An Hilbert-Driven Strategy for Signature-Based Gröbner Basis Algorithms

Bruno Simões

Abstract Gröbner bases are special sets of polynomials with nice properties that can be used to solve many problems in mathematics, natural and technical sciences. Examples of applications in geometric and solid modeling include intersecting surfaces and curves, finding closest point on a curve or on a surface to the given point, finding equations for equidistant curves and surfaces to curves and surfaces defined in terms of polynomial equations, etc. One of the major limitations of the algorithms to compute Gröbner bases is their computation time. We present a new criterion to improve the performance of Gröbner bases algorithms, driven by polynomial signatures. This criterion relies on properties of the Hilbert series and on the information gathered about the syzygy module of the ideal, to discard useless critical pairs.

Keywords Gröbner basis · Hilbert series · Signature-based Strategy

Mathematics Subject Classification (2010) 08A40 · 11Cxx · 12-XX · 13P10 · 11D72

1 Introduction

Geometric and solid modeling have received great attention from the academic and industrial communities throughout the past four decades, and still they can intrigue us with their issues concerning the representation and manipulation of objects. Many of the geometric formulations in these two fields, such as curves and surfaces, can be represented in terms of polynomial equations. Such algebraic representations are also useful to describe their problems and to derive a solution e.g. boundary computations.

B. Simões (✉)
GraphiTech Foundation, Via alla Cascata, 56/c, 38123 Povo, Italy
e-mail: bruno.simoes@graphitech.it

R. De Amicis and G. Conti (eds.), *Future Vision and Trends on Shapes, Geometry and Algebra*, Springer Proceedings in Mathematics & Statistics 84,
DOI: 10.1007/978-1-4471-6461-6_2, © Springer-Verlag London 2014

The task of solving polynomial systems, especially of geometric constraints, is therefore a fundamental requirement in many applications e.g. mechanical assembly planning, tolerance analysis, constraint-based sketching and design, kinematic analysis of robots, and other mechanisms. An important class of problems involves finding the orientations, positions and dimensions of a set of geometric entities, which have to satisfy a set of geometric constraints. Earlier approaches to solve large constraint systems of this type have relied on semi-automatic procedures but automated approaches based on problem modeling have emerged recently in the literature, thereby opening doors to a larger set of unsolved problems and stressing the need for extremely efficient algorithms. The necessity of solving algebraic equations is also present in surface intersection algorithms, collision detection, ray tracing of curves and surfaces, manipulation of offsets of curves and surfaces [13] and geometric theorem proving [12, 15].

Techniques for solving non-linear polynomial systems can be categorized into geometric, symbolic and numeric methods. Symbolic methods based on algorithms for computing Gröbner bases or Resultants can be used for eliminating indeterminates and thereby reducing problems to a search of polynomials roots in the univariate case. Also, methods based on the computation of Gröbner bases have, for instance, other interesting properties such as a practical approach to check whenever a polynomial system has solutions or not. These techniques are an extraordinary example of how an idea used to solve one problem can become the key for solving a large variety of other problems, including in different areas. However, existing algorithms are known to be efficient only for polynomial systems of low degree. One of the major problems arises from the fact that finding the roots of univariate polynomials can be ill-conditioned for polynomials of degree greater than 14, as shown by Wilkinson [19]. As a result, the implementation of these algebraic methods with finite arithmetic precision is considered to be challenging as it constrains the performance of the resulting algorithms. Nevertheless, the prevailing viewpoint is that using algebraic methods in geometric and solid modeling usually leads to a better theoretical understanding of the problems. Therefore, they can be used to uncover new opportunities in the upcoming paradigms of smart geometry, but at the moment, their practical impact is still not clear.

Numeric methods can be sub-categorized into homotopy and iterative methods. The performance of the homotopy methods can be quite reasonable but it usually requires a solid theoretical background of the subject. Homotopy methods based on continuation techniques rely mostly on path-following techniques in the complex space. In theory, each path being followed should converge to a geometrically isolated solution but in practice we have to deal with additional issues, for example, the different paths being followed might not be geometrically isolated.

Iterative methods, e.g. Newton's method, are procedures to compute a sequence of improving approximate solutions to the problem. They are most suitable for local analysis and they work well when provided with a good initial guess of the solution. Though, supplying such a good guess in applications such as geometric constraint systems or intersections is not a trivial task. Recently, iterative methods based on interval arithmetic have received a considerable amount of attention in computer

graphics and geometric modeling. The resulting algorithms are robust, though their convergence can sometimes be relatively slow.

This paper is devoted to efficient computations of Gröbner basis, with a particular emphasis on signature-based attempts. Our main result is based upon the idea that we can extend signature-based attempts by using the properties of the Hilbert series, and improve its computational efficiency.

The structure of this paper is the following. In Sect. 2, we recall the basic concepts and terminology. In Sect. 3, we show that improvements to the state-of-the-art are still possible by taking advantage of the data collected by signature-based techniques. In Sect. 4, we benchmark some of the fastest algorithms to compute a Gröbner basis against a standard database of examples, and we assess the performance of our algorithm. We shall see that it provides good results. We conclude this paper with a short list of remarks and future directions regarding the current results.

2 The Theory of Gröbner Bases

As often happens, the invention of the theory of Gröbner bases can be associated to several mathematicians. In our view, the major step was taken by Bruno Buchberger during his PhD thesis [3]. First, he formulated the concept of Gröbner bases, extending a suggestion of his advisor Wolfgang Gröbner. Such influence is also acknowledged with his terminology. Lastly, he found an algorithm to compute them, as well as a proof for the fundamental theorem on which the correctness and termination of the algorithm hinges.

This section attempts to present in a self-contained manner the basic facts about the theory of Gröbner basis. We start with a short introduction to polynomial rings and their ideals. Then, we bring the reader into the realm of orderings. Term orderings are an important tool because they enable us to write polynomials in a well-defined way that can then be implemented on a computer. After ordering terms in polynomials or tuples of polynomials completely, their leading terms can be singled out and then used to build leading term ideals and modules, which are conceptually much simpler to handle. Then we review the theory of Hilbert series, which is one of the concepts required to fully understand the proposed criterion. Lastly, we introduce the theory of Gröbner bases and the signature-based strategy.

For a more detailed introduction on commutative algebra we refer the reader to [1, 6]. Good books covering those topics with a more detailed introduction to the theory of Gröbner bases and a stronger emphasis on computational aspects are, for example, [14, 15]. Most of the proofs given in this section are either easy or can be found in any introductory book about commutative or computational algebra (for example in the ones mentioned above). We focus ourselves on the theory of Gröbner bases, thus we provide only proofs if they are short, beautiful, and give some deeper insight on the topics covered, otherwise we provide only references.

2.1 Theoretical Foundations

We assume that the reader has some basic knowledge of basic algebra, but we do not think it is harmful if we recall some fundamental definitions. Also, readers familiar with this topic may want to skim this section for notation and terminology.

Let $\mathrm{P} = R[x_1, \ldots, x_n]$ be a polynomial ring over a ring R that consists of the multivariate polynomials of the form:

$$\sum a_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$$

where $a_{\alpha_1,\ldots,\alpha_n} \in R$ and α_i are non-negative integers. Then we have the following definition.

Definition 1 A *term* (or a *power product*) is a product of n indeterminates, each raised to the power of a non-negative integer. It can be written concisely as

$$x^{\alpha} = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \tag{1}$$

where α is the coordinate vector $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$.

Definition 2 The *total degree* of a term x^{α} is simply defined as $\deg(x^{\alpha}) = |\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$. The degree of x^{α} in any indeterminate x_i is $\deg_{x_i}(x^{\alpha}) = \alpha_i$.

We denote the set of all terms involving the indeterminates $x_1, \ldots, x_n$ by the expression $\mathbb{T}^n$. Also, we say that a term $p = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \in \mathbb{T}^n$ is *divisible* by $q = x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathbb{T}^n$ if $\beta_i \leq \alpha_i, \ \forall\ 1 \leq i \leq n$. The definition of the least common multiples and the greatest common divisors of two terms is the following.

Definition 3 Let $\mathrm{P} = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K. Let $t_1 = \prod_{i=1}^{n} x_i^{\alpha_i} \in \mathbb{T}^n$ and $t_2 = \prod_{i=1}^{n} x_i^{\beta_i} \in \mathbb{T}^n$ be two terms. Then we define

$$\mathsf{lcm}(t_1, t_2) = \prod_{i=1}^{n} x_i^{\max\{\alpha_i, \beta_i\}} \quad \text{and} \quad \gcd(t_1, t_2) = \prod_{i=1}^{n} x_i^{\min\{\alpha_i, \beta_i\}}$$

as the *least common multiple* of t_1 and t_2, and the *greatest common divisor* of t_1 and t_2, respectively.

We say that t_1 and t_2 are *co-prime* or relatively prime if $\gcd(t_1, t_2) = 1$.

Definition 4 The *support* of a polynomial f is the set $\mathrm{Supp}(f) = \{x^{\alpha} \in \mathbb{T}^n \mid \mathrm{coef}(c_{\alpha} x^{\alpha}) \neq 0\}$. A polynomial f is said to be *homogeneous of degree d* if all terms have the same total degree d.

Another important definition is the one called *monomial*.

Definition 5 A *monomial* is an element of P of the form $m = ct$, where $c \in R$ is its *coefficient* and $t \in \mathbb{T}^n$ is its *term*. The *total degree* of the monomial m is simply the total degree of t.

