Curso 2005/06
CIENCIAS Y TECNOLOGÍAS/10
I.S.B.N.: 84-7756-698-4

MARÍA DEL SOCORRO GARCÍA ROMÁN

Métodos efectivos en álgebras con bases PBW: *G*-Álgebras y Álgebras de Yang-Baxter

Director
MANUEL DAMIÁN GARCÍA ROMÁN

SERVICIO DE PUBLICACIONES
UNIVERSIDAD DE LA LAGUNA

SOPORTES AUDIOVISUALES E INFORMÁTICOS
Serie Tesis Doctorales

I saw the angel in the marble, and carved until I set him free.

Michelangelo.

Gracias a: / Thanks to:

- *Manolo García Román*, por haberme iniciado y guiado en el apasionante y complejo mundo de la investigación, por todo lo que me ha enseñado, por su inestimable ayuda sin la que este trabajo no habría salido adelante, y por representar un excelente ejemplo como director, investigador, profesor y persona. Gracias por ofrecerme los ánimos necesarios para reponerme a las caídas, por haber creído en mis ideas y proyectos, y por ayudarme a conseguirlos.

- *Mariví Reyes*, por haber seguido siempre de cerca mi trabajo, por su gran ayuda como profesora y como tutora, por sus oportunos y sabios consejos que me han servido en numerosas situaciones, y por su apoyo incondicional a lo largo de todos estos años, animándome siempre a alcanzar mis metas.

- *Alain Verschoren*, por haberme motivado a comenzar la investigación dentro del Álgebra Computacional, por sus siempre interesantes discusiones matemáticas, por la ayuda brindada en la corrección y revisión de mis trabajos, y por la agradable acogida durante mis estancias en la ciudad de Amberes.

- Los profesores del Área de Álgebra del Depto. de Matemática Fundamental de la Universidad de La Laguna, porque a ellos les debo mi formación como algebrista, y porque una parte de las enseñanzas de cada uno de ellos se encuentran reflejadas en esta memoria. Muy especialmente, a *Evelia García* y *Margarita Rivero*, por su atención constante en mi formación, por su inestimable apoyo moral, sus consejos y porque siempre han estado ahí cuando las he necesitado.

- My *other* supervisors, in the International Advanced Master on NA&G (Noncommutative Algebra and Geometry). To my supervisors of the Master thesis: *Fred Van Oystaeyen*, for giving me the opportunity of completing the master, and *Tatiana Gateva Ivanova*, from whom I have learned so many things, for iniciating me into the interesting and thrilling topic of Set-theoretic solutions of the YBE and for spending so long hours on mathematical (and non-mathematical!) discussion. To my supervisor of the geometry project-work, *Peter Fiebig*, who it has been a pleasure to work with, I thank him for his valuable help. I extend this acknowledgement to all professors, lectures and partners met during the completion of the master, in Antwerp 2002-2003.

- *Carmen M.* y *Nelly*, por ser las primeras impulsoras de mi interés y constancia en las Matemáticas.

- *Pepe Bueso*, *Pepe Gómez Torrecillas* y *Javier Lobillo* (Universidad de Granada), por su cálida acogida durante mi estancia en Granada en la que pude compartir interesantes charlas, ideas y trabajos.

- A toda la gente agradable que he conocido en congresos y estancias. A *Paco Calderón* y *Paco Castro* (Universidad de Sevilla), por el interés en mi trabajo y por el tiempo que me han dedicado. A *Diego Ruano* y *Fernando Hernando* (Universidad de Valladolid), por la cantidad de buenos momentos que he vivido junto a ellos en los últimos congresos, por el apoyo brindado y por convertir en risas los nervios previos a una charla.

- *Gobierno de Canarias* y la *Universidad de La Laguna*, por la financiación económica con la que he podido dedicarme a la investigación durante estos años.

- Mi Familia:

  - a mis abuelos *Candelaria* y *Manuel*, quienes me han apoyado siempre, en todas las facetas de mi vida;
  - a mis padres *Nieves* y *José Manuel*, por darme la vida, por su cariño y por haberme enseñado tantas cosas valiosas;
  - a mis hermanos *Mamel*, *Carlos*, *Marian*, *Che*, *Víctor* y *Nini*, porque siempre he podido contar con todos y cada uno de ellos.

  A los *peques* que ya están y a los que vienen en camino, porque representan la alegría de cada día, a mi tía *Veli*, que siempre está ahí, y a mis cuñados/as, por aguantar mis payasadas.

- *Deisy*, *Marga* y *Maris*, por apoyarme en todo momento y hacerme sentir que cuento con una segunda familia.

- Mis compañeras de promoción y de despacho en los años de investigación: *Fefi*, *Judit* y *Maru*, por vivir conmigo los peores y mejores momentos de los últimos años brindándome un gran apoyo moral cuando lo he necesitado, por compartir y aprender de sus inquietudes matemáticas en un ambiente de trabajo en el se han ocurrido miles de anécdotas divertidas, por los buenos momentos que hemos pasado en los viajes y por sus ánimos a seguir "*Pazito a Pazito*".

- *Alejandro*, *Isidro*, *Leyla*, *Pedro* y *Vane*, amigos incondicionales que han vivido día a día en el *backstage* de este trabajo, gracias por apoyarme, aguantarme y darme ánimos constantemente.

- *Alicia*, quien me ha demostrado que la verdadera amistad permanece inmutable en la distancia y en el tiempo.

- *Estrella*, por estar siempre conmigo desde el día en que *nació*...

- *Marcos Lugo*, por ser fuente de mis ilusiones y esperanzas de futuro, por ser la fuerza frente a cualquier reto, en especial la culminación de esta memoria, por haberme apoyado y animado en todo momento, por vivir conmigo los malos y buenos momentos durante la mitad de mi vida, por animarme en cada demostración errónea y sentir como propia la alegría al descubrir cada nuevo teorema. Gracias por tu inmensa paciencia, por tus esfuerzos en comprender mis teorías y por dar un sentido completo a este trabajo.

A mis abuelos,
a mis padres,
a mis hermanos
y a Marcos.

Contents

List of Algorithms

Introduction

The celebrated Poincaré-Birkhoff-Witt Theorem states that if $\{x_1, \ldots, x_n\}$ is a k-basis of the Lie algebra $\mathfrak{g}$, then the set of standard monomials

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n}\}_{\alpha_1,\ldots,\alpha_n \in \mathbb{N}}$$

is a k-basis of the universal enveloping algebra $U(\mathfrak{g})$. This property, which universal enveloping algebras share with many other associative algebras, is one of the reasons why most of the basic algorithms used to study the commutative ring of polynomials also work in a non necessarily commutative context. Indeed, in spite of the theory of Gröbner bases has been extended to algebras with no bases of standard monomials (see the works of Mora in free algebras [70, 71, 73]), it appears that the highest yields from a computational viewpoint are obtained in algebras where such a basis, also called a PBW basis, exists (see [3, 8, 9, 10, 11, 12, 13, 23, 30, 31, 44, 54, 59, 60, 61, 62, 64, 65, 72, et al.]).

This work is devoted to the study, from a computational viewpoint, of the class of algebras where a PBW basis exists. More precisely, we will focus on algebras which are, in addition, presented by a finite set of generators $X = \{x_1, \ldots, x_n\}$ and a finite number of relations arising from a set $Q \subseteq \langle X \rangle \times \mathsf{k}\langle X \rangle$ (the so-called reduction system). As we show in 1.2.4, when $Q = \{(W_\sigma, f_\sigma)\}_\sigma$ is a complete reduction system (in the sense of [57]), compatible with some monomial order on $\langle X \rangle$, and all W_σ's are disordered, then the set of standard monomials on the generators $\{x_1, \ldots, x_n\}$ is a PBW basis of the quotient $\mathsf{k}\langle X \rangle / I_Q$ (where I_Q denotes the two-sided ideal generated by Q) if, and only if, every monomial $x_j x_i$ with $i < j$ is the leading term of a relation in Q. Note that the latter may be checked effectively.

Our main case studies are the class of G-Algebras, which is certainly the most profusely studied class of algebras in the literature on effective methods in non-commutative algebras, and the class of Yang-Baxter Algebras, far less known at least in computational contexts.

Amongst not necessarily commutative algebras, the former have a nice computational treatment, not only because they have PBW bases, but also because the multiplication is compatible with the exponents. Essentially, these are the reasons why the theory of Gröbner bases on the commutative polynomial ring (see [1, 18, 46, et al.]) can be extended to the context of G-Algebras just by mimicking the notions and the results. This class of algebras includes many universal enveloping algebras, Weyl algebras, Quantum spaces, etc. It was introduced in the seminal paper of Kandri-Rody and Weispfenning [54] under the name of *Solvable polynomial algebras*, after the initial work of Galligo in the Weyl algebra (see [23]) and the one of Apel and Lassner in universal enveloping algebras of finite-dimensional Lie algebras ([3]). In [59] Kredel also contributed in the main points of this theory, which has recently been surveyed by Bueso, Castro, Gómez Torrecillas, Lobillo and Verschoren ([9, 10, 11, 12, 13, 44, 65]) (who use the name *PBW algebra* instead of G-Algebra), Li ([64]), Levandovskyy ([60, 61, 62]), and the author ([24, 26, 27, 28, 29, 30, 31]) (also under the name of PBW algebra). In [9, 10, 11, 13, 65, et al.] the theory of Gröbner bases is extended to the more general class of *left* (or *right*) *PBW rings*.
Many algebraic and homological objects have been studied in the context of G-Algebras with a computational purpose: left syzygy modules and free resolutions ([61, 13]), graded and filtered left modules, homogeneous Gröbner bases, functors Hom and Ext, the Gelfand-Kirillov dimension, primality of two-sided ideals (see [8, 10, 12, 13, 44, 65]), projective dimension of modules ([22]), etc.

Concerning the class of Yang-Baxter Algebras, they have recently been proved to have an associated semigroup of skew-polynomial type (see [40]) and hence, to fit in our computational setting. This class of algebras arises from square-free nondegenerate involutive set-theoretic solutions of the Yang Baxter Equation, from here on called *square-free solutions of the YBE*, which have became an attractive research topic to scientists and mathematicians since the middle of nineteen sixties. First, many solutions of this equation were found by studying certain related algebraic structures: the Hopf algebras (see e.g. [55]). In 1990 Drinfeld ([19]) suggested looking for the so-called *set-theoretic solutions*, which are the simplest class of solutions. In this sense, Weinstein and Xu [81] found in 1992 a way to construct set-theoretic solutions by studying the Poisson group. Afterwards, Etingof, Schedler and Soloviev [21] studied set-theoretic solutions satisfying invertibility, unitarity and nondegeneracy. They introduced several constructions of such solutions. They also gave their classification in terms of Group Theory and showed their geometric and algebraic interpretations. Meanwhile, Lu, Yan and Zhu

([66]) proposed a method to construct set-theoretic solutions which generalizes the earlier ones of Weinstein-Zu and Etingof-Schedler-Soloviev. Whereas these results are based on algebro-geometric and topological methods, T. Gateva-Ivanova ([38, 39, 40]) introduced a combinatorial approach to this topic focusing on the behaviour of the set of relations $\Re(X,r)$, uniquely determined by each solution (X,r). If (X,r) is a square-free solution of the YBE, then the set $\Re(X,r)$ satisfies the so-called *Cyclic Condition*, which is essential in combinatorial techniques in this context. This approach has been used, for example, in order to obtain algebraic and homological properties (see [42]) of the Yang-Baxter Algebra associated to each square-free solution of the YBE.

The contents of this work are organized as follows.

The background on reduction systems and ambiguities of reduction, including Bergman's Diamond Lemma and an algorithm of reduction adapted to perform a two-sided division in the free algebra (Algorithm 1), are collected in Chapter 1. In this chapter we also recall the equivalence between the notions of two-sided Gröbner basis in the free algebra and complete reduction system, which allows us to prove that Levandovskyy's Non-Degeneracy Conditions (see [61]) stated on any G-Algebra $\mathsf{k}\langle X\rangle/I_Q$ are equivalent to the overlap ambiguities of Bergman to be resolvable (see [7]), or equivalently, the (noetherian) rewriting system Q' (see [57]) arising from Q to be complete (see Th. 1.1.25 and Remark 2.1.3).
In the last section of Chapter 1 we prove our characterization of algebras with PBW bases (Th. 1.2.4) and we give, using a technique developed in detail in Chapter 2, the reason why the Reduction Algorithm also yields a two-sided division in algebras with a PBW basis (Th. 1.2.11), or more precisely, in *standard finitely presented algebras* $R = \mathsf{k}\langle X\rangle/I_Q$, with $X = \{x_1,\ldots,x_n\}$ and where I_Q denotes the two-sided ideal generated by a complete reduction system $Q = \{(x_jx_i, f_{ji}) \,/\, 1 \leq i < j \leq n\}$.

In Chapter 2 we analyze our first example of algebras with PBW bases: the class of G-Algebras. These algebras are defined, in addition to have a PBW basis on a finite set of generators $\{x_1,\ldots,x_n\}$, by the property that the *exponent* of the skew-commutator $p_{ij} = x_jx_i - c_{ij}x_ix_j$ is bounded by the *exponent* of the product x_ix_j, which is $(0,\ldots,\overset{-i-}{1},\ldots,\overset{-j-}{1},\ldots,0)$, for all $1 \leq i < j \leq n$. The class of G-Algebras includes universal enveloping algebras of finite dimensional Lie algebras, iterated Ore extensions, many

quantum groups ($M_q(2)$, Quantum spaces, etc.) and it is closed under taking the opposite algebra and tensor products, as we show in the second section of this chapter.

In the first four sections of Chapter 2, we recall the basic background of the theory of Gröbner basis in the context of G-Algebras. We follow the notation and terminology of [13]. In the fourth section, devoted to some of the classical applications of Gröbner bases, we contribute with an algorithm to compute the codimension of a left submodule (right submodule or subbimodule) $M \subseteq R^s$ when R is a G-Algebra and M is cofinite (see Algorithms 8 and 9).

In the fifth section we propose a new method, that we reported first in [28], to effectively handle bimodules by using directly their two-sided generator systems as input data. We apply this method in order to compute two-sided Gröbner bases for bimodules over a G-Algebra (see Algorithm 10) in an alternative way to the Right Closure Method of Kandri-Rody and Weispfenning (see [54]). This new algorithm calls once the left Buchberger Algorithm, instead of the a priori unknown number of calls typical of the Right Closure Method. A comparison between both algorithms is carried out by discussing some explicit examples.

In the sixth section the above-mentioned technique to handle bimodules is also applied in order to compute *syzygy bimodules*. These bimodules were first introduced by Mora for homogeneous two-sided ideals in the context of non-commutative graded structures ([71]), and then, independently, by the author ([27, 30]) for not necessarily homogeneous bimodules over a G-Algebra. We show that the syzygy bimodules, which can be viewed as the two-sided counterpart of the left syzygy module, reveal to be useful at solving some computational problems when two-sided input data are given. We devise algorithms to compute finite intersections of subbimodules of free modules, presentations and free resolutions of subbimodules of free modules, two-sided division ideals of R, etc. In case the bimodules are generated by elements of the *centralizer*, some of these results are enhanced and many computations can be simplified.

In the last section we present an algorithm to compute a presentation of $\mathrm{Tor}_k(M, N)$ in the context of G-Algebras.

In Chapter 3 we focus on our second example of algebras with a PBW basis: the Yang-Baxter Algebras, defined from square-free solutions of the Yang-Baxter equation. If $X = \{x_1, \ldots, x_n\}$, then the bijection $r : X \times X \longrightarrow X \times X$ is a set-theoretic solution of the Yang-Baxter Equation if

$$(r \times \mathrm{Id})(\mathrm{Id} \times r)(r \times \mathrm{Id}) = (\mathrm{Id} \times r)(r \times \mathrm{Id})(\mathrm{Id} \times r).$$

In case r is a square-free solution of the YBE, the set of standard monomials in X is a k-basis of the algebra generated by X with relations $\{x_jx_i - r(x_jx_i)\}_{1\leq i<j\leq n}$ (see Prop. 3.3.13).
As we show throughout the whole chapter, a combinatorial approach may be used in order to develop algorithmic methods in the context of set-theoretic solutions of the YBE. After showing some ways of representing and classifying square-free solutions of the YBE, we focus on the isomorphisms and automorphisms of the solutions by following this combinatorial-computational approach. The results presented in this part are generalizations of those that we first proved in [25, 33]. In particular, we describe a method based on the recent notion of *star* of an element to compute the set of isomorphisms of two non-degenerate, involutive set-theoretic solutions. The usefulness of computing the group of automorphisms of a solution is justified at the end of the first section, where we devise some algorithms which require automorphisms in order to compute new solutions by gluing any other two solutions. We also find a bijective correspondence between the set of left extensions of two disjoint non-degenerate involutive set-theoretic solutions (X, r_X), (Y, r_Y) and the morphisms from the group $\mathcal{G}(Y, r_Y)$ associated to (Y, r_Y) and the group of automorphisms $\mathrm{Aut}(X, r_X)$ of (X, r_X).
In the last section we discuss the equivalence, proved by T. Gateva-Ivanova and M. Van den Bergh [40, 42], between square-free solutions of the YBE, semigroups of skew-polynomial type and semigroups of I-type. The theory of reduction systems and Gröbner basis surveyed in the first chapter is used in this context to prove (in an alternative way to that of [40]) that the Yang-Baxter Algebra $\mathcal{A}(\mathsf{k}, X, r)$ associated to a square-free solution (X, r) of the YBE is an algebra with a PBW basis. Finally, we show how the behaviour of semigroups of skew-polynomial type is completely determined by a family of Linear Programming problems.

Throughout both Chapters 2 and 3 we illustrate theoretic notions with explicit examples. In order to perform the computation of the examples, we have encoded one each libraries of procedures (included in the companion CD; see also [32]) using the package of symbolic computation *Maple*. This software must be viewed as part of the PhD thesis.
The library corresponding to G-Algebras includes from basic arithmetics involving elements in a G-Algebra to all the algorithms listed in Chapter 2. The library of methods concerning set-theoretic solutions includes algorithms which allow us to recognize whether a set of relations determines a square-free solution of the YBE, to compute all possible orders $\preceq$ on $X = \{x_1, \ldots, x_n\}$ such that the Yang-Baxter semigroup $\mathcal{S}(X, r)$ is of skew-polynomial type, to verify when a bijection is an automorphism of a (square-free) nondegenerate

involutive set-theoretic solution, to compute the group of automorphisms of any nondegenerate involutive set-theoretic solution, to glue two square-free solutions of the YBE in order to obtain a new one, etc.

For convenience of the reader, an appendix collecting definitions and examples of the (monomial, admissible, etc.) orders used through the three chapters is included at the end of the work.

There are some open problems stated on the class of standard finitely presented algebras $R = \mathsf{k}\langle X\rangle/I_Q$, where $X = \{x_1, \ldots, x_n\}$ and $Q = \{(x_j x_i, f_{ji})\}_{i<j}$ is a complete reduction system, as considered in Chapter 1.

- To find out which R are Noetherian;
- To develop methods to compute finite Gröbner bases for left and two-sided ideals of R when they exist. Although we do not have compatibility of the exponent of a product of elements of R, an inequality involving the exponent of the product of elements of R is satisfied (see 3 in 1.2.10);
- To extend the technique to handle bimodules shown in Chapter 2 to the context of these algebras. We know that algebras with PBW bases satisfies the key result of this technique (see Corollary 2.5.3);
- To devise algorithms to check the compatibility of reduction systems (e.g., using Linear Programming);
- To find more examples, other than G-Algebras and Yang-Baxter Algebras, of this type of standard finitely presented algebras R;

Some other tasks to do are:

- To code our libraries of procedures built in Maple (see the companion CD, or [32]) to other Computer Algebra systems as *CoCoA* ([17]), *Singular* ([47]), etc.;
- To extend our library of procedures in order to perform computations in algebras as R.

Notation

A *monoid* will be a set endowed with an associative binary operation together with a neutral element. Although it is not correct English, we will use the widely spread term *well-order*, to refer to any total order on a set satisfying that every non-empty subset has a minimal element.

If k is a field and $X = \{x_1, \ldots, x_n\}$ is a non-empty set (or *alphabet*), we denote by $\langle X \rangle$, resp. $\mathsf{k}\langle X \rangle$, the *free monoid*, resp. the *free associative* k-*algebra*, generated by X. The elements of $\langle X \rangle$ are called *words* or *monomials*, whereas those of $\mathsf{k}\langle X \rangle$ are called *polynomials*. A *standard monomial* (on X) will be an element $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \langle X \rangle \subseteq \mathsf{k}\langle X \rangle$ or in any of their epimorphic images, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n = \mathbb{N} \times \overset{-n-}{\cdots} \times \mathbb{N}$. A *standard polynomial* will be a k-linear combination of standard monomials.

We denote by 1 the neutral element of $\langle X \rangle \subseteq \mathsf{k}\langle X \rangle$.

The symbol $\mathbb{N}^{n,(s)}$ denotes the set $\mathbb{N}^n \times \{1, \ldots, s\}$, for every $n, s \geq 1$. The n-tuple $(0, \ldots, \overset{-i-}{1}, \ldots, 0)$ will be denoted by ϵ_i, and $\boldsymbol{x^{(\alpha,i)}}$ will denote the element $(0, \ldots, \overset{-i-}{x^\alpha}, \ldots, 0) \in R^s$ for all $(\alpha, i) \in \mathbb{N}^{n,(s)}$.

A ring will be an associative ring with a unity. For every ring R, R^{op} will denote its opposite ring. In case R is a k-algebra, R^{op} will denote the opposite algebra of R, and R^{env} will denote its *enveloping algebra* $R \otimes_{\mathsf{k}} R^{\mathrm{op}}$.

Furthermore, for any subset F of the free left R-module R^s, we will denote by ${}_R\langle F \rangle$, $\langle F \rangle_R$, and ${}_R\langle F \rangle_R$ (or simply, $\langle F \rangle$), the left R-module, the right R-module, and the R-bimodule, respectively, generated by F.

We denote by $\{\boldsymbol{e_i}\}_{i=1}^s$ the R-module basis of R^s consisting of $\boldsymbol{e_i} = (0, \ldots, \overset{-i-}{1}, \ldots, 0)$.

Chapter 1

Algebras with PBW bases

Following the terminology and results stated in [7, 13, 57, 73, et al.], in this chapter we collect the background on reduction systems and ambiguities of reductions, including Bergman's Diamond Lemma and an algorithm of reduction adapted to perform a two-sided division in the free algebra. We discuss the equivalence between the notions of two-sided Gröbner basis in the free algebra and complete reduction system. This material allow us to prove, e.g., that Levandovskyy's Non-Degeneracy Conditions (see [61]) are equivalent to the overlap ambiguities of Bergman ([7]) to be resolvable (see Remark 2.1.3 in Ch. 2), or, in an alternative way to that of [40], that the Yang-Baxter Algebra $A(k, X, r)$ associated to a square-free solution (X, r) of the Yang-Baxter Equation is an algebra with a PBW basis (see Prop. 3.3.13 in Ch. 3).

In the second section, we obtain a characterization of algebras with PBW bases (Th. 1.2.4). We focus on the particular class of *standard finitely presented algebras* $R = k\langle X\rangle/I_Q$, with $X = \{x_1, \ldots, x_n\}$ and where

$$Q = \{(x_j x_i, f_{ji}) \,/\, 1 \leq i < j \leq n\}$$

is a complete reduction system, of which G-Algebras and Yang-Baxter Algebras (studied in Chapter 2 and 3, respectively) are examples. We endow these algebras with a computational setting in the sense that an algorithm to perform two-sided divisions is devised and a notion of two-sided Gröbner basis (which can be as a generalization of the well-known one for G-algebras) is considered.

1.1 The Diamond Lemma and Gröbner bases on the free algebra

For every monomial $M \in \langle X \rangle$, we shall use the following notation:

- The *multidegree* of M, denoted by $\mathrm{mdeg}(M)$, is defined as the image of M under the monoid epimorphism $\mathrm{mdeg} : \langle X \rangle \to \mathbb{N}^n$ given by $\mathrm{mdeg}(x_i) = \epsilon_i$ for $1 \leq i \leq n$;
- The *total degree* $\deg(M)$ of M is the *length* as a word, i.e., $\deg(M) = |\alpha| = \alpha_1 + \cdots + \alpha_n$ whenever $\mathrm{mdeg}(M) = \alpha = (\alpha_1, \ldots, \alpha_n)$. In this case, the i-th component α_i of $\mathrm{mdeg}(M)$ is denoted by $\deg_{x_i}(M)$;
- The *misordering index* of $M = x_{i_1} \cdots x_{i_r}$ is the number $\nu(M)$ of pairs (i_j, i_k) with $i_j > i_k$ and $1 \leq k < j \leq r$. Thus, M is *standard* (or *ordered*) if $\nu(M) = 0$, and M is *disordered* if $\nu(M) > 0$.

As a convention, we will assume that $\mathrm{mdeg}(1) = (0, \ldots, 0) \in \mathbb{N}^n$, $\deg(1) = 0$ and $\nu(1) = 0$.

1.1.1 Reductions

1.1.1 Definition. A *reduction system* for $\mathsf{k}\langle X \rangle$ is a subset $Q \subseteq \langle X \rangle \times \mathsf{k}\langle X \rangle$. The components of an element σ of Q will be denoted (W_σ, f_σ), where the first component is a word $W_\sigma \in \langle X \rangle$ and the second one is a polynomial $f_\sigma \in \mathsf{k}\langle X \rangle$. Each reduction system Q for $\mathsf{k}\langle X \rangle$ defines a factor algebra $\mathsf{k}\langle X \rangle / I_Q$, where I_Q denotes the two-sided ideal of $\mathsf{k}\langle X \rangle$ generated by all the polynomials $W_\sigma - f_\sigma$, $\sigma \in Q$.

1.1.2 Definition. A *reduction* (associated to $A, B \in \langle X \rangle$ and $\sigma = (W_\sigma, f_\sigma) \in Q$) for a reduction system Q is defined as a k-linear endomorphism $r_{A\sigma B} : \mathsf{k}\langle X \rangle \to \mathsf{k}\langle X \rangle$ which maps $AW_\sigma B$ to $Af_\sigma B$ and fixes all elements of $\langle X \rangle$ other than $AW_\sigma B$. A reduction $r_{A\sigma B}$ *acts trivially* on an element $f \in \mathsf{k}\langle X \rangle$ if $r_{A\sigma B}(f) = f$.

Note that the (composition of) reductions can be viewed as rewriting rules in $\mathsf{k}\langle X \rangle / I_Q$, since $f + I_Q = r(f) + I_Q$, for any reduction r and $f \in \mathsf{k}\langle X \rangle$.

1.1.3 Definition. Let Q be a reduction system for $\mathsf{k}\langle X \rangle$ and $f, g \in \mathsf{k}\langle X \rangle$.

1. The polynomial f is said to be *irreducible under* Q if all the reductions act trivially on f. We shall denote by $\langle X \rangle_{\mathrm{irr}}$ the subset of $\langle X \rangle$ consisting of all irreducible monomials, i.e.,

$$\langle X \rangle_{\mathrm{irr}} = \{ M \in \langle X \rangle \,/\, M \neq AW_\sigma B, \forall A, B \in \langle X \rangle, \sigma = (W_\sigma, f_\sigma) \in Q \}.$$

Thus, $1 \in \langle X\rangle_{\text{irr}}$ if, and only if, $W_\sigma \neq 1$, for all $\sigma = (W_\sigma, f_\sigma) \in Q$. The sub-vectorspace of $\mathsf{k}\langle X\rangle$ generated by $\langle X\rangle_{\text{irr}}$, or equivalently, the set of all irreducible elements of $\mathsf{k}\langle X\rangle$ under Q, will be denoted by $\mathsf{k}\langle X\rangle_{\text{irr}}$.

2. The polynomial f *reduces* to g, denoted by $f \to_Q g$, if there exists a finite sequence $r_1, \ldots, r_n$ of reductions such that $g = (r_n \circ \cdots \circ r_1)(f)$. A finite sequence of reductions $r_1, \ldots, r_n$ is *final* on f if $(r_n \circ \cdots \circ r_1)(f) \in \mathsf{k}\langle X\rangle_{\text{irr}}$.

3. f is said to be *reduction-finite* if for every infinite sequence $r_1, r_2, \ldots$ of reductions there exists $m > 0$ such that r_i acts trivially on $(r_{i-1} \circ \cdots \circ r_1)(f)$, for all $i > m$. We denote by $\mathsf{k}\langle X\rangle_{\text{fin}}$ the k-vectorspace consisting of all reduction-finite elements of $\mathsf{k}\langle X\rangle$. Note that if $f \in \mathsf{k}\langle X\rangle_{\text{fin}}$, any maximal sequence of reductions $r_1, r_2 \ldots$ such that each r_i acts non-trivially on $(r_{i-1} \circ \cdots \circ r_1)\ (f)$ will be finite, and therefore, it will be a final sequence. Hence, for all $f \in \mathsf{k}\langle X\rangle_{\text{fin}}$, there exists $g \in \mathsf{k}\langle X\rangle_{\text{irr}}$ such that $f \to_Q g$.

4. f is said to be *reduction-unique* if $f \in \mathsf{k}\langle X\rangle_{\text{fin}}$ and the image of f under any final sequence of reductions is unique; this common value will be denoted by $r_Q(f)$. The sub-vectorspace of $\mathsf{k}\langle X\rangle_{\text{fin}}$ consisting of all reduction-unique elements of $\mathsf{k}\langle X\rangle$ is denoted by $\mathsf{k}\langle X\rangle_{\text{un}}$.

Thus, we have the following diagram of k-vectorspaces:

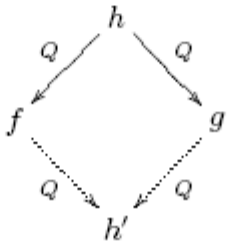
$$\mathsf{k}\langle X\rangle_{\text{irr}} \xhookrightarrow{i} \mathsf{k}\langle X\rangle_{\text{fin}} \xhookrightarrow{i} \mathsf{k}\langle X\rangle$$

and the k-linear map $r_Q : \mathsf{k}\langle X\rangle_{\text{un}} \to \mathsf{k}\langle X\rangle_{\text{irr}}$, which maps every polynomial f to its unique value $r_Q(f)$.

1.1.4 Definition. Let Q be a reduction system for $\mathsf{k}\langle X\rangle$.

1. Q is said to be *confluent* if for all $f, g, h \in \mathsf{k}\langle X\rangle$ such that $h \to_Q f$ and $h \to_Q g$, there exists $h' \in \mathsf{k}\langle X\rangle$ satisfying $f \to_Q h'$ and $g \to_Q h'$.

   This property, called *confluence* or *diamond condition* by Bergman ([7]), can be represented by the following diagram:



2. Q is said to be *noetherian* (or *terminating*) if there is no infinite sequence in $\mathsf{k}\langle X\rangle$

$$f_1 \xrightarrow{r_1} f_2 \xrightarrow{r_2} \cdots \longrightarrow f_n \xrightarrow{r_n} \cdots,$$

where each r_i is a reduction, or equivalently, if $\mathsf{k}\langle X\rangle_{\text{fin}} = \mathsf{k}\langle X\rangle$.

3. A noetherian and confluent system Q is called a *complete reduction system.*

1.1.2 Ambiguities and Diamond Lemma

1.1.5 Definition. Let Q be a reduction system for $\mathsf{k}\langle X\rangle$ and (σ, τ, A, B, C) a 5-tuple, where $\sigma, \tau \in Q$ and $A, B, C \in \mathsf{k}\langle X\rangle$.

1. (σ, τ, A, B, C) is an *overlap ambiguity* for Q if A, B, C are monomials different from 1, $W_\sigma = AB$ and $W_\tau = BC$. An overlap ambiguity (σ, τ, A, B, C) is said to be *resolvable* if there exist compositions of reductions r and r' satisfying $r(f_\sigma C) = r'(Af_\tau)$ (the confluence condition on the results of the two ways of reducing ABC). The *S-polynomial associated to the overlap ambiguity* (σ, τ, A, B, C) is defined as

$$S(\sigma, \tau, A, B, C) = A(W_\tau - f_\tau) - (W_\sigma - f_\sigma)C = f_\sigma C - Af_\tau.$$

2. (σ, τ, A, B, C) is an *inclusion ambiguity* if $\sigma \neq \tau$, $W_\tau = B$ and $W_\sigma = ABC$. In this case, the ambiguity is *resolvable* if $r(Af_\tau B) = r'(f_\sigma)$, for some compositions of reductions r, r'. The *S-polynomial associated to the inclusion ambiguity* (σ, τ, A, B, C) is

$$S(\sigma, \tau, A, B, C) = A(W_\tau - f_\tau)B - (W_\sigma - f_\sigma) = f_\sigma - Af_\tau B.$$

Recall that a partial order $\preceq$ on a monoid $\mathcal{M}$ is said to be a *monoid order* if

$$M_1 \preceq M_2 \Rightarrow AM_1B \preceq AM_2B, \text{ where } A, B, M_1, M_2 \in \mathcal{M}. \tag{1.1}$$

If $\mathcal{M}$ is *cancelative* (i.e. $AM = BM$ or $MA = MB$ implies $A = B$), then condition (1.1) can be replaced by

$$M_1 \prec M_2 \Rightarrow AM_1B \prec AM_2B,\ A, B, M_1, M_2 \in \mathcal{M}. \tag{1.2}$$

1.1.6 Definition. A partial monoid order $\preceq$ on $\langle X\rangle$ is said to be *compatible* with a reduction system Q for $\mathsf{k}\langle X\rangle$ (Q is said to be *compatible with* $\preceq$ as well) if for all $\sigma = (W_\sigma, f_\sigma) \in Q$, the polynomial f_σ is a linear combination of monomials M such that $M \prec W_\sigma$.

In the literature, a reduction system Q together with a compatible total order is also known as a *rewriting system* (see e.g. [57]), and irreducible polynomials under such a Q would be called *normal elements modulo* $\{W_\sigma - f_\sigma\}_{\sigma\in Q}$ in [35, 36, et al.].
Recall that a partial order $\preceq$ on a set $\mathcal{S}$ is said to satisfy the *descending chain condition* (or *d.c.c.*, for short) if for every chain $s_1 \succeq s_2 \succeq \cdots \succeq s_n \succeq \cdots$ of elements of $\mathcal{S}$, there exists $m \geq 1$ such that $s_n = s_m$, for all $n \geq m$. Some authors (see e.g. [57]) call the partial orders satisfying the d.c.c. *well-founded* orders.

1.1.7 Remark. [13] If $\preceq$ is a monoid partial order on $\langle X\rangle$, compatible with a reduction system Q and satisfying the d.c.c., then $\mathsf{k}\langle X\rangle_{\text{fin}} = \mathsf{k}\langle X\rangle$, that is, Q is noetherian. Therefore, for all $f \in \mathsf{k}\langle X\rangle$, there exists $g \in \mathsf{k}\langle X\rangle_{\text{irr}}$ such that $f \to_Q g$.

Let Q be a reduction system for $\mathsf{k}\langle X\rangle$ and $\preceq$ a monoid partial order on $\langle X\rangle$. For each monomial $M \in \langle X\rangle$, let us denote by Y_M the sub-vectorspace of $\mathsf{k}\langle X\rangle$ spanned by all polynomials $A(W_\sigma - f_\sigma)B$ satisfying $AW_\sigma B \prec M$, where $\sigma \in Q$, $A, B \in \langle X\rangle$.

1.1.8 Definition. Let Q be a reduction system for $\mathsf{k}\langle X\rangle$ and $\preceq$ a monoid partial order on $\langle X\rangle$ compatible with Q. An overlap, resp. inclusion, ambiguity (σ, τ, A, B, C) is said to be *resolvable relative to* $\preceq$ if $f_\sigma C - Af_\tau \in Y_{ABC}$, resp. if $Af_\tau C - f_\sigma \in Y_{ABC}$.

1.1.9 Remark. [7] Any resolvable ambiguity is resolvable relative to $\preceq$. This may be proved directly by using the Reduction Theorem 1.1.16.

There is a result due to Newman [74, Sect. 3] (cf. [7]) written in a graph-theoretic formulation which states that, assuming the *d.c.c.* and the *confluence condition* on a oriented graph, the reduction procedure on the graph yields unique canonical forms for elements of the original algebraic object. This result was often called *Diamond Lemma*.
Bergman translated it to the context of associative rings, avoiding the graph formulation. The advantage presented by his result, *Bermang's Diamond Lemma*, is that the d.c.c. and the confluence condition need only be verified for monomials.

1.1.10 Theorem. (Bergman's Diamond Lemma) [7] *Let Q be a reduction system for $\mathsf{k}\langle X\rangle$, and $\preceq$ a monoid partial order on $\langle X\rangle$ compatible with Q, satisfying the d.d.c.. The following conditions are equivalent:*

1. *All ambiguities for Q are resolvable;*

2. *All ambiguities for Q are resolvable relative to $\preceq$;*

3. *All elements of $k\langle X\rangle$ are reduction-unique under Q;*

4. *The set $\{M + I_Q \,/\, M \in \langle X\rangle_{\mathrm{irr}}\}$ is a k-basis of the algebra $k\langle X\rangle/I_Q$.*

When these conditions hold, $k\langle X\rangle/I_Q$ can be identified with the k-vectorspace $k\langle X\rangle_{\mathrm{irr}}$, whose multiplication is given by $f \cdot g = r_Q(fg)$, for all $f, g \in k\langle X\rangle_{\mathrm{irr}}$.

The original proof can be found in [7]. In [13] there is a detailed one.

1.1.3 Reduction algorithm

Until the end of this chapter we shall deal with more specific orders on $\langle X\rangle$: the so-called *monomial orders*. The following definition is equivalent to some appearing in different contexts, e.g., in [61], in [70] under the name of *positive term ordering*, or in [73], as *semigroup ordering*.

1.1.11 Definition. A partial order $\preceq$ defined on a cancelative monoid $\mathcal{M}$ is said to be *monomial* if $\preceq$ is a monoid total well-order on $\mathcal{M}$.
In particular, when the monoid $\mathcal{M}$ is $\mathbb{N}^n$, a monomial order on $\mathbb{N}^n$ is also called an *admissible order*.

1.1.12 Example. Let X be a finite set. The order $\preceq_{deglex}$ on $\langle X\rangle$ is a monomial order, whereas $\preceq_{lex}$ is not (see the definitions in Appendix A). However, the lexicographical order has an analogous definition on $\mathbb{N}^n$ (see Appendix A) so that it is an admissible order on $\mathbb{N}^n$. There is also a degree lexicographical order defined on $\mathbb{N}^n$, which is an admissible order.

1.1.13 Remark. The proofs of the following statements can be looked up in [1, 13, 18, et al.].

- If $\preceq$ is a total order on a set S, then $\preceq$ is a well-order if, and only if, it satisfies the d.c.c..

- If $\preceq$ is a monoid total order on $\langle X\rangle$, resp. on $\mathbb{N}^n$ (or in general, on any cancelative monoid), then the d.c.c. implies $1 \prec M$ for all $M \in \langle X\rangle \setminus \{1\}$, resp. $0 \prec \alpha$ for all $\alpha \in \mathbb{N}^n \setminus \{0\}$.

- In the case of the monoid $\mathbb{N}^n$, the d.c.c. is also a necessary condition for $0 \preceq \alpha, \forall\, \alpha \in \mathbb{N}^n$ (by using *Dickson's Lemma* in $\mathbb{N}^n$). Thus, if $\preceq$ is a monoid total order on $\mathbb{N}^n$, then $\preceq$ is an admissible order if, and only if, one of the following equivalent conditions holds:

1. $\preceq$ is a well-order on $\mathbb{N}^n$;
2. $\preceq$ satisfies the d.c.c. on $\mathbb{N}^n$;
3. $0 \preceq \alpha$, for all $\alpha \in \mathbb{N}^n$.

1.1.14 If $\preceq$ is a monomial order on $\langle X \rangle$, then each polynomial $f \in \mathsf{k}\langle X \rangle$ has a unique *representation*

$$f = \sum_{i=1}^{r} \lambda_i M_i,$$

with $\lambda_i \in \mathsf{k}\langle X \rangle \setminus \{0\}$, and $M_1 \succ M_2 \succ \cdots \succ M_r \in \langle X \rangle$. In this case, $M_1 = \max_{\preceq}\{M_i\}_{i=1}^{r}$ is called the *leading monomial* of f and it is denoted by $\operatorname{lm}(f)$. The element λ_1, denoted by $\operatorname{lc}(f)$, is said to be the *leading coefficient* of f. The *leading term* $\operatorname{lt}(f)$ of f is defined as

$$\operatorname{lt}(f) = \operatorname{lc}(f) \operatorname{lm}(f) = \lambda_1 M_1.$$

It is easy to check that

1. $\operatorname{lm}(f+g) \preceq \max\{\operatorname{lm}(f), \operatorname{lm}(g)\}$;
2. $\operatorname{lm}(f+g) \prec \max\{\operatorname{lm}(f), \operatorname{lm}(g)\} \iff \operatorname{lt}(f) = -\operatorname{lt}(g)$,

and that the leading coefficient, monomial and term are compatible with the product of polynomials, in the following sense:

$$\begin{aligned} \operatorname{lc}(fg) &= \operatorname{lc}(f) \operatorname{lc}(g); \\ \operatorname{lm}(fg) &= \operatorname{lm}(f) \operatorname{lm}(g); \\ \operatorname{lt}(fg) &= \operatorname{lt}(f) \operatorname{lt}(g), \end{aligned} \tag{1.3}$$

for all $f, g \in \mathsf{k}\langle X \rangle \setminus \{0\}$.

1.1.15 Note. Every admissible order on $\mathbb{N}^n$ induces a monomial order on $\langle X \rangle$ (see the definition in Appendix A). We denote both orders by the same symbol $\preceq$.
Moreover, it is possible to extend any monomial order $\preceq$ on $\langle X \rangle$ to a partial order on $\mathsf{k}\langle X \rangle$, also denoted by $\preceq$ (see Appendix A). Note that the order $\preceq$ on $\mathsf{k}\langle X \rangle$ inherits the d.c.c. from $\preceq$ on $\langle X \rangle$, i.e., there is no infinite sequence $f_1 \succ f_2 \succ \cdots$ in $\mathsf{k}\langle X \rangle$.

Next we present a slight variation of the procedures which appeared in [5, 61, 73, et al.] for reducing any polynomial to an irreducible one, provided a reduction system. It can also be viewed as a procedure to perform a *two-sided*

division of a non-zero polynomial $f \in \mathsf{k}\langle X\rangle$ by a set of divisors $G = \{g_i\}_i \subset \mathsf{k}\langle X\rangle$, from which the reduction system $Q = \{(\mathrm{lm}\,(g_i), \mathrm{lm}\,(g_i) - \mathrm{lc}\,(g_i)^{-1} g_i)\}_i$ is constructed. One obtains a *remainder* in $\mathsf{k}\langle X\rangle$, and the quotients in the *enveloping algebra* $\mathsf{k}\langle X\rangle \otimes_{\mathsf{k}} (\mathsf{k}\langle X\rangle)^{\mathrm{op}}$. Recall that $\mathsf{k}\langle X\rangle$ is a left $\mathsf{k}\langle X\rangle \otimes_{\mathsf{k}} (\mathsf{k}\langle X\rangle)^{\mathrm{op}}$-module with the action $(f \otimes g)h = fhg$, for $f, g, h \in \mathsf{k}\langle X\rangle$.

1.1.16 Theorem. (Reduction Theorem) *Let $\preceq$ be a monomial order on $\langle X\rangle$, compatible with a reduction system Q for $k\langle X\rangle$. Every polynomial $f \in k\langle X\rangle \setminus \{0\}$ can be written as*

1. *$f = q + r$, where*
2. *$q = \sum_{\sigma \in Q} q_\sigma (W_\sigma - f_\sigma)$, with*

$$q_\sigma = \sum_{\mathrm{i;\,finite}} \lambda_{\sigma,i} (A_{\sigma,i} \otimes B_{\sigma,i}), \text{ and } A_{\sigma,i} W_\sigma B_{\sigma,i} \preceq \mathrm{lm}\,(f);$$

3. *if $r \neq 0$, then $r \in k\langle X\rangle_{\mathrm{irr}}$ and $\mathrm{lm}\,(r) \preceq \mathrm{lm}\,(f)$.*

Proof. The proof is based on the construction, in each step j of the procedure, of polynomials $p^{(j)}, q^{(j)}, r^{(j)} \in \mathsf{k}\langle X\rangle$ satisfying the following conditions:

1. $f = p^{(j)} + q^{(j)} + r^{(j)}$, where
2. $q^{(j)} = \sum_{\sigma \in Q} q^j_\sigma (W_\sigma - f_\sigma)$, with

$$q^j_\sigma = \sum_{\mathrm{i;\,finite}} \lambda^j_{\sigma,i} (A^j_{\sigma,i} \otimes B^j_{\sigma,i}), \text{ and } A^j_{\sigma,i} W_\sigma B^j_{\sigma,i} \preceq \mathrm{lm}\,(f);$$

3. if $r^{(j)} \neq 0$, then $r^{(j)} \in \mathsf{k}\langle X\rangle_{\mathrm{irr}}$ and $\mathrm{lm}\,(r^{(j)}) \preceq \mathrm{lm}\,(f)$;
4. if $p^{(j)} \neq 0$, then $\mathrm{lm}\,(p^{(j+1)}) \prec \mathrm{lm}\,(p^{(j)}) \preceq \mathrm{lm}\,(f)$.

The method starts with $p^{(0)} = f$, $q^{(0)} = 0$ and $r^{(0)} = 0$. Let us see how to construct the step $j+1$ from the step j.
If $\mathrm{lm}\,(p^{(j)}) \in \langle X\rangle_{\mathrm{irr}}$, then put

$$\begin{aligned} p^{(j+1)} &:= p^{(j)} - \mathrm{lt}\,(p^{(j)}), \\ q^{(j+1)} &:= q^{(j)}, \\ r^{(j+1)} &:= r^{(j)} + \mathrm{lt}\,(p^{(j)}). \end{aligned}$$

In the other case, if $\mathrm{lm}\,(p^{(j)}) \notin \langle X\rangle_{\mathrm{irr}}$, then pick $A, B \in \langle X\rangle$ and $\sigma = (W_\sigma, f_\sigma) \in Q$ such that $\mathrm{lm}\,(p^{(j)}) = AW_\sigma B$, and put

$$\begin{aligned} p^{(j+1)} &:= p^{(j)} - \mathrm{lc}\,(p^{(j)})A(W_\sigma - f_\sigma)B, \\ q^{(j+1)} &:= q^{(j)} + \mathrm{lc}\,(p^{(j)})(A \otimes B)(W_\sigma - f_\sigma) \\ &= q^{(j)} + \mathrm{lc}\,(p^{(j)})A(W_\sigma - f_\sigma)B, \\ r^{(j+1)} &:= r^{(j)}. \end{aligned}$$

Thus, we obtain a strictly descending sequence

$$\mathrm{lm}\,(f) \succeq \mathrm{lm}\,(p^{(1)}) \succ \mathrm{lm}\,(p^{(2)}) \succ \cdots \succ \mathrm{lm}\,(p^{(n)}) \succ \cdots,$$

which must stop for some $m \geq 1$, i.e., there exists $m \geq 1$ such that $p^{(m)} = 0$, since $\preceq$ satisfies the d.c.c. on $\langle X\rangle$. □

1.1.17 Corollary. *If Q is a reduction system for $\mathsf{k}\langle X\rangle$, compatible with a monomial order $\preceq$ on $\langle X\rangle$, then the set*

$$\{M + I_Q \;/\; M \in \langle X\rangle_{\mathrm{irr}}\}$$

is a generator system of $\mathsf{k}\langle X\rangle/I_Q$ as a k-vectorspace, i.e., $\mathsf{k}\langle X\rangle = \mathsf{k}\langle X\rangle_{\mathrm{irr}} + I_Q$.

Algorithm 1 Reduction in $\mathsf{k}\langle X\rangle$

Require: $f \in \mathsf{k}\langle X\rangle$, and Q a reduction system, compatible with a monomial order $\preceq$ on $\langle X\rangle$;
Ensure: $q, r \in \mathsf{k}\langle X\rangle$ such that $f = q + r$, satisfying conditions 1, 2 and 3 in 1.1.16;
Initialization: $p := f$, $q := 0$, $r := 0$;
while $p \neq 0$ **do**
  if $\mathrm{lm}\,(p) \notin \langle X\rangle_{\mathrm{irr}}$ **then**
    Take $A, B \in \langle X\rangle$ and $\sigma = (W_\sigma, f_\sigma) \in Q$ such that $\mathrm{lm}\,(p) = AW_\sigma B$;
    $p := p - \mathrm{lc}\,(p)(A(W_\sigma - f_\sigma)B)$;
    $q := q + \mathrm{lc}\,(p)(A(W_\sigma - f_\sigma)B)$;
  else
    $p := p - \mathrm{lt}\,(p)$;
    $r := r + \mathrm{lt}\,(p)$;
  end if
end while
Return q, r.

1.1.18 Remark. Theorem 1.1.16 provides a method (Algorithm 1) to compute for any non-zero polynomial $f \in \langle X \rangle$ a representation as in 1.1.16. Note that effectiveness of this algorithm requires to solve the problem of deciding if a monomial M is irreducible or not, that is, if M belongs to the set $\{AW_\sigma B \,/\, A, B \in \langle X \rangle, \sigma \in Q\}$.
Thus, if the reduction system Q is finite, the ground field k is computable and the monomial order $\preceq$ on $\langle X \rangle$ is *decidable* (i.e. it is possible to effectively order a finite set of monomials, e.g., $\preceq_{deglex}$ (cf. [73])), then Algorithm 1 is effective. In [73] a discussion on the effectiveness of such algorithm as well as of the computation of Gröbner bases can be found.

1.1.19 Definition. Under the assumptions of 1.1.16, a *normal form* or *remainder* of f by Q is any polynomial $r \in \mathsf{k}\langle X \rangle$ satisfying conditions 1, 2 and 3 in 1.1.16. Every normal form of f by Q is denoted by $\overline{f}^{Q}$.

