Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

162

Computer Algebra

EUROCAL'83, European Computer Algebra Conference
London, England, March 1983

Edited by J. A. van Hulzen

Springer-Verlag
Berlin Heidelberg New York Tokyo

Lecture Notes in Computer Science
Computer Algebra — EUROCAL'83
Proceedings

Editor

J. A. van Hulzen
Twente University of Technology
Department of Computer Science
P.O.Box 217, 7500 AE Enschede, The Netherlands

CR Subject Classifications (1982): I.1., J.2.

ISBN 3-540-12868-9 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-12868-9 Springer-Verlag New York Heidelberg Berlin Tokyo

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2145/3140-543210

A NOTE ON THE COMPLEXITY OF CONSTRUCTING GRÖBNER-BASES

B.Buchberger

Mathematisches Institut
Universität Linz
A4040 LINZ, Austria

ABSTRACT

In the bivariate case, upper bounds for the degrees and the number of polynomials occuring in Gröbner-bases of polynomial ideals are given. In the case of the total degree ordering of monomials, the upper bound for the degrees is linear in the maximal degree of the polynomials in the given basis of the ideal. In the general case, the upper bound for the degrees is quadratic. The upper bound for the number of polynomials is linear in the minimal degree of the polynomials in the given basis. All the bounds are shown to be tight. The relevance of these bounds for constructive polynomial ideal theory is indicated.

Acknowledgement
This work was sponsored by the Austrian "Fonds zur Förderung der wissenschaftlichen Forschung" (Project Nr. 4567). Special thanks to D. Lazard who made a number of extremely valuable comments on the content of the paper (see below).

BACKGROUND AND MOTIVATION

The concept of Gröbner-bases for polynomial ideals has been introduced implicitly in /Buchberger 65, 70/ (where an algorithm for constructing such bases was established) and explicitly in /Buchberger 76a/. Gröbner-bases have since been treated in a number of papers, see /Buchberger, Loos 82, Section 12/ for a fairly complete bibliography and a brief introduction into the subject. We assume here that the reader is familiar with the concept, motivation, algorithmic construction and application of Gröbner-bases. (Also /Buchberger 79/ seems to be suitable as an easy introduction).

In the multivariate case, little is known about the complexity of constructing Gröbner-bases (and of similar algorithms). In the univariate case, the Gröbner-basis algorithm specializes to Euclid's algorithm whose complexity has been extensively studied (see /Loos 82/ for a survey). In the general case we have the complexity results of /Hermann 26/ for the degrees of polynomials in her standard bases (Hermann-bases, see also /Seidenberg 74/) and the recent results of /Cardoza, Lipton, Meyer 76/ and /Mayr, Meyer 81/ on the intrinsic space complexity of solving the uniform word problem for commutative semigroups (which is a special case of deciding membership for polynomial ideals given by bases). These results indicate that the construction of standard bases for polynomial ideals, intrinsically, is an exponential problem (if n, the number of variables, enters the complexity considerations).

Still, for practical applications it is important to investigate the complexity of constructing standard bases for fixed $n \geq 2$ and to establish bounds that are as tight as possible (and to improve the algorithms). In this paper, we consider $n = 2$. The Gröbner-basis algorithm is of particular interest in this case for practical applica-

tions, see /Guiver 82/ and /Sakata 81/. Also, tight bounds for the complexity (in particular for the degrees of the polynomials) of Gröbnerbases are interesting for a theoretical reason: the connection between resultants and Gröbner-bases is still not very well understood. There were two attempts to combine the use of resultants and of the reductions used in the Gröbner-basis algorithm in order to improve computations: /Schaller 79/ and /Pohst, Yun 81/. However, these computational considerations did not add to an understanding of the fundamental connection between the two concepts.

