Möller's Algorithm

Teo Mora (theomora@disi.unige.it)

Duality was introduced in Commutative Algebra in 1982 by the seminal paper [14] but the relevance of this result became clear after

– the same duality exposed in [14] was indipendently applied in [5, 28] to produce an algorithm for solving any squarefree 0-dimensional ideal $\mathsf{I} \subset K[X_1, \ldots, X_n]$ and

– the algorithm developed in [14] was improved in [18] and applied in order to solve the FGLM-problem;

– the ideas of [14] and [18] were merged in [26] (see also [22]) proposing an algorithm which produces the Gröbner basis of an affine ideal $\mathsf{I} = \cap_{i=1}^{r} \mathfrak{q}_i \subset K[X_1, \ldots, X_n]$, where each $\mathfrak{q}_i$ is a primary ideal at an algebraic point, equivalently given by its inverse system, or Gröbner basis, or even any basis (see [27]).

This led to formalize under the label of *Möller's Algorithm* [2], the algorithm proposed in [14, 19, 18, 26] which solves the following

Problem 1. *Let*

- $\mathcal{P} := k[X_1, \ldots, X_n]$ *the polynomial ring over a field* k*,*
- $\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}$,
- $\mathcal{P}^*$ *the* $\mathcal{P}$*-module of the* k*-linear functionals over* $\mathcal{P}$*.*

Given a finite set $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ *of linearly independent* k*-linear functionals such that* $\mathsf{I} := \{f \in \mathcal{P} : \ell_i(f) = 0, \forall i\}$ *is a zero-dimensional ideal and a term-ordering* $<$*, to compute*

- *the Gröbner basis of* I *wrt* $<$*;*
- *the corresponding Gröbner escalier* $\mathbf{N}_<(\mathsf{I}) \subset \mathcal{T}$*;*
- *a set* $\mathbf{q} := \{q_1, \ldots, q_s\} \subset \mathcal{P}$ *which is triangular to* $\mathbb{L}$ *and satisfiles* $\mathrm{Span}_k(\mathbf{q}) = \mathrm{Span}_k(\mathbf{N}_<(\mathsf{I})) \cong \mathcal{P}/\mathsf{I}$*;*

- *the square matrices* $\left(a_{lj}^{(h)}\right)$ *defined by the equalities*

$$X_h q_l = \sum_j a_{lj}^{(h)} q_j, \bmod \mathsf{I}, \forall l, j, h, 1 \leq l, j \leq s, 1 \leq h \leq n.$$

The most relevant application of Möller's Algorithm are Multivartiate Lagrange Interpolation (where the functionals are evaluations at points) and the solution of the

Problem 2 (FGLM Problem). *Given*

- *a termordering* $<$ *on* $\mathcal{T}$ *,*
- *a zero-dimensional ideal* $\mathsf{I} \subset \mathcal{P}$*, and*
- *its reduced Gröbner basis* $G_{\prec}$ *w.r.t. the term-ordering* $\prec$*,*

deduce the Gröbner basis $G_{<}$ *of* I *w.r.t.* $<$*.*

The importance of the FGLM-Problem is based on the well-known fact that Gröbner bases wrt a lexicographical ordering $<$ have elimination properties crucial into most of the solving algorithms, like Gianni-Kalkbrener [20, 21] and triangular sets [23, 24, 3, 4], but are very hard to be computed, and on the less known fact that degrevlex is "optimal" [7].

A sort of FGLM-like algorithm for changing basis is already found in [12, 13] and later in [31]; but already Todd-Coxeter Algorithm [32] can be interpreted (see [29]) as an instance of Möller's Algorithm.

Möller's Algorithm solves the FGLM-Problem only for 0-dimensional ideals; [25] extends it to multidim. ideals but the performarce is poor. The same holds for the Gröbner Walk Algorithm [17]. At the present state-of-the-art, the most efficient solution of the FGLM-Problem is definitely Traverso's Hilbert Driven [34] but recently appeared new promising proposals [6, 30].

In an informal talk at MEGA-92, Traverso [33] proposed to use the structure of a 0-dimensional ideal $\mathsf{I} \subset K[X_1, \ldots, X_n]$, which is produced by Möller's Algorithm, in order to reduce its algebraic operations to linear algebra operations; this led to the notions [2] of *border basis, Gröbner and linear representations, Gröbner description* of a 0-dimensional ideal.

Möller's Algorithm has been generalized to projective points [1] (for a similar, but different approach, see [15, 16]) and to non-commutative polynomial rings [8].

The specialization of Möller's Algorithm to *binomial* ideals led promising results in decoding linear codes [9, 10, 11].

