SPECIAL SESIONS

Applications of Computer Algebra - ACA2018

June 18–22, 2018

Santiago de Compostela, Spain

S11
Algorithms for Zero-Dimensional Ideals

Tuesday

Tue 19th, 10:30 - 11:00, Aula 1 – Robin Larrieu:
Fast Gröbner basis computation and polynomial reduction in the generic bivariate case

Tue 19th, 11:30 - 12:30, Aula 1 – Lorenzo Robbiano:
Special Properties of Zero-Dimensional Ideals: new Algorithms

Tue 19th, 12:30 - 13:00, Aula 1 – Martin Kreuzer:
Computing Subschemes of the Border Basis Scheme

Tue 19th, 13:00 - 13:30, Aula 1 – Simone Naldi:
On the computation of algebraic relations of bivariate polynomials

Tue 19th, 15:30 - 16:30, Aula 1 – Daniel Augot:
On the decoding of interleaved and folded Reed-Solomon codes

Tue 19th, 16:30 - 17:00, Aula 1 – Teo Mora:
Solving and bonding 0-dimensional ideals: Möller Algorithm and Macaulay Bases

Tue 19th, 17:30 - 18:00, Aula 1 – Michela Ceria:
Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game

Tue 19th, 18:00 - 18:30, Aula 1 – Hamid Rahkooy:
Computing Recurrence Relations of n-dimensional Sequences Using Dual of Ideals

Wednesday

Wed 20th, 10:00 - 11:00, Aula 1 – Mariemi Alonso:
Border basis, Hilbert Scheme of points and flat deformations

Wed 20th, 11:30 - 12:00, Aula 1 – Teo Mora:
De Nugis Groebnerialium 5: Noether, Macaulay, Jordan

Wed 20th, 12:00 - 12:30, Aula 1 – Thibaut Verron:
Signature-based Criteria for Möller's Algorithm for Computing Gröbner Bases over PID's

Wed 20th, 12:30 - 13:00, Aula 1 – Anna Bigatti:
Computing and Using Minimal Polynomials

Organizers

Vincent Neiger
XLIM – University of Limoges, France

Hamid Rahkooy
University of Waterloo, Canada

Éric Schost
University of Waterloo, Canada

Aim and cope

In the last decades, a lot of progress has been made on the study of efficient algorithms related to zero-dimensional ideals, including for solving polynomial systems, i.e. determining the finite set of roots common to a given collection of multivariate polynomials. During this process, it has turned out that these algorithms heavily rely on some routines from linear algebra. This session will focus on the design and the implementation of algorithms specifically tailored for the particular linear algebra problems encountered in this kind of computations. Applications of these techniques will also be considered, such as algebraic cryptanalysis and decoding algorithms for algebraic geometry codes.

Polynomial system solving often involves computing a first Groebner basis, typically with the F5 algorithm, and then working on finding a representation of the sought roots, using for example the FGLM algorithm. In the first step, one has to deal with matrices of large dimension which are sparse and exhibit a noticeable structure. The second step corresponds to finding the nullspace of a matrix with a multi-Krylov structure: the matrix is formed by some vector and its images by successive powers of the so-called multiplication matrices.

It has been observed that these multiplication matrices are most often sparse, a feature that one wants to exploit to obtain faster algorithms. So far, two approaches have been used to achieve this. One is inspired from the block Wiedemann algorithm, involving the computation of the generator for a linearly recurrent matrix sequence; the other one relies on the computation of generators for a multi-dimensional linearly recurrent sequence. This revived interest into the latter problem, with the goal of designing algorithms which outperform the Sakata algorithm, known for its applications to the decoding of algebraic geometry codes. Some approaches have already been described, involving computations with matrices that have a multi-layered block-Hankel structure.

This session aims at gathering the main actors behind the recent advances, and naturally all researchers interested in this topic and its future

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Border basis, Hilbert Scheme of points and flat deformations

Mariemi Alonso[1], **Jerome Brachat**[2], **Bernard Mourrain**[3]

A natural question when studying systems of polynomial equations is how to characterize the family of ideals which defines a fixed number μ of points counted with multiplicities. Understanding the allowed perturbations of a zero-dimensional algebra, which keep the number of solutions constant, is an actual challenge, in the quest for efficient and stable numerical polynomial solvers.

From a theoretical point of view, this question is related to the study of the Hilbert Scheme of μ points introduced by Grothendieck.

Many works were developed to analyze its geometric properties, (eg. Hartshorne (1965), [3] nad many others). Though the Hilbert functor is known to be representable its effective representation is still under investigation. Using the persistence theorem of Gotzmann (1978) , a global explicit description of the Hilbert scheme is given in [4] as a sub-scheme of a product of two Grassmannians. Equations defining $\mathrm{Hilb}^{\mu}(\mathbb{P}^n)$ in a single Grassmannian are also given in [4]. These equations, obtained from rank conditions in the vector space of polynomials in successive "degrees", have a high degree in the Plücker coordinates.

In the last years the problem of representation is also studied through sub-functor constructions and open covering of charts of the Hilbert scheme. Covering charts corresponding to subsets of ideals with a fixed initial ideal for a given term ordering . These ideas, starting with the proof of the irreducibility of Harthorne (1965), an Bayer 's PhD (1982)), were analyzed in several works, from the 80's; Carrá-Ferro (1988), Mark Haiman (1994), Huibregtse (2002), and more recent in [5] and [7].

These open subsets can be embedded into affine open subsets of the Hilbert scheme, corresponding to ideals associated to quotient algebras with a given monomial basis. Explicit equations of these affine varieties are developed for some special cases in the references above, and using syzygies or in more general setting in [5]. Their methods rely on simple algebraic construction and avoid the usual embeddings into high dimensional spaces. In this way, in [6] the authors obtain equations of low degree in a Grasmaniann for general Hilbert schemes.

In this talk, we concentrate in the punctual Hilbert scheme, and we show how to use Boorder basis to get new equations of it, of degree two in the Plucker coordinates of a Grasmaniann, which are simpler than Bayer and Iarrobino-Kanev equations [1]. Next, using Border basis we get an easy description of the tangent space at a point of $\mathrm{Hilb}^{\mu}(\mathbb{P}^n)$ [1]. We give also an effective criterion to test if a perturbed system

remains on the Hilbert scheme of the initial equations (test for a flat deformation), which involves a particular formal reduction with respect to border bases [2].

Finally, we introduce a "Newton Method" in the Hilbert scheme of points to find (numerically) a Border basis of a system of equations by using the knowledge of a border basis for some values of the coefficients nearby the ones of the given equations [2].

Keywords: Border basis, punctual Hilbert scheme, effective flat deformation of points

References

[1] MARIEMI ALONSO, JEROME BRACHAT, BERNARD MOURRAIN, The Hilbert Scheme of points and its link with border basis. *arXiv:0911.3503*, (2010).

[2] MARIEMI ALONSO, JEROME BRACHAT, BERNARD MOURRAIN, Flat Deformation of Points Communication in *MEGA2011*, Stockholm, May 30$^{\text{th}}$-June 3$^{\text{rd}}$, 2011.

[3] ANTHONY A. IARROBINO, Hilbert scheme of points: overview of last ten years. In *Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985)*, vol. 46 of *Proc. Sympos. Pure Math.*, Amer. Math. Soc., Providence, RI, 1987.

[4] ANTHONY IARROBINO; VASSIL KANEV, In Appendix C of *Power sums, Gorenstein algebras, and determinantal loci*. vol. 1721 *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1999.

[5] CRISTINA BERTONE, PAOLO LELLA, MARGHERITA ROGGERO, A Borel open cover of the Hilbert scheme, *J. Symb. Comput* **53** , 119–135 (2013).

[6] JEROME BRACHAT, PAOLO LELLA, BERNARD MOURRAIN, MARGHERITA ROGGERO, Extensors and the Hilbert scheme, *Annali della Scuola Normale Superiore di Pisa,Classe di Scienze,* **doi 10.2422/2036-2145.201407_003**, (2015).

[7] MATHIAS LEDERER, Groebner strata in the Hilbert scheme of points, *J. Commut. Algebra* **3**(3), 349–404 (2011).

[1]Departmento de Álgebra, Geometría y Topología
Complutense University
Plaza de Ciencias 3, 28040 Madrid (Spain)
mariemi@ucm.es

[3]Univ. Cote-d'Azur, Inria
Sophia-Antipolis, France
bernard.mourrain@inria.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the decoding of interleaved and folded Reed-Solomon codes

Daniel Augot[1]

In 2006, great progress has been made in algebraic coding theory, where codes reaching the so-called list decoding capacity were contructed by Guruswami and Rudra [4], elaborating on the ideas of Parvaresh and Vardy [5]. At the heart of these constructions lies the simple notion of *folding* the codes, which is a very simple construction, at the cost of shortening the underlying Reed-Solomon codes and augmenting the size of the alphabet.

Later, Guruswami proposed another decoding method, call "linear algebraic" [3], which appears to be easier to deal with, from the computer algebra point of view.

Both these methods rely heavily on finite fields and their properties, a fact which is strange in this area, since the simple, classical, Guruswami-Sudan list decoding algorithm [1] works over any field, and all the arguments for proving its validity, studying its list size and decoding radius does not depend on the field. In other words, the Guruswami-Sudan list decoding algorithm can be said to be of "geometric" nature, while the decoding algorithms of folded Reed-Solomon have an "arithmetic" nature.

