{:}(XYZW)^\infty$ can be computed from a DegRevLex-Gröbner basis of $H := I_L + (XYZW - u)$. This approach is much faster than the inhomogeneous one (see Algorithm EATI in Section 3).

The remaining question is how to fix the first problem and recently several new ideas were developed to attack it. The most relevant ones are described in Sturmfels (1996, Chapter 12), for instance, a substantial improvement can be obtained from the following simple equality

$$I_L : (XYZW)^\infty = ((((I_L : X^\infty) : Y^\infty) : Z^\infty) : W^\infty).$$

A priori this way seems to be hopeless, as we trade one for four Gröbner basis computations, but, as we said, I_L is homogeneous and so, to compute $I_L : X^\infty$ it suffices to compute a Gröbner basis G of I_L with respect to a DegRevLex-order with X smallest indeterminate and then divide each polynomial in G by the maximum power of X which divides it. Thus, we obtain a new ideal which is again homogeneous and we continue with the next Gröbner basis, which we perform in the same way (now Y is the smallest indeterminate), and so on. We call this a *sequential approach*, in the sense that one performs the saturations with respect to the indeterminates in sequence.

Before continuing, one word should be spent on the fact that these approaches also have many other benefits. The most important one is that we do not need to saturate with respect to *all* the indeterminates, as it is very easy to see that at most half of them suffice (see Hosten and Thomas, 1998) and often many fewer are enough. To explain this fact, let us have a look at our example. We have to saturate the ideal $I_L = (X^7 - YZ,\ X^4W - Y^3)$. We may argue as follows. If we invert X, then the first polynomial tells us that also Y and Z become invertible modulo I_L. But then the second polynomial tells us that W also becomes invertible modulo I_L. This implies (see Corollary 2.6) that we obtain the solution simply by performing $I_L : X^\infty$.

Another important feature is that if H is an ideal such that $I_L \subseteq H \subseteq \mathcal{I}$, then instead of saturating I_L, we may saturate H. This enables us to

(a) adjoin *more* generators to I_L. This fact is mainly used in PATI (see below).
(b) compute with *pure vectors.*

Sentence (b) simply means that if T_1, T_2, T are power products and during a computation we produce $TT_1 - TT_2$, we may replace it by $T_1 - T_2$. This fact was already pointed out and used in Pottier (1994) and Thomas (1997) to *remove* the polynomial structure. Indeed, binomials can be substituted by vectors of integers, where, for instance, $X^4W - Y^3$ becomes $(4, -3, 0, 1)$. Note that in this way, $X^9YW - X^5Y^4$ also becomes $(4, -3, 0, 1)$.

Nice!

Having said all these things, it is now time to explain our contribution. First of all, we describe some conditions in Section 2 which allow us to keep the number of indeterminates that are necessary to saturate I_L low. In particular, we indicate (see Corollary 2.9) how to extend the method of Hosten–Shapiro (see Hosten and Shapiro, 1997).

Then a new idea is to use the homogeneous elimination seen before, combined with more theoretical results described in Subsection 3.1. The output is an algorithm, called EATI (Elimination Algorithm for Toric Ideals), which almost always performs much better than the others. Another main idea is to substitute the sequential procedure described previously with a *parallel* one. More precisely, suppose that we have already computed $I_L \subset k[X_1, \ldots, X_n]$ and we know that we have to saturate it with respect to a set of r indeterminates, say $X_1, \ldots, X_r$. Now suppose that we have r processors. Then the strategy goes as follows. Each processor computes the saturation with respect to a single indeterminate, say X_i, by computing a DegRevLex-Gröbner basis, where X_i is the smallest indeterminate. Since we use vectors of integers, the computation of the Gröbner basis produces an intermediate ideal which contains $I_L : X_i^\infty$, is X_i-saturated and is contained in $\mathcal{I}$. Now suppose the processor works degree by degree. Sometimes a critical pair produces a binomial, which reduces to a homogeneous binomial *of smaller degree* because we cancel out monomial factors, as we explained before. When this phenomenon happens, the new element is passed to the other processors, which interrupts their computation and starts again at the correct degree where the new element is placed. The new algorithm is called PATI (Parallel Algorithm for Toric Ideals); it has a nice behaviour even on a sequential machine mainly because of its *cooperative* nature: namely, each of the r Gröbner basis computations benefits from the information coming from the others, in particular, less critical pairs are necessary and more reductors are available (see Section 3). Our algorithms have been implemented in CoCoA (see `http://cocoa.dima.unige.it`), and our choice for CoCoA 3.6 was EATI.

2. Saturating with a Low Number of Indeterminates

As we said in the introduction, it is important to detect a small set *SatInd* of indeterminates, such that the saturation of a given ideal with respect to the product of all the indeterminates is the same as the saturation with respect to the product of the indeterminates in *SatInd*. We start by recalling a few facts about the saturation of ideals.

DEFINITION 2.1. Let A be a ring, let I be an ideal in A, and let F be a non-zero divisor in A. The **saturation** of I with respect to F is the ideal

$$IA_F \cap A = \{G \in A | GF^i \in I \text{ for some } i \in \mathbb{N}\},$$

that we denote by $I : F^\infty$.

The ideal I is said to be F**-saturated** if $I = I : F^\infty$.

