De Nugis Groebnerialium 2: Applying Macaulay's Trick in order to easily write a Gröbner basis

Ferdinando Mora*

December 20, 2002

The difference between literature and journalism is that journalism is unreadable and literature is not read.
Oscal Wilde
Technical writing has qualities of literature and journalism.
Boo Barkee

Abstract

A trick introduced by Macaulay, in order to blow up a monomial ideal into a point ideal whose maximal ideal is the given monomia ideal, is sligtly generalized to allow to write down a Gröbner basis whose maximal ideal is a given monomial ideal.

Key Words: Macaulay's bound, Gröbner basis

1 Introduction

Assume you need to write down easily an ideal basis which is a Gröbner/standard one without performing any single test, but in a such way that in order to verify such property an outsider (or a computer) has no better way than applying Buchberger's Algorithm to your output.

*DISI, Univ. Genova, Viale Dodecaneso 35, 16146 Genova, `theomora@disi.unige.it`

Clearly, if you simply write down a monomial ideal, you are sure that you have a Gröbner basis, but everybody else can reach the same conclusion just giving a glance to your basis.

Macaulay himself had essentially the same problem: he needed to show, for any Hilbert function $H(t)$ which is "admissible" for a zero-dimensional ideal, the existence of a "point-ideal" (i.e. a radical zero-dimensional ideal) having such Hilbert function.

The "obvious" solution of writing down the lex-segment ideal having the same Hilbert function[1] was not satisfactory for him since it just gave a trivial primary ideal at the origin.

In order to obtain a radical zero-dimensional ideal whose leading term ideal is the obtained monomial ideal, thus having the required Hilbert function, Macaulay performed an elementary (but far to be obvious) trick.

In order to solve your problem all you need to do is to perform an obvious generalization of Macaulay's trick.

2 Notation

Let k be a field, $\mathbf{T}$ the commutative free semigroup generated by $X_1, \ldots, X_n$, whose elements are the monomials $X_1^{e_1} \cdots X_n^{e_n} : e_i \in \mathbb{N}$; $<$ a total ordering on $\mathbf{T}$ which is a semigroup ordering, i.e. compatible with the product:

$$\forall t, t_1, t_2 \in \mathbf{T}, t_1 < t_2 \Longrightarrow tt_1 < tt_2.$$

We will then consider the polynomial ring

$$\mathcal{P} := k[\mathbf{T}] = k[X_1, \ldots, X_n]$$

whose elements have a unique *ordered* representation as a linear combination of elements of $\mathbf{T}$:

$$f = \sum_{i=1}^{s} c_i t_i : c_i \in k \setminus \{0\}, t_i \in \mathbf{T}, t_1 > \cdots > t_s.$$

[1]This is the ideal which is obtained by considering the set of all the monomials and, for each degree $d \in \mathbb{N}$, removing from it the last $H(d)$ monomials w.r.t. the lexicographical ordering.

The non obvious part of this construction is the proof given by Macaulay that the result is really an ideal.

So to each non-zero element $f \in \mathcal{P}$, we can associate $T(f) := t_1$, the *maximal term* of f, and $\mathrm{lc}(f) := c_1$, the *leading coefficient* of f; and to each subset $G \subset \mathcal{P}$ we associate the set

$$T\{G\} := \{T(f) \in \mathbf{T} : f \in G\} \subset \mathbf{T},$$

and the semigrup ideal $T(G) \subset \mathbf{T}$ generated by it.

Remark that if $\mathcal{I} \subset \mathcal{P}$ is an ideal, then $T\{\mathcal{I}\} = T(\mathcal{I})$; such semigroup ideal of $\mathbf{T}$ is called the *term ideal* of $\mathcal{I}$.

Buchberger algorithm and theory and the related notion of Gröbner bases [2, 3] were introduced to study polynomial ring ideals and require the assumption that $<$ is a well-ordering, so that, in particular, $X_i > 1$, $\forall i$. The notion of standard bases and Hironaka theory [9] were instead introduced to study ideals in the series ring $k[[X_1, \dots, X_n]]$ and therefore require the consideration of orderings $<$ which are not well-orderings but which satisfy sufficiently good properties.

