Algorithms Seminar 2002–2004,
F. Chyzak (ed.), INRIA, (2005), pp. 85–92.

Available online at the URL
http://algo.inria.fr/seminars/.

On the Complexity of a Gröbner Basis Algorithm

Magali Bardet
Spaces Project, LIP6 and INRIA (France)

November 25, 2002

Summary by Bruno Salvy

Abstract

While the computation of Gröbner bases is known to be an EXPSPACE-complete problem, the generic behaviour of algorithms for their computation is much better. We study generic properties of Gröbner bases and analyse precisely the best algorithm currently known, F_5.

1. Gröbner Bases

Gröbner bases are a fundamental tool in computational algebra. They provide a multivariate generalization of Euclidean division and Euclid's algorithm for the gcd, as well as a generalization of Gaussian elimination to higher degrees. A very clear introduction is given in [3]; in this section we recall the basic definitions and properties.

1.1. **Definitions.** We consider polynomials in $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a field. The first step is to define a generalization of the univariate degree.

Definition 1. A *monomial ordering* is a total order on the set of monomials $\mathbf{x}^\alpha$ that is compatible with the product and such that 1 is the smallest monomial.

A monomial ordering can be given by a nonsingular real matrix A: the vectors of exponents are multiplied by the matrix and the resulting vectors are compared lexicographically. A technical condition encodes that 1 is minimal. Basic examples of orderings are: the lexicographic order, with identity matrix; the total degree order, also called *grevlex*, whose matrix has a first line of 1's above an antidiagonal matrix of -1's; the elimination orders whose matrix decompose diagonally into blocks of grevlex matrices. An order is said to *refine the degree* when the corresponding matrix has a fist line of 1's.

A polynomial can be expanded as a sum of terms, each term being a monomial times a coefficient. The *leading term* $\mathrm{LT}(p)$ of a polynomial p is then defined with respect to any monomial ordering.

The next step is to define an analogue of the Euclidean division. This process is called *reduction*, it depends on a given monomial ordering. Given a polynomial f and a set of polynomials $B = \{f_1, \ldots, f_s\}$, it returns a polynomial r such that

$$f = a_1 f_1 + \cdots + a_s f_s + r, \qquad \text{where } a_i \in \mathbb{K}[\mathbf{x}] \text{ for } i = 1, \ldots, s,$$

and the leading monomials of the f_i's do not divide that of r. One says that f *reduces* to r by B.

Definition 2. A *Gröbner basis* of an ideal $\mathfrak{I} \subset \mathbb{K}[\mathbf{x}]$ for a given monomial ordering is a finite set $B \subset \mathfrak{I}$ such that any $f \in \mathfrak{I}$ reduces to 0 by B. The basis is called *reduced* when the f_i's all have leading coefficient 1 and when none of the f_i's involves a monomial which reduces by $B \setminus \{f_i\}$.

An important consequence of the Hilbert basis theorem is the existence of Gröbner bases, thus of finite sets of generators, for all polynomial ideals. For a given monomial ordering, any ideal has a single reduced Gröbner basis.

1.2. **Examples.**

Example 1: gcd. In the univariate case, $\mathbb{K}[x]$ is principal, meaning that any ideal can be generated by a single generator. One possible choice for the generator is the gcd of its elements, which is also the only element of its reduced Gröbner basis.

Example 2: an intersection. Consider the system $\{f = x^2 + y^2 - 2, g = xy - 1\}$. These equations describe the intersection of a circle and a hyperbola, at points where they are tangent. The Gröbner basis for the ideal generated by $\{f, g\}$ for the lexicographic order with $x \prec y$ is $\{f_1 = (y^2 - 1)^2, f_2 = x - 2y + y^3\}$, while the Gröbner basis for the total degree order is $\{f, g, f_2\}$. Note that the multiplicities are preserved in this computation.

1.3. **Applications.**

Polynomial-system solving. Like in the previous example, using a lexicographic order yields a triangular system that can then be solved equation by equation.

Elimination. In Example 2, f_1 is a polynomial where the variable x has been eliminated between f and g. More generally, elimination can be computed using elimination orders. Geometrically, elimination corresponds to projection. It can be used to compute implicitizations, envelopes,....