Next we show that ideals generated by terms are finitely generated. The importance of such result is self-evident in the next sections. However, it should be already clear that statements about "finiteness" are extremely valuable from a computational point of view.

Definition 6 A *monoid* $(\Gamma, +)$ is a set Γ together with an associative operation + on it, such that there exists an identity. A monoid whose operation is commutative is called a *commutative monoid*.

In this paper, the operations are always considered to be commutative, and we shall use the term "monoid" to denote a commutative monoid.

Definition 7 Let $(\Gamma, \cdot)$ be a monoid. A non-empty subset $\Delta \subseteq \Gamma$ is called a *monomial ideal* in Γ if the following property holds: $\Delta \cdot \Gamma \subseteq \Delta$.

Proposition 1 *The following conditions are equivalent for a monoid* $(\Gamma, \cdot)$.

1. *Every monomial ideal in* Γ *is finitely generated.*
2. *Every ascending chain* $\Delta_1 \subseteq \Delta_2 \subseteq \ldots$ *of monomial ideals in* Γ *is eventually stationary.*
3. *Every non-empty set of monomial ideals in* Γ *has a maximal element with respect to inclusion.*

The monoid Γ *is said to be Noetherian if these conditions are satisfied. The same claim is valid for the monoid* $(\mathbb{N}^n, +)$.

Proof See, for example, Sect. 1.3 in [14].

This proposition provides an important finiteness condition for ideals in polynomial rings.

Corollary 1 (Dickson's Lemma) *Every set of terms* $X \subseteq \mathbb{T}^n$ *contains a finite subset* $Y \subseteq X$ *such that each* $p \in X$ *is a multiple of some term in* Y.

Proof Let log:$\mathbb{T}^n \to \mathbb{N}^n$ be the map given by $x_1^{\alpha} \ldots x_n^{\alpha} \to (\alpha_1, \ldots, \alpha_n)$. Such map is clearly an isomorphism of monoids. Hence, the monomial ideal $(\log(t_1), \log(t_2), \ldots) \subseteq \mathbb{N}^n$ is finitely generated by the previous proposition, and there exists a number $i > 0$ such that this monomial ideal is generated by $\log(t_1), \ldots, \log(t_i)$ where $t_i \in \mathbb{T}^n$. Therefore, we have that the set of terms $\{t_1, \ldots, t_i\}$ generates the monomial ideal $(\log(t_1), \log(t_2), \ldots) \subseteq \mathbb{T}^n$.

The generalization of the Dickson's Lemma is given by the following theorem.

Theorem 1 (Structure Theorem for Monomial Modules) *Let $M \subseteq \mathrm{P}^r$ be a monomial module.*

1. *The module M is finitely generated. That is, $M = \langle t_1 e_{\alpha_1}, \ldots, t_s e_{\alpha_s} \rangle$, where s is finite, $t_1, \ldots, t_s \in \mathbb{T}^n$ and $\alpha_i \in \{1, \ldots, r\} \subset \mathbb{N}$*
2. *There are monomial ideals $I_1, \ldots, I_r \subseteq \mathrm{P}$ such that M is of the form $M \cong \oplus_{i=1}^r I_i e_i$.*

Proof Assume $B \subseteq \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ to be a system of generators of the monomial module M. Let $B_i = \{t \mid te_i \in B\} \subseteq \mathbb{T}^n$ be a set of terms with $1 \leq i \leq r$. By Dickson's Lemma, the monomial ideal $I_i = (B_i)$ has a finite systems of generators $S_i \subseteq B_i$. Clearly, the P-module M is then generated by $S_1 e_1 \cup \ldots \cup S_r e_r \subseteq \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. This proves the finiteness and also the claim that $M = \sum_{i=1}^r I_i e_i$. The fact that this sum is direct follows from $M \subseteq \oplus_{i=1}^r \mathrm{P} e_i$.

There is an analogy between Theorem (1.1) and Proposition (1.1) that implies that the analogue of Proposition (1.2) holds for monomial modules as well.

Corollary 2 *Every ascending chain of monomial submodules of P^r is eventually stationary.*

Proof Let $M_1 \subset M_2 \subset \ldots$ be a strictly ascending chain of monomial submodules of P^r, and assume that such chain exists. Then we have that $\langle t_1, \ldots, t_i \rangle \subseteq M_i$ for all $i \geq 1$ because these are all modules generated by terms. Assume that we can find for every $i \geq 1$ a $i + 1$ such that $t_{i+1} \notin \langle t_1, \ldots, t_i \rangle$. Then the monomial submodule $\langle t_1, t_2, \ldots \rangle$ of P^r is not finitely generated. This represents a contradiction to Theorem 1.

Lastly, we shall see the uniqueness for systems of generators of monomial modules.

Proposition 2 *Assume $M \subseteq P^r$ to be a monomial submodule. Then there exists a unique minimal element in the set of all systems of generators of M with respect to inclusion. We denote such set as the minimal monomial system of generators of M.*

Proof See, for example, Sect. 1.3 in [14].

One of the questions that remains unanswered is: in how many different ways can we write a polynomial $p \in \mathrm{P}$? Clearly, the terms in the support of a polynomial can be ordered by decreasing or increasing degree. However, that is not enough since different terms can have the same degree. Our next task is to equip them with a certain additional property called a term ordering, which allow us to define them uniquely. This fundamental property is the key for the finiteness of most algorithms we shall encounter later.

In the univariate case the operation is straightforward because we can define $x^a \succ x^b$ as being true if and only if $a > b$. But for the multivariate case we need to find a new relation that is capable of providing such uniqueness and that is consistent with polynomial multiplication.

Definition 8 A *total ordering* is a set S and a relation on that set that satisfies the conditions for a partial ordering plus an additional condition known as the comparability condition. A relation $\leq$ is said to be a total ordering on a set S if the following properties hold.

- Reflexivity: $a \leq a$ for all $a \in S$.
- Antisymmetry: $a \leq b$ and $b \leq a$ implies $a = b$.
- Transitivity: $a \leq b$ and $b \leq c$ implies $a \leq c$.
- Comparability (trichotomy law): For any $a, b \in S$, either $a < b$, $a > b$ or $b = a$.

The first three axioms define only a *partial ordering*, whereas the addition of the trichotomy law defines a total ordering. Every totally ordered set that is finite is well ordered.

Definition 9 A *well-ordering* on a given set is a total ordering such that any non-empty subset has a smallest element w.r.t $\succ$.

Definition 10 An *ordering* $\succ$ is an *admissible term ordering* if it satisfies three conditions:

1. It is a total ordering on the set of all terms $\mathbb{T}^n$.
2. It is multiplicative; i.e., $x^a \succ x^b$ implies $x^{a+c} \succ x^{b+c}$ for all $a, b, c \in \mathbb{N}^n$.
3. It is a well-ordering, namely, the constant term is the smallest.

Term orderings have other useful properties. Once we fix an ordering, every polynomial f has a unique leading term. Moreover, that unique leading term is the largest term in the polynomial (w.r.t. that term ordering) with a nonzero coefficient in the expansion of f.

Definition 11 Let $f = c_\alpha x^\alpha + \sum c_k x^{\beta_k} \in \mathrm{P}$ such that $x^\alpha \succ x^{\beta_k}$ and $c_\alpha \neq 0$. Then:

- $\mathsf{LC}_\succ(f) = c_\alpha$ is the *leading coefficient* of f.
- $\mathsf{LT}_\succ(f) = x^\alpha$ is the *leading term* of f.
- $\mathsf{LM}_\succ(f) = \mathsf{LC}_\succ(f) * \mathsf{LT}_\succ(f) = c_\alpha x^\alpha$ is the *leading monomial* of f.

Up to now, we saw how to define polynomials uniquely in P. Next we extend the definition of term orderings on polynomial rings to the one on monomial modules. There are two reasons that can justify our interest in such orderings. First we are interested in the computation of Gröbner bases of modules. Lastly, signature-based algorithms work with elements of such modules. Hence, we start with a review of the Definition 1.

Definition 12 Assume M to be a free P-module of rank r with canonical basis elements e_i. A *module term* in M is an element of the form $t = x^\alpha e_i$ where x^α is a term in P. The set of all module terms is denoted $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$.

The set of all module terms $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ is obviously a disjoint union of r copies of $\mathbb{T}^n$, where e_1, ..., e_r merely indicate the copy we are considering.

Definition 13 Let $x^\alpha e_i$ and $x^\beta e_j$ be two module terms in $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. We say that $x^\alpha e_i$ divides $x^\beta e_j$ if and only if $i = j$ and $x^\alpha \mid x^\beta$, for all $x^\alpha, x^\beta \in \mathbb{T}^n$. We use $x^\alpha e_i \mid x^\beta e_j$ as a shorthand notation for this operation.

Before we move into the realms of module orderings, we shall revise a few other properties of module terms.

Definition 14 Let M to be a free P-module of rank r with canonical basis elements e_i, and R be a ring. The expression term shall denote a module term if no confusion arises. Hence, it can be said

1. A *monomial* $m = ct$ in M is a term $t \in M$ times a coefficient $c \in R$.
2. The *index of a term* $t = x^\alpha e_i$ is denoted $index(t) = i$.
3. Computing the *degree of a term* $m = x^\alpha e_i$ can be reduced to the one of the term $x^\alpha \in \mathrm{P}$, as defined in Definition 4: $\deg(m) := \deg(x^\alpha) = \sum_{i=1}^{n} \alpha_i$.