Definition 2.1 *A total semigroup ordering $<$ on $\mathbf{T}$ is called* inf-limited *([15] I.3.2) if for each $t \in \mathbf{T}$ and each decreasing infinite sequence*

$$t_1 > t_2 > \cdots t_n > \cdots$$

in $\mathbf{T}$, there is $n \in \mathbb{N}$ s.t. $t_n < t$.

Obviously a well-ordering is inf-limited, while the converse doesn't hold.

Given an inf-limited ordering $<$ on $\mathbf{T}$, we consider, following [15], the "completion" ring $\mathcal{P}\hat{\ } \subseteq k[[X_1, \dots, X_n]]$ consisting of those series

$$f = \sum_{t \in \mathbf{T}} c_t t \in k[[X_1, \dots, X_n]]$$

s.t. $\mathrm{supp}(f) := \{t \in \mathbf{T} : c_t \neq 0\}$ does not contain any increasing infinite sequence

$$t_1 < t_2 < \cdots t_n < \cdots.$$

As a consequence each non-zero series $f \in \mathcal{P}\hat{\ }$ has a unique *ordered* representation

$$f = \sum_{i=1}^{\infty} c_i t_i : c_i \in k \setminus \{0\}, t_i \in \mathbf{T}, t_1 > \cdots > t_s > \cdots,$$

and we can associate to it the *maximal term* $T(f) := t_1$, the *leading coefficient* $\mathrm{lc}(f) := c_1$; also to each subset $G \subset \mathcal{P}\hat{}$ we associate the set

$$T\{G\} := \{T(f) \in \mathbf{T} : f \in G\} \subset \mathbf{T},$$

and the semigrup ideal $T(G) \subset \mathbf{T}$ generated by it; if $\mathcal{I} \subset \mathcal{P}\hat{}$ is an ideal, then $T\{\mathcal{I}\} = T(\mathcal{I})$ is a semigroup ideal of $\mathbf{T}$, the *term ideal* of $\mathcal{I}$.

Obviously, if $<$ is a well-ordering, we have $\mathcal{P}\hat{} = \mathcal{P}$ and the notations given here coincide with the one introduced before.

Definition 2.2 *Let $<$ be an inf-limited ordering on $\mathbf{T}$. A finite set $G \subset \mathcal{P}\hat{}$ is called a* standard basis *of the ideal $\mathcal{I} \subset \mathcal{P}\hat{}$ it generates, if $T(G) = T(\mathcal{I})$.*

If $<$ is a well-ordering, $G \subset \mathcal{P}$ is called a Gröbner basis *of the ideal it generates.*

We recall that when one has a finite basis for a polynomial ideal $\mathcal{I} \subset \mathcal{P}$, Gröbner bases can be computed via Buchberger algorithm [2, 3], and standard bases of $\mathcal{I}\mathcal{P}\hat{}$ via the tangent cone algorithm [14].

These algorithms include a procedure which allows to test if a given finite basis $G \subset \mathcal{P}$ is a standard basis of the ideal it generates. In order to describe it (cf. [16]) we introduce the following

Definition 2.3 *Let*

- $<$ *be an inf-limited ordering on* $\mathbf{T}$,
- $\mathcal{I} \subset \mathcal{P}\hat{}$ *be an ideal of* $\mathcal{P}\hat{}$,
- $G = \{g_1, \dots, g_r\} \subset \mathcal{I}$ *be a finite basis of* $\mathcal{I}$ *s.t.* $\mathrm{lc}(g) = 1, \forall g \in G$.