LEMMA 2.2. *Let I, J be ideals in A such that $I \subseteq J \subseteq I : F^\infty$. Then $J : F^\infty = I : F^\infty$.*

PROOF. Clearly $I : F^\infty \subseteq J : F^\infty \subseteq (I : F^\infty) : F^\infty$. But it is easy to check that $(I : F^\infty) : F^\infty = I : F^\infty$, and this concludes the proof.□

Now we give an easy lemma concerning saturation with respect to a product and its factors.

LEMMA 2.3. *Let I be an ideal in A. Then*

(1) $I : (FG)^\infty = (I : F^\infty) : G^\infty$.
(2) If I is F-saturated and G-saturated, then I is FG-saturated.

PROOF. The proof of (1) is an easy exercise and (2) follows immediately from (1).□

COROLLARY 2.4. *Let I and J be ideals in A, such that $I \subseteq J \subseteq I : (FG)^\infty$. If J is F-saturated and G-saturated, then $J = I : (FG)^\infty$.*

PROOF. By Lemma 2.3, 2) we have that $J = J : (FG)^\infty$ and by Lemma 2.2 we conclude that $J = I : (FG)^\infty$.□

PROPOSITION 2.5. *Let I be an ideal in A and F, G non-zero divisors in A. Then the following conditions are equivalent*

(1) $I : F^\infty$ *is G-saturated.*
(2) $I : F^\infty = I : (FG)^\infty$.
(3) IA_F *is G-saturated.*
(4) $IA_F = IA_{FG} \cap A_F$.

PROOF. The equivalence between (1) and (2) follows from the formula

$$I : F^\infty \subseteq (I : F^\infty) : (G)^\infty = I : (FG)^\infty,$$

where the last equality comes from Lemma 2.3. The equivalence between (3) and (4) follows from the formula

$$IA_F \subseteq IA_F : (G)^\infty = (IA_F)A_G \cap A_F = IA_{FG} \cap A_F.$$

From (4) it follows that

$$IA_F \cap A = IA_{FG} \cap A_F \cap A = IA_{FG} \cap A,$$

hence (2) follows. It remains to show that (2) implies (4). Let $r \in IA_{FG} \cap A_F$. Then there exist $\alpha, \beta \in \mathbb{N}$ such that

$$r = \frac{i}{(FG)^\beta} = \frac{a}{F^\alpha},$$

with $i \in I$ and $a \in A$. Then $F^\alpha r \in A \cap IA_{FG} = A \cap IA_F \subseteq IA_F$. Therefore $r \in IA_F$ and we are done.□

COROLLARY 2.6. *Let I be an ideal in A and F, G non-zero divisors in A and assume that G is a non-zero divisor in* A_F/IA_F. *Then* $I : F^\infty = I : (FG)^\infty$.
In particular the conclusion is valid in the following cases

(1) G is invertible in A_F/IA_F.
(2) IA_F *is prime and* $G \notin IA_F$.

PROOF. By assumption A_F/IA_F embeds in $(A_F/IA_F)_G$, which is canonically isomorphic to A_{FG}/IA_{FG}. Therefore $IA_F = IA_{FG} \cap A_F$ and we conclude by Proposition 2.5.□

DEFINITION 2.7. A **binomial** is a difference of power products. A **binomial ideal** is an ideal generated by binomials. If T_1, T_2 are coprime power products, then $T_1 - T_2$ is said to be a **pure binomial**.

DEFINITION 2.8. We denote by *Indets* the set of all the indeterminates and if $E \subset \{1, \ldots, n\}$ by $SatInd_E$ the corresponding subset of *Indets*. Then we denote by $\Pi := \prod_{i \in \{1,\ldots,n\}} X_i$ and by $\Pi_E := \prod_{i \in E} X_i$.

COROLLARY 2.9. (Hosten–Shapiro) *Let I be an ideal in R generated by pure binomials. Then there exists* $E \subset \{1, \ldots, n\}$ *and* $\#(E) \leq \frac{n}{2}$, *such that* $I : {\Pi_E}^\infty = I : \Pi^\infty$.

PROOF. If a binomial $A - B$ is in I, then inverting all the indeterminates in A causes the indeterminates in B to become invertible modulo I. Since $\mathrm{GCD}(A, B) = 1$, either A or B has a number of indeterminates which is smaller than or equal to the total number of indeterminates involved in A and B. If this is true for all the indeterminates then we are done, otherwise we repeat the argument with the remaining ones. At the end, we have inverted all the indeterminates modulo I just by inverting at most half of them, and we conclude by Corollary 2.6.□

This Corollary yields a procedure, called HS, which allows us to saturate with respect to a remarkably small number of indeterminates. However, there are several situations where such bound can be improved as we are going to see.

EXAMPLE 2.1. Let $I := (X_1X_2 - X_3X_4)$. It is a prime ideal, hence $I := I : \Pi^\infty$. We observe that HS would require a saturation with two indeterminates, e.g. X_1X_2.