1.1.20 Lemma. *Let Q be a reduction system for $k\langle X \rangle$ compatible with a monomial order $\preceq$ on $\langle X \rangle$. For any $f \in k\langle X \rangle \setminus \{0\}$, and any reduction r acting non-trivially on f, namely $r = r_{A\sigma B}$ with $\sigma = (W_\sigma, f_\sigma) \in Q$,*

i) $r(f) \prec f$, where $\preceq$ is the order on $k\langle X \rangle$ defined from $\preceq$ on $\langle X \rangle$ (see Appendix A);

ii) $f - r(f) = \lambda A(W_\sigma - f_\sigma)B$, for some $\lambda \in k \setminus \{0\}$, $A, B \in \langle X \rangle$.

Proof. Since $r = r_{A\sigma B}$ acts non-trivially on f, we can write

$$f = \lambda A W_\sigma B + \sum_{\text{i; finite}} \lambda_i M_i, \tag{1.4}$$

where $\lambda, \lambda_i \in \mathsf{k} \setminus \{0\}$, $M_i \in \langle X \rangle$ and $M_i \neq AW_\sigma B$, for all i.
We use induction on the number n of monomials of f. If $n = 1$, then $f = \lambda AW_\sigma B$, and the result trivially follows. Let us check the case $n = 2$. Assume that

$$f = \lambda AW_\sigma B + \mu M,$$

where $M \neq AW_\sigma B$ and $\lambda, \mu \in \mathsf{k} \setminus \{0\}$. It follows that

$$\begin{aligned} f - r(f) &= (\lambda AW_\sigma B + \mu M) - (\lambda A f_\sigma B + \mu M) \\ &= \lambda A(W_\sigma - f_\sigma)B. \end{aligned}$$

If $M \prec AW_\sigma B$, then $\operatorname{lm}(r(f)) \preceq \max\{A \operatorname{lm}(f_\sigma) B, M\} \prec \operatorname{lm}(f)$. Otherwise, if $AW_\sigma B \prec M$, then $\operatorname{lm}(f) = M = \operatorname{lm}(r(f))$, but also

$$r(f) - \operatorname{lt}(f) = \lambda A f_\sigma B \prec AW_\sigma B = f - \operatorname{lt}(f).$$

In both cases, $r(f) \prec f$. Assume now that the result is satisfied by any polynomial on which r acts non-trivially, with a number of monomials less than n. Let us prove it for the case when f has n monomials. If we write f as in (1.4), then

$$r(f) = \lambda A f_\sigma B + \sum_i \lambda_i M_i,$$

and obviously, $f - r(f) = \lambda A(W_\sigma - f_\sigma)B$. If $\mathrm{lm}\,(f) = AW_\sigma B$, then $\mathrm{lm}\,(r(f)) \prec \mathrm{lm}\,(f)$, and therefore, $r(f) \prec f$. Otherwise, there exists a monomial M_0 in the set of monomials $\{M_i\}_i$ of f such that $\mathrm{lm}\,(f) = M_{i_0} = \mathrm{lm}\,(r(f))$. Note that

$$f - \mathrm{lt}\,(f) = \lambda A W_\sigma B + \sum_{i \neq i_0} \lambda_i M_i,$$

is a polynomial with $n-1$ monomials and that r acts non-trivially on it. Thus, applying the induction, we conclude that $r(f - \mathrm{lt}\,(f)) \prec f - \mathrm{lt}\,(f)$, and hence, $r(f) \prec f$. □

1.1.21 Corollary. *Let Q be a reduction system for $\mathsf{k}\langle X\rangle$, compatible with a monomial order $\preceq$ on $\langle X\rangle$.*
Then, for all $f \in \mathsf{k}\langle X\rangle$ and all final sequences of reductions $r_1, \ldots, r_n$ on f, $(r_n \circ \cdots \circ r_1)(f)$ is a normal form of f (by 1.1.7 and the d.c.c. on the order $\preceq$ on $\mathsf{k}\langle X\rangle$, we already know that for each polynomial f there exists such a sequence).
In particular, if $f \in \mathsf{k}\langle X\rangle_{\mathrm{un}}$, then $r_Q(f)$ is a normal form of f by Q.

Proof. The statement 1.1.21 can be proved by applying induction on the length n of a final sequence of reductions $r_1, \ldots, r_n$ on a polynomial $f \notin \mathsf{k}\langle X\rangle_{\mathrm{irr}}$ (if $f \in \mathsf{k}\langle X\rangle_{\mathrm{irr}}$, it trivially holds that $(r_n \circ \cdots \circ r_1)(f) = f$ is a normal form of f). For each $i \in \{1, \ldots, n\}$ assume w.l.o.g. that $r_i = r_{A_i \sigma_i B_i}$ for some $A_i, B_i \in \langle X\rangle$ and $\sigma_i \in Q$ such that r_i acts non-trivially on $(r_{i-1} \circ \cdots \circ r_1)(f)$. From Lemma 1.1.20, one can check that

$$f - (r_i \circ \cdots \circ r_1)(f) = \sum_{j=1}^{i} \lambda_j A_j (W_{\sigma_j} - f_{\sigma_j}) B_j, \quad \lambda_j \in \mathsf{k} \setminus \{0\},$$

with $A_j W_{\sigma_j} B_j \preceq \mathrm{lm}\,(f)$, and $\mathrm{lm}\,((r_i \circ \cdots \circ r_1)(f)) \preceq \mathrm{lm}\,(f)$. □

1.1.22 Note. The converse of Corollary 1.1.21 is not always true, i.e., there exist normal forms $\overline{f}^{Q}$ of f such that $\overline{f}^{Q} \neq (r_n \circ \cdots \circ r_1)(f)$ for all final sequences of reductions $r_1, \ldots, r_n$ on f.
Indeed, for the alphabet $X = \{x_1, x_2, x_3\}$, consider the reduction system $Q = \{(x_3x_2, x_2), (x_3x_1, x_3), (x_2x_1, x_1)\}$ for $\mathsf{k}\langle X\rangle$, compatible with the order

$\preceq_{deglex}$ on $\langle X\rangle$. The polynomial $f = x_3^4 - x_3x_1 + x_2x_1$ can be written as

$$f = x_3(x_2x_1 - x_1) - (x_3x_2 - x_2)x_1 + x_3^4,$$

with $x_3x_2x_1 \preceq_{deglex} x_3^4 = \mathrm{lm}\,(f)$. Hence, $x_3^4 \in \mathsf{k}\langle X\rangle_{\mathrm{irr}}$ is a normal form of f. But $f \not\to_Q x_3^4$.

1.1.4 Two-sided Gröbner bases

1.1.23 Definition. Let $\preceq$ be a monomial order on $\langle X\rangle$ and G a subset of $\mathsf{k}\langle X\rangle$. We shall denote by $\mathrm{M}\,(G)$ the *set of monomials* $\{\mathrm{lm}\,(g)/g \in G\backslash\{0\}\} \subseteq \langle X\rangle$ of G. The *leading ideal of* G, denoted by $\mathrm{L}\,(G)$, is the two-sided ideal generated by $\mathrm{M}\,(G)$, i.e.,

$$\mathrm{L}\,(G) = {}_{\mathsf{k}\langle X\rangle}\langle\, \mathrm{lm}\,(g) \,/\, g \in G \setminus \{0\} \,\rangle_{\mathsf{k}\langle X\rangle}.$$

Note that if G is a two-sided generator system of a two-sided ideal $I \subseteq \mathsf{k}\langle X\rangle$, it can easily be checked that

$$\mathrm{M}\,(G) \subseteq \mathrm{L}\,(G) \cap \langle X\rangle \subseteq \mathrm{L}\,(I) \cap \langle X\rangle = \mathrm{M}\,(I), \tag{1.5}$$

$$\langle X\rangle \setminus \mathrm{M}\,(I) \subseteq \langle X\rangle_{\mathrm{irr}} \subseteq \langle X\rangle \setminus \mathrm{M}\,(G), \tag{1.6}$$

with respect to the reduction system $Q = \{(\mathrm{lm}\,(g), \mathrm{lm}\,(g) - \mathrm{lc}\,(g)^{-1}g)\}_{g\in G}$ for $\mathsf{k}\langle X\rangle$.

1.1.24 Definition. Let $\preceq$ be a monomial order on $\langle X\rangle$, and I a two-sided ideal of $\mathsf{k}\langle X\rangle$. A two-sided generator system G of I is said to be a *two-sided Gröbner basis for* I with respect to $\preceq$ if $\mathrm{L}\,(G) = \mathrm{L}\,(I)$.
A set $G \subseteq \mathsf{k}\langle X\rangle$ is a *two-sided Gröbner basis* if G is a two-sided Gröbner basis for the two-sided ideal ${}_{\mathsf{k}\langle X\rangle}\langle G\rangle_{\mathsf{k}\langle X\rangle}$ generated by G.

Trivially, a two-sided ideal $I \subseteq \mathsf{k}\langle X\rangle$ is always a two-sided Gröbner basis for itself. The condition of being a two-sided Gröbner basis in the free algebra $\mathsf{k}\langle X\rangle$ can be characterized in different ways. Essentially, two-sided Gröbner bases may be viewed as sets $G \subseteq \mathsf{k}\langle X\rangle$ for which the reduction system $Q = \{(\mathrm{lm}\,(g), \mathrm{lm}\,(g) - \mathrm{lc}\,(g)^{-1}g)\}_{g\in G}$ satisfies (one of) the conditions of the Diamond Lemma. In the following result we collect some alternative definitions of the notion of two-sided Gröbner basis. Most of them are very well-known. In the literature, they usually appear independently in the context of reductions systems (see e.g. [57]), and in the context of leading ideals and normal forms (see e.g. [73]). Here we recall the most important ones from both points of view, unifying the notation, and we add two more characterizations (2 and 3), naturally arising from Definition 1.1.24.

1.1.25 Theorem. *Let $\preceq$ be a monomial order on $\langle X\rangle$. Let G be a two-sided generator system of a two-sided ideal I of $k\langle X\rangle$ and consider the reduction system $Q = \{(\mathrm{lm}\,(g), \mathrm{lm}\,(g) - \mathrm{lc}\,(g)^{-1}g)\}_{g\in G}$ for $k\langle X\rangle$.*
The following conditions are equivalent:

1. *G is a two-sided Gröbner basis for I;*
2. *$\mathrm{L}\,(G)\bigcap\langle X\rangle = \mathrm{M}\,(I)$;*
3. *$\langle X\rangle_{\mathrm{irr}} = \langle X\rangle \setminus \mathrm{M}\,(I)$;*
4. *All ambiguities of Q are resolvable;*
5. *All ambiguities of Q are resolvable relative to $\preceq$;*
6. *All elements of $k\langle X\rangle$ are reduction-unique under Q;*
7. *The set $\{M + I \,/\, M \in \langle X\rangle_{\mathrm{irr}}\}$ is a k-basis of the algebra $k\langle X\rangle/I$;*
8. *$k\langle X\rangle = k\langle X\rangle_{\mathrm{irr}} \bigoplus I$, or equivalently, $k\langle X\rangle_{\mathrm{irr}} \bigcap I = \{0\}$;*
9. *$k\langle X\rangle/I \cong k\langle X\rangle_{\mathrm{irr}}$;*
10. *Q is complete, or equivalently, noetherian;*
11. *All $f \in I$ has a unique normal form $\overline{f}^{Q}$, which is 0;*
12. *For all $f \in k\langle X\rangle \setminus \{0\}$, $f \in I$ if, and only if, f can be written as*

$$f = \sum_{g\in G} q_g g, \text{ with } q_g = \sum_{\text{finite}} \lambda_{i,g}(A_{i,g} \otimes B_{i,g}),$$

and $\mathrm{lm}\,(f) = \max_{\preceq}\{A_{i,g}\mathrm{lm}\,(g)B_{i,g}\}_{i,g}$;

13. *For all $f \in I$, $f \to_Q 0$, or equivalently, for all $f \in k\langle X\rangle$,*

$$f \in I \iff f \to_Q 0;$$

14. *Every $f \in k\langle X\rangle$ has a unique normal form $\overline{f}^{Q}$;*
15. *$S(\sigma, \tau, A, B, C) \to_Q 0$, for every S-polynomial $S(\sigma, \tau, A, B, C)$;*

Proof. Equations (1.5), (1.6) lead us to the equivalence between the first 3 statements. The equivalences between 4, 5, 6 and 7 are given by the Diamond Lemma in 1.1.10. The ones between 7, 8 and 9 are results of Linear algebra.
(6) $\Leftrightarrow$ (10). Assume that all polynomials are reduction-unique under Q. From 1.1.7 it follows that Q is noetherian. Let us see that it is confluent. Suppose that $f \to_Q g_1$ and $f \to_Q g_2$, with $f, g_1, g_2 \in \mathsf{k}\langle X\rangle$. Also by 1.1.7, $g_1 \to_Q h_1$ and $g_2 \to_Q h_2$, for some $h_1, h_2 \in \mathsf{k}\langle X\rangle_{\text{irr}}$. Therefore, $f \to_Q h_1$ and $f \to_Q h_2$. Since $f \in \mathsf{k}\langle X\rangle_{\text{un}}$, one has $h_1 = h_2$. Conversely, if Q is complete and if for an arbitrary polynomial $f \in \mathsf{k}\langle X\rangle$, $f \to_Q g_1$ and $f \to_Q g_2$ with $g_1, g_2 \in \mathsf{k}\langle X\rangle_{\text{irr}}$, then there exists $h' \in \mathsf{k}\langle X\rangle$ such that $g_1 \to_Q h'$ and $g_2 \to_Q h'$. Since g_1 and g_2 are irreducible, $h' = g_1 = g_2$. Hence, f is reduction-unique under Q.
(1) $\Rightarrow$ (8) $\Rightarrow$ (11) $\Rightarrow$ (1). Suppose $\mathrm{L}(G) = \mathrm{L}(I)$. If $f \in \mathsf{k}\langle X\rangle_{\text{irr}} \bigcap I$, then f has to be zero, because otherwise, $\mathrm{lm}(f) \in \mathrm{L}(G)$ implies $\mathrm{lm}(f) = A\,\mathrm{lm}(g)\,B$, for some $g \in G$ and $A, B \in \langle X\rangle$, which is a contradiction since $\mathrm{lm}(f) \in \langle X\rangle_{\text{irr}}$. Assuming 8, for all $f \in I \setminus \{0\}$, every normal form $\overline{f}^{Q}$ of f has to be zero since there exists $q \in I$ such that $\overline{f}^{Q} = f - q \in \mathsf{k}\langle X\rangle_{\text{irr}} \bigcap I$. Now, suppose 11 and let us see that $\mathrm{L}(G) = \mathrm{L}(I)$. If $f \in I \setminus \{0\}$, then, since $\overline{f}^{Q} = 0$,

$$f = \sum_{k,g \in G} \lambda_{k,g} A_{k,g} (\mathrm{lm}(g) - (\mathrm{lm}(g) - \mathrm{lc}(g)^{-1} g)) B_{k,g},$$

with $\lambda_{k,g} \in \mathsf{k}$, $A_{k,g}, B_{k,g} \in \langle X\rangle$, and

$$A_{k,g}\mathrm{lm}(g)B_{k,g} \preceq \mathrm{lm}(f). \tag{1.7}$$

Thus, there exist k, g such that either $\mathrm{lm}(f) = A_{k,g}\mathrm{lm}(g)B_{k,g}$, or

$$\begin{aligned} \mathrm{lm}(f) &= \mathrm{lm}\left(A_{k,g}(\mathrm{lm}(g) - \mathrm{lc}(g)^{-1} g) B_{k,g}\right) \\ &= A_{k,g}\mathrm{lm}\left(\mathrm{lm}(g) - \mathrm{lc}(g)^{-1} g\right) B_{k,g} \\ &\prec A_{k,g}\mathrm{lm}(g)B_{k,g}, \end{aligned}$$

but this is a contradiction with Equation (1.7). Hence, $\mathrm{lm}(f) \in \mathrm{L}(G)$.
(11) $\Rightarrow$ (12) $\Rightarrow$ (1). If 11 holds, then the statement 12 is a consequence of Theorem 1.1.16. Condition 12 implies that G is a two-sided Gröbner basis for I, since $\mathrm{lm}(f) \in \mathrm{L}(G)$ for all $f \in I$.
(11) $\Rightarrow$ (13) $\Rightarrow$ (15) $\Rightarrow$ (4). The first implication is a consequence of 1.1.21, and the second one is perfectly straightforward. Assume now that all the S-polynomials can be reduced to zero, and let us see that all ambiguities are resolvable. Let (σ, τ, A, B, C) be an overlap ambiguity, and $S(\sigma, \tau, A, B, C)$ its associated S-polynomial. Since $S(\sigma, \tau, A, B, C) \to_Q 0$, there exists a

composition of reductions such that $r(f_\sigma C - A f_\tau) = 0$. Hence $r(f_\sigma C) = r(A f_\tau)$, so (σ, τ, A, B, C) is resolvable. Analogously, inclusion ambiguities are resolvable.
(1) $\Rightarrow$ (14) $\Rightarrow$ (4). Under the assumption of 1, if r and r' are two normal forms of f, then

$$r - r' = (f - q) - (f - q') = q' - q \in I \cap \mathsf{k}\langle X\rangle_{\mathrm{irr}},$$

for some $q, q' \in I$. Therefore $r = r'$, since in other case, $\mathrm{lm}\,(r - r') \in \mathrm{L}\,(G)$, so $\mathrm{lm}\,(r - r') = A\,\mathrm{lm}\,(g)\,B$ for some $A, B \in \langle X\rangle$ and $g \in G$, which is impossible because $\mathrm{lm}\,(r - r') \in \langle X\rangle_{\mathrm{irr}}$. Assuming 14, the statement 4 is a consequence of 1.1.21. □

1.1.26 Remark. Under the assumptions of Theorem 1.1.25, if G is a two-sided Gröbner basis for I, then the converse of 1.1.21 is true, i.e., for all $f \in \mathsf{k}\langle X\rangle$,

$$\overline{f}^{Q} \text{ is a normal form of } f \iff f \to_Q \overline{f}^{Q} \text{ and } \overline{f}^{Q} \in \mathsf{k}\langle X\rangle_{\mathrm{irr}}.$$

Indeed, from 1.1.7 it follows that for all $f \in \mathsf{k}\langle X\rangle$, there exists $g \in \mathsf{k}\langle X\rangle_{\mathrm{irr}}$ such that $f \to_Q g$. From 1.1.21 we have that g is a normal form of f. Thus, any normal form $\overline{f}^{Q}$ of f has to be g since f has a unique normal form (by 14 in 1.1.25).

1.2 Obtaining algebras with PBW bases from reduction systems

In this section we find necessary and sufficient conditions for obtaining algebras with PBW bases in terms of reduction systems, assuming certain hypotheses.

1.2.1 Definition. Let R be a k-algebra. R is an *algebra with a PBW basis* if there exist $x_1, \ldots, x_n \in R$ such that the set of standard monomials $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ is a basis of R as a k-vectorspace.

The k-algebras with PBW bases are also recognized in the literature as *polynomial algebras over* k (see, e.g., [13]). The basis $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ of such algebras is usually called a *PBW basis*.

1.2.2 Lemma. *Let* $X = \{x_1, \ldots, x_n\}$ *and* $Q \subseteq \langle X\rangle \times k\langle X\rangle$ *a reduction system for* $k\langle X\rangle$. *Then*

1. $\langle X\rangle_{\mathrm{irr}} \subseteq \{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ *if, and only if,* $\{x_j x_i \,/\, 1 \leq i < j \leq n\} \subseteq \{AW_\sigma B \,/\, A, B \in \langle X\rangle,\ (W_\sigma, f_\sigma) \in Q\}$;

2. $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\} \subseteq \langle X\rangle_{\mathrm{irr}}$ *if, and only if,* $\{W_\sigma \,/\, (W_\sigma, f_\sigma) \in Q\} \subseteq \{Ax_j x_i B \,/\, 1 \leq i < j \leq n,\ A, B \in \langle X\rangle\}$.

Proof. Suppose that $\langle X\rangle_{\mathrm{irr}} \subseteq \{x^\alpha\}_{\alpha\in\mathbb{N}^n}$. Then, for $j > i$, $x_j x_i \notin \langle X\rangle_{\mathrm{irr}}$. So, $x_j x_i = AW_\sigma B$ for some $A, B \in \langle X\rangle$ and $(W_\sigma, f_\sigma) \in Q$. Conversely, if $\{x_j x_i\}_{i<j} \subseteq \{AW_\sigma B \,/\, A, B \in \langle X\rangle,\ (W_\sigma, f_\sigma) \in Q\}$, then all $M \in \langle X\rangle_{\mathrm{irr}}$ is a standard monomial, since in other case $M = Ax_j x_i B$ for some $j > i$ and $A, B \in \langle X\rangle$, and therefore,

$$M = Ax_j x_i B = A(CW_\sigma D)B = (AC)W_\sigma(DB)$$

for some $C, D \in \langle X\rangle$, and $(W_\sigma, f_\sigma) \in Q$, which is a contradiction as M is irreducible.

To prove the statement 2, first assume that $\{x^\alpha\}_{\alpha\in\mathbb{N}^n} \subseteq \langle X\rangle_{\mathrm{irr}}$. No W_σ such that $(W_\sigma, f_\sigma) \in Q$ is a standard monomial, since $W_\sigma \notin \langle X\rangle_{\mathrm{irr}}$. Hence, $W_\sigma = Ax_j x_i B$, for some $j > i$ and $A, B \in \langle X\rangle$. Conversely, if $\{W_\sigma\}_{(W_\sigma,f_\sigma)\in Q} \subseteq \{Ax_j x_i B \,/\, 1 \leq i < j \leq n,\ A, B \in \langle X\rangle\}$, then every standard monomial is irreducible. Indeed, if there exists $\alpha \in \mathbb{N}^n$ such that $x^\alpha \notin \langle X\rangle_{\mathrm{irr}}$, then $x^\alpha = AW_\sigma B$ and $W_\sigma = Cx_j x_i D$ for some $A, B, C, D \in \langle X\rangle$, $(W_\sigma, f_\sigma) \in Q$, $j > i$. This leads to the following impossible equality on $\langle X\rangle$

$$x^\alpha = CAx_j x_i BD.$$

□

1.2.3 Corollary. *Let* $X = \{x_1, \ldots, x_n\}$ *and* $Q \subseteq \langle X\rangle \times k\langle X\rangle$ *a reduction system for* $k\langle X\rangle$. *Then* $\langle X\rangle_{\mathrm{irr}} = \{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ *if, and only if, the set* $\{W_\sigma \,/\, (W_\sigma, f_\sigma) \in Q\}$ *can be written as*

$$\{x_j x_i \,/\, 1 \leq i < j \leq n\} \cup \{A_l x_{j_l} x_{i_l} B_l\}_{l\in\Lambda}$$

for some set Λ, *with* $1 \leq i_l < j_l \leq n$, $A_l, B_l \in \langle X\rangle$ *and* $(A_l, B_l) \neq (1, 1)$.

If, in addition, Q *has no inclusion ambiguities, then*

$$\langle X\rangle_{\mathrm{irr}} = \{x^\alpha \,/\, \alpha \in \mathbb{N}^n\} \iff \{W_\sigma \,/\, (W_\sigma, f_\sigma) \in Q\} = \{x_j x_i \,/\, 1 \leq i < j \leq n\}.$$

Proof. Assume that $\langle X\rangle_{\mathrm{irr}} = \{x^\alpha\}_{\alpha\in\mathbb{N}^n}$. First, by 1.2.2, for all $(W_\sigma, f_\sigma) \in Q$, we may find $j_\sigma > i_\sigma$ and $A_\sigma, B_\sigma \in \langle X\rangle$ such that

$$W_\sigma = A_\sigma x_{j_\sigma} x_{i_\sigma} B_\sigma. \tag{1.8}$$

Furthermore, for all $j > i$, there are $C, D \in \langle X\rangle$, $(W_\sigma, f_\sigma) \in Q$ satisfying

$$x_j x_i = CW_\sigma D = CA_\sigma x_{j_\sigma} x_{i_\sigma} B_\sigma D \text{ in } \langle X\rangle.$$

Hence, $C = A_\sigma = B_\sigma = D = 1$ and $(j,i) = (j_\sigma, i_\sigma)$, which implies that

$$\{x_j x_i\}_{j>i} \subseteq \{W_\sigma \,/\, (W_\sigma, f_\sigma) \in Q\}. \tag{1.9}$$

From (1.8) and (1.9) we have

$$\{W_\sigma \,/\, (W_\sigma, f_\sigma) \in Q\} = \{x_j x_i \,/\, 1 \leq i < j \leq n\} \cup \{A_\sigma x_{j_\sigma} x_{i_\sigma} B_\sigma\}_{\sigma\in\Lambda}$$

for some set Λ, with $(A_\sigma, B_\sigma) \neq (1,1)$ and $j_\sigma > i_\sigma$. The "if" part follows in a straightforward way from 1.2.2.
Now assume that there are no inclusion ambiguities in Q, and $\langle X\rangle_{\text{irr}} = \{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$. Then, for all $(W_\sigma, f_\sigma) \in Q$, we already know that

$$W_\sigma = Ax_j x_i B = ACW_{\sigma'} DB = ACW_{\sigma'} DB$$

for some $j > i$, $A, B, C, D \in \langle X\rangle$, and $(W_{\sigma'}, f_{\sigma'}) \in Q$. So, $W_\sigma = W_{\sigma'}$ and $A = B = C = D = 1$, which implies $W_\sigma = x_j x_i$. Therefore,

$$\{W_\sigma \,/\, (W_\sigma, f_\sigma) \in Q\} = \{x_j x_i \,/\, 1 \leq i < j \leq n\}.$$

□

In 1.1.25 we saw that complete reduction systems for $\mathsf{k}\langle X\rangle$ are closely related with two-sided Gröbner bases in $\mathsf{k}\langle X\rangle$. In the following result we give, assuming certain hypotheses, necessary and sufficient conditions for obtaining algebras with PBW bases in terms of reduction systems and two-sided Gröbner bases.

1.2.4 Theorem. *Let $X = \{x_1, \ldots, x_n\}$ and Q a reduction system for $\mathsf{k}\langle X\rangle$, compatible with a monomial order $\preceq$ on $\langle X\rangle$, satisfying that all W_σ are disordered, i.e.,*

$$\forall\, \sigma = (W_\sigma, f_\sigma) \in Q,\ W_\sigma = Ax_j x_i B, \text{ for some } A, B \in \langle X\rangle, j > i. \tag{1.10}$$

Consider the following statements:

1. *$k\langle X\rangle/I_Q$ is a k-algebra with a PBW basis. More precisely, $\{X^\alpha\}_{\alpha\in\mathbb{N}^n}$ is a k-basis of R, where X^α denotes $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ and $X_i = x_i + I_Q$;*
2. *$\{x_j x_i \,/\, 1 \leq i < j \leq n\} \subseteq \{W_\sigma \,/\, \sigma \in Q\}$, or equivalently, $\langle X\rangle_{\text{irr}} = \{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$;*

3. *The set* $G = \{W_\sigma - f_\sigma\}_{\sigma\in Q}$ *is a two-sided Gröbner basis for* I_Q, *or equivalently,* Q *is complete.*

Then,

A) If 2 holds, then 1 is equivalent to 3.

B) Assuming 3, the statements 1 and 2 are equivalent.

In addition, if Q *has no inclusion ambiguities, then condition 2 can be replaced by*

2'. $\{W_\sigma \,/\, \sigma \in Q\} = \{x_j x_i \,/\, 1 \leq i < j \leq n\}$.

Proof.

A) Assume that 2 holds. Note that, from 1.2.2, it follows that condition (1.10) is equivalent to $\{x^\alpha\}_{\alpha\in\mathbb{N}^n} \subseteq \langle X\rangle_{\text{irr}}$. Thus, by Corollary 1.2.3, $\{x_j x_i\}_{1\leq i<j\leq n} \subseteq \{W_\sigma\}_{\sigma\in Q}$ if, and only, if $\langle X\rangle_{\text{irr}} = \{x^\alpha\}_{\alpha\in\mathbb{N}^n}$. Therefore, $\{X^\alpha\}_{\alpha\in\mathbb{N}^n} = \{M + I_Q\}_{M\in\langle X\rangle_{\text{irr}}}$. At this point, the result directly follows by applying Theorem 1.1.25.

B) Suppose that the set $G = \{W_\sigma - f_\sigma\}_{\sigma\in Q}$ is a two-sided Gröbner basis for I_Q, which by Theorem 1.1.25, is equivalent to Q being complete, or to $\{M + I_Q \,/\, M \in \langle X\rangle_{\text{irr}}\}$ being a k-basis of $\mathsf{k}\langle X\rangle/I_Q$, or $\mathsf{k}\langle X\rangle = \mathsf{k}\langle X\rangle_{\text{irr}} \bigoplus I_Q$. The "if" part of the equivalence between 1 and 2 is clear. Now, assume that $\{X^\alpha\}_{\alpha\in\mathbb{N}^n}$ is a basis of $\mathsf{k}\langle X\rangle/I_Q$ as a k-vectorspace. Recall that condition (1.10) is equivalent to $\{x^\alpha\}_{\alpha\in\mathbb{N}^n} \subseteq \langle X\rangle_{\text{irr}}$, so let us prove that every irreducible monomial is standard. Let $M \in \langle X\rangle_{\text{irr}}$. The projection of M on $\mathsf{k}\langle X\rangle/I_Q$ can be written as $M + I_Q = \sum_\alpha \lambda_\alpha x^\alpha + I_Q$. Since every x^α is irreducible, there exists α_0 such that $\lambda_{\alpha_0} = 1$ and $\lambda_\alpha = 0$, for all $\alpha \neq \alpha_0$. Hence, $M - x^{\alpha_0} \in \mathsf{k}\langle X\rangle_{\text{irr}} \bigcap I_Q$, and therefore, $M = x^{\alpha_0}$. □

1.2.5 Note. The equivalence between 1 and 3 with several restrictions appeared in [54, 73, 45, et al.] (cf. [61]), and in the more restricted context of G-Algebras, in [13, 61].

The algebras studied in the subsequent chapters (G-Algebras and Yang-Baxter Algebras) fit the hypothesis and satisfy the conditions 1, 2 and 3 of Theorem 1.2.4. In particular, this result can be viewed as a generalization of the results [61, Th. 2.3] and [13, Ch. 3, Th. 4.7] stated in the context of G-Algebras (see Remark 2.1.3).

1.2.6 Example. Let $R = \mathsf{k}\{x_1, \ldots, x_n;\ Q,\ \preceq\}$ be a *G-Algebra* (also called *PBW algebra* in [10, 44, 11, 12, 13, 65, et al.], or *Solvable polynomial algebra* in [59, 54, et al.]), where $\preceq$ is an admissible order on $\mathbb{N}^n$,

$$Q = \{x_j x_i - q_{ji} x_i x_j - p_{ji} \,/\, 1 \leq i < j \leq n\},$$

with $q_{ji} \in \mathsf{k}\backslash\{0\}$, and the p_{ji}'s are standard polynomials such that $\exp(p_{ji}) \prec \epsilon_i + \epsilon_j$ (Chapter 2 is devoted to the study of this class of algebras). The reduction system for $\mathsf{k}\langle X\rangle$

$$Q' = \{(x_j x_i,\ q_{ji} x_i x_j + p_{ji}) \,/\, 1 \leq i < j \leq n\}$$

is compatible with the monomial order on $\langle x_1, \ldots, x_n\rangle$, induced from $\preceq$ on $\mathbb{N}^n$ (see Appendix A). Indeed,

$$\mathrm{lm}\,(q_{ji} x_i x_j + p_{ji}) = x_i x_j \prec x_j x_i,\ \forall\, 1 \leq i < j \leq n.$$

By 1.2.4, Q is a two-sided Gröbner basis for $I_{Q'}$, since $\{x^\alpha + I_{Q'}\}_{\alpha\in\mathbb{N}^n}$ is a k-basis of $R \cong \mathsf{k}\langle X\rangle/I_{Q'}$.

1.2.7 Example. Let $X = \{x_1, \ldots, x_n\}$, and let (X, r) be a *square-free solution of the Yang-Baxter equation.* Consider the *Yang-Baxter Algebra* $\mathcal{A}(\mathsf{k}, X, r)$ associated to (X, r), i.e., $\mathcal{A}(\mathsf{k}, X, r) = \mathsf{k}\langle X\rangle/I_Q$, where Q is the reduction system

$$\{(x_j x_i,\ x_{i'} x_{j'}) \,/\, x_j x_i = x_{i'} x_{j'} \in \Re(X, r),\ 1 \leq i < j \leq n\}$$

for $\mathsf{k}\langle X\rangle$ (the definitions of these notions can be found in Chapter 3). It is known ([40]) that there exists an order $\preceq$ on $X = \{x_1 \prec \cdots \prec x_n\}$ satisfying the inequalities $i' < j'$, $j > i'$ and $i < j'$, for all relations $x_j x_i = x_{i'} x_{j'} \in \Re(X, r)$ with $j > i$. Thus, Q is compatible with the monomial order $\preceq_{deglex}$ on $\langle X\rangle$, and by Theorem 1.2.4, $\{x^\alpha + I_Q\}_{\alpha\in\mathbb{N}^n}$ is a k-basis of $\mathcal{A}(\mathsf{k}, X, r)$ (already known from [40]), since Q is a complete reduction system (see a proof in 3.3. 13).

Whilst the monomial orders on $\langle x_1, \ldots, x_n\rangle$ are used to define the leading term, the leading monomial and the leading coefficient of every polynomial of the free algebra $\mathsf{k}\langle x_1, \ldots, x_n\rangle$, it is usual for the k-algebras with a PBW basis $\{x^\alpha / \alpha \in \mathbb{N}^n\}$ to take admissible orders on $\mathbb{N}^n$ (see e.g. [10, 11, 12, 13, 65] for the case of G-Algebras).

1.2.8 Let $\preceq$ an admissible order on $\mathbb{N}^n$. If R is a k-algebra with a PBW basis $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$, then every element $f \in R \setminus \{0\}$ has a unique *standard representation*

$$f = \sum_{\alpha\in\mathbb{N}^n} \lambda_\alpha x^\alpha,$$

with $\lambda_\alpha \in \mathsf{k}$, and $\lambda_\alpha = 0$, except for a finite number of terms. The *Newton diagram* of f is

$$\mathcal{N}(f) = \{\alpha \in \mathbb{N}^n \,/\, \lambda_\alpha \neq 0\}$$

(sometimes we will use $\mathcal{N}_R(f)$, for emphasizing the underlying algebra R). Note that $\mathcal{N}(f+g) \subseteq \mathcal{N}(f) \cup \mathcal{N}(g)$, for all $f, g \in R$, and $\mathcal{N}(f) \neq \emptyset$ if, and only if, $f \neq 0$. The *exponent* of $f \neq 0$, denoted by $\exp_R(f)$ (or simply by $\exp(f)$ when the underlying algebra R is clear from the context), is defined as

$$\exp_R(f) = \max_{\preceq} \mathcal{N}(f).$$

The *leading monomial* of $f \neq 0$, denoted by $\mathrm{lm}_R(f)$, is $x^{\exp_R(f)}$, whilst $\mathrm{lc}_R(f) = \lambda_{\exp_R(f)}$ is called the *leading coefficient* of f. The *leading term* $\mathrm{lt}_R(f)$ of f is the product of both $\mathrm{lc}_R(f)$ and $\mathrm{lm}_R(f)$, i.e.,

$$\mathrm{lt}_R(f) = \lambda_{\exp_R(f)} x^{\exp_R(f)}.$$

For the sake of briefness, we will agree that $\exp_R(0) = -\infty$, and the monoid structure and the admissible order $\preceq$ on $\mathbb{N}^n$ will be extended to $\mathbb{N}^n \cup \{-\infty\}$ by

$$\begin{aligned} &\text{i)} \ -\infty \prec \alpha, \\ &\text{ii)} \ -\infty + \alpha = \alpha + (-\infty) = -\infty + (-\infty) = -\infty, \end{aligned} \tag{1.11}$$

for all $\alpha \in \mathbb{N}^n$. With these notations, it is easy to check that

1. $\exp_R(f+g) \preceq \max\{\exp_R(f), \exp_R(g)\}$;

2. $\exp_R(f+g) \prec \max\{\exp_R(f), \exp_R(g)\} \iff \mathrm{lt}_R(f) = -\mathrm{lt}_R(g)$.

1.2.9 Remark. If R is a k-algebra with a PBW basis $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ and $\preceq$ is an admissible order on $\mathbb{N}^n$, then the values $\mathrm{lm}_R(f)$, $\mathrm{lc}_R(f)$, resp. $\mathrm{lt}_R(f)$ of an element $f \in R \setminus \{0\}$ are $\mathrm{lm}(f)$, $\mathrm{lc}(f)$, resp. $\mathrm{lt}(f)$ (defined in 1.1.14), when f is regarded as a polynomial in $\mathsf{k}\langle x_1, \ldots, x_n\rangle$ and the monomial order on $\langle x_1, \ldots, x_n\rangle$ associated to the admissible order $\preceq$ on $\mathbb{N}^n$ is considered (see the definition in Appendix A).

In formulas (1.3) we pointed out that there is compatibility of these values when they are applied to the product of polynomials in $\mathsf{k}\langle x_1, \ldots, x_n\rangle$. In general, such compatibility does not hold for $\mathrm{lm}_R(f)$, $\mathrm{lc}_R(f)$, $\mathrm{lt}_R(f)$ in k-algebras with PBW bases. However, an inequality involving the exponent of the product of elements of R is satisfied (see 3 in 1.2.10 below). In Chapter 2 we will recall that the later condition becomes an equality when R is a G-Algebra, and even more, this equality is a necessary and sufficient condition for a pair $(R, \preceq)$ (consisting of a k-algebra R with a PBW basis and an admissible order $\preceq$) to be a G-Algebra (see Theorem 2.1.4).

From here until the end of this chapter we will deal with finitely presented k-algebras

$$R = \mathsf{k}\langle X\rangle / I_Q, \tag{1.12}$$

with $X = \{x_1, \ldots, x_n\}$ and where

$$Q = \{(x_j x_i, f_{ji}) \,/\, 1 \leq i < j \leq n\}$$

is a complete reduction system with respect to the monomial order $\preceq$ on $\langle X\rangle$ induced by an admissible order $\preceq$ on $\mathbb{N}^n$ (see Appendix A). Note, by 1.2.4, that the set $\{x^\alpha + I_Q \,/\, \alpha \in \mathbb{N}^n\}$ is a PBW basis of R. These algebras are particular cases of the so-called *standard finitely presented algebras* (see e.g. [34, 36]).

1.2.10 Lemma. *Let $\preceq$ an admissible order on $\mathbb{N}^n$, and let $R = k\langle X\rangle/I_Q$, where $Q = \{(x_j x_i, f_{ji}) \,/\, 1 \leq i < j \leq n\}$ is a complete reduction system with respect to the monomial order $\preceq$ on $\langle X\rangle$ induced by $\preceq$ on $\mathbb{N}^n$.*
For all elements $F, G \in R \setminus \{0\}$, namely, $F = f + I_Q$, $G = g + I_Q$ with f, g polynomials of $k\langle X\rangle$,

1. $\exp_R(F) \preceq \mathrm{mdeg}(\mathrm{lm}\,(f))$;
2. $\exp_R(F) = \alpha$, *whenever* $\mathrm{lm}\,(f) = x^\alpha$;
3. $\exp_R(FG) \preceq \exp_R(F) + \exp_R(G)$.

Proof. Let us prove 1. By Theorem 1.1.16, $f = h + \overline{f}^{Q}$, with $h \in I_Q$ and $\overline{f}^{Q} \in \mathsf{k}\langle X\rangle_{\mathrm{irr}}$ such that $\mathrm{lm}\,(\overline{f}^{Q}) \preceq \mathrm{lm}\,(f)$ whenever $\overline{f}^{Q} \neq 0$. If $\overline{f}^{Q} \in I_Q$, the proof trivially finishes. Otherwise, since $\overline{f}^{Q}$ is a standard polynomial it follows that

$$\exp_R(F) = \exp_R(\overline{f}^{Q} + I_Q) = \mathrm{mdeg}(\mathrm{lm}\,(\overline{f}^{Q})) \preceq \mathrm{mdeg}(\mathrm{lm}\,(f)).$$

To prove 2, take $f = \lambda x^\alpha + \sum_{M \prec x^\alpha} \lambda_M M \in \mathsf{k}\langle X\rangle$. By statement 1 and $\nu(x^\alpha) = 0$, for every monomial M of this sum we have

$$\exp_R(\overline{M}^{Q} + I_Q) = \exp_R(M + I_Q) \preceq \mathrm{mdeg}(M) \prec \alpha,$$

where $\overline{M}^{Q}$ is the normal form of M. Hence,

$$F = \lambda(x^\alpha + I_Q) + \sum_{\exp_R(\overline{M}^{Q} + I_Q) \prec \alpha} \lambda_M \overline{M}^{Q} + I_Q,$$

and therefore, $\exp_R(F) = \alpha$.

Finally, let us check the statement 3. Let $\overline{f}^Q, \overline{g}^Q$ the normal forms of $f, g \in \mathsf{k}\langle X\rangle$, respectively. Then

$$\begin{aligned}
\exp_R(FG) &= \exp_R((\overline{f}^Q + I_Q)(\overline{g}^Q + I_Q)) \\
&= \exp_R(\overline{f}^Q\overline{g}^Q + I_Q) \\
&= \exp_R(\overline{(\overline{f}^Q\overline{g}^Q)}^Q + I_Q) \\
&= \mathrm{mdeg}(\mathrm{lm}(\overline{(\overline{f}^Q\overline{g}^Q)}^Q)) \qquad [\text{by statement 2}] \\
&\preceq \mathrm{mdeg}(\mathrm{lm}(\overline{f}^Q\overline{g}^Q)) \qquad [\mathrm{lm}(\overline{(\overline{f}^Q\overline{g}^Q)}^Q) \preceq \mathrm{lm}(\overline{f}^Q\overline{g}^Q)] \\
&= \mathrm{mdeg}(\mathrm{lm}(\overline{f}^Q)\mathrm{lm}(\overline{g}^Q)) \qquad [\text{by expressions (1.3)}] \\
&= \mathrm{mdeg}(\mathrm{lm}(\overline{f}^Q)) + \mathrm{mdeg}(\mathrm{lm}(\overline{g}^Q)) \\
&= \exp_R(\overline{f}^Q + I_Q) + \exp_R(\overline{g}^Q + I_Q) \ [\text{by statement 2}] \\
&= \exp_R(F) + \exp_R(G).
\end{aligned}$$

□

From the following result we devise an algorithm (Algorithm 2) to perform two-sided divisions in algebras $R = \mathsf{k}\langle X\rangle/I_Q$ as in (1.12). More precisely, we can divide a non-zero element $F \in R$ by a set of divisors $\{G_1, \ldots, G_s\} \subset R$, obtaining a remainder in R, and some quotients in the *enveloping algebra* $R \otimes_{\mathsf{k}} R^{\mathrm{op}}$. Recall that R is a left $R \otimes_{\mathsf{k}} R^{\mathrm{op}}$-module with the action $(P_1 \otimes P_2)H = P_1 H P_2$, for $P_1, P_2, H \in R$.

1.2.11 Theorem. *Let $\preceq$ an admissible order on $\mathbb{N}^n$, and let $R = k\langle X\rangle/I_Q$, where $Q = \{(x_j x_i, f_{ji}) \,/\, 1 \leq i < j \leq n\}$ is a complete reduction system with respect to the monomial order $\preceq$ on $\langle X\rangle$ induced by $\preceq$ on $\mathbb{N}^n$.*
Let $\{G_1, \ldots, G_s\} \subseteq R \setminus \{0\}$. Every element $F \in R \setminus \{0\}$ can be written as

1. *$F = \sum_{i=1}^{s} P_i G_i + F'$ with $F' \in R$, $P_i \in R \otimes_k R^{\mathrm{op}}$ satisfying*
2. *$\exp_R(P_i G_i) \preceq \exp_R(F)$, for all $1 \leq i \leq s$;*
3. *if $F' \neq 0$, then $\exp_R(F') \preceq \exp_R(F)$ and there exists a standard polynomial $f' \in k\langle X\rangle$ such that $F' = f' + I_Q$ and*

$$x^\alpha \notin L(\{g_1, \ldots, g_s\}),\ \forall\, x^\alpha \text{ monomial of } f',$$

where $G_i = g_i + I_Q$, for some $g_i \in k\langle X\rangle$.

Proof. Let $F = f + I_Q \in R \setminus \{0\}$ and $G_i = g_i + I_Q$, with $f, g_i \in \mathsf{k}\langle X\rangle$, $\forall i$. We can assume w.l.o.g. that f is a standard polynomial (if not, we

Algorithm 2 Two-sided division

Require: Let $F = f + I_Q$, $G_1 = g_1 + I_Q$, $\ldots$, $G_s = g_s + I_Q \in R \setminus \{0\}$, where $R = \mathsf{k}\langle X\rangle/I_Q$ is a standard finitely presented algebra as in (1.12) and $f, g_i \in \mathsf{k}\langle X\rangle$;

Ensure: $P_1, \ldots, P_s \in R \otimes_{\mathsf{k}} R^{\mathrm{op}}$ and $F' \in R$ such that $F = \sum_{i=1}^{s} P_i G_i + F'$ satisfying conditions 2 and 3 of 1.2.11;

Initialization: $Q' := \{(\mathrm{lm}\,(g_i), \mathrm{lm}\,(g_i) - \mathrm{lc}\,(g_i)^{-1} g_i)\}_{i=1}^{s}$;

if f is not a standard polynomial **then**

Using Algorithm 1, compute the normal form ${}^{Q}\overline{f}$ of f;

$f := {}^{Q}\overline{f}$;

end if

Reduce f under the reduction system $Q \cup Q'$ (using Algorithm 1) in order to get ${}^{Q\cup Q'}\overline{f} \in \mathsf{k}\langle X\rangle$, and $p_i, q_{kj} \in \mathsf{k}\langle X\rangle \otimes_{\mathsf{k}} (\langle X\rangle)^{\mathrm{op}}$, for $1 \leq i \leq s$, $1 \leq j < k \leq n$, satisfying

$$f = \sum_{i=1}^{s} p_i g_i + \sum_{1\leq j<k\leq n} q_{kj}(x_k x_j - f_{kj}) + {}^{Q\cup Q'}\overline{f},$$

and conditions 2 and 3 of 1.1.16;

Put $F' := {}^{Q\cup Q'}\overline{f} + I_Q$, and $P_i := p_i + I_Q$, for all $1 \leq i \leq s$;

Return F', P_i, for all $1 \leq i \leq s$.

take ${}^{Q}\overline{f} \in \mathsf{k}\langle X\rangle_{\mathrm{irr}}$). Consider the reduction system $Q \cup Q'$ for $\mathsf{k}\langle X\rangle$, where $Q' = \{(\mathrm{lm}\,(g_i), \mathrm{lm}\,(g_i) - \mathrm{lc}\,(g_i)^{-1} g_i)\}_{i=1}^{s}$. Note that $Q \cup Q'$ is compatible with the monomial order on $\langle X\rangle$. From Theorem 1.1.16, there are some $p_i, q_{kj} \in \mathsf{k}\langle X\rangle \otimes_{\mathsf{k}} (\mathsf{k}\langle X\rangle)^{\mathrm{op}}$ and ${}^{Q\cup Q'}\overline{f} \in \mathsf{k}\langle X\rangle$ such that

$$f = \sum_{i=1}^{s} p_i g_i + \sum_{1\leq j<k\leq n} q_{kj}(x_k x_j - f_{kj}) + {}^{Q\cup Q'}\overline{f},$$

where $\mathrm{lm}\,(p_i g_i) \preceq \mathrm{lm}\,(f)$, and if ${}^{Q\cup Q'}\overline{f} \neq 0$, then $\mathrm{lm}\,({}^{Q\cup Q'}\overline{f}) \preceq f$ and ${}^{Q\cup Q'}\overline{f}$ is irreducible under $Q \cup Q'$. Projecting the polynomial f on R we get

$$F = f + I_Q = \sum_{i=1}^{s} (p_i + I_Q) G_i + ({}^{Q\cup Q'}\overline{f} + I_Q).$$

Taking $P_i = p_i + I_Q$, since f and $\overline{f}^{Q \cup Q'}$ are standard polynomials, from 1.2. 10 it follows that

$$\begin{aligned}\exp_R(P_iG_i) &= \exp_R((p_i + I_Q)(g_i + I_Q)) \\ &\preceq \mathrm{mdeg}(\mathrm{lm}\,(p_ig_i)) \\ &\preceq \mathrm{mdeg}(\mathrm{lm}\,(f)) \\ &= \exp_R(F),\end{aligned}$$

and $\exp_R(\overline{f}^{Q \cup Q'} + I_Q) = \mathrm{mdeg}(\mathrm{lm}\,(\overline{f}^{Q \cup Q'})) \preceq \mathrm{mdeg}(\mathrm{lm}\,(f)) = \exp_R(F)$. Moreover, since $\overline{f}^{Q \cup Q'}$ is irreducible under Q', we have $x^\alpha \notin L(\{g_1, \ldots, g_s\})$, for all x^α monomial of $\overline{f}^{Q \cup Q'}$. □

1.2.12 Note. If the underlying field k is computable and the monomial order on $\langle X \rangle$ is decidable, then Algorithm 2 is effective (see Remark 1.1.18).

1.2.13 Definition. Let R be a k-algebra with basis $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ and $\preceq$ an admissible order on $\mathbb{N}^n$. For every subset $\mathcal{B}$, the *set of exponents* of $\mathcal{B}$, denoted by $\mathrm{Exp}_R(\mathcal{B})$, is defined as

$$\mathrm{Exp}_R(\mathcal{B}) = \{\exp_R(F) \,/\, F \in \mathcal{B} \setminus \{0\}\},$$

and

$$L_R(\mathcal{B}) = \{x^{\beta+\gamma} \,/\, \beta \in \mathrm{Exp}_R(\mathcal{B}), \gamma \in \mathbb{N}^n\}.$$

1.2.14 Lemma. *Let R be a k-algebra with basis $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ and $\preceq$ an admissible order on $\mathbb{N}^n$. Let I a two-sided ideal of R, and $\mathcal{B}$ a two-sided generator system of I. The following conditions are equivalent:*

1. $L_R(\mathcal{B}) = L_R(I)$;
2. *For all $f \in I \setminus \{0\}$, there exists $g \in \mathcal{B}$ such that $\mathrm{lm}_R(g) | \mathrm{lm}_R(f)$, i.e., if $\mathrm{lm}_R(g) = x^\alpha$ and $\mathrm{lm}_R(f) = x^\beta$, then $\alpha_i \leq \beta_i$, for all $1 \leq i \leq n$;*
3. $\mathrm{Exp}_R(I) = \bigcup_{f \in \mathcal{B}} \exp_R(f) + \mathbb{N}^n$.