References

[1] Abbott J.; Bigatti A.; Kreuzer M.; Robbiano L. Computing Ideals of Points. *J. Symb.Comp.* , **30** (2000), 341–356

[2] Alonso M.E., Marinari M.G., The big Mother of all Dualities: Möller Algorithm, *Comm. Alg.* (2003), 374–383

[3] Aubry P, Lazard D., Moreno Maza M., On the theories of triangular sets, *J. Symb. Comp.* **28** (1999), 105–124.

[4] Aubry P., Moreno Maza M., *Triangular Set for Solving Polynomial Systems: A Comparative Implementation of Four Methods*, J. Symb. Comp. **28** (1999), 125–154

[5] Auzinger, W., Stetter, H.J. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Internat. Schriftenreihe Numer. Math. 86*, Birkhäuser, **1988**; 11–30.

[6] Basiri A., Faugère J.-C., Changing the ordering of Gröbner Bases with LLL: Case of Two Variables, *Proc. ISSAC'03* (2003) 23-28

[7] Bayer D., Stillman M., A Theorem on Refining Division Orders by the Reverse Lexicographic Order, *Duke J. Math.* **55** (1987), 321–328.

[8] Borges-Trenard M.A., Borges-Quintana M., Computing Gröbner Bases by FGLM Techniques in a Noncommutative Settings.*J. Symb.Comp.* , **30** (2000), 429–449

[9] M. Borges-Quintana, M. A. Borges-Trenard, E. Martinez-Moro A general framework for applying FGLM techniques to linear codes Accepted at *AAECC 16* http://arxiv.org/abs/math.AC/0509186

[10] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, E. Martinez-Moro Groebner bases and combinatorics for binary codes http://arxiv.org/abs/math.CO/0509164

[11] M. Borges-Quintana, M. Borges-Trenard, E. Martinez-Moro On a Grobner bases structure associated to linear codes Acepted at *Journal of Discrete Mathematical Sciences & Cryptography* http://arxiv.org/abs/math.AC/0506045

[12] Buchberger B., Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, *Ph. D. Thesis*, Innsbruch, (1965)

[13] Buchberger B., Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem, *Aeq. Math.* **4** (1970), 374–383

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

[15] Cioffi F. Minimally generating ideals of fat points in polynomial time using linear algebra. *Ricerche di Matematica* **XLVII**, (1999), 55–63

[16] Cioffi F., Orecchia F.Computation of minimal generators of ideals of fat points. *Proc. ISSAC'01* (2001), 72–76

[17] Collard S., Mall D., Kalkbrener M., The Gröbner Walk (1993)

[18] Faugère J.C., Gianni P., Lazard D., Mora T. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering.*J. Symb. Comp.* **16** (1993), 329–344.

[19] P. Gianni, Algebraic solution of systems of polynomial equations using Gröbner bases, *L. N. Comp. Sci.* **356** (1989), 247-257.

[20] Gianni P., Properties of Gröbner Bases under Specialization, *L. N. Comp. Sci.* **378** (1987), 293–297, Springer

[21] Kalkbrener, M. Solving Systems of Algebraic Equations by Using Gröbner Bases, *L. N. Comp. Sci.* **378** (1987), 282–292, Springer

[22] Lakshman Y.N., A Single Exponential Bound on the Complexity of Computing Gröbner Bases of Zero Dimensional Ideals , *Progress in Mathematics* **94** (1990), 227–234, Birkhäuser

[23] Lazard D., Solving zero-dimensional algebraic systems *J. Symb. Comp.* **15** (1992), 117–132

[24] Lazard, D., A new method for solving algebraic systems of posisitive dimension *Disc. Appl. Math.* **33** (1991), 147–160

[25] S. Licciardi, Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion, *Proc. ISSAC'94* (1994) 191-196

[26] Marinari M.G., Möller H.M., Gröbner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points. *J AAECC* (1993), *4*, 103–145.

[27] Marinari M.G., Möller H.M., On multiplicities in Polynomial System Solving. *Trans. AMS* **348** (1996), 3283–3321.

[28] Möller. H.M., Stetter, H.J. Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. *Numer. Math.* **1995**, *70*, 311–329

[29] Reinhert B., Madlener K., A Note on Nielsen Reduction and Coset Enumeration. *Proc. ISSAC'98* , (1998), 171-178

[30] Sala M. , Personal communication (2005)

[31] Sasaki T. , Some algebraic algorithms based on head term elimination over polynomial ring Changing the ordering of Gröhbner Bases with LLL: Case of Two Variables, *L. N. Comp. Sci.* **378** (1987), 24–31, Springer

[32] J. Todd, H. Coxeter, A practical method for enumerating cosets of a finite abstract group. *Proc. Edinburgh Math. Soc.*, **5**(1936)

[33] Traverso C. et al. Natural representation of algebraic numbers. Informal talk at MEGA-92, Nice, 1992.

[34] Traverso C., Hilbert function and the Buchberger algorithm, *J. Symb. Comp.* **22** (1996), 355–376