We can write a element $f \in M$ as a sum of monomials

$$f = \sum_{i=1}^{r} \left(\sum_{\alpha \in \mathbb{N}^n}^{\text{finite}} c_\alpha x^\alpha \right) e_i$$

such that $c_\alpha \in R$ and $x^\alpha \in \mathbb{T}^n$. However, this representation is again unique only up to the order of the monomials. Thus, a term ordering on M is also required. Naturally, this is just a generalization of a term ordering on P that takes into account the canonical basis elements e_i,

Definition 15 Let $\succ_\sigma$ be a term ordering on P and $M = \oplus_{i=1}^{r} = \mathrm{P}e_i$ a free P-module of rank r with canonical basis elements e_i. A *module term ordering* $\succ$ is a compatible total ordering on the set of all terms of M such that $x^\alpha e_j \succ x^\beta e_j \Rightarrow x^\gamma x^\alpha e_i \succ x^\gamma x^\beta e_j$ and $x^\alpha \succ_\sigma x^\beta \Rightarrow x^\alpha e_i \succ x^\beta e_i$, for all $\alpha, \beta, \gamma \in \mathbb{N}^n$ and $i, j \in \{1, \ldots, r\}$.

Clearly, a term ordering on the polynomial ring P can also be understood as a module term ordering on the module $\mathrm{P} \cong \mathrm{P}e_1$. Therefore, the last definition is just a generalization of the Definition 10.

Definition 16 Given a module ordering $\succ$ on M, every element $f \in M$ can be uniquely represented by $f = c_\alpha x^\alpha e_i + f'$, and for all nonzero terms $c_\beta x^\beta e_j$ of f' it holds that $x^\alpha e_i \succ x^\beta e_j$.

Once we fix a module ordering, every polynomial f has the following properties.

Definition 17 Let f be a polynomial in a module M.

- the leading term of f is $\mathsf{LT}_\succ(f) = x^\alpha e_i$,
- the leading coefficient of f is $\mathsf{LC}_\succ(f) = c_\alpha$,
- the leading monomial of f is $\mathsf{LM}_\succ(f) = c_\alpha x^\alpha e_i$,

Likewise in the polynomial case, we shall always equip a module M with a module term ordering $\succ$. Hence, the use of the notation M implies also the use of a module term ordering on M.

Next we review a few more properties concerning ideals and modules such as the relation they have with their leading term ideals and modules. These properties will come in handy once we need an answer to questions like: Let I be an ideal in a polynomial ring $\mathrm{P} = K[x_1, \ldots, x_n]$ over a field K. Obviously, the residue class ring P/I can be viewed as a K-vector space. So, is it possible to exhibit an explicit basis?

We shall see that with the help of leading terms, the Macaulay's Basis Theorem yields a noteworthy answer to this question. This theorem is based on the assumption that the module ordering is a term ordering and the base ring is a field. That underlines for the first time the theoretical importance of term orderings.

Definition 18 Let $M \subseteq \mathrm{P}^r$ be a P-submodule and $\succ$ fixed term ordering.

1. The module $\mathsf{LT}_\succ(M) = \langle \mathsf{LT}_\succ(m) \mid m \in M \backslash \{0\} \rangle$ is said to be the *leading term module* of M with respect to $\succ$.
2. If $M \subseteq \mathrm{P}$ then we say that $\mathsf{LT}_\succ(M) \subseteq \mathrm{P}$ is the *leading term ideal* generated by the leading terms of all the elements in M with respect to $\succ$. A term x^α is called *standard* if it does not belong to $\mathsf{LT}_\succ(M)$.

Assume that $m_1, \ldots, m_s \in \mathrm{P}^r$ are non-zero vectors and that $M = \langle m_1, \ldots, m_s \rangle \subseteq \mathrm{P}^r$ is the submodule generated by them. Then the inclusion given by $\langle \mathsf{LT}_\succ(m_1), \ldots, \mathsf{LT}_\succ(m_s) \rangle \subseteq \mathsf{LT}_\succ(M)$ holds.

Definition 19 Let $M \subseteq \mathrm{P}^r$ be a module. We denoted by $\mathsf{LT}_\succ\{M\}$ the *monomodule* $\{\mathsf{LT}_\succ(m) \mid m \in M \backslash \{0\}\} \subseteq \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$.

Theorem 2 (Macaulay's Basis Theorem) *Let* $\mathrm{P} = K[x_1, \ldots, x_n]$ *be a polynomial ring over* K. *Let* $M \subseteq \mathrm{P}^r$ *be a* P*-submodule,* $\succ$ *a term ordering on* $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, *and* B *the set of all terms in* $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle \backslash \mathsf{LT}_\succ\{M\}$. *Then the residue classes of the elements of* B *form a basis of the* K*-vector space* P^r/M.

Proof See, for example, Sect. 1.5 in [14].

This theorem shows how to compute effectively P^r/M. First we need to compute $\mathsf{LT}_\succ(M)$ for a term ordering $\succ$, and then we represent each element as a unique and finite linear combination of the residue classes of the elements of $B = \mathbb{T}^n \langle e_1, \ldots, e_r \rangle \backslash \mathsf{LT}_\succ\{M\}$.

We have not seen yet how to compute efficiently $\mathsf{LT}_\succ(M)$. However, this is one of the subjects of the Sect. 2.2. Next, we recall the notion of homogeneous ideals and graded submodules.

Definition 20 The ring R is said to be a *Γ-graded ring* if there exist abelian subgroups R_γ, and

1. $R = \oplus_{\gamma \in \Gamma} R_\gamma$, and
2. for all $\gamma, \gamma' \in \Gamma$ it holds that $R_\gamma R_{\gamma'} \subseteq R_{\gamma+\gamma'}$.

We say that elements $r \in R_\gamma$ are *homogeneous of degree* γ and have all $\deg(r) = \gamma$. Additionally, the element 0 is a homogeneous element of R of every degree. Lastly, the decomposition of every element into its homogeneous components is unique. That property is a consequence of the direct sum in the Definition 20.

A natural way to extend the Definition 20 to R-modules is to use again the monoid Γ as the set of possible degrees. However doing so is not sufficiently general. The following definition underlines for now how to proceed.

Definition 21 Let R be a Γ-graded ring and $(\Omega, *)$ a Γ-monomodule. We say that M is a *Ω-graded R-module* if there exist abelian subgroups M_ω such that

1. $M = \oplus_{\omega \in \Omega} M_\omega$, and
2. for all $\gamma \in \Gamma, \omega \in \Omega$ it holds that $R_\gamma M_\omega \subseteq M_{\gamma * \omega}$.

Additionally, we say that a R-submodule N of M is a *Ω-graded R-submodule* of M if $N = \oplus_{\omega \in \Omega}(N \cap M_\omega)$, and that a Γ-graded submodule of R is a Γ-homogeneous ideal of R. For the sake of simplicity we call it *homogeneous ideal* of R if Γ is obvious from the context.

The following proposition and its corollary are very handy, especially for practical purposes. They allow us to quickly prove that some submodule is Ω-graded by exhibiting a homogeneous system of generators, and at the same time it give us a convenient representation of arbitrary homogeneous elements in terms of those homogeneous generators.

Proposition 3 *Let $N \subseteq M$ be a R-submodule and $N_\omega = N \cap M_\omega$ for all $\omega \in \Omega$. Then the following three conditions are equivalent.*

1. $N = \oplus_{\omega \in \Omega} N_\omega$.
2. *Let $n = \sum_{\omega \in \Omega} n_\omega$ be the decomposition of $n \in N$ into its homogeneous components, then $n_\omega \in N$ for all $\omega \in \Omega$.*
3. *There is a system of generators of N which consists only of homogeneous elements.*

Proof See, for example, Sect. 1.7 in [14].

Corollary 3 *Let $N \subseteq M$ be a Ω-graded R-submodule and $\{n_\gamma \mid \gamma \in \Gamma\}$ be a set of homogeneous generators of N. Suppose that the right-cancellation law holds in Ω and that $\omega \in \Omega$. Then we can say that every element $n \in N_\omega$ has a representation $n = \sum_{\gamma \in \Gamma} r_\gamma n_\gamma$ such that $r_\gamma \in R$ are homogeneous elements and $\deg(r_\gamma) * \deg(n_\gamma) = \omega$ for every $\gamma \in \Gamma$.*

Proof See, for example, Sect. 1.7 in [14].

Next we give a definition of homogenization and dehomogenization of polynomials.

Definition 22 Given any polynomial $p \in \mathrm{P} = R[x_1, \ldots, x_n]$ and an extra indeterminate x_0, we say that $p^h = x_0^{\deg(p)} p\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in \mathrm{P}$ denotes the homogenization of p with respect to x_0. Hence, p^h is homogeneous polynomial of degree $\deg(p)$.

Definition 23 Conversely, for every homogeneous polynomial $\mathrm{P} \in R[x_0, \ldots, x_n]$ there exists a dehomogenization with respect to x_0 defined by $\mathrm{P}^{deh} = \mathrm{P}(1, x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$.

Let us recall now the definition of Hilbert functions and Hilbert series. These are two concepts that have an essential role throughout the next section.

Let $P = K[x_0, \ldots, x_n]$ be a graded polynomial ring, where each x_i is a homogeneous component of degree one.

Definition 24 The *Hilbert function* of the finitely generated P-module M is defined by the following map

$$\begin{aligned} \mathsf{HF}(M, d) : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ v &\mapsto \dim(M_d) \end{aligned}$$

where M_d is the degree d part of M.