Recently, /Bayer 82/ has given an interesting approach to bringing the concepts together: Euclid's algorithm, Gauss' algorithm and the Gröbner-basis algorithm are viewed as special procedures of computing certain determinants ("resultants") in the univariate, linear multivariate, and general case, respectively. The present author intends to give a more specific connection between the concepts along the same lines in a future paper, by connecting one single matrix with a system of polynomials whose "normal form" by elementary row and column transformation answers questions about the solvability of the system and similar questions and whose transformation into normal form can be viewed as an application of the Gröbner-basis algorithm. The practicability of this approach heavily depends on the availability of (realistic) bounds for the degrees of the polynomials in Gröbner-bases. Essentially the same approach is pursued in /Lazard 83/.

This paper extends a result given in /Buchberger 79/ (an upper bound for the degrees of the polynomials in bivariate Gröbner-bases) to its "nearly" best possible form and gives some new results. D. Lazard meanwhile was able to totally fill the gaps between lower and upper bounds left open in this paper. We indicate his results in parentheses. The proofs of his results appear in /Lazard 83/, these proceedings. Still, we think that our proof methods, which are totally distinct from the algebraic geometry approach of Lazard, may present some interest in themselves and, furthermore, the combination of the methods may yield some new insights. Also, our Theorem 1 holds for all polynomials occurring during the execution of the Gröbner-basis algorithm whereas Lazard's version, I think, can be asserted for the final outcome of the algorithm only.

N O T A T I O N

Let K be an arbitrary field. By $K[x,y]$ we denote the ring of bivariate polynomials over K and by $[x,y]$ the set of bivariate monomials. An "admissible" ordering of the monomials is a linear ordering $\prec$ on $[x,y]$ satisfying:

$1 \prec t$ (for all monomials $t \neq 1$) and

$s \prec t \Longrightarrow s.u \prec t.u$ (for all monomials s, t, u).

For $f \in K[x,y]$, LC(f) and LM(f) denote the leading coefficient and the leading monomial of f w.r.t. $\prec$ (if $\prec$ is clear from the context), D(f) is the degree of f. For s, $t \in [x,y]$, $E^i(t)$ denotes the exponent of t at the i-th variable (i=1,2), and LCM(s,t) is the least common multiple of s and t. We say that s divides t (t is a multiple of s) iff $E^1(s) \leq E^1(t)$ and $E^2(s) \leq E^2(t)$. For $F \subset K[x,y]$, ID(F) is the ideal generated by F, MAXD(F) = max {D(f) / $f \in F$}, MIND(F) = min {D(f) / $f \in F$}. ID(F) is zero-dimensional iff F, viewed as a system of algebraic equations, has only finitely many

solutions (see any text on algebraic geometry). G is a minimal Gröbner-basis for F iff G is a Gröbner-basis for F and deleting a polynomial in G destroys the property of being a Gröbner-basis for F; a minimal Gröbner-basis is reduced iff all the polynomials in G are reduced w.r.t. the other polynomials in G (see /Buchberger 76b/).

Examples: The "total degree" ordering and the "purely lexicographical" ordering are admissible orderings. $\{1,x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3,\ldots\}$ and $\{1,x,x^2,x^3,\ldots, y,xy,x^2y,\ldots,y^2,xy^2,x^2y^2,\ldots\}$ is the set $[x,y]$ enumerated in the total degree and purely lexicographic ordering, respectively. Let $f:= 5x^5y + 3xy^2 - xy$. Then $LC(f) = 5$, $LM(f) = x^5y$, if we use the total degree ordering, and $LC(f) = 3$, $LM(f) = xy^2$, if we use the purely lexicographical ordering. $D(f) = 6$. Let $s:= x^5y$, $t:= xy^2$, then $E^1(s) = 5$, $E^2(s) = 1$, $LCM(s,t) = x^5y^2$. s divides LCM(s,t), but s does not divide t.

R E S U L T S

Theorem 1: Let F be a finite set of polynomials in $K[x,y]$. Then all the polynomials h occurring during the application of the Gröbner-basis algorithm to the input F (using total degree ordering of monomials), in particular the polynomials h in the final Gröbner-basis, satisfy

$D(h) \leq 2.MAXD(F)$ (D. Lazard: $D(h) \leq 2.MAXD(F)-1$).