At the heart of the basic Guruswami-Sudan algorithm lies a bivariate interpolation problem, i.e. one has to find the vanishing ideal of a set of points given by the instance of decoding problem. Then it is followed by the so-called root-finding step: the codewords which are looked for correspond to components to a curve. Similary, when generalizing to interleaved codes, the vanishing ideal of points in a higher dimensionnal space has to be computed. But in that case, the root-finding is ill-founded, and one should look for a zero dimensional ideal over the field of rational functions (or equivalently, a bivariate curve). This problem is cirvumvented using folding, and root-finfing then involves a lot properties of finite fields.

In this talk, I will describe a potential path to new ideas for having a decoding algorithm of folded Reed-Solomon codes which does not assume the finiteness of the field, and may be more natural, with better list size. But first, for didactical purposes, I will recall the basic problems and settings posed by list decoding, recalling the "Shannon" versus "Hamming" opposed situations, and why list decoding bridges them [2].

References

[1] V. Guruswami and M. Sudan. On representations of algebraic-geometry codes. *Information Theory, IEEE Transactions on*, 47(4):1610–1613, 2001.

[2] Venkatesan Guruswami. List decoding of binary codes - a brief survey of some recent results. In Yeow M. Chee, Chao Li, San Ling, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, volume 5557 of *Lecture Notes in Computer Science*, pages 97–106, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[3] Venkatesan Guruswami. Linear-algebraic list decoding of folded Reed-Solomon codes. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, June 8-10, 2011*, pages 77–85, 2011.

[4] Venkatesan Guruswami and Atri Rudra. Explicit capacity-achieving list-decodable codes. In *STOC '06: Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 1–10, New York, NY, USA, 2006. ACM.

[5] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *FOCS 2005: Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, Pittsburgh, United States*, pages 285–294, 2005.

[1]INRIA Saclay-Île-de-France, and École polytechnique
Palaiseau, France
daniel.augot@inria.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computing and Using Minimal Polynomials

John Abbott[1], **Anna M. Bigatti**[1], **Elisa Palezzato**[2], **Lorenzo Robbiano**[1]

Given a zero-dimensional ideal I in a polynomial ring, many computations start by finding univariate polynomials in I. Searching for a univariate polynomial in I is a particular case of considering the minimal polynomial of an element in P/I. It is well known that minimal polynomials may be computed via elimination, therefore this is considered to be a "resolved problem". But being the key of so many computations, it is worth investigating its meaning, its optimization, its applications.

If K is a field and R is a zero-dimensional affine K-algebra, *i.e.* a zero-dimensional algebra of type $R = K[x_1, \ldots, x_n]/I$, then R is a finite-dimensional K-vector space. Consequently, it is not surprising that minimal and characteristic polynomials can be successfully used to detect properties of R. This point of view was taken systematically in the book [7] where the particular importance of minimal polynomials (rather greater than that of characteristic polynomials) emerged quite clearly. That book also described several algorithms which use minimal polynomials as a crucial tool. The approach taken there was a good source of inspiration for our research, so we decided to delve into the theory of minimal polynomials, their uses, and their applications (for the details, see the full paper [6]).

First, we describe some algorithms for computing the minimal polynomial of an element of R and of a K-endomorphism of R. They refine similar algorithms examined in [7], and have been implemented and compared in CoCoALib [2].

We also address the problem of using a modular approach for computing minimal polynomials of elements of an affine $\mathbb{Q}$-algebra. As always with a modular approach, various obstacles have to be overcome (see for instance the discussion contained in [4] and in [5]). In particular, we deal with the notion of *reduction of an ideal modulo* p, and we introduce the *σ-denominator* of an ideal (for a term-ordering σ). Then we show that almost all primes are *good* which paves the way to the construction of the modular algorithm, and we reconstruct the rational polynomial using fault-tolerant rational reconstruction [1].

Minimal polynomials can be successfully and efficiently used to compute several important invariants of zero-dimensional affine K-algebras. More specifically, we describe some algorithms which show respectively how to determine whether a zero-dimensional ideal is radical, and how to compute the radical of a zero-dimensional ideal. Then we present some algorithms which determine whether a zero-dimensional ideal is maximal or primary. The techniques used depend very much on the field K. The main distinction is between small finite fields and fields of characteristic zero or

big fields of positive characteristic. In particular, it is noteworthy that in the first case Frobenius spaces play a fundamental role.

Finally, we describe how to compute the primary decomposition of a zero-dimensional affine K-algebra. They are inspired by the content of Chapter 5 of [7], but they present many novelties.

All these algorithms have been implemented in CoCoALib [2], and are accessible from CoCoA [3]. Their merits are also illustrated by good timings.

This research was partly supported by the project H2020-FETOPN-2015-CSA_712689 of the European Union

Keywords: Minimal polynomial, Gröbner bases, elimination, primary decomposition, radical.

References

[1] J. Abbott, *Fault-Tolerant Modular Reconstruction of Rational Numbers*, J. Symb. Comp. **80** (2017), pp. 707–718.

[2] J. Abbott and A.M. Bigatti, *CoCoALib: a C++ library for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it/cocoalib`

[3] J. Abbott, A.M. Bigatti, L. Robbiano, *CoCoA: a system for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it`

[4] J. Abbott, A.M. Bigatti, L. Robbiano, *Implicitization of Hypersurfaces*, J. Symb. Comput. **81** (2017), pp. 20–40.

[5] J. Abbott, A.M. Bigatti, L. Robbiano, *Ideals Modulo p*, `arxiv:1801.06112`, 2018

[6] J. Abbott, A. Bigatti, E. Palezzato, L. Robbiano, *Computing and Using Minimal Polynomials*, `arXiv:1704.03680`, 2017.

[7] M. Kreuzer and L. Robbiano, *Computational Linear and Commutative Algebra*, Springer, Heidelberg (2016).

[1]Dipartiment di Matematica
Università degli Studi di Genova
Via Dodecaneso 35, 16146, Genova
`abbott,bigatti@dima.unige.it`
`lorobbiano@gmail.com`

[2]Department of Mathematics
Hokkaido University
Kita 10, Nishi 8, Kita-Ku, Sapporo, Hokkaido, 060-0810
palezzato@math.sci.hokudai.ac.jp

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game.

Michela Ceria[1], **Teo Mora**[2]

In 1990 Cerlienco and Mureddu [4] gave a combinatorial algorithm which, given an ordered set of points $\underline{\mathbf{X}} = [P_1, ..., P_N] \subset \mathbf{k}^n$, $\mathbf{k}$ a field, returns the lexicographical Gröbner escalier $\underline{\mathsf{N}(I(\mathbf{X}))} \subset \mathcal{T} := \{x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n} \,|\, \gamma := (\gamma_1, ..., \gamma_n) \in \mathbb{N}^n\}$ of the vanishing ideal $I(\mathbf{X}) := \{f \in \mathcal{P} : f(P_i) = 0, \forall i \in \{1, ..., N\}\} \subset \mathcal{P} := \mathbf{k}[x_1, ..., x_n]$. Such algorithm actually returns a bijection (labelled *Cerlienco-Mureddu correspondence* in [9, II,33.2]) $\Phi_{\underline{\mathbf{X}}} : \underline{\mathbf{X}} \to \underline{\mathsf{N}(I(\mathbf{X}))}$. The algorithm is inductive and thus has complexity $\mathcal{O}\left(n^2N^2\right)$, but it has the advantage of being iterative, in the sense that, given an ordered set of points $\underline{\mathbf{X}} = [P_1, ..., P_N]$, its related escalier $\underline{\mathsf{N}(I(\mathbf{X}))}$ and correspondence $\Phi_{\underline{\mathbf{X}}}$, for any point $Q \notin \underline{\mathbf{X}}$ it returns a term $\tau \in \mathcal{T}$ such that, denoting $\underline{\mathbf{Y}}$ the ordered set $\underline{\mathbf{Y}} := [P_1, ..., P_N, Q]$, $\underline{\mathsf{N}(I(\mathbf{Y}))} = \underline{\mathsf{N}(I(\mathbf{X}))} \sqcup \{\tau\}$, $\Phi_{\underline{\mathbf{Y}}}(P_i) = \Phi_{\underline{\mathbf{X}}}(P_i)$ for all i and $\tau = \Phi_{\underline{\mathbf{Y}}}(Q)$. In order to produce the lexicographical Gröbner escalier with a better complexity, [6] gave a completely different approach (*Lex Game*): given a set of (not necessarily ordered) points $\mathbf{X} = \{P_1, ..., P_N\} \subset \mathbf{k}^n$ they built a trie (*point trie*) representing the coordinates of the points and then used it to build a different trie, the *lex trie*, which allows to reed the lexicographical Gröbner escalier $\mathsf{N}(I(\mathbf{X}))$. Such algorithm has a very better complexity, $\mathcal{O}\left(nN + N\min(N, nr)\right)$, where $r < n$ is the maximal number of edges from a vertex in the point tree, but in order to obtain it, [6] was forced to give up iterativity. In 1982 Buchberger and Möller [2] gave an algorithm (*Buchberger-Möller algorithm*) which, for any term-ordering $<$ on $\mathcal{T}$ and any set of (not necessarily ordered) points $\mathbf{X} = \{P_1, ..., P_N\} \subset \mathbf{k}^n$ iterating on the $<$-ordered set $\mathsf{N}(I(\mathbf{X}))$, returns the Gröbner basis of $I(\mathbf{X})$ with respect to $<$, the set $\mathsf{N}(I(\mathbf{X}))$ and a family $[f_1, \cdots, f_N] \subset \mathcal{P}$ of separators of $\mathbf{X}$ *id est* a set of polynomials such that

$$f_i(P_j) = \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j. \end{cases}.$$

Later Möller [8] extended the same algorithm to any finite set of functionals defining a 0-dimensional ideal, thus absorbing also the FGLM-algorithm [5] and, on the other side, proving that Buchberger-Möller algorithm has the FGLM-complexity [5] $\mathcal{O}(n^2N^3f)$ where f is the average cost of evaluating a functional at a term*.