For each pair $i, j, 1 \leq i < j \leq r$, let us denote $T(i,j), t_{ij}, t_{ji} \in \mathbf{T}$ the terms s.t.

$$t_{ij}T(g_i) = T(i,j) = \mathrm{lcm}(T(g_i), T(g_j) = t_{ji}T(g_j) \tag{1}$$

and let

$$S(i,j) := t_{ij}g_i - t_{ji}g_j.$$

We call S-pairs *of G the elements of*

$$\{S(i,j) : 1 \leq i < j \leq r\}$$

and we say that $S(i,j)$ has a weak standard representation *w.r.t. G if $\exists\{h_l\} \subset \mathcal{P}\hat{}$ s.t.*

– $S(i,j) = \sum_{l=1}^{r} h_l g_l$,

– $T(i,j) > T(h_l g_l), \forall l$.

Theorem 2.4 (Buchberger) *With the same notation as above, then the following conditions are equivalent:*

1. *G is a standard basis of $\mathcal{I}$;*
2. *Each S-pair $S(i,j), 1 \leq i < j \leq r$, has a weak standard representation w.r.t. G.*

Proof: cf. [16] Th. 3.7. □

3 Result

The problem we intend to solve is the following:

Problem 3.1 *Given a finite set of terms $m_1, \ldots, m_r \in \mathbf{T}$ and an inf-limited ordering $<$ on $\mathbf{T}$, produce a set of elements $g_1, \ldots, g_r \in \mathcal{P}\hat{}$ s.t.*

– $T(g_i) = m_i, \forall i$,

– *$G := \{g_1, \ldots, g_r\}$ is a standard basis;*

so that, denoting $\mathcal{I}$ the ideal generated by G in $\mathcal{P}\hat{}$, it holds

– $T(\mathcal{I}) = T(G) = (m_1, \ldots, m_r)$.

To solve it, we need just to introduce a suitable notation. Let

$$M := \{n_1, \ldots, n_s\} \subset \mathbf{T}$$

be a finite sequence[2] s.t.

– $\forall i, 1 \leq i \leq r, \exists J_i \subset \{1, \ldots, s\} : m_i = \prod_{l \in J_i} n_l$,

– $\forall i, j, 1 \leq i < j \leq r, \operatorname{lcm}(m_i, m_j) = \prod_{l \in J_i \cup J_j} n_l$.

[2] *Caveat lector!* A *sequence* and not just a *set*. If we have $m_1 := X^2, m_2 := XY$, we must return $n_1 := n_2 := X, n_3 := Y$ and $J_1 := \{1,2\}, J_2 := \{1,3\}$

Clearly such a list M can be easily obtained, by repeated gcd's.

Now let us choose, $\forall l, 1 \le l \le s$, an element $h_l \in \mathcal{P}\hat{}$ s.t.

- $T(h_l) < n_l$

and let us define

- $\gamma_l := n_l - h_l, \forall l, 1 \le l \le s$,
- $g_i := \prod_{l \in J_i} \gamma_l, \forall i, 1 \le i \le r$.

Clearly, with this notation, for each pair $i, j, 1 \le i < j \le r$, it holds by construction

- $t_{ij} = \prod_{l \in J_j \setminus J_i} n_l$,
- $t_{ji} = \prod_{l \in J_i \setminus J_j} n_l$.

where t_{ij}, t_{ji} are the elements satifying Eq. 1.

Proposition 3.2 *$G := \{g_1, \ldots, g_r\}$ is a standard basis.*

Proof: We have to prove, for each pair $i, j, 1 \le i < j \le r$, that the S-pair $S(i, j)$ has a standard representation. To do so, let us define

$$\phi_{ij} := \left(\prod_{l \in J_j \setminus J_i} \gamma_l \right) - t_{ij}, \quad \phi_{ji} := \left(\prod_{l \in J_i \setminus J_j} \gamma_l \right) - t_{ji}.$$

