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

Michela Ceria and Teo Mora

Abstract. In 1990 Cerlienco and Mureddu gave a combinatorial iterative algorithm which, given an ordered set of points, returns the lexicographical Gröbner escalier of the ideal of these points. There are many alternatives to this algorithm; the most efficient is the Lex Game, which is not iterative on the points, but its performances are definitely better.
In this paper, we develop an iterative alternative to Lex Game algorithm, whose performances are very near to those of the original Lex Game, by means of the Bar Code, a diagram which allows to keep track of information on the points and the corresponding monomials, that are lost and usually recomputed many times in Cerlienco-Mureddu algorithm. Using the same Bar Code, we will also give an efficient algorithm to compute squarefree separator polynomials of the points and the Auzinger-Stetter matrices with respect to the lexicographical Gröbner escalier of the ideal of the points.

Extended abstract

In 1990 Cerlienco and Mureddu [5, 6, 7] 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 [12, 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 $\mathcal{O}\left(n^2 N^2\right)$, 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 $\mathsf{N}(I(\mathbf{X}))$ 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 $\underline{\mathbf{Y}} := [P_1, ..., P_N, Q]$,

- $\mathsf{N}(I(\mathbf{Y})) = \mathsf{N}(I(\mathbf{X})) \sqcup \{\tau\}$,
- $\Phi_{\underline{\mathbf{Y}}}(P_i) = \Phi_{\underline{\mathbf{X}}}(P_i)$ for all i and $\tau = \Phi_{\underline{\mathbf{Y}}}(Q)$.

In order to produce the lexicographical Gröbner escalier with a better complexity, [8] 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, $\mathcal{O}(nN + N\min(N, nr))$, where $r < n$ is the maximal number of edges from a vertex in the point tree, but in order to obtain it, [8] 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 $<$, 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 s.t. $f_i(P_j) = \delta_{ij}$.
Later Möller [11] extended the same algorithm to any finite set of functionals defining a 0-dimensional ideal, thus absorbing also the FGLM-algorithm and, on the other side, proving that Buchberger-Möller algorithm has the FGLM-complexity $\mathcal{O}(n^2N^3f)$ where f is the avarage cost of evaluating a functional at a term[1].
Möller [11] gave also an alternative algorithm (*Möller algorithm*) which, for any term-ordering $<$ on $\mathcal{T}$, given an ordered set of points[2] $[P_1, ..., P_N] \subset \mathbf{k}^n$, 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. $q_i(P_j) = \delta_{i,j}$
- 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 corresondence.

Later, Mora [12, II,29.4] remarked that, since the complexity analisis of both Buchberger-Möller and Möller algorithm were assuming to perform Gaussian reduction on an N-square matrix and to evaluate each monomial in the set

$$\mathsf{B}(I(\mathbf{X})) := \{\tau x_j, \tau \in \mathsf{N}(I(\mathbf{X}_\sigma)), 1 \leq j \leq n\}$$

[1]A more precise evaluation was later given by Lundqvist[9], namely

$$\mathcal{O}(\min(n, N)N^3 + nN^2 + nNf + \min(n, N)N^2 f).$$

[2]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.

over each point $P_i \in \mathbf{X}$, within that complexity one can use all the information which can be deduced by the computations $\tau(P_i), \tau \in \mathsf{B}(I(\mathbf{X})), 1 \le i \le N$; he therefore introduced the notion of ***structural description*** of a 0-dimensional ideal [12, 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 degrobnerizing 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* [12, II.29.3.3] *id est* the assignment of

- a $\mathbf{k}$-linearly independent ordered set $[q_1, \ldots, q_N] \subset \mathcal{P}/I$
- n N-square matrices $\left(a_{lj}^{(h)}\right), 1 \le h \le n$,

which satisfiy

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

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 $\sigma \le N$

- the lexicographical Gröbner escalier $\mathsf{N}(I(\mathbf{X}_\sigma))$, the related Cerlienco-Mureddu corresondence,
- a family of squarefree separators for $\mathbf{X}_\sigma$,
- the n N-square Auzinger-Stetter matrices $\left(a_{lj}^{(h)}\right), 1 \le h \le n$, which satisfy condition 2. above with respect the linear basis $\mathsf{N}(I(\mathbf{X}_\sigma))$.

The advantage is that, any time 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 intrinsecally 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, 4], essentially a reformulation of the point trie which describes in a compact way the combinatorial strucure of a (non necessarily 0-dimensional) ideal; the Bar Code allows to remember and reed those data which Cerlienco-Mureddu algorithm is forced to inductively recompute. Actually, once the point trie is computed as in [8] 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 obtain using Lagrange interpolation via data easily deduced from the point trie as suggested in [8, 9] with complexity $\mathcal{O}(N \cdot \min(N, nr)$.

The computation of the Auzinger-Stetter matrices is based on Lundqvist result [10, Lemma 3.2] and can be inductively performed with complexity[3] $\mathcal{O}\left(N \cdot (nN^2)\right)$.

References

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

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

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

[4] Ceria, M., *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets.*, submitted

[5] Cerlienco L., Mureddu M., *Algoritmi combinatori per l'interpolazione polinomiale in dimensione* ≥ 2, preprint (1990).

[6] Cerlienco L., Mureddu M., *From algebraic sets to monomial linear bases by means of combinatorial algorithms*, Discrete Math. 139, $73 - 87$.

[7] Cerlienco L., Mureddu M., *Multivariate Interpolation and Standard Bases for Macaulay Modules*, J. Algebra 251 (2002), $686 - 726$.

[8] Felszeghy B., Ráth B., Rónyai L., *The lex game and some applications*, J. Symbolic Computation 41 (2006), $663 - 681$.

[9] Lundqvist S., *Complexity of comparing monomials and two improvements of the BM-algorithm.* L. N. Comp. Sci. 5393 (2008), 105–125, Springer

[10] Lundqvist S., *Vector space bases associated to vanishing ideals of points*, Journal of Pure and Applied Algebra, 214, Issue 4, (2010), pagg $309 - 321$.

[11] Marinari M.G, Mora T., Moeller H.M., *Gröbner bases of ideals defined by functionals with an application to ideals of projective points* , Appl. Algebra Engrg. Comm. Comput. 4 (1993), 103-145.

[12] Mora T., *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016).

Michela Ceria
Department of Computer Science University of Milan Milano, Italy
e-mail: `michela.ceria@gmail.com`

Teo Mora
Department of Mathematics University of Genoa Genoa, Italy
e-mail: `theomora@disi.unige.it`

[3]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 $\mathcal{O}\left(N^\omega\right), \omega < 2.39$.