Upper-bound of Reduction Operators and Computation of Syzygies

Cyrille Chenavier
Université Paris-Diderot - Paris 7.
INRIA, équipe πr^2.

1 Introduction

Several constructive methods in algebra are based on the computation of syzygies. For instance, a generating set of syzygies offers criteria to detect useless critical pairs during Buchberger's algorithm, that is critical pairs whose corresponding S-polynomials reduces into zero [8]. Such criteria improve the complexity of Buchberger's algorithm since most of the time is spent in computing into zero. Another application scope is homological/homotopical algebra where syzygies enable us to construct resolutions of monoids or algebras [1, 6, 7]. Several methods for computing syzygies were introduced: Squier's theorem states that the module of syzygies of a convergent string rewriting system is spanned by confluence diagrams [9, 10], which imply that syzygies can be computed by a completion-reduction procedure [5]. Moreover, the syzygies of a regular sequence are spanned by principal syzygies [4]. In [2], a general method for computing syzygies of a set of polynomials equations is given.

In this work, we are interested in the computation of syzygies of linear rewriting systems. Our motivation is to develop a general framework which can be specialised to various structures whose underlying sets of terms are vector spaces: polynomials algebras, tensor algebras, Lie algebras, operads... We fix a vector space V and a basis G of V: when V is a polynomial algebra, G is the set of monomials, for tensor algebras, G is the set of words, for instance. We consider linear rewriting systems described by *reduction operators*. Given a well-order $<$ on G, a reduction operator is an idempotent endomorphism of V such that for every $g \notin \operatorname{im}(T)$, $T(g)$ is a linear combination of elements of G strictly smaller than g for $<$. Such an operator encodes the reductions

$$v \underset{T}{\longrightarrow} T(v),$$

for every vector $v \notin \operatorname{im}(T)$.

Given a set $F = \{T_1, \cdots, T_n\}$ of reduction operators, the syzygies of F are the elements of the kernel of the map

$$\begin{aligned} \pi_F : \ \ker(T_1) \oplus \cdots \oplus \ker(T_n) &\longrightarrow V. \\ (v_1, \cdots, v_n) &\longmapsto \sum_{i=1}^{n} v_i \end{aligned}$$

In [3, Proposition 2.1.14], it is shown that the set of reduction operators admits a lattice structure. Our method for constructing a linear basis of $\mathbf{Syz}(F)$ works as follows: $\mathbf{Syz}(f_1, f_2)$ is isomorphic to the kernel of the upper bound $T_1 \vee T_2$ of T_1 and T_2. Moreover, for every integer $2 \leq k \leq n-1$, we have onto morphisms:

$$\begin{aligned} \mathbf{Syz}(T_1, \cdots, T_{k+1}) &\longrightarrow \mathbf{Syz}(T_1 \wedge \cdots \wedge T_k, T_{k+1}), \\ (v_1, \cdots, v_{k+1}) &\longmapsto \left(\sum_{i=1}^{k} v_i, v_{k+1}\right) \end{aligned}$$

where $T_1 \wedge \cdots \wedge T_k$ is the lower bound of $\{T_1, \cdots, T_k\}$. Hence, if a linear basis $\mathscr{B}_k$ of $\mathbf{Syz}(T_1, \cdots, T_k)$ is known, we construct a linear basis of $\mathbf{Syz}(f_1, \cdots, f_{k+1})$ by taking the union of $\mathscr{B}_k$ with pre-images of elements of a linear basis of $\mathbf{Syz}(T_1 \wedge \cdots \wedge T_k, T_{k+1})$. This method provides successively linear bases of $\mathbf{Syz}(T_1, T_2)$, $\mathbf{Syz}(T_1, T_2, T_3)$, ..., $\mathbf{Syz}(T_1, \cdots, T_n) = \mathbf{Syz}(F)$.

2 Reduction Operators

2.1. Notations. We fix a well-ordered set $(G,<)$ and a commutative field $\mathbb{K}$. Every vector v of the vector space $\mathbb{K}G$ spanned by G admits a greatest element, written $\lg(v)$, in its decomposition with respect to G. We extend the order $<$ on G into an order on $\mathbb{K}G$ defined by $v_1 < v_2$ if $v_1 = 0$ and $v_2 \neq 0$ or if $\lg(v_1) < \lg(v_2)$.