*A more precise evaluation was later given by Lundqvist, namely $\mathcal{O}(\min(n, N)N^3 + nN^2 + nNf + \min(n, N)N^2f)$.

Möller [8] gave also an alternative algorithm (*Möller algorithm*) which, for any term-ordering $<$ on $\mathcal{T}$, given an ordered set of points[†] $[P_1, ..., P_N] \subset \mathbf{k}^n$, for each $\sigma \leq N$, denoting $\mathbf{X}_\sigma = \{P_1, ..., P_\sigma\}$ returns, with complexity $\mathcal{O}(nN^3 + fnN^2)$

- the Gröbner basis of the ideal $I(\mathbf{X}_\sigma)$;
- the correlated escalier $\mathsf{N}(I(\mathbf{X}_\sigma))$;
- a term $t_\sigma \in \mathcal{T}$ such that $\mathsf{N}(I(\mathbf{X}_\sigma) = \mathsf{N}(I(\mathbf{X}_{\sigma-1})) \sqcup \{\tau\}$,
- a triangular set $\{q_1, \cdots, q_\sigma\} \subset \mathcal{P}$ s.t. $q_i(P_j) = \begin{cases} 0 & i < j \\ 1 & i = j, \end{cases}$
- whence a family of separators can be easily deduced by Gaussian reduction,
- a bijection Φ_σ such that $\Phi_\sigma(P_i) = \tau_i$ for each $i \leq \sigma$, which moreover if $<$ is lexicographical, then coincides with Cerlienco-Mureddu correspondence.

Later, Mora [9, II,29.4] remarked that, since the complexity analysis of both Buchberger-Möller and Möller algorithms were assuming to perform Gaussian reduction on an N-square matrix and to evaluate each monomial in the set $\mathsf{B}(I(\mathbf{X})) := \{\tau x_j, \tau \in \mathsf{N}(I(\mathbf{X}_\sigma)), 1 \leq j \leq n\}$ over each point $P_i \in \mathbf{X}$, within that complexity one can use all the informations which can be deduced by the computations $\tau(P_i), \tau \in \mathsf{B}(I(\mathbf{X})), 1 \leq i \leq N$; he therefore introduced the notion of *structural description* of a 0-dimensional ideal [9, II.29.4.1] and gave an algorithm which computes such structural description of each ideal $I(\mathbf{X}_\sigma)$. Also anticipating the recent mood of degroebnerizing effective ideal theory, Mora, in connection with Auzinger-Stetter matrices and algorithm [1], proposed to present a 0-dimensional ideal $I \subset \mathcal{P}$ and its quotient algebra $\mathcal{P}/I$ by giving its *Gröbner representation* [9, II.29.3.3] *id est* the assignment of a $\mathbf{k}$-linearly independent ordered set $[q_1, \ldots, q_N] \subset \mathcal{P}/I$ and n N-square matrices $\left(a_{lj}^{(h)}\right), 1 \leq h \leq n$, which satisfy

1. $\mathcal{P}/I \cong \mathrm{Span}_{\mathbf{k}}\{q_1, \ldots, q_N\}$,
2. $x_h q_l = \sum_j a_{lj}^{(h)} q_j, 1 \leq j, l \leq N, 1 \leq h \leq n.$

Since Möller algorithm and Mora's extension is inductive, our aim is to give an algorithm which given an ordered set of points $\mathbf{X} = [P_1, ..., P_N] \subset \mathbf{k}^n$ produces for each $\sigma \leq N$ the lexicographical Gröbner escalier $\mathsf{N}(I(\mathbf{X}_\sigma))$, the related Cerlienco-Mureddu correspondence, a family of squarefree separators for $\mathbf{X}_\sigma$, and the n N-square Auzinger-Stetter matrices $\left(a_{lj}^{(h)}\right), 1 \leq h \leq n$, which satisfy condition 2. above with respect the linear basis $\mathsf{N}(I(\mathbf{X}_\sigma))$. The advantage is that, any time

[†] Actually the algorithm is stated for an ordered finite set of functionals $[\ell_1, ..., \ell_N] \subset \mathrm{Hom}_{\mathbf{k}}(\mathcal{P}, \mathbf{k})$ such that for each $\sigma \leq N$ the set $\{f \in \mathcal{P} : \ell_i(f) = 0, \forall i \leq s\}$ is an ideal.

a *new* point is to be considered, the old data do not need to be modified and actually can simplify the computation of the data for the new ideal. Since the Lex Game approach which has no tool for considering the order of the points has no way of using the data computed for the ideal $I(\mathbf{X}_{\sigma-1})$ in order to deduce those for $I(\mathbf{X}_{\sigma})$, while Möller algorithm and Mora's extension are iterative on the ordered points and intrinsically produce Cerlienco-Mureddu correspondence, in order to achieve our aim, we need to obtain a variation of Cerlienco-Mureddu algorithm which is not inductive. Our tool is the Bar Code [3], essentially a reformulation of the point trie which describes in a compact way the combinatorial structure of a (non necessarily 0-dimensional) ideal; the Bar Code allows to remember and read those data which Cerlienco-Mureddu algorithm is forced to inductively recompute. Actually, once the point trie is computed as in [6] with inductive complexity $\mathcal{O}(N \cdot N\log(N)n)$, the application of the Bar Code allows to compute the lexicographical Gröbner escaliers $\mathsf{N}(I(\mathbf{X}_{\sigma}))$ and the related Cerlienco-Mureddu correspondences, with iterative complexity $\mathcal{O}(N \cdot (n + \min(N, nr))) \sim \mathcal{O}(N \cdot nr)$. The families of separators can be iteratively obtained using Lagrange interpolation via data easily deduced from the point trie as suggested in [6] with complexity $\mathcal{O}(N \cdot \min(N, nr))$. The computation of the Auzinger-Stetter matrices is based on Lundqvist result [7, Lemma 3.2] and can be inductively performed with complexity[‡] $\mathcal{O}\left(N \cdot (nN^2)\right)$.

Keywords: zero-dimensional ideal, Cerlienco-Mureddu algorithm, lex game

References

[1] W. AUZINGER; H.J. STETTER, An Elimination Algorithm for the Computation of all Zeros of a System of Multivariate Polynomial Equations. *I.S.N.M.* **86**, 11–30 (1988).

[2] H.M. MÖLLER; B. BUCHBERGER, The construction of multivariate polynomials with preassigned zeros, *L. N. Comp. Sci.* **144**, 24–31 (1982).

[3] M. CERIA, Bar Code for monomial ideals, submitted to Journal of Symbolic Computations, special issue for MEGA 2017.

[4] L. CERLIENCO L.; M. MUREDDU, From algebraic sets to monomial linear bases by means of combinatorial algorithms. *Discrete Math.* **139**, 73-87 (1995).

[5] J.C. FAUGÈRE; P. GIANNI; D. LAZARD D; T. MORA, Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *J.S.C.* **16**, 329–344 (1993).

[‡]Naturally, our decision of giving an algorithm which can produce data for the the vanishing ideal when a new point is considered forbid us of using the new better algorithms for matrix multiplication; thus our complexity is $\mathcal{O}\left(N^3\right)$ and not $\mathcal{O}\left(N^{\omega}\right), \omega < 2.39$.

[6] B. FELSZEGHY; B. RÁTH; L. RÓNYAI The lex game and some applications. *J.S.C.* **4**, 663-681 (2006).

[7] S. LUNDQVIST, Vector space bases associated to vanishing ideals of points. *J.P.A.A.* **214**(4), 309-321 (2010).

[8] M.G. MARINARI; T. MORA; H.M. MÖLLER, Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *J. AAECC* **4**, 103-145 (1993).

[9] T. MORA Solving Polynomial Equation Systems (4 Vols.). Cambridge Univ. Press, Cambridge, 2003–16.

[1]Department of Computer Science
University of Milan
Via Comelico 39, Milano, Italy
michela.ceria@gmail.com

[2]Department of Mathematics
University of Genoa
Via Dodecaneso 35
theomora@disi.unige.it

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Subschemes of the Border Basis Scheme

Martin Kreuzer[1], **Le Ngoc Long**[1], **Lorenzo Robbiano**[2]

All 0-dimensional ideals in a polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K having a fixed colength μ are parametrized by the Hilbert scheme $\mathrm{Hilb}^\mu(\mathbb{A}^n)$. Since it is not easy to find the equations defining these moduli schemes, we may opt to study border basis schemes. They are open subschemes of the Hilbert scheme which cover it and can be defined using easily computable quadratic equations.