(By the "Gröbner-basis algorithm" we mean the author's algorithm introduced in /Buchberger 65/ in the version described in /Buchberger 79/, where an "overlap-lemma" ("Criterion 2" and "Criterion 3" in /Buchberger 79/) is used in order to detect situations in which certain "critical pairs" (S-polynomials) need not be considered in the course of the algorithm.)

Corollary 1: Let F be a finite set of polynomials in $K[x,y]$ and G a minimal Gröbner-basis for F w.r.t. the total degree ordering of monomials. Then

$MAXD(G) \leq 2.MAXD(F) (-1)$.

Corollary 2: Let F be a finite set of polynomials in $K[x,y]$ such that ID(F) is zero-dimensional and let G be a minimal reduced Gröbner-basis for F w.r.t. an arbitrary admissible ordering of monomials. Then

$MAXD(G) \leq 4.MAXD(F)^2$ (D. Lazard: $MAXD(G) \leq MAXD(F)^2$, condition on zero-dimensionality can be dropped).

Proposition 1: For every natural number d there is an $F \subset K[x,y]$ with $d = MAXD(F)$ such that for all Gröbner-bases for F (w.r.t. the total degree ordering of monomials)

$MAXD(G) \geq 2d - 1$.

Proposition 2: For every natural number d there is an $F \subset K[x,y]$ with $d = MAXD(F)$ such that for all Gröbner-bases for F (w.r.t. the purely lexicographical ordering of monomials)

$MAXD(G) \geq d^2-d+1$ (D. Lazard: $MAXD(G) \geq d^2$).

Theorem 2: Let F be a finite set of polynomials in $K[x,y]$ and G a minimal Gröbner-basis for F w.r.t. an arbitrary admissible odering of monomials. Then

$|G| \leq MIND(LM(F)) + 1$.

Proposition 3: For every natural number d there is an $F \subset K[x,y]$ with $d = MIND(LM(F))$ such that for all Gröbner-bases G for F (w.r.t. an arbitrary admissible ordering)

$$|G| > d + 1.$$

Remarks:

The upper bound obtained in Theorem 1 should be compared with the following upper bound for the degrees of polynomials for Hermann-bases H for F (see /Hermann 26/):

$$MAXD(H) \leq MAXD(F) + MAXD(F)^2.$$

(The correction in /Seidenberg 74/ of Hermann's results indicates that Hermann's bound should even read $MAXD(F)^4$ in this case). The comparison gives some optimism that Hermann's upper bounds can be improved essentially also in the case n>3.

Repeating the arguments in /Buchberger 79/, the following upper bound for the number of steps (in the uniform cost measure) for constructing a Gröbner-basis G for F may be obtained from Theorem 1:

$$3/2 \cdot (|F| + 2.(MAXD(F)+2)^2)^4.$$

From the proof of Corollary 2 one sees, that for arbitrary (not necessarily reduced) minimal Gröbner-bases G for F one has

$$MAXD(LM(G)) \leq 4.MAXD(F)^2.$$

/Schaller 79/ showed that, in the case of the purely lexicographical ordering, the degrees of polynomials occurring in (the computation of) a Gröbner-basis G for bivariate F can be bounded by $2.MAXD(F)^2$. Proposition 2 shows that this bound can not be improved essentially. Rather, the possibility of quadratic growth is essentially connected with the purely lexicographic ordering. Thus, this ordering, though indispensable for elimination purposes (see /Trinks 78/), computationally may have disadvantages when compared with the total degree ordering (see Theorem 1).

REMARKS ABOUT THE PROOFS

The intuitions for the proofs of Theorem 1 and Theorem 2 can be obtained from a geometrical representation of the bivariate monomials in the plane ((x^i,y^j) is represented as the point with cartesian coordinates (i,j), see /Buchberger 79/) and a clear understanding of the Gröbner-basis algorithm, in particular the use of the "overlap-lemma". The formal verification of the geometrical and algorithmic intuitions, however, is tedious. In this paper we, therefore, give only a sketch of the proofs. We even must omit the precise definition of some auxiliary notions and rather rely on an intuitive understanding of some of the expressions used. All the formal details are contained in the technical report /Buchberger 82/.