2.2. Definition. A linear endomorphism T of $\mathbb{K}G$ is called a *reduction operator* if it is a projector and if for every $g \in G$, we have $T(g) \leq g$. We write $\mathbf{RO}(G,<)$ the set of reduction operators and for every $T \in \mathbf{RO}(G,<)$, we write

$$\mathrm{Red}(T) = \Big\{ g \in G \;\mid\; T(g) \neq g \Big\}.$$

2.3. T-decompositions. A reduction operator being a projector, the kernel of T admits as a basis the set of $g - T(g)$, where g belongs to $\mathrm{Red}(T)$, that is every $v \in \ker(T)$ admits a unique decomposition

$$v = \sum_{g \,\in\, \mathrm{Red}(T)} \lambda_g \left(g - T(g)\right). \tag{1}$$

The decomposition (1) is called the *T-decomposition* of v.

2.4. Lattice Structure. Recall from [3, Proposition 2.1.14] that the map

$$\begin{aligned} \ker : \mathbf{RO}(G,<) &\longrightarrow \Big\{\text{subspaces of } \mathbb{K}G\Big\}, \\ T &\longmapsto \ker(T) \end{aligned}$$

is a bijection. Given a subspace V of $\mathbb{K}G$, we write $\ker^{-1}(V)$ the unique reduction operator with kernel V. Then, $(\mathbf{RO}(G,<), \preceq, \wedge, \vee)$ is a lattice where

i. $T_1 \preceq T_2$ if $\ker(T_2) \subseteq \ker(T_1)$,

ii. $T_1 \wedge T_2 = \ker^{-1}(\ker(T_1) + \ker(T_2))$,

iii. $T_1 \vee T_2 = \ker^{-1}(\ker(T_1) \cap \ker(T_2))$.

3 Syzygies

We fix a subset $F = \{T_1, \cdots, T_n\}$ of $\mathbf{RO}(G,<)$ and we let

$$\ker(F) = \ker(T_1) \oplus \cdots \oplus \ker(T_n).$$

An element of $\ker(F)$ is written $(v_1, \cdots, v_n)$, where each v_i belongs to $\ker(T_i)$.

3.1. Notation. For every integer $1 \leq i \leq n$ and for every $g \in \mathrm{Red}(T_i)$, we let

$$b_{i,g} = (0, \cdots, 0, g - T_i(g), 0, \cdots, 0).$$

The set

$$\mathscr{B} = \Big\{ b_{i,g} \;\mid\; 1 \leq i \leq n \text{ and } g \in \mathrm{Red}(T_i) \Big\},$$

is a linear basis of $\ker(F)$.

3.2. Definition. Consider the linear map

$$\begin{aligned} \pi_F : \ker(F) &\longrightarrow \ker(\wedge F). \\ (v_1, \cdots, v_n) &\longmapsto \sum_{i=1}^{n} v_i \end{aligned}$$

We write

$$\mathbf{Syz}(F) = \ker(\pi_F).$$

The elements of $\mathbf{Syz}(F)$ are called the *syzygies* of F.

3.3. Canonical Decompositions. By definition of syzygies, we have a linear isomorphism

$$\overline{\pi_F} \ : \ \ker(F) / \mathbf{Syz}(F) \ \xrightarrow{\sim} \ \ker(\wedge F).$$

Moreover, $\ker(F) / \mathbf{Syz}(F)$ admits as a basis a subset $\mathscr{B}(F)$ of $\mathscr{B}$, so that

$$\Big\{ g \ - \ T_i(g) \ \mid \ b_{i,g} \ \in \ \mathscr{B}(F) \Big\}, \tag{2}$$

is a basis of $\ker(\wedge F)$. The decomposition of an element v of $\ker(\wedge F)$ with respect to (2) is called a *canonical decomposition* of v *with respect to* F.

3.4. Remark. Following the terminology of [3, Section 2.1.9], $\mathscr{B}(F)$ can be chosen in such a way that it is also *reduced* and this choice is unique, which motivates the terminology of "canonical basis". In the sequel, we do not assume that $\mathscr{B}(F)$ is reduced.