Proof. (1) $\Leftrightarrow$ (2). If $L_R(\mathcal{B}) = L_R(I)$, then for all $f \in I \setminus \{0\}$, $\mathrm{lm}_R(f) = x^\alpha \in L_R(\mathcal{B})$. Thus, $x^\alpha = x^{\beta+\gamma}$, with $\beta = \exp_R(g)$, for some $g \in \mathcal{B} \setminus \{0\}$ and $\gamma \in \mathbb{N}^n$. Hence, $\alpha = \beta + \gamma$, and therefore, $\alpha_i \leq \beta_i$, for all i. Conversely, assuming 2, for all $x^\alpha \in L_R(I)$ there exist $\gamma \in \mathbb{N}^n$, $\beta = \exp_R(f)$ with $f \in I$ such $\alpha = \beta + \gamma$. But there also exist $g \in \mathcal{B}$ such that $\mathrm{lm}_R(g) | \mathrm{lm}_R(f)$. Writing $\exp_R(g) = \beta_0$ we have that $\beta = \beta_0 + \delta$ for some $\delta \in \mathbb{N}^n$. Hence, $x^\alpha = x^{\beta_0+\delta+\gamma} \in L_R(\mathcal{B})$.

The equivalence between the two last statements is straightforward. □

Next we propose a definition of two-sided Gröbner basis for ideals of k-algebras with PBW bases. In particular, when R is a G-Algebra this definition is equivalent to the one appearing in [60, 62] and in [10, 11, 12, 13, 65].

1.2.15 Definition. Let R be a k-algebra with basis $\{x^\alpha / \alpha \in \mathbb{N}^n\}$ and $\preceq$ an admissible order on $\mathbb{N}^n$. Let I a two-sided ideal of R. A two-sided generator system $\mathcal{B}$ of I is said to be a *two-sided Gröbner basis for* I if one of the conditions of 1.2.14 holds.
A nonempty set $\mathcal{B} \subseteq R$ is said to be a *two-sided Gröbner basis* if $\mathcal{B}$ is a two-sided Gröbner basis for ${}_R\langle \mathcal{B} \rangle_R$.

1.2.16 Note. There are k-algebras with PBW bases in which every two-sided ideal has a finite two-sided Gröbner basis (e.g. the G-Algebras, studied in Chapter 2), but obviously the existence of a finite two-sided Gröbner is not always guaranteed in the context of algebras with PBW bases.

1.2.17 Proposition. *Let $\preceq$ an admissible order on $\mathbb{N}^n$, and let $R = k\langle X \rangle / I_Q$, where $Q = \{(x_j x_i, f_{ji}) \,/\, 1 \leq i < j \leq n\}$ is a complete reduction system with respect to the monomial order $\preceq$ on $\langle X \rangle$ induced by $\preceq$ on $\mathbb{N}^n$. Let $\mathcal{B} = \{G_1, \ldots, G_s\} \subseteq R$, where $G_i = g_i + I_Q$. The polynomials g_i can be supposed to be standard, i.e., $g_i \in k\langle X \rangle_{\text{irr}}$ (otherwise, we take ${}^Q\overline{g_i}$).*
If $B = \{g_1, \ldots, g_s\} \cup \{x_j x_i - f_{ji} \,/\, 1 \leq i < j \leq n\}$ is a two-sided Gröbner basis in $k\langle X \rangle$, then $\mathcal{B}$ is a two-sided Gröbner basis in R.

Proof. Let $F \in {}_R\langle \mathcal{B} \rangle_R$. It can be written as

$$F = f + I = \sum_i P_i G_i = \sum_i p_i g_i + I_Q,$$

with $f \in \mathsf{k}\langle X \rangle_{\text{irr}}$, $P_i \in R \otimes_{\mathsf{k}} R^{\text{op}}$, $p_i \in \mathsf{k}\langle X \rangle \otimes_{\mathsf{k}} (\mathsf{k}\langle X \rangle)^{\text{op}}$. Thus, $f \in {}_{\mathsf{k}\langle X \rangle}\langle B \rangle_{\mathsf{k}\langle X \rangle}$, and $\operatorname{lm}(f) \in \mathrm{L}(B)$. Therefore, there exist $A, B \in \langle X \rangle$ such that either $\operatorname{lm}(f) = A \operatorname{lm}(g_l) B$ for some $l \in \{1, \ldots, s\}$, or $\operatorname{lm}(f) = A \operatorname{lm}(x_j x_i - f_{ji}) B$ for some $j > i$. But the latter is not possible since $\operatorname{lm}(x_j x_i - f_{ji}) = x_j x_i$ and $\operatorname{lm}(f)$ is standard. Hence,

$$\begin{aligned} \exp_R(F) &= \exp_R(f + I) \\ &= \operatorname{mdeg}(\operatorname{lm}(f)) \\ &= \operatorname{mdeg}(A) + \operatorname{mdeg}(\operatorname{lm}(g_l)) + \operatorname{mdeg}(B) \\ &= \exp_R(G_l) + \operatorname{mdeg}(AB). \end{aligned}$$

□

Chapter 2

Effective computations in G-Algebras

First developed in the ring of polynomials, methods based on Gröbner bases also work in some non-commutative rings. Mora ([73]) was the first to introduce a unified theory of Gröbner bases, for commutative and non-commutative algebras. Amongst not necessarily commutative algebras, the so-called G-Algebras have a nice computational treatment not only because they have PBW bases, but also because the multiplication is compatible with the exponents. Essentially, these are the reasons why the theory of Gröbner bases on the commutative polynomial ring (found in [1, 18, 46, et al.]) can be extended to the context of G-Algebras, by mimicking the notions and the results.

After the first results of Galligo in the Weyl algebra (see [23]) and those of Apel and Lassner in tensor algebras of finite-dimensional Lie algebras ([3]), Kandri-Rody and Weispfenning ([54]) were the first who studied Gröbner bases in G-Algebras (which they called *Solvable polynomial algebras*). This class of algebras includes many quantum groups (Weyl algebras, Quantum spaces, etc). Kredel in [59] also contributed in the main points of this theory, which has recently been surveyed by Bueso, Castro, Gómez Torrecillas, Lobillo and Verschoren ([9, 10, 11, 12, 13, 44, 65]) (who use the name *PBW algebra* instead of G-Algebra), Li ([64]) and Levandovskyy ([60, 61, 62]). In [9, 10, 11, 13, 65, et al.] the theory of Gröbner bases is extended to some classes of algebras more general than G-Algebras: the so-called *left* (and *right*) *PBW rings*, and *PBW rings*. The latter, which contain the class of G-Algebras, are particular cases of left (and right) PBW rings.

Besides Gröbner bases, many related homological and algebraic objects have been studied in the context of G-Algebras from a computational point of

view. For example, the author of [61] studies the *left syzygy module* in the context of G-Algebras and use these modules to compute free resolutions of left modules. This is done in [13] in the more general context of left PBW rings, where the authors also develop the study of graded and filtered left modules, homogeneous Gröbner bases, homogenization, computation of functors Hom and Ext, etc. Likewise, algorithms to compute the Gelfand-Kirillov dimension, to check whether a two-sided ideal is prime or not and to compute the projective dimension of a module can be found in [8, 10, 22, 65]. In these generalizations, authors were mainly interested in one-sided ideals and modules, whereas methods for the two-sided counterparts are adaptations in order to deal with the two-sided input data. However, we will show along this chapter that those "mends" are not necessary.

In the first four sections of the current chapter, we recall the basic background of the theory of Gröbner bases in the context of G-Algebras. We closely follow the notation, terminology and results of [13]. In the fourth section, where we recall some of the classical applications of Gröbner bases, we contribute with an algorithm to compute the codimension of a left submodule (right submodule or subbimodule) $M \subseteq R^s$ when R is a G-Algebra in case M is cofinite (see Algorithms 8 and 9). In the fifth section we propose a new method, that we made known first in [28], to effectively handle bimodules by using directly their two-sided generator systems as input data. We apply it, for example, for computing two-sided Gröbner bases for bimodules over a G-Algebra (see Algorithm 10) by an alternative way to the already known *Right Closure Method* (Algorithm 2.3.21). This new algorithm call once the left Buchberger algorithm, instead of the a priori unknown number of calls typical of the Right Closure Method. A comparison between both algorithms is discussed on some explicit examples. In the sixth section the aforementioned technique to handle bimodules is also applied in order to compute *syzygy bimodules*, first introduced by Mora ([71]) for homogeneous two-sided ideals in the context of non-commutative graded structures, and then, independently, by the authors ([27, 30]) for not necessarily homogeneous R-bimodules over a G-Algebra R. We show that syzygy bimodules, which can be viewed as the two-sided counterpart of the left syzygy module, reveal to be useful at solving some computational problems when, as natural, two-sided input data are given, e.g., computation of finite intersections of subbimodules of R^s, presentations and free resolutions of subbimodules of R^s, two-sided division ideals of R, etc. In case the bimodules are generated by elements of the *centralizer*, some of these results are enhanced and many computations can be simplified. In the last section we present an algorithm to compute a presentation of the *Tor* functor in the context of G-Algebras.

In this chapter we work on the free module R^s over a G-Algebra R, but obviously, all the results are also valid for $s = 1$, i.e., when the underlying structure is R and ideals are considered. In fact, in the literature ([1, 13, 18]) the theory of Gröbner bases and Syzygy modules was first developed in R, and then it was extended to R^s by mimicking the notions and the results. Our first results, for the case $s = 1$, may be found in [24].

Most of explicit examples shown in this chapter have been obtained from a library of procedures built by the authors. This library, coded using the package of symbolic computation Maple, is included in the CD at the back page of this work (see also [32]).

2.1 Preliminaries

Throughout this section, $\preceq$ will be an admissible order on $\mathbb{N}^n$, that is (as we recalled in 1.1.13), a total order on $\mathbb{N}^n$ satisfying

i) $0 \prec \alpha$, for all $\alpha \in \mathbb{N}^n \setminus \{0\}$;

ii) $\alpha \prec \beta \Longrightarrow \alpha + \gamma \prec \beta + \gamma$, for all $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Examples of admissible orders may be found in the Appendix A.

2.1.1 Definition. A set of *quantum relations* is a set

$$Q = \{x_j x_i - q_{ji} x_i x_j - p_{ji};\ 1 \leq i < j \leq n\} \subseteq \mathsf{k}\langle x_1, \ldots, x_n\rangle, \tag{2.1}$$

where $q_{ji} \in \mathsf{k} \setminus \{0\}$ and each p_{ji} is a standard polynomial of $\mathsf{k}\langle x_1, \ldots, x_n\rangle$.

A set Q of quantum relations is said to be *bounded* by an admissible order $\preceq$ on $\mathbb{N}^n$ if

$$\exp(p_{ji}) \prec \epsilon_i + \epsilon_j, \quad \forall\, 1 \leq i < j \leq n.$$

The following notion can be found in the literature under the names of *Solvable polynomial algebra* in [54], of *PBW algebras* in [10, 11, 12, 13, 65, et al.], or of *G-Algebras* in [60, 61, 62, et al.].

2.1.2 Definition. Let $R = \mathsf{k}\langle x_1, \ldots, x_n\rangle / I_Q$, where I_Q denotes the two-sided ideal of $\mathsf{k}\langle x_1, \ldots, x_n\rangle$ generated by a set Q of quantum relations. R is called a *G-Algebra* if

1. the set of standard monomials $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ is a k-basis of R (where x^α also denotes its epimorphic image $x^\alpha + I_Q$), and

2. there exists an admissible order "$\preceq$" for which Q is bounded.

The G-Algebra R defined above is usually denoted by $\mathsf{k}\{x_1,\ldots,x_n;\ Q,\preceq\}$. This notation appears, e.g., in the book of Kredel ([59]), or in the works of Bueso, Castro, Gómez Torrecillas, Lobillo and Verschoren ([9, 10, 11, 12, 13, 44, 65]), where G-Algebras are studied in the more general context of *left* (and *right*) *PBW rings* and *PBW rings*.

2.1.3 Remark. As proved in [61, Th. 2.3], given a set of bounded quantum relations $Q = \{x_jx_i - q_{ji}x_ix_j - p_{ji};\ 1 \leq i < j \leq n\}$, condition 1 of 2.1.2 is equivalent to

1'. *Non-degeneracy conditions:* for all $1 \leq i < j < k \leq n$, the elements

$$\mathcal{NDC}_{ijk} = q_{ki}q_{kj}p_{ji}x_k - x_kp_{ji} + q_{kj}x_jp_{ki} - q_{ji}p_{ki}x_j + p_{kj}x_i - q_{ji}q_{ki}x_ip_{kj}$$

reduces to 0 under the reduction system $Q' = \{(x_jx_i, q_{ji}x_ix_j + p_{ji}\}_{j>i}$ for $\mathsf{k}\langle x_1,\ldots,x_n\rangle$,

or to

1". Q is a two-sided Gröbner basis for I_Q.

An alternative way of proving these equivalences is by using the theory of reduction system surveyed in Chapter 1. The equivalence between 1 and 1" is given by Theorem 1.2.4, since $\{W_\sigma\}_{\sigma\in Q'} = \{x_jx_i\}_{1\leq i<j\leq n}$.
$(1') \Leftrightarrow (1'')$. Note that for Q' there are no inclusion ambiguities, and the overlap ones are exactly $(\sigma_{kj}, \sigma_{ji}, x_k, x_j, x_i)$ for $1 \leq i < j \leq n$, where $\sigma_{kj} = (x_kx_j, q_{kj}x_jx_k + p_{kj})$ and $\sigma_{ji} = (x_jx_i, q_{ji}x_ix_j + p_{ji})$. Therefore, the S-polynomials are

$$S(\sigma_{kj},\sigma_{ji},x_k,x_j,x_i) = (q_{kj}x_jx_k + p_{kj})x_i - x_k(q_{ji}x_ix_j + p_{ji}),\quad 1 \leq i < j \leq n,$$

which can be reduced to $\mathcal{NDC}_{ijk}$ as follows:

$$\begin{aligned}
S(\sigma_{kj},\sigma_{ji},x_k,x_j,x_i) &= q_{kj}x_jx_kx_i + p_{kj}x_i - q_{ji}x_kx_ix_j - x_kp_{ji}\\
&\to_{Q'} q_{ki}q_{kj}x_jx_ix_k + q_{kj}x_jp_{ki} + p_{kj}x_i -\\
&\quad q_{ji}q_{ki}x_ix_kx_j - q_{ji}p_{ki}x_j - x_kp_{ji}\\
&\to_{Q'} q_{ji}q_{ki}q_{kj}x_ix_ix_k + q_{ki}q_{kj}p_{ji}x_k + q_{kj}x_jp_{ki} + p_{kj}x_i -\\
&\quad q_{ji}q_{ki}q_{kj}x_ix_jx_k - q_{ji}q_{ki}x_ip_{kj} - q_{ji}p_{ki}x_j - x_kp_{ji}\\
&= \mathcal{NDC}_{ijk}.
\end{aligned}$$

Hence, non-degeneracy conditions imply $S(\sigma_{kj},\sigma_{ji},x_k,x_j,x_i) \to_{Q'} 0$, for all $i < j < k$. Conversely, if all S-polynomials reduce to 0 under Q', then by

1.1.25, Q' is complete. From the confluence condition (see 1.1.4), it follows that $\mathcal{NDC}_{ijk} \rightarrow_{Q'} 0$, for all $i < j < k$.
Thus, non-degeneracy conditions, which may be checked by computer, correspond to the overlap ambiguities of Bergman to be resolvable or the (noetherian) rewriting system Q' to be complete. Moreover, they can be viewed as generalized *Jacobi identities* (see 2.2). Indeed, they are the same in the universal enveloping algebra of a finite-dimensional Lie algebra, when $q_{ji} = 1$ and p_{ji} are linear polynomials, for all $1 \leq i < j \leq n$ (cf. [60, 61])).
It is easy to check that the equivalent conditions given in [13, Ch. 3, Th. 4.7] are also obtained from the theory of reduction systems studied in the first chapter.

What makes G-Algebras to be *close to commutative* (in their computational behaviour) is essentially that there is compatibility of the exponent of products (see condition 3 below). The proof that this property becomes a characterization of G-Algebras may be found in [13, 65, et al.].

2.1.4 Theorem. [13, 65] *Let $\preceq$ be an admissible order on $\mathbb{N}^n$ and let R be a k-algebra such that $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ is a PBW basis. The following statements are equivalent:*

1. *the order $\preceq$ is compatible with the variables $x_1, \ldots, x_n$, in the sense that for all $1 \leq i < j \leq n$, there exists $q_{ji} \in k \setminus \{0\}$ such that*

$$\exp\left(x_j x_i - q_{ji} x_i x_j\right) \prec \epsilon_i + \epsilon_j;$$

2. *for all $\alpha, \beta \in \mathbb{N}^n$, there exists $q_{\alpha\beta} \in k \setminus \{0\}$ such that*

$$x^\alpha x^\beta = q_{\alpha\beta} x^{\alpha+\beta} + p_{\alpha\beta},$$

   for some $p_{\alpha\beta} \in R$ satisfying $\exp(p_{\alpha\beta}) \prec \alpha + \beta$;

3. *$\exp(fg) = \exp(f) + \exp(g)$, for all $f, g \in R$.*

It is shown in [13] that the existence of an admissible order by which a given set of quantum relations is bounded can be effectively decided by *linear programming methods*, and that, in case the existence test is positive, such an order can be computed (by using the *Simplex algorithm*).
Some of the following properties are direct consequences of Theorem 2.1.4.

2.1.5 Corollary. *Let $R = k\{x_1, \ldots, x_n;\, Q, \preceq\}$ be a G-Algebra. Then,*

1. *R is a domain;*

2. *R is left and right Noetherian;*

3. $\mathrm{lc}_R(fg) = \mathrm{lc}_R(f)\,\mathrm{lc}_R(g)q_{\exp(f)\exp(g)}$;

4. $\mathrm{lm}_R(fg) = \mathrm{lm}_R(\mathrm{lm}_R(f)\,\mathrm{lm}_R(g))$;

5. $\mathrm{lt}_R(fg) = \mathrm{lc}_R(f)\,\mathrm{lc}_R(g)q_{\exp(f)\exp(g)}\mathrm{lm}_R(\mathrm{lm}_R(f)\,\mathrm{lm}_R(g))$,

for all $f, g \in R \setminus \{0\}$.

Proof. If $f, g \in R \setminus \{0\}$, then from condition 3 of 2.1.4 it follows that

$$\exp(fg) = \exp(f) + \exp(g) \in \mathbb{N}^n.$$

Hence, $\exp(fg) \neq -\infty$, and so, $fg \neq 0$. Therefore, R is a domain. The statement 2 will be justified later (in 2.3.12).
Now let $f, g \in R \setminus \{0\}$, written in their standard representation as

$$f = \lambda_\alpha x^\alpha + f', \qquad g = \mu_\beta x^\beta + g',$$

where $\mathrm{lc}_R(f) = \lambda_\alpha$, $\mathrm{lc}_R(g) = \mu_\beta$, $\mathrm{lm}_R(f) = x^\alpha$, $\mathrm{lm}_R(g) = x^\beta$, $f' = \sum_{\gamma \prec \alpha} \lambda_\gamma x^\gamma$ and $g' = \sum_{\delta \prec \beta} \mu_\delta x^\delta$. Thus,

$$fg = \lambda_\alpha \mu_\beta x^\alpha x^\beta + \lambda_\alpha x^\alpha g' + \mu_\beta f' x^\beta + f'g'.$$

From the statement 2 of 2.1.4,

$$fg = \lambda_\alpha \mu_\beta q_{\alpha\beta} x^{\alpha+\beta} + \lambda_\alpha \mu_\beta p_{\alpha\beta} + \lambda_\alpha x^\alpha g' + \mu_\beta f' x^\beta + f'g'.$$

with $q_{\alpha\beta} \in \mathsf{k} \setminus \{0\}$ and $\exp(p_{\alpha\beta}) \prec \alpha + \beta$. At this point the proof of the statements 3, 4 and 5 easily finishes since

$$\begin{aligned}
\exp(x^\alpha g') &= \exp(x^\alpha) + \exp(g') \prec \alpha + \beta,\\
\exp(f' x^\beta) &= \exp(f') + \exp(x^\beta) \prec \alpha + \beta,\\
\exp(f'g') &= \exp(f') + \exp(g) \prec \alpha + \beta.
\end{aligned}$$

□

2.2 Examples of G-Algebras

Amongst the examples of G-Algebras, one can find the commutative polynomial ring $k[x_1, \ldots, x_n]$, some iterated Ore extensions as the Weyl algebra $A_n(k)$, the enveloping algebra of any finite-dimensional Lie algebra, a pretty large class of quantum groups just as the multiparameter n-dimensional Quantum space $\mathcal{O}_q(\mathbb{A}^n)$, the bialgebra of Quantum matrices $M_q(2)$, etc. Next we list some of them.

The commutative polynomial ring.

The *commutative polynomial ring* $\mathsf{k}[x_1, \ldots, x_n]$ is obviously a G-Algebra. Indeed,

$$k[x_1, x_2, \ldots, x_n] = \mathsf{k}\{x_1, x_2, \ldots, x_n;\ \{x_j x_i - x_i x_j\}_{1 \leq i < j \leq n},\ \preceq\},$$

where $\preceq$ can be any admissible order on $\mathbb{N}^n$.

The multiparameter Quantum space.

For any matrix $\mathbf{q} = (q_{ij}) \in M_{n \times n}(\mathsf{k})$ assumed to be multiplicatively anti-symmetric (i.e., with non-zero entries, $q_{ii} = 1$ and $q_{ji} = q_{ij}^{-1}$, for every $1 \leq i, j \leq n$), the *multiparameter n-dimensional Quantum space associated to* $\mathbf{q}$, denoted by $\mathcal{O}_{\mathbf{q}}(\mathsf{k}^n)$ or by $\mathsf{k}_{\mathbf{q}}[x_1, \ldots, x_n]$, is defined as the quotient

$$\frac{\mathsf{k}\langle x_1, \ldots, x_n \rangle}{I_Q},$$

where I_Q denotes the two-sided ideal generated by $x_j x_i - q_{ji} x_i x_j$, for all $1 \leq i < j \leq n$. Therefore,

$$\mathsf{k}_{\mathbf{q}}[x_1, \ldots, x_n] = \mathsf{k}\{x_1, \ldots, x_n;\ Q,\ \preceq\},$$

the G-Algebra with quantum relations

$$Q = \{x_j x_i - q_{ji} x_i x_j;\ 1 \leq i < j \leq n\}$$

and any admissible order $\preceq$ on $\mathbb{N}^n$.

The (affine) Quantum space.

As a particular case of 2.2, when

$$\mathbf{q} = \begin{bmatrix} 1 & q^{-1} & \cdots & q^{-1} \\ q & 1 & \cdots & q^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ q & q & \cdots & 1 \end{bmatrix}$$

for some $q \in \mathsf{k} \setminus \{0\}$, we obtain the *$n$-dimensional affine Quantum space*, denoted by $\mathsf{k}_q[x_1, \ldots, x_n]$ or by $\mathcal{O}_q(\mathsf{k}^n)$.

Iterated Ore Extensions.

The previous examples are particular cases of *iterated Ore extensions* of the field k, i.e., algebras of the type

$$\mathsf{k}[x_1;\sigma_1,\delta_1][x_2;\sigma_2,\delta_2]\cdots[x_n;\sigma_n,\delta_n].$$

Let $R_0 = \mathsf{k}$ and for each $1 \leq j \leq n$, let $R_j = R_{j-1}[x_j;\sigma_j,\delta_j]$, the Ore extension associated to a quasi-derivation (σ_j,δ_j) on R_{j-1}. Recall that given a ring endomorphism σ_j of R_{j-1} and a endomorphism δ_j of the additive group R_{j-1} satisfying $\delta_j(rs) = \sigma_j(r)\delta_j(s) + \delta_j(r)s$ for $r, s \in R_{j-1}$, the *Ore extension associated to* (σ_j,δ_j) is the unique ring R_j (up to isomorphisms) such that

1. R_{j-1} is a subring of R_j;
2. there exists $x_j \in R_j$ such that R_j is freely generated as a left R_{j-1}-module by $\{1, x_j, {x_j}^2, \ldots, x_j^n, \ldots\}$;
3. $x_j r = \sigma_j(r)x_j + \delta_j(r)$, for all $r \in R_{j-1}$.

When $\sigma_j = \mathrm{Id}_{R_{j-1}}$, i.e. the identity map on R_{j-1}, the Ore extension associated to (σ_j,δ_j), usually denoted as $R_j = R_{j-1}[x_j;\delta_j]$, is called a *ring of differential operators* over R_{j-1}.
The authors of [13] introduce methods to obtain left PBW rings as iterations of Ore extensions (see [13, Sect. 3, Ch. 2]). One of these methods, specified in the particular case of G-Algebras, is the following.

2.2.1 Proposition. [13] *Let $S = k[x_1;\sigma_1,\delta_1][x_2;\sigma_2,\delta_2]\cdots[x_n;\sigma_n,\delta_n]$ be an iterated Ore extension of the field k, and consider the lexicographical order $\preceq_{lex}$ on $\mathbb{N}^n$ with $\epsilon_1 \prec_{lex} \cdots \prec_{lex} \epsilon_n$. If*

$$\sigma_i(\lambda) = \lambda \text{ and } \delta_i(\lambda) = 0,\ \forall\, \lambda \in k, \tag{2.2}$$

and for all $j > i$ there exist $q_{ji} \in k \setminus \{0\}$ and $f_{ji} \in k[x_1;\sigma_1,\delta_1]\cdots[x_{i-1};\sigma_{i-1},\delta_{i-1}]$ such that

$$\sigma_j(x_i) = q_{ji}x_i + f_{ji}, \tag{2.3}$$

then

$$S = k\{x_1,\ldots,x_n;\ Q,\ \preceq_{lex}\},$$

the G-Algebra with quantum relations

$$Q = \{x_j x_i - q_{ji}x_i x_j - f_{ji}x_j - \delta_j(x_i)\ /\ 1 \leq i < j \leq n\}.$$

The previous result has a kind of converse (see [13, Ch. 3, Th. 6.1]), which yields a test for checking whether some G-Algebras are iterated Ore extensions of the ground field.

The bialgebra of Quantum matrices $M_q(2)$.

The bialgebra of *Quantum matrices*, denoted by $M_q(2)$ or by $O_q(M_2(\mathsf{k}))$, is defined as the quotient of the free algebra $\mathsf{k}\langle a,b,c,d\rangle$ by a two-sided ideal as follows

$$M_q(2) = \frac{\mathsf{k}\langle a,b,c,d\rangle}{\left\langle \begin{matrix} ba-qab, & ca-qac, & ad-da-(q^{-1}-q)bc \\ bc-cb, & db-qbd, & dc-qcd \end{matrix} \right\rangle}$$

In [55, Th. IV.4.1] is shown that $M_q(2)$ is the iterated Ore extension

$$\mathsf{k}[a;1_k,0][b;\sigma_2,0][c;\sigma_3,0][d;\sigma_4,\delta_4],$$

where $\sigma_1 = \mathrm{Id}_{\mathsf{k}}$, σ_2, σ_3 and σ_4 are the ring k-homomorphisms given by

$$\begin{array}{lll} \sigma_2 : A_1 \longrightarrow A_1 & \sigma_3 : A_2 \longrightarrow A_2 & \sigma_4 : A_3 \longrightarrow A_3 \\ \quad a \longmapsto qa. & \quad a \longmapsto qa, & \quad a \longmapsto a, \\ & \quad b \longmapsto b. & \quad b \longmapsto qb, \\ & & \quad c \longmapsto qc. \end{array}$$

with $A_1 = \mathsf{k}[a;0]$, $A_2 = A_1[b;\sigma_2,0]$, $A_3 = A_2[c;\sigma_3,0]$ and δ_4 is the additive endomorphism on A_3, determined by

$$\begin{array}{rl} \delta_4 : & A_3 \longrightarrow A_3 \\ & \lambda b^j c^k \longmapsto 0, \\ & \lambda a^i b^j c^k \longmapsto \lambda(q-q^{-1})\frac{1-q^{2i}}{1-q^2} a^{i-1} b^{j+1} c^{k+1}, \end{array}$$

for all $\lambda \in \mathsf{k}$, $i > 0$, $j,k \geq 0$.
Since conditions (2.2) and (2.3) in 2.2 are satisfied, it follows that

$$M_q(2) = \mathsf{k}\{a,b,c,d;\ Q,\ \preceq_{lex}\},$$

the G-Algebra with set of quantum relations

$$Q = \left\{ \begin{matrix} ba-qab, & ca-qac, & ad-da-(q^{-1}-q)bc \\ bc-cb, & db-qbd, & dc-qcd \end{matrix} \right\}$$

Note that this result is also true for the order $\preceq_\omega$ (defined from the lexicographical order $\preceq_{lex}$ with $\epsilon_1 \prec_{lex} \epsilon_2 \prec_{lex} \cdots \prec_{lex} \epsilon_n$ (see Appendix A)), for any $\omega = (\omega_1,\omega_2,\omega_3,\omega_4) \in \mathbb{N}^4$ such that

$$\omega_2 + \omega_3 \leq \omega_1 + \omega_4.$$

In particular, $M_q(2)$ is a G-Algebra for the order $\preceq_{deglex}$.

The universal enveloping algebras $U(\mathfrak{g})$ of a finite-dimensional Lie algebra $\mathfrak{g}$.

A *Lie algebra* over a field k is a k-vectorspace $\mathfrak{g}$ together with a k-bilinear map (called *Lie product*) $[-,-] : \mathfrak{g} \times \mathfrak{g} \longrightarrow \mathfrak{g}$ satisfying, for all $x, y, z \in \mathfrak{g}$:

1. $[x, x] = 0$;
2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (*Jacobi identity*).

Note that from 1, it follows that the Lie product $[-,-]$ is anti-symmetric as well.

If $\{x_i\}_{i\in I}$ is a k-basis of $\mathfrak{g}$, then the *universal enveloping algebra of* $\mathfrak{g}$, denoted by $U(\mathfrak{g})$, is (isomorphic to) the quotient

$$\frac{\mathsf{k}\langle x_i\rangle_{i\in I}}{I_Q},$$

where I_Q is the two-sided ideal

$$I_Q = \langle x_j x_i - x_i x_j - [x_j, x_i] \,/\, i, j \in I\rangle$$

of $\mathsf{k}\langle x_i\rangle_{i\in I}$. The celebrated *Poincaré-Birkhoff-Witt's Theorem* asserts that given a total order in the set of indexes I, the set of standard monomials

$$\{x_{i_1} \cdots x_{i_n} \,/\, n \in \mathbb{N},\ \{i_1, \ldots, i_n\} \subseteq I,\ i_1 \leq \cdots \leq i_n\}$$

is a k-basis of $U(\mathfrak{g})$ (see [49, 52] for a proof).

As a straightforward consequence of this result, the universal enveloping algebra of a finite-dimensional Lie algebra is a G-Algebra, as it is proved in [13] and we recall next, with a slightly different reformulation which allows us to add more possibilities for the admissible order.

2.2.2 Proposition. *Let $(\mathfrak{g}, [-,-])$ be a Lie algebra over a field k, with k-basis $\{x_1, \ldots, x_n\}$. Then, the universal enveloping algebra is*

$$U(\mathfrak{g}) = k\{x_1, \ldots, x_n;\ Q,\ \preceq_\omega\},$$

the G-Algebra where

$$Q = \{x_j x_i - x_i x_j - [x_j, x_i] \,/\, 1 \leq i < j \leq n\},$$

$\preceq_\omega$ is the ω-weighted lexicographical order on $\mathbb{N}^n$ (obtained from both variants $\epsilon_1 \prec_{lex} \cdots \prec_{lex} \epsilon_n$ and $\epsilon_1 \succ_{lex} \cdots \succ_{lex} \epsilon_n$ of $\preceq_{lex}$ (see Appendix A)), and $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{N}^n$ is such that

$$\omega_1 \leq \cdots \leq \omega_n \qquad \text{and} \qquad \omega_n < \omega_i + \omega_j, \quad \forall\, 1 \leq i < j \leq n-1.$$

In particular, $U(\mathfrak{g})$ is a G-Algebra for the order $\preceq_{deglex}$, which is obtained from $\preceq_\omega$ when $\omega = \epsilon_1 + \cdots + \epsilon_n$.

Proof. Since $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ is a k-algebra of $U(\mathfrak{g})$, it only remains to check that the set of quantum relations Q is bounded by $\preceq_\omega$, when $\omega \in \mathbb{N}^n$ is taken as above. For this purpose, let us first prove that

$$\epsilon_n \prec_\omega \epsilon_i + \epsilon_j, \qquad 1 \leq i < j \leq n. \tag{2.4}$$

- If $1 \leq i < j \leq n-1$, then

  $$|\epsilon_n|_\omega = \omega_n < \omega_i + \omega_j = |\epsilon_i + \epsilon_j|_\omega.$$

  Therefore, $\epsilon_n \prec_\omega \epsilon_i + \epsilon_j$.

- If $1 \leq i < j = n$, and $\omega_i \neq 0$, then

  $$|\epsilon_n|_\omega = \omega_n < \omega_i + \omega_n = |\epsilon_i + \epsilon_j|_\omega.$$

  Otherwise, if $\omega_i = 0$ then

  $$|\epsilon_n|_\omega = \omega_n = 0 + \omega_n = |\epsilon_i + \epsilon_j|_\omega \quad \text{and} \quad \epsilon_n \prec_{lex} \epsilon_i + \epsilon_n.$$

  In both cases, $\epsilon_n \prec_\omega \epsilon_i + \epsilon_n$.

Besides, for all $1 \leq i < j \leq n$ we can write $[x_j, x_i] = \sum_{l=1}^n \lambda_l x_l$, for some $\lambda_l \in \mathsf{k}$. Hence, since $\epsilon_l \prec_\omega \epsilon_{l+1}$ for all $1 \leq l \leq n-1$,

$$\exp\left([x_j, x_i]\right) = \exp\left(\sum_{l=1}^n \lambda_l x_l\right) \preceq_\omega \max\{\exp\left(x_l\right)\}_{l=1}^n = \max\{\epsilon_l\}_{l=1}^n = \epsilon_n. \tag{2.5}$$

From (2.4) and (2.5), we get

$$\exp\left([x_j, x_i]\right) \prec_\omega \epsilon_i + \epsilon_j.$$

□

The universal enveloping algebra $\mathbf{U(\mathfrak{sl}(2))}$ of traceless 2×2-matrices.

Let k be a field of positive characteristic, and let $M_2(\mathsf{k})$ be the k-algebra of 2×2-matrices over k. Consider the Lie algebra $\mathfrak{gl}(2) = (M_2(\mathsf{k}), [-,-])$ with Lie product $[A, B] = AB - BA$. The k-vectorspace $\mathfrak{gl}(2)$ has as a k-basis the set consisting of

$$X = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1, \end{bmatrix},$$

whose products are

$$[Y,X] = -H, \quad [H,X] = 2X, \quad [H,Y] = -2Y, \quad [I,X] = [I,Y] = [I,H] = 0.$$

The Lie algebra $\mathfrak{sl}(2)$ is defined as the subalgebra of $\mathfrak{gl}(2)$ consisting of all matrices of trace zero. The set $\{X,Y,H\}$ constitutes a k-basis of $\mathfrak{sl}(2)$. Thus, its universal enveloping algebra $U(\mathfrak{sl}(2))$ can be constructed as

$$\frac{\mathsf{k}\langle X,Y,H\rangle}{\langle YX - XY + H,\ HX - XH - 2X,\ HY - YH + 2Y\rangle}$$

From Proposition 2.2.2 it follows that for all $\omega \in \mathbb{N}^3$ such that

$$\omega_1 \leq \omega_2 \leq \omega_3 < \omega_1 + \omega_2,$$

we obtain that

$$U(\mathfrak{sl}(2)) = \mathsf{k}\{X,Y,H;\ Q,\ \preceq_\omega\},$$

the G-Algebra with quantum relations

$$Q = \{YX - XY + H,\ HX - XH - 2X,\ HY - YH + 2Y\}.$$

Weyl algebras.

Let $\mathfrak{g}_n$ be the Lie algebra with k-basis $\{x_1,\ldots,x_n,y_1,\ldots,y_n\}$ and whose Lie product is the k-bilinear map given by

$$[y_i,x_j] = -[x_j,y_i] = \delta_{ij}, \qquad [x_i,x_j] = [y_i,y_j] = 0,$$

for all $i,j \in \{1,\ldots,n\}$. The *n-th Weyl algebra* $A_n(\mathsf{k})$ is the universal enveloping algebra $U(\mathfrak{g}_n)$, i.e.,

$$A_n(\mathsf{k}) = \frac{\mathsf{k}\langle x_1,\ldots,x_n,y_1,\ldots,y_n\rangle}{I_Q},$$

where I_Q is the two-sided ideal generated by

$$Q = \left\{ \begin{array}{ll} x_jx_i - x_ix_j, & 1 \leq i < j \leq n \\ y_jx_i - x_iy_j - \delta_{ij}, & 1 \leq i,j \leq n \\ y_jy_i - y_iy_j, & 1 \leq i < j \leq n. \end{array} \right\}$$

From Proposition 2.2.2, the n-th Weyl algebra $A_n(k)$ is the G-Algebra

$$\mathsf{k}\{x_1,\ldots,x_n,y_1,\ldots,y_n;\ Q,\ \preceq\}.$$

Note that $\preceq$ can be any admissible order on $\mathbb{N}^{2n}$.
In [69, 1.3.2] it is shown that the n-th Weyl algebra is an iterated Ore extension. More precisely,

$$A_n(\mathsf{k}) \cong \mathsf{k}[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n][y_1;\alpha_1,\eta_1]\cdots[y_n;\alpha_n,\eta_n],$$

with

$$\sigma_i = \mathrm{Id}; \quad \delta_i = 0; \quad \alpha_i = \mathrm{Id}; \quad \eta_i = \frac{\delta}{\partial x_i}.$$

for all $1 \leq i \leq n$.

The Diamond Algebra.

Let $\mathbb{C}$ be the field of complex numbers. Consider the Lie algebra with $\mathbb{C}$-basis $\{x_1, x_2, x_3, x_4\}$ and with Lie product given by

$$\begin{array}{lll} [x_1,x_2]=0, & [x_1,x_3]=0, & [x_1,x_4]=0 \\ [x_2,x_3]=x_1, & [x_2,x_4]=x_2, & [x_3,x_4]=-x_3. \end{array}$$

The *Diamond algebra* $\mathfrak{D}$ is defined as the universal enveloping algebra of this Lie algebra, i.e.,

$$\mathfrak{D} = \frac{\mathbb{C}\langle x_1,x_2,x_3,x_4\rangle}{\left\langle \begin{array}{lll} x_2x_1 - x_1x_2, & x_3x_1 - x_1x_3, & x_4x_1 - x_1x_4, \\ x_3x_2 - x_2x_3 + x_1, & x_4x_2 - x_2x_4 + x_2, & x_4x_3 - x_3x_4 - x_3 \end{array} \right\rangle}$$

In view of Proposition 2.2.2, for all $\omega \in \mathbb{N}^4$ such that

$$\omega_1 \leq \omega_2 \leq \omega_3 \leq \omega_4 \quad \text{and} \quad \omega_4 < \omega_i + \omega_j, \ \ \forall\ 1 \leq i < j \leq 3,$$

$\mathfrak{D} = \mathbb{C}\{x_1,x_2,x_3,x_4;\ Q,\ \preceq_\omega\}$ is a G-Algebra, where

$$Q = \left\{ \begin{array}{lll} x_2x_1 - x_1x_2, & x_3x_1 - x_1x_3, & x_4x_1 - x_1x_4, \\ x_3x_2 - x_2x_3 + x_1, & x_4x_2 - x_2x_4 + x_2, & x_4x_3 - x_3x_4 - x_3 \end{array} \right\}$$

(Actually, it is obvious from the quantum relations that ω can be any element of $\mathbb{N}^4$ satisfying $\omega_1 < \omega_2 + \omega_3$).
The Diamond algebra $\mathfrak{D}$ can also be written as an iteration of differential operators rings. Indeed,

$$\mathfrak{D} \cong \mathbb{C}[x_1][x_2;\delta_2][x_3;\delta_3][x_4;\delta_4],$$

where $\delta_2 = 0$, and δ_3, δ_4 are the $\mathbb{C}$-linear maps

$$\begin{aligned} \delta_3 : \mathbb{C}[x_1, x_2] &\longrightarrow \mathbb{C}[x_1, x_2] \\ 1 &\longmapsto 0, \\ x_1^i x_2^j &\longmapsto 0, \qquad \text{if } i \geq 1 \\ x_2^j &\longmapsto (-1)^j x_1^j, \quad \text{if } j \geq 1, \end{aligned}$$

$$\begin{aligned} \delta_4 : \mathbb{C}[x_1, x_2][x_3; \delta_3] &\longrightarrow \mathbb{C}[x_1, x_2][x_3; \delta_3] \\ 1 &\longmapsto 0, \\ x_1^i x_2^j x_3^k &\longmapsto 0, \qquad \text{if } i \geq 1 \\ x_2^j x_3^k &\longmapsto (-1)^j x_2^j x_3^k, \qquad \text{if } (j,k) \neq (0,0). \end{aligned}$$

Other examples of G-Algebras are: the *quantum symplectic space* $\mathcal{O}_q(\mathfrak{sp}(\mathsf{k}^{2n}))$ (cf. [13, Ex. 3.8]), positive (negative) parts of quantized enveloping algebras ([56]) (cf. [60, 62]), some nonstandard quantum deformations ([48, 56]) (cf. [60, 61, 62]), many quantizations of Weyl algebras (e.g., the *multiparameter Weyl algebra* $A_n^{Q,\tau}(\mathsf{k})$ (cf. [13, Ex. 3.5])), conformal $\mathfrak{sl}_2$-algebras ([6]) (cf. [60, 61, 62]), some diffusion algebras ([50]) (cf. [60, 61, 62]), etc.

2.2.1 The tensor product of G-Algebras.

The tensor product of G-Algebras is an G-Algebra as well. This result may be proved using some results of basic Algebra.

2.2.3 Lemma. *Let $\{R_i\}_{i=m}$ be a family of k-algebras written as $R_i = (R_i, \cdot, \eta_i)$, where $\cdot$ denotes the multiplication and η_i the unity.*
The tensor product $R_1 \otimes_{\mathsf{k}} \cdots \otimes_{\mathsf{k}} R_m$ is a k-algebra with the multiplication

$$(r_1 \otimes \cdots \otimes r_m)(s_1 \otimes \cdots \otimes s_m) = r_1 s_1 \otimes \cdots \otimes r_m s_m, \quad r_i, s_i \in R_i,$$

and the unity

$$\begin{aligned} \eta : \ \mathsf{k} &\longrightarrow \textstyle\bigotimes_{i=1}^m R_i \\ \lambda &\longmapsto \lambda \eta_1(1) \otimes \cdots \otimes \eta_m(1). \end{aligned}$$

Furthermore, if $\{e_j^i\}_{j \in \mathfrak{I}_i}$ is a k-basis of R_i for $1 \leq i \leq m$, then

$$B = \{e_{j_1}^1 \otimes \cdots \otimes e_{j_m}^m\}_{j_i \in \mathfrak{I}_i}$$

is a k-basis of $\bigotimes_{i=1}^m R_i$.

Proof. The second part is a particular case of a more general (well-known) fact: let $V_1, \ldots, V_m$ be a familiy of k-vectorspaces of not necessarily finite dimension. If $\{e_j^i\}_{j\in\mathfrak{J}_i}$ is a k-basis of V_i for $1 \leq i \leq m$, then

$$B = \{e_{j_1}^1 \otimes \cdots \otimes e_{j_m}^m\}_{j_i\in\mathfrak{J}_i}$$

is a k-basis of $\bigotimes_{i=1}^m V_i$ (see, e.g.,[58]). □

2.2.4 Theorem. *If $R = k\{x_1, \ldots, x_m; Q_R, \preceq_R\}$ and $S = k\{y_1, \ldots, y_n; Q_S, \preceq_S\}$ are G-Algebras with quantum relations*

$$Q_R = \{x_j x_i - q_{ji} x_i x_j - p_{ji};\ 1 \leq i < j \leq m\},$$

$$Q_S = \{y_j y_i - q'_{ji} y_i y_j - p'_{ji};\ 1 \leq i < j \leq n\},$$

then $R \otimes_k S$ is the G-Algebra denoted by

$$k\{x_1 \otimes 1, \ldots, x_m \otimes 1, 1 \otimes y_1, \ldots, 1 \otimes y_n; Q, \preceq\},$$

with quantum relations

$$Q = \left\{ \begin{array}{ll} (x_j \otimes 1)(x_i \otimes 1) - q_{ji}(x_i \otimes 1)(x_j \otimes 1) - p_{ji} \otimes 1; & 1 \leq i < j \leq m \\ (1 \otimes y_j)(x_i \otimes 1) - (x_i \otimes 1)(1 \otimes y_j); & 1 \leq i \leq m,\ 1 \leq j \leq n \\ (1 \otimes y_j)(1 \otimes y_i) - q'_{ji}(1 \otimes y_i)(1 \otimes y_j) - 1 \otimes p'_{ji}; & 1 \leq i < j \leq n. \end{array} \right\}$$

and "$\preceq$" is one of the elimination orders (see the definition in A.4.7) arising from "$\preceq_R$" and "$\preceq_S$".
Furthermore, for all $f \in R \setminus \{0\}$ and $g \in S \setminus \{0\}$,

$$\exp_{R\otimes_k S}(f \otimes g) = (\exp_R(f), \exp_S(g)). \tag{2.6}$$

Proof. Since $\{x^\alpha \,/\, \alpha \in \mathbb{N}^m\}$ and $\{y^\beta \,/\, \beta \in \mathbb{N}^n\}$ are k-basis of R and S respectively, by Lemma 2.2.3, $R \otimes_k S$ is a k-algebra with k-basis

$$\begin{aligned} &\{x^\alpha \otimes y^\beta \,/\, (\alpha, \beta) \in \mathbb{N}^{n+m}\} \\ &= \{x_1^{\alpha_1} \cdots x_m^{\alpha_m} \otimes y_1^{\beta_1} \cdots y_n^{\beta_n} \,/\, (\alpha, \beta) \in \mathbb{N}^{n+m}\} \\ &= \{(x_1^{\alpha_1} \otimes 1) \cdots (x_m^{\alpha_m} \otimes 1)(1 \otimes y_1^{\beta_1}) \cdots (1 \otimes y_n^{\beta_n}) \,/\, (\alpha, \beta) \in \mathbb{N}^{n+m}\} \\ &= \{(x_1 \otimes 1)^{\alpha_1} \cdots (x_m \otimes 1)^{\alpha_m} (1 \otimes y_1)^{\beta_1} \cdots (1 \otimes y_n)^{\beta_n} \,/\, (\alpha, \beta) \in \mathbb{N}^{n+m}\}. \end{aligned}$$

Let us now prove the identity (2.6). Let $f \in R \setminus \{0\}$ and $g \in S \setminus \{0\}$, with standard representations

$$f = c_\alpha x^\alpha + \sum_{\gamma \prec_R \alpha} c_\gamma x^\gamma \quad \text{and} \quad g = d_\beta y^\beta + \sum_{\delta \prec_S \beta} d_\delta x^\delta$$

in R and S, respectively. Then

$$f\otimes g = c_\alpha d_\beta x^\alpha\otimes y^\beta + \sum_{\delta\prec_S\beta} c_\alpha d_\delta x^\alpha\otimes y^\delta + \sum_{\gamma\prec_R\alpha} c_\gamma d_\beta x^\gamma\otimes y^\beta + \sum_{\gamma\prec_R\alpha,\ \delta\prec_S\beta} c_\gamma d_\delta x^\gamma\otimes y^\delta$$

is the standard representation of $f\otimes g\in R\otimes_{\mathrm{k}} S$, with $\exp_{R\otimes_{\mathrm{k}}S}(f\otimes g) = (\exp_R(f),\exp_S(g))$, since

$$\begin{aligned} \delta\prec_S\beta &\Longrightarrow (\alpha,\delta)\prec(\alpha,\beta),\\ \gamma\prec_R\alpha &\Longrightarrow (\gamma,\beta)\prec(\alpha,\beta),\\ \gamma\prec_R\alpha \text{ and } \delta\prec_S\beta &\Longrightarrow (\gamma,\delta)\prec(\alpha,\beta), \end{aligned}$$

for any of the elimination orders $\preceq^*$ or $\preceq_*$ on $\mathbb{N}^n$. Finally, let us check that both elimination orders are compatible with the variables $(x_1\otimes 1),\dots,(x_m\otimes 1),(1\otimes y_1),\dots,(1\otimes y_n)$ in the sense of the statement 1 of Theorem 2.1.4.

- For all $1\le i<j\le m$,

$$\begin{aligned} (x_j\otimes 1)(x_i\otimes 1) &= x_jx_i\otimes 1\\ &= (q_{ji}x_ix_j+p_{ji})\otimes 1\\ &= q_{ji}x_jx_i\otimes 1 + p_{ji}\otimes 1\\ &= q_{ji}(x_i\otimes 1)(x_j\otimes 1)+p_{ji}\otimes 1. \end{aligned}$$

  By virtue of (2.6),

$$\begin{aligned} \exp_{R\otimes_{\mathrm{k}}S}(p_{ji}\otimes 1) &= (\exp_R(p_{ji}),\exp_S(1))\\ &= (\exp_R(p_{ji}),0)\\ &\prec (\epsilon_i^m+\epsilon_j^m,0)\\ &= \epsilon_i^{m+n}+\epsilon_j^{m+n}, \end{aligned}$$

  where $\epsilon_k^m = (0,\dots,\overset{-k-}{1},\dots,0)\in\mathbb{N}^m$ for $1\le k\le m$, and $\epsilon_k^{m+n} = (0,\dots,\overset{-k-}{1},\dots,0)\in\mathbb{N}^{m+n}$ for $1\le k\le m+n$.