PROOF OF THEOREM 1

1. Observation: From /Buchberger 79/, /Buchberger, Winkler 79/ we know that all the polynomials h occuring during the application of the Gröbner-basis algorithm to the input F (using total degree ordering) satisfy

$D(h) \leq M(F) + W(F)$, where

$M(F) := \max \{ D(LCM(LM(f_1), LM(f_2))) \ / \ f_1, f_2$ are "essential" w.r.t. F $\}$,

$W(F) := \min\{ E^1(LM(f)) \ / \ f \in F \} + \min\{ E^2(LM(f)) \ / \ f \in F \}$.

A pair of polynomials f_1, f_2 in F is "essential" iff the consideration of its "critical pair" (S-polynomial) can not be ruled out by the "overlap-lemma". W(F), the "width" of F, is a measure for the "area left over" by LM(F) (:= $\{LM(f) \ / \ f \in F \}$.

2. Observation: A tedious formal proof shows that M(F) can be represented in the following form

$M(F) = \max (MC(F), MAXD(F))$, where

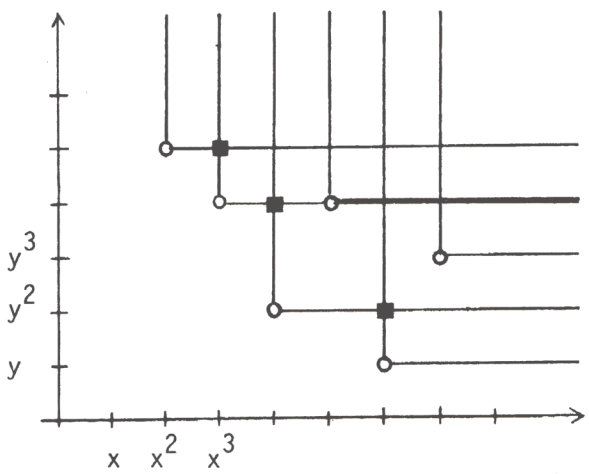
$MC(F) := \max \{ D(LCM(t_1, t_2)) \ /$

t_1, t_2 are leading monomials of polynomials in F,

t_1, t_2 lie on the "contour" of F and

no other such monomial lies "between" them $\}$.

Graphically,



In this picture we see the leading monomials x^6y, x^4y^2, x^3y^4, x^2y^5, x^7y^3, x^5y^4 of a set F of polynomials. Only the first four of these monomials lie on the "contour". The least common multiples of neighbouring monomials on the contour are marked by a black square. From every point corresponding to a leading monomial two lines are drawn (one upwards and one to the right) embracing the area corresponding to monomials which are multiples of the given monomial. MC(F) would be 8 in this example. (Formally, we call a finite set $T \subseteq [x,y]$ a "contour" iff there are no s, $t \in T$ such that $s \neq t$ and s divides t.)

3. Observation: One now proves $M(F) + W(F) \leq 2.MAXD(F)$. Essentially, the representation of M(F) given above and the definition of W(F) involve only the leading monomials of F. Also MAXD(F) = MAXD(LM(F)) (in the total degree ordering!). The proof of $M(F) + W(F) \leq 2.MAXD(F)$, therefore, can be carried out by establishing some lemmas on sets of bivariate monomials whose correctness and proof can easily be guessed from the geometrical interpretation. In more detail, we distinguish the cases $MC(F) \leq MAXD(F)$ and $MC(F) > MAXD(F)$.

In the first case we have

$$M(F) + W(F) = MAXD(F) + W(F) \overset{(1)}{\leq} MAXD(F) + MAXD(F) = 2.MAXD(F).$$

For (1) we need a lemma showing that, for arbitrary sets T of monomials, the width W(T) is ≤ the maximal degree MAXD(T). The proof of this lemma is easy.