Nullstellensatz. This answers the question: does p vanish on the common roots of $(f_1, \ldots, f_s)$? For instance, the polynomial $x - y$ vanishes on the common roots of f and g in our example. This is determined by computing a Gröbner basis of $(f_1, \ldots, f_s, 1 - tp)$ for a new variable t and observing that the result is $\{1\}$ (for any order).

Ideal membership. This answers the question: does p belong to the ideal generated by $(f_1, \ldots, f_s)$? This is decided by reducing p by a Gröbner basis and checking whether the result is 0 or not. Note that in our example, $x - y$ does not belong to the ideal, but $(x - y)^2$ does.

2. Worst-Case Complexities

The worst-case complexity of Gröbner bases has been the object of extensive studies. We refer to [8] for a survey.

2.1. **Polynomial-system solving is hard.** Since Gröbner bases can be used to solve polynomial systems, their complexity is at least that of polynomial-system solving. It turns out that it is not difficult to encode NP-complete problems into polynomial systems, which shows that the worst-case complexity cannot be expected to be too good. We give two examples.

Knapsack problem. Given $n + 1$ natural integers $(b_1, \ldots, b_n, c)$, the problem of solving the overdetermined system

$$\sum_{i=1}^{n} x_i b_i = c, \qquad x_i(1 - x_i) = 0, \quad i = 1, \ldots, n$$

is known as the 0-1 knapsack problem and has been proved to be NP-complete by Karp in 1972.

3-SAT. Given Boolean variables X_i and a number of Boolean clauses each with three literals, i.e., clauses of the form

$$Y_j \vee Y_k \vee Y_\ell, \qquad (Y_j, Y_k, Y_\ell) \in \{X_1, \ldots, X_n, \neg X_1, \ldots, \neg X_n\},$$

3-SAT is the problem of deciding whether there exists a Boolean assignment to the X_i's that makes all the clauses true simultaneously (SAT stands for satisfiability). This is cast into an overdetermined polynomial system using the correspondence $X_i \mapsto x_i$, $\neg X_i \mapsto 1 - x_i$, $X \vee Y \mapsto x + y - xy$, together with the equations $x_i(1 - x_i) = 0$. 3-SAT has been proved to be NP-complete by Cook in 1971.

2.2. **From bad to worse.** Another problem solved by Gröbner bases turns out to have a much worse complexity: Ideal membership is EXPSPACE-complete. This means that any problem that can be solved with exponential space can be reduced to Ideal membership. We recall that complexity classes are ordered as follows:

$$\text{P} \subset \text{NP} \subset \text{PSPACE} \subset \text{EXPTIME} \subset \text{EXPSPACE}.$$

One source of this difficulty comes from multiplicities. Indeed, the Nullstellensatz problem is "only" in PSPACE. Another progress is made if one restricts attention to polynomial systems with only finitely many solutions (these are called *0-dimensional*). The computation of their Gröbner bases is also in PSPACE. If one furthermore demands that after homogenizing the polynomials the system still has finitely many (projective) solutions, then the computation of Gröbner bases falls into NP.

For s equations of degree at most d in n variables, the arithmetic complexity bounds for Gröbner bases are $2^{2^{O(n)}}$ in general, $d^{O(n^2)}$ in the 0-dimensional case and $s^{O(1)}d^{O(n)}$ when the homogenized system has finitely many solutions. These bounds should be compared with Bézout's theorem, stating that the number of solutions, when finite, is bounded by d^n, and is exactly d^n in the homogeneous case.

This picture leads to natural questions that are (partially) adressed in this work:

> *Where are "random" systems? What is the exponent hidden in their $O()$ term? What about* overdetermined *systems having solutions?*

3. Generic Systems and the F_5 Algorithm

We do not deal directly with random systems, but rather with generic ones. We now briefly recall what *generic* means in an algebraic context and describe the generic behaviour of the F_5 algorithm, of which we introduce a simple matrix version.

3.1. Genericity.

Definition 3. A property of points in a space of dimension N is *generic* when it holds at all points except on an algebraic set of dimension at most $N - 1$. (Here, an algebraic set is defined as the zero set of a system of polynomials).