- For $1\le i\le m$ and $1\le j\le n$,

$$(1\otimes y_j)(x_i\otimes 1) = x_i\otimes y_j = 1(x_i\otimes 1)(1\otimes y_j)+0,$$

  and trivially, $\exp(0) = -\infty\prec\epsilon_i^{m+n}+\epsilon_{m+j}^{m+n}$.

- For $1\le i<j\le n$,

$$\begin{aligned} (1\otimes y_j)(1\otimes y_i) &= 1\otimes y_jy_i\\ &= 1\otimes(q'_{ji}y_iy_j+p'_{ji})\\ &= q'_{ji}(1\otimes y_jy_i)+1\otimes p'_{ji}\\ &= q'_{ji}(1\otimes y_i)(1\otimes y_j)+1\otimes p'_{ji}. \end{aligned}$$

Again, applying (2.6),

$$\begin{aligned}\exp_{R\otimes_{\mathsf{k}}S}(1\otimes p'_{ji}) &= (\exp_R(1), \exp_S(p'_{ji}))\\ &= (0, \exp_S(p'_{ji}))\\ &\prec (0, \epsilon_i^n + \epsilon_j^n)\\ &= \epsilon_{m+i}^{m+n} + \epsilon_{m+j}^{m+n}.\end{aligned}$$

Since $R = \mathsf{k}\langle x_1, \ldots, x_m\rangle/I_{Q_R}$ and $S = \mathsf{k}\langle y_1, \ldots, y_n\rangle/I_{Q_S}$, the tensor product $R \otimes_{\mathsf{k}} S$ is (isomorphic to) the factor algebra of

$$\mathsf{k}\langle x_1\otimes 1, \ldots, x_m\otimes 1, 1\otimes y_1, \ldots, 1\otimes y_n\rangle$$

by the two-sided ideal I_Q generated by the set Q described in 2.2.4 (see [68]). □

2.2.5 Example. The $(n+m)$-th Weyl algebra $A_{n+m}(\mathsf{k})$ is the G-Algebra $A_n(\mathsf{k}) \otimes_{\mathsf{k}} A_m(\mathsf{k})$ constructed in Theorem 2.2.4.
Indeed, since

$$A_m(\mathsf{k}) = \mathsf{k}\{x_1, \ldots, x_m, y_1, \ldots, y_m;\ Q_m\ \preceq_{lex}\},$$

with quantum relations

$$Q_m = \left\{ \begin{array}{ll} x_jx_i - x_ix_j, & 1\le i<j\le m\\ y_jx_i - x_iy_j - \delta_{ij}, & 1\le i,j\le m\\ y_jy_i - y_iy_j, & 1\le i<j\le m\end{array}\right\},$$

it follows that

$$\begin{aligned}A_m(\mathsf{k})\otimes_{\mathsf{k}} A_n(\mathsf{k}) = \mathsf{k}\{&(x_1\otimes 1), \ldots, (x_m\otimes 1), (y_1\otimes 1), \ldots, (y_m\otimes 1),\\ &(1\otimes x'_1), \ldots, (1\otimes x'_n), (1\otimes y'_1), \ldots, (1\otimes y'_n);\ Q,\ \preceq_{lex}\},\end{aligned}$$

the G-Algebra whose set of quantum relations Q is given by

$$Q = \left\{ \begin{array}{ll}
(x_j\otimes 1)(x_i\otimes 1) = (x_i\otimes 1)(x_j\otimes 1), & 1\le i<j\le m\\
(y_j\otimes 1)(x_i\otimes 1) = (x_i\otimes 1)(y_j\otimes 1) + \delta_{ij}, & 1\le i<j\le m\\
(y_j\otimes 1)(y_i\otimes 1) = (y_i\otimes 1)(y_j\otimes 1), & 1\le i<j\le m\\
(1\otimes x'_j)(x_i\otimes 1) = (x_i\otimes 1)(1\otimes x'_j), & 1\le i\le m,\ \ 1\le j\le n\\
(1\otimes y'_j)(x_i\otimes 1) = (x_i\otimes 1)(1\otimes y'_j), & 1\le i\le m,\ \ 1\le j\le n\\
(1\otimes x'_j)(y_i\otimes 1) = (y_i\otimes 1)(1\otimes x'_j), & 1\le i\le m,\ \ 1\le j\le n\\
(1\otimes y'_j)(y_i\otimes 1) = (y_i\otimes 1)(1\otimes y'_j), & 1\le i\le m,\ \ 1\le j\le n\\
(1\otimes x'_j)(1\otimes x'_i) = (1\otimes x'_i)(1\otimes x'_j), & 1\le i<j\le n.\\
(1\otimes y'_j)(1\otimes x'_i) = (1\otimes x'_i)(1\otimes y'_j) + \delta_{ij}, & 1\le i<j\le n.\\
(1\otimes y'_j)(1\otimes y'_i) = (1\otimes y'_i)(1\otimes y'_j), & 1\le i<j\le n
\end{array}\right\}$$

But this is exactly the Weyl algebra

$$A_{m+n}(\mathsf{k}) = \mathsf{k}\{z_1, \ldots, z_{m+n}, t_1, \ldots, t_{m+n};\ Q_{m+n},\ \preceq_{lex}\},$$

just by putting

$$\begin{array}{ll} z_i := & x_i \otimes 1, \quad 1 \leq i \leq m; \\ z_{m+i} := & 1 \otimes x'_i, \quad 1 \leq i \leq n; \\ t_i := & y_i \otimes 1, \quad 1 \leq i \leq m; \\ z_{m+i} := & 1 \otimes y'_i, \quad 1 \leq i \leq n. \end{array}$$

By iteration, the result 2.2.4 can easily be generalized for the tensor product of a finite number of G-Algebras. For this purpose, we propose a more general definition of elimination orders on $\mathbb{N}^{n_1} \times \cdots \times \mathbb{N}^{n_m}$, which covers all possible ways of ordering the m components of $\mathbb{N}^{n_1} \times \cdots \times \mathbb{N}^{n_m}$ (see A.4.8 in the Appendix A).

2.2.6 Theorem. *Let $\{R_k\}_{k=1}^m$ be a family of G-Algebras, where each R_k is the G-Algebra $k\{x_{k1}, \ldots, x_{kn_k};\ Q_k, \preceq_k\}$ with quantum relations*

$$Q_k = \{x_{kj}x_{ki} - q_{ji}^k x_{ki}x_{kj} - p_{ji}^k;\ 1 \leq i < j \leq n_k\},$$

and $\preceq_k$ is an admissible order on $\mathbb{N}^{n_k}$.
Then, the tensor product $\bigotimes_{k=1}^m R_k$ is the G-Algebra

$$k\{X_{11}, \ldots X_{1n_1}, \ldots, X_{m1}, \ldots X_{mn_m}; Q, \preceq_\sigma^*\},$$

where X_{ki} denotes the variable $1 \otimes \cdots \otimes \overset{-k-}{x_{ki}} \otimes \cdots \otimes 1$, for $1 \leq k \leq m$, $1 \leq i \leq n_k$, with quantum relations

$$Q = \left\{ \begin{array}{cc} X_{kj}X_{li} = X_{li}X_{kj}, & 1 \leq k \neq l \leq m,\ 1 \leq j \leq n_k,\ 1 \leq i \leq n_l \\ X_{kj}X_{ki} = q_{ji}^k X_{ki}X_{kj} + P_{ji}^k, & 1 \leq i < j \leq n_k \end{array} \right\}$$

where P_{ji}^k is the element $1 \otimes \cdots \otimes \overset{-k-}{p_{ji}^k} \otimes \cdots \otimes 1 \in \bigotimes_{k=1}^m R_k$, and "$\preceq_\sigma^*$" is one amongst the $m!$ generalized elimination orders on $\mathbb{N}^{n_1+\cdots+n_m}$ arising from "$\preceq_1$", ..., "$\preceq_m$" (see definition in A.4.8).
Moreover, if $f_k \in R_k \setminus \{0\}$ for $1 \leq k \leq m$, then

$$\exp_{\bigotimes_{k=1}^m R_k}(f_1 \otimes \cdots \otimes f_m) = (\exp_{R_1}(f_1), \ldots, \exp_{R_m}(f_m)).$$

2.2.2 The opposite algebra of a G-Algebra.

For each k-algebra R, let R^{op} be the algebra with the same underlying additive group than R and with product $r \cdot s = sr$, for $r, s \in R$, where sr is computed in R. It turns out that R^{op} inherits from R the structure of G-Algebra, as it is shown in this subsection.
For any $\alpha = (\alpha_1, \ldots, \alpha_1) \in \mathbb{N}^n$, denote by α^{op} the n-tuple $(\alpha_n, \ldots, \alpha_1)$.
Consider the *write oppositely morphism*, defined as the k-automorphism

$$\begin{aligned} {}^{.op} : \mathsf{k}\langle x_1, \ldots, x_n\rangle &\longrightarrow \mathsf{k}\langle x_1, \ldots, x_n\rangle \\ x_{i_1} \cdots x_{i_n} &\mapsto x_{i_n} \cdots x_{i_1} \end{aligned}$$

The following result may be found in [24], where it is proved in the more general situation when R is a left PBW ring.

2.2.7 Proposition. *Let $R = k\{x_1, \ldots, x_n;\ Q, \preceq\}$ be a G-Algebra with quantum relations*

$$Q = \{x_j x_i - q_{ji} x_i x_j - p_{ji};\ 1 \leq i < j \leq n\},$$

Then, its opposite algebra R^{op} is the G-Algebra

$$k\{x_n, \ldots, x_1;\ Q^{\mathrm{op}}, \preceq^{\mathrm{op}}\},$$

where the elements of Q^{op} are those of Q written oppositely, i.e.,

$$Q^{\mathrm{op}} = \{x_i x_j - q_{ji} x_j x_i - p_{ji}^{op};\ 1 \leq i < j \leq n\},$$

Moreover,

$$\exp_{R^{\mathrm{op}}}(f) = (\exp_R(f))^{\mathrm{op}},$$

for all $f \in R \setminus \{0\}$.

Proof. It is straightforward to see that the set $\{x_n^{\alpha_n} \cdots x_1^{\alpha_1}\}_{\alpha \in \mathbb{N}^n}$ is a k-basis of R^{op}, and that $\exp(p_{ji}^{op}) \prec^{\mathrm{op}} \epsilon_{n-i+1} + \epsilon_{n-j+1}$ for $1 \leq i < j \leq n$. □

2.2.3 The enveloping algebra of a G-Algebra.

The *enveloping algebra* of a k-algebra R, denoted by R^{env}, is defined as the tensor product $R \otimes_{\mathsf{k}} R^{\mathrm{op}}$. The enveloping algebra of a G-Algebra is an example of the construction of Theorem 2.2.4. We find that Theorem 2.2.4 holds not only for the elimination orders on $\mathbb{N}^{2n}$, but also for any of the *composition orders* defined in A.4.10 (see Appendix A).

2.2.8 Theorem. *If $R = k\{x_1, \ldots, x_n;\ Q, \preceq\}$ is a G-Algebra with quantum relations*

$$Q = \{x_j x_i - q_{ji} x_i x_j - p_{ji};\ 1 \leq i < j \leq n\},$$

then R^{env} is the G-Algebra

$$k\{x_1 \otimes 1, \ldots, x_n \otimes 1, 1 \otimes x_n, \ldots, 1 \otimes x_1;\ Q^*, \preccurlyeq\},$$

where

$$Q^* = \left\{ \begin{array}{c} (x_j \otimes 1)(x_i \otimes 1) - q_{ji}(x_i \otimes 1)(x_j \otimes 1) - p_{ji} \otimes 1;\ \ 1 \leq i < j \leq n \\ (1 \otimes x_j)(x_i \otimes 1) - (x_i \otimes 1)(1 \otimes x_j); \qquad\qquad 1 \leq i, j \leq n \\ (1 \otimes x_i)(1 \otimes x_j) - q_{ji}(1 \otimes x_j)(1 \otimes x_i) - 1 \otimes p_{ji}^{op};\ \ 1 \leq i < j \leq n. \end{array} \right\}$$

and "$\preccurlyeq$" is, either any of the elimination orders "$\preceq^*$" or "$\preceq_*$" on $\mathbb{N}^{2n}$ corresponding to "$\preceq$" and "$\preceq^{\text{op}}$" (see definitions in A.4.7), or any of the composition orders "$\preceq^c$" or "$\preceq_c$" on $\mathbb{N}^{2n}$ corresponding to "$\preceq$" (defined in A.4.10).

If $f \in R \setminus \{0\}$ and $g \in R^{\text{op}} \setminus \{0\}$, then

$$\exp_{R^{\text{env}}}(f \otimes g) = (\exp_R(f), \exp_{R^{\text{op}}}(g)) = (\exp_R(f), \exp_R(g)^{\text{op}}),$$

for any of the four orders listed above.

Proof. It only remains to check statement 1 of Theorem 2.1.4 and that $\exp_{R^{\text{env}}}(f \otimes g) = (\exp_R(f), \exp_R(g)^{\text{op}})$. Both are straightforward. □

2.3 Gröbner bases in the free module R^s over a G-Algebra

This section is devoted to recall the theory of Gröbner bases in the context of a free module R^s over a G-Algebra R. We closely follow the terminology and results stated in [13], where the authors introduced the theory of Gröbner bases for (*left*, *right*) *PBW rings* and, in particular, for G-Algebras. Obviously, all the results in the current section hold for $s = 1$, i.e., for ideals of the G-Algebra R. In fact, in the literature, the theory of Gröbner bases and Syzygy modules was first developed for ideals of a ring R, and afterwards it was extended to submodules of the free module R^s by mimicking the notions and the results (as in [1, 18, et al.] when R is the commutative polynomial ring, in [13] when R is a (left, right) PBW ring, or in [13, 60, et al.] when R is a G-Algebra).

Throughout this section we will work on the free module R^s, where R is a G-Algebra and s is a positive integer. In the spirit of [13], we will write the elements of R^s in *bold script* in order to distinguish them from those of R. We will use the R-module basis $\{\boldsymbol{e_i}\}_{i=1}^s$ consisting of $\boldsymbol{e_i} = (0, \ldots, \overset{-i-}{1}, \ldots, 0) \in R^s$ for $1 \leq i \leq s$.

In order to handle computationally the elements of R^s, it is necessary to consider a notion of *exponent* of an element $\boldsymbol{f} \in R^s$, and therefore, a notion of *admissible order* on $\mathbb{N}^{n,(s)} = \mathbb{N}^n \times \{1, \ldots, s\}$ is required for this general case. An element $(\alpha, i) \in \mathbb{N}^{n,(s)}$ is said to have *level* i. The monoid $\mathbb{N}^n$ acts on $\mathbb{N}^{n,(s)}$ as $\alpha + (\beta, i) = (\alpha + \beta, i)$ (or equiv., $(\beta, i) + \alpha = (\alpha + \beta, i)$), for $\alpha \in \mathbb{N}^n$ and $(\beta, i) \in \mathbb{N}^{n,(s)}$.

Dickson's Lemma is the key to prove that many algorithms actually stop in a finite number of steps. For example, it is required in the proof of the *Hilbert's Basis Theorem* (see 2.3.12), on which the *Buchberger algorithm* 2.3.17 is based (see e.g. [1] for the commutative version or [13] for left PBW rings).

The following result is a generalization of Dickson's Lemma in $\mathbb{N}^{n,(s)}$. A detailed proof can be found in [13].

2.3.1 Theorem. (Dickson's Lemma) *Let E be a stable subset of $\mathbb{N}^{n,(s)}$, i.e., $\mathbb{N}^n + E = E$. There is a unique minimal set $\{(\alpha_1, i_1), \ldots, (\alpha_m, i_m)\} \subseteq E$ such that*

$$E = \bigcup_{k=1}^{m} ((\alpha_k, i_k) + \mathbb{N}^n).$$

2.3.2 Definition. A total order "$\preceq$" on $\mathbb{N}^{n,(s)}$ is said to be *admissible* if

1. $(\beta, i) \preceq \alpha + (\beta, i)$, and
2. $(\beta, i) \prec (\gamma, j) \;\Rightarrow\; \alpha + (\beta, i) \prec \alpha + (\gamma, j)$,

for all $\alpha \in \mathbb{N}^n$ and $(\beta, i), (\gamma, j) \in \mathbb{N}^{n,(s)}$.

2.3.3 Note. From condition (1), for all $(\alpha, i) \in \mathbb{N}^{n,(s)}$,

$$(0, i) \preceq \alpha + (0, i) = (\alpha, i),$$

Hence, any admissible order $\preceq$ on $\mathbb{N}^{n,(s)}$ is a refinement of the order $\leq^{n,(s)}$ (see the definition in Appendix A). Indeed,

$$\begin{aligned}(\alpha, i) \leq^{n,(s)} (\beta, j) &\Longrightarrow i = j \text{ and } \beta - \alpha \in \mathbb{N}^n \\ &\Longrightarrow (0, i) \preceq (\beta - \alpha, i) \\ &\Longrightarrow \alpha + (0, i) \preceq \alpha + (\beta - \alpha, i) \\ &\Longrightarrow (\alpha, i) \preceq (\beta, i).\end{aligned}$$

2.3.4 Remark. In view of 2.3.1, every admissible order on $\mathbb{N}^{n,(s)}$ is a well-order.

Given an admissible order in $\mathbb{N}^n$, it is possible to obtain some admissible orders in $\mathbb{N}^{n,(s)}$, such as the *Term Over Position order* (or TOP, for short) which gives more importance to the position (or level) i of each element $(\alpha, i) \in \mathbb{N}^{n,(s)}$ than to the admissible order on $\mathbb{N}^n$, or the *Position Over Term order* (POT, for short) (see A.5.2 in Appendix A for the definitions).

2.3.5 Let R be a k-algebra with a PBW basis, say $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$, and let $\preceq$ be an admissible order on $\mathbb{N}^n$. From here on, we will use the same symbol "$\preceq$" for both, the admissible order on $\mathbb{N}^n$ and the one on $\mathbb{N}^{n,(s)}$. This abuse of notation will be harmless because the meaning will be clear from the context. Moreover, from now until the end of this chapter we will assume that both admissible orders satisfy the following condition of compatibility

$$\alpha \prec \beta \implies (\alpha, i) \prec (\beta, i), \quad \forall\, \alpha, \beta \in \mathbb{N}^n,\ 1 \leq i \leq s \tag{2.7}$$

(e.g., the orders TOP and POT satisfy this condititon).
Let us recall how one may assign an exponent to every $\boldsymbol{f} \in R^s$. For any $(\alpha, i) \in \mathbb{N}^{n,(s)}$, let $\boldsymbol{x^{(\alpha,i)}} = x^\alpha \boldsymbol{e_i} = (0, \ldots, \overset{-i-}{x^\alpha}, \ldots, 0) \in R^s$. Since

$$\{\boldsymbol{x^{(\alpha,i)}} \,/\, (\alpha, i) \in \mathbb{N}^{n,(s)}\}$$

is a k-basis of R^s, every $\boldsymbol{f} \in R^s \setminus \{\boldsymbol{0}\}$ has a unique *standard representation*

$$\boldsymbol{f} = \sum_{(\alpha,i) \in \mathbb{N}^{n,(s)}} \lambda_{(\alpha,i)} \boldsymbol{x^{(\alpha,i)}},$$

with $\lambda_{(\alpha,i)} \in \mathsf{k}$, and all but a finite number of $\lambda_{(\alpha,i)}$'s are zero.

- The *Newton diagram* of $\boldsymbol{f}$ is the set

  $$\mathcal{N}(\boldsymbol{f}) = \{(\alpha, i) \,/\, \lambda_{(\alpha,i)} \neq 0\}$$

  (sometimes we will use $\mathcal{N}_{R^s}(\boldsymbol{f})$, for emphasizing the underlying free module R^s);

- The *exponent* of $\boldsymbol{f}$, denoted by $\exp(\boldsymbol{f})$ (or $\exp_{R^s}(\boldsymbol{f})$, in case we want to stress that $\boldsymbol{f}$ belongs to R^s) is defined as

  $$\exp(\boldsymbol{f}) = \max_{\preceq} \mathcal{N}(\boldsymbol{f});$$

- If $\exp(\boldsymbol{f}) = (\alpha, i) \in \mathbb{N}^{n,(s)}$, then

- i will be called the *level* of $\boldsymbol{f}$ (and also, the *level* of (α, i));
- we will denote by $\overline{\exp(\boldsymbol{f})}$ the element $\alpha \in \mathbb{N}^n$;
- the *leading coefficient* of $\boldsymbol{f}$ is $\operatorname{lc}_{R^s}(\boldsymbol{f}) = \lambda_{(\alpha,i)}$;
- the *leading monomial* of $\boldsymbol{f}$ is $\operatorname{lm}_{R^s}(\boldsymbol{f}) = \boldsymbol{x^{(\alpha,i)}}$;
- the *leading term* of $\boldsymbol{f}$ is $\operatorname{lt}_{R^s}(\boldsymbol{f}) = \operatorname{lc}_{R^s}(\boldsymbol{f})\operatorname{lm}_{R^s}(\boldsymbol{f}) = \lambda_{(\alpha,i)}\boldsymbol{x^{(\alpha,i)}}$.

2.3.6 Lemma. *Let $R = k\{x_1, \ldots, x_n;\ Q, \preceq\}$ be a G-Algebra and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. For any $\beta \in \mathbb{N}^n$, $(\alpha, i) \in \mathbb{N}^{n,(s)}$, if the write $x^\beta x^\alpha = q_{\beta\alpha}x^{\alpha+\beta} + p_{\beta\alpha}$ and $p_{\beta\alpha} = \sum_{\gamma \prec \alpha+\beta} \lambda_\gamma x^\gamma$ (as in Theorem 2.1.4), then the equality*

$$x^\beta \boldsymbol{x^{(\alpha,i)}} = q_{\beta\alpha}\boldsymbol{x^{(\alpha+\beta,i)}} + \sum_{(\gamma,i) \prec (\alpha+\beta,i)} \lambda_\gamma \boldsymbol{x^{(\gamma,i)}}$$

holds in R^s, and therefore,

$$\exp_{R^s}(x^\beta \boldsymbol{x^{(\alpha,i)}}) = (\alpha + \beta, i).$$

Proof. Since $x^\beta x^\alpha = q_{\beta\alpha}x^{\alpha+\beta} + p_{\beta\alpha}$ and $p_{\beta\alpha} = \sum_{\gamma \prec \alpha+\beta} \lambda_\gamma x^\gamma$ in R,

$$\begin{aligned} x^\beta \boldsymbol{x^{(\alpha,i)}} &= x^\beta x^\alpha \boldsymbol{e_i} \\ &= (q_{\beta\alpha}x^{\alpha+\beta} + p_{\beta\alpha})\boldsymbol{e_i} \\ &= q_{\beta\alpha}\boldsymbol{x^{(\alpha+\beta,i)}} + \sum_{\gamma \prec \alpha+\beta} \lambda_\gamma \boldsymbol{x^{(\gamma,i)}}. \end{aligned}$$

Finally, by (2.7), $\gamma \prec \alpha + \beta$ in $\mathbb{N}^n$ implies $(\gamma, i) \prec (\alpha + \beta, i)$ in $\mathbb{N}^{n,(s)}$. □

The following result, proved in [13], gives some properties of the exponent in R^s.

2.3.7 Proposition. *Let $R = k\{x_1, \ldots, x_n;\ Q, \preceq\}$ be a G-Algebra and let $\preceq$ be an admissible order on $\mathbb{N}^{n,(s)}$. For all $\boldsymbol{f}, \boldsymbol{g} \in R^s$ and $h \in R$,*

1. $\mathcal{N}(\boldsymbol{f} + \boldsymbol{g}) \subseteq \mathcal{N}(\boldsymbol{f}) \cup \mathcal{N}(\boldsymbol{g})$;
2. $\exp(\boldsymbol{f} + \boldsymbol{g}) \preceq \max\{\exp(\boldsymbol{f}), \exp(\boldsymbol{g})\}$;
3. $\exp_{R^s}(h\boldsymbol{f}) = \exp_R(h) + \exp_{R^s}(\boldsymbol{f})$;
4. *If $\exp_{R^s}(\boldsymbol{f}) = (\alpha, i)$ and $\exp_R(h) = \beta$, then*

$$\begin{aligned} \operatorname{lc}_{R^s}(h\boldsymbol{f}) &= \operatorname{lc}_R(h)\operatorname{lc}_{R^s}(\boldsymbol{f})q_{\beta\alpha}, \\ \operatorname{lm}_{R^s}(h\boldsymbol{f}) &= \boldsymbol{x^{(\alpha+\beta,i)}}, \\ \operatorname{lt}_{R^s}(h\boldsymbol{f}) &= \operatorname{lc}_R(h)\operatorname{lc}_{R^s}(\boldsymbol{f})q_{\beta\alpha}\boldsymbol{x^{(\alpha+\beta,i)}}, \end{aligned} \tag{2.8}$$

where $x^\beta x^\alpha = q_{\beta\alpha}x^{\alpha+\beta} + p_{\beta\alpha}$ (with notation as in Theorem 2.1.4).

In [13] one can find the Left Division Algorithm in R^s, formulated in order to divide on the left side an element $\boldsymbol{f} \in R^s$ by a subset $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\} \subseteq R^s$ when R is a left PBW ring, and in particular, when R is a G-Algebra. This method is recalled in Theorem 2.3.8 and Algorithm 3 (in the latter, the notation $\overline{(\alpha, i)}$ is used for naming the element $\alpha \in \mathbb{N}^n$, for any $(\alpha, i) \in \mathbb{N}^{n,(s)}$, and the definition of the order $\leq^{n,(s)}$ can be found in Appendix A).

2.3.8 Theorem. (Left Division Algorithm) *Let R be the G-Algebra $k\{x_1, \ldots, x_n; Q, \preceq\}$, $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$, and $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\} \subseteq R^s \setminus \{\boldsymbol{0}\}$. For all $\boldsymbol{f} \in R^s$, there exist $h_1, \ldots, h_r \in R$ and $\boldsymbol{r} \in R^s$ such that*

1. $\boldsymbol{f} = \sum_{i=1}^{r} h_i \boldsymbol{f_i} + \boldsymbol{r}$, *where*
2. *if* $\boldsymbol{r} \neq \boldsymbol{0}$, *then* $\mathcal{N}(\boldsymbol{r}) \cap (\bigcup_{i=1}^{r} \exp(\boldsymbol{f_i}) + \mathbb{N}^n) = \emptyset$ *and* $\exp(\boldsymbol{r}) \preceq \exp(\boldsymbol{f})$;
3. *for* $1 \leq i \leq r$, *either* $h_i = 0$ *or* $\exp_R(h_i) + \exp_{R^s}(\boldsymbol{f_i}) \preceq \exp_{R^s}(\boldsymbol{f})$.

Algorithm 3 Left Division Algorithm in R^s

Require: $\boldsymbol{f}, \boldsymbol{f_1}, \ldots, \boldsymbol{f_r} \in R^s \setminus \{\boldsymbol{0}\}$;

Ensure: $h_1, \ldots, h_r, \boldsymbol{r}$ such that $\boldsymbol{f} = \sum_{i=1}^{r} h_i \boldsymbol{f_i} + \boldsymbol{r}$, with

i) $\boldsymbol{r} = \boldsymbol{0}$ or $\mathcal{N}(\boldsymbol{r}) \cap \bigcup_{i=1}^{r} (\exp(\boldsymbol{f_i}) + \mathbb{N}^n) = \emptyset$, and

ii) $\max\{\exp(\boldsymbol{r}), \{\exp(h_i) + \exp(\boldsymbol{f_i})\}_{i=1}^{r}\} = \exp(\boldsymbol{f})$;

Initialization: $h_1 := 0, \ldots, h_r := 0, \boldsymbol{r} := \boldsymbol{0}, \boldsymbol{g} := \boldsymbol{f}$;

while $\boldsymbol{g} \neq \boldsymbol{0}$ **do**

  if there exists i such that $\exp(\boldsymbol{f_i}) \leq^{n,(s)} \exp(\boldsymbol{g})$ **then**

    Choose i minimal such that $\exp(\boldsymbol{f_i}) \leq^{n,(s)} \exp(\boldsymbol{g})$;

    $a_i = \mathrm{lc}_{R^s}(\boldsymbol{g})(\mathrm{lc}_{R^s}(f_i) q^{\overline{\exp(\boldsymbol{g})} - \overline{\exp(\boldsymbol{f_i})}, \overline{\exp(\boldsymbol{f_i})}})^{-1}$;

    $h_i := h_i + a_i x^{\overline{\exp(\boldsymbol{g})} - \overline{\exp(\boldsymbol{f_i})}}$;

    $\boldsymbol{g} := \boldsymbol{g} - a_i x^{\overline{\exp(\boldsymbol{g})} - \overline{\exp(\boldsymbol{f_i})}} \boldsymbol{f_i}$;

  else

    $\boldsymbol{r} := \boldsymbol{r} + \mathrm{lt}_{R^s}(\boldsymbol{g})$;

    $\boldsymbol{g} := \boldsymbol{g} - \mathrm{lt}_{R^s}(\boldsymbol{g})$;

  end if

end while

Return $h_1, \ldots, h_r, \boldsymbol{r}$.

2.3.9 Definition. Under the assumptions of 2.3.8, a *remainder* of the division of $\boldsymbol{f}$ by the set $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\}$, denoted by $\overline{\boldsymbol{f}}^F$, is any element of

R^s which plays the role of $\boldsymbol{r}$ in 2.3.8, satisfying conditions 1, 2 and 3. Each remainder computed with the previous algorithm obviously depends on the order of the elements $\boldsymbol{f_i}$ in the set F.

At this point, we have reviewed the basic background required for studying Gröbner bases in free module R^s.
Let $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra and let $\preceq$ be an admissible order on $\mathbb{N}^{n,(s)}$. For any subset $F \subset R^s$, its *set of exponents*, denoted by $\mathrm{Exp}\,(F)$ (or by $\mathrm{Exp}_{R^s}(F)$, for emphasizing the underlying free module R^s), is

$$\mathrm{Exp}\,(F) = \{\exp_{R^s}(\boldsymbol{f});\ \boldsymbol{f} \in F\} \subseteq \mathbb{N}^{n,(s)}.$$

From property (3) of 2.3.7, it is clear that the set of of exponents $\mathrm{Exp}\,(M)$ of any left R-module M is a *stable subset* of $\mathbb{N}^{n,(s)}$.

2.3.10 Definition. Let $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$.

1. Let M be a left R-submodule of R^s. A set $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq M \setminus \{0\}$ is said to be a *left Gröbner basis for* M, if

$$\mathrm{Exp}\,(M) = \bigcup_{i=1}^{r} (\exp\,(\boldsymbol{g_i}) + \mathbb{N}^n).$$

2. A set $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq R^s \setminus \{0\}$ is a *left Gröbner basis* if it is a left Gröbner basis for the left R-submodule ${}_R\langle G\rangle$.

In a similar way as in the commutative case, the following well-known result follows from Dickson's Lemma.

2.3.11 Proposition. *Let $R = k\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. Every non-zero left R-submodule M of R^s has a finite left Gröbner basis.*

Proof. For any left R-module M, since $\mathrm{Exp}\,(M)$ is a stable set, Theorem 2.3.1 assures the existence of a set $\{(\alpha_1, i_1), \ldots, (\alpha_m, i_m)\} \subseteq \mathrm{Exp}\,(M)$ such that $\mathrm{Exp}\,(M) = \bigcup_{k=1}^{m}((\alpha_k, i_k) + \mathbb{N}^n)$. Hence, there exists $\boldsymbol{g_k} \in M$ with $\exp\,(\boldsymbol{g_k}) = (\alpha_k, i_k)$ for $1 \leq k \leq m$ satisfying

$$\mathrm{Exp}\,(M) = \bigcup_{k=1}^{m} (\exp\,(\boldsymbol{g_k}) + \mathbb{N}^n).$$

□

2.3.12 Note. Proposition 2.3.11 implies any free module R^s over a G-Algebra R to be left Noetherian, that is, every left R-submodule of R^s is finitely generated. In particular, when $s = 1$, the G-Algebra R is a left Noetherian ring (it is also right Noetherian, see [13]), which is an analog of the well-known *Hilbert's Basis Theorem* in the commutative polynomial ring.

The notion of S-polynomial is generalized in [13] from the commutative case (see [1, 18, et al.]) to left PBW rings (and, in particular, to G-Algebras) in the following way.

2.3.13 Definition. Let $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. Consider $\boldsymbol{f}, \boldsymbol{g} \in R^s \setminus \{\mathbf{0}\}$ with exponents (α, i) and (β, j), respectively. Let

$$\begin{aligned} &\gamma = (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\}) \in \mathbb{N}^n; \\ &a = (\mathrm{lc}_{R^s}(x^{\gamma-\alpha}\boldsymbol{f}))^{-1} \in \mathsf{k}; \\ &b = (\mathrm{lc}_{R^s}(x^{\gamma-\beta}\boldsymbol{g}))^{-1} \in \mathsf{k}, \end{aligned}$$

then the *left S-polynomial* of $\boldsymbol{f}$ and $\boldsymbol{g}$ is

$$SP(\boldsymbol{f}, \boldsymbol{g}) = \begin{cases} 0, & \text{if } i \neq j \\ ax^{\gamma-\alpha}\boldsymbol{f} - bx^{\gamma-\beta}\boldsymbol{g}, & \text{if } i = j. \end{cases}$$

The following result, proved in [13], shows some characterizations of the notion of left Gröbner basis. It can be viewed as the analog to the well-known result in the commutative case (see [1, 18, et al.]).

2.3.14 Theorem. *Let $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. Let $M \subseteq R^s$ be a left R-module and $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq M \setminus \{0\}$. The following statements are equivalent:*

1. *G is a left Gröbner basis for M;*
2. *For all $\boldsymbol{f} \in R^s$, $\boldsymbol{f} \in M$ if, and only if, $\overline{\boldsymbol{f}}^G = 0$;*
3. *For all $\boldsymbol{f} \in M$, there exists $h_1, \ldots, h_r \in R$ such that $\boldsymbol{f} = \sum_{k=1}^{r} h_k \boldsymbol{g_k}$ and $\exp(\boldsymbol{f}) = \max\{\exp(h_k) + \exp(\boldsymbol{g_k}) \,/\, 1 \leq k \leq r\}$;*
4. *For all $\boldsymbol{f} \in M$, the remainder $\overline{\boldsymbol{f}}^G$ is independent of the order of the elements in G;*
5. *$M =_R \langle G \rangle$ and $\overline{SP(\boldsymbol{g_i}, \boldsymbol{g_j})}^G = 0$, $\forall\, i \neq j$.*

From the statement 3 directly follows the following result.

2.3.15 Corollary. *Every left Gröbner basis G for a left R-submodule M of R^s is a generator system of M as a left R-module.*

2.3.16 Remark. [13] Under the assumptions of 2.3.14, the statement 5 implies that every generator system $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$ of the left R-module M satisfying level $(\boldsymbol{g_i}) \neq$ level $(\boldsymbol{g_j})$ for all $i \neq j$ is a left Gröbner basis for M.

The last statement of 2.3.14 yields the theoretical background for the *left Buchberger algorithm*, which computes a left Gröbner basis given a finite generator system of a left R-submodule of R^s. It can be viewed as a generalization of the *Buchberger algorithm* in the commutative case [1, 18]. In [13] we can find this algorithm in the more general context when R is a left PBW ring.

2.3.17 Theorem. (Left Buchberger Algorithm) *Let $R = k\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. Let $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\} \subseteq R^s \setminus \{0\}$ be a generator system of a left R-module $M \subseteq R^s$. Then a left Gröbner basis for M can be constructed in a finite number of steps by putting:*

$$\begin{aligned} G_0 &:= F; \\ G_{i+1} &:= G_i \cup \{^{G_i}\overline{SP(\boldsymbol{f},\boldsymbol{g})} \,/\, \boldsymbol{f},\boldsymbol{g} \in G_i,\ SP(\boldsymbol{f},\boldsymbol{g}) \neq \boldsymbol{0}\}. \end{aligned}$$

If $G_i = G_{i+1}$, then G_i is a left Gröbner basis for M.

2.3.18 Definition. Let $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$.

1. Let M be an R-subbimodule of R^s. A set $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq M \setminus \{0\}$ is said to be a *two-sided Gröbner basis for M*, if

$$\mathrm{Exp}\,(M) = \bigcup_{i=1}^{r} (\exp\,(\boldsymbol{g_i}) + \mathbb{N}^n).$$

2. A set $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq R^s \setminus \{0\}$ is a *two-sided Gröbner basis* if it is a two-sided Gröbner basis for ${}_R\langle G\rangle_R$.

In a way analogous to 2.3.11 and 2.3.15, we have the following result.

2.3.19 Corollary. *Let $R = k\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$.*

1. *Every non-zero R-subbimodule M of R^s has a finite two-sided Gröbner basis.*

Algorithm 4 Left Gröbner Basis Algorithm for Modules

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\} \subseteq R^s \setminus \{\boldsymbol{0}\}$;

Ensure: $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_t}\}$, a left Gröbner basis for ${}_R\langle F\rangle$ (satisfying $F \subseteq G$);

Initialization: $G := F$, $B := \{\{\boldsymbol{f}, \boldsymbol{g}\} \,/\, \boldsymbol{f} \neq \boldsymbol{g} \in G\}$;

while $B \neq \emptyset$ **do**

Choose any $\{\boldsymbol{f}, \boldsymbol{g}\} \in B$;

$B := B \setminus \{\{\boldsymbol{f}, \boldsymbol{g}\}\}$;

$\boldsymbol{h'} := SP(\boldsymbol{f}, \boldsymbol{g})$;

$\boldsymbol{h} := \overline{SP(\boldsymbol{f}, \boldsymbol{g})}^{G}$;

if $\boldsymbol{h} \neq \boldsymbol{0}$ **then**

$B := B \cup \{\{\boldsymbol{p}, \boldsymbol{h}\} \,/\, \boldsymbol{p} \in G\}$;

$G := G \cup \{\boldsymbol{h}\}$;

end if

end while

Return G.

2. *Every two-sided (or left) Gröbner basis G for an R-subbimodule M of R^s is a generator system of M as an R-bimodule, i.e., $M = {}_R\langle G\rangle_R$.*

Proof. The first statement is a direct consequence of Dickson's Lemma (see 2.3.1). For the second one, note that if G is a two-sided Gröbner basis for M, then G is obviously a left Gröbner basis for M. Therefore, by 2.3.15, $M = {}_R\langle G\rangle \subseteq {}_R\langle G\rangle_R$. But also ${}_R\langle G\rangle_R \subseteq M$, since $G \subseteq M$ and M is an R-bimodule. □

2.3.20 Theorem. [13] *Let $R = k\{x_1, \ldots, x_n;\, Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. Let $M \subseteq R^s$ be an R-bimodule and $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq R^s \setminus \{0\}$. The following statements are equivalent:*

1. *G is a two-sided Gröbner basis for M;*
2. *G is a left Gröbner basis (for ${}_R\langle G\rangle$) and $M = {}_R\langle G\rangle_R = {}_R\langle G\rangle$;*
3. *G is a left Gröbner basis (for ${}_R\langle G\rangle$), $M = {}_R\langle G\rangle_R$ and $\boldsymbol{g_k}x_i \in {}_R\langle G\rangle$, for all $k \in \{1, \ldots, r\}$ and $i \in \{1, \ldots, n\}$.*

The last statement of 2.3.20 is the theoretical background of the so-called *Right Closure Method* (see [54, 13, et al.]). It is a version of the Buchberger algorithm which computes a two-sided Gröbner basis for any finite generator

system of an R-subbimodule of R^s. We can find it in [54] for two-sided ideals of a G-Algebra, or an improved version, in [62]. In [13, Ch. 3, Th. 9.10] the authors formulate this algorithm in the more general context that R is a PBW ring satisfying a specific condition involving the division ring on which R is defined.

2.3.21 Theorem. (Right Closure Method) *Let R be the G-Algebra $k\{x_1,\ldots,x_n;Q,\preceq\}$ and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. Let M be an R-subbimodule of R^s, and $F=\{\boldsymbol{f_1},\ldots,\boldsymbol{f_r}\}\subseteq R^s\setminus\{0\}$ such that $M={}_R\langle F\rangle_R$. A two-sided Gröbner basis for M can be constructed in a finite number of steps by putting $B_0:=F$, and for $j\geq 0$:*

$$\begin{array}{rcl} G_j & := & \text{a left Gröbner basis for } {}_R\langle B_j\rangle;\\ B_{j+1} & := & G_j\cup\{{}^{G_j}\overline{\boldsymbol{g}x_i}\ /\ \boldsymbol{g}\in G_j,\ 1\leq i\leq n\}.\end{array}$$

If $G_j=B_{j+1}$, then G_j is a two-sided Gröbner basis for M.

2.3.22 Definition. Let $R=\mathsf{k}\{x_1,\ldots,x_n;\ Q,\preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. A left (resp. two-sided) Gröbner basis $G=\{\boldsymbol{g_1},\ldots,\boldsymbol{g_r}\}\subseteq R^s$ for a left submodule (resp. subbimodule) M of R^s is said to be

1. *minimal*, if $\mathrm{lc}_{R^s}(\boldsymbol{g_i})=1$ and for all $1\leq i\leq r$,
$$\exp(\boldsymbol{g_i})\notin\bigcup_{j\neq i}(\exp(\boldsymbol{g_j})+\mathbb{N}^n);$$
2. *reduced*, if $\mathrm{lc}_{R^s}(\boldsymbol{g_i})=1$, and for all $1\leq i\leq r$,
$$\mathcal{N}(\boldsymbol{g_i})\cap(\bigcup_{j\neq i}(\exp(\boldsymbol{g_j})+\mathbb{N}^n))=\emptyset.$$

2.3.23 Remark. Let $R=\mathsf{k}\{x_1,\ldots,x_n;\ Q,\preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. If $G=\{\boldsymbol{g_1},\ldots,\boldsymbol{g_r}\}\subseteq R^s$ is a left (resp. two-sided) Gröbner basis for a left R-module (resp. R-bimodule) $M\subseteq R^s$ such that $\exp(\boldsymbol{g_i})\in\bigcup_{j\neq i}(\exp(\boldsymbol{g_j})+\mathbb{N}^n)$ for some $1\leq i\leq n$, then $G\setminus\{\boldsymbol{g_i}\}$ is also a left (resp. two-sided) Gröbner basis for M. Hence, it is possible to construct a minimal Gröbner basis from any Gröbner basis for a module $M\subseteq R^s$ just by eliminating unnecessary generators (i.e., those $\boldsymbol{g_i}\in G$ such that $\exp(\boldsymbol{g_i})\in\bigcup_{j\neq i}(\exp(\boldsymbol{g_j})+\mathbb{N}^n)$) and dividing each remaining element by its leading coefficient, as it is shown in Algorithm 6.

Algorithm 5 Right Closure Algorithm

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\} \subseteq R^s \setminus \{\boldsymbol{0}\}$;

Ensure: $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_t}\}$, a two-sided Gröbner basis for ${}_R\langle F\rangle_R$ (satisfying $F \subseteq G$);

```
Initialization: B := F, G = ∅;
while B ≠ G do
    Compute a left Gröbner basis G for ₍R⟨B⟩;
    B := G;
    i := 0;
    while i < n do
        i := i + 1;
        Q := G;
        while Q ≠ ∅ do
            choose p ∈ Q;
            Q := Q \ {p};
            q = G-overline(p x_i);
            if q ≠ 0 then
                B := B ∪ {q};
            end if
        end while
    end while
end while
Return G.
```

Just as in the context of the commutative polynomial ring ([1]) the following result provides a method to compute reduced Gröbner bases (Algorithm 7).

2.3.24 Lemma. [13] *Let $R = k\{x_1, \ldots, x_n;\ Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. If $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq R^s$ is a minimal left (resp. two-sided) Gröbner basis for a left submodule (resp. subbimodule) M of R^s and*

$$\boldsymbol{h_i} = \overline{{}^{G \setminus \{\boldsymbol{g_i}\}}\boldsymbol{g_i}},$$

for some $1 \leq i \leq r$, then $\exp(\boldsymbol{h_i}) = \exp(\boldsymbol{g_i})$ and $H = (G \setminus \{\boldsymbol{g_i}\}) \cup \{\boldsymbol{h_i}\}$ is a minimal left (resp. two-sided) Gröbner basis for M.

2.3.25 Theorem. [13] *Let $R = k\{x_1, \ldots, x_n;\ Q, \preceq\}$ be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. Every non-zero left R-submodule (resp.*

Algorithm 6 Minimal Gröbner Basis

Require: $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq R^s$, a left (resp. two-sided) Gröbner basis for a left R-module (resp. R-bimodule) $M \subseteq R^s$;

Ensure: G', a minimal left (resp. two-sided) Gröbner basis for M;

Initialization: $G' := G$;
for $i = 1$ to r **do**
  if $\exp(\boldsymbol{g_i}) \in \bigcup_{\boldsymbol{h} \in G' \setminus \{\boldsymbol{g_i}\}} (\exp(\boldsymbol{h}) + \mathbb{N}^n)$ **then**
    $G' := G' \setminus \{\boldsymbol{g_i}\}$;
  else
    $G' := G' \setminus \{\boldsymbol{g_i}\} \cup \{\mathrm{lc}_{R^s}(\boldsymbol{g_i})^{-1} \boldsymbol{g_i}\}$;
  end if
end for
Return G'.

Algorithm 7 Reduced Gröbner Basis

Require: $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq R^s$, a minimal left (resp. two-sided) Gröbner basis for a left R-module (resp. R-bimodule) $M \subseteq R^s$;

Ensure: H, a reduced left (resp. two-sided) Gröbner basis for M;

Initialization: $H := G$;
for $i = 1$ to r **do**
  $H := H \setminus \{\boldsymbol{g_i}\}$;
  $\boldsymbol{h} := \overline{\boldsymbol{g_i}}^{H}$; $H := \{\boldsymbol{h}\} \cup H$;
end for
Return H.

R-subbimodule) of R^s has a unique reduced left (resp. two-sided) Gröbner basis with respect to $\preceq$.

2.4 Some applications of Gröbner bases

Classical problems as the *Module Membership problem*, the *Modules Comparison problem*, etc. can effectively be solved by using Gröbner bases. In what follows, we recall briefly some of them. We closely follow the lines of [13], where an algorithm for each of such problems is given in the context of *left PBW rings*, including the class of G-algebras. We contribute with an algorithm to compute the dimension of R^s/M as k-vectorspace, where R is

a G-Algebra and M is either a left submodule or a subbimodule of R^s.
Throughout this section, $R = \mathsf{k}\{x_1, \ldots, x_n;\ Q, \preceq\}$ will be a G-Algebra, and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. In the formulation of the problems and the solutions, "*module*" may be, immaterially, either a left R-submodule $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\rangle$ of R^s, or an R-subbimodule $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\rangle_R$ of R^s. When a left R-module M is considered, a Gröbner basis for M will be referred to a left Gröbner basis for M, whilst if M is an R-bimodule, a Gröbner basis for M can be either a left or a two-sided Gröbner basis for M.

• **Module Membership problem.**
The problem consists in, given $\boldsymbol{f} \in R^s$, deciding whether $\boldsymbol{f}$ belongs to a module $M \subseteq R^s$. If G is a Gröbner basis for M, then

$$\boldsymbol{f} \in M \iff {}^{G}\overline{\boldsymbol{f}} = \boldsymbol{0}.$$

If the answer is "yes", then it is possible to compute $h_1, \ldots, h_r \in R$ such that $\boldsymbol{f} = \sum_{i=1}^{r} h_i \boldsymbol{f_i}$ (see the *Extended Gröbner Basis Algorithm* in [13, Ch. 4, Alg. 9]).

• **Module Comparison problem.**
If we want to determine if two modules M and M' are equal, one of the options below may be used:

1. $M = M'$ if, and only if, they have the same reduced Gröbner basis;
2. $M = M'$ if, and only if, $M \subseteq M'$ and $M' \subseteq M$. These two inclusions can be checked by using the solution given for the Module Membership problem for elements of generator systems of M and M' respectively.

• **Coset representatives for the elements of R^s/M.**
For any Gröbner basis G for a module $M \subseteq R^s$,

$$\boldsymbol{f} + M = \boldsymbol{g} + M \iff {}^{G}\overline{\boldsymbol{f}} = {}^{G}\overline{\boldsymbol{g}}, \quad \boldsymbol{f}, \boldsymbol{g} \in R^s.$$

Hence, $\{{}^{G}\overline{\boldsymbol{f}} \,/\, \boldsymbol{f} \in R^s\}$ is a set of coset representatives of R^s/M.

• **Basis of R^s/M as a k-vectorspace.**
For any module $M \subseteq R^s$, the set

$$\{\boldsymbol{x}^{(\boldsymbol{\alpha},\boldsymbol{i})} \,/\, (\alpha, i) \in \mathbb{N}^{n,(s)} \setminus \mathrm{Exp}\,(M)\}$$

is a k-basis of R^s/M. Consequently,

$$\dim_{\mathsf{k}}(R^s/M) = \sharp\,(\mathbb{N}^{n,(s)} \setminus \mathrm{Exp}\,(M)). \tag{2.9}$$

2.4.1 Remark. Since $\mathbb{N}^{n,(s)} \setminus (\mathrm{Exp}\,(G)+\mathbb{N}^n)$ can be expressed as the disjoint union

$$\bigcup_{k=1}^{s} (\mathbb{N}^n \setminus \bigcup_{\boldsymbol{g}\in G;\, \mathrm{level}\,(\boldsymbol{g})=k} (\overline{\exp\,(\boldsymbol{g})} + \mathbb{N}^n)) \times \{k\},$$

if $G \subseteq R^s$ is a Gröbner basis for a module $M \subseteq R^s$, then

$$\begin{aligned}\dim_{\mathrm{k}}(R^s/M) &= \sharp\,(\mathbb{N}^{n,(s)} \setminus (\mathrm{Exp}\,(G) + \mathbb{N}^n)) \\ &= \sum_{k=1}^{s} \sharp\,(\mathbb{N}^n \setminus (\bigcup_{\boldsymbol{g}\in G;\, \mathrm{level}\,(\boldsymbol{g})=k} \overline{\exp\,(\boldsymbol{g})} + \mathbb{N}^n)).\end{aligned}$$

From a geometric point of view, if we consider the geometric system $(\mathbb{N}^n \times \{1\}) \cup \cdots \cup (\mathbb{N}^n \times \{s\})$ and for each element $\boldsymbol{g} \in G$ we represent $\overline{\exp\,(\boldsymbol{g})}$ as a point in the cartesian (non negative integer) coordinate system $\mathbb{N}^n \times \{k\}$ where $k = \mathrm{level}\,(\boldsymbol{g})$, then the value $\dim_{\mathrm{k}}(R^s/M)$ will automatically be obtained by counting the points inside the sets

$$\mathbb{N}^n \setminus (\bigcup_{\boldsymbol{g}\in G;\, \mathrm{level}\,(\boldsymbol{g})=k} \overline{\exp\,(\boldsymbol{g})} + \mathbb{N}^n),$$

for all $k \in \{1, \ldots, s\}$.