3.5. Purpose. Our purpose is to introduce an algorithm for computing $\mathbf{Syz}(F)$. This algorithm is based on the fact that for every family $U_1, \ \cdots, \ U_k$ of reduction operators, we have a linear map:

$$\begin{aligned} \mathbf{Syz}(U_1, \ \cdots, \ U_k) \ &\longrightarrow \ \mathbf{Syz}(U_1 \wedge \cdots \wedge U_{k-1}, \ U_k). \\ (v_1, \ \cdots, \ v_k) \ &\longmapsto \ \left(\sum_{i=1}^{k-1} v_i, \ v_k \right) \end{aligned}$$

We also need the following:

3.6. Proposition. *Let* $P \ = \ (T_1, \ T_2)$ *be a pair of reduction operators. We have a linear isomorphism*

$$\begin{aligned} \ker(T_1 \vee T_2) \ &\xrightarrow{\sim} \ \mathbf{Syz}(P). \\ v \ &\longmapsto \ (-v, \ v) \end{aligned}$$

3.7. The Algorithm. The algorithm takes as input a finite subset $F \ = \ \{T_1, \ \cdots, \ T_n\}$ of $\mathbf{RO}(G, <)$ and returns a basis of $\mathbf{Syz}(F)$.

Algorithm 1 Computation of a Basis of Syzygies

Initialisation:

- $T \ := \ \mathrm{Id}_{\mathbb{K}G}$;
- $v \ := \ 0$;
- $B \ := \ \emptyset$.

for $i \ = \ 2$ to n **do**
  $T \ = \ T_1 \wedge \cdots \wedge T_{i-1}$;
  for $g_0 \ \in \ \mathrm{Red}(T \vee T_i)$ **do**
    $v \ = \ g_0 \ - \ (T \vee T_i)(g_0)$;
    $\sum \lambda_g (g \ - \ T_i(g))$: the T_i-decomposition of v;
    $\sum \lambda_{j,g'} (g' \ - \ T_j(g'))$: a canonical decomposition of v with respect to $(T_1, \cdots, \ T_{i-1})$;
    $B \ = \ B \ \cup \ \Big\{ \sum (\lambda_g b_{i,g}) \ - \ \sum (\lambda_{j,g'} b_{j,g'}) \Big\}$;
  end for
end for
return B

4 Example

We consider $G = (g_1 < g_2 < g_3 < g_4 < g_5 < g_6)$. We let $F = \{T_1,\ T_2,\ T_3,\ T_4)\}$, where the operators T_i are defined by their matrices with respect to the basis G:

$$T_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$T_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } T_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The vector space $\ker(F)$ is spanned by the following eight vectors:

$b_1 = (g_4 - g_3,\ 0,\ 0,\ 0)$, $b_2 = (g_5 - g_3,\ 0,\ 0,\ 0)$, $b_3 = (g_6 - g_1,\ 0,\ 0,\ 0)$, $b_4 = (0,\ g_4 - g_2,\ 0,\ 0)$

$b_5 = (0,\ g_5 - g_2,\ 0,\ 0)$, $b_6 = (0,\ g_6 - g_2,\ 0,\ 0)$, $b_7 = (0,\ 0,\ g_4 - g_1,\ 0)$, $b_8 = (0,\ 0,\ 0,\ g_5 - g_1)$.

We describe the algorithm of the previous section to compute a linear basis B of $\mathbf{Syz}\,(F)$. We begin with $B = \emptyset$.

4.1. Step 1. We have

$$T_1 \vee T_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The set $\operatorname{Red}(T_1 \vee T_2)$ is reduced to $\{g_5\}$ and $g_5 - (T_1 \vee T_2)(g_5)$ is equal to $g_5 - g_4$. We have

$$\begin{aligned} g_5 - g_4 &= \Big(g_5 - g_3\Big) - \Big(g_4 - g_3\Big) \\ &= \Big(g_5 - T_1(g_5)\Big) - \Big(g_4 - T_1(g_4)\Big), \end{aligned}$$

and

$$\begin{aligned} g_5 - g_4 &= \Big(g_5 - g_2\Big) - \Big(g_4 - g_2\Big) \\ &= \Big(g_5 - T_2(g_5)\Big) - \Big(g_4 - T_2(g_4)\Big). \end{aligned}$$

We have

$$B = \Big\{b_5 - b_4 - b_2 + b_1\Big\}.$$

4.2. Step 2. We have

$$(T_1 \wedge T_2) \vee T_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We need to determine the T_3-decomposition of $g_4 - g_1$ and well as a canonical decomposition of $g_4 - g_1$ with respect to (T_1, T_2). These two decompositions are given by

$$\begin{aligned} g_4 - g_1 &= g_4 - T_3(g_4) \\ &= -\Big(g_6 - g_2\Big) + \Big(g_4 - g_2\Big) + \Big(g_6 - g_1\Big) \\ &= -\Big(g_6 - T_2(g_6)\Big) + \Big(g_4 - T_2(g_4)\Big) + \Big(g_4 - T_1(g_4)\Big), \end{aligned}$$

so that, we have

$$B = \Big\{b_5 - b_4 - b_2 + b_1,\ b_7 + b_6 - b_4 - b_3\Big\}.$$

4.3. Step 3. We have

$$(T_1 \wedge T_2 \wedge T_3) \vee T_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