Example. Two univariate polynomials $A = a_0x^{d_1} + \cdots + a_{d_1}$ and $B = b_0x^{d_2} + \cdots + b_{d_2}$ of degree d_1 and d_2 are generically relatively prime. Indeed, the pair (A, B) can be viewed as a point in a space of dimension $d_1 + d_2 + 2$, with coordinates the a_i's and b_i's. Their gcd is one if and only if there does not exist nonzero polynomials u and v with $\deg u < d_2$ and $\deg v < d_1$ such that $uA + vB = 0$. This is a linear system in the coefficients of u and v that has nonzero solutions if and only if the

determinant of the following *Sylvester matrix* is 0:

$$\begin{pmatrix} a_0 & a_1 & \dots & & \\ & \ddots & & \ddots & \\ & & a_0 & \dots & \\ b_0 & b_1 & \dots & & \\ & \ddots & & \ddots & \\ & & b_0 & \dots & \end{pmatrix}.$$

This determinant is a polynomial in the coordinates of (A, B) (the *resultant* of A and B), which shows that the "bad" points belong to an algebraic set. In order to prove that this algebraic set had dimension smaller than that of the space, it is sufficient to exhibit one point outside of it. Thus the proof is concluded by observing that $X^{d_1} \wedge (X^{d_2} + 1) = 1$.

When the base field $\mathbb{K}$ is $\mathbb{C}$ or $\mathbb{R}$, generic properties hold outside a set of measure 0. When $\mathbb{K}$ is $\mathbb{Q}$ or a finite field with large enough characteristic, then quantitative probability bounds can be obtained in terms of the *degree* d of the algebraic set. For any $S \subset \mathbb{K}$, a point whose coordinates are chosen independently with uniform probability from S has probability at least $1 - d/|S|$ to lie outside of the algebraic set [9, 11]. Thus "generic" is related to "random" in a very precise way.

3.2. **Buchberger's algorithm.** In view of our definition of Gröbner bases above, a property (which could be taken as a definition) is that each element of the ideal has a leading monomial which is a multiple of that of one of the elements of the basis. Buchberger's algorithm consists in producing repeatedly new leading monomials using S-polynomials.

Definition 4. Let f and g be two polynomials and m be the lcm of their leading monomials, then the *S-polynomial* of f and g is

$$S(f, g) := \frac{m}{\mathrm{LT}(f)} f - \frac{m}{\mathrm{LT}(g)} g.$$

In the univariate case, $S(f, g)$ corresponds to the first step in the Euclidean division of f by g. Buchberger's algorithm then proceeds as follows:

Initialization: $B := \{\}$, $S := \{f_1, \dots, f_s\}$
while $S \neq \{\}$ **do**
– pick $f \in S$; $S := S \setminus \{f\}$; reduce f w.r.t. B and call g the resulting polynomial;
– **if** $g \neq 0$ **then** $S := S \cup_{b \in B} S(g, b)$; add g to B
return B

Buchberger proved in his thesis (in 1965) that this algorithm terminates and produces a Gröbner basis. One of the main difficulties with an actual implementation is that the reduction steps often produce 0 and a lot of time is wasted during these useless reductions. Thus, there are many strategies to help "pick" an element in S and predict useless reductions.

3.3. **Macaulay's matrix.** Another approach to polynomial-system solving was described by Macaulay in [7] where he generalized Sylvester's matrix to multivariate polynomials. The idea is to construct a matrix whose lines contain the multiples of the polynomials in the original system, the columns representing a basis of monomials up to a given degree. It was observed by Lazard [6] that for a large enough degree, ordering the columns according to a monomial ordering and performing row reduction without column pivoting on the matrix is equivalent to Buchberger's algorithm. In this correspondence, reductions to 0 correspond to lines that are linearly dependent upon the previous ones and the leading term of a polynomial is given by the leftmost nonzero entry in the corresponding line.

3.4. F_5 **algorithm.** From now on and except in the last section, we restrict attention to fields of coefficients with characteristic 0 and homogeneous polynomials. Given a system of polynomials $f_1, \ldots, f_s$, with $\deg f_i =: d_i$ and $d_1 \leq \cdots \leq d_s$, we denote by $\mathcal{F}_i$ the sub-system $f_1, \ldots, f_i$, by $I(\mathcal{F}_i)$ the ideal it generates and by $I_d(\mathcal{F}_i)$ the vector space of elements of $I(\mathcal{F}_i)$ with degree d.