2.4.2 Example. The set $G = \{g_1, g_2, g_3\}$, with

$$g_1 = xy^2, \quad g_2 = y^3 + x, \quad g_3 = x^2,$$

is a (minimal) left Gröbner basis for the left ideal $I = {}_R\langle xy^2, y^3 + x\rangle$ of the Quantum plane $\mathbb{Q}_2[x, y] = \mathbb{C}\{x, y;\, \{yx - 2xy\},\, \preceq_{lex}\}$. Therefore,

$$\{x^\alpha y^\beta;\ (\alpha, \beta) \in \mathbb{N}^2 \setminus (\mathrm{Exp}\,(G) + \mathbb{N}^2)\}$$

is a $\mathbb{Q}$-basis of $\mathbb{Q}_2[x, y]/I$ (note that in this case $s = 1$). Since $\mathrm{Exp}\,(G) = \{(1, 2), (0, 3), (2, 0)\}$ it follows that

$$\mathbb{N}^2 \setminus (\mathrm{Exp}\,(G) + \mathbb{N}^2) = \{(0, 0), (1, 0), (0, 1), (1, 1), (0, 2)\}$$

(as it is shown in figure 2.1), and

$$\{1, x, y, xy, y^2\}$$

is a $\mathbb{Q}$- basis of $\mathbb{Q}_2[x, y]/I$.

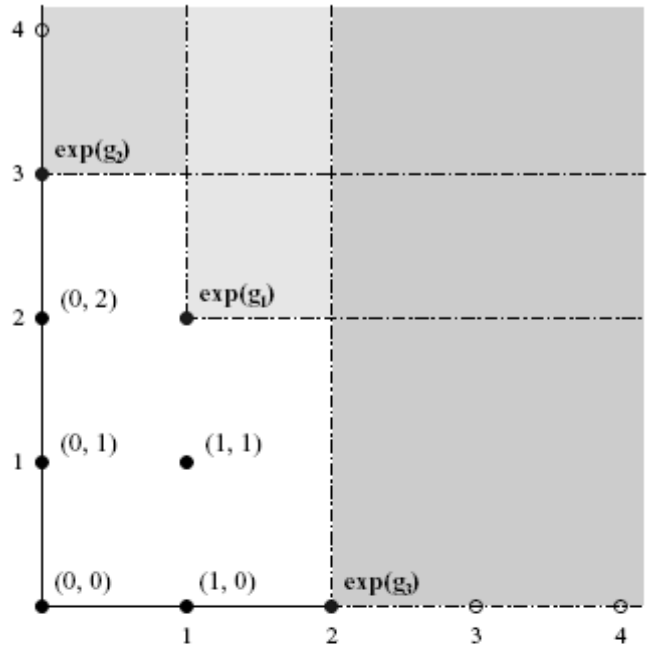


Figure 2.1: Representation of the set $\mathbb{N}^2 \setminus (\mathrm{Exp}\,(G) + \mathbb{N}^2)$ in example 2.4.2

• **Computation of the codimension of a submodule M.**
The *codimension* of a module $M \subseteq R^s$, $\mathrm{codim_k}(M)$, is defined as the k-dimension of R^s/M. In case $\mathrm{codim_k}(M)$ is finite, M is said to be *cofinite*. Next, we present an effective method for deciding when a module $M \subseteq R^s$ is cofinite and, in that case, we show how $\mathrm{codim_k}(M)$ can effectively be computed using the formula stated in 2.4.1 (see Algorithms 8 and 9).

The following result provides an effective test for checking whether a module $M \subseteq R^s$ is cofinite or not, just by browsing the set of exponents of a Gröbner basis for M. It is an extended version (for modules) of a known result for ideals (in the context of commutative polynomial rings see, e.g., [1], or for left PBW rings and, consequently, G-Algebras see [13]).

2.4.3 Proposition. *If $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$ is a Gröbner basis for a module $M \subseteq R^s$, then M is cofinite if, and only if, for all $1 \leq k \leq s$, $1 \leq i \leq n$, there exist $j \in \{1, \ldots, r\}$ and $\nu \in \mathbb{N}$ such that $\exp(\boldsymbol{g_j}) = (\nu\epsilon_i, k)$, where $\epsilon_i = (0, \ldots, \overset{i}{1}, \ldots, 0) \in \mathbb{N}^n$.*

Proof. Assume that $\dim_k(R^s/M) < \infty$. If we suppose for a while that there exist $k \in \{1, \ldots, s\}$ and $i \in \{1, \ldots, n\}$ satisfying

$$\exp(\boldsymbol{g_j}) \neq (\nu\epsilon_i, k),\ \forall\, j \in \{1, \ldots, r\},\ \nu \in \mathbb{N},$$

then it is easy to check that

$$\{(\nu\epsilon_i, k) \,/\, \nu \in \mathbb{N}^n\} \subseteq \mathbb{N}^{n,(s)} \setminus (\mathrm{Exp}\,(G) + \mathbb{N}^n) = \mathbb{N}^{n,(s)} \setminus \mathrm{Exp}\,(M),$$

but this is a contradiction since the left hand side is an infinite set and the right hand side is a finite set (see Eq. (2.9)).
Conversely, as for all $1 \leq k \leq s$ and $1 \leq i \leq n$, there exists $j_{ki} \in \{1, \ldots, r\}$ and $\nu_{ki} \in \mathbb{N}$ such that $\exp(\boldsymbol{g_{j_{ki}}}) = (\nu_{ki}\epsilon_i, k)$, then

$$\mathbb{N}^{n,(s)} \setminus \mathrm{Exp}\,(M) \subseteq \bigcup_{1 \leq k \leq s} \{(\alpha, k) \in \mathbb{N}^{n,(s)} \,/\, \alpha_i < \nu_{ki}, \forall\, 1 \leq i \leq n\},$$

where $\alpha = (\alpha_1, \ldots, \alpha_n)$. Indeed, let $(\alpha, k) \in \mathbb{N}^{n,(s)} \setminus \mathrm{Exp}\,(M)$ and suppose that there exists $i \in \{1, \ldots, n\}$ such that $\alpha_i \geq \nu_{ki}$. Then

$$\begin{aligned}(\alpha, k) &= (0, \ldots, \overset{-i-}{\nu_{ki}}, \ldots, 0, k) + (\alpha_1, \ldots, \alpha_i \overset{-i-}{-} \nu_{ki}, \ldots, \alpha_n) \\ &= \exp(\boldsymbol{g_{ki}}) + \beta,\end{aligned}$$

where $\beta = (\alpha_1, \ldots, \alpha_i \overset{-i-}{-} \nu_{ki}, \ldots, \alpha_n) \in \mathbb{N}^n$. Thus, $(\alpha, k) \in \mathrm{Exp}\,(M)$ - a contradiction. Therefore, $\mathbb{N}^{n,(s)} \setminus \mathrm{Exp}\,(M)$ is finite since $\bigcup_{1 \leq k \leq s} \{(\alpha, k) \in \mathbb{N}^{n,(s)} \,/\, \alpha_i < \nu_{ki}, \forall\, 1 \leq i \leq n\}$ is a finite set. □

2.4.4 Theorem. *The codimension of a cofinite module $M \subseteq R^s$ can be computed by the following method:*

1. *Compute a Gröbner basis $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$ for M (using Algorithm 4 if M is a left R-module, or using Algorithm 5 if M is an R-bimodule);*
2. *Check whether in each level k of the geometric system $(\mathbb{N}^n \times \{1\}) \cup \cdots \cup (\mathbb{N}^n \times \{s\})$ (see 2.4.1), every axe of $\mathbb{N}^n \times \{k\} \cong \mathbb{N}^n$ is "touched" by, at least, one point $\overline{\exp(\boldsymbol{g})}$ for some $\boldsymbol{g} \in G$ such that $\mathrm{level}(\boldsymbol{g}) = k$;*
3. *If the answer in step 2 is "no", then $\mathrm{codim}_k(M)$ is infinite. Otherwise, compute the value codimension as follows:*
   (a) *Compute a minimal Gröbner basis $G' = \{\boldsymbol{g'_1}, \ldots, \boldsymbol{g'_t}\}$ from G (using Algorithm 6), and put codimension $:= 0$;*
   (b) *For every $k \in \{1, \ldots, s\}$ and $i \in \{1, \ldots, n\}$, denote by (α^{ik}, k) the (only) element of $\mathrm{Exp}\,(G')$ such that $\alpha^{ik} = (0, \ldots, \overset{i}{\nu_{ik}}, \ldots, 0)$ for some $\nu_{ik} \in \mathbb{N}$. For every $k \in \{1, \ldots, s\}$, consider the n-cube*

$$\mathcal{C}_k := \mathbb{N}^n \setminus (\bigcup_{1 \leq i \leq n} \alpha^{ik} + \mathbb{N}^n)$$

   inside $\mathbb{N}^n \times \{k\} \cong \mathbb{N}^n$;

(c) *For all* $k \in \{1, \ldots, s\}$ *and all* $(\beta_1, \ldots, \beta_n) \in \mathcal{C}_k$,
if for all $\boldsymbol{g} \in G'$ *with* level $(\boldsymbol{g}) = k$, *there exists an index* $l_{\boldsymbol{g}} \in \{1, \ldots, n\}$ *such that the* $l_{\boldsymbol{g}}$*-th component of* $\overline{\exp(\boldsymbol{g})}$ *is strictly greater than* $\beta_{l_{\boldsymbol{g}}}$, *then let codimension* := *codimension* + 1.

Proof. Note that step 2 is just to check finiteness of $\dim_k(M/R^s)$ by means of the equivalent condition of 2.4.3, that is, for all $k \in \{1, \ldots, s\}$ and $i \in \{1, \ldots, n\}$, there exists

$$(\alpha^{ik}, k) \in \operatorname{Exp}(G) \text{ such that } \alpha^{ik} = (0, \ldots, \overline{\nu_{ik}}^{i-}, \ldots, 0)$$

for some $\nu_{ik} \in \mathbb{N}$. If the algorithm does not stop before step 3, and G' is a minimal Gröbner basis for M, then, the pair $(\alpha^{ik}, k) \in \operatorname{Exp}(G')$ is unique for each fixed k, i. Indeed, if $(\alpha^{ik}, k) \neq (\beta^{ik}, k) \in \operatorname{Exp}(G')$ with $\alpha^{ik} = (0, \ldots, \overline{\nu_{ik}}^{i-}, \ldots, 0)$ and $\beta^{ik} = (0, \ldots, \overline{\mu_{ik}}^{i-}, \ldots, 0)$, then either $\nu_{ik} < \mu_{ik}$ or $\nu_{ik} > \mu_{ik}$. Therefore, either $(\beta^{ik}, k) = (\alpha^{ik}, k) + \gamma$ or $(\alpha^{ik}, k) = (\beta^{ik}, k) + \gamma$, for some $\gamma \in \mathbb{N}^n \setminus \{0\}$, but this is not possible because G' is minimal.
From Eq. (2.9), $\operatorname{codim}_k(M) = \sharp\,(\mathbb{N}^{n,(s)} \setminus \operatorname{Exp}(M))$. On the other hand, it is easy to check that

$$\mathbb{N}^{n,(s)} \setminus \operatorname{Exp}(M) \subseteq \bigcup_{1 \leq k \leq s} \mathcal{C}_k \times \{k\},$$

where $\mathcal{C}_k$ is the n-cube in $\mathbb{N}^n \times \{k\}$, determined by

$$\mathbb{N}^n \setminus (\bigcup_{1 \leq i \leq n} \alpha^{ik} + \mathbb{N}^n).$$

Hence, in order to compute $\operatorname{codim}_k(M)$ it is enough to count, for all $k \in \{1, \ldots, s\}$, the points $(\beta, k) \in \mathcal{C}_k \times \{k\}$ such that (β, k) belongs to $\mathbb{N}^{n,(s)} \setminus \operatorname{Exp}(M)$, or equivalently, the points $(\beta, k) \in \mathcal{C}_k \times \{k\}$ satisfying

$$\beta \in \mathbb{N}^n \setminus (\bigcup_{\boldsymbol{g} \in G; \text{level}\,(\boldsymbol{g}) = k} \overline{\exp(\boldsymbol{g})} + \mathbb{N}^n).$$

This is what is described in step 3c). □

2.4.5 Note. The method of Theorem 2.4.4 also works with $G' = G$ a not necessarily minimal Gröbner basis, that is, step 3a) may be avoided. In that case, in step 3b), since the elements $(\alpha^{ik}, k) \in \operatorname{Exp}(G)$ such that $\alpha^{ik} = (0, \ldots, \overline{\nu_{ik}}^{i-}, \ldots, 0)$ are not necessarily unique, we may put for all $k \in \{1 \ldots, s\}$ and $i \in \{1 \ldots, n\}$,

$$\nu_{ik} := \min\{\mu_{ik} \,/\, \exists\,(\beta^{ik}, k) \in \operatorname{Exp}(G),\ \beta^{ik} = (0, \ldots, \overline{\mu_{ik}}^{i-}, \ldots, 0)\} \in \mathbb{N},$$

Algorithm 8 Cofinite Module

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\} \subseteq R^s$, a generator system of a module $M \subseteq R^s$ ($M = {}_R\langle F\rangle$ or $M = {}_R\langle F\rangle_R$);

Ensure: *cofinite*= FALSE, if M is a cofinite module, and *cofinite*= TRUE, otherwise. If the latter holds, it returns the value of $\mathrm{codim_k}(M)$ in the variable *codimension*;

Initialization: *cofinite*:=TRUE, $i := 1$, $k := 1$;
Compute a Gröbner basis $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$ for M;
while *cofinite*= TRUE and $k \leq s$ and $i \leq n$ **do**
  if $\nexists\, \exp(\boldsymbol{g}) \in G$ such that $\exp(\boldsymbol{g}) = (\nu\epsilon_i, k)$ for some $\nu \in \mathbb{N}$ **then**
    cofinite :=FALSE;
  else
    if $i = n$ **then**
      $k := k + 1$; $i := 1$;
    else
      $i := i + 1$;
    end if
  end if
end while
if *cofinite* = TRUE **then**
  Compute a minimal Gröbner basis G' from G;
  codimension:= 0;
  for $k = 1$ to s **do**
    For $1 \leq i \leq n$, let $(\alpha^{ik}, k) \in \mathrm{Exp}(G')$ s.t. $\alpha^{ik} = (0, \ldots, \overline{\nu_{ik}}^{i}, \ldots, 0)$ for some $\nu_{ik} \in \mathbb{N}$;
    $(\beta_1, \ldots, \beta_n) := (0, \ldots, 0)$;
    Codimension(n,k); {call to Algorithm 9}
  end for
end if
Return *cofinite* and, if *cofinite* = TRUE, return also *codimension*.

Algorithm 9 Codimension

Require: n_{coord} a positive integer, and $k \in \{1, \ldots, s\}$;
  if $n_{coord} = 1$ **then**
    $\beta_1 := 0$;
    while $\forall \boldsymbol{g} \in G$ with level $(\boldsymbol{g}) = k$, there exists $l_{\boldsymbol{g}} \in \{1, \ldots, n\}$ such that the $l_{\boldsymbol{g}}$-th component of $\overline{\exp(\boldsymbol{g})}$ is strictly greater than the $l_{\boldsymbol{g}}$-th component of $(\beta_1, \ldots, \beta_n)$ (current point) **do**
      codimension:= *codimension* + 1;
      $\beta_1 := \beta_1 + 1$;
    end while
  else
    for all $j = 0$ to $(\nu_{n_{coord}\, k} - 1)$ **do**
      Codimension($n_{coord} - 1$,k); {call to Algorithm 9}
      $\beta_{n_{coord}} := \beta_{n_{coord}} + 1$;
    end for
  end if

and $\alpha^{ik} := (0, \ldots, \overset{-i-}{\nu_{ik}}, \ldots, 0)$. The n-cubes will be determined by these new elements (α^{ik}, k).

2.4.6 Remark. From Theorem 2.4.4 we devise Algorithms 8 and 9. The first checks if a module $M \subseteq R^s$ is cofinite, and in that case, it calls the latter to compute $\mathrm{codim_k}(M)$. This one is a recursive algorithm. With recursiveness, we reduce a n-dimensional problem to another one of dimension 1. Actually, there are s problems in dimension n, one for each level k of the geometric system $\mathbb{N}^{n,(s)} = (\mathbb{N}^n \times \{1\}) \cup \cdots \cup (\mathbb{N}^n \times \{s\})$, and each problem is reduced to dimension 1, where they are solved by a simple search through the set $\{\boldsymbol{g} \in G' / \text{level}\,(\boldsymbol{g}) = k\}$. Note that for each $k \in \{1, \ldots, s\}$, Algorithm 9 actually stops. In fact, it calls itself $\prod_{i=2}^{n} \nu_{ik}$ times. Moreover, with the computation of a minimal Gröbner basis G' in Algorithm 8, the search in Algorithm 9 is improved, since there are no redundant elements.

2.4.7 Example. Let us take up again the example 2.4.2, where the minimal left Gröbner basis $G = \{g_1 = xy^2,\ g_2 = y^3 + x,\ g_3 = x^2\}$ for the left ideal $I = {}_R\langle xy^2, y^3 + x\rangle$ of the Quantum plane $\mathbb{Q}_2[x, y] = \mathbb{C}\{x, y; \{yx - 2xy\}, \preceq_{lex}\}$ was considered.

Let us compute the codimension of I by Algorithm 8.

Initialization: *cofinite*:=TRUE, $i := 1$, $k := 1$, $G := \{xy^2,\ y^3 + x,\ x^2\}$.

First step by the *while* loop (i=1):

$\exp(g_3) = ((2, 0), 1)$ has the second component different from 0; $i = 2$.

Second step by the *while* loop (i=2):
$\exp(g_2) = ((0,3),1)$ has the first component different from 0; $i = 3$.

As *cofinite* = TRUE, we continue with the *if*-clause:
$G = \{xy^2,\ y^3 + x,\ x^2\}$ is a minimal left Gröbner basis for I.

$$\alpha^1 = (2,0),\ \nu_1 = 2, \quad \alpha^2 = (0,3),\ \nu_2 = 3, \quad (\beta_1, \beta_2) = (0,0).$$

Call to Codimension(2, 1):

- **First step by the *for* loop (j=0)**:

  Codimension(1, 1):

  ***while* loop**:

  As $(1,2)$, $(0,3)$ and $(2,0)$ have some component greater than the correspondent component of $(0,0)$, then *codimension* := 1.

  As $(1,2)$, $(0,3)$ and $(2,0)$ have some component greater than the correspondent component of $(1,0)$, then *codimension* := 2.

  None component of $(2,0)$ is greater than the correspondent of $(2,0)$.

- **Second step by the *for* loop (j=1)**:

  Codimension(1, 1):

  ***while* loop**:

  As $(1,2)$, $(0,3)$ and $(2,0)$ have some component greater than the correspondent component of $(0,1)$, then *codimension* := 3.

  As $(1,2)$, $(0,3)$ and $(2,0)$ have some component greater than the correspondent component of $(1,1)$, then *codimension* := 4.

  None component of $(2,0)$ is greater than the correspondent of $(2,1)$.

- **Third step by the *for* loop (j=2)**:

  Codimension(1,1):

  ***while* loop**:

  As $(1,2)$, $(0,3)$ and $(2,0)$ have some component greater than the correspondent component of $(0,2)$, then *codimension* := 5.

  None component of $(1,2)$ is greater than the correspondent of $(1,2)$.

Return *cofinite*=TRUE and *codimension*=5.

More applications of left and two-sided Gröbner bases in the free module R^s over a G-Algebra R will be shown in Section 2.6, where Gröbner bases will be required in the computation of *left syzygy modules* and *syzygy bimodules*, as well as some derived problems on left modules and bimodules: computation of presentations and free resolutions, finite intersections, division ideals, etc.

2.5 New methods for handling bimodules

As we have seen along this chapter, methods based on Gröbner bases have been developed not only for left (and right) modules, but also for R-bimodules over a G-Algebra R. Nevertheless, in these generalizations, the authors ([13, 60, et al.]) are mainly interested in one-sided ideals and modules, whereas methods for the two-sided counterparts are adaptations to deal with the two-sided input. For example, to compute the intersection of two bimodules $M, N \subseteq R^s$ provided a set of generators as an R-bimodule for each of them, say $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_r} \rangle_R$ and $N = {}_R\langle \boldsymbol{g_1}, \ldots, \boldsymbol{g_t} \rangle_R$, the method used so far consists in computing first two-sided Gröbner bases G and H for M and N resp., and afterwards, since G and H are in particular generator systems for M and N as left R-modules, apply already known algorithms to compute the intersection $M \cap N$ of two left R-submodules of R^s (this can be done by using, for example, the procedure based on elimination or that based on left syzygy modules, see [13] for both).

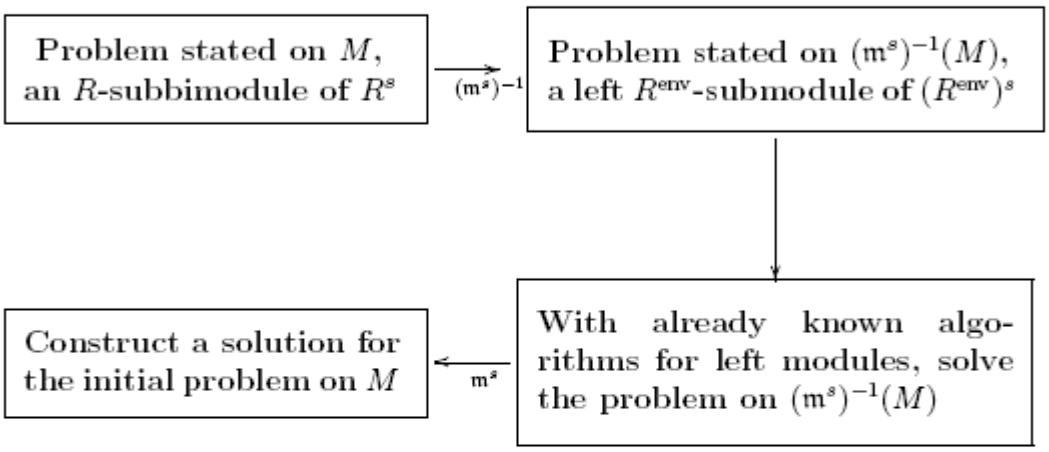
In this section we propose a new method, that we made known first in [28], to perform effective computations on bimodules by handling directly their (two-sided) generator systems as input data, and therefore, avoiding unnecessary initial two-sided Gröbner basis computations.

Though we apply this technique on R-subbimodules of R^s when R is a G-Algebra, there is no reason why it could not be applied when R and its enveloping algebra $R^{\mathrm{env}} = R \otimes_{\mathsf{k}} R^{\mathrm{op}}$ are "effective algebras", in the sense that the theory of Gröbner bases (divisions, computation of Gröbner bases, etc.) can be extended in order to be used with left R-submodules of R^s. As we will see later, by using this technique many algorithms for bimodules may easily be devised. We first used it in [24, 26] in order to construct an algorithm for computing two-sided Gröbner bases for two-sided ideals of G-Algebras.

Our method, outlined in the diagram (2.10), is based on the very well-known fact that if R is a k-algebra, then the R-bimodules are exactly the left modules over the enveloping algebra R^{env}. More precisely, through the morphism $\mathfrak{m}^s : (R^{\mathrm{env}})^s \longrightarrow R^s$ described in (2.11), we can translate any problem stated on a bimodule $M \subseteq R^s$ into a problem stated on the left R^{env}-module

$(\mathfrak{m}^s)^{-1}(M) \subseteq (R^{\mathrm{env}})^s$. When R, and therefore R^{env}, is a G-Algebra already known algorithms for left R-modules can be applied in order to solve the problem for $(\mathfrak{m}^s)^{-1}(M)$. Once we have a solution of this left module, we push it through $\mathfrak{m}^s$ into a solution of the initial problem on M.
This method can be applied, for example, for computing two-sided Gröbner bases for bimodules as we will see in Section 2.5.1, or the *Syzygy Bimodule*, studied in Section 2.6.

TECHNIQUE TO HANDLE BIMODULES:



(2.10)

Let us start with the first step of the method above, i.e. how to move the data of a bimodule M to $(\mathfrak{m}^s)^{-1}(M)$ through $(\mathfrak{m}^s)^{-1}$. We fix previously some notation and we point out some considerations which will be used from here on in this chapter.

2.5.1 Let R be a ring. It is well-known that R-bimodules are exactly left $R \otimes_{\mathbb{Z}} R^{\mathrm{op}}$-modules. Thus, when we know a finite set of generators of a bimodule M, say $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$, then for all $\boldsymbol{f} \in M$,

$$\boldsymbol{f} = \sum_{i;\,\text{finite}} p_i \boldsymbol{f_i}$$

for some $p_i \in R \otimes_{\mathbb{Z}} R^{\mathrm{op}}$. Note also that if M is an R-bimodule and $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle$ or $M = \langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$, then $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$.
Consider the free modules R^s and $(R \otimes_{\mathbb{Z}} R^{\mathrm{op}})^s$ of rank $s \geq 1$. When $\boldsymbol{f} = (f_1, \ldots, f_s)$, $\boldsymbol{g} = (g_1, \ldots, g_s) \in R^s$, we shall denote by $\boldsymbol{f} \otimes \boldsymbol{g}$ the element

$$(f_1 \otimes g_1, \ldots, f_s \otimes g_s) \in (R \otimes_{\mathbb{Z}} R^{\mathrm{op}})^s.$$

The left $R \otimes_{\mathbb{Z}} R^{\mathrm{op}}$-module structure of R^s is given by

$$(r \otimes r')\, \boldsymbol{f} = (r f_1 r', \ldots, r f_s r'),$$

and the R-bimodule structure of $(R \otimes_{\mathbb{Z}} R^{\mathrm{op}})^s$ by

$$r(\boldsymbol{f} \otimes \boldsymbol{g})r' = (r f_1 \otimes g_1 r', \ldots, r f_s \otimes g_s r'),$$

where $r, r' \in R$ and $\boldsymbol{f} = (f_1, \ldots, f_s)$, $\boldsymbol{g} = (g_1, \ldots, g_s) \in R^s$.
We will denote by $\mathfrak{m}^s$ the epimorphism of left $R \otimes_{\mathbb{Z}} R^{\mathrm{op}}$-modules

$$\mathfrak{m}^s = \mathfrak{m} \times \overset{s}{\cdots} \times \mathfrak{m} : (R \otimes_{\mathbb{Z}} R^{\mathrm{op}})^s \longrightarrow R^s, \tag{2.11}$$

where $\mathfrak{m}(r \otimes r') = rr'$, for $r, r' \in R$.
The following is a result of basic Algebra.

Lemma. Let S be a ring. If $\psi : A \longrightarrow B$ is a morphism of left S-modules, then there exists a bijection

$$\begin{array}{rcl} \{N \subseteq A \,/\, \mathrm{Ker}\,(\psi) \subseteq N \in S\text{–Mod}\} & \longrightarrow & \{M \subseteq \mathrm{Im}\,(\psi) \,/\, M \in S\text{–Mod}\} \\ N & \rightarrow & M_N := \psi(N), \\ N_M := \psi^{-1}(M) & \leftarrow & M. \end{array}$$

In particular, since $\mathfrak{m}^s : (R \otimes_{\mathbb{Z}} R^{\mathrm{op}})^s \longrightarrow R^s$ is a morphism of left $R \otimes_{\mathbb{Z}} R^{\mathrm{op}}$-modules, we have the bijection

$$\begin{array}{rcl} \left\{ \begin{array}{c} N \subseteq (R \otimes_{\mathbb{Z}} R^{\mathrm{op}})^s \text{ such that} \\ \mathrm{Ker}\,(\mathfrak{m}^s) \subseteq N,\ N \in R \otimes_{\mathbb{Z}} R^{\mathrm{op}}\text{–Mod} \end{array} \right\} & \longrightarrow & \{M \subseteq R^s \,/\, M \in R\text{–Bimod}\} \\ N & \rightarrow & M_N := \mathfrak{m}^s(N), \\ N_M := (\mathfrak{m}^s)^{-1}(M) & \leftarrow & M \end{array} \tag{2.12}$$

Note that if R is a k-algebra, then the maps (2.11) and (2.12) are also valid for the *enveloping algebra* $R^{\mathrm{env}} = R \otimes_{\mathsf{k}} R^{\mathrm{op}}$.

Proposition 2.5.2 is a generalization of a result formulated for $s = 1$, which we proved in [24].

2.5.2 Proposition. *Let R be a k-algebra.*

1. *If M is an R-subbimodule of R^s, and $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$, or $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle$, or $M = \langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$, then*

$$N_M = {}_{R^{\mathrm{env}}}\langle \boldsymbol{f_1} \otimes \mathbf{1}, \ldots, \boldsymbol{f_t} \otimes \mathbf{1} \rangle + \mathrm{Ker}\,(\mathfrak{m}^s);$$

2. $\mathrm{Ker}\,(\mathfrak{m}^s) = {}_{R^{\mathrm{env}}}\langle \boldsymbol{f}\otimes \mathbf{1} - \mathbf{1}\otimes \boldsymbol{f}\ ;\ \boldsymbol{f}\in R^s\rangle$;

3. *If R has a generator system (as a k-vectorspace) consisting of standard monomials, say $\{x^\alpha \,/\, \alpha\in\mathbb{N}^n\}$, then*

$$\mathrm{Ker}\,(\mathfrak{m}^s) = {}_{R^{\mathrm{env}}}\langle\{\boldsymbol{x}^{(\boldsymbol{\epsilon_j},\boldsymbol{k})}\otimes\mathbf{1} - \mathbf{1}\otimes\boldsymbol{x}^{(\boldsymbol{\epsilon_j},\boldsymbol{k})}\}_{1\le j\le n, 1\le k\le s}\rangle.$$

The statements 1 and 2 are also valid for any ring R, considering $R\otimes_{\mathbb{Z}} R^{\mathrm{op}}$ instead of R^{env}.

Proof. Let us prove the statement 1. If $M = {}_R\langle \boldsymbol{f_1},\dots,\boldsymbol{f_t}\rangle_R$, then for every $\boldsymbol{g}\in N_M = (\mathfrak{m}^s)^{-1}(M)$, its image can be written as

$$\mathfrak{m}^s(\boldsymbol{g}) = \sum_{i=1}^{t} p_i\boldsymbol{f_i},$$

for some elements $p_i\in R^{\mathrm{env}}$. Therefore, putting

$$\boldsymbol{f} = \sum_{i=1}^{t} p_i(\boldsymbol{f_i}\otimes\mathbf{1}) \in {}_{R^{\mathrm{env}}}\langle \boldsymbol{f_1}\otimes 1,\dots,\ \boldsymbol{f_t}\otimes\mathbf{1}\rangle,$$

it follows that

$$\begin{aligned}\mathfrak{m}^s(\boldsymbol{f}-\boldsymbol{g}) &= \mathfrak{m}^s\Big(\sum_{i=1}^{t} p_i(\boldsymbol{f_i}\otimes\mathbf{1})\Big) - \mathfrak{m}^s(\boldsymbol{g})\\ &= \sum_{i=1}^{t} p_i\mathfrak{m}^s(\boldsymbol{f_i}\otimes 1) - \sum_{i=1}^{t} p_i\boldsymbol{f_i}\\ &= \mathbf{0}.\end{aligned}$$

Hence, $\boldsymbol{g}\in {}_{R^{\mathrm{env}}}\langle \boldsymbol{f_1}\otimes\mathbf{1},\dots,\ \boldsymbol{f_t}\otimes\mathbf{1}\rangle + \mathrm{Ker}\,(\mathfrak{m}^s)$. Conversely, $\mathrm{Ker}\,(\mathfrak{m}^s)\subseteq N_M$ and $\boldsymbol{f_i}\otimes\mathbf{1}\in N_M$ for $1\le i\le t$.
With regard to the statement 2, clearly $\boldsymbol{f}\otimes\ 1 - 1\otimes\boldsymbol{f}\in\mathrm{Ker}\,(\mathfrak{m}^s)$ for all $\boldsymbol{f}\in R^s$. On the other hand, every $\boldsymbol{g}\in\mathrm{Ker}\,(\mathfrak{m}^s)$ can be written as

$$\boldsymbol{g} = \sum_{i=1}^{s} g_i\boldsymbol{e_i}$$

where $g_i = \sum_{k\in\Lambda_i} r_{ik}\otimes r'_{ik}\in R^{\mathrm{env}}$ and $\boldsymbol{e_i} = (0,\dots,\overset{-i-}{1\otimes 1},\dots,0)$ for $1\le i\le s$. Since $\mathfrak{m}^s(\boldsymbol{g}) = \mathbf{0}$, clearly

$$0 = \mathfrak{m}(g_i) = \sum_{k\in\Lambda_i} r_{ik}r'_{ik}$$

for all $1 \leq i \leq s$. Hence,

$$\begin{aligned}\boldsymbol{g} &= \sum_{i=1}^{s} g_i \boldsymbol{e_i} \\ &= \sum_{i=1}^{s} ((\sum_{k\in\Lambda_i} -r_{ik}r'_{ik} \otimes 1) + g_i)\boldsymbol{e_i} \\ &= \sum_{i=1}^{s} (\sum_{k\in\Lambda_i} (-r_{ik} \otimes 1)(r'_{ik} \otimes 1 - 1 \otimes r'_{ik}))\boldsymbol{e_i} \\ &= \sum_{i=1}^{s} \sum_{k\in\Lambda_i} (-r_{ik} \otimes 1)(r'_{ik}\boldsymbol{e_i} \otimes \mathbf{1} - \mathbf{1} \otimes r'_{ik}\boldsymbol{e_i}).\end{aligned}$$

Therefore, $\boldsymbol{g} \in {}_{R^{\mathrm{env}}}\langle \boldsymbol{f} \otimes \mathbf{1} - \mathbf{1} \otimes \boldsymbol{f} \,;\, \boldsymbol{f} \in R^s \rangle$.
Finally, let us prove the statement 3. As

$$\mathrm{Ker}\,(\mathfrak{m}^s) = \mathrm{Ker}\,(\mathfrak{m}) \times \overset{s}{\ldots} \times \mathrm{Ker}\,(\mathfrak{m}),$$

it is enough to prove this for the case $s = 1$, i.e., to prove that

$$\mathrm{Ker}\,(\mathfrak{m}) = {}_{R^{\mathrm{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \,/\, 1 \leq j \leq n \rangle. \tag{2.13}$$

Once this is proved, every $\boldsymbol{g} \in \mathrm{Ker}\,(\mathfrak{m}^s)$ can be written as $\boldsymbol{g} = \sum_{k=1}^{s} g_k \boldsymbol{e_k}$ where $\{\boldsymbol{e_k}\}_{k=1}^{s}$ is the canonical basis of $(R^{\mathrm{env}})^s$ as a R^{env}-module, and

$$g_k = \sum_{j=1}^{n} p_{kj}(x_j \otimes 1 - 1 \otimes x_j)$$

with $p_{kj} \in R^{\mathrm{env}}$. Since $g_k \in \mathrm{Ker}\,(\mathfrak{m})$,

$$\boldsymbol{g} = \sum_{k=1}^{s}\sum_{j=1}^{n} p_{kj}(x_j \otimes 1 - 1 \otimes x_j)\boldsymbol{e_k} = \sum_{k=1}^{s}\sum_{j=1}^{n} p_{kj}(\boldsymbol{x^{(\epsilon_j,k)}} \otimes \mathbf{1} - \mathbf{1} \otimes \boldsymbol{x^{(\epsilon_j,k)}}).$$

This fact, together with the assertion 2 in the Proposition implies the statement 3.
So, let us prove Eq. (2.13) which, by the statement 2, is equivalent to prove that

$$f \otimes 1 - 1 \otimes f \in {}_{R^{\mathrm{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \,/\, 1 \leq j \leq n \rangle, \quad \forall\, f \in R.$$

If $f = \sum_{\alpha\in\mathbb{N}^n} \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in R$, then in R^{env} we have

$$\begin{aligned}f \otimes 1 - 1 \otimes f = &((\sum_{\alpha} \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n - 1}) \otimes 1)(x_n \otimes 1 - 1 \otimes x_n) \\ &+ ((\sum_{\alpha} \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n - 1}) \otimes x_n) - (1 \otimes (\sum_{\alpha} \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n})).\end{aligned}$$

Since

$$A_1^n = ((\sum_\alpha \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n - 1}) \otimes 1)(x_n \otimes 1 - 1 \otimes x_n)$$

is an element of ${}_{R^{\text{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \,/\, 1 \leq j \leq n\rangle$, to prove that

$$f \otimes 1 - 1 \otimes f \in {}_{R^{\text{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \,/\, 1 \leq j \leq n\rangle$$

is equivalent to prove that

$$f \otimes 1 - 1 \otimes f - A_1^n \in {}_{R^{\text{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \,/\, 1 \leq j \leq n\rangle.$$

But

$$\begin{aligned} f \otimes 1 - 1 \otimes f - A_1^n = &((\sum_\alpha \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n - 2}) \otimes x_n)(x_n \otimes 1 - 1 \otimes x_n) \\ &+ ((\sum_\alpha \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n - 2}) \otimes x_n^2) - (1 \otimes (\sum_\alpha \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n})). \end{aligned}$$

So, taking

$$A_2^n = ((\sum_\alpha \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n - 2}) \otimes x_n)(x_n \otimes 1 - 1 \otimes x_n) \in {}_{R^{\text{env}}}\langle x_j \otimes 1 - 1 \otimes x_j / 1 \leq j \leq n\rangle,$$

to prove that

$$f \otimes 1 - 1 \otimes f \in {}_{R^{\text{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \,/\, 1 \leq j \leq n\rangle$$

is equivalent to prove that

$$f \otimes 1 - 1 \otimes f - A_1^n - A_2^n \in {}_{R^{\text{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \,/\, 1 \leq j \leq n\rangle.$$

Repeating this process, at some point we only have to prove that

$$f \otimes 1 - 1 \otimes f - \sum_{i=2}^{n} \sum_{j=1}^{\alpha_i} A_j^i - \sum_{j=1}^{\alpha_1 - 1} A_j^1 \in {}_{R^{\text{env}}}\langle \{x_j \otimes 1 - 1 \otimes x_j\}_{1 \leq j \leq n}\rangle,$$

where

$$A_j^i = ((\sum_\alpha \lambda_\alpha x_1^{\alpha_1} \cdots x_i^{\alpha_i - j}) \otimes x_i^{j-1} x_{i+1}^{\alpha_{i+1}} \cdots x_n^{\alpha_n})(x_i \otimes 1 - 1 \otimes x_i),$$

for $1 \leq i \leq n$, $1 \leq j \leq \alpha_i$, and indeed,

$$\begin{aligned} &f \otimes 1 - 1 \otimes f - \sum_{i=2}^{n} \sum_{j=1}^{\alpha_i} A_j^i - \sum_{j=1}^{\alpha_1 - 1} A_j^1 = \\ &= (\sum_\alpha \lambda_\alpha (1 \otimes x_1^{\alpha_1 - 1} \cdots x_n^{\alpha_n}))(x_1 \otimes 1 - 1 \otimes x_1) \\ &+ ((\sum_\alpha \lambda_\alpha (1 \otimes x_1^{\alpha_1} \cdots x_n^{\alpha_n})) - (1 \otimes (\sum_\alpha \lambda_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n})) \\ &= (\sum_\alpha \lambda_\alpha (1 \otimes x_1^{\alpha_1 - 1} \cdots x_n^{\alpha_n}))(x_1 \otimes 1 - 1 \otimes x_1). \end{aligned}$$

Therefore,

$$f \otimes 1 - 1 \otimes f \in {}_{R^{\mathrm{env}}}\langle x_j \otimes 1 - 1 \otimes x_j \;/\; 1 \leq j \leq n \rangle.$$

□

As a direct consequence of 2.5.2, we have:

2.5.3 Corollary. *If $R = k\{x_1, \ldots, x_n;\ Q; \preceq\}$ and M is an R-subbimodule of R^s with $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$ (or $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle$, or $M = \langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$), then*

$$N_M = {}_{R^{\mathrm{env}}}\langle\ \{\boldsymbol{f_i} \otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(\epsilon_j,k)}} \otimes \mathbf{1} - \mathbf{1} \otimes \boldsymbol{x^{(\epsilon_j,k)}}\}_{1 \leq j \leq n,\ 1 \leq k \leq s}\ \rangle.$$

2.5.1 Computing two-sided Gröbner bases

Let $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ and $\preceq$ an admissible order on $\mathbb{N}^{n,(s)}$. As an alternative to the Right Closure Method (Algorithm 5) for computing two-sided Gröbner bases for R-subbimodules of R^s, we propose a new algorithm which improves the former, since it calls only once the left Buchberger algorithm (Algorithm 4), although it uses more variables and input elements.
Our method, first devised in the context of two-sided ideals ([24]) and afterwards generalized to bimodules ([30]), arises from the technique described in Section 2.5 for handling bimodules. More precisely, following the diagram (2.10), it consists of four steps:

1. Let $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t} \rangle_R$ be an R-subbimodule of R^s;
2. Consider the left R^{env}-submodule

   $$N_M = {}_{R^{\mathrm{env}}}\langle\ \{\boldsymbol{f_i} \otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(\epsilon_j,k)}} \otimes \mathbf{1} - \mathbf{1} \otimes \boldsymbol{x^{(\epsilon_j,k)}}\}_{1 \leq j \leq n,\ 1 \leq k \leq s}\ \rangle$$

   of $(R^{\mathrm{env}})^s$;
3. Using the left Buchberger algorithm (Algorithm 4) in the free module $(R^{\mathrm{env}})^s$, compute a left Gröbner basis G' for N_M;
4. Using the epimorphism of left R^{env}-modules $\mathfrak{m}^s$, obtain a two-sided Gröbner basis $G \subseteq R^s$ for M.

Note that with the results given so far, the first three steps can be carried out algorithmically. Let us show the results which allow to perform the last step.

2.5.4 Lemma. *Let $R = k\{x_1, \ldots, x_n;\ Q;\ \preceq\}$ be a G-Algebra. Consider the order* TOP *(or* POT*) on both $\mathbb{N}^{n,(s)}$ (for the exponents of R^s) and $\mathbb{N}^{2n,(s)}$ (for the exponents of $(R^{\mathrm{env}})^s$) (see A.5.2 for a definition).*

- *Taking $\preceq^*$ or $\preceq^c$ on $\mathbb{N}^{2n}$ (for the exponents of R^{env}), if $\boldsymbol{h} \in (R^{\mathrm{env}})^s$ satisfies that $\exp_{(R^{\mathrm{env}})^s}(\boldsymbol{h}) = (\alpha, 0, i) \in \mathbb{N}^{2n,(s)}$, then $\boldsymbol{h} \notin \mathrm{Ker}\,(\mathrm{m}^s)$ and $\exp_{R^s}(\mathrm{m}^s(\boldsymbol{h})) = (\alpha, i)$;*
- *Taking $\preceq_*$ or $\preceq_c$ on $\mathbb{N}^{2n}$ (for the exponents of R^{env}), if $\boldsymbol{h} \in (R^{\mathrm{env}})^s$ satisfies that $\exp_{(R^{\mathrm{env}})^s}(\boldsymbol{h}) = (0, \alpha, i) \in \mathbb{N}^{2n,(s)}$, then $\boldsymbol{h} \notin \mathrm{Ker}\,(\mathrm{m}^s)$ and $\exp_{R^s}(\mathrm{m}^s(\boldsymbol{h})) = (\alpha^{\mathrm{op}}, i)$.*

Proof. Let us prove the first statement. Suppose that $\boldsymbol{h} \in (R^{\mathrm{env}})^s$ has $((\alpha, 0), i)$ as exponent for some $\alpha \in \mathbb{N}^n$ and $i \in \{1, \ldots, s\}$, or equivalently, that $\boldsymbol{h}$ admits a representation

$$\boldsymbol{h} = \lambda(\boldsymbol{x}^{(\boldsymbol{\alpha},\boldsymbol{i})} \otimes \mathbf{1}) + \sum_{(\beta,\gamma,j) \prec (\alpha,0,i)} \lambda_{(\beta\gamma j)}\, \boldsymbol{x}^{(\boldsymbol{\beta},\boldsymbol{j})} \otimes \boldsymbol{x}^{(\boldsymbol{\gamma^{\mathrm{op}}},\boldsymbol{j})}. \tag{2.14}$$

There are four cases depending on the order taken for R^{env} and for $(R^{\mathrm{env}})^s$:

1. If we consider $\preceq^*$ on $\mathbb{N}^{2n}$ (for the exponents of R^{env}), then
   (a) If we take TOP for the exponents of $(R^{\mathrm{env}})^s$, then $(\beta, \gamma, j) \prec_{TOP} (\alpha, 0, i)$ implies either $\gamma = 0$ and $\beta \prec \alpha$, or $\gamma = 0$, $\beta = \alpha$ and $j > i$. Both cases lead us to $(\beta, j) \prec_{TOP} (\alpha, i)$ when TOP in considered for R^s. Hence,
   $$\mathrm{m}^s(\boldsymbol{h}) = \lambda\, \boldsymbol{x}^{(\boldsymbol{\alpha},\boldsymbol{i})} + \sum_{(\beta,j) \prec_{TOP} (\alpha,i)} \lambda_{(\beta 0 j)}\, \boldsymbol{x}^{(\boldsymbol{\beta},\boldsymbol{j})}.$$
   Therefore, $\exp_{R^s}(\mathrm{m}^s(\boldsymbol{h})) = (\alpha, i)$ and $\mathrm{m}^s(\boldsymbol{h}) \neq \mathbf{0}$.
   (b) If we consider POT for the exponents of $(R^{\mathrm{env}})^s$, then $(\beta, \gamma, j) \prec_{POT} (\alpha, 0, i)$ implies either $j > i$ or $j = i$ and $\gamma = 0$ and $\beta \prec \alpha$. Depending on these possibilities, by Eq. (2.14) and property 2.3.6, we can write
   $$\begin{aligned}\mathrm{m}^s(\boldsymbol{h}) &= \lambda\, \boldsymbol{x}^{(\boldsymbol{\alpha},\boldsymbol{i})} + \sum_{(\beta,\gamma,j);\, j>i} \lambda_{(\beta\gamma j)}\, x^{\beta} \boldsymbol{x}^{(\boldsymbol{\gamma^{\mathrm{op}}},\boldsymbol{j})} + \sum_{(\beta,0,i);\, \beta \prec \alpha} \lambda_{(\beta 0 i)}\, \boldsymbol{x}^{(\boldsymbol{\beta},\boldsymbol{i})} \\ &= \lambda\, \boldsymbol{x}^{(\boldsymbol{\alpha},\boldsymbol{i})} + \sum_{(\beta+\gamma^{\mathrm{op}},j) \prec_{POT} (\alpha,i)} \lambda_{(\beta\gamma j)}\, (q_{\beta\gamma^{\mathrm{op}}} \boldsymbol{x}^{(\boldsymbol{\beta+\gamma^{\mathrm{op}}},\boldsymbol{j})} + p_{\beta\gamma^{\mathrm{op}}} \boldsymbol{e_j}) \\ &\quad + \sum_{(\beta,i) \prec_{POT} (\alpha,i)} \lambda_{(\beta 0 i)}\, \boldsymbol{x}^{(\boldsymbol{\beta},\boldsymbol{i})}\end{aligned}$$

where $\exp_{R^s}(p_{\beta\gamma^{\mathrm{op}}}\boldsymbol{e_j}) \prec_{POT} (\beta+\gamma^{\mathrm{op}}, j)$. Hence, $\exp_{R^s}(\mathrm{m}^s(\boldsymbol{h})) = (\alpha, i)$ and $\mathrm{m}^s(\boldsymbol{h}) \neq \mathbf{0}$.

2. If, instead, we consider $\preceq^c$ on $\mathbb{N}^{2n}$ (for the exponents of R^{env}), then

   (a) For the order TOP for the exponents of $(R^{\mathrm{env}})^s$, the inequality $(\beta,\gamma,j) \prec_{TOP} (\alpha,0,i)$ implies either $\beta+\gamma^{\mathrm{op}} \prec \alpha$ or $\beta=\alpha$, $\gamma=0$ and $j>i$. Therefore, by virtue of Equation (2.14) and property 2.3.6,

$$\begin{aligned}\mathrm{m}^s(\boldsymbol{h}) &= \lambda\,\boldsymbol{x^{(\alpha,i)}} + \sum_{(\beta,\gamma,j);\,\beta+\gamma^{\mathrm{op}}\prec\alpha} \lambda_{(\beta\gamma j)}\, x^{\beta}\boldsymbol{x^{(\gamma^{\mathrm{op}},j)}} + \sum_{(\alpha,0,j);\,j>i} \lambda_{(\alpha 0 j)}\,\boldsymbol{x^{(\alpha,}}\\ &= \lambda\,\boldsymbol{x^{(\alpha,i)}} + \sum_{(\beta+\gamma^{\mathrm{op}},j)\prec_{TOP}(\alpha,i)} \lambda_{(\beta\gamma j)}\,(q_{\beta\gamma^{\mathrm{op}}}\boldsymbol{x^{(\beta+\gamma^{\mathrm{op}},j)}} + p_{\beta\gamma^{\mathrm{op}}}\boldsymbol{e_j})\\ &\quad + \sum_{(\alpha,j)\prec_{TOP}(\alpha,i)} \lambda_{(\alpha 0 j)}\,\boldsymbol{x^{(\alpha,j)}}\end{aligned}$$

   and $\exp_{R^s}(p_{\beta\gamma^{\mathrm{op}}}\boldsymbol{e_j}) \prec_{TOP} (\beta+\gamma^{\mathrm{op}}, j)$. Then, $\exp_{R^s}(\mathrm{m}^s(\boldsymbol{h})) = (\alpha, i)$ and $\mathrm{m}^s(\boldsymbol{h}) \neq \mathbf{0}$.