EXAMPLE 2.2. Let $I := (X_1X_2X_3 - X_4X_5X_6,\ X_5X_7 - X_1X_2X_6)$. The application of HS would suggest saturating with respect to $X_1X_2X_3$ (or other triples of indeterminates like for instance $X_5X_7X_4$). But much better can be done. Namely we let $E := \{5\}$ hence $\Pi_E := X_5$; then $X_7 = \frac{X_1X_2X_6}{X_5}$ in R_{X_5}, so that $R_{X_5}/IR_{X_5} \cong k[X_1, X_2, X_3, X_4, X_5, X_6]_{X_5}/(X_1X_2X_3 - X_4X_5X_6)$, which is an integral domain. In conclusion, IR_{X_5} is prime, hence we apply Corollary 2.6, (2) and conclude that $I : {X_5}^\infty = I : \Pi^\infty$, i.e. it suffices to saturate I simply with X_5.

EXAMPLE 2.3. Here we consider the Example on p. 333 of Li *et al.* (1997). Let $I := (X_2X_4 - X_6X_8,\ X_2X_8^2 - X_4^3,\ X_1X_3 - X_5X_7,\ X_1^2X_7 - X_3^2X_5)$. The application of HS would suggest we saturate with respect to $X_1X_3X_4$ (or $X_4X_5X_7, \dots$). Let us see how to use Corollary 2.6 to obtain a better result. Let $E := \{1,\ 4\}$ hence $\Pi_E := X_1X_4$ and let us invert it; looking at the first two equations we see that X_2, X_6, X_8 also become invertible modulo $IR_{X_1X_4}$. The third equation becomes $X_3 - \frac{X_5X_7}{X_1}$. Substituting into the fourth equation, yields $X_1^2X_7 - \frac{X_5^3X_7^2}{X_1^2}$, equivalently $X_1^4X_7 - X_5^3X_7^2 = X_7(X_1^4 - X_5^3X_7)$. This means that if $J := I + (X_1^4 - X_5^3X_7)$, then $I : \Pi^\infty = J : \Pi^\infty$. But $JR_{X_1X_4} = (X_2X_4 - X_6X_8,\ X_2X_8^2 - X_4^3,\ X_3 - \frac{X_5X_7}{X_1},\ X_1^4 - X_5^3X_7)$, hence in $R_{X_1X_4}/JR_{X_1X_4}$ all the indeterminates are invertible, so that $J : (X_1X_4)^\infty = I : \Pi^\infty$ by Corollary 2.6, (1).

The next result is very helpful in the computation of the homogeneous primitive partition identities (see Sturmfels, 1996, Chapter 6). A first hint to the result was given by Sturmfels in a private communication to La Scala.

COROLLARY 2.10. *Let I be the ideal generated by $\{X_1X_3Y_2^2 - X_2^2Y_1Y_3,\ X_1^2X_4Y_2^3 - X_2^3Y_1^2Y_4, \dots, X_1^{n-1}X_{n+1}Y_2^n - X_2^nY_1^{n-1}Y_{n+1}\}$ in the ring $k[X_1, \dots, X_{n+1}, Y_1, \dots, Y_{n+1}]$. To compute the distribution of the homogeneous primitive partition identities it suffices to compute $I : (X_1Y_2)^\infty$.*

PROOF. It is known (see Sturmfels, 1996 p. 49) that in order to compute the homogeneous primitive partition identities we have to find the Graver basis elements for A, where

$$A := \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & n+1 \end{pmatrix},$$

hence, (see Sturmfels, 1996 Theorem 7.1 p. 55) we have to compute the toric ideal corresponding to the matrix

$$\Lambda(A) := \begin{pmatrix} A^t & I \\ 0 & I \end{pmatrix}.$$

A set of generators of the kernel ideal is $\{X_1X_3Y_2^2 - X_2^2Y_1Y_3,\ X_1^2X_4Y_2^3 - X_2^3Y_1^2Y_4, \dots, X_1^{n-1}X_{n+1}Y_2^n - X_2^nY_1^{n-1}Y_{n+1}\}$, so the problem is to compute $I : \Pi^\infty$. Let $\Pi_E := X_1Y_2$. If we invert Π_E the first equation becomes $X_3 - \frac{X_2Y_1Y_3}{X_1Y_2^2}$; we do the same with the subsequent equations up to the last one, which becomes $X_{n+1} - \frac{X_2^nY_1^{n-1}Y_{n+1}}{X_1^{n-1}Y_2^n}$, hence $IR_{X_1Y_2}$ is prime and we may conclude by Corollary 2.6, (2).□

3. Computing the Saturation with Respect to a Set of Indeterminates

Let $\mathbf{w} := (w_0,\ w_1,\ \dots,\ w_n)$, where $w_i \in \mathbb{N}^+$ for $i = 0, \dots, n$; let k be a field and $X_0, \dots, X_n$ independent indeterminates over k. We consider the polynomial ring $S := k[X_0, \dots, X_n]$ graded over $\mathbf{w}$, i.e. $\deg(X_i) = w_i$.

We recall the following well-known theorem, from which one can draw an efficient way to compute $I : {X_0}^\infty$, the saturation of I with respect to an indeterminate X_0. For the sake of completeness, we include the easy proof.