More precisely, let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an *order ideal*, i.e. a divisor closed finite subset of the set of terms in P, and let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ be the *border* of $\mathcal{O}$ which is defined by $\partial\mathcal{O} = (x_1\mathcal{O} \cup \cdots \cup x_n\mathcal{O}) \setminus \mathcal{O}$. After introducing new indeterminates c_{ij} for $1 \leq i \leq \mu$ and $1 \leq j \leq \nu$, we form the *generic $\mathcal{O}$-border prebasis* $G = \{g_1, \ldots, g_\nu\}$, where $g_j = b_j - \sum_{i=1}^{\mu} c_{ij}\, t_i$, and the *generic formal multiplication matrices* $\mathcal{A}_r = (a_{ij}^{(r)}) \in \mathrm{Mat}_\mu(K[c_{ij}])$, where

$$a_{ij}^{(r)} \;=\; \begin{cases} \delta_{im} & \text{if } x_r t_j = t_m \\ c_{im} & \text{if } x_r t_j = b_m \end{cases}$$

for $r = 1, \ldots, n$. It is well-known that the substitution of concrete values $c_{ij} \mapsto \gamma_{ij}$ with $\gamma_{ij} \in K$ into G yields an *$\mathcal{O}$-border basis* G_Γ, i.e. a system of generators of $I_\Gamma = \langle G_\Gamma \rangle$ such that the terms in $\mathcal{O}$ represent a vector space basis of P/I_Γ if and only if the commutators of $\mathcal{A}_1, \ldots, \mathcal{A}_n$ vanish at the point $\Gamma = (\gamma_{ij}) \in K^{\mu\nu}$. Hence the ideal $I(\mathbb{B}_\mathcal{O})$ generated by the entries of these commutators defined a subscheme $\mathbb{B}_\mathcal{O}$ of $\mathbb{A}^{\mu\nu}$ whose K-rational points correspond 1–1 to the 0-dimensional ideals of colength μ having an $\mathcal{O}$-border basis. This scheme is called the *$\mathcal{O}$-border basis scheme*, and given $\mathcal{O}$, its vanishing ideal is easy to compute. It has been studied previously in [1] and [2].

Having a good parametrization of all 0-dimensional ideals of a given colength invites the question how one can describe the loci of ideals with certain additional properties, e.g. algebraic properties such as defining a Gorenstein ring, or geometric properties such as the Cayley-Bacharach property. Based on the algorithms developed in [3] and on further characterizations, e.g. of the properties of being strictly Gorenstein or a strict complete intersection, we develop algorithms for computing the defining ideals of a number of subschemes of the border basis scheme $\mathbb{B}_\mathcal{O}$.

The first and most straightforward one is the locus of all 0-dimensional ideals I_Γ such that P/I_Γ is a (locally) Gorenstein ring. It was given in [3], Alg. 5.4 and uses the facts that this property is characterized by having a cyclic canonical module and that the multiplication maps on the canonical module are given by the transposes of the multiplication maps on the ring.

A more tricky case is the property of P/I_Γ to be a *strict Gorenstein ring*, i.e. of its graded ring $\mathrm{gr}_{\mathcal{F}}(P/I_\Gamma)$ with respect to the degree filtration $\mathcal{F}$ to be a Gorenstein local ring. In this case we can use the characterization which says that P/I_Γ has to have a symmetric affine Hilbert function and the Cayley-Bacharach property. However, both of these conditions require us to fix the Hilbert function.

The closed subscheme of $\mathbb{B}_\mathcal{O}$ whose K-rational points Γ correspond to rings P/I_Γ whose affine Hilbert function is dominated by a given Hilbert function $\mathcal{H}$ is called the *$\overline{\mathcal{H}}$-subscheme* of $\mathbb{B}_\mathcal{O}$ and is denoted by $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$. The open subscheme of $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$ whose K-rational points Γ correspond to rings P/I_Γ having exactly the affine Hilbert function $\mathcal{H}$ is denoted by $\mathbb{B}_\mathcal{O}(\mathcal{H})$. Both for $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$ and for the complement of $\mathbb{B}_\mathcal{O}(\mathcal{H})$ inside $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$ we provide explicit algorithms to calculate their defining equations. Thus we may operate on the set of ideals having a fixed Hilbert function.

The most useful of these sets is the *degree filtered $\mathcal{O}$-border basis scheme* $\mathbb{B}_\mathcal{O}^{\mathrm{df}}$ which corresponds to the Hilbert function of $\mathcal{O}$ itself. In this setting we provide explicit algorithms for calculating the locus of all points Γ such that P/I_Γ has the Cayley-Bacharach property, and then the locus corresponding to the strict Gorenstein rings P/I_Γ mentioned above.

Finally, we consider the locus corresponding to all strict complete intersection ideals I_Γ, i.e. to all such ideals for which the degree form ideal $\mathrm{DF}(I_\Gamma)$ is generated by a homogeneous regular sequence. To characterize this locus, we use a suitable version of an old result by Wiebe (see [4], Satz 3) which says that a local ring R with maximal ideal $\mathfrak{m}$ is a complete intersection if and only if the 0-th Fitting ideal of $\mathfrak{m}$ satisfies $\mathrm{Fitt}_0(\mathfrak{m}) \neq \langle 0 \rangle$. Based on a parametrization of all rings $P/\mathrm{DF}(I_\Gamma)$ using the *homogeneous $\mathcal{O}$-border basis scheme*, we succeed in constructing a version of Wiebe's result which works for families of 0-dimensional ideals and allows us to describe the locus of all strict complete intersections in the moduli space via explicit polynomial equations.

Keywords: border basis, Gorenstein ring, complete intersection

References

[1] M. KREUZER AND L. ROBBIANO, Deformations of border bases. *Coll. Math.* **59**, 275–297 (2008).

[2] M. KREUZER AND L. ROBBIANO, The geometry of border bases. *J. Pure Appl. Alg.* **215**, 2005–2018 (2011).

[3] M. KREUZER, L.N. LONG AND L. ROBBIANO, On the Cayley-Bacharach property. *arxiv:1804.09469* [math.AC] (2018).

[4] H. WIEBE, Über homologische Invarianten lokaler Ringe (in German). *Math. Ann.* **179**, 257–274 (1969).

[1]Faculty of Informatics and Mathematics
University of Passau
D-94030 Passau, Germany
martin.kreuzer@uni-passau.de,
nglong16633@gmail.com

[2]Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35
I-16146 Genova, Italy
lorobbiano@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Fast Gröbner basis computation and polynomial reduction in the generic bivariate case

Joris van der Hoeven[1], **Robin Larrieu**[1]

Let $A, B \in \mathbb{K}[X, Y]$ be two bivariate polynomials over an effective field $\mathbb{K}$, and let G be the reduced Gröbner basis of the ideal $I := \langle A, B \rangle$ generated by A and B with respect to the usual degree lexicographic order. Assuming A and B sufficiently generic, we design a quasi-optimal algorithm for the reduction of $P \in \mathbb{K}[X, Y]$ modulo G, where "quasi-optimal" is meant in terms of the size of the input A, B, P. Immediate applications are an ideal membership test and a multiplication algorithm for the quotient algebra $\mathbb{A} := \mathbb{K}[X, Y]/\langle A, B \rangle$, both in quasi-linear time. Moreover, we show that G itself can be computed in quasi-linear time with respect to the output size.

Keywords: Polynomial reduction, Gröbner basis, Complexity, Algorithm

References

[1] JORIS VAN DER HOEVEN; ROBIN LARRIEU, Fast Gröbner basis computation and polynomial reduction in the generic bivariate case. Preprint at `https://hal.archives-ouvertes.fr/hal-01770408/`

[2] JORIS VAN DER HOEVEN; ROBIN LARRIEU, Fast reduction of bivariate polynomials with respect to sufficiently regular Gröbner bases. Proceedings *ISSAC 2018* (to appear). Preprint at `http://hal.archives-ouvertes.fr/hal-01702547`.

[1]Laboratoire d'informatique de l'École polytechnique
LIX, UMR 7161 CNRS
Campus de l'École polytechnique
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau, France
`vdhoeven@lix.polytechnique.fr`
`larrieu@lix.polytechnique.fr`

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

De Nugis Groebnerialium 5: Noether, Macaulay, Jordan*

Teo Mora[1]

The true power of Lasker-Noether decomposition theorem grants that each ideal in a Noetherian ring has an irredundant (and reduced) representation as finite intersection of *irreducible* primary ideals and, in the polynomial ring over a field, there is an algorithm (due to Macaulay) which effectively computes such decomposition. Moreover, once a frame of coordinates is fixed, such decomposition is unique. I am wondering since years whether this result could allow to define (if and when it exists) an *intrinsic coordinate frame* for primary ideals. Recently I realized that generalized eigenvectors could be a potential solution, thus allowing me to give a potential definition.

In connection with Lasker-Noether primary decomposition, Emmy Noether stated [4] that

Definition 1 (Noether)**.** Let R be a commutative ring with unity and let $\mathfrak{a} \subset R$ be an ideal.