   (b) If we take POT for the exponents of $(R^{\mathrm{env}})^s$, then $(\beta,\gamma,j) \prec_{POT} (\alpha,0,i)$ implies either $j>i$ or $j=i$ and $\beta+\gamma^{\mathrm{op}}=0$. This is equivalent to $(\beta+\gamma^{\mathrm{op}}, j) \prec_{POT} (\alpha, i)$. Therefore,

$$\mathrm{m}^s(\boldsymbol{h}) = \lambda\,\boldsymbol{x^{(\alpha,i)}} + \sum_{(\beta+\gamma^{\mathrm{op}},j)\prec_{POT}(\alpha,i)} \lambda_{(\beta\gamma j)}\,(q_{\beta\gamma^{\mathrm{op}}}\boldsymbol{x^{(\beta+\gamma^{\mathrm{op}},j)}} + p_{\beta\gamma^{\mathrm{op}}}\boldsymbol{e_j})$$

   with $\exp_{R^s}(p_{\beta\gamma^{\mathrm{op}}}\boldsymbol{e_j}) \prec_{POT} (\beta+\gamma^{\mathrm{op}}, j)$. So, $\exp_{R^s}(\mathrm{m}^s(\boldsymbol{h})) = (\alpha, i)$ and $\mathrm{m}^s(\boldsymbol{h}) \neq \mathbf{0}$.

The second statement of 2.5.4 can be proved analogously, starting from a representation of the type

$$\boldsymbol{h} = \lambda(\mathbf{1}\otimes\boldsymbol{x^{(\alpha^{\mathrm{op}},i)}}) + \sum_{(\beta,\gamma,j)\prec(0,\alpha,i)} \lambda_{(\beta\gamma j)}\,\boldsymbol{x^{(\beta,j)}}\otimes\boldsymbol{x^{(\gamma^{\mathrm{op}},j)}}$$

in $(R^{\mathrm{env}})^s$. □

The connection between left Gröbner bases of $(R^{\mathrm{env}})^s$ and two-sided Gröbner bases of R^s is given by the following result.

2.5.5 Theorem. *Let $R = k\{x_1,\ldots,x_n; Q, \preceq\}$ be a G-Algebra. Let $M \subseteq R^s$ be an R-bimodule and consider in R^{env} the G-Algebra structure given in Proposition 2.2.8 (where the order is one amongst $\preceq^*$, $\preceq^c$, $\preceq_*$ and $\preceq_c$).*

If G is a left Gröbner basis for $N_M = (\mathfrak{m}^s)^{-1}(M)$ with TOP *(resp.* POT*) on $\mathbb{N}^{2n,(s)}$, then the set $\mathfrak{m}^s(G) \setminus \{\mathbf{0}\}$ is a two-sided Gröbner basis for M with* TOP *(resp.* POT*) on $\mathbb{N}^{n,(s)}$.*

Proof. Let $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_t}\} \subseteq (R^{\text{env}})^s$ be a left Gröbner basis for N_M. Suppose that $G \cap \text{Ker}\,(\mathfrak{m}^s) = \{\boldsymbol{g_{r+1}}, \ldots, \boldsymbol{g_t}\}$, that is,

$$\mathfrak{m}^s(G) \setminus \{\mathbf{0}\} = \{\mathfrak{m}^s(\boldsymbol{g_1}), \ldots, \mathfrak{m}^s(\boldsymbol{g_r})\} \subseteq M \setminus \{\mathbf{0}\}.$$

Let us see that

$$\text{Exp}\,(M) = \bigcup_{i=1}^{r} \exp_{R^s}(\mathfrak{m}^s(\boldsymbol{g_i})) + \mathbb{N}^n.$$

The inclusion $\text{Exp}\,(M) \supseteq \bigcup_{i=1}^{r} \exp_{R^s}(\mathfrak{m}^s(\boldsymbol{g_i})) + \mathbb{N}^n$ is obvious. Let $\boldsymbol{f} \in M \setminus \{0\}$, with standard representation

$$\boldsymbol{f} = \lambda \boldsymbol{x^{(\alpha,i)}} + \sum_{(\beta,j) \prec (\alpha,i)} \lambda_{(\beta,j)} \boldsymbol{x^{(\beta,j)}}.$$

We distinguish two cases:

1. The order in the G-Algebra R^{env} is either $\preceq^*$ or $\preceq^c$. In this case we have
$$\boldsymbol{f} \otimes \mathbf{1} = \lambda \boldsymbol{x^{(\alpha,i)}} \otimes \mathbf{1} + \sum_{(\beta,j) \prec (\alpha,i)} \lambda_{(\beta,j)} \boldsymbol{x^{(\beta,j)}} \otimes \mathbf{1}.$$
Since $(\beta, j) \prec_{TOP} (\alpha, i)$, resp. $(\beta, j) \prec_{POT} (\alpha, i)$, implies $(\beta, 0, j) \prec_{TOP} (\alpha, 0, i)$, resp. $(\beta, 0, j) \prec_{POT} (\alpha, 0, i)$, it follows that
$$\exp_{(R^{\text{env}})^s}(\boldsymbol{f} \otimes \mathbf{1}) = (\alpha, 0, i) \in \mathbb{N}^{2n,(s)}. \tag{2.15}$$
Besides, as $\boldsymbol{f} \otimes \mathbf{1} \in N_M$ and G is a Gröbner basis for N_M, from the statement 4 of 2.3.14,
$$\boldsymbol{f} \otimes \mathbf{1} = \sum_{i=1}^{t} p_i \boldsymbol{g_i},$$
with $p_i \in R^{\text{env}}$, and $\exp_{(R^{\text{env}})^s}(\boldsymbol{f} \otimes \mathbf{1}) = \exp_{R^{\text{env}}}(p_k) + \exp_{(R^{\text{env}})^s}(\boldsymbol{g_k})$ for some $1 \leq k \leq t$. Therefore, if we denote by $(\beta, \beta') \in \mathbb{N}^{2n}$ the exponent of p_k and by $(\gamma, \gamma', j) \in \mathbb{N}^{2n,(s)}$ the exponent of $\boldsymbol{g_k}$, from Equation (2.15) we obtain
$$(\alpha, 0, i) = (\gamma, \gamma', j) + (\beta, \beta') = (\beta + \gamma, \beta' + \gamma', j). \tag{2.16}$$
So, $j = i$, $\beta' = \gamma' = 0$ and $\alpha = \beta + \gamma$. Hence,
$$\exp_{(R^{\text{env}})^s}(\boldsymbol{g_k}) = (\gamma, 0, i),$$

and by virtue of 2.5.4, $\mathrm{m}^s(\boldsymbol{g_k}) \neq \mathbf{0}$ (so, $k \in \{1, \ldots, r\}$), and

$$\exp_{R^s}(\mathrm{m}^s(\boldsymbol{g_k})) = (\gamma, i).$$

Taking up the proof in Equation (2.16) again, we conclude that

$$\exp_{R^s}(\boldsymbol{f}) = (\alpha, i) = (\gamma, i) + \beta = \exp_{R^s}(\mathrm{m}^s(\boldsymbol{g_k})) + \beta,$$

that is, $\exp_{R^s}(\boldsymbol{f}) \in \bigcup_{i=1}^{r} \exp_{R^s}(\mathrm{m}^s(\boldsymbol{g_i})) + \mathbb{N}^n$.

2. The order in R^{env} is either $\preceq_*$ or $\preceq_c$. Then the exponent of the element

$$\mathbf{1} \otimes \boldsymbol{f} = \lambda \mathbf{1} \otimes \boldsymbol{x^{(\alpha,i)}} + \sum_{(\beta,j) \prec (\alpha,i)} \lambda_{(\beta,j)} \mathbf{1} \otimes \boldsymbol{x^{(\beta,j)}}$$

is $(0, \alpha^{\mathrm{op}}, i) \in \mathbb{N}^{2n,(s)}$. Indeed, for any of the orders TOP and POT on $\mathbb{N}^{n,(s)}$, $(\beta, j) \prec (\alpha, i)$ implies $(0, \beta^{\mathrm{op}}, j) \prec (0, \alpha^{\mathrm{op}}, i)$. On the other hand, as $\mathbf{1} \otimes \boldsymbol{f} \in N_M$,

$$\mathbf{1} \otimes \boldsymbol{f} = \sum_{i=1}^{t} p_i \boldsymbol{g_i},$$

with $p_i \in R^{\mathrm{env}}$, and $\exp_{(R^{\mathrm{env}})^s}(\boldsymbol{f} \otimes \mathbf{1}) = \exp_{R^{\mathrm{env}}}(p_k) + \exp_{(R^{\mathrm{env}})^s}(\boldsymbol{g_k})$ for some $1 \leq k \leq t$. Therefore,

$$(0, \alpha^{\mathrm{op}}, i) = (\beta + \gamma, \beta' + \gamma', j).$$

where $(\beta, \beta') = \exp_{R^{\mathrm{env}}}(p_k)$ and $(\gamma, \gamma', j) = \exp_{(R^{\mathrm{env}})^s}(\boldsymbol{g_k})$. Hence,

$$\exp_{(R^{\mathrm{env}})^s}(\boldsymbol{g_k}) = (0, \gamma', i),$$

and from 2.5.4 it follows that $\mathrm{m}^s(\boldsymbol{g_k}) \neq \mathbf{0}$ (so, $k \in \{1, \ldots, r\}$), and

$$\exp_{R^s}(\mathrm{m}^s(\boldsymbol{g_k})) = (\gamma'^{\mathrm{op}}, i).$$

Therefore,

$$\exp_{R^s}(\boldsymbol{f}) = (\alpha, i) = (\gamma'^{\mathrm{op}}, i) + \beta'^{\mathrm{op}} = \exp_{R^s}(\mathrm{m}^s(\boldsymbol{g_k})) + \beta'^{\mathrm{op}},$$

and $\exp_{R^s}(\boldsymbol{f}) \in \bigcup_{i=1}^{r} \exp_{R^s}(\mathrm{m}^s(\boldsymbol{g_i})) + \mathbb{N}^n$.

□

Theorem 2.5.5 together with the previous results in this section provides an algorithm for computing two-sided Gröbner bases for bimodules (see Algorithm 10).

Algorithm 10 Two-sided Gröbner bases (alternative)

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\} \subseteq R^s \setminus \{0\}$;
Ensure: $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$, a two-sided Gröbner basis for ${}_R\langle F\rangle_R$ such that $F \subseteq G$;

Initialization: $B := \{\boldsymbol{f_i} \otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(\epsilon_j,k)}} \otimes 1 - 1 \otimes \boldsymbol{x^{(\epsilon_j,k)}}\}_{1\leq j\leq n,\ 1\leq k\leq s}$;
Using the left Buchberger algorithm 4, compute a left Gröbner basis G' in the free module $(R^{\mathrm{env}})^s$ for the input data B;
If $G' = \{\boldsymbol{g'_1}, \ldots, \boldsymbol{g'_{t'}}\}$ with $\boldsymbol{g'_i} = (\sum_{j\in\mathfrak{I}_i} p_{ij}^1 \otimes q_{ij}^1, \ldots, \sum_{j\in\mathfrak{I}_i} p_{ij}^s \otimes q_{ij}^s)$, take $\boldsymbol{g_i} := (\sum_{j\in\mathfrak{I}_i} p_{ij}^1 q_{ij}^1, \ldots, \sum_{j\in\mathfrak{I}_i} p_{ij}^s q_{ij}^s)$;
$G := \emptyset$;
for all $i = 1$ to t' **do**
  if $\boldsymbol{g_i} \neq 0$ **then**
    $G := G \cup \{\boldsymbol{g_i}\}$;
  end if
end for
Return G.

The advantage of this algorithm over the Right Closure Method is that only one call to the left Buchberger algorithm is done, whereas the Right Closure Method (Algorithm 5) makes an, a priori, unknown number of calls.

Next, a comparison between both algorithms is discussed on some explicit examples. The computations of these examples, as well as all examples in this chapter, were obtained by using a library of procedures we have implemented in the language of the package of symbolic computation Maple 6 (see [32]). The Right Closure algorithm, which we collect in Algorithm 5 (just as it appears in [54] for two-sided ideals or in [13] for bimodules over *PBW algebras*), was also coded in this library in order to compare the outputs and the computation times with those of Algorithm 10.

In the examples, computation times correspond to a Pentium III 700 MHz personal computer with 176 Mb RAM.

2.5.6 Example. Let R be the Quantum plane, i.e., $R = \mathbb{C}\{x, y;\ \{yx - qxy\},\ \preceq_{(1,3)}\}$, where $\preceq_{(1,3)}$ is the $(1,3)$-weighted lexicographical order defined from $\preceq_{lex}$ with $\epsilon_1 \prec_{lex} \epsilon_2$, and put $q = i$. Let $F = \{(2x, x^2y, xy^2 + y^2), (xy, 0, -x^2y^2), (x^2, 2, 0)\} \subset R^3$ and consider the order TOP for the exponents of R^3.

The Right Closure algorithm calls the left Buchberger algorithm twice and takes 56.6 seconds to compute a (non-reduced) two-sided Gröbner basis G_1

Module	Size of reduced	Right Closure Method			Algorithm 10		
		Size	Time	Red. time	Size	Time	Red. tim
$\mathbb{C}_q[x,y]^3$	4	17	56.6	22.7	12	**43.0**	13.0
$M_q(2)^2$	8	28	167.6	101.5	17	**37.9**	9.8
$\mathfrak{D}$	6	38	1907.5	709.6	14	**93.7**	53.1
$U(\mathfrak{sl}(2))$	10	29	735.2	487.1	11	**113.8**	58.7
$U(\mathfrak{g}_2)$	14	88	24176.9	12583.0	46	**13522.1**	3728.7

Table 2.1: Comparison between Algorithm 5 and Algorithm 10

consisting of 17 elements.
Algorithm 10 takes 43.0 seconds to compute a (non-reduced) two-sided Gröbner basis G_2 with 12 elements.
After reducing G_1 or G_2, we obtain the reduced two-sided Gröbner basis

$$\{(x^2,0,0),\ (2x,0,y^2),\ (xy,0,0),\ (0,1,0)\}$$

of ${}_R\langle F\rangle_R$. The reduction of G_1 takes 22.7 seconds whereas the reduction of G_2 takes 13.0 seconds.

2.5.7 Example. Now consider the algebra $M_q(2) = \mathbb{C}\{x,y,z,t;Q,\preceq_{deglex}\}$ of Quantum matrices (see 2.2) where $\preceq_{deglex}$ is the degree lexicographical order with $\epsilon_1 \prec_{deglex} \cdots \prec_{deglex} \epsilon_4$, and $Q = \{yx-qxy, ty-qyt, zx-qxz, tz-qzt, zy-yz, tx-xt-(q^{-1}-q)yz\}$. Put again $q=i$, and consider the order "POT" for the exponents of R^2. Let $F = \{(-xzt+y, 2xy^3z), (x^2zt, y^2)\} \subset R^2$.
The Right Closure algorithm computes a two-sided Gröbner basis G_1 consisting of 28 elements in 167.6 seconds, calling the left Buchberger algorithm twice.
Algorithm 10 takes 37.9 seconds to compute a two-sided Gröbner basis G_2 with 17 elements. The reduction of G_1 takes 101.5 seconds whilst the reduction of G_2 takes 9.8 seconds. The reduced two-sided Gröbner basis for ${}_R\langle F\rangle_R$ is

$$\{\ (xzt-y,0),\ (xy,y^2),\ (0,y^3),\ (0,y^2z),\ (yz^2t,0),\ (0,y^2t),\ (y^2,0),\ (0,xy^2)\}.$$

Table 2.1 shows a comparison between both algorithms for the previous and some other explicit examples. The first column represents the free module where the computations are performed and the second represents the size of the reduced two-sided Gröbner basis for the corresponding example. For both algorithms, the column "Time" [1] represents the elapsed time to compute a

[1]The computation times shown in Table 2.1 correspond to a Pentium III 700 MHz personal computer with 176 Mb RAM.

(not necessarily reduced) two-sided Gröbner basis, and its number of elements is shown in the column "Size". We also give the time taken in addition to reduce the basis.

• The first two rows gather the times and sizes of the examples described above.

• The third row represents the computation of two-sided Gröbner bases in the *Diamond algebra* (see 2.2) $\mathfrak{D} = \mathbb{C}\{x, y, z, t;\ Q, \preceq_{lex}\}$ where $\preceq_{lex}$ is the lexicographical order with $\epsilon_1 \prec_{lex} \ldots \prec_{lex} \epsilon_4$ and $Q = \{yx - xy, zx - xz, tx - xt, zy - yz + x, ty - yt + y, tz - zt - z\}$. The input data is $F = \{4x^2t + 5x^2y, 8z^3t + 9yz\}$. In this case, the Right Closure algorithm makes 3 calls to the left Buchberger algorithm in order to compute a two-sided Gröbner basis.

• The fourth row is concerned with the example `AnnFD-sl2-2` (see [62]), consisting in computing a two-sided Gröbner basis in the universal enveloping algebra of traceless 2×2-matrices $U(\mathfrak{sl}(2)) = \mathsf{k}\{e, f, h; Q, \preceq_{deglex}\}$, where $Q = \{fe - ef + h, he - eh - 2e, hy - yh + 2f\}$. The input data is $F = \{e^3, f^3, (h-2)h(h+2)\}$.

• The last row of the table represents the results for the example `TwoGB-g2-2` described in [62]. It consists in computing a two-sided Gröbner basis for the ideal generated by the square of the element x_1 of the algebra $U(\mathfrak{g}_2)$, which is generated by 14 elements[2]. Here we use the degree lexicographical order $\preceq_{deglex}$ on $\mathbb{N}^{14}$.

2.6 Syzygy bimodule and some applications

The notion of *syzygy bimodule*, first introduced by Mora for homogeneous two-sided ideals in the context of non-commutative graded structures ([71]), and then, independently, by the authors ([27, 30]) for not necessarily homogeneous bimodules over a G-Algebra, can be viewed as the two-sided counterpart of the left syzygy module (or the syzygy module in commutative polynomial rings), since it presents some similar properties and applications.

In this section we will see that syzygy bimodules can be computed in the context of G-Algebras. More precisely, following the method for handling bimodules described in 2.5, we construct an algorithm for computing the syzygy bimodule of any finite subset F of a free module R^s over a G-Algebra R.

[2]See `http://www.singular.uni-kl.de/plural/DEMOS/Leipzig/Applications/G2/index.html` for a definition of $U(\mathfrak{g}_2)$ and a complete description of this example.

Likewise, we shall show that syzygy bimodules reveal to be useful in solving some computational problems when, as natural, two-sided input data are given. Amongst these problems there are: computation of finite intersections of subbimodules of R^s, presentations and free resolutions of subbimodules of R^s, two-sided division ideals of R, etc. (we presented some of these applications in [30, 27]).

Moreover, in case the bimodules are generated by elements of the *centralizer*, some of these results are enhanced and many computations can be simplified (e.g., the computation of two-sided division ideals). These particular cases are gathered at the end of the section.

We start recalling from [13] the notion of left syzyzy module and an algorithm to compute it.

2.6.1 Definition. Let R be a ring, S a left R-module, and $\{f_1, \ldots, f_t\} \subseteq S$. The *left syzygy module* of the matrix

$$F = \begin{bmatrix} f_1 \\ \vdots \\ f_t \end{bmatrix} \in M_{t\times 1}(S),$$

denoted by $Syz^l(F)$, or equivalently by $Syz^l(f_1, \ldots, f_t)$, is the kernel of the homomorphism of left R-modules $R^t \to S$; $(r_1, \ldots, r_t) \mapsto \sum_{i=1}^{t} r_i f_i$.

Note that the previous morphism surjects onto the left R-module ${}_R\langle f_1, \ldots, f_t\rangle$, and therefore,

$$R^t/Syz^l(F) \;\cong\; {}_R\langle f_1, \ldots, f_t\rangle \;\text{ as left } R\text{−modules.}$$

When R is the commutative polynomial ring it is possible to compute $Syz^l(F)$ for any finite set $F \subseteq R^s$ (see, e.g., [46, Alg. 2.5.4]. In [13] one can find another algorithm which computes a set of generators of $Syz^l(F)$ when R is a G-Algebra (even, when R is a left PBW ring), provided that a finite set of input data $F \subset R^s$ is given (note that in this algorithm (see [13, Ch. 5, Th. 2.3]), the rows r_i's of the matrix $I_s - PQ$ are not necessary when a Gröbner basis G for ${}_R\langle F\rangle$ contains the set F, as is highlighted in [13, Exercise 5.1]). This algorithm is shown below as Algorithm 11, and will be used within Algorithm 12.

Regarding once again R^s as a left R^{env}-module, we propose the following definition of *syzygy bimodule*.

Algorithm 11 Left Syzygy Module

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\} \subseteq R^s \setminus \{0\}$;
Ensure: H, a finite generator system of $Syz^l(F)$ as a left R-module;

Initialization: Run the left Buchberger algorithm for the input data F in order to compute:
- a left Gröbner basis $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$ for ${}_R\langle F\rangle$ such that $F \subseteq G$,
- the elements $h_{ij}^k \in R$ such that $SP(\boldsymbol{g_i}, \boldsymbol{g_j}) = \sum_{k=1}^{r} h_{ij}^k \boldsymbol{g_k}$ for all $1 \leq i < j \leq r$, and
- the matrix $Q \in M_{r\times t}(R)$ such that $(\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}) = (\boldsymbol{f_1}, \ldots, \boldsymbol{f_t})Q^t$;

for all $1 \leq i < j \leq r$ **do**
  if level $(\boldsymbol{g_i})$ = level $(\boldsymbol{g_j})$ **then**
    Compute r_{ij}, r_{ji} such that $SP(\boldsymbol{g_i}, \boldsymbol{g_j}) = r_{ij}\boldsymbol{g_i} - r_{ji}\boldsymbol{g_j}$;
    Let $\boldsymbol{p_{ij}} := (0, \ldots, \overset{i}{r_{ij}}, \ldots, 0) - (0, \ldots, \overset{j}{r_{ji}}, \ldots, 0) - (h_{ij}^1, \ldots, h_{ij}^r)$;
  end if
end for

Let $H := \{\boldsymbol{p_{ij}}Q \;/\; 1 \leq i < j \leq r,\ \text{level}\,(\exp\,(\boldsymbol{g_i})) = \text{level}\,(\exp\,(\boldsymbol{g_j}))\}$;
Return H.

2.6.2 Definition. Let R be a k-algebra, S an R-bimodule and $\{f_1, \ldots, f_t\} \subseteq S$. The *syzygy bimodule* of the matrix

$$F = \begin{bmatrix} f_1 \\ \vdots \\ f_t \end{bmatrix} \in M_{t\times 1}(S),$$

denoted by $Syz(F)$ or $Syz(f_1, \ldots, f_t)$, is the kernel of the homomorphism of left R^{env}-modules

$$\begin{aligned} (R^{\text{env}})^t &\longrightarrow S \\ (h_1, \ldots, h_t) &\longmapsto \sum_{i=1}^{t} h_i f_i. \end{aligned}$$

In the previous definition, since the R-bimodules are exactly the left R^{env}-modules,

$$(R^{\text{env}})^t / Syz(F) \;\cong\; {}_R\langle f_1, \ldots, f_t\rangle_R \;\text{ as } R\text{–bimodules.}$$

Likewise, note that

$$Syz^l(F) \subseteq \mathfrak{m}^s(Syz(F)). \tag{2.17}$$

Indeed, for all $\boldsymbol{g} = (g_1, \ldots, g_t) \in Syz^l(f_1, \ldots, f_t)$,

$$\sum_{i=1}^{t} (g_i \otimes 1) f_i = \sum_{i=1}^{t} g_i f_i = 0.$$

Hence, $\boldsymbol{g} = \mathfrak{m}^s(\boldsymbol{g} \otimes \mathbf{1})$, with $\boldsymbol{g} \otimes \mathbf{1} \in Syz(f_1, \ldots, f_t)$. In 2.6.24 we will study the syzygy bimodule in some situations where inclusion (2.17) becomes an equality.

2.6.3 Note. After having defined syzygy bimodules, a natural question arises: since R-bimodules are also right $(R^{\text{env}})^{\text{op}}$-modules, where $(R^{\text{env}})^{\text{op}} = R^{\text{op}} \otimes_{\mathsf{k}} R$, why did we not define the syzygy bimodule of a set $F = \{f_1, \ldots, f_t\} \subseteq S$ as the kernel of the homomorphism of right $(R^{\text{env}})^{\text{op}}$-modules $((R^{\text{env}})^{\text{op}})^t \to S$, $(h_1, \ldots, h_t) \mapsto \sum_{i=1}^{t} f_i * h_i$ [3]?. The answer is that in both cases we obtain the same bimodule for $Syz(F)$ because $f * h = hf$ for all $h \in R^{\text{env}}$ and $f \in S$.

If $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ is a G-Algebra, we can compute the syzygy bimodule of a matrix $F \in M_{t\times 1}(R^s)$ by using again the technique of Section 2.5, that is, we can move the problem to the context of the enveloping algebra in order to use methods on the left side. Following the diagram (2.10), the method consists of the following steps:

1. The syzygy bimodule $Syz(F)$ of a set $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\} \subseteq R^s$ is required;

2. State the problem of computing the left syzygy module $Syz^l(G)$ of the set

$$G = \{\boldsymbol{f_i} \otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(\epsilon_j, k)}} \otimes 1 - \mathbf{1} \otimes \boldsymbol{x^{(\epsilon_j, k)}}\}_{1\leq j\leq n,\ 1\leq k\leq s} \subseteq (R^{\text{env}})^s;$$

3. Using the Left Syzygy Module Algorithm (Algorithm 11) in the free module $(R^{\text{env}})^s$, compute a set of generators H of $Syz^l(G)$ as a left R^{env}-module;

4. Using the morphism $\mathfrak{m}^s$, obtain a set of generators of $Syz(F)$ as an R-bimodule.

The following result shows that the last step can be carried out computationally. As a consequence, we devise Algorithm 12.

[3] The symbol $*$ denotes the right multiplication of $S \in \text{Mod-}(R^{\text{env}})^{\text{op}}$, given by $f \cdot (r \otimes r') = rfr'$.

2.6.4 Proposition. *Let $R = k\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra and $\{\boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\} \subseteq R^s$. If $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\} \subset (R^{\mathrm{env}})^{t+sn}$ is a generator system of*

$$Syz^l(\ \{\boldsymbol{f_i} \otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(\epsilon_j,k)}} \otimes \mathbf{1} - \mathbf{1} \otimes \boldsymbol{x^{(\epsilon_j,k)}}\}_{1\leq j\leq n,\ 1\leq k\leq s}\ )$$

as a left R^{env}-module, then

$$Syz(\boldsymbol{f_1}, \ldots, \boldsymbol{f_t}) = {}_R\langle \boldsymbol{h_1}', \ldots, \boldsymbol{h_r}' \rangle_R,$$

where $\boldsymbol{h_i} = (\boldsymbol{h_i}', \boldsymbol{h_i}'') \in (R^{\mathrm{env}})^t \times (R^{\mathrm{env}})^{sn}$, for all $1 \leq i \leq r$.

Proof. Note that for any $\boldsymbol{g} = (g_1, \ldots, g_t) \in Syz(\boldsymbol{f_1}, \ldots, \boldsymbol{f_t})$,

$$\sum_{i=1}^{t} g_i(\boldsymbol{f_i} \otimes \mathbf{1}) \in \mathrm{Ker}\ (\mathrm{m}^s).$$

Therefore, by 2.5.2, there exists $\boldsymbol{g'} = (g'_{11}, \ldots, g'_{1s}, \ldots, g'_{n1}, \ldots, g'_{sn}) \in (R^{\mathrm{env}})^{sn}$ such that

$$\sum_{i=1}^{t} g_i(\boldsymbol{f_i} \otimes \mathbf{1}) = \sum_{1\leq j\leq n;\ 1\leq k\leq s} g'_{jk}(\boldsymbol{x^{(\epsilon_j,k)}} \otimes \mathbf{1} - 1 \otimes \boldsymbol{x^{(\epsilon_j,k)}}).$$

Hence, $\boldsymbol{h} = (\boldsymbol{g}, -\boldsymbol{g'})$ is in $Syz^l(\{\boldsymbol{f_i}\otimes\mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(\epsilon_j,k)}}\otimes\mathbf{1}-\mathbf{1}\otimes\boldsymbol{x^{(\epsilon_j,k)}}\}_{1\leq j\leq n,\ 1\leq k\leq s})$. At this point, the proof may easily be finished. □

Algorithm 12 Syzygy Bimodule

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\} \subseteq R^s \setminus \{0\}$;
Ensure: H, a finite generator system of $Syz(F)$ as an R-bimodule;

Initialization: $B := \{\boldsymbol{f_i} \otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(\epsilon_j,k)}} \otimes 1 - 1 \otimes \boldsymbol{x^{(\epsilon_j,k)}}\}_{1\leq j\leq n,\ 1\leq k\leq s}$;

Using the Left Syzygy Module Algorithm (Algorithm 11), compute in $(R^{\mathrm{env}})^s$ a generator system $H = \{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\}$ of $Syz^l(B)$;

If $\boldsymbol{h_i} = (\boldsymbol{h_i}', \boldsymbol{h_i}'') \in (R^{\mathrm{env}})^t \times (R^{\mathrm{env}})^{sn}$ for $1 \leq i \leq r$, put
$H := \{\boldsymbol{h_1}', \ldots, \boldsymbol{h_r}'\}$.
Return H;

2.6.5 Example. Let R be the quantum plane $\mathbb{C}\{x, y;\ \{yx - qxy\}, \preceq_{(2,1)}\}$, with $q = i$, and consider the order POT for the exponents of R^2. Let $F = \{(x+1, y), (xy, 0)\} \subseteq R^2$.

Running Algorithm 12, which was implemented in the library of procedures [32], it takes 13.4 seconds to compute the R-bimodule generator system H of $Syz(F)$ consisting of 8 elements:

$$H = \{\ (1\otimes y - y\otimes 1, (-1+i)1\otimes 1),\ ((-\frac{1}{2}+\frac{i}{2})y\otimes x + (-\frac{1}{2}+\frac{i}{2})xy\otimes 1,$$
$$1\otimes x + 1\otimes 1),\ (0, 1\otimes y + iy\otimes 1),\ ((-\frac{1}{2}+\frac{i}{2})y\otimes x + (-\frac{1}{2}+\frac{i}{2})xy\otimes 1,$$
$$ix\otimes 1 + 1\otimes 1),\ ((-\frac{1}{2}-\frac{i}{2})y\otimes x + (-\frac{1}{2}-\frac{i}{2})xy\otimes 1, i\otimes x + i\otimes 1),$$
$$(-y\otimes y + y^2\otimes 1, i\otimes y - iy\otimes 1),\ ((\frac{1}{2}+\frac{i}{2})1\otimes x^2 - ix\otimes x +$$
$$((-\frac{1}{2}+\frac{i}{2})x^2\otimes 1, 0),\ (\frac{1}{2}+\frac{i}{2})1\otimes xy + (-\frac{1}{2}+\frac{i}{2})y\otimes x$$
$$+(-\frac{1}{2}-\frac{i}{2})x\otimes y + (\frac{1}{2}+\frac{i}{2})xy\otimes 1, 0)\ \}.$$

Although elimination techniques are useful at solving several problems in Module Theory (computation of intersections, quotient ideals, etc.), they appear to be computationally inefficient, mainly because elimination orders are unavoidably used.

It has been noted, first in the commutative case (cf. [1, page 171]) and then using left syzygy R-modules when R is a left PBW ring, and in particular a G-Algebra (cf. [13, page 203]), that syzygies provide a more efficient treatment, for example, in the computation of intersections of left R-submodules of R^s, ideal quotients, kernels of homomorphisms of left R-submodules, etc. In [14] a set of algorithms based on tag-variables and elimination is proposed for commutative polynomial rings, e.g., to compute division ideals (also called *colons*) and intersections. These algorithms, written in an elegant way, are broadly equivalent to algorithms based on syzygies.

In what follows, we will see that some of these applications of left syzygies can be generalized using the new definition of syzygy bimodules, so that, for example, we devise an algorithm to compute a finite intersection $\bigcap_{i=1}^{r} M_i$ of R-subbimodules of R^s when (as natural) a set of generators for each M_i as an R-bimodule is given. Though this problem in particular can be solved by the analogous method for computing the intersection of left R-modules [13] (computing a priori a two-sided Gröbner basis for each M_i in order to have left generators systems of each M_i), the advantage offered when syzygy bimodules are used is that we avoid the initial computations of two-sided Gröbner bases.

The following result states a general property for obtaining finite generator

systems for a left R-module N and its epimorphic image (under $\mathfrak{m}^s$) M when these modules are defined as truncated syzygy bimodules.

2.6.6 Lemma. *Let R be a k-algebra, S an R-bimodule, $p \geq 1$, and*

$$H = \left[\frac{H_1}{H_2}\right] \in M_{(s+p)\times 1}(S)$$

i.e. H is a matrix of size $(s+p)\times 1$ with entries in S, where

$$H_1 \in M_{s\times 1}(S), \quad H_2 \in M_{p\times 1}(S).$$

Consider the left R^{env}-module

$$N = \{\boldsymbol{h}' \in (R^{\mathrm{env}})^s \,/\, \exists\, \boldsymbol{h}'' \in (R^{\mathrm{env}})^p,\ (\boldsymbol{h}', \boldsymbol{h}'') \in Syz(H)\} \subseteq (R^{\mathrm{env}})^s,$$

and the R-bimodule $M = \mathfrak{m}^s(N)$ (see definition of $\mathfrak{m}^s$ in (2.11)), that is,

$$M = \{\boldsymbol{f} \in R^s \,/\, \exists\, (\boldsymbol{h}', \boldsymbol{h}'') \in Syz(H) \subseteq (R^{\mathrm{env}})^s \times (R^{\mathrm{env}})^p,\ f = \mathfrak{m}^s(\boldsymbol{h}')\} \subseteq R^s.$$

If $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_t}\} \subseteq (R^{\mathrm{env}})^{s+p}$ is a generator system of $Syz(H)$ as a left R^{env}-module, where $\boldsymbol{h_i} = (\boldsymbol{h_i}', \boldsymbol{h_i}'') \in (R^{\mathrm{env}})^s \times (R^{\mathrm{env}})^p$, then

$$N = {}_{R^{\mathrm{env}}}\langle \boldsymbol{h_1}', \ldots, \boldsymbol{h_t}' \rangle,$$

and

$$M = {}_R\langle \mathfrak{m}^s(\boldsymbol{h_1}'), \ldots, \mathfrak{m}^s(\boldsymbol{h_t}') \rangle_R.$$

Proof. Note that N actually is a left R^{env}-submodule of $(R^{\mathrm{env}})^s$, since $Syz(H) \in R^{\mathrm{env}}$-Mod. If $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_t}\}$ is a left generator system of $Syz(H)$ where $\boldsymbol{h_i} = (\boldsymbol{h_i}', \boldsymbol{h_i}'') \in (R^{\mathrm{env}})^s \times (R^{\mathrm{env}})^p$, then obviously, $\boldsymbol{h_i}' \in N$ for all $i \in \{1, \ldots, t\}$. Conversely, for every $\boldsymbol{h} \in N$, there exists $\boldsymbol{h}'' \in (R^{\mathrm{env}})^p$ such that $(\boldsymbol{h}, \boldsymbol{h}'') \in Syz(H)$. Hence,

$$(\boldsymbol{h}, \boldsymbol{h}'') = \sum_{i=1}^{t} p_i (\boldsymbol{h_i}', \boldsymbol{h_i}''),$$

for some $p_i \in R^{\mathrm{env}}$. Therefore, $\boldsymbol{h} = \sum_{i=1}^{t} p_i \boldsymbol{h_i}'$.
Finally, the image of the set of generators $\{\boldsymbol{h_1}', \ldots, \boldsymbol{h_t}'\}$ of N under the homomorphism $\mathfrak{m}^s$ of left R^{env}-modules becomes a set of generator of M as a left R^{env}-module, or equivalently, as an R-bimodule. □

When R is a G-Algebra, Lemma 2.6.6 applied in different situations provides algorithms to solve some problems (like computing intersection of R-bimodules, presentations, etc.) which we describe below. We can find in [13] analogous methods in the context of left PBW rings for solving each of these problems for left modules, using left syzygy modules instead of syzygy bimodules.

2.6.1 Finite intersection of subbimodules of R^s

2.6.7 Proposition. *Let R be a k-algebra, and let $\{M_i\}_{i=1}^r$ be a family of R-subbimodules of R^s. If $M_i = {}_R\langle \boldsymbol{f_1^i}, \ldots, \boldsymbol{f_{t_i}^i}\rangle_R$, then*

$$\bigcap_{i=1}^{r} M_i = \{\boldsymbol{f} \in R^s / \exists (\boldsymbol{h'}, \boldsymbol{h''}) \in Syz(H) \subseteq (R^{\mathrm{env}})^s \times (R^{\mathrm{env}})^{\sum_{j=1}^{r} t_j},\ \boldsymbol{f} = \mathrm{m}^s(\boldsymbol{h'})\},$$

where

$$H = \left[\frac{H_1}{H_2}\right] = \left[\begin{array}{ccc} I_s & \cdots & I_s \\ \hline \boldsymbol{f_1^1} & \cdots & \boldsymbol{0} \\ \vdots & & \vdots \\ \boldsymbol{f_{t_1}^1} & \cdots & \boldsymbol{0} \\ \vdots & & \vdots \\ \boldsymbol{0} & \cdots & \boldsymbol{f_1^r} \\ \vdots & & \vdots \\ \boldsymbol{0} & \cdots & \boldsymbol{f_{t_r}^r} \end{array}\right] \in M_{(s+\sum_{i=1}^{r} t_i)\times 1}(R^{rs}),$$

and $I_s \in M_{s\times s}(R)$ denotes the identity matrix of size $s \times s$ with entries in R.

Proof. If $\boldsymbol{f} \in \bigcap_{i=1}^r M_i$, then for all $i \in \{1, \ldots, r\}$ $\boldsymbol{f}$ can be written as $\boldsymbol{f} = \sum_{k=1}^{t_i} h_k^i \boldsymbol{f_k^i}$, with $h_k^i \in R^{\mathrm{env}}$, and one can easily check that

$$(\boldsymbol{f} \otimes \boldsymbol{1}, -h_1^1, \ldots, -h_{t_1}^1, \ldots, -h_1^r, \ldots, -h_{t_r}^r) \in Syz(H).$$

Conversely, if $(\boldsymbol{h'}, \boldsymbol{h''}) \in Syz(H)$ and $\boldsymbol{f} = \mathrm{m}^s(\boldsymbol{h'})$, then

$$\begin{aligned} 0 &= \boldsymbol{h'}H_1 + \boldsymbol{h''}H_2 \\ &= (\boldsymbol{f} \otimes \boldsymbol{1})H_1 + \boldsymbol{h''}H_2 \\ &= (\boldsymbol{f} + \sum_{k=1}^{t_1} h_k^1 \boldsymbol{f_k^1}), \ldots, \boldsymbol{f} + \sum_{k=r}^{t_r} h_k^r \boldsymbol{f_k^r}) \end{aligned}$$

where $\boldsymbol{h''} = (h_1^1, \ldots, h_{t_1}^1, \ldots, h_1^r, \ldots, h_{t_r}^r)$. Hence, $\boldsymbol{f} \in \bigcap_{i=1}^r M_i$. □

The following result is a direct consequence of 2.6.6 and 2.6.7.

2.6.8 Corollary. *Let R be a k-algebra and $\{M_i\}_{i=1}^r$ a family of R-subbimodules of R^s with $M_i = {}_R\langle \boldsymbol{f_1^i}, \ldots, \boldsymbol{f_{t_i}^i}\rangle_R$. Consider the matrix H as in 2.6.7. If $Syz(H) = {}_R\langle \boldsymbol{g_1}, \ldots, \boldsymbol{g_t}\rangle_R$ with $\boldsymbol{g_k} = (\boldsymbol{g_k}', \boldsymbol{g_k}'') \in (R^{\mathrm{env}})^s \times (R^{\mathrm{env}})^{\sum_{j=1}^{r} t_j}$ for all $1 \le k \le t$, then*

$$\bigcap_{i=1}^{r} M_i \ = \ {}_R\langle \mathrm{m}^s(\boldsymbol{g_1}'), \ldots, \mathrm{m}^s(\boldsymbol{g_t}')\rangle_R.$$

Algorithm 13 Intersection of R-subbimodules of R^s

Require: $\{M_i\}_{i=1}^r$, a family of R-subbimodules of R^s with $M_i = {}_R\langle \boldsymbol{f_1^i}, \ldots, \boldsymbol{f_{t_i}^i} \rangle_R$;
Ensure: M, a finite generator system of $\bigcap_{i=1}^r M_i$ as an R-bimodule;

Initialization:

$$H := \begin{bmatrix} I_s & \cdots & I_s \\ \boldsymbol{f_1^1} & \cdots & \mathbf{0} \\ \vdots & & \vdots \\ \boldsymbol{f_{t_1}^1} & \cdots & \mathbf{0} \\ \vdots & & \vdots \\ \mathbf{0} & \cdots & \boldsymbol{f_1^r} \\ \vdots & & \vdots \\ \mathbf{0} & \cdots & \boldsymbol{f_{t_r}^r} \end{bmatrix} \in M_{(s+\sum_{j=1}^r t_j)\times rs}(R);$$

Using the Syzygy Bimodule Algorithm (Algorithm 12), compute a generator system $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_t}\}$ of $Syz(H)$ as an R-bimodule;
If $\boldsymbol{g_k} = (\boldsymbol{g_k}', \boldsymbol{g_k}'')$ where $\boldsymbol{g_k}' \in (R^{\mathrm{env}})^s$ and $\boldsymbol{g_k}'' \in (R^{\mathrm{env}})^{\sum_{j=1}^r t_j}$ for $1 \leq k \leq t$, take $M := \{\mathrm{m}^s(\boldsymbol{g_1}'), \ldots, \mathrm{m}^s(\boldsymbol{g_t}')\}$;
Return M.

2.6.9 Note. We will see later (in 2.6.25) how the previous result can be improved without assuming any extra condition. For example, it is possible to give a generator system for the left R^{env}-module $\bigcap_{i=1}^r (\mathrm{m}^s)^{-1}(M_i)$, a two-sided Gröbner basis for $\bigcap_{i=1}^r M_i$, a left Gröbner basis for $Syz(H)$, etc.

The previous results may be used in order to effectively compute finite intersections of R-subbimodules of R^s. We write this method in algorithmic notation under the name of Algorithm 13.

2.6.10 Example. Let R be the quantum plane (as in example 2.6.5) and consider the order POT for the exponents of R^2. Let M_1 and M_2 be the R-subbimodules of R^2 generated by $\{(2x^2+2x, -y), (0, -8), (-3xy, 0)\}$ and $\{(x+2, 0), (1, -y)\}$, respectively.

Using the library [32], Algorithm 13 takes 109.1 seconds to compute the

R-bimodule generator system M of $M_1 \cap M_2$, consisting of 12 elements:

$$\begin{aligned}M = \{\ &(\frac{4i}{3}x^2y + \frac{7}{3}xy, \frac{2i}{3}y^2),\ (-\frac{2i}{3}x^3 + (-\frac{4}{3} - \frac{2i}{3})x^2 - \frac{4}{3}x, \frac{i}{3}xy + \frac{2}{3}y),\\ &(-\frac{5}{3}x^2y + \frac{8i}{3}xy, -\frac{4}{3}y^2),\ ((-1 - \frac{5i}{3})x^3 + (-\frac{19}{3} - \frac{5i}{3})x^2 - \frac{16}{3}x,\\ &\frac{4i}{3}xy + \frac{8}{3}y),\ (\frac{10}{3}x^2y + (-1 - \frac{13i}{3})xy, \frac{8}{3}y^2),\ (\frac{2}{3}x^2 + \frac{2}{3}x, -\frac{4}{3}y),\\ &(\frac{4}{3}x^2y^2 - \frac{7}{3}xy^2, -\frac{2}{3}y^3),\ (-\frac{2}{3}x^3 - 2x^2 - \frac{4}{3}x, \frac{1}{3}xy + \frac{2}{3}y),\\ &((\frac{4}{3} + \frac{4i}{3})x^2y + (\frac{4}{3} - \frac{4i}{3})xy, (\frac{2}{3} + \frac{2i}{3})y^2),\ (\frac{-2i}{3}x^3y - 2x^2y\\ &+\frac{4i}{3}xy, -\frac{i}{3}xy^2 - \frac{2}{3}y^2),\ ((-\frac{2}{3} + \frac{2i}{3})x^3 + (-\frac{2}{3} + \frac{2i}{3})x^2, 0),\\ &(-\frac{4}{3}x^2y + (-\frac{2}{3} + \frac{2i}{3})xy, 0)\ \}.\end{aligned}$$

2.6.2 Presentation of M/N

Let $N \subseteq M$ be subbimodules of R^t. Taking into account again that the left R^{env}-modules are the R-bimodules, the question of finding a presentation of M/N as a quotient $(R^{\mathrm{env}})^s/K$ of a free module over the enveloping algebra R^{env} by a subbimodule K arises naturally.

2.6.11 Proposition. *Let R be a k-algebra, S an R-bimodule, and let $N \subseteq M$ be R-subbimodules of S. If $M = {}_R\langle f_1, \ldots, f_s\rangle_R$ and $N = {}_R\langle g_1, \ldots, g_r\rangle_R$, then*

$$M/N \ \cong\ (R^{\mathrm{env}})^s/K,$$

as R-bimodules, where

$$K = \{\boldsymbol{h}' \in (R^{\mathrm{env}})^s \ / \ \exists\, \boldsymbol{h}'' \in (R^{\mathrm{env}})^r, (\boldsymbol{h}', \boldsymbol{h}'') \in Syz(f_1, \ldots, f_s, g_1, \ldots, g_r)\}.$$

Proof. Let K be the kernel of the epimorphism of R-bimodules

$$\begin{aligned}\varphi : (R^{\mathrm{env}})^s &\longrightarrow M/N\\ (h_1, \ldots, h_s) &\mapsto \sum_{i=1}^{s} h_i f_i + N.\end{aligned}$$

So, $M/N \cong (R^{\text{env}})^s/K$, and for $\boldsymbol{h} = (h_1, \ldots, h_s) \in (R^{\text{env}})^s$,

$$\begin{aligned}
\boldsymbol{h} \in K &\iff \sum_{i=1}^{s} h_i f_i \in N \\
&\iff \exists\, \boldsymbol{h''} = (h''_1, \ldots, h''_r) \in (R^{\text{env}})^r \text{ such that } \sum_{i=1}^{s} h_i f_i = \sum_{j=1}^{r} h''_j g_j \\
&\iff \exists\, \boldsymbol{h''} \in (R^{\text{env}})^r \text{ such that } (\boldsymbol{h}, \boldsymbol{h''}) \in Syz(f_1, \ldots, f_s, g_1, \ldots, g_r).
\end{aligned}$$

□

Proposition 2.6.11, together with 2.6.6, implies the following result.

2.6.12 Corollary. *Let R be a k-algebra, S an R-bimodule, and let $N \subseteq M$ be subbimodules of S such that $M = {}_R\langle f_1, \ldots, f_s\rangle_R$ and $N = {}_R\langle g_1, \ldots, g_r\rangle_R$. If $Syz(f_1, \ldots, f_s, g_1, \ldots, g_r) = {}_R\langle \boldsymbol{h_1}, \ldots, \boldsymbol{h_l}\rangle_R$ with $\boldsymbol{h_k} = (\boldsymbol{h_k}', \boldsymbol{h_k}'') \in (R^{\text{env}})^s \times (R^{\text{env}})^r$ for all $1 \leq k \leq l$, then*

$$M/N \cong (R^{\text{env}})^s/K, \quad \text{where } K = {}_{R^{\text{env}}}\langle \boldsymbol{h_1}', \ldots, \boldsymbol{h_l}'\rangle.$$

We extract Algorithm 14 from 2.6.12, where $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ is assumed to be a G-Algebra, and $S = R^t$.

Algorithm 14 Presentation of M/N

Require: $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\rangle_R$, $N = {}_R\langle \boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\rangle_R$, with $N \subseteq M \subseteq R^t$;

Ensure: $K = {}_{R^{\text{env}}}\langle \boldsymbol{h_1}', \ldots, \boldsymbol{h_l}'\rangle \subseteq (R^{\text{env}})^t$ such that $M/N \cong (R^{\text{env}})^s/K$;

Using the Syzygy Bimodule Algorithm (Algorithm 12), compute a set of generators $H = \{\boldsymbol{h_1}, \ldots, \boldsymbol{h_l}\} \subseteq (R^{\text{env}})^{s+r}$ of $Syz(f_1, \ldots, f_s, g_1, \ldots, g_r)$ as an R-bimodule;

If $\boldsymbol{h_k} = (\boldsymbol{h_k}', \boldsymbol{h_k}'') \in (R^{\text{env}})^s \times (R^{\text{env}})^r$ for $1 \leq k \leq l$, put
$K := {}_{R^{\text{env}}}\langle \boldsymbol{h_1}', \ldots, \boldsymbol{h_l}'\rangle$;
Return K.

2.6.3 Two-sided free resolutions of bimodules

We can compute a free resolution of any subbimodule $M \subseteq R^t$ when R is a G-Algebra, just combining the method described in 2.6.2 for computing presentations of R-bimodules and the already known method to compute free

resolution for left modules over G-Algebras (see [13, 60]). More precisely, we show how to compute an exact complex

$$\cdots \longrightarrow (R^{\mathrm{env}})^{s_t} \xrightarrow{\partial_{t-1}} (R^{\mathrm{env}})^{s_{t-1}} \cdots \xrightarrow{\partial_1} (R^{\mathrm{env}})^{s_1} \xrightarrow{\partial_0} (R^{\mathrm{env}})^{s_0} \xrightarrow{\varepsilon} M \longrightarrow 0, \tag{2.18}$$

of R-bimodules and homomorphisms of R-bimodules. We shall call this type of resolutions a *two-sided free resolution of* M.