THEOREM 3.1. *Let I be an ideal in S homogeneous with respect to $\mathbf{w}$ and σ a term-order represented by a matrix whose first row is $\mathbf{w}$ and second row is $(-1,\ 0,\ \dots,\ 0)$. Let $\{{X_0}^{a_1}F_1, {X_0}^{a_2}F_2, \dots, {X_0}^{a_r}F_r\}$ be a σ-Gröbner basis of I of $\mathbf{w}$-homogeneous elements, where $X_0 \nmid F_i$ for $i := 1, \dots, r$. Then $\{F_1, \dots, F_r\}$ is a σ-Gröbner basis of $I : {X_0}^\infty$.*

PROOF. Let F be a polynomial in $I : {X_0}^\infty$; we need to show that there exists i such that $\mathrm{Lt}_\sigma(F_i) \mid \mathrm{Lt}_\sigma(F)$. The assumption that $F \in I : {X_0}^\infty$ means that there exists $m \in \mathbb{N}$ such that ${X_0}^m \cdot F \in I$. As a consequence ${X_0}^m \cdot \mathrm{Lt}_\sigma(F) \in \mathrm{Lt}_\sigma(I)$, hence, there exists an index i such that ${X_0}^{a_i} \cdot \mathrm{Lt}_\sigma(F_i) \mid {X_0}^m \cdot \mathrm{Lt}_\sigma(F)$. But $X_0 \nmid F_i$, hence $X_0 \nmid \mathrm{Lt}_\sigma(F_i)$ by the assumption on σ, hence $\mathrm{Lt}_\sigma(F_i) \mid \mathrm{Lt}_\sigma(F)$ and this concludes the proof.□

Now we wish to extend the method explained in Theorem 3.1 to the general case. We need the following technical result.

LEMMA 3.2. *Let $A \subset B$ be an inclusion of rings, I an ideal in A, L an ideal in B and assume that $IB \cap A = I$. Then*

(1) The canonical homomorphism $A/I \to B/IB$ is injective.
(2) Identifying A/I with its canonical image in B/IB, we have

$$((IB + L) \cap A)/I = ((IB + L)/IB) \cap (A/I).$$

PROOF. The easy proof is left to the reader.□

COROLLARY 3.3. *Let $\mathbf{w} := (w_0,\ w_1,\ \dots,\ w_n)$, where $w_i \in \mathbb{N}^+$ for $i := 0, \dots, n$ and let $S := k[X_0, X_1, \dots, X_n]$ be graded over $\mathbf{w}$. Let J be a homogeneous ideal in S with respect to $\mathbf{w}$, F a non-zero homogeneous polynomial of S of degree d and $S[U] := k[U, X_0, X_1, \dots, X_n]$ graded over $\mathbf{w}' := (d,\ w_0,\ w_1,\ \dots,\ w_n)$. Let σ be a term-order on $S[U]$ represented by a matrix whose first row is $\mathbf{w}'$ and second row is $(-1,\ 0,\ \dots,\ 0)$.*

Let $\{U^{a_1}F_1, U^{a_2}F_2, \ldots, U^{a_r}F_r\}$ *be a* σ*-Gröbner basis of* $(F-U, J)$ *of* $\mathbf{w}'$*-homogeneous elements, where* $U \not| F_i$ *for* $i := 1, \ldots, r$*. Then*

$$JS_F \cap S = J : (F)^\infty = (F_1', \ldots, F_r'),$$

where F_i' *is the polynomial obtained by substituting* U *with* F *in* F_i*.*

PROOF. Using the Theorem 3.1 applied to the ideal $(F-U, J)S[U]$ we deduce that $(F-U, J)S[U]_U \cap S[U] = (F_1, \ldots, F_r)$, hence $(F_1, \ldots, F_r)/(F-U) = ((F-U, J)S[U]_U \cap S[U])/(F-U)$. Now we apply Lemma 3.2 to $A := S[U]$, $B := S[U]_U$, $I := (F-U)A$, $L := JB$ and we obtain $((F-U, J)S[U]_U \cap S[U])/(F-U) = ((F-U, J)S[U]_U/(F-U)) \cap S[U]/(F-U)$ We observe that $((F-U, J)S[U]_U/(F-U)) \cong JS_F$ and $S[U]/(F-U) \cong S$ and we are done.□

Our goal is to compute the saturation of a $\mathbf{w}$-homogeneous binomial ideal I with respect to the product of all the indeterminates. As we said in the introduction, a well-known method (see Pottier, 1994) suggests we remove monomial factors from the binomials during the computation of the Gröbner basis. So we need the following definitions.

DEFINITION 3.4. Let F be a binomial, $F := TT_1 - TT_2$ with T_1 and T_2 coprime. Then we call the pure binomial $T_1 - T_2$ the **saturation** of F, and we denote it by *Sat(F)*.

DEFINITION 3.5. Let L be a list of binomials ordered by a term-order σ and F a binomial. We define the **saturating remainder** of F with respect to L, and we denote it by SatRem(F), the binomial obtained in the following way: if F' is obtained as an **intermediate** step during the division of F by L, then F' is replaced by Sat(F'). We define the **saturating S-polynomial** of F and G to be the binomial Sat($SP(F, g)$), which we simply denote by Sat$SP(F, G)$.

Now we need a general result.

LEMMA 3.6. *Let* I *be an ideal in a polynomial ring and* σ *a term-order. Suppose that during the computation of a* σ*-Gröbner basis of* I *via the Buchberger Algorithm we substitute* some *polynomials with one of their factors. Then we compute the* σ*-Gröbner basis of an ideal* J *which contains* I*.*

PROOF. The easy proof is left to the reader.□

COROLLARY 3.7. *Let* I , $\mathbf{w}$ *and* σ *be as in Theorem 3.1. Suppose that during the computation of a* σ*-Gröbner basis of* I *we use the following strategy*

(a) *we discard* some *of the pairs* (F, G) *with the property that* $Rem(SP(F, G)) = 0$.
(b) *we substitute* all *the polynomials* F *with* $Sat(F)$*.*

Then we obtain a σ*-Gröbner basis of an ideal* J *such that* $I : {X_0}^\infty \subseteq J = J : {X_0}^\infty$.