Faugère's F_5 algorithm [5] avoids "useless" lines coming from the relations $f_i f_j = f_j f_i$. We now present a matrix version of this algorithm. The algorithm is incremental in d, then in i. It constructs submatrices $M_{d,i}$ of the Macaulay matrix and performs a row reduction on them. The incremental step from $i-1$ to i introduces the lines corresponding to mf_i for all monomials m of degree $D - d_i$ that *do not appear as leading monomials* in the reduced $M_{D-d_i,i-1}$. This matrix is then reduced and stored in $M_{d,i}$. The algorithm stops when a large enough D has been reached.

The number of linearly independent lines in the matrix $M_{d,s}$ is the number of linearly independent polynomials in $I_d(\mathcal{F}_s)$. Subtracting this from the number of monomials of degree d (the number of columns of the matrix), one gets a function $\mathrm{HF}(d)$ known as the *Hilbert function* of the ideal. For large enough d, this function is a polynomial in d (the *Hilbert polynomial*). The generating series $H(z) = \sum_{d \geq 0} \mathrm{HF}(d) z^d$ is called the *Hilbert series* and geometric information related to the algebraic set can be read off from it. The smallest value of d such that the Hilbert function is equal to the Hilbert polynomial is called the *index of regularity* $i_{\mathrm{reg}}(I)$ of the ideal. The homogeneity hypothesis makes the above quantities intrinsic to the ideal, that is, they do not depend on the chosen ordering.

3.5. **Regular systems.** A striking result of [5] is that for *regular systems*, F_5 does not perform any useless reduction to 0.

Geometrically, the system $\mathcal{F}_s$ is regular when for each $i = 1, \ldots, s$, the algebraic set defined by $\mathcal{F}_i$ has codimension i. Algebraically, this is expressed by the fact that f_i is not a zero-divisor in the quotient $\mathbb{A}_i := \mathbb{K}[\mathbf{x}]/I(\mathcal{F}_{i-1})$. In other words, if there exists g such that $gf_i = 0$ in $\mathbb{A}_i$, then $g \in I(\mathcal{F}_{i-1})$. It is not difficult to see that among systems of degrees $(d_1, \ldots, d_s)$, the regular ones are generic. Classical properties of regular systems are: *(i)* the system $\mathcal{F}_s$ is regular if and only if its Hilbert series is given by

$$H(z) = \frac{\prod_{i=1}^{s} (1 - z^{d_i})}{(1-z)^n}; \tag{1}$$

(ii) the index of regularity is

$$1 + \sum_{i=1}^{s} (d_i - 1); \tag{2}$$

(iii) after a generic linear change of variables, the highest degree of elements of a Gröbner basis for the *grevlex* order is the index of regularity.

3.6. **Semi-regular systems.** Regular systems have at most as many polynomials as variables. We now generalize this definition, before stating our main result on the complexity of F_5.

Definition 5. A 0-dimensional system $\mathcal{F}_s$ is *semi-regular* when $gf_i = 0$ in $\mathbb{A}_i$ and $\deg(gf_i) < i_{\mathrm{reg}}(I(\mathcal{F}_s))$ imply $g \in I(\mathcal{F}_{i-1})$, for $i = 1, \ldots, s$.

The system $\mathcal{F}_s$ is semi-regular if and only if its Hilbert series is $[H(z)]$. Here, the bracket of a power series f is a power series whose coefficients are 0 starting at the index of the first negative coefficient of f, and are those of f before. It follows from this series that 0-dimensional regular systems are semi-regular; this new definition also accommodates overdetermined systems. The following proposition gives a way to compute i_{reg} efficiently.

Proposition 1. *For a semi-regular system, the degree of regularity is the index of the first non-positive coefficient in the series* (1).

We are now in a position to state the main result of this work:

Theorem 1. [1] *For a semi-regular system,* (i) *there is no reduction to 0 in the algorithm F_5 for degrees smaller than i_{reg};* (ii) *the number of operations in $\mathbb{K}$ performed by F_5 is bounded by*

$$O\left(\binom{i_{reg}+n}{n}^{\omega}\right).$$

The exponent ω is the exponent in the complexity of matrix multiplication. The best known bound for general matrices in characteristic 0 is $\omega < 2.39$. We refer to [2, Chapters 15–16] for these questions.

4. Asymptotic Analysis

If $i_{\text{reg}} \sim \lambda n$ as $n \to \infty$, then the logarithm of the binomial in Theorem 1 is equivalent to $((1+\lambda)\ln(1+\lambda) - \lambda \ln \lambda)n$, while a "natural" size of the problem given by Bézout's theorem is $n \ln d$. We now describe how precise asymptotic information on i_{reg} can be obtained for semi-regular systems. Since the case when $s \leq n$ is given by (2), we concentrate on the overdetermined case.