Our starting point is the R-bimodule $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_{s_0}} \rangle_R \subseteq R^t$. Using Algorithm 14 we can compute a set of generators $\{\boldsymbol{f_1^1}, \ldots, \boldsymbol{f_{s_1}^1}\}$ of a bimodule $K_0 \subseteq (R^{\mathrm{env}})^{s_0}$ where $M \cong (R^{\mathrm{env}})^{s_0}/K_0$. In other words, we obtain a short exact sequence of R-bimodules

$$\begin{array}{ccccc} & & (R^{\mathrm{env}})^{s_0} & \xrightarrow{\varepsilon} & M \longrightarrow 0 \\ & \overset{i_0}{\nearrow} & & & \\ K_0 & & & & \end{array} \tag{2.19}$$

where i_0 denotes the inclusion map and $\varepsilon : (R^{\mathrm{env}})^{s_0} \to M$ is the epimorphism of R-bimodules determined by $\varepsilon(h_1, \ldots, h_s) = \sum_{i=1}^{s_0} h_i \boldsymbol{f_i}$. At this point, since R^{env} is a G-Algebra, algorithms to compute a presentation of left modules can be applied, see e.g. [13, Ch. 6, Th. 3.1] (note that in that result the requirement of a Gröbner basis for M is not necessary). Let us recall how this works.

2.6.13 Theorem. [13] *Let R be a left PBW ring (e.g. a G-Algebra), and let $N \subseteq M$ be left R-modules of R^t such that $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_s} \rangle$ and $N = {}_R\langle \boldsymbol{g_1}, \ldots, \boldsymbol{g_r} \rangle$.*
If $Syz^l(H) = {}_R\langle \boldsymbol{p_1}, \ldots, \boldsymbol{p_l} \rangle$ with $\boldsymbol{p_k} = (\boldsymbol{p_k}', \boldsymbol{p_k}'') \in R^s \times R^r$ for all $1 \leq k \leq l$, then

$$M/N \cong R^s/K, \quad \text{where } K = {}_R\langle \boldsymbol{p_1}', \ldots, \boldsymbol{p_l}' \rangle.$$

Taking up our problem, if we apply 2.6.13 to the left R^{env}-module $K_0 = {}_{R^{\mathrm{env}}}\langle \boldsymbol{f_1^1}, \ldots, \boldsymbol{f_{s_1}^1} \rangle \subseteq (R^{\mathrm{env}})^{s_0}$ (with $N = 0$), then $K_0 \cong (R^{\mathrm{env}})^{s_1}/K_1$, for some $K_1 = {}_{R^{\mathrm{env}}}\langle \boldsymbol{f_1^2}, \ldots, \boldsymbol{f_{s_2}^2} \rangle$. So far, we have constructed the complex of R-bimodules and homomorphisms of R-bimodules

$$\begin{array}{ccccccc} & & (R^{\mathrm{env}})^{s_1} & \overset{\partial_0 = i_0 \circ \varepsilon_1}{\cdots\cdots\cdots\cdots\cdots\cdots} & (R^{\mathrm{env}})^{s_0} & \xrightarrow{\varepsilon} & M \longrightarrow 0 \\ & \overset{i_1}{\nearrow} & & \searrow^{\varepsilon_1} & & \overset{i_0}{\nearrow} & \\ K_1 & & & & K_0 & & \end{array}$$

where i_1 denotes the inclusion map and $\varepsilon_1 : (R^{\mathrm{env}})^{s_1} \to K_0$ is the epimorphism of R-bimodules determined by $\varepsilon_1(h_1, \ldots, h_{s_1}) = \sum_{i=1}^{s_1} h_i \boldsymbol{f_i^1}$. The iteration of this process yields the required exact complex of R-bimodules.

2.6.14 Proposition. *If $R = k\{x_1, \dots, x_n; Q, \preceq\}$ is a G-Algebra, then any R-bimodule $M \subseteq R^t$ has a two-sided free resolution*

$$0 \longrightarrow (R^{\mathrm{env}})^{s_m} \xrightarrow{\partial_{m-1}} (R^{\mathrm{env}})^{s_{m-1}} \cdots \xrightarrow{\partial_1} (R^{\mathrm{env}})^{s_1} \xrightarrow{\partial_0} (R^{\mathrm{env}})^{s_0} \xrightarrow{\varepsilon} M \longrightarrow 0$$

of length $m \leq 2n+1$.

Proof. This fact is a direct consequence of the celebrated *Hilbert's Syzygies Theorem* which states that every left R-module N over a G-Algebra $R = \mathsf{k}\{x_1, \dots, x_n; Q, \preceq\}$ has a (left) free resolution

$$0 \longrightarrow R^{s_m} \xrightarrow{\partial_{m-1}} R^{s_{m-1}} \cdots \xrightarrow{\partial_1} R^{s_1} \xrightarrow{\partial_0} R^{s_0} \xrightarrow{\varepsilon} N \longrightarrow 0$$

of length m at most n (we can find the proof in [60] and, using different methods, in [13], where it is proved in the more general context of left PBW rings).

More precisely, for any R-bimodule $M = {}_R\langle \boldsymbol{f_1}, \dots, \boldsymbol{f_s}\rangle_R \subseteq R^t$ we start with a short exact sequence as (2.19) where $M \cong (R^{\mathrm{env}})^s/K_0$. But we know that for the left R^{env}-module K_0 there exists a free resolution of length at most $m \leq 2n$ (since the enveloping algebra R^{env} of R has $2n$ variables). But these two complexes can be glued through the morphism $\partial = i \circ \varepsilon_1$, which satisfies that

$$\mathrm{Im}\,(\partial_0) = \mathrm{Ker}\,(\varepsilon_1) = \mathrm{Ker}\,(\partial) \quad \text{and} \quad \mathrm{Im}\,(\partial) = \mathrm{Im}\,(i) = \mathrm{Ker}\,(\varepsilon).$$

So, we have built a two-sided free resolution of M

$$0 \longrightarrow (R^{\mathrm{env}})^m \xrightarrow{\partial_{m-1}} \cdots \xrightarrow{\partial_0} (R^{\mathrm{env}})^{s_0} \xrightarrow{\partial = i\circ\varepsilon_1} (R^{\mathrm{env}})^s \xrightarrow{\varepsilon} M \longrightarrow 0$$

$$\varepsilon_1 \searrow \quad \nearrow i$$

$$K_0$$

of length $m+1 \leq 2n+1$. □

2.6.4 Two-sided division ideals

Recall that if $M \subseteq S$ is a left R-module and $G \subseteq S$ (where R is a ring and S is a left R-module), the *left division ideal (over R) of M by G* is defined as the left ideal

$${}_R(M : G) = \{\, f \in R \,/\, fG \subseteq M\} \leq R.$$

The *right division ideal* (*over* R) of a right R-module $M \subseteq S$ by a set $G \subseteq S$, denoted as $(M : G)_R$, is defined symmetrically.

In [13, page 214] we can find an algorithm to compute left division ideals (called also *left quotient ideals*) provided that R is a left PBW ring, the set G is finite, and a finite set of generators of M is given.

Next we propose a notion of two-sided division ideal, which can be viewed as the two-sided counterpart of left (and right) division ideals over a ring R.

2.6.15 Definition. Let R be a k-algebra, and S an R-bimodule. Let M be an R-subbimodule of S, and $G \subseteq S$. We define the *two-sided division ideal* (*over* R) *of* M *by* G as the image of the left ideal ${}_{R^{\mathrm{env}}}(M : G)$ of R^{env} under the epimorphism $\mathfrak{m}$, i.e.,

$$ {}_R(M : G)_R = \{\mathfrak{m}(h) \,/\, h \in R^{\mathrm{env}}, hG \subseteq M\}. $$

Note that ${}_R(M : G)_R$ is a two-sided ideal of R.

The following properties are clear from the definitions.

2.6.16 Proposition. *Let R be a k-algebra, and S an R-bimodule. Let M be an R-subbimodule of S and $G \subseteq S$.*

1. ${}_R(M : G) \subseteq {}_R(M : G)_R$ *and* $(M : G)_R \subseteq {}_R(M : G)_R$;
2. $G \subseteq M \iff {}_{R^{\mathrm{env}}}(M : G) = R^{\mathrm{env}} \iff {}_R(M : G)_R = R$;
3. *If* $G = \{g_1, \ldots, g_r\}$, *then* ${}_{R^{\mathrm{env}}}(M : G) = \bigcap_{i=1}^{r} {}_{R^{\mathrm{env}}}(M : \{g_i\})$;
4. *For every* $g \in S$, *we have* ${}_{R^{\mathrm{env}}}(M : \{g\}) = \{h \in R^{\mathrm{env}} \,/\, hg \in M \cap {}_R\langle g\rangle_R\}$, *and consequently,*

$$ {}_R(M : \{g\})_R = \{\mathfrak{m}(h) \,/\, h \in R^{\mathrm{env}},\ hg \in M \cap {}_R\langle g\rangle_R\}. $$

2.6.17 Proposition. *Let R be a k-algebra and S an R-bimodule. If* $M = {}_R\langle f_1, \ldots, f_t\rangle_R \subseteq S$ *and* $G = \{g_1, \ldots, g_r\} \subseteq S$, *then*

$$ {}_{R^{\mathrm{env}}}(M : G) = \{h' \in R^{\mathrm{env}} \,/\, \exists \boldsymbol{h}'' \in (R^{\mathrm{env}})^{rt}, (h', \boldsymbol{h}'') \in Syz(H)\}, $$

and hence,

$$ {}_R(M : G)_R = \{f \in R \,/\, \exists (h', \boldsymbol{h}'') \in Syz(H) \subseteq R^{\mathrm{env}} \times (R^{\mathrm{env}})^{rt}, f = \mathfrak{m}(h')\}, $$

where

$$H = \left[\frac{H_1}{H_2}\right] = \left[\begin{array}{ccc} g_1 & \cdots & g_r \\ \hline f_1 & \cdots & 0 \\ \vdots & & \vdots \\ f_t & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & f_1 \\ \vdots & & \vdots \\ 0 & \cdots & f_t \end{array}\right] \in M_{(1+rt)\times 1}(S^r).$$

Proof. Let $h \in R^{\text{env}}$.

$$\begin{aligned} h \in {}_{R^{\text{env}}}(M:G) &\iff \forall\, 1 \le i \le r,\ -hg_i = \sum_{j=1}^{t} h_j^i f_j, \text{ for some } h_j^i \in R^{\text{env}} \\ &\iff \exists\, \boldsymbol{h}'' = (h_1^1, \ldots, h_t^1, \ldots, h_1^r, \ldots, h_t^r) \in (R^{\text{env}})^{rt} \text{ such that} \\ &\quad (h, \boldsymbol{h}'') \in Syz(H), \end{aligned}$$

where H is as in 2.6.17. □

As a consequence of 2.6.17 and 2.6.6, the computation of a two-sided division ideal can be reduced to the computation of a syzygy bimodule.

2.6.18 Corollary. *Let R be a k-algebra, S an R-bimodule, $M = {}_R\langle f_1, \ldots, f_t\rangle_R \subseteq S$ and $G = \{g_1, \ldots, g_r\} \subseteq S$.*
If $Syz(H) = {}_R\langle \boldsymbol{h_1}, \ldots, \boldsymbol{h_l}\rangle_R$ (where H is a matrix as in 2.6.17) with $\boldsymbol{h_k} = (h'_k, \boldsymbol{h_k}'') \in R^{\text{env}} \times (R^{\text{env}})^{rt}$ for all $1 \le k \le l$, then

$${}_{R^{\text{env}}}(M:G) = {}_{R^{\text{env}}}\langle h'_1, \ldots, h'_l\rangle,$$

and

$${}_R(M:G)_R = {}_R\langle \mathfrak{m}(h'_1), \ldots, \mathfrak{m}(h'_l)\rangle_R.$$

When $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ is a G-Algebra and S is the free module R^s, from Corollary 2.6.18, this result may be used to devise an effective method to compute ${}_R(M:G)_R$ (Algorithm 15).

2.6.5 Simplified computations using centralizers

Alternative methods can be used for some of the problems described above in cases where the centralizer of a bimodule plays a role. We shall see, in

Algorithm 15 Two-sided division ideals

Require: $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\rangle_R \subseteq R^s$ and $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq R^s$;

Ensure: B, a finite generator system of ${}_R(M : G)_R$ as a two-sided ideal;

Initialization: Let H be the matrix defined in 2.6.17;

Using the Syzygy Bimodule Algorithm (Algorithm 12) compute a generator system $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_l}\}$ of $Syz(H)$ as an R-bimodule;

If $\boldsymbol{h_k} = (h_k{}', \boldsymbol{h_k}'')$ where $h_k{}' \in R^{\mathrm{env}} \times (R^{\mathrm{env}})^{rt}$, put
$B := \{\mathfrak{m}(h_1{}'), \ldots, \mathfrak{m}(h_l{}')\}$;
Return B.

particular, how the computation of syzygy bimodules and division ideals can easily be simplified.

Let us recall some definitions.

2.6.19 Definition. Let R be a ring, and M an R-bimodule.

1. The *centralizer* of M is the set
$$\mathrm{Cen}_R(M) = \{f \in M \,/\, rf = fr, \forall\, r \in R\}.$$
2. The bimodule M is said to be *centralizing* if M is generated as a left R-module (or equivalently, as a right R-module) by $\mathrm{Cen}_R(M)$.

2.6.20 Remark. Let R be a ring and M an R-bimodule. By 2.5.2,

$$\begin{aligned}\mathrm{Cen}_R(M) &= \{f \in M \,/\, (r \otimes 1 - 1 \otimes r)f = 0,\ \forall\, r \in R\}\\ &= \{f \in M \,/\, \mathrm{Ker}\,(\mathfrak{m}) \cdot f = 0\}\\ &= \mathrm{Ann}\,{}^r_M(\mathrm{Ker}\,(\mathfrak{m}))\end{aligned}$$

(where $\mathrm{Ann}\,{}^r_M(F)$ denotes the *right annihilator* of F, defined as the set $\{m \in M \,/\, Fm = 0\}$ when S is a ring, $F \subseteq S$ and M is a left S-module).

If, in addition, R is a k-algebra with a generator system as a k-vectorspace consisting of standard monomials, say $\{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$ (or, in particular, $R = \mathsf{k}\{x_1, \ldots, x_n;\, Q, \preceq\}$ is a G-Algebra), then

$$\mathrm{Cen}_R(M) = \{f \in M \,/\, x_j f = f x_j,\ \forall\, 1 \leq j \leq n\}.$$

2.6.21 Proposition. *Let R be a ring and M an R-bimodule. If $\{f_1, \ldots, f_t\} \subseteq M$ is such that*

$$\mathrm{Ker}\,(\mathfrak{m}) \subseteq \bigcap_{i=1}^{t} R^{\mathrm{env}}\,(0 : \{f_i\}),$$

then $\{f_1, \ldots, f_t\} \subseteq \mathrm{Cen}_R(M)$, *and therefore,* ${}_R\langle f_1, \ldots, f_t\rangle$ *is a centralizing bimodule.*

Proof. Note that $f \in \mathrm{Cen}_R(M)$ if, and only if, $(r \otimes 1 - 1 \otimes r)f = 0$ for all $r \in R$. Hence, the assertion is clear since $\mathrm{Ker}\,(\mathfrak{m}) = {}_{R^{\mathrm{env}}}\langle r \otimes 1 - 1 \otimes r \,/\, r \in R\rangle$ (see 2.5.2). □

2.6.22 Lemma. *Let* R *be a* k*-algebra,* S *an* R*-bimodule and let*

$$H = \begin{bmatrix} g_1 \\ \vdots \\ g_s \end{bmatrix} \in M_{s\times 1}(S).$$

The following conditions are equivalent:

1. *The rows* $g_1, \ldots, g_s$ *of* H *are elements of* $\mathrm{Cen}_R(S)$;
2. $\mathfrak{m}^s(\boldsymbol{h})H = \boldsymbol{h}H$, $\forall\, \boldsymbol{h} \in (R^{\mathrm{env}})^s$;
3. *The map* $R^s \longrightarrow S$; $(r_1, \ldots, r_s) \mapsto \sum_{i=1}^s r_i g_i$ *is a homomorphism of* R*-bimodules;*
4. $(\boldsymbol{f} \otimes \boldsymbol{1})H = (\boldsymbol{1} \otimes \boldsymbol{f})H$, $\forall\, \boldsymbol{f} \in R^s$;
5. $\mathrm{Ker}\,(\mathfrak{m}^s) \subseteq Syz(g_1, \ldots, g_s)$.

Furthermore, if any of the previous conditions holds, then $Syz^l(g_1, \ldots, g_s) = \mathfrak{m}^s(Syz(g_1, \ldots, g_s))$.

Proof. Implication $1 \Rightarrow 2$ is straightforward. For the converse, note that for any $r \in R$ and $i \in \{1, \ldots, s\}$, taking $\boldsymbol{h} = (0, \ldots, \overset{-i-}{1 \otimes r}, \ldots, 0) \in (R^{\mathrm{env}})^s$ it follows that

$$rg_i = \mathfrak{m}^s(\boldsymbol{h})H = \boldsymbol{h}H = (1 \otimes r)g_i = g_i r.$$

Let us see $1 \iff 3$. The "only if" is clear. On the other hand, assume that $\varphi^l : R^s \longrightarrow S$, given by $\varphi^l(r_1, \ldots, r_s) = \sum_{i=1}^s r_i g_i$, is a homomorphism of R-bimodules. Then, for all $r \in R$ and $i \in \{1, \ldots, s\}$,

$$rg_i = \varphi^l((1 \otimes r)(0, \ldots, \overset{-i-}{1}, \ldots, 0)) = (1 \otimes r)\varphi^l(0, \ldots, \overset{-i-}{1}, \ldots, 0) = g_i r.$$

The remaining equivalences are sketched in the sequence:

$$\begin{aligned} g_i \in \mathrm{Cen}_R(S),\ \forall\, 1 \le i \le s &\iff (r \otimes 1 - 1 \otimes r)g_i = 0, \forall\, r \in R,\ 1 \le i \le s \\ &\iff (\boldsymbol{f} \otimes \boldsymbol{1})H = (\boldsymbol{1} \otimes \boldsymbol{f})H, \forall\, \boldsymbol{f} \in R^s \\ &\iff \mathrm{Ker}\,(\mathfrak{m}^s) \subseteq Syz(H), \end{aligned}$$

where the last equivalence is a consequence of the statement 2 of 2.5.2. □

The following result is the key for the rest of this section. Compare with Lemma 2.6.6.

2.6.23 Theorem. *Let R be a k-algebra, S an R-bimodule, and $H = [\frac{H_1}{H_2}] \in M_{(s+p)\times 1}(S)$. Let $N \subseteq (R^{\mathrm{env}})^s$ be the left R^{env}-module and $M = \mathfrak{m}^s(N) \subseteq R^s$ the R-bimodule defined from H as in Lemma 2.6.6. Suppose that the matrix H_1 satisfies any of the equivalent conditions of Lemma 2.6.22. Then,*

1. $M = \{\boldsymbol{f} \in R^s \,/\, \exists\, \boldsymbol{h''} \in (R^{\mathrm{env}})^p, (\boldsymbol{f}\otimes \mathbf{1}, \boldsymbol{h''}) \in Syz(H)\}$
   $= \{\boldsymbol{f} \in R^s \,/\, \exists\, \boldsymbol{h''} \in (R^{\mathrm{env}})^p, (1\otimes \boldsymbol{f}, \boldsymbol{h''}) \in Syz(H)\}$;
2. $\mathrm{Ker}\,(\mathfrak{m}^s) \subseteq N$ *and* $N = (\mathfrak{m}^s)^{-1}(M)$. *Therefore, if* $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\rangle_R$, *or* $M = \langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\rangle_R$, *or* $M = \langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\rangle_R$, *then*
$$N = {}_{R^{\mathrm{env}}}\langle\ \{\boldsymbol{f_i}\otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(e_j,k)}}\otimes \mathbf{1} - 1\otimes \boldsymbol{x^{(e_j,k)}}\}_{1\le j\le n,\ 1\le k\le s}\rangle.$$
3. *Suppose that $R = k\{x_1, \ldots, x_n; Q, \preceq\}$ is a G-Algebra. For the exponents of the elements of both free modules $(R^{\mathrm{env}})^{s+p}$ and R^s, consider the order* POT *with* $\exp(\boldsymbol{e_1}) > \exp(\boldsymbol{e_2}) > \cdots$, *and for those of R^{env}, consider any of the orders $\preceq^*, \preceq^c, \preceq_*$, or $\preceq_c$.*

   If $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_t}\}$ is a left Gröbner basis for $Syz(H) \subseteq (R^{\mathrm{env}})^{s+p}$ as a left R^{env}-module with $\boldsymbol{h_i} = (\boldsymbol{h_i}', \boldsymbol{h_i}'') \in (R^{\mathrm{env}})^s \times (R^{\mathrm{env}})^p$, then
$$\{\boldsymbol{h_1}', \ldots, \boldsymbol{h_t}'\} \setminus \{\mathbf{0}\}$$
   is a left Gröbner basis for N, and
$$\{\mathfrak{m}^s(\boldsymbol{h_1}'), \ldots, \mathfrak{m}^s(\boldsymbol{h_t}')\} \setminus \{\mathbf{0}\}$$
   is a two-sided Gröbner basis for M.

Proof. The statement 1 can easily be checked by using conditions 2 and 4 of Lemma 2.6.22.
By the statement 2, it is enough to prove that $\mathrm{Ker}\,(\mathfrak{m}^s) \subseteq N$ (see the bijection 2.12). But, from condition 5 of 2.6.22 applied to the matrix H_1, for all $\boldsymbol{f} \in R^s$, $(\boldsymbol{f}\otimes \mathbf{1} - \mathbf{1}\otimes \boldsymbol{f}, \mathbf{0}) \in Syz(H)$. Hence, $\boldsymbol{f}\otimes \mathbf{1} - \mathbf{1}\otimes \boldsymbol{f} \in N$, and therefore,
$$\mathrm{Ker}\,(\mathfrak{m}^s) = {}_{R^{\mathrm{env}}}\langle \boldsymbol{f}\otimes \mathbf{1} - \mathbf{1}\otimes \boldsymbol{f} \,/\, \boldsymbol{f} \in R^s\rangle \subseteq N.$$
The second part of the statement 2 is justified by 2.5.3.
Let us prove the statement 3. If $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_t}\}$ is a left Gröbner basis for $Syz(H)$, then, obviously, $\{\boldsymbol{h_1}', \ldots, \boldsymbol{h_t}'\} \subseteq N$. Pick $\boldsymbol{h} \in N \setminus \{\mathbf{0}\}$. There exists

$\boldsymbol{h}'' \in (R^{\text{env}})^p$ such that $(\boldsymbol{h}, \boldsymbol{h}'') \in Syz(H)$. Moreover, as $\boldsymbol{h} \neq \mathbf{0}$ and the order on $(R^{\text{env}})^{s+p}$ is POT,

$$\exp_{(R^{\text{env}})^s}(\boldsymbol{h}) = \exp_{(R^{\text{env}})^{s+p}}((\boldsymbol{h}, \boldsymbol{h}'')) = (\alpha_1, \alpha_2) + \exp_{(R^{\text{env}})^{s+p}}(\boldsymbol{h_j}),$$

for some $j \in \{1, \ldots, t\}$ and $\alpha_1, \alpha_2 \in \mathbb{N}^n$. The level of that element $\boldsymbol{h_j}$ has to be the level of $\boldsymbol{h}$, which is in $\{1, \ldots, s\}$, so $\boldsymbol{h_j}' \neq \mathbf{0}$ and $\exp_{(R^{\text{env}})^{s+p}}(\boldsymbol{h_j}) = \exp_{(R^{\text{env}})^s}(\boldsymbol{h_j}')$. Therefore,

$$\exp_{(R^{\text{env}})^s}(\boldsymbol{h}) = (\alpha_1, \alpha_2) + \exp_{(R^{\text{env}})^s}(\boldsymbol{h_j}') \in \bigcup_{i=1}^{t} \exp_{(R^{\text{env}})^s}(\boldsymbol{h_j}') + \mathbb{N}^n.$$

Hence, $\{\boldsymbol{h_1}', \ldots, \boldsymbol{h_t}'\} \setminus \{\mathbf{0}\}$ is a left Gröbner basis for N and, by 2.5.5, $\{\mathfrak{m}^s(\boldsymbol{h_1}'), \ldots, \mathfrak{m}^s(\boldsymbol{h_t}')\} \setminus \{\mathbf{0}\}$ is a two-sided Gröbner basis for M. □

Just applying Theorem 2.6.23 in different situations where the centralizer is involved, we will show how some of the problems described previously based on the computation of syzygy bimodules, even the computation of the syzygy bimodule itself, can be simplified.

• **Simplified computation of the syzygy bimodule $Syz(F)$ when $F \subseteq \mathrm{Cen}_R(R^t)$.**

When $F \subseteq \mathrm{Cen}_R(R^t)$, it turns out that the syzygy bimodule $Syz(F)$ is the left R^{env}-module $(\mathfrak{m}^s)^{-1}(Syz^l(F))$, which, in this case, becomes an R-bimodule. We take profit of this fact to compute $Syz(F)$ by using a more simple method than that of Algorithm 12.

2.6.24 Proposition. *Let R be a k-algebra, and M a centralizing R-bimodule, say $M = {}_R\langle f_1, \ldots, f_s\rangle$, with $\{f_1, \ldots, f_s\} \subseteq \mathrm{Cen}_R(M)$. Then $Syz^l(f_1, \ldots, f_s)$ is an R-subbimodule of R^s with contracted (via $\mathfrak{m}^s$) left R^{env}-module $Syz(f_1, \ldots, f_s)$, and therefore,*

$$Syz^l(f_1, \ldots, f_s) = \mathfrak{m}^s(Syz(f_1, \ldots, f_s)).$$

Furthermore, if $R = k\{x_1, \ldots, x_n; Q, \preceq\}$ is a G-Algebra, then $Syz(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ can be computed by Algorithm 16. Moreover, if $G \subseteq (R^{\text{env}})^s$ is a left Gröbner basis for $Syz(f_1, \ldots, f_s)$ as a left R^{env}-module, then $\mathfrak{m}^s(G) \setminus \{0\}$ is a two-sided Gröbner basis for $Syz^l(f_1, \ldots, f_s)$, considering the orders specified in 2.6.23.

Proof. Since condition 1 of Lemma 2.6.22 is satisfied for

$$H = H_1 = \begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix}$$

Algorithm 16 Syzygy bimodule (centralizing case)

Require: $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\rangle_R$, with $\{\boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\} \subseteq \mathrm{Cen}_R(R^t)$;

Ensure: B, a finite generator system of $Syz(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ as a left R^{env}-module;

Using the Left Syzygy Module Algorithm (Algorithm 11), compute a generator system $\{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$ of $Syz^l(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ as a left R-module;

Put $B := \{\boldsymbol{g_i} \otimes 1\}_{i=1}^{r} \cup \{\boldsymbol{x^{(\epsilon_j,k)}} \otimes \mathbf{1} - \mathbf{1} \otimes \boldsymbol{x^{(\epsilon_j,k)}}\}_{1\leq j\leq n,\ 1\leq k\leq t}$;

Return B.

one may apply Theorem 2.6.23. If $N = Syz(f_1, \ldots, f_s)$, from the statement 1 of 2.6.23, one obtains

$$\begin{aligned}
\mathfrak{m}^s(N) &= \{\boldsymbol{g} \in R^s \,/\, \boldsymbol{g} \otimes \mathbf{1} \in Syz(f_1, \ldots, f_s)\} \\
&= \{(r_1, \ldots, r_s) \in R^s \,/\, \sum_{i=1}^{s} (r_i \otimes 1) f_i = 0\} \\
&= \{(r_1, \ldots, r_s) \in R^s \,/\, \sum_{i=1}^{s} r_i f_i = 0\} \\
&= Syz^l(f_1, \ldots, f_s).
\end{aligned}$$

□

• **Finite intersection of bimodules.**

The matrix H in our solution for computing an intersection $\bigcap_{i=1}^{r} M_i$ of R-subbimodules of R^s (see 2.6.8) fits the initial hypothesis of Theorem 2.6.23 without any extra condition, since H_1 is of the type $[I_s \cdots I_s]$.

In 2.6.7 we proved that the R-bimodule M defined from the matrix H as in Lemma 2.6.6 is exactly this intersection, i.e.,

$$M = \bigcap_{i=1}^{r} M_i.$$

Therefore, from the statement 2 of 2.6.23, the left R^{env}-module N defined from H is the intersection of the contracted (via $\mathfrak{m}^s$) left R^{env}-modules associated to the M_i's. Indeed,

$$N = (\mathfrak{m}^s)^{-1}(\bigcap_{i=1}^{r} M_i) = \bigcap_{i=1}^{r} (\mathfrak{m}^s)^{-1}(M_i).$$

2.6.25 Proposition. *Let R be a k-algebra and $\{M_i\}_{i=1}^r$ a family of R-subbimodules of R^s, each of them given by $M_i = {}_R\langle \boldsymbol{f_1^i}, \ldots, \boldsymbol{f_{t_i}^i}\rangle_R$. Consider the matrix $H \in M_{s+\sum_{i=1}^r t_i}(R^{rs})$ as in 2.6.7.*
If $M = \bigcap_{i=1}^r M_i = {}_R\langle \boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\rangle_R$, or $M = {}_R\langle \boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\rangle$, or $M = \langle \boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\rangle_R$, then

$$\bigcap_{i=1}^{r}(\mathfrak{m}^s)^{-1}(M_i) = {}_{R^{\mathrm{env}}}\langle \{\boldsymbol{g_i}\otimes \mathbf{1}\}_{i=1}^r \cup \{\boldsymbol{x^{(\epsilon_j,k)}}\otimes \mathbf{1} - \mathbf{1}\otimes \boldsymbol{x^{(\epsilon_j,k)}}\}_{1\le j\le n,\ 1\le k\le s}\rangle.$$

Moreover, if $R = k\{x_1, \ldots, x_n;\ Q,\ \preceq\}$ is a G-Algebra, and $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_t}\}$ is a left Gröbner basis for $Syz(H) \subseteq (R^{\mathrm{env}})^{s+\sum_{i=1}^r t_i}$ as a left R^{env}-module with $\boldsymbol{h_i} = (\boldsymbol{h_i}', \boldsymbol{h_i}'') \in (R^{\mathrm{env}})^s \times (R^{\mathrm{env}})^{\sum_{i=1}^r t_i}$, then

$$\{\boldsymbol{h_1}', \ldots, \boldsymbol{h_t}'\} \setminus \{\mathbf{0}\}$$

is a left Gröbner basis for $\bigcap_{i=1}^r (\mathfrak{m}^s)^{-1}(M_i)$ and

$$\{\mathfrak{m}^s(\boldsymbol{h_1}'), \ldots, \mathfrak{m}^s(\boldsymbol{h_t}')\} \setminus \{\mathbf{0}\}$$

is a two-sided Gröbner basis for $\bigcap_{i=1}^r M_i$, considering the orders specified in 2.6.23.

• Computation of presentations for centralizing bimodules.
When $R = \mathsf{k}\{x_1, \ldots, x_n;\ Q,\ \preceq\}$ is a G-Algebra and $M \subseteq R^t$ is a centralizing bimodule, say generated by $\{\boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\} \subseteq \mathrm{Cen}_R(M)$, it is possible to compute a presentation $M \cong R^s/L$, where $L = {}_R\langle H\rangle = \langle H\rangle_R$. Such presentations are required, e.g. in the computation of Ext (see [12]) or, as we will show in Section 2.7, in the computation of Tor.
An approach to this question is to compute the left syzygy module $Syz^l(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ (by e.g. Algorithm 11) and afterwards, since $Syz^l(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ is an R-bimodule (see 2.6.24), to compute a two-sided Gröbner basis H of this module by any of the Algorithms 5 or 10. Thus, $M \cong R^s/Syz^l(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ with $Syz^l(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s}) = {}_R\langle H\rangle = \langle H\rangle_R$.
An alternative method is proposed in the following result, which is written with algorithmic notation in Algorithm 17.

2.6.26 Proposition. *Let $R = k\{x_1, \ldots, x_n;\ Q,\ \preceq\}$ be a G-Algebra and $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\rangle$ a centralizing R-bimodule with $\{\boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\} \subseteq \mathrm{Cen}_R(R^t)$. For the exponents of the elements of both free modules $(R^{\mathrm{env}})^{s+p}$ and R^s, consider the order* POT *with $\exp(\boldsymbol{e_1}) > \exp(\boldsymbol{e_2}) > \cdots$, and for those of R^{env} consider any of the orders $\preceq^*, \preceq^c, \preceq_*$, or $\preceq_c$.*

If $G \subseteq (R^{\mathrm{env}})^s$ is a left Gröbner basis for $Syz(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$, then

$$M \cong R^s / Syz^l(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s}) \text{ as } R - \text{bimodules},$$

where $Syz^l(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ is generated by the two-sided Gröbner basis $\mathfrak{m}^s(G) \setminus \{\mathbf{0}\}$.

Algorithm 17 Presentation of centralizing bimodules

Require: $M = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_s} \rangle_R$, with $\{\boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\} \subseteq \mathrm{Cen}_R(R^t)$;

Ensure: L, a subbimodule of M such that $M \cong R^s / L$, with $L = {}_R\langle H \rangle = \langle H \rangle_R$;

Compute a left generator system $B \subseteq (R^{\mathrm{env}})^s$ of $Syz(\boldsymbol{f_1}, \ldots, \boldsymbol{f_s})$ by using Algorithm 16 (or by Algorithm 12);

Using the left Buchberger Algorithm (Algorithm 4), compute a left Gröbner basis $\{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\} \subseteq (R^{\mathrm{env}})^s$ for ${}_{R^{\mathrm{env}}}\langle B \rangle$;

Put $H := \{\mathfrak{m}^s(\boldsymbol{g_1}), \ldots, \mathfrak{m}^s(\boldsymbol{g_r})\}$, and $L := {}_R\langle H \rangle$;
Return L.

Proof. The proof arises from 2.6.24 and the fact that the map $R^s \longrightarrow R^t$; $(r_1, \ldots, r_s) \mapsto \sum_{i=1}^{s} r_i \boldsymbol{f_i}$, is a homomorphism of R-bimodules (see 2.6.22) with M as image. □

• Simplified computation of two-sided division ideals of R-bimodules by subsets $G \subseteq \mathrm{Cen}_R(R^s)$.

Let us come back to the problem (considered in 2.6.18) of computing the left division ideal ${}_{R^{\mathrm{env}}}(M : G)$ and the two-sided division ideal ${}_R(M : G)_R$. The following result shows that in case $G \subseteq \mathrm{Cen}_R(R^s)$, then the two-sided division ideal ${}_R(M : G)_R$ is exactly the left division ideal ${}_R(M : G) = \{f \in R \mid fg_i \in M, \ 1 \leq i \leq r\}$ over R. Hence, we obtain an alternative, direct method to compute ${}_R(M : G)_R$ and ${}_{R^{\mathrm{env}}}(M : G)$.

2.6.27 Proposition. *Let R be a k-algebra and S an R-bimodule. Let $M = {}_R\langle f_1, \ldots, f_t \rangle_R \subseteq S$ and $G = \{g_1, \ldots, g_r\} \subseteq \mathrm{Cen}_R(S)$. Then, ${}_R(M : G)$ is a two-sided ideal of R. Actually,*

$${}_R(M : G) = {}_R(M : G)_R,$$

and its contracted left ideal of R^{env} is

$$(\mathfrak{m})^{-1}({}_R(M : G)) = {}_{R^{\mathrm{env}}}(M : G).$$

Furthermore, if $R = k\{x_1,\ldots,x_n;Q,\preceq\}$ *is a G-Algebra, then the ideals* ${}_R(M:G)_R$ *and* ${}_{R^{\mathrm{env}}}(M:G)$ *can be computed by Algorithm 18. Moreover, if* $\{\boldsymbol{h_1},\ldots,\boldsymbol{h_l}\}$ *is a left Gröbner basis for* $Syz(H)$ *(H as in 2.6.17) with* $\boldsymbol{h_i} = (h_i', \boldsymbol{h_i}'') \in R^{\mathrm{env}} \times (R^{\mathrm{env}})^{rt}$, *then*

$$\{h_1', \ldots, h_l'\} \setminus \{0\}$$

is a left Gröbner basis for ${}_{R^{\mathrm{env}}}(M:G)$ *and*

$$\{\mathfrak{m}(h_1'), \ldots, \mathfrak{m}(h_l')\} \setminus \{0\}$$

is a two-sided Gröbner basis for ${}_R(M:G)_R$, *considering the orders specified in 2.6.23.*

Proof. Pick $r \in {}_R(M:G)_R$. There exists $h \in R^{\mathrm{env}}$ such that $hG \subseteq M$ and $\mathfrak{m}(h) = r$. If we write $h = \sum_{i;\,\mathrm{finite}} a_i \otimes b_i$, then for all $g \in G$

$$rg = \mathfrak{m}(h)g = \sum_i a_i b_i g = \sum_i a_i g b_i = \sum_i (a_i \otimes b_i)g = hg \in M.$$

Hence, ${}_R(M:G) = {}_R(M:G)_R$. Besides, we know from 2.6.17 that the two-sided ideal of R defined from the matrix H as in Lemma 2.6.6 is ${}_R(M:G)_R$, and that the left ideal of R^{env} defined from H is ${}_{R^{\mathrm{env}}}(M:G)$. At this point the proof directly follows from 2.6.23. □

Algorithm 18 Division ideals (centralizing case)

Require: $M = {}_R\langle \boldsymbol{f_1},\ldots,\boldsymbol{f_s}\rangle_R$, with $\{\boldsymbol{f_1},\ldots,\boldsymbol{f_s}\} \subseteq \mathrm{Cen}_R(R^t)$;

Ensure: B and B', finite generator systems of ${}_R(M:G)$ and ${}_R(M:G)_R$, respectively;

Using, e.g., the algorithm which can be found in [13, page 214], compute a generator system $H = \{h_1,\ldots,h_l\}$ of ${}_R(M:G)$ as a left R-module;

Put $B := H$; $B' := \{h_i \otimes 1\}_{i=1}^{l} \cup \{x_j \otimes 1 - 1 \otimes x_j\}_{1\le j\le n}$;
Return B, B'.

2.7 Effective computation of $\mathrm{Tor}_k(M,N)$

Unlike $\mathrm{Ext}_k(M,N)$ (see [11] when R is a G-Algebra), there are not known effective methods to compute $\mathrm{Tor}_k(M,N)$ for a pair of R-modules M and N over a non-commutative ring R. In this section, we devise an algorithm to

compute a presentation of $\mathrm{Tor}_k(M,\ N)$ when R is a G-Algebra, N is a left R-module, and M is a finitely presented R-bimodule, i.e., $M \cong R^m/L$ for a subbimodule L of R^m.

Our method follows basically the lines of [46] for the computation of Tor in the commutative case. The main difference between our approach and the one in [46] arises from the fact that, in general, $\mathrm{Tor}_k(M,N)$ is just an abelian group when M and N are left R-modules. This lack of structure avoids the computation of $\mathrm{Tor}_k(M,N)$ using Gröbner bases techniques, so we ask for a two-sided structure on M. Indeed, when M is an R-bimodule, then $\mathrm{Tor}_k(M,N)$ is a left R-module. We show that if, in addition, M is finitely presented as an R-bimodule and N is a finitely presented left R-module, then effective techniques involving Gröbner bases may be used to compute $\mathrm{Tor}_k(M,N)$ for any $k \geq 0$.

The ingredients of our method are exactly:

- the standard algorithm to compute left syzygies (Algorithm 11), and an algorithm to compute a free resolution of the left R-module N given a finite system of generators of N (such algorithm may be found in [13, 60, et al.]);
- a finite presentation of the R-bimodule M, as $M \cong R^m/L$, with L a subbimodule of R^m (see, e.g., Algorithm 17 to compute such a presentation in case M is a centralizing R-bimodule);
- theorem 2.7.2;

Our algorithm, described in detail in 2.7.3, shares the approach of [12] to compute $\mathrm{Ext}_k(M,N)$.

2.7.1 Isomorphisms related to tensor product

This subsection is devoted to fixing notation and describing some isomorphisms which will be used later.

Let R be a ring and M an R-bimodule.

For all $s \geq 1$, the map $\alpha : M^s \longrightarrow M \otimes_R R^s;\ \alpha(f_1,\ldots,f_s) = \sum_{i=1}^{s} f_i \otimes \boldsymbol{e_i}$, where $\{\boldsymbol{e_1},\ldots,\boldsymbol{e_s}\}$ is the canonical basis of R^s, is an isomorphism of left R-modules.

Indeed, α is the composition of the isomorphisms

$$\begin{array}{ccccc} M^s & \longrightarrow & (M \otimes_R R)^s & \longrightarrow & M \otimes_R R^s \\ (f_1,\ldots,f_s) & \mapsto & (f_1 \otimes 1,\ldots,f_s \otimes 1) & \mapsto & \sum_{i=1}^{s} f_i \otimes \boldsymbol{e_i}. \end{array} \tag{2.20}$$

On the other hand, if A is a subbimodule of R^m and B is a left submodule of R^s, then

$$\begin{array}{rcl}\beta : (R^m \otimes_R R^s)/T & \longrightarrow & (R^m/A) \otimes_R (R^s/B) \\ (\boldsymbol{f} \otimes \boldsymbol{g}) + T & \mapsto & (\boldsymbol{f} + A) \otimes (\boldsymbol{g} + B),\end{array} \tag{2.21}$$

where $T = R^m \otimes B \ + \ A \otimes_R R^s$, is an isomorphism of left R-modules.

Furthermore, if $\{\boldsymbol{a_1}, \ldots, \boldsymbol{a_r}\}$ is a generator system of A such that $A = {}_R\langle \boldsymbol{a_1}, \ldots, \boldsymbol{a_r}\rangle = \langle \boldsymbol{a_1}, \ldots, \boldsymbol{a_r}\rangle_R$, and $\{\boldsymbol{b_1}, \ldots, \boldsymbol{b_t}\}$ is a generator system of B as a left R-module, then

$$\{\boldsymbol{a_i} \otimes \boldsymbol{b_j} \ / \ 1 \leq i \leq r, \ 1 \leq j \leq t\}$$

is a generator system of $A \otimes_R B$ as a left R-module, since for all $\boldsymbol{a} = \sum_{l=l}^{r} p_l \boldsymbol{a_l} \in A$ and $\boldsymbol{b} = \sum_{j=1}^{t} p'_j \boldsymbol{b_j} \in B$ with $p_l, p'_j \in R$, we have that

$$\begin{aligned}\boldsymbol{a} \otimes \boldsymbol{b} &= \sum_{j,l} p_l \boldsymbol{a_l} \otimes p'_j \boldsymbol{b_j} \\ &= \sum_{j,l} p_l (\boldsymbol{a_l} p'_j) \otimes \boldsymbol{b_j} \\ &= \sum_{j,l} p_l (\sum_{i=1}^{r} p_i^{jl} \boldsymbol{a_i}) \otimes \boldsymbol{b_j} \\ &= \sum_{i,j,l} p_l p^{jl} \boldsymbol{a_i} \otimes \boldsymbol{b_j}.\end{aligned}$$

From here on until the end of the section, let $0 \to L \to R^m \xrightarrow{p_M} M \to 0$ be a finite presentation of the R-bimodule M, and let $H = \{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\} \subseteq R^m$ be a two-sided generator system of L in such a way that $L = {}_R\langle H\rangle = \langle H\rangle_R$ (e.g. when H is a two-sided Gröbner basis for L). Note that we can use Algorithm 17 to compute such a presentation in case R is a G-Algebra and M is a centralizing R-bimodule.

If N is a left R-module and $0 \to B \to R^s \xrightarrow{p_N} N \to 0$ is a presentation of N, then the map

$$\begin{array}{rcl}\gamma : R^{ms}/\alpha^{-1}(T) & \longrightarrow & M \otimes_R N \\ \boldsymbol{e_{ij}} + \alpha^{-1}(T) & \longmapsto & p_M(\boldsymbol{e'_j}) \otimes p_N(\boldsymbol{e_i})\end{array} \tag{2.22}$$

is an isomorphism of left R-modules, where $T = R^m \otimes_R B \ + \ L \otimes_R R^s$, and $\{\boldsymbol{e_1}, \ldots, \boldsymbol{e_s}\}$, $\{\boldsymbol{e'_1}, \ldots, \boldsymbol{e'_m}\}$, and $\{\boldsymbol{e_{11}}, \ldots, \boldsymbol{e_{1m}}, \ldots, \boldsymbol{e_{s1}}, \ldots, \boldsymbol{e_{sm}}\}$ are the canonical bases of R^s, R^m, and $R^{ms} = (R^m)^s$, respectively, where $\boldsymbol{e_{ij}} = (\boldsymbol{0_{R^m}}, \ldots, \overset{-i-}{\boldsymbol{e'_j}}, \ldots, \boldsymbol{0_{R^m}})$.

Indeed, γ is the composition of isomorphisms

$$R^{ms}/\alpha^{-1}(T) \xrightarrow{\bar{\alpha}} (R^m \otimes_R R^s)/T \xrightarrow{\beta} (R^m/L) \otimes_R (R^s/B) \xrightarrow{\bar{p}_M \otimes \bar{p}_N} M \otimes_R N$$

where $\bar{\alpha}$, $\bar{p_M}$, and $\bar{p_N}$ are obtained by factoring $\alpha : R^{ms} \longrightarrow (R^m \otimes_R R^s)/T$, $p_M : R^m \longrightarrow M$, and $p_N : R^s \longrightarrow N$, respectively, through the quotient.
Moreover, if $\{\boldsymbol{g_1}, \ldots, \boldsymbol{g_t}\}$ is a generator system of B as a left R-module, with $\boldsymbol{g_k} = (g_{k1}, .., g_{ks})$, then

$$\{\ (\boldsymbol{e'_j} g_{k1}, \ldots, \boldsymbol{e'_j} g_{ks})\ \}_{\substack{1 \le k \le t \\ 1 \le j \le m}} \ \cup\ \{\ (\boldsymbol{0_{R^m}}, \ldots, \overset{-i-}{\boldsymbol{h_l}}, \ldots, \boldsymbol{0_{R^m}})\ \}_{\substack{1 \le i \le s, \\ 1 \le l \le r}} \tag{2.23}$$

is a generator system of $\alpha^{-1}(T) = \alpha^{-1}(R^m \otimes_R B) + L^s$ as a left R-module, since

$$\{\ \boldsymbol{e'_j} \otimes \boldsymbol{g_k}\ \}_{\substack{1 \le j \le m, \\ 1 \le k \le t}} \ \cup\ \{\ \boldsymbol{h_l} \otimes \boldsymbol{e_i}\ \}_{\substack{1 \le l \le r, \\ 1 \le i \le s}}$$

is a generator system of $T = R^m \otimes_R B + L \otimes_R R^s$ and

$$\begin{aligned}
\alpha^{-1}(T) &= \alpha^{-1}(R^m \otimes_R B) + \alpha^{-1}(L \otimes_R R^s) \\
&= \alpha^{-1}(R^m \otimes_R B) + L^s \\
&= {}_R\langle\ \alpha^{-1}(\boldsymbol{e'_j} \otimes \boldsymbol{g_k}),\ \alpha^{-1}(\boldsymbol{h_l} \otimes \boldsymbol{e_i})\ \rangle_{i,j,k,l} \\
&= {}_R\langle\ (g_{k1}\boldsymbol{e'_j}, \ldots, g_{ks}\boldsymbol{e'_j}), (\boldsymbol{0_{R^m}}, \ldots, \overset{-i-}{\boldsymbol{h_l}}, \ldots, \boldsymbol{0_{R^m}})\ \rangle_{i,j,k,l}.
\end{aligned}$$

2.7.2 Algorithm to compute $\mathrm{Tor}_k(M, N)$

Until the end of the section, let $R = \mathsf{k}\{x_1, \ldots, x_n; Q, \preceq\}$ be a G-Algebra and N a finitely generated left R-module. Let

$$\ldots \xrightarrow{\partial_{k+1}} R^{s_k} \xrightarrow{\partial_k} R^{s_{k-1}} \longrightarrow \cdots \xrightarrow{\partial_1} R^{s_0} \xrightarrow{\partial_0} N \longrightarrow 0 \tag{2.24}$$

be a free resolution of N, where ∂_k is the matrix

$$\begin{bmatrix} \boldsymbol{g_1^k} \\ \vdots \\ \boldsymbol{g_{s_k}^k} \end{bmatrix}$$

with $\boldsymbol{g_i^k} = (g_{i1}^k, \ldots, g_{is_{k-1}}^k) \in R^{s_{k-1}}$ for $k \ge 1$ and $1 \le i \le s_k$ (an algorithm to compute it may be found in [13, Ch. 6], or in [60]).
In this subsection, assuming that M is a finitely presented R-bimodule, we show a method to compute $\mathrm{Tor}_k(M, N)$, i.e., to compute the k-th homology module of the complex

$$\ldots \xrightarrow{\mathrm{Id}_M \otimes \partial_{k+1}} M \otimes_R R^{s_k} \xrightarrow{\mathrm{Id}_M \otimes \partial_k} \ldots \xrightarrow{\mathrm{Id}_M \otimes \partial_1} M \otimes_R R^{s_0} \longrightarrow 0. \tag{2.25}$$

2.7.1 Remark. The case $k=0$ may be treated apart, since $\mathrm{Tor}_0(M,N) \cong M \otimes_R N$.

We start with the presentations $0 \to L \to R^m \to M \to 0$ and $0 \to \mathrm{Ker}\,\partial_0 \to R^{s_0} \to N \to 0$ of the R-bimodule M and of the left R-module N, respectively. Since $\{\boldsymbol{g_1^1}, \ldots, \boldsymbol{g_{s_1}^1}\}$ is a generator system of $\mathrm{Ker}\,\partial_0 = \mathrm{Im}\,\partial_1$ as a left R-module and

$$\gamma : R^{ms_0}/(\alpha^{-1}(R^m \otimes_R \mathrm{Ker}\,\partial_0) + L^{s_0}) \longrightarrow \mathrm{Tor}_0(M,N),$$

as in (2.22) is an isomorphism of left R-modules, we completely describe a presentation of $\mathrm{Tor}_0(M,N)$ by giving the generator system

$$\{\ (\boldsymbol{e'_j} g^1_{l1}, \ldots, \boldsymbol{e'_j} g^1_{ls_0})\ \}_{\substack{1\le l\le s_1,\\ 1\le j\le m}} \ \cup\ \{\ (\boldsymbol{0_{R^m}}, \ldots, \overset{-i-}{\boldsymbol{h_l}}, \ldots, \boldsymbol{0_{R^m}})\ \}_{\substack{1\le i\le s_0,\\ 1\le l\le r}}$$

of $\alpha^{-1}(R^m \otimes_R \mathrm{Ker}\,\partial_0) + L^{s_0}$, where $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\}$ is a two-sided Gröbner basis for L (see (2.23)).