Definition 25 The *Hilbert polynomial* $q(d)$ is the unique polynomial in d such that the equivalence $q(d) = \mathsf{HF}(M, d)$ holds for all $d >> 0$. Let S be the support of M. Then, the Hilbert polynomial $q(d)$ has the following form $q(d) = \frac{i}{r!}d^r + \cdots$ where i is the degree of S and r is its dimension.

A compact representation of the dimensions of the homogeneous components is given by introducing the Hilbert series. This representation of the Hilbert function is desirable if we want to manipulate it on a computer. From now we shall use "computing the Hilbert function" and "computing the Hilbert series" interchangeably.

Definition 26 Let $M = \oplus_{n \geq 0} M_n$ be a finitely generated P-module M. The *Hilbert series* of M is defined by the generating function

$$\mathsf{HS}(M, t) = \sum_{d=-\infty}^{\infty} \mathsf{HF}(M, d) t^d$$

where $g(t)$ is a Laurent polynomial in t.

We conclude this introduction with a noteworthy theorem, which claims that, for a polynomial ring P and a homogeneous ideal I, the Hilbert series of P/I has always the form of a rational function.

Theorem 3 (Hilbert, Serre) *Given a graded polynomial ring* $\mathrm{P} = K[x_0, \ldots, x_n]$ *and a graded ideal* I *in* P, *then the Hilbert series of* P/I *can be expressed as*

$$\mathsf{HS}(P/I, t) = \frac{g(t)}{(1-t)^{n+1}}$$

where $g(t)$ *is a polynomial in* t *with integer coefficients. Moreover, the following relation holds,*

$$\mathsf{HS}(P/I, t) = \mathsf{HS}(P, t) - \mathsf{HS}(I, t)$$

Proof See, for example, Sect. 5.2 in [15].

2.2 Gröbner Bases Theory

Let us assume for now that we want to compute $\mathsf{LT}_{\succ}(I)$ for a given ideal $I = \langle f_1, \ldots, f_s \rangle$. It is worth mentioning that a direct computation of $\mathsf{LT}_{\succ}(I)$ is impossible because it requires the computation of the leading term of each polynomial in the ideal I. As an alternative, we might want to consider the monomial ideal generated by the leading terms of the generators,

$$\langle \mathsf{LT}_{\succ}(f_1), \ldots, \mathsf{LT}_{\succ}(f_s) \rangle \subseteq \mathsf{LT}_{\succ}(I)$$

At this point, one might ask: is it is possible to produce a set of generators for which these two ideals are the same? The answer to this question is exactly the notion of a Gröbner basis.

Definition 27 Given an ideal $I \subseteq \mathrm{P}$ and a fixed term ordering $\succ$. A finite set of polynomials $\mathscr{G} \subseteq I \backslash \{0\}$ is a *Gröbner basis* of $I \backslash \{0\}$ if and only if the leading term of every element of I is divisible by one term in the set $\mathscr{G}$,

$$\langle \mathsf{LT}_{\succ}(g) \mid g \in \mathscr{G} \rangle = \mathsf{LT}_{\succ}(I)$$

Henceforth we have all the tools that are necessary to check if a set of polynomials is a Gröbner basis for some ideal I. Let us see an example of how to do it:

Example 1 Let $\succ_{\mathrm{Lex}}$ be a fixed term ordering and $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 - x \rangle$ an ideal in P. Then we have that $\langle f_1, f_2 \rangle$ is not a Gröbner basis for I. Although we have $x^2 = yf_1 - xf_2 \Rightarrow x^2 \in I \Rightarrow x^2 = \mathsf{LT}_{\succ}(x^2) \in \langle \mathsf{LT}_{\succ}(I) \rangle$, we also have that x^2 is not divisible by $\mathsf{LT}_{\succ}(f_1) = x^3$ or by $\mathsf{LT}_{\succ}(f_2) = x^2y$, which means that $x^2 \notin \langle \mathsf{LT}_{\succ}(f_1), \mathsf{LT}_{\succ}(f_2) \rangle$.

Up to now, we saw that Gröbner bases are not defined uniquely, e.g, the Definition 27 does not require a Gröbner basis to be minimal. Therefore, one can add redundant

elements of I to $\mathcal{G}$ and get another Gröbner basis. This means that any finite subset of I that contains a Gröbner basis for I is also a Gröbner basis. Nevertheless, this lack of uniqueness can be solved by readjusting the definition of Gröbner basis into something called reduced Gröbner bases.

Definition 28 A Gröbner basis $\mathcal{G}$ is a *reduced Gröbner basis* if

1. for each $g \in \mathcal{G}$, the coefficient $\mathsf{LC}_{\succ}(g)$ is 1,
2. $\mathsf{LT}_{\succ}(I)$ is minimally generated by the set $\{\mathsf{LT}_{\succ}(g) : g \in \mathcal{G}\}$, and
3. no trailing term of any $g \in \mathcal{G}$ lies in $\mathsf{LT}_{\succ}(I)$.

A basic concept behind the theory of Gröbner bases is the idea of *reduction* and *normal form*.

Definition 29 Let f be a polynomial in P and $\mathcal{G}$ a Gröbner basis for an ideal $I \subseteq \mathrm{P}$. Then there is a unique $r \in \mathrm{P}$ such that:

- the polynomial $f - r$ is in I, and
- no term of r is divisible by any term in $\mathsf{LT}_{\succ}(\mathcal{G})$.

The polynomial r is called the *normal form* of f with respect to $\mathcal{G}$, and can be obtained by reducing f repeatedly by polynomials of $\mathcal{G}$, until it is *irreducible*. We denote the normal form of f as $r = \mathsf{NR}_{\succ,\mathcal{G}}(f)$.

Theorem 4 *$\mathcal{G}$ is a Gröbner basis of an ideal I if and only if the following holds*

$$f \in I \iff \mathsf{NR}_{\succ,\mathcal{G}}(f) = 0$$

Proof Let f be an arbitrary polynomial in the ideal I. Then the division of f by $\mathcal{G}$ yields the following form

$$f = e_1 g_1 + \cdots + e_m g_m + r$$

Hence $r \in I$ because $f - r \in I$. Assume that $r \neq 0$. Then we can find a k such that $\mathsf{LT}_{\succ}(g_k)$ divides $\mathsf{LT}_{\succ}(r)$, since $\mathcal{G}$ is a Gröbner basis. This is a contradiction to the fact that r is reduced with respect to $\mathcal{G}$. Thus, r must be equal to zero.

Another worth mentioning theorem that shall be introduced concerns the existence of reduced Gröbner bases.

Theorem 5 *Every nonzero polynomial ideal has a unique reduced Gröbner basis.*

Proof See, for example, the proof of Theorem 2.4.13 of Sect. 2.4 in [14].

2.2.1 Buchberger's Algorithm

Buchberger introduced in his PhD dissertation [3] an algorithm to systematically compute a reduced Gröbner basis $\mathscr{G}$ for any ideal I. It turns out that the concept of a Gröbner bases is intimately related to the concept of S-polynomials.

Definition 30 Let $g_1, g_2 \in \mathrm{P}$. The *S-polynomial* of g_1 and g_2 is defined to be

$$S_{1,2} = \frac{p}{\mathsf{LM}_{\succ}(g_1)} g_1 - \frac{p}{\mathsf{LM}_{\succ}(g_2)} g_2$$

where p is the least common multiple: $p = \mathsf{lcm}(\mathsf{LT}_{\succ}(g_1), \mathsf{LT}_{\succ}(g_2))$,

Although the notion of S-polynomials is the nucleus of *algorithmic* Gröbner bases theory, the notion of Gröbner bases is independent of the notion of S-polynomials as it also gives many interesting results for the *non-algorithmic* polynomial ideal theory.

Theorem 6 (Buchberger's Criterion) *Let* $I = \langle g_1, \ldots, g_m \rangle \subseteq \mathrm{P}$, $\mathscr{G}$ *a set of polynomials* $\{g_1, \ldots, g_m\}$, *and* $\mathbb{B} = \{(i, j) \mid 1 \leq i < j \leq m, e_i = e_j\}$, *where* $\mathsf{LM}_{\succ}(g_i) = c_i t_i e_i$. *Then the following conditions are equivalent:*

1. *The set* $\mathscr{G}$ *is a Gröbner basis of* I *w.r.t.*$\succ$.
2. *For all pairs* $(i, j) \in \mathbb{B}$, *we have* $\mathrm{NR}_{\succ,\mathscr{G}}(\mathrm{S_{i,j}}) = 0$.

Proof See, for example, Sect. 2.5 in [16].

With this criterion, one can easily recreate Buchberger's algorithm [1985], which computes the reduced Gröbner basis $\mathscr{G}$ for any finite set of polynomials. The basic Buchberger's algorithm is the following:

Input:
A set F of generators $\{f_1, \ldots, f_m\}$ of the ideal I.
A term ordering $\succ$.
Output:
A Gröbner basis of I.