In the second case we have

$$M(F) + W(F) = MC(F) + W(F) \overset{(2)}{=} MC(F) + WC(F) \overset{(3)}{\leq} 2.MAXDC(F) \leq 2.MAXD(F).$$

Here, WC(F) is the "width" of the set of leading monomials on the contour of LM(F) and MAXDC(F) is the maximal degree of these monomials. For (2) we need a lemma showing that the width of a set of monomials is determined by the monomials on the contour. The proof of this lemma is easy. For (3) we need a lemma showing that for contours T

$$MC(T) + WC(T) \leq 2.MAXD(T)$$

The proof of this lemma is a little more complicated, although still easy (draw a picture!)

P R O O F O F C O R O L L A R Y 1

One minimal Gröbner-basis G for F w.r.t. the total degree ordering may be obtained by, first, computing a Gröbner-basis H for F (applying the Gröbner-basis algorithm to F) and then canceling polynomials in H whose leading monomials are multiples of other polynomials in H (see /Buchberger 76b/). By Theorem 1 we have MAXD(H) ≤ 2.MAXD(F)-1 and, hence, MAXD(G) ≤ MAXD(H) ≤ 2.MAXD(F)-1. Furthermore, for arbitrary minimal Gröbner-bases G', G" for F: LM(G') = LM(G") (see /Buchberger 76b/) and, therefore MAXD(G') = MAXD(G"). Hence, MAXD(G) ≤ 2.MAXD(F)-1 for arbitrary minimal Gröbner-bases G for F.

P R O O F O F C O R O L L A R Y 2

The residue class ring V:= $K[x,y]/ID(F)$ is a vector space. If G is a Gröbner-basis for F w.r.t. an arbitrary admissible ordering R of monomials, then

$$B_R := \{ C(t) \in [x,y] \mid t \text{ is in normal form w.r.t. G (relative to R)} \},$$

where C(t) denotes the residue class of t w.r.t. ID(F), is a linearly independent basis for V (see /Buchberger 65, 70/). In case F is zero-dimensional, V has finite vector space dimension. Every linearly independent basis for V, then, has the same number of elements. In particular, all sets B_R (for the different admissible orderings R) have the same number of elements. Now, let G be a minimal Gröbner-basis for F w.r.t. the total degree ordering R_0 and let F be zero-dimensional. By Corollary 1,

(1) MAXD(G) ≤ 2.MAXD(F) =: d.

Among the polynomials of G there must be two polynomials p and q such that $LM(p) = x^k$ and $LM(q) = y^l$ (otherwise B_{R_0} would be infinite, see /Buchberger 70/). Because of (1) we have

(2) k, l ≤ d.

The elements of B_{R_0}, therefore, can only consist of such C(t), where t satisfies $E^1(t) < k$, $E^2(t) < l$. Hence,

(3) $|B_{R_0}| \leq k.l \leq d^2$.

Now we know that $|B_R| = |B_{R_0}|$ for arbitrary admissible orderings R and therefore

(4) $|B_R| \leq 4.MAXD(F)^2$.

Assume now that G is a minimal reduced Gröbner-basis for F w.r.t. an arbitrary admissible ordering R and assume, furthermore, that $g \in G$ is such that $e := D(g) > 4.MAXD(F)^2$. Let s be a monomial occuring in g such that $D(s)=e$ and $i_1 = E^1(s)$, $i_2 = E^2(s)$, i.e. $e = i_1 + i_2$. Then for all monomials $t \neq s$ dividing s, t must be in B_R (otherwise g would not be part of a minimal reduced Gröbner-basis). There are $(i_1+1).(i_2+1)-1 = (i_1+1).(e-i_1+1)-1 = i_1.(e-i_1)+e \geq e > 4.MAXD(F)^2$, such monomials, i.e. by (4), there are more than $|B_R|$ such monomials, a contradiction!

