# Fast construction of a lexicographic Gröbner basis of the vanishing ideal of a set of points

X. Dahan[1]

[1] *Ochanomizu University, Japan, dahan.xavier@ocha.ac.jp, xdahan@gmail.com*

**Problem** Given a set $V$ of Zariski-closed points lying in $\bar{k}^n$, $\bar{k}$ an algebraic closure of a base field of interest $k$, its *vanishing ideal* $I(V) \subset k[X_1,\ldots,X_n]$ is the radical, 0-dimensional ideal of polynomials vanishing on $V$. We are interested in constructing a minimal lexicographic Gröbner basis $\mathscr{G}$ of $I = I(V)$.

**Result** The main outcome is Result 1. below. In HPC, a complexity analysis often precedes an implementation, and a challenge is indeed that benchmarks meet the expected complexity bounds. This is where lies this work (A preliminary implementation is available in Maple, but cannot be qualified as HPC currently).

*Notations* Lex, LexGB stands for lexicographic and lexicographic Gröbner basis respectively. Given a set $E \subset k[X_1,\ldots,X_n]$, then $E_{\leq \ell}$ denotes the set $E \cap k[X_1,\ldots,X_\ell]$.

1. There is a minimal lexicographic Gröbner basis $\mathscr{G}$ whose any of its polynomial can be computed in $O(\mathsf{A}(D_1) + \mathsf{A}(D_2) + \cdots + \mathsf{A}(D_n))$ arithmetic operations where $D_i = |V_{\leq i}| = \dim_k(k[X_1,\ldots,X_i]/I_{\leq i})$, and $\mathsf{A}(d)$ is the number of arithmetic operations over $k$ necessary to build Lagrange idempotents of $d$ points by using sub-product tree techniques ($\mathsf{A}(d) = \mathsf{M}(d)\log(d)$. Using Schönhage-Strassen fast multiplication one has $\mathsf{M}(d) = O(d\log(d)\log\log(d))$, or $\mathsf{M}(d) = d^2$ using naive polynomial multiplication).
2. the polynomials in $\mathscr{G}$ present a special structure, sort of redundant factors that allows to recycle already computed polynomials and Lagrange cofactors (and those computed in the sub-product trees) to considerably lower the number of arithmetic operations to compute new polynomials in $\mathscr{G}$.
3. Any polynomial in $\mathscr{G}$, say w.l.o.g. in $k[X_1,\ldots,X_n] \setminus k[X_1,\ldots,X_{n-1}]$, verifies a generalization of Gianni-Kalkbrener theorem: if $\alpha \in V_{\leq \ell}$ is such that $\deg_{X_{\ell+1}}(g(\alpha, X_{\ell+1},\ldots,X_n)) < \deg_{X_{\ell+1}}(g)$, then $g(\alpha, X_{\ell+1},\ldots,X_n) = 0$.
4. $\mathscr{G}$ is not the reduced Gröbner basis in general, hence has more coefficients, but its coefficients are smaller.
5. to $V$, we first build its *decomposition points tree* $\mathscr{T}(V)$. The *arithmetic* complexity for solving "Problem" depends only of the shape of this tree (of course

not the case for the bit complexity where the bit-size of the input points matters also).

**Brief overview of previous works** The above results are related to a number of previous works. We only refer to the most relevant ones that put into perspective the above statements. The numbering below refers to that of above.

1. Lederer [10] who has produced the most accomplished interpolation formulas focuses on the *reduced* Gröbner basis, which complicates his task quite considerably. This leaves a sharp complexity analysis quite difficult — indeed there is none; this stems for the fact that many additional polynomials must be computed on demand to cancel too large monomials. The reduced lexGB has a less satisfactory specialization property (see [1, 8]).

Before it was understood that the configuration of points in $V$ could give the set of standard monomials for the lexicographic oder (Cf. [3, 13, 6, 5]), algorithms based on linear algebra were predominant. They give roughly an $O(nD^3)$ [2, 14] arithmetic cost (but are *not* constrained to the lex order).