Clearly, since

$$t_{ij} = T\left(\prod_{l \in J_j \setminus J_i} \gamma_l \right), \quad t_{ji} = T\left(\prod_{l \in J_i \setminus J_j} \gamma_l \right),$$

it holds

$$T(\phi_{ij}) < t_{ij}, \quad T(\phi_{ji}) < t_{ji}.$$

Therefore we can claim that

$$S(i, j) = -\phi_{ij} g_i + \phi_{ji} g_j$$

is the required standard representation. In fact we have

$$\begin{aligned}
0 &= -\prod_{l\in J_i\cup J_j}\gamma_l + \prod_{l\in J_j\cup J_i}\gamma_l \\
&= -\left(\prod_{l\in J_j\setminus J_i}\gamma_l\right) g_i + \left(\prod_{l\in J_i\setminus J_j}\gamma_l\right) g_j \\
&= -(\phi_{ij}+t_{ij})g_i + (\phi_{ji}+t_{ji})g_j \\
&= -\phi_{ij}g_i + \phi_{ji}g_j - (t_{ij}g_i - t_{ji}g_j) \\
&= -\phi_{ij}g_i + \phi_{ji}g_j - S(i,j),
\end{aligned}$$

so that, the claim holds, since

$$T(\phi_{ij}g_i) < t_{ij}T(g_i) = T(i,j) = t_{ji}T(g_j) > T(\phi_{ji}g_j).$$

□

4 Macaulay's result

As I stated in the introduction, the result above is a generalization of the one by Macaulay ([12], p. 548) who constructed a zero-dimensional ideal having an assigned Hilbert function, starting from a monomial ideal with that assigned Hilbert function and constructing a zero-dimensional ideal having it as its associated monomial escalier.

Let $<$ be a degree-compatible ordering on $\mathbf{T}$, i.e. a well-ordering s.t.

$$\forall t_1, t_2 \in \mathbf{T}, \deg(t_1) < \deg(t_2) \Longrightarrow t_1 < t_2,$$

and let

$$\mathcal{J} = (m_1, \ldots, m_r) \subset \mathbf{T} \subset \mathcal{P}$$

be a 0-dimensional monomial ideal of $\mathcal{P}$, where

$$\forall l, m_l = X_1^{e_{1l}} \cdots X_n^{e_{nl}}.$$

Since $\mathcal{J}$ is 0-dimensional

$$\forall i, \exists d_i : X_i^{d_i} \in \mathcal{J} \text{ and } e_{il} \leq d_i, \forall l.$$

Let us then take distinct elements

$$a_{ij} \in k, 1 \le i \le n, 0 \le j < d_i : a_{ij} \ne a_{ik}, \forall i, j, k, j \ne k,$$

and, $\forall l, 1 \le l \le r$, let us define

$$g_l := \prod_{i=1}^{n} \prod_{j=0}^{e_{il}-1} (X_i - a_{ij}).$$

It is then evident that

- $T(g_l) = m_l, \forall l, 1 \le l \le r$, so that
- $G := \{g_1, \dots, g_r\} \subset \mathcal{P} = k[X_1, \dots, X_n]$ is a Gröbner basis and
- the ideal $\mathcal{I}$ generated by G is a 0-dimensional ideal s.t. $T(\mathcal{I}) = \mathcal{J}$.

Moreover, denoting $\mathbf{N}(\mathcal{I}) := \{t \in \mathbf{T} \setminus \mathcal{J}\}$, to each term

$$t = X_1^{e_1} \cdots X_n^{e_n} \in \mathbf{N}(\mathcal{I})$$

let us associate the affine point

$$P(t) := (a_{1e_1}, \dots a_{ne_n}) \in k^n.$$

Then the set of the (simple) roots of $\mathcal{I}$ is $\{P(t) : t \in \mathbf{N}(\mathcal{I})\}$.[3]

5 Applications

The scenario I sketched in the Introduction is less queer that it seems and is in fact quite normal in mathematical investigations or arguments, where the power of computer algebra systems is completely useless.

In fact what suggested writing this note on Macaulay's trick is that it has been such a very helpful tool in my activity to consider it worthwhile to be shared with the community.

[3]I thanks Luciana Ramella for having pointed me that the above construction (used and generalized by [8], [4] and [11]) goes back to Macaulay.