P R O O F O F P R O P O S I T I O N 1

For $d \geq 3$ take

$F := \{ \underline{xy}^{d-1}-x^d, \underline{y}^d \}$ (the leading monomials are underlined).

The Gröbner-basis algorithm yields

$G' := \{ \underline{xy}^{d-1}-x^d, \underline{y}^d, \underline{x^d y}, \underline{x}^{2d-1} \}$.

G' is a minimal Gröbner-basis for F, $MAXD(G') = 2d-1$. If G is some other Gröbner-basis for F, then LM(G) must contain all the underlined leading monomials in G' (see /Buchberger 76/). Hence, $MAXD(G) \geq MAXD(G') \geq 2d-1$ for arbitrary Gröbner-basis G for F. (For $d<2$ it is easy to construct suitable examples F).

P R O O F O F P R O P O S I T I O N 2

We take Lazard's example

$F := \{ \underline{y}^d-x, \underline{y}-x^d \}$.

The Gröbner-basis algorithm yields $G' := \{ \underline{y}-x^d, \underline{x}^{d^2}-x \}$. G' is a minimal Gröbner-basis for F, $MAXD(G') = t^2$. By the same argument as above $MAXD(G) \geq MAXD(G') \geq d^2$ for all other Gröbner-bases G for F.

P R O O F O F T H E O R E M 2

(1) The basic structure of the proof is:

$$|G| \overset{(2)}{=} |LM(G)| \overset{(3)}{\leq} MIND(LM(G))+1 \overset{(4)}{\leq} MIND(LM(F))+1$$

(2): G is minimal; (3): LM(G) is a contour; (4): G is a Gröbner-basis for F

(2) For minimal Gröbner-bases G we know (see /Buchberger 76b/):
$g_1, g_2 \in G, g_1 \neq g_2 \Rightarrow LM(g_1) \neq LM(g_2)$.

(3) In a minimal Gröbner-basis G, LM(G) is a contour (see /Buchberger 76b/).
We need the following
Lemma: Let $M \subseteq [x,y]$, $t_0 \in M$. Then: M is a contour $\Rightarrow |M| \leq D(t_0)+1$.
Using this lemma, we immediately obtain $|LM(G)| \leq MIND(LM(G))+1$.

(4) Since G is a Gröbner-basis, for all $f \in F$ there is a $g \in G$ such that LM(g) divides LM(f) (otherwise some $f \in F$ could not be reduced to 0 modulo G). Let f_0 be such that $D(LM(f_0)) = MIND(LM(F))$ and g_0 such that $LM(g_0)$ divides $LM(f_0)$. Then $MIND(LM(G)) \leq D(LM(g_0)) \leq D(LM(f_0)) = MIND(LM(F))$.

Again, the proof is reduced to the proof of a lemma on certain sets of monomials, see

(3). Using the definitions

$M_{lu} := \{ t \in M \mid E^1(t) < E^1(t_0),\ E^2(t) > E^2(t_0) \}$,

$M_{ul} := \{ t \in M \mid E^1(t) > E^1(t_0),\ E^2(t) < E_2(t_0) \}$,

it is clear that M is the disjoint union of M_{lu}, $\{t_0\}$, and M_{ul}. Hence,

$$\| M \| = \| M_{lu} \| + 1 + \| M_{ul} \| .$$

Now,

(1) $\| M_{lu} \| \leq E^1(t_0)$ and

(2) $\| M_{ul} \| \leq E^2(t_0)$.

From (1), (2) we get

$$\| M \| \leq E^1(t_0) + 1 + E^2(t_0) = D(t_0) + 1.$$

(1), (2) are easy, see /Buchberger 82/.

(Remark: The proof method used here is not applicable for n>3. For example, starting from $t_0 := x^2yz$ we can define arbitrarily large contours M with $t_0 \in M$:

$M := \{ x^2yz, x^t, x^{t-1}z, \ldots, xz^{t-1}, z^t \}$ $(t \geq 4)$

is a contour with t+2 elements.)