$\mathfrak{a}$ is said to be

- *reducible* if there are two ideals $\mathfrak{b}, \mathfrak{c} \subset R$ such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \mathfrak{b} \supset \mathfrak{a}, \mathfrak{c} \supset \mathfrak{a}$;
- *irreducible* if it is not reducible.

Proposition 2 (Lasker–Noether)**.** *In a Noetherian ring R each ideal $\mathfrak{f} \subset R$ is a finite intersection of irreducible ideals: $\mathfrak{f} = \cap_{i=1}^{r} \mathfrak{i}_i$.*

Definition 3 (Noether)**.** Let R be a Noetherian ring and $\mathfrak{f} \subset R$ an ideal. A representation $\mathfrak{f} = \cap_{i=1}^{r} \mathfrak{i}_i$, of $\mathfrak{f}$ as intersection of finite irreducible ideals is called a *reduced representation* if, for each $I, 1 \leq I \leq r$,

- $\mathfrak{i}_I \not\supseteq \bigcap\limits_{\substack{i=1 \\ i \neq I}}^{r} \mathfrak{i}_i$, and
- there is no irreducible ideal $\mathfrak{i}'_I \supset \mathfrak{i}_I$ such that $\mathfrak{f} = \left(\bigcap\limits_{\substack{i=1 \\ i \neq I}}^{r} \mathfrak{i}_i \right) \bigcap \mathfrak{i}'_I$. □

*This note was devised while attending to the CIRM, Luminy, *Workshop Symmetry and Computational*; thanks to the organizers for the hospitality and stimulation. I am also grateful to Elisa Gorla which pointed me to Jordan blocks and Michela Ceria for fruitable discussions.

Proposition 4 (Noether)**.** *In a Noetherian ring R, each ideal $\mathfrak{f} \subset R$ has a reduced representation as intersection of finite irreducible ideals.*

Let us denote $\mathcal{P} := K[X_1, \cdots, X_n]$ the polynomial ring over the field K and

$$\mathcal{T} := \{X_1^{a_1}, \cdots, X_n^{a_n} : (a_1, \cdots, a_n) \in \mathbb{N}\}.$$

Example 5 (Hentzelt). 1. The decompositions

$$(X^2, XY) = (X) \cap (X^2, XY, Y^\lambda), \text{ for each } \lambda \in \mathbb{N}, \lambda \geq 1,$$

where $\sqrt{(X^2, XY, Y^\lambda)} = (X, Y) \supset (X)$, show that embedded components are not unique; however, $(X^2, Y) \supseteq (X^2, XY, Y^\lambda)$, for each $\lambda > 1$, shows that (X^2, Y) is a reduced embedded irreducible component and that $(X^2, XY) = (X) \cap (X^2, Y)$ is a reduced representation.

2. The decompositions $(X^2, XY) = (X) \cap (X^2, Y + aX)$, for each $a \in \mathbb{Q}$, where $\sqrt{(X^2, Y + aX)} = (X, Y) \supset (X)$, and, clearly, each $(X^2, Y + aX)$ is reduced, show that also reduced representation is not unique; remark that, setting $a = 0$ we find again the decomposition $(X^2, XY) = (X) \cap (X^2, Y)$ found above.

This set of examples suggested Emmy Noether to intersect all irreducible components which share the same associated prime and to distinguish primaries between *embedded* and *isolated* in order to give her uniqueness result on irredundant primary representation.

Some time before, Macaulay [3], through his theory of *inverse systems* and *dialytic arrays* studied the inner structure of $(X_1, \ldots, X_n)$-primary ideals at the origin in the polynomial ring $K[X_1, \cdots, X_n] =: \mathcal{P}$ giving an efficient algorithm which later Gröbner [2, pp.177–178] realized was computing the reduced representation of a $(X_1, \ldots, X_n)$-primary ideal and which can be easily generalized to [5, II.Corollary 32.3.3] produce a reduced representation of each $(X_1, \ldots, X_n)$-closed ideal.

Example 6. Given the monomial ideal $I := (X^3, XY, Y^3)$ Macaulay starts with the functionals $M(t)(\cdot), t \in \mathcal{T}$ which associate to each polynomial the coefficient of t in its expansion, the *escalier* $\mathcal{T}/I$ and the "corners" X^3, Y^3 getting the two modules

$$\mathrm{Span}_K\{M(X^2), XM(X^2), X^2M(X^2)\} = \mathrm{Span}_K\{M(X^2), M(X), M(1)\}$$

and $\mathrm{Span}_K\{M(Y^2), YM(Y^2), Y^2M(Y^2)\} = \mathrm{Span}_K\{M(Y^2), M(Y), M(1)\}$ which are dual to the ideals (X^3, Y) and (X, Y^3) whence $I = (X^3, Y) \cap (X, Y^3)$.

Notwithstanding Hentzelt's example, Macaulay's solution in a sense is "unique"; namely it depends on a precise frame of coordinates, since each component is computed by Macaulay essentially by repeatedly multiplying some functionals by the variables.

Example 7. The ideal $(X_1, X_2)^2$ has all the irreducible decompositions

$$(X_1, X_2)^2 = ((aX + bY)^2, cX + dY) \cap (aX + bY, (cX + dY)^2), ad - cb = 1.$$

Example 8. Apparently, Example 7 is all one needs to dismiss the question posed on the title; however if we consider any linear form $\ell \in K[X_1, X_2, X_3]$ s.t. $\mathrm{Span}_K = \{X_1, X_2, \ell\} = \mathrm{Span}_K = \{X_1, X_2, X_3\}$ we realize that in the (X_1, X_2, X_3)-primary ideal

$$\begin{aligned} J &:= (X_1, X_2, X_3)^2 \cap (X_1, X_2, \ell^3) \\ &= (X_1^2, X_1X_2, X_2^2, X_1X_3, X_2X_3, X_3^3) \\ &= ((aX + bY)^2, cX + dY, X_3) \cap (aX + bY, (cX + dY)^2, X_3) \cap (X_1, X_2, \ell^3) \end{aligned}$$

the coordinate X_3 plays a rôle at least as the direction of the plane (X_1, X_2).

Let us consider a $(X_1, \ldots, X_n)$-primary ideal $I \subset K[X_1, \cdots, X_n] =: \mathcal{P}$, the unique order ideal $\mathbf{N}(I) \subset \mathcal{T}$ such that $\mathrm{Span}_K\{\mathbf{N}(I)\} = \mathcal{P}/I$, a linear form

$$\ell \in \mathrm{Span}_K\{X_1, \cdots, X_n\} =: \mathcal{B}_1,$$

the Auzinger-Stetter[1] matrix A describing the effect of the morphism $A \to A : f \mapsto \ell f$ on $\mathbf{N}(I)$ and its Jordan normal form J.

Denoting, for $k, 1 \leq k \leq \#\mathbf{N}(J)$, $\rho_k := \mathrm{rank}(A^{k-1}) - \mathrm{rank}(A^k)$, $\mu_0 := \rho_1$ and $\mu_i := \rho_i - \rho_{i+1}$ for each $i, 1 \leq i < l := max(k : \rho_k \neq 0)$. Note that $\mu_0 = \sum_{i>0} \mu_i = \#\mathcal{B}_1 = n$ is the number of Jordan blocks of J. Note also that the following conditions are equivalent

1. there are n values $i_1 > i_2 > \ldots > i_n$ with $\mu_{i_j} = 1$,
2. $\mu_i \in \{0, 1\}$ for each i.

If this happens we can choose n generalized eigenvectors v_j each of ranks i_j in a such way that the eigenvectors $w_j := A^{i_j - 1}v_j$ satisfy $\mathrm{Span}_K\{w_1, \cdots, w_n\} =: \mathcal{B}_1$ and we can inductively choose each w_j in such a way that the basis $\{w_1, \cdots, w_n\}$ is orthogonal.

Definition 9. If the conditions above are satisfied the ordered set $\{w_1, \cdots, w_n\}$ is called the *intrinsic coordinate frame* for the $(X_1, \ldots, X_n)$-primary ideal I.

Of course this definition requires to settle technical problems which Numerical Analysis can answer, starting from the crucial questions: is this frame "unique" and in which sense? ℓ must be "generic" in some sense, but in which sense? Example 8 suggests that we can assume to have ℓ in a Zariski open.

The other problem is to consider a $(X_1, \ldots, X_n)$-closed ideal I with the origin as singular point and study if the application of this tecnique to sufficiently many ideals $I \cap (X_1, \ldots, X_n)^d$ can impose an intrinsic coordinate frame at the singular point of I, following the track of computation for the ideal $I = (X_1^3 - X_1^2 - X_2^2)$ performed in [5, II.Examples 32.4.2,32.7.1].

Keywords: 0-dimensional primaries, primary decomposition, Jordan blocks

References

[1] W. AUZINGER; H.J. STETTER, An Elimination Algorithm for the Computation of all Zeros of a System of Multivariate Polynomial Equations. *I.S.N.M.* **86**, 11–30 (1988)

[2] W. GRÖBNER W., *Moderne Algebraische Geometrie II*. Bibliographische Institut, Mannheim, 1970.

[3] F. S. MACAULAY, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press, Cambridge, 1916.

[4] E. NOETHER, Idealtheorie in Ringbereichen. *Math. Annales* **83**, 25–66 (1921).

[5] T. MORA Solving Polynomial Equation Systems (4 Vols.). Cambridge Univ. Press, Cambridge, 2003–16.