0.1 Set $\mathscr{G}$ equal to F;
0.2 Let B be the set of pairs $\{(i, j) \mid g_i, g_j \in \mathscr{G}, i > j\}$;
0.3 **while** $B \neq \emptyset$ **do**
0.4 Choose a pair $(i, j) \in B$;
0.5 Set $B := B \setminus \{(i, j)\}$;
0.6 Compute S_{ij} and let $h = \mathrm{NR}_{\succ,\mathscr{G}}(\mathrm{S_{ij}})$;
0.7 **if** $h = 0$ **then**
0.8 Go to line 3;
0.9 **end**
0.10 **if** $h \neq 0$ **then**
0.11 Add h to $\mathscr{G}$;
0.12 Build new all critical pairs containing h and add them to B;
0.13 Go to step 3;
0.14 **end**
0.15 **end**
0.16 **return** $\mathscr{G}$

Algorithm 1: Buchberger's Algorithm

Although, Buchberger's algorithm is undeniably simple, the proof of its termination is not trivial. The algorithm initializes with a finite number of pairs of polynomials, which correspond to the S-polynomials to be computed. Some of those pairs lead to zero reductions while others contribute to the Gröbner basis. Hence, $\mathscr{G}$ is expected to grow, as well as the number of additional pairs that have to be considered.

Theorem 7 *Buchberger's algorithm terminates after a finite number of steps.*

Proof Let $\mathscr{G}_n$ denote the trial Gröbner basis that is produced by the algorithm at the n-th iteration step. We know that $\mathscr{G}_1 \subset \mathscr{G}_2 \subset \mathscr{G}_3 \subset \ldots$, however, the most important part is that the sets of leading terms increase as well: $\mathsf{LT}_{\succ}(\mathscr{G}_1) \subset \mathsf{LT}_{\succ}(\mathscr{G}_2) \subset \mathsf{LT}_{\succ}(\mathscr{G}_3) \subset \cdots$. By Dickson's Lemma [1913], this process ends in a finite number of steps, once the sequence of leading terms stabilizes. See [3] for a complete proof.

2.2.2 Introduction to Signature-Based Strategies

The main idea of the signature-based strategies for computing a Gröbner basis is to associate each polynomial with a signature on which the criteria and reduction steps depend. The concept was initially proposed by [7] together with his F5 algorithm [7], and has become extremely popular partly due to its good performances.

The most efficient variants of F5 are: the F5C algorithm by [5], the F5 with extended criteria by [11], the Gao-Guan-Volny (G2V) [8], and the Gao-Volny-Wang (GVW) [9]. The main differences between these algorithms are the extra conditions implemented to ensure correctness of the strategy.

Suppose, for example, that f and g are two polynomials, where t_f and t_g are terms such that the leading terms of $t_f f$ and $t_g g$ are the same. Then a necessary condition to reject the critical pair of f and g is that, there exists some known polynomial h such that its signature is a factor of $t_f f'$s or $t_g g'$s signature. We shall see that this condition alone is not sufficient to ensure correctness. Thus, existing implementations use different extra conditions.

In this section, we give a brief introduction to signature-based strategies. First, we recall the concept of polynomial signature. Then, we describe a generic footprint for signature-based algorithms. Lastly, we introduce a detailed description of the GVW algorithm. For proofs of the correctness and termination, see for example, [4, 5, 7, 8, 11, 17]. However, most of these proofs assume the input to be homogeneous, or the critical pair that is associated to the smallest signature to be computed first. These are extra requirements can affect the performance of the algorithm by making it less efficient.

Let $\mathrm{P} = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K and $\succ$ be a fixed term ordering in P. Let $I = \langle F \rangle \subset R$ be an ideal generated by the elements of $F = \{g_1, \ldots, g_m\}$, where each $g_i \in \mathrm{P}$.

$$I = \langle g_1, \ldots, g_m \rangle = \{u_1 g_1 + \cdots + u_m g_m : u_1, \ldots, u_m \in \mathrm{P}\} \subseteq \mathrm{P} \tag{2}$$

Then we can define the following map

$$\begin{aligned} \phi : \mathrm{P}^m &\longrightarrow I \\ \sum_{i=1}^{m} u_i \mathbf{e}_i &\mapsto \sum_{i=1}^{m} u_i g_i \end{aligned}$$

such that the u_i's are polynomials in P, and $\mathbf{e}_1, \ldots, \mathbf{e}_m$ are the canonical generators of the free P-module P^m. We have that the elements $\mathbf{u} \in R^m$ with $\phi(\mathbf{u}) = 0$ are called *syzygies* of $g_1, \ldots, g_m$. We use the notation $\mathbf{H} = \mathrm{Syz}(F)$ to represent the module of all such syzygies.

$$\mathbf{H} = \{(u_1, \ldots, u_m) \in P^m : u_1 g_1 + \cdots + u_m g_m = 0\} \tag{3}$$

We denote elements of P^m, which we see as row vectors, with bold letters e.g. $\mathbf{g}$, $\mathbf{u}$ etc. Next, we consider the following P-submodule of $\mathrm{P}^m \times \mathrm{P}$:

$$M = \{(\mathbf{u}, v) \in \mathrm{P}^m \times \mathrm{P} : \mathbf{u}\mathbf{g}^t = v\} \tag{4}$$

generated by

$$(\mathbf{e}_1, g_1), (\mathbf{e}_2, g_2), \ldots, (\mathbf{e}_m, g_m) \tag{5}$$

Now that all the settings are in place, we introduce our first definition of polynomial signature.

Definition 31 [7] Let $\mathrm{P} = K[x_1, \ldots, x_n]$ and v a polynomial in the ideal $I \subseteq \mathrm{P}$. Let $u_1, \ldots, u_m \in \mathrm{P}$ and $\mathbf{u} \in \mathrm{P}^m$ such that $v = \phi(\mathbf{u})$, where $\mathbf{u} := \sum_{i=1}^{m} u_i \mathbf{e}_i$. We say that $\mathsf{LT}_{\succ}(\mathbf{u})$ is a *signature* of $(\mathbf{u}, v) \in \mathrm{P}^m \times \mathrm{P}$. Moreover, $v \in \mathrm{P}$ has an unique and minimal signature if a term ordering is fixed.

Signature-based algorithms follow also Buchbergers algorithm footprints. Hence, we shall define a similar concept to the one of critical pairs.

Definition 32 Suppose $(\mathbf{u}_1, v_1), (\mathbf{u}_2, v_2) \in \mathrm{P}^m \times \mathrm{P}$ are two pairs with v_1 and v_2 both nonzero. Let

$$t_1 = \frac{\mathsf{lcm}(\mathsf{LT}_{\succ}(v_1), \mathsf{LT}_{\succ}(v_2))}{\mathsf{LT}_{\succ}(v_1)}, \quad t_2 = \frac{\mathsf{lcm}(\mathsf{LT}_{\succ}(v_1), \mathsf{LT}_{\succ}(v_2))}{\mathsf{LT}_{\succ}(v_2)}$$

Suppose $\max(t_1\, \mathsf{LT}_{\succ}(\mathbf{u}_1), t_2\, \mathsf{LT}_{\succ}(\mathbf{u}_2)) = t_i\, \mathsf{LT}_{\succ}(\mathbf{u}_i)$. Then

- We call $t_i(\mathbf{u}_i, v_i) = (t_i \mathbf{u}_i, t_i v_i)$ a *J-pair*[1] of $(\mathbf{u}_1, v_1)$ and $(\mathbf{u}_2, v_2)$, and
- $t_i\, \mathsf{LT}_{\succ}(\mathbf{u}_i)$ their *J-signature*.

Since the J-signature of $(\mathbf{u}_1, v_1)$ and $(\mathbf{u}_2, v_2)$ is unique, then we are allowed to pick either $t_1(\mathbf{u}_1, v_1)$ or $t_2(\mathbf{u}_2, v_2)$ as a J-pair if $t_1\, \mathsf{LT}_{\succ}(\mathbf{u}_1) = t_2\, \mathsf{LT}_{\succ}(\mathbf{u}_2)$. Also, it is only necessary to keep one J-pair per distinct J-signature.

[1] J means "joint" of the two pairs.

The terms t_1 and t_2 used in J-pairs are exactly the same as those used in Buchberger's S-polynomial $t_1 v_I - c t_2 v_2$, where $c = \mathsf{LC}_\succ(v_I)/\mathsf{LC}_\succ(v_2)$. The main difference between these two concepts is that J-pairs postpone the computation of S-polynomials until the reduction phase, as we work with their signatures. This idea should become more clear with the introduction of the GVW algorithm.

We revise now the reduction process, which shall depend as well on the concept of signature.