5.1 Easy-to-compute standard bases

In an investigation directed toward a computational proof of Hironaka's preparation theorem, M.E.Alonso and I needed to write down some standard basis whose stairs have a required shape; as it is well known a standard basis of a given series ideal is hard to compute — in fact, a termination condition for the tangent cone algorithm is not known, — and, moreover, is 0-dimensional in the general case, which was useless for our application.

For our computation we needed to have a series ideal $\mathcal{I} \in k[[X_1, X_2]]$ s.t. $T(\mathcal{I}) = (X_1X_2, X_2^2)$ for an ordering s.t. $1 > X_1 > X_2$. Macaulay's Trick gave us the elementary solution $\mathcal{I} := (g_1g_2, g_2^2)$, where $g_1 := \sum_{i=1}^{\infty} X_1^i$, $g_2 := \sum_{i=1}^{\infty} X_2^i$.

5.2 Gröbner bases and cryptography

Barkee et al.[4] [1] proposed and successfully attacked a crypto-system using Gröbner bases. Their approach began claiming that

> Somehow Archibald has produced an ideal $I \subset k[X_1, \ldots, X_n]$ of which he secretly owns a hard-to-compute Gröbner basis, so allowing him to compute canonical forms in polynomial time.

Roughly, their basic idea was to write down such a "hard-to-compute" Gröbner basis G to be used as private key and to generate from it a basis B to be used as public key, in such a way that G is the Gröbner basis of the ideal generated by B but it was hard to compute G from the knowledge of B.

Of course, the seriousness of their argument is based on the ability by Archibald to write down such Gröbner basis and a basis which is not easy

[4] It is my duty here to deny the false information contained in [10] which attributes to me [1].

I have nothing to do with that paper and its ideas, my only contribution being to explain to the authors how Archibald could apply Macaulay's Trick in order to effectively implement their proposal.

I asked them not to publish that detail in order to allow me to write this note; they agreed and offered me in exchange a guest star appearance under the pseudonym of Theo Moriarty. I loved this pseudonym so much that I used it in my annotated edition of Thritemius' *Steganography* [17] to compute by Buchbgerer's algorithm. Macaulay's Trick is now an essential tool.

Since, notwithstanding the boasting title of [1], the status on the applicability of Gröbner bases to cryptography is still an open question[5], a different and successfull scheme applying Gröbner bases to cryptography could require an elementary way to write down easily a private key Gröbner basis G.

In fact, the core of such scheme could be a successfull protocol to derive from G a public key B, which generates the same ideal as G but from which G is hard to be computed; then Macaulay's Trick provides this required tool to write down elementarily the Gröbner basis G to be used as private key in such scheme.

5.3 Möller's result

Möller and Sauer [13] recently proved that, for any term ordering $<$ and any ideal

$$\mathsf{I} := \{f_1, \ldots, f_n\} \in k[X_1, \ldots, X_n] : T(f_i) = X_i^{\deg(f_i)}, \forall i,$$

the Gröbner basis wrt $<$ of the ideal I^d, for each $d \in \mathbb{N}$, is

$$G_d := \{\prod_{i=1}^{n} f_i^{d_i} : \sum_{i=1}^{n} d_i = d\}.$$

An elementary proof of his result can be easily deduced from Macaulay's Trick simply by remarking that

- the result is obviously true for the monomial ideal

$$\mathsf{J} := \{X_1^{\deg(f_1)}, X_2^{\deg(f_2)}, \ldots, X_n^{\deg(f_n)}\},$$

  so that

$$\mathsf{J}^d := \{\prod_{i=1}^{n} X_i^{\deg(f_i) d_i} : \sum_{i=1}^{n} d_i = d\},$$

[5]In fact their successfully attack heavely took advantage on the density of the chosen basis and doesn't rule out the applicability of sparse Gröbner bases.

Remark also that the proposal by Fellows and Koblitz[5, 6, 7] which applies to cryptography polynomial ideals having a "supersparse" bases, in the sense that they mainly consist of monomials, is not yet been broken but there are indications that its stength is really bases exactly on its "supersparsity".