PROOF. The easy proof based on Theorem 3.1 and Lemma 3.6 is left to the reader.□

Suppose that we want to saturate a binomial ideal I with respect to all the indeterminates and that we know that it suffices to saturate it with respect to a subset of indeterminates $SatInd_E$, $E \subset \{1,\dots,n\}$, which is always the case as we have seen in Section 2. We describe two new algorithms, which do the job:

3.1. ELIMINATION ALGORITHM FOR TORIC IDEALS (EATI)

DEFINITION 3.8. Let σ be a term-order and $F := T_1 - T_2$ a binomial such that $T_1 >_\sigma T_2$. Then we call as usual *leading term* of F the power-product T_1 and we denote it by $\mathrm{Lt}_\sigma(F)$. Similarly, we call the power-product T_2 the **tail** of F, and we denote it by $\mathrm{Tl}_\sigma(F)$. If it is not necessary to specify σ, we simply write $\mathrm{Lt}(F)$ and $\mathrm{Tl}(F)$.

DEFINITION 3.9. We denote by σ a term order on $S[U] := k[U, X_0, \dots, X_n]$ represented by a matrix whose first row is $\mathbf{w} := (d, w_0, \dots, w_n)$, second row is $(-1, \ 0, \ \dots, \ 0)$ and following rows $(0, \ \dots, \ -1, \ \dots, \ 0)$ with -1 in ith position for each $i \in E$.

DEFINITION 3.10. Let L be a list of binomials ordered by a term-order σ and F a binomial. We define the **elimination-saturating remainder** of F with respect to L and, we denote it by *ElimSatRem(F)*, the binomial obtained in the following way: let $F' =$ *SatRem(F)*. If U divides $\mathrm{Tl}(F')$, then we perform the substitution $U \mapsto \Pi_E$ and obtain a binomial F''. If $\mathrm{Lt}(F') = \mathrm{Lt}(F'')$ then *ElimSatRem(F)* returns *Sat*(F''), otherwise it returns F'.

PROPOSITION 3.11. *Let I be an ideal generated by binomials. The following algorithm returns a Gröbner basis $\mathcal{G}$ of the ideal $(I, \Pi_E - U)$ with respect to σ. The subset $\mathcal{G}'$ of the binomials F in $\mathcal{G}$ such that $U \nmid \mathrm{Tl}(F)$ is a Gröbner basis of the toric ideal $(I : \Pi_E^\infty)$ with respect to σ.*

ALGORITHM EATI

Start with:
$\mathcal{F}$ the list containing a set of binomial generators of I and the binomial $\Pi_E - U$,
d the minimum degree in $\mathcal{F}$,
$\mathcal{G} := \emptyset$ and Pairs $:= \emptyset$.
While $d < \infty$ do these steps:

(1) take a pair C of degree d from Pairs and compute
$F :=$ *ElimSatRem*(*SatSP*(C)) wrt the elements of $\mathcal{G}$.
If $F \neq 0$ then add F to $\mathcal{G}$ and add the pairs given by F and the elements of $\mathcal{G}$ to Pairs.
If $\deg(F) < d$ go to 3, otherwise take another pair of degree d and repeat.
(2) take a binomial F of degree d from $\mathcal{F}$ and compute
$F :=$ *ElimSatRem(F)* wrt the elements of $\mathcal{G}$.
If $F \neq 0$ then then add F to $\mathcal{G}$ and add the pairs given by F and the elements of $\mathcal{G}$ to Pairs.
If $\deg(F) < d$ go to 3, otherwise take another binomial of degree d and repeat.
(3) $d :=$ minimum degree in $\mathcal{F}$ and Pairs.

PROOF. First we prove that $\mathcal{G}'$ is a Gröbner basis. We need to show that any S-polynomial given by binomials in $\mathcal{G}'$ reduces to zero with respect to $\mathcal{G}'$. Note that, by definition of elimination-saturating remainder, each binomial F in $\mathcal{G}\backslash\mathcal{G}'$ have $U|\,\mathrm{Tl}(F)$ and the substitution $U \mapsto \Pi_E$ would give $\mathrm{Lt}(F) < \mathrm{Tl}(F)$. This means that the smallest saturating indeterminate X_k appears in $\mathrm{Lt}(F)$, more precisely $\deg_{X_k}(\mathrm{Lt}(F)) \geq \deg_U(\mathrm{Tl}(F))$. Therefore, such a binomial cannot be a reducer for a binomial F' in $k[X_0, X_1, \ldots, X_n]$ as the smallest indeterminate X_k cannot appear in $\mathrm{Lt}(F')$. So the reduction to zero of any S-polynomial given by binomials in $\mathcal{G}'$ is performed by elements of $\mathcal{G}'$ itself.