Definition 33 Let $(\mathbf{u}_1, v_1), (\mathbf{u}_2, v_2) \in \mathrm{P}^m \times \mathrm{P}$ be any two pairs. If v_2 is nonzero, $\mathsf{LT}_\succ(v_2)$ divides $\mathsf{LT}_\succ(v_I)$ and $\mathsf{LT}_\succ(t\mathbf{u}_2) \succeq \mathsf{LT}_\succ(\mathbf{u}_1)$ then we say $(\mathbf{u}_1, v_I)$ is *top-reducible* by $(\mathbf{u}_2, v_2)$. The corresponding *top-reduction* is

$$(\mathbf{u}_1, v_I) - ct(\mathbf{u}_2, v_2) = (\mathbf{u}_I - ct\mathbf{u}_2, v_I - ctv_2), \tag{6}$$

where $t = \mathsf{LT}_\succ(v_1)/\mathsf{LT}_\succ(v_2)$ and $c = \mathsf{LC}_\succ(v_1)/\mathsf{LC}_\succ(v_2)$.
When v_2 is zero and $\mathbf{u}_1, \mathbf{u}_2 \neq 0$, then we say that $(\mathbf{u}_1, v_1)$ is top-reducible by $(\mathbf{u}_2, 0)$ if $\mathsf{LT}_\succ(\mathbf{u}_2)$ divides $\mathsf{LT}_\succ(\mathbf{u}_1)$. For such scenario the top-reduction is

$$(\mathbf{u}_1, v_I) - ct(\mathbf{u}_2, v_2) = \left(\mathbf{u}_I - \frac{\mathsf{LM}_\succ(\mathbf{u}_I)}{\mathsf{LM}_\succ(\mathbf{u}_2)}\mathbf{u}_2, v_I\right)$$

Every time we perform a top-reduction, we cancel the leading term in the v-part without increasing the signature of $(\mathbf{u}_1, v_1)$. Moreover, we can say that,

Definition 34 A top-reduction is called *regular top-reduction*, if

$$\mathsf{LT}_\succ(\mathbf{u}_1 - ct\mathbf{u}_2) = \mathsf{LT}_\succ(\mathbf{u}_1),$$

and *super top-reduction* otherwise. This means that the signature of $(\mathbf{u}_1, v_1)$ becomes smaller under a super top-reduction and remains unchanged under a regular top-reduction. Observe that a super top-reduction happens if

$$\mathsf{LT}_\succ(t\mathbf{u}_2) = \mathsf{LT}_\succ(\mathbf{u}_1) \text{ and } \frac{\mathsf{LC}_\succ(\mathbf{u}_1)}{\mathsf{LC}_\succ(\mathbf{u}_2)} = \frac{\mathsf{LC}_\succ(\mathrm{v}_1)}{\mathsf{LC}_\succ(\mathrm{v}_2)}$$

Furthermore, if a pair $(\mathbf{u}_1, v_1)$ is top-reducible by $(\mathbf{u}_2, 0)$, then the top-reduction is always a super top-reduction. Hence we do not have to perform the reduction. Also, a pair $(\mathbf{u}_1, 0)$ is never top-reducible by $(\mathbf{u}_2, v_2)$ for $v_2 \neq 0$. Note that we do not have to perform reductions for the super top-reduction case.

Lemma 1 *Let t be a term in P. If a pair $t(\mathbf{u}_1, v_1)$ is (regular) top-reducible by $(\mathbf{u}_2, v_2)$, where both v_1 and v_2 are nonzero, then $t_1(\mathbf{u}_1, v_1)$ is a J-pair of $(\mathbf{u}_1, v_1)$ and $(\mathbf{u}_2, v_2)$, where*

$$t_1 = \frac{\mathsf{lcm}(\mathsf{LT}_\succ(v_1), \mathsf{LT}_\succ(v_2))}{\mathsf{LT}_\succ(v_1)}$$

and t_1 is a divisor of t. Furthermore, $t_1(\mathbf{u}_1, v_1)$ is (regular) top-reducible by $(\mathbf{u}_2, v_2)$.

Proof See, for example, [8].

Proposition 4 *Suppose that* $L = \{(\mathbf{u}_1, v_1), \ldots, (\mathbf{u}_k, v_k)\}$ *is a strong Gröbner basis for* M*, that is, every pair* $(\mathbf{u}, v) \in M$ *is top-reducible by some pair in* L*. Then one can derive the following conclusions*

- *The set* $\mathscr{G}_0 = \{v_i : 1 \leq i \leq k\}$ *is a Gröbner basis for the ideal* $I = \langle g_1, \ldots, g_m \rangle$*, and*
- *The set* $\mathscr{G}_1 = \{\mathbf{u}_i : v_i = 0,\ 1 \leq i \leq k\}$ *is a Gröbner basis for the syzygy module of* $\mathbf{g} = (g_1, \ldots, g_m)$*.*

A strong Gröbner basis for $M \subset \mathrm{P}^m \times \mathrm{P}$ is a Gröbner basis for M as a submodule of P^{m+1}. However the converse may not be true for an arbitrary submodule M of P^{m+1}. This is why we call the basis a strong Gröbner basis.

Proof In order to prove that $\mathscr{G}_1$ is a Gröbner basis for the syzygy module of $\mathbf{g}$, one can deduce from equations (3) and (4) that we must have $(\mathbf{u}, 0) \in M$ for any $\mathbf{u} = (u_1, \ldots, u_m)$ in the syzygy module of $\mathbf{g}$. Now, suppose that $(\mathbf{u}, 0)$ is top-reducible by some pair $(\mathbf{u}_i, v_i)$ in L. Then by Definition (34), v_i must be zero. Therefore, $\mathbf{u}_i \in \mathscr{G}_1$ and $\mathsf{LT}_{\succ}(\mathbf{u})$ is reducible by $\mathsf{LT}_{\succ}(\mathbf{u}_i)$.

Now, to prove that $\mathscr{G}_0$ is a Gröbner basis for I, assume $v \in I$ and nonzero. Then we know there exists $\mathbf{u} = (u_1, \ldots, u_m) \in \mathrm{P}^m$ so that $\mathbf{u}\mathbf{g}^t = v$, hence $(\mathbf{u}, v) \in M$. Among all such $\mathbf{u}$, we pick the one having the smallest leading term. Since $(\mathbf{u}, v) \in M$, it is top-reducible by some $(\mathbf{u}_i, v_i)$ where $1 \leq i \leq k$. Assume, by absurd, that $v_i = 0$. Then we could use $(\mathbf{u}_i, 0)$ to reduce $(\mathbf{u}, v)$ to get a $\mathbf{u}'$ such that $\mathbf{u}'\mathbf{g}^t = v$, with $\mathsf{LT}_{\succ}(\mathbf{u}')$ smaller than $\mathsf{LT}_{\succ}(\mathbf{u})$, which contradicts the initial minimality of $\mathsf{LT}_{\succ}(\mathbf{u})$. So $v_i \neq 0$ and $\mathsf{LT}_{\succ}(v_i)$ divides $\mathsf{LT}_{\succ}(v)$. Therefore, we have that $\mathscr{G}_0$ is a Gröbner basis for I.

Definition 35 Let L be any set of pairs in M as defined in (4). We say that $(\mathbf{u}, v)$ is *eventually super top-reducible* by L if there is a sequence of regular top-reductions of $(\mathbf{u}, v)$ by pairs in L that reduce $(\mathbf{u}, v)$ to a pair $(\mathbf{u}', v')$ that is no longer regular top-reducible by L but is super top-reducible by at least one pair in L.

Theorem 8 *Let* L *be any set of pairs in* M *as defined in* (4)*. Then* L *is a strong Gröbner basis for* M *if and only if for every distinct J-signature from* L *there is at least one J-pair from* L *with the same J-signature that is eventually super top-reducible by* L*.*

Proof See [8] for a proof of this theorem.

Theorem 9 *If the Algorithm 2 terminates, then* V *is a Gröbner basis for* $I = \langle g_1, g_2, \ldots, g_m \rangle$ *and* $\mathbf{H}$ *is a Gröbner basis for the leading terms of the syzygy module of* $(g_1, g_2, \ldots, g_m)$*.*

Proof See [8] for a proof of this theorem.

The algorithm that puts together all the pieces follows next.

Input:
List of polynomials $g_1, \ldots, g_m \in \mathrm{P} = K[x_1, \ldots, x_n]$,
A term ordering for P, and
A term ordering on P^m
Output:
A Gröbner basis V of $I = \langle g_1, \ldots, g_m \rangle$, and
A Gröbner basis H of $\mathsf{LT}_\succ(\mathbf{H})$, the leading terms of the syzygy module
Variables:
U a list of terms T_i, representing signatures of $(\mathbf{u}_i, v_i) \in M$,
V a list of polynomials v_i for $(\mathbf{u}_i, v_i) \in M$,
H a list of $\mathsf{LT}_\succ(\mathbf{u})$ were $\mathbf{u} \in R^m$ is a syzygy found so far,
JP a list of pairs (t, i) s.t. $t(u_i, v_i)$ is the J-pair of $(\mathbf{u}_i, v_i)$ and $(\mathbf{u}_j, v_j)$ for some $j \neq i$.
Algorithm:
1.1 Initialize U as $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$;
1.2 Initialize V as $\{g_1, \ldots, g_m\}$;
1.3 Add the leading terms of the principle syzygies $g_j \mathbf{e}_i - g_i E_j$ for $1 \leq i < j \leq m$ to H ;
1.4 Compute all the J-pairs of $(\mathbf{e}_1, g_1), \ldots, (\mathbf{e}_m, g_m)$;
1.5 Add to the list JP all J-pairs whose signatures are distinct and not reducible by H ;
1.6 **while** *JP is not empty* **do**
1.7 Take a minimal pair (t, i) from JP (w.r.t. signature) ;
1.8 Delete the pair (t, i) from the list JP ;
1.9 **while** $t(T_i, v_i)$ *is regular top-reducible by the pairs in*(U, V) **do**
1.10 Perform regular top-reduction, say to get(T, v) ;
1.11 **end**
1.12 **if** $v = 0$ **then**
1.13 Append T to H ;
1.14 Delete every J-pair (t, j) in JP whose signature tT_j is divisible by T ;
1.15 **end**
1.16 **if** $v \neq 0$ *and* (T, v) *is not super top-reducible by* (U, V) **then**
1.17 Append T to U and v to V;
1.18 Form all J-pairs for (T, v) and (T_j, v_j), $1 \leq j \leq |U| - 1$,and ;
1.19 Consider only J-pairs whose signatures are not reducible by H, and ;
1.20 Add to JP only the J-pair with minimal $\mathsf{LT}_\succ(v)$ for each distinct signature T ;
1.21 Add leading terms of the principle syzygies, $vT_j - v_j T$ for $1 \leq j \leq |U| - 1$, to H ;
1.22 **end**
1.23 **end**
1.24 **return** V and H;

Algorithm 2: The GVW algorithm

3 The Hilbert-Driven Strategy

In the previous section, we introduced the notion of Hilbert series and we have shown its connection to the Hilbert polynomial. In this section, we introduce a new criterion to signature-based strategies that is based on the so-called *Hilbert-driven Gröbner basis algorithm*, originally presented by [18].