- and that Macaulay's Trick produces G_d from J^d by substituting each occurence of $X_i^{\deg(f_i)}$ with f_i.

Therefore G_d is a Gröbner basis of the ideal it generates and satisfies $T(G_d) = \mathsf{J}^d$; as a consequence, since I^d and J^d have the same Hilbert function, the same Hilbert function is shared also by (G_d). Then the obvious remark that $G_d \subset \mathsf{I}^d$ is sufficient to deduce the required statement $(G_d) = \mathsf{I}^d$.

5.4 Buchberger's First Criterion

As Boo Barkee pointed to me, Prop. 3.2 is essentially a "globalization" of the first criterion to detect useless pairs introduced by Buchberger, which states

Proposition 5.1 (Buchberger's First Criterion)
$T(g_i)T(g_j) = T(i,j) \Longrightarrow S(i,j)$ *has a standard representation.*

Proof: Adapting the notation of the proof of Prop. 3.2, we have $t_{ij} = T(g_j)$ and $t_{ji} = T(g_i)$ so we have just to choose

$$n_1 := T(g_j), n_2 := T(g_j), h_1 := g_j - T(g_j), h_2 := g_i - T(g_i),$$

in order to obtain

$$\gamma_1 = g_j, \gamma_2 = g_i, \phi_{ij} = h_1 = g_j - T(g_j), \phi_{ji} = h_2 = g_i - T(g_i)$$

and deduce Buchberger's formula

$$S(i,j) = -\phi_{ij} g_i + \phi_{ji} g_j.$$

□

References

[1] B. Barkee, D.C. Can, J. Ecks, T. Moriarty, R.F. Ree (1994). Why you cannot even hope to use Gröbner Bases in Public Key Cryptography. *J. Symb.Comp.* **18**, 497–501.

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

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

[4] J. Briançon and A. Galligo (1973). Déformations distinguées de points. *Astérisque* **7-8**,129–138.

[5] M.R. Fellows, N. Koblitz, Kid krypto. Advances in Cryptography – Crypto'92,*Lect. N. Comp. Sci.* **740** 371–389

[6] M.R. Fellows, N. Koblitz, Combinatorially based cryptography for children (and adults). *Congressus Numerantium* **99** (1994) 9–41

[7] M.R. Fellows, N. Koblitz, Combinatorial cryptosystems galore! *Contemporary Math.* **168** 51–61 (1994)

[8] R. Hartshorne (1966). Connectedness of the Hilbert scheme. *Math. Inst. des Hautes Etudes Sci.* **29**, 261–304.

[9] H. Hironaka (1964). Resolution of singularities of an algebraic variety over a field of characteristic zero. *Ann. Math.* **79**, 109–326.

[10] N. Koblitz, Algebraic Aspects of Cryptography, Springer (1998)

[11] D. Lazard (1985). Ideal basis and Primary decomposition: case of two variables. *J. Symb. Comp.* **1**, 261–270.

[12] F.S. Macaulay (1927). Some properties of enumeration in the theory of modular systems. *Proc. London Math. Soc.* **26**, 531–555.

[13] H.M. Möller, T. Sauer, Multivariate refinable functions of high approximation order via quotient ideals of Laurent polynomials. (2002)

[14] F. Mora (1982). An algorithm to compute the equations of tangent cones. Proc. EUROCAM 82, *Lect. N. Comp. Sci.* **144**, 158–165.

[15] T. Mora (1988). Seven variations on standard bases. Preprint.
`hhtpp:// ftp.disi.unige.it/persons/MoraF/7Varietions.tar.gz`.

[16] T. Mora (1994). An introduction to commutative and non-commutative Gröbner bases. *Theor. Comp. Sci.***134**, 131–173.

[17] Joanne Trithemio, *Steganographia*, annotated edition by D. Assereto, T. Moriarty

ftp:// www.disi.unige.it/persons/MoraF/STEGA/aaa.html.