[1]Department of Mathematics
University of Genoa
Via Dodecaneso 35
theomora@disi.unige.it

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Solving and bonding 0-dimensional ideals: Möller Algorithm and Macaulay Bases

Teo Mora[1]

Denote by $\mathcal{P} := \mathbf{k}[x_1, ..., x_n]$ the polynomial ring over the field $\mathbf{k}$, by $\bar{\mathbf{k}}$ the algebraic closure of $\mathbf{k}$, by $\mathbf{m} = (x_1, ..., x_n) \subset \mathcal{P}$ the maximal ideal at the origin and by

$$\mathcal{T} := \{x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n} \,|\, \gamma := (\gamma_1, ..., \gamma_n) \in \mathbb{N}^n\}$$

the semigroup of terms in $\mathcal{P}$ which is its "natural" basis as a $\mathbf{k}$-vector space.

The $\mathbf{k}$-vector space of the linear morphisms $L : \mathcal{P} \to \mathbf{k}$, $\hat{\mathcal{P}} = \mathrm{Hom}_{\mathbf{k}}(\mathcal{P}, \mathbf{k})$ has a natural structure as $\mathcal{P}$-module which is obtained by defining, for each $\ell \in \hat{\mathcal{P}}$ and $f \in \mathcal{P}$, $\ell \cdot f \in \hat{\mathcal{P}}$ as

$$g \mapsto (\ell \cdot f)(g) = \ell(fg), \forall g \in \mathcal{P}.$$

Macaulay [4, 5] under the notion of *inverse system* proposed a representation of $\hat{\mathcal{P}}$ as a series ring $\mathbf{k}[[x_1^{-1}, ..., x_n^{-1}]]$ and specialized his approach in order to describe, under the name of *Noetherian equations*, the structure of both $\mathbf{m}$-primary ideals at the origin and $\mathbf{m}$-closed* ideals. In order to do so he restricted himself to the polynomial ring

$$\mathcal{P} = \mathbf{k}[x_1, ..., x_n] \cong \mathbf{k}[x_1^{-1}, ..., x_n^{-1}] \subset \mathbf{k}[[x_1^{-1}, ..., x_n^{-1}]] = \hat{\mathcal{P}} = \mathrm{Hom}_{\mathbf{k}}(\mathcal{P}, \mathbf{k})$$

representing it as the $\mathbf{k}$-vector space $\mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ generated by the set $\mathbb{M} = \{M(\tau) : \tau \in \mathcal{T}\}$ of functionals bihortogonal to the set $\mathcal{T}$ defined by

$$M(\tau) : \mathcal{P} \to \mathbf{k}, \quad f = \sum_{t \in \mathcal{T}} c(f, t)t \mapsto c(f, t), \forall f \in \mathcal{P},$$

so that each polynomial $f \in \mathcal{P}$ is represented as $f = \sum_{\tau \in \mathcal{T}} M(\tau)\tau$. In order to impose a $\mathcal{P}$-module structure on it, he defined, for each $j, 1 \le j \le n$, the linear maps

$$\sigma_j : \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \to \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), \quad \tau \mapsto \sigma_j(M(\tau)) := \begin{cases} M(\omega) & \text{if } \tau = x_j\omega \\ 0 & \text{if } x_j \nmid \tau; \end{cases}$$

since it holds $\sigma_i\sigma_j = \sigma_j\sigma_i$ for each pair $1 \le i, j \le n$, this, for each $\upsilon = x_1^{\gamma_1} \cdots x_n^{\gamma_n} \in \mathcal{T}$, defines a unique map

$$\sigma_\upsilon := \sigma_1^{\gamma_1} \cdots \sigma_n^{\gamma_n} : \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \to \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), \quad \tau \mapsto \sigma_\upsilon(M(\tau)) := \begin{cases} M(\omega) & \text{if } \tau = \upsilon\omega \\ 0 & \text{if } \upsilon \nmid \tau. \end{cases}$$

*id est ideals $I \subset \mathcal{P}$ s.t. $I = \bigcup_d I + \mathbf{m}^d$.

Therefore for each $f = \sum_{t\in\mathcal{T}} c(f,t)t \in \mathcal{P}$ a map $\sigma_f : \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \to \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is uniquely defined as $\sigma_f = \sum_{t\in\mathcal{T}} c(f,t)\sigma_t$ and under this definition $\mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is naturally endowed with the $\mathcal{P}$-module structure defined by

$$\ell \cdot f := \sigma_f(\ell) \in \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), \forall \ell \in \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), f \in \mathcal{P}.$$

Definition 10. A vector subspace $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is called

- x_j*-stable* if for each $\ell \in \Lambda, \sigma_j(\ell) \in \Lambda$;
- *stable* if for each $\ell \in \Lambda$ and each $f \in \mathcal{P}, \sigma_f(\ell) \in \Lambda$. □

Lemma 11. *Any vector subspace $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is stable iff it is x_j-stable, for each j.*

Theorem 12. *Let $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \subset \hat{\mathcal{P}}$ be any finite dimensional* $\mathbf{k}$*-vector subspace. Then, the following conditions are equivalent:*

1. *Λ is stable.*
2. *the vector space $\mathfrak{I}(\Lambda) := \{f \in \mathcal{P} : \ell(f) = 0, \forall \ell \in \Lambda\} \subset \mathcal{P}$ is an ideal and $\mathfrak{I}(\Lambda) \subset \mathbf{m}$.*

Denoting, for each $\mathbf{k}$-vector subspace $P \subset \mathcal{P}$,

$$\mathfrak{M}(P) := \{\ell \in \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) : \ell(f) = 0, \forall f \in P\} \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$$

it holds

Theorem 13. *The mutually inverse maps $\mathfrak{I}(\cdot)$ and $\mathfrak{M}(\cdot)$ give a biunivocal, inclusion reversing, correspondence between the set of the* $\mathbf{m}$*-closed ideals $I \subset \mathcal{P}$ and the set of the stable* $\mathbf{k}$*-sub vector spaces $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$.* □

Gröbner[3] gave a natural description of each functional $M(\tau) \in \mathbb{M}$ in terms of differential operations, setting, for each $(i_1, \ldots, i_n) \in \mathbb{N}^n$, $\tau := x_1^{i_1} \ldots x_n^{i_n}$ and denoting

$$D(\tau) := D(i_1, \ldots, i_n) : \mathcal{P} \to \mathcal{P}$$

the differential operator $D(\tau) := D(i_1, \ldots, i_n) = \frac{1}{i_1! \cdots i_n!} \frac{\partial^{i_1+\cdots+i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}$, so that, for each $\tau \in \mathcal{P}$, it holds $M(\tau)(\cdot) = D(\tau)(\cdot)(0, \ldots, 0)$.

Gröbner's formulation has the only weakness of requiring that $(\mathbf{k}) = 0$, but this problem is trivially fixed using the Hesse derivates $D_i^{(j)}(x_i^m) = \begin{cases} \binom{m}{j} x^{m-j} & \text{if } m \geq j \\ 0 & \text{if } m < j \end{cases}$ thus obtaining $M(\tau)(\cdot) = D_1^{(i_1)} \cdots D_n^{(i_n)}(\cdot)(0, \ldots, 0)$.

Given a termordering $<$ on $\mathcal{T}$, for each $\ell = \sum_{\upsilon\in\mathcal{T}} \xi(\upsilon, \ell)\upsilon$ we denote

$$\mathbf{T}_<(\ell) := \min_< (\upsilon : \xi(\upsilon, \ell) \neq 0) .$$

Definition 14. [1] Let $I \subset \mathcal{P}$ be an $\mathbf{m}$-closed ideal. A $\mathbf{k}$-basis $\{\ell_1, \ell_2, \ldots, \ell_i, \ldots\}$ of the stable $\mathbf{k}$-sub vector space $\Lambda := \mathfrak{M}(I)$ is called the *Macaulay basis* of Λ w.r.t. a termordering $<$ if

- $\mathbf{T}_<\{\Lambda\} := \{\mathbf{T}_<(\ell_i)\} \subset \mathcal{T}\}$ is an order ideal;
- $\ell_i = M(\mathbf{T}_<(\ell_i)) + \sum_{v \in \mathcal{T} \setminus \mathbf{T}_<(\Lambda)} \xi(v, \ell_i) v$ for suitable $\xi(v, \ell_i) \in \mathbf{k}$ and for each i. □

Given a 0-dimensional ideal $I \subset \mathcal{P}$ there are different techniques for computing its roots $\mathfrak{Z}(I) \subset \bar{\mathbf{k}}^n$ (see [9, III]) and, for each such root $\mathsf{a} \in \mathfrak{Z}(I)$, the correlated primary component of I (see [9, II.ch.35]); given an $\mathbf{m}$-closed ideal through any finite (not necessarily Gröbner) basis, [7] (see also [1]) computes, for any $\delta \in \mathbb{N}$, the Macaulay basis of $\bigcup_{d \leq \delta} I + \mathbf{m}^d$.

The procedure given by Macaulay [5] allows to produce the irreducible reduced decomposition of any $\mathbf{m}$-primary ideal.