Now we prove that $\mathcal{G}'$ is a Gröbner basis for $(I : \Pi^\infty)$. By Corollary 3.3 we have that $(I : \Pi^\infty)$ is generated by the substitution $U \mapsto \Pi_E$. Let $F \in \mathcal{G}\backslash\mathcal{G}'$ and perform the substitution. We have seen that this operation gives UF'. This implies that F' is in $(I : \Pi^\infty)$ and then reduces to zero with respect to $\mathcal{G}'$. Therefore all elements in $\mathcal{G}\backslash\mathcal{G}'$ generate redundant generators for the toric ideal.□

3.2. PARALLEL ALGORITHM FOR TORIC IDEALS (PATI)

DEFINITION 3.12. For all $i = 1, \ldots, n$, we denote by σ_i a term order represented by a matrix whose first row is $\mathbf{w}$ and following row is $(0, \ \ldots, \ -1, \ \ldots, 0)$ with -1 in ith position.

We call a σ_i-**Gröbner basis** a Gröbner basis with respect to σ_i.

PROPOSITION 3.13. *Let I be an ideal generated by binomials. The following algorithm returns $\#(E)$ Gröbner bases of the ideal I.*

ALGORITHM PATI

Start with:
$\mathcal{F}$ the list containing a set of binomial generators of I,
d the minimum degree in $\mathcal{F}$,
$\mathcal{G}_{\sigma_i} := \emptyset$ and $\mathrm{Pairs}_{\sigma_i} := \emptyset$, for each $i \in E$.
While $d < \infty$ do these steps:

(1) take a pair C of degree d from some $\mathrm{Pairs}_{\sigma_j}$ and compute
$F :=$ *SatRem(SatSP(C))* wrt the elements of $\mathcal{G}_{\sigma_j}$.
If $F \neq 0$ and $\deg(F) = d$ then add F to $\mathcal{G}_{\sigma_j}$ and add the pairs given by F and the elements of $\mathcal{G}_{\sigma_j}$ to $\mathrm{Pairs}_{\sigma_j}$, then take another pair of degree d and repeat.
If $F \neq 0$ and $\deg(F) < d$, update $\mathcal{G}_{\sigma_i}$ and $\mathrm{Pairs}_{\sigma_i}$, for each $i \in E$, as described in 2 and then go to 3.
(2) take a binomial F of degree d from $\mathcal{F}$ and compute, for each $i \in E$,
$F_i :=$ *SatRem(F)* wrt $\mathcal{G}_{\sigma_i}$. If for some j, $\deg(F_j) < \deg(F)$ then repeat the reduction on $F := F_i$.
If $F \neq 0$ ($\Leftrightarrow F \notin I \Leftrightarrow F_i \neq 0$ for each $i \in E$) then, for each $i \in E$, add F_i to $\mathcal{G}_{\sigma_i}$ and add the pairs given by F_i and the elements of $\mathcal{G}_{\sigma_i}$ to $\mathrm{Pairs}_{\sigma_i}$.
(3) $d :=$ minimum degree in $\mathcal{F}$ and $\mathrm{Pairs}_{\sigma_i}$.

PROOF. We prove the correctness of the Algorithm PATI. As we see in the description above, when *SatRem(SatSP(C))* has smaller degree than *Rem(SP(C))* during the computation of the σ_i-Gröbner basis for some i, then we pass the polynomial to the computation of all the j-Gröbner bases, $j \neq i$. In this way we are computing $\#(E)$ Gröbner bases of an ideal which changes during the computation itself, but which is, at any time, the same for all the term orders.

At the end, we obtain $\#(E)$ Gröbner bases of an ideal J such that $J \subseteq I : \Pi_E{}^\infty$, because the only changes to the original ideal I are divisions by power products. Moreover, $I : X_i^\infty \subseteq J = J : X_i^\infty$ for all $i \in E$, by Corollary 3.7. Now we use Corollary 2.4 and we obtain $J = I : \Pi_E{}^\infty$, where as usual $\Pi_E := \prod_{i \in E} X_i$ and $I : \Pi_E{}^\infty = I : \Pi^\infty$.□

A line of PATI reads

add the pairs given by F_i and the elements of $\mathcal{G}_{\sigma_i}$ to Pairs_{σ_i}.

In this subsection we describe some criteria in order to delete unnecessary critical pairs in the Algorithm PATI. First, we check that the classical criteria can be used.

REMARK 3.14. The first remark is that if M_i denotes the module generated by the syzygies in $Pairs_{\sigma_i}$ (see Capani *et al.*, 1997, Section 3 for a detailed description), we can substitute $Pairs_{\sigma_i}$ with any subset of it which contains a minimal set of generators of M_i. For the remaining ones it is well known that the corresponding S-polynomial would reduce to zero, hence we may apply Corollary 3.7. Moreover, there is no problem in using the *coprime* criterion because if F, G are such that $\text{Lt}(F)$ and $\text{Lt}(G)$ are coprime, then clearly $SP(F, G)$ reduces to zero and again we may apply Corollary 3.7.

Now we describe one more criterion, which turns out to be very important for the optimization of PATI.

We have seen that, during the computation, Algorithm PATI always uses pure binomials. We recall that we denote by $SatInd_E$ the subset of indeterminates which we use to saturate the binomial ideal I.

PROPOSITION 3.15. - **Criterion Tail.** *Let F and G be two binomials. If Ind denotes the set of indeterminates which divide* $\text{GCD}(\text{Tl}_{\sigma_i}(F), \text{Tl}_{\sigma_i}(G))$, *assume that there exist $h > i$ such that $X_h \in SatInd_E \cap Ind$. Then the pair associated to (F, G) can be discarded from the set* Pairs_{σ_i}.