A related problem concerns the computation of a separating basis of the vector space $k[X_1,\dots,X_n]/I$. By "separating" we mean polynomials $\{p_v\}_{v\in V}$ such that $p_v(w) = \delta_{vw}$ (Kronecker symbol). Such a basis is closely related to multivariate Lagrange bases: Lundqvist [12] claims a cost of $O(D^2)$ points, but using fast interpolation it can be reduced to a complexity similar to that stated in Result 1. above. As for Hermite interpolation, in [11] linear algebra exploits the possibly very low displacement rank of the interpolating matrix to propose $O((\tau+3)D^2)$ (for Vandermonde we have $\tau = 2$ hence of the same order of Lagrange interpolation with naive multiplication).

2. Starting with Lazard's structural theorem ([9], lexGB in two variables), several authors have shown that a somewhat comparable result holds for more than two variables (to cite a few [13], and implicitly in [5, 10, 6]), at least in the radical 0-dimensional case. However, few, if none, considered the relationship between factors of two different polynomials in $\mathscr{G}$. This is a key point to recycle computations and to dramatically decrease the complexity, even if it is not easy to quantify.

3. The stability of Gröbner bases under specialization refers to the fact that a specialized Gröbner basis remains a Gröbner basis of the specialized ideal. Beyond the seminal Gianni-Kalkbrener result [7], Becker [1] then Kalkbrener [8] showed that whenever a degree decrease occurs after specialization, then the polynomial reduces to zero modulo the other polynomials. As stated, the specific Gröbner basis that we construct verifies a stronger property: no degree decrease, or else it specializes to zero, as in Gianni-Kalkbrener's theorem.

4. The maximal bit-size among all coefficients of polynomials appearing in $\mathscr{G}$ can be estimated to be *roughly* in $O(nD^2h^2)$ where $h$ is the maximal bit-size of the components of input points. This strategy follows that of [4]. Again, obtaining such a sharp result for the reduced lexGB is not easy.

5. this is interesting if we see the formula constructing the basis $\mathscr{G}$ as an algebraic circuit that computes the polynomials in $\mathscr{G}$. This circuit depends only of the shape of the tree.

**Implementation** We have implemented *naively* the interpolation formula that computes $\mathscr{G}$ in Maple and will show experimental results that illustrate all the points mentioned above.

## References

[1] T. Becker. Gröbner bases versus *D*-Gröbner bases, and Gröbner bases under specialization. *Applicable Algebra in Engineering , Communications and Computing*, 5:1–8, 1994.

[2] B. Buchberger and H. Möller. The construction of multivariate polynomials with preassigned zeros. In *Lecture Notes in Computer Science (EUROCAM'82)*, volume 144, pages 24–31, London, UK, 1982.

[3] L. Cerlienco and M. Mureddu. From algebraic sets to monomial linear bases by means of combinatorial algorithms. *Discrete Mathematics*, 139(1-3):73–87, 1995.

[4] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 103–110. ACM Press, 2004.

[5] B. Felszeghy, B. Ráth, and L. Rónyai. The lex game and some applications. *J. of Symbolic Comput.*, 41(6):663 – 681, 2006.

[6] S. Gao, V. Rodrigues, and J. Stroomer. Gröbner basis structure of finite sets of points. http://www.math.clemson.edu/~sgao/pub.html, 2003. Preprint (16 pages).

[7] P. Gianni. Properties of Gröbner bases under specialization. In J.H. Davenport, editor, *In Proc. of EUROCAL'87*, Lecture Notes in Computer Science (378), pages 293–297. Springer, Berlin, 1987.

[8] M. Kalkbrener. On the stability of Gröbner bases under specialization. *J. Symbolic Comput.*, 24(2):51–58, 1997.

[9] D. Lazard. Ideal bases and primary decomposition: case of two variables. *J. Symbolic Comput.*, 1(3):261–270, 1985.

[10] M. Lederer. The vanishing ideal of a finite set of closed points in affine space. *J. of Pure and Applied Algebra*, 212:1116–1133, 2008.

[11] Na Lei, Yuan Teng, and Yu-xue Ren. A fast algorithm for multivariate hermite interpolation. *Applied Mathematics-A Journal of Chinese Universities*, 4(29):438–454, 2014.

[12] Samuel Lundqvist. Vector space bases associated to vanishing ideals of points. *Journal of Pure and Applied Algebra*, 214(4):309 – 321, 2010.

[13] M. G. Marinari and T. Mora. A remark on a remark by Macaulay or enhancing Lazard structural theorem. *Bull. Iranian Math. Soc.*, 29(1):1–45, 85, 2003.

[14] M.G. Marinari, H. M. Moeller, and 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.