The converse problem can be stated as

> given a finite set $\mathcal{Z} \subset \mathbf{k}^n$ and, for each $\mathsf{a} = (a_1, \ldots, a_n) \in \mathcal{Z}$, denoting
>
> $$\lambda_{\mathsf{a}} : \mathcal{P} \to \mathcal{P} \quad f(x_1, \ldots, x_n) \mapsto f(x_1 + a_1, \ldots, x_n + a_n),$$
>
> a stable $\mathbf{k}$-sub vector spaces $\Lambda_{\mathsf{a}} \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ describe the 0-dimensional ideal $I = \bigcap_{\mathsf{a} \in \mathcal{Z}} \lambda_{\mathsf{a}}^{-1} (\mathfrak{I}(\Lambda_{\mathsf{a}}))$

Möller Algorithm [6] solves it; actually given any finite set of linearly independent functionals $\{\ell_1, \ldots, \ell_N\}$ properly ordered so that each sub vector space $L_i = \{\ell_1, \ldots, \ell_i\}, 1 \leq i \leq N$ is a $\mathcal{P}$-module so that each $I_i := \mathfrak{I}(L_i)$ is a 0-dimensional ideal, for each i returns the separators of the functionals L_i, the *Gröbner represantion* [9, II.29.3.3;III.pg.xvi] of each ideal I_i, producing in particular the order ideal (*escalier*) $\mathbf{N}(I_i)$ which is a $\mathbf{k}$-basis of the algebra $\mathcal{P}/I_i$ and also [8] the related Cerlienco–Mureddu Correspondence[†]

References

[1] M.E. ALONSO; M.G. MARINARI; T. MORA, The Big Mother of All the Dualities, II: Macaulay Bases. *J. AAECC* **17**, 409–451 (2006).

[2] M. CERIA; T. MORA Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game. This issue.

[3] W. GRÖBNER W., *Algebraische Geometrie II*. Bibliographische Institut, Mannheim, 1970.

[†] So in particular the results discussed in [2] hold for any 0-dimensional ideal.

[4] F. S. MACAULAY, On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers. *Math. Ann.* **74**,66–121 (1913).

[5] F. S. MACAULAY, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press, Cambridge, 1916.

[6] M.G. MARINARI; T. MORA; H.M. MÖLLER, Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *J. AAECC* **4**, 103-145 (1993).

[7] M.G. MARINARI; T. MORA; H.M. MÖLLER, On multiplicities in Polynomial System Solving. *Trans. AMS* **348**, 3283–3321 (1996).

[8] M.G. MARINARI; M.T. MORA, Cerlienco-Mureddu Correspondence and Lazard Structural Theorem. *Investication Operacional* **27**, 155-178 (2006).

[9] T. MORA Solving Polynomial Equation Systems (4 Vols.). Cambridge Univ. Press, Cambridge, 2003–16.

[1]Department of Mathematics
University of Genoa
Via Dodecaneso 35
theomora@disi.unige.it

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the computation of algebraic relations of bivariate polynomials

Simone Naldi[1], **Vincent Neiger**[1], and **Grace Younes**[2]

Computing algebraic relations (or syzygies) between multivariate polynomials is a central topic in computational commutative algebra. Given $f_1, \ldots, f_m \in K[X]$, $X = (X_1, \ldots, X_n)$, and a zero-dimensional ideal $I \subset K[X]$, this problem amounts to finding $p_1, \ldots, p_m \in K[X]$ satisfying

$$p_1 f_1 + \cdots + p_m f_m \in I.$$

More precisely, one goal is to compute a Gröbner basis of the module of all such relations. In some applications, for instance in decoding algorithms from coding theory, one just needs to compute one relation satisfying degree bounds which are given a priori.

A well known particular case is the computation of Padé approximants of polynomial functions $h \in K[X]$, namely $a, b \in K[X]$ satisfying $a = bh$ in the coordinate ring $K[X]/I$. This problem can be interpreted as a structured linear system of equations.

In the univariate case, iterative algorithms have been developed in [1, 6]. Similar algorithms appeared for the multivariate case for example in [2, 4], leading to complexity bounds that are cubic in the degree of I and linear in the number of variables.

For the computation of univariate relations, divide-and-conquer variants of the mentioned algorithms have been given in [1, 3, 5]. However, to the best of our knowledge no similar improvements have been obtained in multivariate settings. In this talk we will report on ongoing work aiming at algorithmic improvements in the bivariate case and for ideals I that have some special structure.

Keywords: Padé approximants, syzygies, structured matrices, divide and conquer

References

[1] BECKERMANN, B., LABAHN, G. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM Journal on Matrix Analysis and Applications*, 15(3), 804-823 (1994).

[2] P. FITZPATRICK, Solving a multivariable congruence by change of term order. *J. Symb. Comp.* **24** 575–589 (1997).

[3] GIORGI, P., JEANNEROD, C. P., VILLARD, G. On the complexity of polynomial matrix computations. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation* pp. 135-142 (2003, August).

[4] MARINARI, M. G., MOELLER, H. M., MORA, T. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing*, 4(2), 103-145 (1993).

[5] V. NEIGER, V.T. XUAN, Computing canonical bases of modules of univariate relations. *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, Kaiserslautern, Germany, July 2017.

[6] VAN BAREL, M., BULTHEEL, A. A general module theoretic framework for vector M-Padé and matrix rational interpolation. *Numerical Algorithms*, 3(1), 451-461 (1992).

[1]XLIM
Université de Limoges
123 avenue Albert Thomas - 87000, Limoges, France
simone.naldi@unilim.fr
vincent.neiger@unilim.fr

[2]UVSQ - Université de Versailles Saint-Quentin-en-Yvelines
55 avenue de Paris
78035 Versailles cedex, France
younessgrace@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computing Recurrence Relations of $n-$dimensional Sequences Using Dual of Ideals

Angelos Mantzaflaris[1], **Hamid Rahkooy**[2], **Éric Schost**[2]

We consider the problem of computing the ideal of linear recurrence relations of a sequence over $\mathbb{N}^n$. We call this ideal the annihilator of the sequence. We restrict ourselves to the case that the annihilator is $\mathfrak{m}-$primary, which allows us to assume that the values of the sequence is zero outside a finite set $\mathcal{M}$, hence the input is the values over $\mathcal{M}$. Our algorithm can easily be generalized into arbitrary number of sequences whose annihilator is zero-dimensional.

Berlekamp and Massey considered the problem for sequences over $\mathbb{N}$ and gave an algorithm for it in 1960s [2, 7]. Sakata generalized the problem into the sequences over $\mathbb{N}^n$ [10]. In terms of Macaulay's *Inverse System* [5], the annihilator is the orthogonal of the inverse system of a given element. In other words, the problem is to find the ideal, for which the dual module is given. Marinari, Mora, Möller and Alonso introduced algorithms for this duality problem [1, 6], considering it as a generalization of FGLM [4].

A first approach to solve this problem is to consider a recurrence relation with symbolic coefficients and plug in the sequence in order to obtain linear equations. This leads to solving a Hankel matrix of size $s = |\mathcal{M}|$. Let d be the dimension of the quotient of the polynomial ring with the annihilator, as a vector space, and δ be the size of the border of the annihilator. Faugere, et. al. in [3] consider $\mathcal{M}$ to be the set of tuples $(a_1, \cdots, a_n)$, with $a_1 + \cdots + a_n \leq t$, for some $t \in \mathbb{N}$, and give an algorithm of complexity $O(s^\omega + \delta d^\omega)$, where ω is the constant in the complexity of matrix multiplication. In a recent work, Mourrain presented an algorithm —in a more general setting for computing border basis— with complexity $O(nd^2s)$ [8].

Motivated by Mourrain's *Integration Method* [9] for fast computation of the dual of an $\mathfrak{m}-$primary ideal, we convert the problem of computing the annihilator into the problem of finding the dual of a certain ideal. Unlike all other algorithms, our algorithm essentially looks for the linear dependencies among the values of the sequence, going from the largest tuple in $\mathcal{M}$ to the smaller ones. The complexity of our algorithm is $O\left(n(s-d)^3 + n(s-d)C + ns\right)$, where C is the cost of the integrations done during the integration method. We present classes of sequences for which $s - d$ is small while s and d are large enough, hence our algorithm is faster than all above algorithms. We have implemented our algorithm in Maple and our experiments show drastic reduction in the size of the matrices when $s - d$ is small.

Keywords: Linear recurrent sequences; Berlekamp-Massey Algorithm; Sakata's Problem; 0-dimensional ideal; n-dimensional sequences; dual of ideals.

References

[1] M. E. ALONSO; M. G. MARINARI; T. MORA, The big mother of all dualities 2: Macaulay bases. *Applicable Algebra in Engineering, Communication and Computing* **17**(6), 409–451 (2006).

[2] E. BERLEKAMP, Nonbinary bch decoding. *IEEE Transactions on Information Theory* **14**(2), 242–242 (1968).

[3] J. BERTHOMIEU; B. BOYER; J-C. FAUGÈRE, Linear algebra for computing gröbner bases of linear recursive multidimensional sequences. *ournal of Symbolic Computation* **83**(Supplement C) 36– 67 (2017).

[4] J. C. FAUGÈRE; P. GIANNI; D. LAZARD; T. MORA, Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation* **16**(4), 329–344 (1993).