Current attempts based on this strategy have a common drawback: one needs to know the Hilbert series beforehand in order to take advantage of it. Some work about how to compute it efficiently can be found in [2]. In some special cases we have all the information we need about the Hilbert series without any further computations.

Theorem 10 *Let $\succ$ be a term ordering on P, and $I \subset P$ a homogeneous ideal. Then we have the following relation*

$$\mathsf{HP}(\mathrm{P}/I, t) = \mathsf{HP}(\mathrm{P}/\mathsf{LT}_\succ(I), t)$$

Proof See for example Sect. 5.2 in [10].

Using the above theorem one can derive a few other properties, which are nicely described through the following statement.

Corollary 4 *Let $I \in P$ be an ideal and $\succ$ a term ordering. Let $\mathscr{G} = \{g_1, \ldots, g_s\} \subset I$. Then it holds:*

1. $\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(I), d) \leq \mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(\mathscr{G}), d)$ *for all* d.
2. *If* $\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(I), d) = \mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(\mathscr{G}), d)$ *for all* d, *then* $\mathscr{G}$ *is a Gröbner basis for* I.

Proof The proof follows easily from the fact that $\mathsf{LT}_{\succ}(\mathscr{G}) \subset \mathsf{LT}_{\succ}(I)$. Having $\mathsf{LT}_{\succ}(\mathscr{G}) \subset \mathsf{LT}_{\succ}(I)$, the equality of the Hilbert functions follows from the equality of the leading ideals, i.e. $\mathsf{LT}_{\succ}(\mathscr{G}) = \mathsf{LT}_{\succ}(I)$. But this is just the definition of $\mathscr{G}$ being a Gröbner basis for I.

Corollary 5 *Let $\succ_1$ and $\succ_2$ be two term orderings on* P *and* $I \subseteq \mathrm{P}$ *an ideal.*

1. *If I is homogeneous, then* $\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ 1}(I), d) = \mathsf{HF}(\mathrm{P}/I, d) = \mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ 2}(I), d)$ *for all* d.
2. *If I is inhomogeneous, then* $\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ 1}(I), d) = \mathsf{HF}(\mathrm{P}/I, d) - \mathsf{HF}(\mathrm{P}/I, d-1) = \mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ 2}(\mathscr{G}), d)$ *for all* d.

Proof See for example [18].

Another important corollary, which is given by Traverso in [18], describes how to use the Hilbert series to improve the computations of Gröbner basis for inhomogenous ideals.

Corollary 6 *Let $I \subset \mathrm{P}$ be an ideal and $\succ_1$ and $\succ_2$ two term orderings on* P. *Let $\mathscr{G}_1$ be a Gröbner basis for I w.r.t. $\succ_1$. Set $\mathscr{G}_1$ as an input for the computation of a Gröbner basis $\mathscr{G}_2$ for I w.r.t. $\succ_2$. Then we can use the following variant algorithm:*

1. *Consider critical pairs by increasing degree.*
2. *If the degree decreases during a reduction step, then the reduced element can be deleted and the next pair can be computed.*

This corollary is very useful when the computation of a Gröbner basis w.r.t. $\succ_1$ is easier than the computation w.r.t.$\succ_2$.

The next theorem from [18] gives one of the most important results of this section.

Theorem 11 *Let I and J be two homogeneous ideals in* P *such that $J \subset I$. By Theorem there exist polynomials $p(t) = \sum_{i=0}^{v} p_i t^i$ and $q(t) = \sum_{j=0}^{w} q_j t^j$ such that the corresponding Hilbert series are*

$$\mathsf{HS}(\mathrm{P}/I, t) = \frac{p(t)}{(1-t)^n} \text{ and } \mathsf{HS}(\mathrm{P}/\mathrm{J}, \mathrm{t}) = \frac{\mathrm{q(t)}}{(1-\mathrm{t})^{\mathrm{n}}}.$$

Then the following conditions are equivalent:

1. $\mathsf{HF}(\mathrm{P}/I, t) = \mathsf{HF}(\mathrm{P}/J, t)$ *for all* $1 \leq t \leq d-1$ *and* $\mathsf{HF}(\mathrm{P}/I, d) < \mathsf{HF}(\mathrm{P}/J, d)$.
2. $p(i) = q(i)$ *for* $1 \leq i \leq d-1$ *and* $p(d) < q(d)$.

Definition 36 Let $(p_1, \ldots, p_r)$ be a sequence of polynomials in P. Let F be a finitely generated module in M. We call $(p_1, \ldots, p_r)$ a *sequence regular* if for each $1 \leq i \leq r$ it holds that p_i is not a zero divisor in $F/\langle p_1, \ldots, p_{i-1}\rangle$

From the definition above, we have that an important property of a complete intersection $V(I)$ is that we can compute the corresponding Hilbert series of I without computing a Gröbner basis for I beforehand. The following lemma shows how.

Lemma 2 *If $V(I)$ is a complete intersection for $I = \langle f_1, \ldots, f_r\rangle$ where f_i is homogeneous of degree $\deg(f_i) = d_i$ for all $1 \leq i \leq r$, then the Hilbert series is given by*

$$\mathsf{HS}(\mathrm{P}/I, t) = \frac{\prod_{i=1}^{r}(1 - t^{d_i})}{(1-t)^n} \tag{7}$$

Now we have all the tools required to describe the idea behind the Hilbert-driven algorithm.

Let $\succ_1$ be a term ordering on P and let I be the ideal for which we want to compute a Gröbner basis. Assume that we know the Hilbert function $\mathsf{HF}(\mathrm{P}/I, t)$. Keep in mind that it can be a consequence of one of the following facts

1. A previous Gröbner basis computation for I w.r.t. some other term ordering.
2. Or a special shape of the ideal I: a complete intersection where the formula is known (see Eq. 7).

If I is homogeneous then we compute the Gröbner basis $\mathscr{G}$ for I by increasing degree. Assume that we have an intermediate Gröbner basis $\mathscr{G}$ for some degree $d \geq 0$. Then we compute the Hilbert function $\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(\mathscr{G}), t)$. It holds that $\mathscr{G}$ is a Gröbner basis for I if

$$\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(\mathscr{G}), t) = \mathsf{HF}(t) \text{ for all } t \leq d.$$

Next, we shall see how to incorporate this strategy into signature-based algorithms. Our implementation is based on the footprints of the algorithm of [9]. Thereby, the output of the algorithm not only returns a Gröbner basis of the ideal I, but also a Gröbner basis of the leading terms of the syzygy module of the same ideal.

The idea of Algorithm 3 is the following. Let α_k and β_k be two variables used to keep track of the number of generators of degree k in the Gröbner basis and in the leading terms of the syzygy module, which shall then used to avoid unnecessary computations of the Hilbert series. Then, if the equality $\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(\mathscr{G}), k) = \mathsf{HF}(k) - \mathsf{HF}(\mathrm{P}/H, k-d)$ holds for all k, we have that $\mathscr{G}$ is a Gröbner basis of I and H is a Gröbner basis for the leading terms of the syzygy module. See lines 28–29. Otherwise, we know that there exists a minimal degree d for each we need

to compute more generators. That degree d also gives us a bound for the minimal degree of the S-polynomials that we need to compute.

Next we give the pseudo-code of the algorithm that puts together all the ideas discussed. The reader should keep in mind that this strategy highly depends on the order in which the J-pairs are processed. If the first J-pairs are the useful ones, the optimization is best. If those are at the end of the list of pairs to be reduced, then we still have to compute the zero reductions of all useless pairs before them.