4.1. **Principle.** The pth coefficient of the series (1) is given by the Cauchy integral representation

$$C(p) = \frac{1}{2i\pi} \oint \frac{\prod_{i=1}^{s}(1-z^{d_i})}{(1-z)^n} \frac{dz}{z^{p+1}}. \tag{3}$$

A preliminary analysis reveals that the degree of regularity grows roughly linearly with n. The analysis is then based on computing the asymptotic expansion of $C(\lambda n)$ for fixed λ, and then determining an asymptotic expansion $\lambda(n)$ that makes this behaviour vanish asymptotically.

4.2. **Few more equations than unknowns.** When $s = n + k$, with fixed k, it is convenient to rewrite the integral (3) as

$$C(p) = \frac{1}{2i\pi} \oint \underbrace{\prod_{i=1}^{s} \frac{1-z^{d_i}}{1-z} \frac{1}{z^{p+1}}}_{F_p(z)} (1-z)^k \, dz.$$

The coefficients can then be analyzed precisely using the *saddle-point method*. The integral is concentrated in the neighborhood of a saddle point ρ, characterized by $F_p'(\rho) = 0$. In the neighborhood of this point, the integrand behaves like $\exp(cz^2)$, and the next step of the method is to perform the quadratic change of variables $F_p(z) = F_p(\rho)\exp(-u^2)$. The integral is then approximated by

$$\frac{F_p(\rho)}{2i\pi} \int_{-\infty}^{\infty} e^{-u^2} (1-z(u))^k \frac{dz}{du} \, du. \tag{4}$$

The value of i_{reg} is obtained by choosing p such that this integral vanishes. At the first order, this is achieved by taking p such that $z(u) \sim \rho = 1$. Injecting this estimate in $F_p'(\rho) = 0$ gives the dominant term of the behaviour. The next one is obtained by renormalizing (4) in terms of the kth *Hermite polynomial* that satisfies

$$H_k(x) = \frac{2^k}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-u^2} (x+iu)^k \, du.$$

The final result is the following.

Theorem 2. *The degree of regularity of a semi-regular system of $s = n+k$ homogeneous polynomials of degree $d_1, \dots, d_{n+k}$ in n variables behaves asymptotically like*

$$\sum_{i=1}^{s} \frac{d_i - 1}{2} - \alpha_k \sqrt{\sum_{i=1}^{s} \frac{d_i^2 - 1}{6}} + O(1), \qquad n \to \infty,$$

where α_k is the largest zero of the kth Hermite polynomial.

It is actually possible to compute a full asymptotic expansion. For $s = n + 1$, $\alpha_1 = 0$ and the result found is in agreement with the exact result due to Szanto [10]. Also, from the practical point of view, this result shows in particular that linear equations do not increase the complexity.

4.3. **More equations.** The theorem above quantifies the gain in complexity obtained by adding more information in the form of extra equations. We now perform a similar analysis for systems with αn equations, $\alpha \geq 1$ being fixed.

In this case, the factor $(1 - z)^k$ is not a small perturbation any longer. The behaviour of the integrand changes qualitatively and the integral is then dominated by *two conjugate saddle points* $R_\pm$. The contributions of these saddle points to the integral are conjugate values whose sum does not vanish. This qualitative analysis reveals that a new phenomenon must occur for the integral to vanish: the index p must be such that *the saddle points coalesce*, giving rise to a double saddle point. This happens when both F' and F'' vanish and these equations are sufficient to give the first-order behaviour of i_{reg}, where now

$$F = \frac{\prod_{i=1}^{s} (1 - z^{d_i})}{(1 - z)^n} \frac{1}{z^{p+1}}.$$

A more precise analysis is achieved by capturing the coalescence of R_+ and R_- by means of a cubic change of variables $F(z) = P(u) = \exp(\frac{u^3}{3} + au^2 + c)$, where a and c are chosen so that the values of P at its saddle points 0 and $-2a$ is the same as that of F at R_- and R_+. The integral is then renormalized to

$$\frac{1}{2\pi} \int \exp P(u)\, du = \exp(c + \frac{2}{3}a^3)\, \mathrm{Ai}(a^2),$$

where Ai is the classical Airy function. The technicalities omitted here lead to the following result.