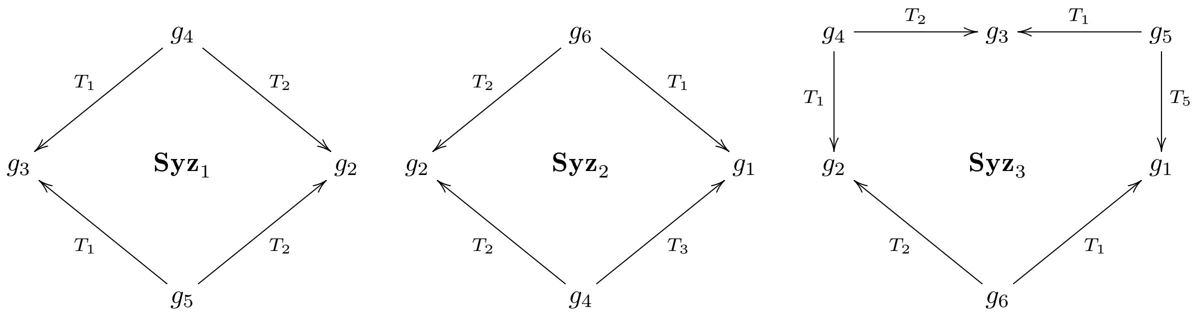
The T_4-decomposition of $g_5 - g_1$ and a canonical decomposition of $g_5 - g_1$ with respect to (T_1, T_2, T_3) are given by

$$\begin{aligned} g_5 - g_1 &= g_5 - T_4(g_5) \\ &= -\Big(g_6 - g_2\Big) + \Big(g_4 - g_2\Big) + \Big(g_6 - g_1\Big) + \Big(g_5 - g_3\Big) - \Big(g_4 - g_3\Big) \\ &= -\Big(g_6 - T_2(g_6)\Big) + \Big(g_4 - T_2(g_4)\Big) + \Big(g_6 - T_1(g_6)\Big) + \Big(g_5 - T_1(g_5)\Big) - \Big(g_4 - T_1(g_4)\Big), \end{aligned}$$

so that, we have

$$B = \Big\{b_5 - b_4 - b_2 + b_1,\ b_7 + b_6 - b_4 - b_3,\ b_8 + b_6 - b_4 - b_3 - b_2 + b_1\Big\}.$$

4.4. Remark. The syzygies $\mathbf{Syz}_1 = b_5 - b_4 - b_2 + b_1$, $\mathbf{Syz}_2 = b_7 + b_6 - b_4 - b_3$ and $\mathbf{Syz}_3 = b_8 + b_6 - b_4 - b_3 - b_2 + b_1$ have the following geometric interpretations:



References

[1] David J. Anick. On the homology of associative algebras. *Trans. Amer. Math. Soc.*, 296(2):641–659, 1986.

[2] Alberto Arri and John Perry. The F5 criterion revised. *J. Symbolic Comput.*, 46(9):1017–1029, 2011.

[3] Cyrille Chenavier. Reduction Operators and Completion of Rewriting Systems. *J. Symbolic Comput.*, 2017.

[4] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic). ACM, New York, 2002.

[5] Stéphane Gaussent, Yves Guiraud, and Philippe Malbos. Coherent presentations of Artin monoids. *Compos. Math.*, 151(5):957–998, 2015.

[6] Yves Guiraud and Philippe Malbos. Higher-dimensional normalisation strategies for acyclicity. *Adv. Math.*, 231(3-4):2294–2351, 2012.

[7] Yuji Kobayashi. Complete rewriting systems and homology of monoid algebras. *J. Pure Appl. Algebra*, 65(3):263–275, 1990.

[8] Hans-Michael Möller, Teo Mora, and Carlo Traverso. Gröbner bases computation using syzygies. In *Papers from the international symposium on Symbolic and algebraic computation*, pages 320–328. ACM, 1992.

[9] Craig C. Squier. Word problems and a homological finiteness condition for monoids. *J. Pure Appl. Algebra*, 49(1-2):201–217, 1987.

[10] Craig C. Squier, Friedrich Otto, and Yuji Kobayashi. A finiteness condition for rewriting systems. *Theoret. Comput. Sci.*, 131(2):271–294, 1994.