PROOF. By assumption, there exists $h \in E$ such that $X_h | \text{GCD}(\text{Tl}(F), \text{Tl}(G))$. This implies that $\text{SP}_{\sigma_i}(F, G) = X_h \cdot H$ for a suitable binomial H (not necessarily pure). Therefore $H \in I : X_h^\infty \subseteq J$, hence $SP(F, G)$ will reduce to zero and we apply Corollary 3.7.□

REMARK 3.16. The criterion above can be applied because even if the σ_h-Gröbner basis is not computed yet, we know that sooner or later it will be computed. At that time we have the necessary polynomials which reduce $SP(F, G)$ to zero. But this is of no concern, as the critical pairs can be handled in any order.

The following Lemma tells us that the criterion Tail applies when $\deg(SatSP(F, G)) < \deg(SP(F, G))$ as both assume that $\text{GCD}(\text{Tl}(F), \text{Tl}(G)) \neq 1$.

LEMMA 3.17. *Let F and G be two pure binomials. Then the following conditions are equivalent*

(1) $SP(F,G) = SatSP(F,G)$.
(2) $\mathrm{GCD}(\mathrm{Tl}(F), \mathrm{Tl}(G)) = 1$.

PROOF. The easy proof is left to the reader.□

3.3. REMARKS

Algorithm PATI works very well (even on a sequential machine) mainly because of its *cooperative* nature. We mean that every σ_i-Gröbner basis takes advantage of the information coming from the others. In particular the ideal J, of which we compute $\#(E)$ Gröbner bases, changes during the computation, but is always the same for every $i \in E$. This implies that

(a) we may use Criterion Tail.
(b) for every $i \in E$, the corresponding computation benefits from more reductors. The drawback can be space complexity, but only on a sequential machine.
(c) we may use an Hilbert-driven strategy (see Traverso, 1996 and Caboara *et al.*, 1996). Namely, when we finish the computation of the i-Gröbner basis for some i in some degree d we know the dimension of the current ideal J in degree d. We obtain this information computing the Hilbert function of the partial i-Gröbner basis (see Bigatti, 1997) and then we compare it with the Hilbert functions of the j-Gröbner basis, for each $j \neq i$. The difference between the two values is the missing number of elements of the j-Gröbner basis in degree d. If it is zero, we can delete all the pairs of degree d from the computation of the j-Gröbner basis. The Hilbert function of the i-Gröbner basis holds for all computations of degree d unless we find a new generator F, whose degree is obviously smaller than d. In this case the ideal is modified and so also the Hilbert function. This can be very useful at the end of the computation.

Another way of lowering the complexity of computing toric ideals is to detect small sets $E \subset \{1, \ldots, n\}$, such that it suffices to saturate with respect to the indeterminates in E. The idea could be to generalize the argument given in Example 2.3. Of course the greatest benefit would go to the sequential algorithm and to PATI run on a sequential machine.

Example	Ind	Gens	Sat	GB	PATI	Seq	EATI
Rnd6x12,0-3	12	48	2	1030	6.89 s	5.64 s	6.75 s
Rnd6x12,0-3	12	48	3	1068	11.36 s	8.74 s	12.13 s
Rnd6x12,0-3	12	48	3	882	6.71 s	5.55 s	6.34 s
VT5,4,2	45	320	2	789	12.92 s	12.66 s	6.76 s
VT7,4,1	35	224	3	308	1.42 s	1.57 s	0.61 s
VT4,4,4	35	248	2	526	3.97 s	3.88 s	2.12 s
HS2,10	45	280	5	568	14.25 s	12.64 s	2.61 s
HS3,8	56	384	3	1127	60.82 s	56.32 s	22.30 s
CG11	55	352	6	902	71.12 s	80.17 s	11.05 s
CG12	66	432	6	1344	230.32 s	289.90 s	32.16 s
HPPI10	20	8	2	1830	21.85 s	18.12 s	10.40 s
HPPI11	22	9	2	3916	127.85 s	132.73 s	79.10 s
HPPI12	24	10	2	8569	771.37 s	903.51 s	560.74 s
DiagG4x5,3	40	208	7	163	0.92 s	0.87 s	0.61 s
DiagS5x5,3	100	704	5	854	46.03 s	45.00 s	25.75 s

4. Description of the Examples and Timings

The examples which are randomly generated are denoted by the prefix "Rnd". For instance, Rnd6x12,0-3 is a random matrix of dimensions 6 by 12 with integer entries in the range 0–3. We give three examples of this sort as their behaviour may vary.

The following examples have a combinatorial structure. For a complete description see the indicated chapters in Sturmfels (1996).

The first class of "combinatorial" examples in our list is given by the Veronese-type varieties that we have denoted by the "VT" prefix. For instance, according to Sturmfels notation of section 14.A, VT5,4,2 is the Veronese-type variety with parameters $d = 5, r = 5, s_1, \ldots, s_d = 2$.

The examples of "HS" type are configurations corresponding to rth hyper-simplexes (see Chapter 9 and p. 84 of Sturmfels, 1996). For instance, HS3,8 is the configuration of the third hyper-simplex of $\mathbf{R}^8$ (equivalent to VT8,3,1).