Theorem 3. *The degree of regularity of a semi-regular system of $s = \alpha n$ homogeneous polynomials of degree $d_1, \dots, d_{\alpha n}$ in n variables behaves asymptotically like*

$$\phi(\rho) n - a_1 \left(\frac{9}{2} \rho^2 \phi''(\rho) \right)^{1/3} n^{1/3} + \cdots, \qquad n \to \infty$$

where

$$\phi(z) = \frac{z}{1 - z} - \frac{1}{n} \sum_{i=1}^{s} \frac{d_i z^{d_i}}{1 - z^{d_i}},$$

ρ is the positive zero of $\phi'(z)$, and a_1 is the largest zero of the Airy function.

Moreover, in the neighbourhood of $\alpha = 1$, one gets

$$\phi(\rho) = \frac{1}{n} \sum_{i=1}^{s} \frac{d_i - 1}{2} - \sqrt{\sum_{i=1}^{s} \frac{d_i^2 - 1}{3n}} \sqrt{\alpha - 1} + \cdots$$

which is consistent with our previous result.

5. **Extensions**

5.1. **Affine case.** Up to now, we have considered only systems of homogeneous polynomials. When given nonhomogeneous polynomials, it is always possible to use an extra variable x_0 to make them homogeneous, choose a monomial order that makes this variable x_0 smaller than the other ones, compute the corresponding Gröbner basis, and set x_0 to 1 in the result. This gives the correct Gröbner basis and some of our analysis applies. However, in the overdetermined case, the homogenized system is not semi-regular (it is not 0-dimensional). It is therefore necessary to refine the analysis. This is done in [1].

5.2. **Positive characteristic.** An important application of Gröbner bases in cryptography involves overdertermined systems over the field $\mathbb{F}_2$ with two elements and moreover the solutions themselves are sought in $\mathbb{F}_2$. In that case, it is convenient to modify the algorithm F_5 so that "useless" lines coming from $f_i^2 = f_i$ are not computed. This results in an efficient algorithm that has been used to break a cryptographic challenge [4]. The analysis proceeds as before, the degree of regularity being now the first nonpositive coefficient in the series

$$\frac{(1+z)^n}{\prod_{i=1}^{s}(1+z^{d_i})}.$$

Bibliography

[1] Bardet (Magali), Faugère (Jean-Charles), and Salvy (Bruno). – On the complexity of Gröbner basis computation for regular and semi-regular systems. – 2005. In preparation.

[2] Bürgisser (Peter), Clausen (Michael), and Shokrollahi (M. Amin). – *Algebraic complexity theory*. – Springer-Verlag, Berlin, 1997, *Grundlehren der Mathematischen Wissenschaften*, vol. 315, xxiv+618p.

[3] Cox (David), Little (John), and O'Shea (Donal). – *Ideals, varieties, and algorithms*. – Springer-Verlag, New York, 1997, second edition, xiv+536p.

[4] Faugère (J.-C.) and Joux (A.). – Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using gröbner bases. In Boneh (D.) (editor), *Crypto'2003. Lecture Notes in Computer Science*, pp. 44–60. – Springer-Verlag, 2003.

[5] Faugère (Jean-Charles). – A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In Mora (Teo) (editor), *ISSAC 2002*. pp. 75–83. – ACM Press, 2002. Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, July 07–10, 2002, Université de Lille, France.

[6] Lazard (D.). – Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra*, pp. 146–156. – Springer, Berlin, 1983. Proceedings EUROCAL'83, London 1983.

[7] Macaulay (F. S.). – *The algebraic theory of modular systems*. – Cambridge University Press, Cambridge, 1994, *Cambridge Mathematical Library*, xxxii+112p. Revised reprint of the 1916 original.

[8] Mayr (Ernst W.). – Some complexity results for polynomial ideals. *Journal of Complexity*, vol. 13, n° 3, 1997, pp. 303–325.

[9] Schwartz (J. T.). – Fast probabilistic algorithms for verification of polynomial identities. *Journal of the Association for Computing Machinery*, vol. 27, n° 4, 1980, pp. 701–717.

[10] Szanto (Agnes). – Multivariate subresultants using Jouanolou's resultant matrices. *Journal of Pure and Applied Algebra*, 2004. – To appear.

[11] Zippel (Richard). – Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, pp. 216–226. – Springer, Berlin, 1979.