Input:
An ideal $I = \langle g_1, \ldots, g_m \rangle \in \mathrm{P} = K[x_1, \ldots, x_n]$,
A term ordering for P, and a term ordering on P^m
$\mathsf{HF}(w) := \mathsf{HF}(\mathrm{P}/I, w)$ **the Hilbert function of** I **(Optional)**
Output:
A Gröbner basis V for I and,
A Gröbner basis H for $\mathsf{LT}_{\succ}(\mathbf{H})$, the leading terms of the syzygy module
Variables:
U a list of terms T_i, representing sig. of $(\mathbf{u}_i, v_i) \in M$,
V a list of polynomials v_i for $(\mathbf{u}_i, v_i) \in M$,
H a list of $\mathsf{LT}_{\succ}(\mathbf{u})$ were $\mathbf{u} \in \mathrm{P}^m$ is a syzygy found so far,
JP a list of pairs (t, i) s.t. $t(u_i, v_i)$ is the J-pair of $(\mathbf{u}_i, v_i)$ and $(\mathbf{u}_j, v_j)$ for some $j \neq i$.
Algorithm:
2.1 U = $\{\mathrm{e}_1, \ldots, \mathrm{e}_m\}$ and V = $\{g_1, \ldots, g_m\}$;
2.2 Add the leading terms of the principle syzygies $g_j \mathrm{e}_i - g_i \mathrm{e}_j$ for $1 \leq i < j \leq m$ to H ;
2.3 Compute all the J-pairs of $(\mathrm{e}_1, g_1), \ldots, (\mathrm{e}_m, g_m)$;
2.4 Add to the list JP all J-pairs whose signatures are distinct and not reducible by H ;
2.5 **Initialize** d **with the minimal degree in JP** ;
2.6 **while** JP is not empty **do**
2.7 Take a minimal pair (t, i) from JP (with respect to signature) ;
2.8 Delete the pair (t, i) from the list JP ;
2.9 **while** $t(T_i, v_i)$ *is regular top-reducible by the pairs in* (U, V) **do**
2.10 **Perform regular top-reductions if the degree is** $\geq d$**, say to get** (T, v) **of degree** k**. Else Goto 6** ;
2.11 **end**
2.12 **if** $v = 0$ **then**
2.13 Append T to H ;
2.14 Delete every J-pair (t, j) in JP whose signature tT_j is divisible by T ;
2.15 $\beta_k \leftarrow \beta_k + 1$;
2.16 **end**
2.17 **if** $v \neq 0$ *and* (T, v) *is not super top-reducible by* (U, V) **then**
2.18 Append T to U and v to V;
2.19 Form all J-pairs for (T, v) and (T_j, v_j), $1 \leq j \leq |U| - 1$, and ;
2.20 Consider only J-pairs whose signatures are not reducible by H, and ;
2.21 Add to JP J-pairs with minimal $\mathsf{LT}_{\succ}(v)$ for each distinct signature T ;
2.22 Add LTs of the principle syzygies, $vT_j - v_j T$ for $1 \leq j \leq |U| - 1$, to H ;
2.23 **Update** β_k ;
2.24 $\alpha_k \leftarrow \alpha_k + 1$;
2.25 **end**
2.26 **if** $\mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(V), w) = \mathsf{HF}(w) - \mathsf{HF}(\mathrm{P/H, w - d})$ **for all** w **then**
2.27 **return V and H**;
2.28 **end**
2.29 $d \leftarrow \min\{w \in \mathbb{N} \mid \mathsf{HF}(\mathrm{P}/\mathsf{LT}_{\succ}(V), w) \neq \mathsf{HF}(w) - \mathsf{HF}(\mathrm{P/H, w - d})\}$;
2.30 **end**
2.31 **return** V and H;

Algorithm 3: Signature-based algorithm using Hilbert series

Table 1 Timings $\mathbb{F}_{32003}$ in seconds

System	F5	F5E	GGV	GWV	New Alg.	CoCoA
Katsura 9	14.98	14.87	17.63	14.95	15.35	15.12
Katsura 10	153.35	152.39	192.20	152.32	165.32	142.21
Eco 8	2.24	0.38	0.49	0.69	0.35	0.44
Eco 9	77.13	8.19	13.51	8.23	7.21	13.26
F744	19.35	8.79	26.86	10.65	8.69	8.11
Cyclic 7	7.01	7.22	33.85	9.12	7.12	7.78
Cyclic 8	7,310.39	4,961.58	2,6242.12	5,961	6,267.58	4,410.39

Table 2 Number of critical pairs and zero reductions

System	F5		F5E		GGV		GWV		New Alg.	
Katsura 9	886	0	886	0	886	0	886	0	**886**	**0**
Katsura 10	1,781	0	1,781	0	1,781	0	1,781	0	**1,781**	**0**
Eco 8	830	322	565	57	2,012	57	602	57	**532**	**50**
Eco 9	2,087	929	1,278	120	5,794	120	1,778	120	**1,572**	**116**
F744	1,324	342	1,151	169	2,145	169	1,351	169	**1,091**	**162**
Cyclic 7	1,018	76	978	36	3,072	36	1,073	36	**978**	**30**
Cyclic 8	7,066	244	5,770	244	24,600	244	7,760	244	**7,592**	**239**

4 Experimental Results

In this section, we assess the performance of our algorithm against a standard database of examples to benchmark Gröbner basis algorithms.

We have implemented both GVW and new criteria in CoCoALib, and observed that both provide reasonable results. Also, the reader should keep in mind that this algorithm return more than just a Gröbner basis for the input ideal. All tests were run on Mac OS X with a 2.6 GHZ Intel Core i7 processor and 8GB DDR3 of memory.

The first benchmark compares the computation times of several examples over a field $\mathbb{F}_{32003}$. In order to ease the identification of our algorithm, we label it as *New Alg*. The computation times follow below:

We can draw two conclusions from this benchmark. First, the our algorithm is in general faster than the original algorithm—GWV, and in some cases it can be up to six times faster than GGV. Finally, we can see that there is not a clear winner but at comparable times our algorithm provides a Gröbner basis for the input ideal and a Gröbner basis for the leading terms of the syzygy module of the ideal.

Another way to compare the algorithm's performance is to use a computer independent measure, were we take into consideration the number of J-pairs processed and the number of J-pairs reducing to zero; therefore not producing any useful data. The data belonging to this measure can also be used to relate the amount of time required to compute the Gröbner basis (see Table 1) with the number of zero reductions predicted (Table 2).

5 Conclusions and Future Work

In this paper, we describe several strategies to improve the efficiency of the computation of a Gröbner basis. Despite any benefit that these approaches might have, they often have drawbacks, too. For example, one has often to consider restrictions on the input. Moreover, the efficiency of these methods is highly dependent of the behavior of the data during the computations, which cannot be known beforehand. Thus, these improvements do not provide us with a fail-proof optimization to compute Gröbner bases. To get a Gröbner basis in an efficient way, one has to implement and combine most of the presented ideas with well-designed heuristics.

The signature-based algorithms are not an exception. However, we can see that in most cases they will find more useless critical pairs than Buchberger's Criteria. Within the signature-based algorithms, performance is affected by restrictions on the reduction process and by the overhead that is generated due to how aggressive is the signature-based criteria chosen. Thus, again the question is not about getting a universal best algorithm, but even more about how to combine the signature-based world with already highly efficient improvements of the classic world without harming the performance or causing wrong results.

We developed a new strategy to the signature-based algorithms, which was built on top of previous literature concerning Hilbert series. There are two conclusions that can be drawn from the benchmarks. First, the our algorithm is in general faster than the original algorithm—GWV, and in some cases it can be up to six times faster than GGV. Finally, we can see that there is not a clear winner, but at comparable times our algorithm provides a Gröbner basis for the input ideal and a Gröbner basis for the leading terms of the syzygy module of the ideal.

Acknowledgments The author would like to thank to Prof. Lorenzo Robbiano for his thought provoking lectures and valuable comments. This work has been funded by the Marie-Curie Network SAGA (FP7, GA no. 214584).

References

1. Atiyah, M.F., MacDonald, I.G.: Introduction to Commutative Algebra. Addison-Wesley, London (1969)
2. Bigatti, A.M.: Computation of hilbert-poincaré series. J. Pure Appl. Algebra **119**(3), 237–253 (1997)
3. Buchberger, B.: An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (German). Univ. of Innsbruck, Austria (1965)
4. Eder, C.: On the criteria of the f5 algorithm. In: arXiv:0804.2033v1 (2008)
5. Eder, C., Perry, J.: F5c: a variant of faugre's f5 algorithm with reduced gröbner bases. J Symbolic Comput. **45**(12), 1442–1458 (2010)
6. Eisenbud, D.: Commutative Algebra: With a View Toward Algebraic Geometry. Springer, Berlin (2008)
7. Faugre, J.C.: A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In: Proceedings of ISSAC'02, pp. 75–82. ACM Press, New York (2002)

8. Gao, S., Guan, Y., Volny, F.I.: A new incremental algorithm for computing gröbner bases. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ISSAC '10, pp. 13–19. ACM, New York, NY (2010). doi:10.1145/1837934.1837944. http://doi.acm.org/10.1145/1837934.1837944
9. Gao, S., Volny, F.I., Wang, M.: A new algorithm for computing gröbner bases. In: Cryptology ePrint Archive: Report (2010)
10. Greuel, G., Pfister, G.: A Singular Introduction to Commutative Algebra. Springer, Berlin (2007)
11. Hashemi, A., Ars, G.: Extended f5 criteria. J Symbolic Comput. **45**(12), 1330–1340 (2010)
12. Hoffmann, C.M.: Geometric and Solid Modeling: An Introduction. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1989)
13. Hoffmann, C.M.: A dimensionality paradigm for surface interrogations. Comput. Aided Geom. Des. **7**(6), 517–532 (1990)
14. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra. Springer, Berlin (2000)
15. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra, 0th edn. Springer, Berlin (2005)
16. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra, 2nd edn. Springer, Berlin (2009)
17. Stegers, T.: Faugres F5 algorithm revisited (2005)
18. Traverso, C.: Hilbert functions and the buchberger algorithm. J. Symb. Comput. **22**(4), 355–376 (1996). doi:10.1006/jsco.1996.0056. http://dx.doi.org/10.1006/jsco.1996.0056
19. Wilkinson, J.H.: The evaluation of the zeros of ill-conditioned polynomials. part i. Numerische Mathematik **1**, 150–166 (1959)



http://www.springer.com/978-1-4471-6460-9

Future Vision and Trends on Shapes, Geometry and Algebra

de Amicis, R.; Conti, G. (Eds.)
2014, VIII, 162 p. 45 illus., 35 illus. in color., Hardcover
ISBN: 978-1-4471-6460-9