PROOF OF PROPOSITION 3

Take

$F := \{ x^d, x^{d-1}y, \ldots, xy^{d-1}, y^d \}$.

F is a minimal Gröbner-basis (w.r.t. every admissible ordering). For any other Gröbner-basis G for F we have LM(F) $\subset$ LM(G) (see /Buchberger 76b/). Hence,

$$\| G \| \geq \| LM(G) \| \geq \| LM(F) \| = \| F \| = d+1.$$

References

Bayer, D.A., 82:
The Division Algorithm and the Hilbert Scheme. Harvard University, Cambridge, Mass., Math. Dptmt: Ph.D. Thesis, June 1982.

Buchberger, B., 65:
An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German). Univ. of Innsbruck, Austria: Math. Inst., Ph.D. Thesis 1965.

Buchberger, B., 70:
An Algorithmical Criterion for the Sovability of Algebraic Systems of Equations (German). Aequationes mathematicae 4/3, 374-383 (1970).

Buchberger, B., 76a:
A Theoretical Basis for the Reduction of Polynomials to Canonical Form. ACM SIGSAM Bull. 10/3, 19-29 (1976).

Buchberger, B., 76b:
Some Properties of Gröbner-Bases for Polynomial Ideals. ACM SIGSAM Bull. 10/4, 19-24 (1976).

Buchberger, B., 79:
A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Bases. Proc. EUROSAM 1979, Marseille, Lect. Notes Comput. Sci. 72, 3-21 (1979).

Buchberger, B., 82:
Miscellaneous Results on Gröbner-Bases for Polynomial Ideals II. Technical Report, Dpmt. of Computer and Information Sciences, University of Delaware, to appear (1982).

Buchberger, B., Loos, R., 82:
Algebraic Simplification. In: Computer Algebra (B. Buchberger, G. Collins, R. Loos eds.), Springer, Wien-New York, 1982, 11-43.

Buchberger, B., Winkler, F., 79:
Miscellaneous Results on the Construction of Gröbner-Bases for Polynomial Ideals I. Technical Report Nr. 137, Mathematisches Institut, Universität Linz, Austria (1979).

Cardoza, E., Lipton, R., Meyer, A.R., 76:
Exponential Space Complete Problems for Petri Nets and Commutative Semigroups. Conf. Record of the 8th Annual ACM Symp. on Theory of Computing, 50-54 (1976).

Guiver, J.P., 82:
Contributions to Two-Dimensional System Theory. Univ. of Pittsburgh, Math. Depmt.: Ph.D. Thesis 1982.

Hermann, G., 26:
Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. 95, 736-788 (1926).

Lazard, D., 83:
Gröbner bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations. These proceedings.

Loos, R., 82:
Generalized Polynomial Remainder Sequences. In: Computer Algebra (B. Buchberger, G. Collins, R. Loos eds.), Springer, Wien-New York, 1982, 115-137.

Mayr, E.W., Meyer, A.R., 81:
The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals. M.I.T.: Lab. Comput. Sci. Rep. LCS/TM-199 (1981).

Pohst, M., Yun, D.Y.Y., 81:
On Solving Systems of Algebraic Equations Via Ideal Bases and Elimination Theory SYMSAC 1981, 206-211.

Sakata, S., 81:
On Determining the Independent Point Set for Doubly Periodic Arrays and Encoding Two-Dimensional Cyclic Codes and Their Duals. IEEE Trans. on Information Theory, IT-27/5, 556-565.

Schaller, S., 79:
Algorithmic Aspects of Polynomial Residue Class Rings. University of Wisconsin, Madison: Ph.D. Thesis, Comput. Sci. Tech. Rep. 370, 1979.

Seidenberg, A., 74:
Constructions in Algebra. Trans. AMS 197, 273-313 (1974).

Trinks, W., 78:
On B. Buchberger's method of Solving Algebraic Equations (German). J. Number Theory 10/4, 475-488 (1978).