[5] F. S. MACAULAY, *The Algebraic Theory of Modular Systems*. Cambridge mathematical library. Cambridge University Press, Cambridge, New York, Melbourne, 1994.

[6] M. G. MARINARI; H. M. MÖLLER; T. MORA, Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing* **4**(2), 103–145 (1993).

[7] J. MASSEY, Shift-register synthesis and bch decoding. *IEEE Transactions on Information Theory* **15**(1), 122–127 (1969).

[8] B MOURRAIN, Fast algorithm for border bases of artinian gorenstein algebras. In *International Symposium on Symbolic and Algebraic Computation*, M. Burr (eds.), 333–340, ACM, New York, 2017.

[9] B. MOURRAIN Isolated points, duality and residues. *Journal of Pure and Applied Algebra* **117 & 118**, 469–493 (1997).

[10] S. SAKATA Extension of the Berlekamp-Massey algorithm to N dimensions. *Information and Computation* **84**(2), 207–239 (1990).

[1]Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Linz, Austria
angelos.mantzaflaris@oeaw.ac.at

[2]Cheriton School of Computer Science
University of Waterloo
Canada
hamid.rahkooy@uwaterloo.ca
eschost@uwaterloo.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Special Properties of Zero-Dimensional Ideals: new Algorithms

Lorenzo Robbiano[1]

An affine 0-dimensional K-algebra is a ring of type P/I where K is a field, I is an ideal in $P = K[x_1, \ldots, x_n]$, and $\dim_K(P/I) < \infty$. In this talk some features of 0-dimensional affine K-algebras will be investigated: having the Cayley-Bacharach property, being locally Gorenstein, and being locally a complete interesection. In particular, the history of these properties and the modern approach via computational methods will be discussed.

Let us have a better look at the content of the presentation.

In book [2] we construct the theory of commuting families of endomorphisms of a finite dimensional K-vector space V, i.e., of families of endomorphisms of V which commute pairwise. In particular, we transfer the concept of commendability from a single endomorphism to a commuting family. It turns out that is strong enough for a fundamental theorem: a family is commendable if and only if V is a cyclic module with respect to the dual family. As abstract this may seem, it is the heart of some of the most powerful algorithms. The reason is that a zero-dimensional affine algebra R over a field K is identified with a commuting family via its multiplication family $\mathcal{F}$. This identification brings the extensive linear algebra preparations to fruition, and surprising connections between the two fields appear: the generalized eigenspaces of $\mathcal{F}$ are the local factors of R, the joint eigenvectors of $\mathcal{F}$ are the separators of R, there is a commendable endomorphism in $\mathcal{F}$ if and only if R is curvilinear, and the family $\mathcal{F}$ is commendable if and only if R is a *locally Gorenstein ring*. From this link a beautiful algorithm can be constructed which checks whether a zero-dimensional affine algebra is locally Gorenstein or not.

The notion of *complete intersection subscheme* is ubiquitous in Algebraic Geometry and Commutative Algebra where it takes the name of *ideal generated by a regular sequence*. Surprisingly, an old result by Wiebe (see [6]) can be successfully used to check whether an affine 0-dimensional local K-algebra is a complete intersection or not. And the full process is algorithmic.

The history of the *Cayley-Bacharach property (CBP)* goes back to Pappus Alexandrinus (ca. 320) and keeps going on. Some steps and turns will be illustrated. Recently, it became clear that, in order to study general versions of the CBP, it is preferable to formulate it as a property of the respective coordinate rings rather than sets of points or 0-dimensional schemes. In this vein, we defined in [2] the CBP for 0-dimensional affine algebras with a fixed presentation with arbitrary K and linear

maximal ideals, and provided several algorithms to check it. A couple of years ago the most general definition of the CBP to date was given by Long in [5] where he considered it for presentations of arbitrary 0-dimensional affine algebras over arbitrary base fields. The definition in [5] and a clever use of teh canonical module is the starting point of [3] where we study this very general version of the CBP and find efficient algorithms for checking it.

All the examples mentioned in the talk were computed with CoCoA (see [1]).

Keywords: Cayley-Bacharach, Gorenstein, canonical module, complete intersection

References

[1] J. Abbott, A.M. Bigatti, L. Robbiano, *CoCoA: a system for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it`

[2] M. Kreuzer, L. Robbiano, COMPUTATIONAL LINEAR AND COMMUTATIVE ALGEBRA,
Springer 2016

[3] M. Kreuzer, L. N. Long, L. Robbiano, *On the Cayley-Bacharach Property* Preprint (2017).

[4] M. Kreuzer, L. N. Long, L. Robbiano, *Subschemes of the Border Basis Scheme*, Preprint (2018)

[5] L.N. Long, Various differents for 0-dimensional schemes and appplications, dissertation, University of Passau, Passau, 2015.

[6] H. Wiebe, über homologische Invarianten lokaler Ringe, Math. Ann. **179** (1969), 257-274.

[1]Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35, 16146 Genova
`lorobbiano@gmail.com`

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Signature-based Criteria for Computing Weak Gröbner Bases over PIDs

Thibaut Verron[1], **Maria Francis**[1]

The theory of Gröbner bases was introduced by Buchberger in 1965 [2] and has since become a fundamental algorithmic tool in computer algebra. Over the past decades, many algorithms have been developed to compute Gröbner bases more and more efficiently. The latest iteration of such algorithms is the class of signature-based algorithms, which introduce the notion of signatures and use it to detect and prevent unnecessary or redundant reductions. This technique was first introduced for Algorithm F5 [5], and there have been many research works in this direction [3].

All these algorithms are for ideals in polynomial rings over fields. Gröbner bases can be defined and computed over commutative rings [1, Ch. 4], and can be used in many applications [7]. An important particular case is that where the coefficient ring is a Principal Ideal Domain (PID), for example $\mathbb{Z}$ or the ring of univariate polynomials over a field.

If the coefficient ring is not a field, there are two ways to define Gröbner bases, namely weak and strong bases. Strong Gröbner bases ensure that normal forms can be computed as in the case of fields. But computing a strong Gröbner basis is more expensive than a weak one, and if the base ring is not a Principal Ideal Domain (PID), then some ideals exist which do not admit a strong Gröbner basis. On the other hand, weak Gröbner bases, or simply Gröbner bases, always exist for polynomial ideals over a Noetherian commutative ring. They do not necessarily define a unique normal form, but they can be used to decide ideal membership.

Recent works have focused on generalizing signature-based techniques to Gröbner basis algorithms over rings. First steps in this direction, adding signatures to a modified version of Buchberger's algorithm for strong Gröbner bases over Euclidean rings [6], were presented in [4]. The paper proves that a signature-based Buchberger's algorithm for strong Gröbner bases cannot ensure correctness of the result after encountering a "signature-drop", but can nonetheless be used as a prereduction step in order to significantly speed up the computations.

Here we consider the problem of computing a weak Gröbner basis of a polynomial ideal with coefficients in a PID, using signature-based techniques. The proof-of-concept algorithm that we present is adapted from that the general algorithm due to Möller [8], which considers combinations and reductions by multiple polynomials at once. The way the signatures are ordered ensures that no reductions leading to signature-drops can happen. In particular, we could prove that the algorithm terminates and computes a signature Gröbner basis with elements ordered with non-decreasing signatures. This property allows us to examine classic signature-based

criteria, such as the syzygy criterion, the F5 criterion and the singular criterion, and show how they can be adapted to the case of PIDs. In particular, when the input forms a regular sequence, the algorithm performs no reductions to zero.

We have written a toy implementation in Magma of the algorithms presented, with the F5 and singular criteria. Möller's algorithm, without signatures, works for polynomial systems over any Noetherian commutative ring. The signature-based algorithm is only proved to be correct and to terminate for PIDs, but with minimal changes, it can be made to accomodate inputs with coefficients in a more general ring. Interestingly, early experimental data with coefficients in a multivariate polynomial ring (a Unique Factorization Domain which is not a PID) suggest that the signature-based algorithm might work over more general rings than just PIDs.

Keywords: Gröbner bases, Signature-based algorithms, Principal Ideal Domains

References

[1] ADAMS, W. & LOUSTAUNAU, P. (1994). *An Introduction to Gröbner Bases*. American Mathematical Society.

[2] BUCHBERGER, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. Ph.D. thesis, University of Innsbruck, Austria.

[3] EDER, C. & FAUGÈRE, J.-C. (2017). A Survey on Signature-based Algorithms for Computing Gröbner Bases. *Journal of Symbolic Computation* **80**, 719–784.

[4] EDER, C., PFISTER, G. & POPESCU, A. (2017). On Signature-Based Gröbner Bases over Euclidean Rings. In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17. New York, NY, USA: ACM.

[5] FAUGÈRE, J. C. (2002). A New Efficient Algorithm for Computing GrÖbner Bases without Reduction to Zero (F5). In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02. New York, NY, USA: ACM.

[6] LICHTBLAU, D. (2012). Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.* **56**(1), 177–194 (2013).

[7] LICHTBLAU, D. (2013). Applications of Strong Gröbner Bases over Euclidean Domains. *Int. J. Algebra* **7**(5-8), 369–390.

[8] MÖLLER, H. M. (1988). On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation* **6**(2-3), 345–359.

[1]Institute for Algebra
Johannes Kepler University
4040 Linz, Austria
thibaut.verron@jku.at
maria.francis@jku.at