The "CGn" examples are given by the node-edge incidence matrices of the complete graphs on n nodes. More specifically, the toric ideal is the kernel of the following map: $x_{ij} \mapsto t_i t_j \quad 1 \leq i < j \leq n$ (equivalent to VTn,2,1).

Other examples we have considered are homogeneous primitive partition identities (see Chapter 6 of Sturmfels, 1996), denoted by the "HPPI" prefix.

The example DiagG4x5,3 is the toric ideal which describes the algebra generated by the diagonal terms of 3×3-minors of a 4×5 generic matrix. The example DiagS5x5,3 corresponds to 3×3-minors of a 5×5 symmetric matrix.

The examples were computed on a SUNW,Ultra-1, RAM 64Mb, 140 Mhz, compiled with gcc -O2. The meaning of the columns is the following:

"Ind" denotes the number of indeterminates in the corresponding example;
"Gens" denotes the number of the binomials given in input;
"Sat" is the number of indeterminates which we use to saturate;
"GB" is the number of elements in the final Gröbner basis;
"PATI" is the timing in seconds obtained with the algorithm PATI;
"Seq" is the timing in seconds obtained with the sequential algorithm;
"EATI" is the timing in seconds obtained with the algorithm EATI.

Great advantage in the computation is given by the coding of the leading terms of the binomials as described in Bigatti (1997). Briefly, we associate to any monomial with support $\{x_{i_o}, \ldots, x_{i_t}\}$ a 32-bit unsigned integer whose binary expansions have 1s in the i_jth places and 0s elsewhere. This representation, which takes very little memory, allows us to compare the supports very quickly via built-in bitwise functions.

References

Adams, W., Loustaunau, P. (1994). *An Introduction to Gröbner Bases*, GSM 3. Providence, RI, American Mathematical Society.

Bigatti, A. M. (1997). Computation of Hilbert-Poincaré series. *J. Pure Appl. Algebra*, **119**, 237–253.

Buchberger, B. (1985). An algorithmic method in polynomial ideal theory. Chapter 6. In Bose, N. K., ed., *Progress, Directions, and Open Problems in Multidimensional Systems Theory*, pp. 184–232. Dodrecht, Reidel Publishing Company.

Caboara, M., De Dominicis, G., Robbiano, L. (1996). Multigraded Hilbert functions and Buchberger algorithm. In Lakshman, Y. N., ed., *Proceedings of ISSAC '96* , pp. 72–78. New York, ACM.

Capani, A., De Dominicis, G., Niesi, G., Robbiano, L. (1997). Computing minimal finite free resolutions. *J. Pure Appl. Algebra*, **117&118**, 105–117.

Capani, A., Niesi, G., Robbiano, L. (1995). CoCoA, a system for doing computations in commutative algebra. Available via anonymous ftp from `cocoa.dima.unige.it`.

Capani, A., Niesi, G., Robbiano, L. (1997). Some Features of CoCoA 3. *Moldova J. Comput. Sci.*, **4/3**, 296–314.

Conti, P., Traverso, C. (1991). Buchberger algorithm and integer programming. In Springer, ed., *Proceedings AAECC-9*, LNCS 539, pp. 130–139. New York, Springer.

Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties, and Algorithms.* New York, Springer.

Di Biase, F., Urbanke, R. (1995). An algorithm to calculate the kernel of certain polynomial ring homomorphisms. *Exp. Math.*, **4**, 227–234.

Eisenbud, D., Sturmfels, B. (1996). Binomial ideals. *Duke Math. J.*, **84**, 1–45.

Hosten, S., Shapiro, J. (1997). Primary decompositions of lattice basis ideals. To appear.

Hosten, S., Sturmfels, B. (1995). GRIN: An implementation of Gröbner bases for integer programming. In Balas, E. J. C., ed., *Integer Programming and Combinatorial Optimization*, LNCS 920, pp. 267–276. New York, Springer.

Hosten, S., Thomas, R. (1998). Gröbner bases and integer programming. In *Gröbner Bases and Applications*, LMSLNS **251**, pp. 144–158. Cambridge, Cambridge University Press.

Li, Q., Guo, Y., Ida, T., Darligton, J. (1997). The minimised geometric buchberger algorithm: an optimal algebraic algorithm for integer programming. In *Proceedings of ISSAC-97*, pp. 331–338. New York, ACM.

Pottier, L. (1994). Gröbner bases of toric ideals. Research report 2224, INRIA, Sophia Antipolis.

Robbiano, L., Sweedler, M. (1988). Bases of subalgebras. In *Commutative Algebra Proceedings*, LNM 1430, Salvador, Brasil. New York, Springer.

Sturmfels, B. (1996). *Gröbner bases and convex polytopes*, ULS 8, Providence, RI, American Mathematical Society.

Thomas, R. (1997). A geometric Buchberger algorithm for integer programming. *Math. Oper. Res.*, **77**, 357–387.

Thomas, R., Weismantel, R. (1997). Truncated Gröbner bases for integer programming. *Appl. Algebra Eng., Commun. Comput.*, **8**, 241–257.

Traverso, C. (1996). Hilbert Functions and the Buchberger Algorithm. *J. Symb. Comput.*, **22**, 355–376.

Originally Received 17 February 1998
Accepted 15 December 1998