Let us return to the general case. Consider again the presentation $0 \to L \to R^m \overset{p_M}{\to} M \to 0$ of the R-bimodule M and the free resolution (2.24) of N.

For all $k \ge 1$, let

$$d_k = \gamma_{k-1}^{-1} \circ (\mathrm{Id}_M \otimes \partial_k) \circ \gamma_k,$$

where $\gamma_k : R^{ms_k}/L^{s_k} \longrightarrow M \otimes_R R^{s_k}$ is the isomorphism defined as in (2.22) with $N = R^{s_k}$.

Clearly, the complex

$$\cdots \longrightarrow R^{ms_k}/L^{s_k} \xrightarrow{d_k} R^{ms_{k-1}}/L^{s_{k-1}} \xrightarrow{d_{k-1}} \cdots \xrightarrow{d_1} R^{ms_0}/L^{s_0} \longrightarrow 0 \qquad (2.26)$$

is isomorphic to the one in (2.25), so $\mathrm{Tor}_k(M,N)$ may be computed as the homology of (2.26).

By definition, for all $1 \le i \le s_k$, $1 \le j \le m$,

$$\begin{aligned} d_k(\boldsymbol{e_{ij}} + L^{s_k}) &= \gamma_{k-1}^{-1}(\mathrm{Id}_M \otimes \partial_k)\,\gamma_k(\boldsymbol{e_{ij}} + L^{s_k}) \\ &= \gamma_{k-1}^{-1}((\mathrm{Id}_M \otimes \partial_k)\,(p_M(\boldsymbol{e'_j}) \otimes \boldsymbol{e_i})) \\ &= \gamma_{k-1}^{-1}(p_M(\boldsymbol{e'_j}) \otimes (g^k_{i1}, \ldots, g^k_{is_{k-1}})) \\ &= (g^k_{i1}\boldsymbol{e'_j}, \ldots, g^k_{is_{k-1}}\boldsymbol{e'_j}) + L^{s_{k-1}}. \end{aligned} \qquad (2.27)$$

Let $\widetilde{d_k} : R^{ms_k} \longrightarrow R^{ms_{k-1}}$ be the block-built matrix

$$A_k = \left[\begin{array}{c|c|c} g^k_{11}I_m & \cdots & g^k_{1s_{k-1}}I_m \\ \hline \vdots & & \vdots \\ \hline g^k_{s_k1}I_m & \cdots & g^k_{s_ks_{k-1}}I_m \end{array}\right] \in M_{ms_k \times ms_{k-1}}(R),$$

where I_m denotes the $(m \times m)$-identity matrix. Since A_k is built of blocks which are elements of R times the identity matrix, we have $\widetilde{d_k}(L^{s_k}) \subseteq L^{s_{k-1}}$, and the diagram

$$\begin{array}{ccc} R^{ms_k} & \xrightarrow{\pi_k} & R^{ms_k}/L^{s_k} \\ \Big\downarrow{\scriptstyle \widetilde{d_k}} & & \Big\downarrow{\scriptstyle d_k} \\ R^{ms_{k-1}} & \xrightarrow[\pi_{k-1}]{} & R^{ms_{k-1}}/L^{s_{k-1}} \end{array}$$

is commutative, where π_k denotes the projection on the quotient.
The discussion above proves the following result:

2.7.2 Theorem. *With the previous notation, for all $k \geq 1$,*

1. $\operatorname{Ker} d_k = \operatorname{Ker} \pi_{k-1}\widetilde{d_k}/L^{s_k}$;
2. $\operatorname{Im} d_k = \operatorname{Im} \pi_{k-1}\widetilde{d_k} \subseteq R^{ms_{k-1}}/L^{s_{k-1}}$ *is generated by*

$$\{(g_{i1}^k \boldsymbol{e'_j}, \ldots, g_{is_{k-1}}^k \boldsymbol{e'_j}) + L^{s_{k-1}}\}_{\substack{1 \leq i \leq s_k \\ 1 \leq j \leq m}}$$

as a left R-module (note that $(g_{i1}^k \boldsymbol{e'_j}, \ldots, g_{is_{k-1}}^k \boldsymbol{e'_j})$ is the $(j+m(i-1))$-th row of A_k);.

3. $\operatorname{Tor}_k(M,N) \cong \operatorname{Ker} d_k / \operatorname{Im} d_{k+1} = \operatorname{Ker} \pi_{k-1}\widetilde{d_k} / ({}_R\langle \text{rows of } A_{k+1}\rangle + L^{s_k})$.

2.7.3 Remark. To compute $\operatorname{Tor}_k(M,N)$ we start with a finite presentation $0 \to L \to R^m \stackrel{p_M}{\to} M \to 0$ of the R-bimodule M (say, for example, we have computed a two-sided Gröbner basis $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\} \subseteq R^m$ of the R bimodule L) and a free resolution of the left R-module N as (2.24).
The matrix A_k is block-built as above, using the matrix

$$\partial_k = \begin{bmatrix} \boldsymbol{g_1^k} \\ \vdots \\ \boldsymbol{g_{s_k}^k} \end{bmatrix}$$

The set $\{ (\boldsymbol{0_{R^m}}, \ldots, \overset{-i-}{\boldsymbol{h_l}}, \ldots, \boldsymbol{0_{R^m}}) \}_{i,l=1}^{s_k,r}$ is a generator system (in fact, note that it is a two-sided Gröbner basis when $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\}$ so is) of L^{s_k} as an R-bimodule.
Then, we compute the kernel of $\pi_{k-1}\widetilde{d_k} : R^{ms_k} \longrightarrow R^{ms_{k-1}}/L^{s_{k-1}}$ using syzygies. Indeed (see [12]), let H_k be the matrix

$$H_k = \left[\frac{A_k}{A'_k}\right] \in M_{(ms_k + rs_{k-1}) \times ms_{k-1}}(R),$$

where A'_k is the matrix whose rows are the generators of $L^{s_{k-1}}$ as a left R-module. Then, if

$$Syz^l(H_k) = {}_R\langle \boldsymbol{p_1}, \ldots, \boldsymbol{p_t}\rangle, \quad \text{with } \boldsymbol{p_i} = (\boldsymbol{p'_i}, \boldsymbol{p''_i}) \in R^{ms_k} \times R^{rs_{k-1}},$$

then $\mathrm{Ker}\ \pi_{k-1}\widetilde{d_k} = {}_R\langle \boldsymbol{p'_1}, \ldots, \boldsymbol{p'_t}\rangle$.

This may be summarized in algorithmic notation, as it is described in Algorithm 19.

2.7.4 Remark. If the R-bimodule M is not centralizing, but we know a set $H = \{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\}$ satisfying $M \cong R^m/{}_R\langle H\rangle$ and ${}_R\langle H\rangle = \langle H\rangle_R$, (e.g., when H is a two-sided Gröbner basis (for ${}_R\langle H\rangle$)), then $\mathrm{Tor}_k(M,N)$ may still be computed by our algorithm.

2.7.5 Example. Let $R = U(\mathfrak{sl}(2))$, the universal enveloping algebra of the Lie algebra of traceless 2×2-matrices, where $k = \mathbb{C}$ (or $k = \mathbb{Q}$). We know that R is the G-Algebra $\mathsf{k}\{x,y,z;\ Q\ \preceq_\omega\}$ with $Q = \{\ yx - xy + z,\ zx - xz - 2x,\ zy - yz + 2y\ \}$ and, say, $\omega = (1,2,2)$.
Let $N = R^2/B$, where B is the left R-module generated by

$$g_1 = (y^3, x),\ g_2 = (y, xz),\ g_3 = (0, xy^2z - 2yz^2 + 2yz - x).$$

The left syzygy module $Syz^l(g_1,g_2,g_3)$ is generated by $g = (1, -y^2, 1) \in R^3$, and, hence,

$$0 \longrightarrow R \xrightarrow{\delta_1} R^3 \xrightarrow{\delta_0} N \longrightarrow 0, \tag{2.28}$$

where $\partial_0 = \begin{bmatrix} g_1 \\ g_2 \\ g_3 \end{bmatrix}$ and $\partial_1 = [g]$, is a free resolution of N.
Let L be the R-bimodule generated by $\{(C,1),(1,C)\}$, where C is the *Casimir element* $z^2/2 + 2xy - z$ (a well-known central element of $U(\mathfrak{sl}(2))$), and let $M = R^2/L$.
For all $k \geq 2$ we have $\mathrm{Tor}_k(M,N) = 0$, as the free resolution (2.28) of N has length 2.
For $k = 0$, we have (see 2.7.1) that $\mathrm{Tor}_0(M,N) \cong R^6\ /\ (\alpha^{-1}(R^2 \otimes_R B) + L^3)$, and

$$\{\ (1,0,-y^2,0,1,0)\ ,\ (0,1,0,-y^2,0,1)\ ,\ (C,1,0,0,0,0)\ ,\ (0,0,C,1,0,0)\ ,$$
$$(0,0,0,0,C,1)\ ,\ (1,C,0,0,0,0)\ ,\ (0,0,1,C,0,0)\ ,\ (0,0,0,0,1,C)\ \}$$

is a generator system of $\alpha^{-1}(R^2 \otimes_R B) + L^3$ as a left R-module.

Algorithm 19 Presentation of $\mathrm{Tor}_k(M,N)$

Require: $k \geq 0$, $N = {}_R\langle \boldsymbol{f_1}, \ldots, \boldsymbol{f_s}\rangle \subseteq R^t$, and $M = {}_R\langle \boldsymbol{f'_1}, \ldots, \boldsymbol{f'_m}\rangle_R$ with $\{\boldsymbol{f'_1}, \ldots, \boldsymbol{f'_m}\} \subseteq \mathrm{Cen}_R(R^{t'})$;

Ensure: A presentation $\mathrm{Ker}\, d_k/\mathrm{Im}\, d_{k+1}$ of the left R-module $\mathrm{Tor}_k(M,N)$;

Using Algorithm 17, compute a set $H = \{\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}\} \subseteq R^m$ such that $M \cong R^m/L$, with $L = {}_R\langle H\rangle = \langle H\rangle_R$;

Compute a free left resolution

$$\left\{ R^{s_j},\ \partial_j = \begin{bmatrix} g^j_{11} & \cdots & g^j_{1s_{j-1}} \\ \vdots & & \vdots \\ g^j_{s_j 1} & \cdots & g^j_{s_j s_{j-1}} \end{bmatrix} \right\}_{j\geq 0}$$

of the left R-module N (this step may be accomplished by using the very well-known algorithm which may be found in [13, 60]).

Compute the block-built matrices

$$A_k = \left[\begin{array}{c|c|c} g^k_{11}I_m & \cdots & g^k_{1s_{k-1}}I_m \\ \hline \vdots & & \vdots \\ \hline g^k_{s_k 1}I_m & \cdots & g^k_{s_k s_{k-1}}I_m \end{array}\right], \quad A_{k+1} = \left[\begin{array}{c|c|c} g^{k+1}_{11}I_m & \cdots & g^{k+1}_{1s_k}I_m \\ \hline \vdots & & \vdots \\ \hline g^{k+1}_{s_{k+1}1}I_m & \cdots & g^{k+1}_{s_{k+1}s_k}I_m \end{array}\right];$$

Compute the matrices A'_k and A'_{k+1} whose rows are $(\boldsymbol{0_{R^m}}, \ldots, \overset{-i-}{\boldsymbol{h_l}}, \ldots, \boldsymbol{0_{R^m}})$ for $1 \leq l \leq r$, and $1 \leq i \leq s_{k-1}$ resp. $1 \leq i \leq s_k$.

Compute a generator system $\{\boldsymbol{p_1}, \ldots, \boldsymbol{p_l}\} \subseteq R^{ms_k} \times R^{rs_{k-1}}$ of the left syzygy module of the matrix $\left[\dfrac{A_k}{A'_k}\right]$.

The set $\{\boldsymbol{p'_1}, \ldots, \boldsymbol{p'_l}\}$, where $\boldsymbol{p'_i}$ consists of the first ms_k coordinates of $\boldsymbol{p_i}$ for all i, is a left generator system of $\mathrm{Ker}\, d_k$;

The set whose elements are the rows of A_{k+1} and the rows of A'_{k+1} is a left generator system of $\mathrm{Im}\, d_{k+1}$;

Return $\mathrm{Ker}\, d_k$, $\mathrm{Im}\, d_{k+1}$.

For $k=1$, we have $\mathrm{Tor}_1(M,N) \cong \mathrm{Ker}\,(\pi_0\widetilde{d_1})\ /\ ({}_R\langle\text{rows of } A_2\rangle + L)$, but in this particular example $A_2 = 0$ since $\partial_2 = 0$.
As pointed out in 2.7.3, $\mathrm{Ker}\,\pi_0\widetilde{d_1}$ is obtained from the left syzygy module of the rows of

$$A_1 = \begin{bmatrix} 1 & 0 & -y^2 & 0 & 1 & 0 \\ 0 & 1 & 0 & -y^2 & 0 & 1 \end{bmatrix}$$

and the generators of L^3. Indeed, by picking up just the first two components of each element of the generator system

$$\begin{aligned}\{&(z^2+4xy-2z, 2, -2, 2y^2, -2, 0, 0, 0)\ ,\\ &(1, z^2/2+2xy-z, 0, 0, 0, -1, y^2, -1)\ ,\\ &(8xy-4z, -4z^4-4xyz^2+2z^3+4, -4, 4y^2, -4, 2y^2,\\ &\qquad -2y^2z^2+16y^2z-32y^2, 2z^2)\}\end{aligned}$$

of $Syz^l(A_1)$, we obtain the generator system

$$\{\ (2C, 2)\ ,\ (1, C)\ ,\ (8xy-4z, -z^4-4xyz^2+2z^3+4)\ \}$$

of $\mathrm{Ker}\,\pi_0\widetilde{d_1}$. Therefore, $\mathrm{Tor}_1(M,N) \cong \mathrm{Ker}\,\pi_0\widetilde{d_1}/L = 0$, since $(8xy-4z, -z^4-4xyz^2+2z^3+4) \in L$ (one may check this by dividing the element by a two-sided Gröbner basis for L).

Chapter 3

Square-free solutions of YBE and Yang-Baxter Algebras

As we pointed out in Chapter 1, Yang-Baxter Algebras are a particular class of algebras with PBW bases. They are defined from solutions of the Yang-Baxter equation, which has became an attractive research topic to scientists and mathematicians since the middle of nineteen sixties. First, many solutions of this equation were found by studying certain related algebraic structures: the Hopf algebras (see e.g. [55]). In 1990 Drinfeld [19] suggested looking for the so-called *set-theoretic solutions*, which are the simplest class of solutions. In this sense, Weinstein and Xu [81] found in 1992 a way to construct set-theoretic solutions by studying the Poisson group. Afterwards, Etingof, Schedler and Soloviev [21] studied set-theoretic solutions satisfying invertibility, unitarity and nondegeneracy. They introduced several constructions of such solutions, they gave their classification in terms of group theory and showed their geometric and algebraic interpretations. Meanwhile, Lu, Yan and Zhu [66] proposed a method to construct set-theoretic solutions which generalizes the earlier ones of Weinstein-Zu and Etingof-Schedler-Soloviev. Whereas these results are based on algebro-geometric and topological methods, T. Gateva-Ivanova introduces a combinatorial approach to this topic focusing on the behaviour of the set of relations $\Re(X,r)$, uniquely determined by each solution (X,r) (see [38, 39, 40]). If a solution (X,r) is square-free, then the set $\Re(X,r)$ satisfies the so-called *Cyclic Condition*, which is essential in combinatorial techniques in this context. This approach has been applied, for example, in order to obtain algebraic and homological properties (see [42]) of the Yang-Baxter Algebra $\mathcal{A}(\mathsf{k},X,r)$, the Yang-Baxter group $\mathcal{G}(X,r)$ and the Yang-Baxter semigroup $\mathcal{S}(X,r)$ associated to each square-free solution (X,r).

As we show throughout the whole chapter, the combinatorial approach of T. Gateva-Ivanova can be used in order to develop algorithmic methods in the context of (square-free) solutions of the YBE. After recalling some ways of representing and classifying square-free solutions, we study isomorphisms and automorphisms of solutions by following this combinatorial-computational approach. The usefulness of computing the group of automorphisms of a solution is justified at the end of the first section, where we construct some algorithms which require automorphisms in order to compute *extensions* of solutions (i.e. new solutions obtained by gluing two solutions).

In the last section we discuss the equivalence, proved by T. Gateva-Ivanova [40, 42] and M. Van den Bergh [42], between square-free solutions of the YBE, semigroups of skew-polynomial type and semigroups of I-type. The theory of reduction systems and Gröbner basis surveyed in the first chapter can be used in this context to prove (cf. [40]) that the Yang-Baxter Algebra $\mathcal{A}(\mathsf{k}, X, r)$ of any square-free solution (X, r) is an algebra with a PBW basis. Finally, we show how the behaviour of semigroups of skew-polynomial type can be determined completely by a family of Linear Programming problems.

Throughout the whole chapter we illustrate theoretic notions with explicit examples. In order to do these computations we have encoded a library of procedures, included in the CD at the back page of this work (see also [32]), using the package of symbolic computation *Maple*. It allows us to recognize when a set of relations determines a square-free solution, to compute all possible orders $\preceq$ on $X = \{x_1 \prec \cdots \prec x_n\}$ (renaming the variables x_i's if necessary) such that the Yang-Baxter semigroup $\mathcal{S}(X, r)$ is of skew-polynomial type, to verify when a bijection is an automorphism of a square-free solution, to compute the group of automorphisms of any square-free solution, to glue two square-free solutions in order to obtain other square-free solution, etc.

3.1 Square-free solutions of the Yang-Baxter equation

We start this section recalling some basic notions and results in the topic of set-theoretic solutions of the Yang-Baxter equation, mostly collected from the works of T. Gateva-Ivanova [35, 36, 42, 40] and P. Etingof, T. Schedler and A. Soloviev (see e.g. [21]). We focus on square-free solutions of the Yang-Baxter equation, viewed from a combinatorial approach, where the so-called *Cyclic Condition* plays an important role.

3.1.1 First notions

The *Yang-Baxter equation* (YBE, for short) first appeared in 1967 in Statistical Mechanics, and it became one of the basic equations of Mathematical Physics. Since then, many scientists and mathematicians are devoted to find solutions of this equation. In this historical context, the YBE was formulated in the following way, as we can find in [55].

3.1.1 Definition. Let V be a vectorspace over a field k and R a linear automorphism of $V \otimes_{\mathsf{k}} V$.

1. R is a *solution of the (classical) YBE* if the equality

$$(R \otimes \mathrm{Id}_V)(\mathrm{Id}_V \otimes R)(R \otimes \mathrm{Id}_V) = (\mathrm{Id}_V \otimes R)(R \otimes \mathrm{Id}_V)(\mathrm{Id}_V \otimes R) \quad (3.1)$$

   holds in the group of automorphisms of $V \otimes_{\mathsf{k}} V \otimes_{\mathsf{k}} V$.

2. R is called a *solution of the Quantum Yang-Baxter equation* (QYBE, for short) or an *R-matrix* if

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}, \quad (3.2)$$

   where $R^{ij} : V \otimes_{\mathsf{k}} V \otimes_{\mathsf{k}} V \longrightarrow V \otimes_{\mathsf{k}} V \otimes_{\mathsf{k}} V$ means R acting on the i-th and j-th components.

   A solution R of the QYBE satisfying $R^{12}R^{12} = \mathrm{Id}_{V \otimes V}$ is known in the literature (see e.g. [68]) as a *Yang-Baxter operator*.

3.1.2 Example. Let V be an arbitrary vectorspace over a field k. The *flip* $\tau_{V,V} : V \otimes_{\mathsf{k}} V \longrightarrow V \otimes_{\mathsf{k}} V$ defined as $\tau_{V,V}(x \otimes y) = y \otimes x$ for all $x, y \in V$ is a solution of both the YBE and QYBE. It is called the *trivial solution*.

The problem of finding all the solutions of the YBE is an open problem. If $\{v_i\}_i$ is a basis of the finite dimensional vectorspace V, each automorphism can be represented as $R \in V \otimes_{\mathsf{k}} V$ by

$$R(v_i \otimes v_j) = \sum_{k,l} C_{ij}^{kl} v_k \otimes v_l.$$

Hence, R is a solution of the YBE if, and only if,

$$\sum_{p,q,r,x,y,z} (C_{ij}^{pq}\delta_{kr})(\delta_{px}C_{qr}^{yz})(C_{xy}^{lm}\delta_{zn}) = \sum_{p,q,r,x,y,z} (\delta_{ip}C_{jk}^{qr})(C_{pq}^{xy}\delta_{rz})(\delta_{xl}C_{yz}^{mn}),$$

for all i, j, k, l, m, n, or equivalently,

$$\sum_{p,q,y} C_{ij}^{pq} C_{qk}^{yn} C_{py}^{lm} = \sum_{y,q,r} C_{jk}^{qr} C_{iq}^{ly} C_{yr}^{mn}, \quad \forall\, i, j, k, l, m, n.$$

This formulation of the problem involves $(\dim_{\mathsf{k}}(V))^6$ cubic equations on the $(\dim_{\mathsf{k}}(V))^4$ coefficients C_{ij}^{kl} of R, which gives a hint of the difficulty. However, in the last two decades many solutions of the YBE have been found, and the related algebraic structures (Hopf algebras) have been intensively studied. Most of the solutions found were "deformations" of the trivial solution. At the beginning of the 1990's, Majid [67] introduced and studied the *matched pairs of groups* in order to produce solutions. In 1991 Drinfeld [19] set the problem of finding the so-called *set-theoretic solutions*, the simplest class of solutions, which in general are not obtained as deformations of the trivial solution.

3.1.3 Definition. Let X be a non-empty set. A bijective map r of $X \times X$ onto itself is a *set-theoretic solution of the YBE* if the equality

$$r_1 r_2 r_1 = r_2 r_1 r_2 \tag{3.3}$$

holds in $X \times X \times X$, where

$$\begin{aligned} r_1 : X \times X \times X &\longrightarrow X \times X \times X & \qquad r_2 : X \times X \times X &\longrightarrow X \times X \times X \\ (x, y, z) &\mapsto (r(x, y), z) & (x, y, z) &\mapsto (x, r(y, z)). \end{aligned}$$

From now on, we shall refer to the equality (3.3) as *YB condition*, *braid relation* or *YB diagram* (if we represent it by a diagram). In case r is a set-theoretic solution, (X, r) is called a *braided set*.
Similarly, r is a *set-theoretic solution of the QYBE* if the Quantum Yang-Baxter Equation (3.2) holds in $X \times X \times X$ where R^{ij} is the bijection defined as r acting on the i-th and j-th components.

Clearly, each set-theoretic solution (X, r) of the YBE induces a solution $R : V \otimes_{\mathsf{k}} V \longrightarrow V \otimes_{\mathsf{k}} V$ of the classical YBE where V is the k-vectorspace spanned by X.

3.1.4 Example. Let $X = \{x_1, x_2, x_3\}$ and r the involutive map (i.e., $r^2 = \mathrm{Id}_{X \times X}$) defined as

$$\begin{aligned} r : X \times X &\longrightarrow X \times X \\ (x_1, x_2) &\leftrightarrow (x_2, x_1) \\ (x_1, x_3) &\leftrightarrow (x_3, x_2) \\ (x_2, x_3) &\leftrightarrow (x_3, x_1) \\ (x_i, x_i) &\leftrightarrow (x_i, x_i), \quad 1 \leq i \leq 3. \end{aligned}$$

Then, (X, r) is a set-theoretic solution of the YBE. In fact, this solution and the trivial one are the only (up to re-indexing the variables) set-theoretic

involutive, nondegenerate square-free solutions (see 3.1.6 for definitions) of the YBE for a set X of 3 elements.

One can associate to (X, r) the following products of disjoint cycles in $\mathrm{Sym}(X)$

$$\sigma_1 = (x_3)(x_2x_1), \qquad \sigma_2 = (x_2)(x_1),$$

meaning

$$\begin{array}{ll} r(x_i, x_i) = & (x_i, x_i), \qquad\qquad 1 \leq i \leq 3, \\ r(x_2, x_3) = & (\sigma_1(x_3), \sigma_1^{-1}(x_2)) = (x_3, x_1), \\ r(x_3, x_2) = & (\sigma_1(x_2), \sigma_1^{-1}(x_3)) = (x_1, x_3), \\ r(x_1, x_2) = & (\sigma_2(x_2), \sigma_2^{-1}(x_1)) = (x_2, x_1), \end{array}$$

and so on. As we will recall later (see condition (6) of 3.1.19), this notation can be used in order to represent any square-free solution of the YBE.

The following well known fact (see e.g. [21]) gives the relation between the set-theoretic solutions of the YBE and the set-theoretic solutions of the QYBE.

3.1.5 Proposition. *Let r: $X \times X \longrightarrow X \times X$ be a bijection, and let $f, g : X \times X \longrightarrow X$ be the maps such that $r(x, y) = (f(x, y), g(x, y))$. Let $R = \tau \circ r$ where $\tau : X \times X \longrightarrow X \times X$ denotes the* flip map *given by $\tau(x, y) = (y, x)$, for all $x, y \in X$.*

Then, r is a set-theoretic solution of the YBE if, and only if, R is a set-theoretic solution of the QYBE. Furthermore, $r^2 = \mathrm{Id}_{X\times X}$ if, and only if, R satisfies $R^{21}R = \mathrm{Id}_{X\times X}$, where $R^{21}(x, y) = (f(y, x), g(y, x))$ for $x, y \in X$.

In what follows, X will be a finite non-empty set and we will denote by $\mathrm{Sym}(X)$ the *group of permutations* of X, with product $fg = f \circ g$. For any integer $m \geq 2$, we will identify the cartesian product $X \times \overset{m}{\cdots} \times X$ and the set X^m of monomials of length m in the alphabet X. As usually, given a bijection $r : X \times X \longrightarrow X \times X$ the map $r^{i,i+1} : X^m \longrightarrow X^m$ is defined as $r^{i,i+1} = \mathrm{Id}_{X^{i-1}} \times r \times \mathrm{Id}_{X^{m-i-1}}$.

We are interested in set-theoretic solutions of the YBE which satisfy certain conditions. They are recalled below following the terminology of [21] and [38].

3.1.6 Definition. Let $r : X^2 \longrightarrow X^2$ be a bijection given by its component maps $\mathcal{L}_x, \mathcal{R}_y : X \longrightarrow X$ as $r(xy) = \mathcal{L}_x(y)\mathcal{R}_y(x)$.

1. The map r, or equiv. the set (X, r), is *involutive* if $r^2 = \mathrm{Id}_{X^2}$. A braided and involutive set (X, r) is called a *symmetric set*;

2. The map r, or equiv. the set (X, r), is *nondegenerate* if the component maps
$$\mathcal{L}_x : X \longrightarrow X, \qquad \mathcal{R}_y : X \longrightarrow X$$
are bijective for all $x, y \in X$;

3. The map r, or equiv. the set (X, r), is *square-free* if $r(xx) = xx$ for all $x \in X$.

3.1.7 Remark. From now on, a nondegenerate involutive set-theoretic solution (X, r) (that is, a nondegenerate symmetric set (X, r)) will be simply called a *solution (of the YBE)*.

Throughout this chapter, the set X of any solution (X, r) is supposed to be finite.

Recall that the n-th *Braid group* $\mathcal{B}_n$ is finitely presented via generators $\{b_1, \ldots, b_{n-1}\}$ and defining relations
$$\left\{ \begin{array}{ll} b_i b_j = b_j b_i, & |i-j| > 1; \\ b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}, & 1 \leq i \leq n-2 \end{array} \right\}.$$

The *symmetric group* $\mathcal{S}_n$ is the quotient of $\mathcal{B}_n$
$$\mathcal{S}_n = \mathcal{B}_n / \langle b_i^2 = 1 \rangle_{i=1}^{n-1}.$$

3.1.8 Proposition. [21] *Let $n > 2$ and $X = \{x_1, \ldots, x_n\}$. Then the following two conditions hold for each integer $m \geq 3$.*

- *The assignment $b_i \longrightarrow r^{i,i+1}$ for $1 \leq i \leq m-1$ extends to an action of $\mathcal{B}_m$ on X^m if, and only if, (X, r) is a braided set.*
- *The assignment $b_i \longrightarrow r^{i,i+1}$ for $1 \leq i \leq m-1$ extends to an action of S_m on X^m if, and only if, (X, r) is a symmetric set.*

The (nondegenerate, involutive, set-theoretic) solutions of the YBE have been studied in many papers like [81, 21, 66, 75]. In [42] it was shown first the close relation between the square-free solutions, the semigroups of skew-polynomial type, and semigroups of I-type. This motivated the conjecture of Gateva-Ivanova (see 3.3.12), recently verified in [40], that the three notions: the square-free solutions, the semigroups of skew-polynomial type, and semigroups of I-type, are equivalent.

We will focus on square-free solutions (X, r), from which Yang-Baxter Algebras, treated in the next section, are obtained.

3.1.9 Example. The *trivial solution* $\tau : X^2 \longrightarrow X^2$ given by $\tau(xy) = yx$ for all $x, y \in X$, is an example of square-free solution of the YBE.

3.1.10 Example. If (X, r_X) and (Y, r_Y) are square-free solutions, then the pair $(X \times Y, r_{X\times Y})$ where $r_{X\times Y} = (\mathrm{Id}_X \times \tau \times \mathrm{Id}_Y) \circ (r_X \times r_Y) \circ (\mathrm{Id}_X \times \tau^{-1} \times \mathrm{Id}_Y)$ and $\tau : X \times Y \longrightarrow Y \times X$ is the flip map, is a square-free solution of the YBE as well, called the *cartesian product of* (X, r_X) and (Y, r_Y).

3.1.11 Example. (Lyubashenko; see [19])
Let X be a non-empty set and $\mathcal{L}, \mathcal{R} : X \longrightarrow X$ maps. Let

$$\begin{aligned} r : X^2 &\longrightarrow X^2 \\ xy &\mapsto \mathcal{L}(y)\mathcal{R}(x). \end{aligned}$$

i) (X, r) is a nondegenerate set if, and only if, $\mathcal{L}$ and $\mathcal{R}$ are bijections;
ii) (X, r) is a braided set if, and only if, $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$;
iii) (X, r) is involutive if, and only if, $\mathcal{L} = \mathcal{R}^{-1}$.

In this case (X, r) is called a *permutational solution.*
Note that there exists a unique square-free permutational solution, namely the identity solution: $r_\sigma = \mathrm{Id}_{X^2}$. However, as we will see in 3.1.19, each square-free solution behaves *locally* as a permutational solution.

3.1.12 Definition. [21] Let (X, r_X) and (Y, r_Y) be solutions. A bijection $\varphi : X \longrightarrow Y$ is an *isomorphism* from (X, r_X) to (Y, r_Y) if the diagram

$$\begin{array}{ccc} X \times X & \xrightarrow{r_X} & X \times X \\ {\scriptstyle \varphi\times\varphi}\downarrow & & \downarrow{\scriptstyle \varphi\times\varphi} \\ Y \times Y & \xrightarrow{r_Y} & Y \times Y \end{array} \tag{3.4}$$

is commutative. In that case, (X, r_X) and (Y, r_Y) are called *isomorphic solutions*. We denote by $\mathrm{Is}(X, Y)$ the set of isomorphisms from (X, r_X) to (Y, r_Y).

3.1.13 Note. Clearly $\varphi \in \mathrm{Is}(X, Y)$ if, and only if, $\varphi^{-1} \in \mathrm{Is}(Y, X)$. Hence, the relation defined for two arbitrary solutions (X, r_X) and (Y, r_Y) as

$$(X, r_X) \sim (Y, r_Y) \iff \exists\, \varphi \in \mathrm{Is}(X, Y)$$

is an equivalence relation.

We will recall some concepts which can be found in the literature [7, 21, 40, 66, 67] concerning some algebraic structures associated to each solution, or more generally, to each bijection $r : X^2 \longrightarrow X^2$. We follow the notation of [40].

3.1.14 Definition. Let X be a non-empty set and $r : X^2 \longrightarrow X^2$ a bijection.

- The *set of relations* [1] *associated to* (X, r) is

$$\Re(X, r) = \{xy = \hat{y}\check{x} \;/\; r(xy) = \hat{y}\check{x} \text{ in } X^2\}.$$

- The semigroup $\mathcal{S}(X, r)$ generated by X with defining relations $\Re(X, r)$, is called the *semigroup associated to* (X, r).

- The *group associated to* (X, r) is the group $\mathcal{G}(X, r)$ generated by X with defining relations $\Re(X, r)$. If (X, r) is a solution, then $\mathcal{G}(X, r)$ is also called the *structure group* of (X, r).

- For a field k, the k-*algebra associated to* (X, r), denoted by $\mathcal{A}(\mathsf{k}, X, r)$, is defined as the k-algebra generated by X with defining relations $\Re(X, r)$, i.e., $\mathcal{A}(\mathsf{k}, X, r)$ is the factor algebra

$$\frac{\mathsf{k}\langle X\rangle}{\mathsf{k}\langle X\rangle \langle\, xy - \hat{y}\check{x} \;/\; r(xy) = \hat{y}\check{x} \text{ in } X^2 \,\rangle_{\mathsf{k}\langle X\rangle}}.$$

3.1.15 Notation. *From here on, the symbol $*$ in a relation of $\Re(X, r)$ will mean the existence of a variable which satisfies the relation, for instance, we will write $xy = z* \in \Re(X, r)$ if, and only if, there exists $t \in X$ such that $xy = zt \in \Re(X, r)$.*

Based on the notion of *Yang-Baxter Algebra* given by Manin [68] consisting in any quadratic algebra with defining relations determined by a Yang-Baxter operator, T. Gateva-Ivanova introduced in [40] the following concepts.

3.1.16 Definition. If (X, r) is a square-free solution, then $\mathcal{S}(X, r)$, $\mathcal{G}(X, r)$ and $\mathcal{A}(\mathsf{k}, X, r)$ are respectively called the *Yang-Baxter semigroup*, the *Yang-Baxter group* and the *Yang-Baxter Algebra* associated to (X, r) [2].

3.1.17 Example. If $X = \{x_1, \ldots, x_n\}$ and r is the trivial solution (see 3.1.9), then $\mathcal{S}(X, r)$ is the *free abelian semigroup* $[x_1, \ldots, x_n]$ generated by X, $\mathcal{G}(X, r)$ is the *free abelian group* $\mathbb{Z}^X$ generated by X, and the Yang-Baxter Algebra $\mathcal{A}(\mathsf{k}, X, r)$ is the commutative polynomial ring $\mathsf{k}[x_1, \ldots, x_n]$.

[1] Some authors (see e.g. [40]) remove from $\Re(X, r)$ the relations "$xy = \hat{y}\check{x}$" when $x = \hat{y}$ and $y = \check{x}$ Note that in that case the associated structures $\mathcal{S}(X, r)$, $\mathcal{G}(X, r)$ and $\mathcal{A}(\mathsf{k}, X, r)$ are exactly the same as the ones defined above.

[2] Sometimes square-freeness is not required in the definitions of Yang-Baxter semigroup, Yang-Baxter group and Yang-Baxter Algebra (e.g., [40]).

3.1.18 Note. It is proved in [42] that if (X,r) is a square-free solution, then the semigroup $\mathcal{S}(X,r)$ is (left and right) *cancelative*, that is, $\forall\ g,g',h \in \mathcal{S}(X,r)$,

$$(gh = g'h \ \text{ or } \ hg = hg') \implies g = g'$$

Furthermore, it can also be extracted from the results of [42], that each element $g \in \mathcal{G}(X,r)$ can be presented as $g = u^{-1}v$, for some $u,v \in \mathcal{S}(X,r)$.

The proof of Theorem 3.1.19 can be found in [40].

3.1.19 Theorem. *Let $X = \{x_1,\dots,x_n\}$ and $r : X^2 \longrightarrow X^2$ be a bijection represented by its components as $r(xy) = \mathcal{L}_x(y)\mathcal{R}_y(x)$ for $x,y \in X$. Consider the following properties:*

1. (a) *(X,r) is left nondegenerate, that is, $\mathcal{L}_x$ is bijective $\forall x \in X$;*
   (b) *(X,r) is right nondegenerate, i.e., $\mathcal{R}_y$ is bijective $\forall y \in X$;*
2. (a) *(Right Ore condition) $\forall\, a,b \in X$, $\exists!\ x,y \in X$ such that $ax = by \in \Re(X,r)$;*
   (b) *(Left Ore condition) $\forall\ a,b \in X$, $\exists!\ t,z \in X$ such that $za = tb \in \Re(X,r)$;*
3. *(X,r) is square-free;*
4. (a) *$\mathcal{L}_x(y) \neq x$, $\forall\ y \neq x$;*
   (b) *$\mathcal{R}_y(x) \neq y$, $\forall\ x \neq y$;*
5. *For all $x,y \in X$, if $xy = \hat{y}\check{x} \in \Re(X,r)$, then*
   (a) *the relations $x\hat{y} = *\check{x}$, $\check{x}y = \hat{y}*$, $\hat{y}x = *y$, $y\check{x} = x*$ are in $\Re(X,r)$, that is, $\mathcal{R}_{\hat{y}}(x) = \mathcal{R}_y(x)$, $\mathcal{L}_{\check{x}}(y) = \mathcal{L}_x(y)$, $\mathcal{R}_x(\hat{y}) = \mathcal{R}_{\check{x}}(\hat{y})$, and $\mathcal{L}_y(\check{x}) = \mathcal{L}_{\hat{y}}(\check{x})$;*
   (b) *there exists $z,t \in X$ such that $xxy = z\check{x}\check{x}$ in $\mathcal{S}(X,r)$ and $xyy = \hat{y}\hat{y}t$ in $\mathcal{S}(X,r)$;*
6. (Cyclic condition, T. Gateva-Ivanova, [38])
   For all $x \neq y \in X$ there exists a unique pair of disjoint cycles $(\mathcal{L}_y^x, \mathcal{L}_x^y)$ called pair of relative cycles, $\mathcal{L}_y^x = (x_1x_2\cdots x_k)$ with $x = x_1$ and $\mathcal{L}_x^y = (y_1y_2\cdots y_m)$ with $y = y_1$, such that for $1 \leq i \leq k$, $1 \leq j \leq m$

$$r(x_iy_j) = \sigma(y_j)\sigma^{-1}(x_i), \quad r(y_jx_i) = \sigma(x_i)\sigma^{-1}(y_j), \tag{3.5}$$

   where $\sigma = \mathcal{L}_y^x\mathcal{L}_x^y$.
   (Note that $\mathcal{L}_{y_j}^{x_i} = \mathcal{L}_y^x$ and $\mathcal{L}_{x_i}^{y_j} = \mathcal{L}_x^y$, for all $1 \leq i \leq k$, $1 \leq j \leq m$).

Then,

A) 1a is equivalent to 2a, and 1b is equivalent to 2b.

B) Assuming 1, the statements 3 and 4 are equivalent.

C) If (X,r) is a braided set satisfying 1 and 3, then 5 holds.

D) If r is involutive, then the statements 5 and 6 are equivalent.

3.1.20 Corollary. *Every square-free solution of the YBE satisfies the conditions 1 to 6 of Theorem 3.1.19.*

It is well-known that there exist left and right actions of the group $\mathcal{G}(X,r)$ associated to any solution (X,r) on the set X, as the following result shows.

3.1.21 Proposition. [21] *Let (X,r) be a nondegenerate braided set. Assume that r is represented by its components as $r(xy) = \mathcal{L}_x(y)\mathcal{R}_y(x)$ for $x,y \in X$. The group homomorphism $\mathcal{L} : \mathcal{G}(X,r) \longrightarrow \mathrm{Sym}(X)$; $x \mapsto \mathcal{L}_x$ induces the left action of $\mathcal{G}(X,r)$ on the set X given by:*

$$\begin{aligned} &\mathcal{G}(X,r) \times X \longrightarrow X \\ &(x_{i_1} \cdots x_{i_s}, y) \;\mapsto\; \mathcal{L}_{x_{i_1}\cdots x_{i_s}}(y) = (\mathcal{L}_{x_{i_1}} \circ \cdots \circ \mathcal{L}_{x_{i_s}})(y). \end{aligned}$$

Similarly, the group homomorphism $\mathcal{R} : \mathcal{G}(X,r) \longrightarrow \mathrm{Sym}(X)$; $x \mapsto \mathcal{R}_x$ induces a right action of $\mathcal{G}(X,r)$ on X.

Proof. Consider the YB diagram

$$\begin{array}{ccc} x\ y\ z & \xrightarrow{\quad r_2 \quad} & x\ \mathcal{L}_y(z)\ \mathcal{R}_z(y) \\ {\scriptstyle r_1}\downarrow & & \downarrow{\scriptstyle r_1} \\ \mathcal{L}_x(y)\ \mathcal{R}_y(x)\ z & & \mathcal{L}_x\mathcal{L}_y(z)\ \mathcal{R}_{\mathcal{L}_y(z)}(x)\ \mathcal{R}_z(y) \\ {\scriptstyle r_2}\downarrow & & \vdots{\scriptstyle r_2} \\ \mathcal{L}_x(y)\ \mathcal{L}_{\mathcal{R}_y(x)}(z)\ \mathcal{R}_z\mathcal{R}_y(x) & \xrightarrow{r_1} & \mathcal{L}_{\mathcal{L}_x(y)}\mathcal{L}_{\mathcal{R}_y(x)}(z)\ \mathcal{R}_{\mathcal{L}_{\mathcal{R}_y(x)}(z)}\mathcal{L}_x(y)\ \mathcal{R}_z\mathcal{R}_y(x) \end{array}$$

From the last r_2-arrow we obtain that $\mathcal{L}_x\mathcal{L}_y = \mathcal{L}_{\mathcal{L}_x(y)}\mathcal{L}_{\mathcal{R}_y(x)}$. The proof easily follows. □

These and other actions of the group $\mathcal{G}(X,r)$ are studied in detail in [40] in the case when (X,r) is a square-free solution.

3.1.22 Notation. *Let (X,r) be a solution and $y \in X$. We denote by $\mathcal{O}_y$ the orbit of y under the left action of $\mathcal{G}(X,r)$ on X, i.e.,*

$$\mathcal{O}_y = \{\mathcal{L}_g(y) \,/\, g \in \mathcal{G}(X,r)\}.$$

3.1.23 Remark. Proposition 3.1.21 is a consequence of the following more general result of [21]. Let (X,r) be a nondegenerate set. Then (X,r) is braided if, and only if, the following conditions are simultaneously satisfied:

i) The assignment $x \mapsto \mathcal{R}_x$ provides a right action of $\mathcal{G}(X,r)$ on X;

ii) The assignment $x \mapsto \mathcal{L}_x$ provides a left action of $\mathcal{G}(X,r)$ on X;

iii) the linking relation

$$\mathcal{R}_{\mathcal{L}_{\mathcal{R}_y(x)}(z)}(\mathcal{L}_x(y)) = \mathcal{L}_{\mathcal{R}_{\mathcal{L}_y(z)}(x)}(\mathcal{R}_z(y))$$

holds for all $x,y,z \in X$.

3.1.24 Proposition. [40] *Let (X,r) be a square-free solution of the YBE.*

1. *With the notation of the statement 6 in 3.1.19, for a fixed $x \in X$, let $\mathcal{L}_x^{y_1},\ldots,\mathcal{L}_x^{y_m}$ be all the cycles in $\mathrm{Sym}(X)$ associated to the pair (x,y_i) for all $y_i \in X$, $y_i \neq x$. Then,*

$$\mathcal{L}_x = (x)\cdot \mathcal{L}_x^{y_1}\cdots\mathcal{L}_x^{y_m};$$

2. *For all $x \in X$,*

$$\mathcal{R}_x = \mathcal{L}_x^{-1};$$

3. *For all $x,y \in X$,*

$$r(x,y) = (\mathcal{L}_x(y), \mathcal{L}_y^{-1}(x)).$$

Consequently, every square-free solution (X,r) is uniquely determined by the left action $\mathcal{L}$ of $G(X,r)$ on X, or more precisely, by the set

$$\{\mathcal{L}_x \,/\, x \in X\}.$$

3.1.2 Representations of square-free solutions

In this section we show some ways, proposed by T. Gateva-Ivanova, of representing any square-free solution (X,r): by using cycles of $\mathrm{Sym}(X)$, via the left action of $\mathcal{G}(X,r)$ on X, and geometrically by drawing its associated *graph*. To illustrate these methods, we will see how the following square-free solution can be represented by using each of them.

Let $X = \{x_1, \ldots, x_6\}$. Consider the square-free solution of the Yang-Baxter equation defined as the map $r : X^2 \longrightarrow X^2$ satisfying $r^2 = \mathrm{Id}_{X^2}$, $r(x_ix_i) = x_ix_i$ for $1 \leq i \leq 6$, and

$$\begin{array}{lll} r(x_1x_2) = x_2x_1, & r(x_1x_3) = x_4x_2, & r(x_1x_4) = x_3x_2, \\ r(x_1x_5) = x_6x_4, & r(x_1x_6) = x_5x_4, & r(x_2x_3) = x_4x_1, \\ r(x_2x_4) = x_3x_1, & r(x_2x_5) = x_6x_3, & r(x_2x_6) = x_5x_3, \\ r(x_3x_4) = x_4x_3, & r(x_3x_5) = x_6x_2, & r(x_3x_6) = x_5x_2, \\ r(x_4x_5) = x_6x_1, & r(x_4x_6) = x_5x_1, & r(x_5x_6) = x_6x_5. \end{array} \tag{3.6}$$

• **The set of pairs of relative cycles.**

Analogously as in Example 3.1.4, the set of relations $\Re(X, r)$ of any square-free solution can be represented by using cycles of $\mathrm{Sym}(X)$. More precisely, according to the Cyclic Condition, to each square-free solution (X, r) one can associate a set of products of cycles of type $\sigma = \mathcal{L}_y^x \mathcal{L}_x^y \in \mathrm{Sym}(X)$ for all $x, y \in X$ which determines r uniquely.

3.1.25 Definition. Let (X, r) be a square-free solution of the YBE where $X = \{x_1, \ldots, x_n\}$. The *set of pairs of relative cycles* of (X, r) is defined as

$$\mathcal{C}(X, r) = \{\sigma_{ij} = \mathcal{L}_{x_i}^{x_j} \mathcal{L}_{x_j}^{x_i} \,/\, 1 \leq i < j \leq n\},$$

where $(\mathcal{L}_{x_i}^{x_j}, \mathcal{L}_{x_j}^{x_i})$ is the pair of relative cycles associated to x_i, x_j obtained from the Cyclic Condition (statement 6 of 3.1.19).

Note from 3.1.25 that any square-free solution (X, r) is well determined by $\mathcal{C}(X, r)$ since

$$r(x_ix_j) = \sigma_{ij}(x_j)\sigma_{ij}^{-1}(x_i), \quad r(x_jx_i) = \sigma_{ij}(x_i)\sigma_{ij}^{-1}(x_j),$$

for all $x_i, x_j \in X$ with $i < j$.

3.1.26 Convention. *We will often omit in the set $\mathcal{C}(X, r)$ the products of relative cycles of type $\sigma_{ij} = (x_i)(x_j)$, i.e., the pairs of relative cycles associated to $x_i, x_j \in X$ such that $r(x_ix_j) = x_jx_i$.*

3.1.27 Example. For the square-free solution (X, r) of the YBE given in (3.6), the pairs of relative cycles are

$$\begin{array}{ll} \mathcal{L}_{x_2}^{x_1} = (x_1), & \mathcal{L}_{x_1}^{x_2} = (x_2), \\ \mathcal{L}_{x_4}^{x_3} = (x_3), & \mathcal{L}_{x_3}^{x_4} = (x_4), \\ \mathcal{L}_{x_6}^{x_5} = (x_5), & \mathcal{L}_{x_5}^{x_6} = (x_6), \\ \mathcal{L}_{x_3}^{x_1} = \mathcal{L}_{x_4}^{x_1} = \mathcal{L}_{x_3}^{x_2} = \mathcal{L}_{x_4}^{x_2} = (x_1x_2), & \mathcal{L}_{x_1}^{x_3} = \mathcal{L}_{x_1}^{x_4} = \mathcal{L}_{x_2}^{x_3} = \mathcal{L}_{x_2}^{x_4} = (x_3x_4), \\ \mathcal{L}_{x_5}^{x_1} = \mathcal{L}_{x_6}^{x_1} = \mathcal{L}_{x_5}^{x_4} = \mathcal{L}_{x_6}^{x_4} = (x_1x_4), & \mathcal{L}_{x_1}^{x_5} = \mathcal{L}_{x_1}^{x_6} = \mathcal{L}_{x_4}^{x_5} = \mathcal{L}_{x_4}^{x_6} = (x_5x_6), \\ \mathcal{L}_{x_5}^{x_2} = \mathcal{L}_{x_6}^{x_2} = \mathcal{L}_{x_5}^{x_3} = \mathcal{L}_{x_6}^{x_3} = (x_2x_3), & \mathcal{L}_{x_2}^{x_5} = \mathcal{L}_{x_2}^{x_6} = \mathcal{L}_{x_3}^{x_5} = \mathcal{L}_{x_3}^{x_6} = (x_5x_6). \end{array}$$

Therefore,

$$\mathcal{C}(X,r) = \{(x_6x_5)(x_3x_2), (x_6x_5)(x_4x_1), (x_4x_3)(x_2x_1)\}.$$

• **The left action of the Yang-Baxter Group $\mathcal{G}(X,r)$ on X.**
By 3.1.24, any square-free solution (X,r) of the YBE is uniquely determined by the set $\{\mathcal{L}_x \,/\, x \in X\}$. Moreover, if for a fixed $x \in X$ we write

$$\{\mathcal{L}_x^{y_1}, \ldots, \mathcal{L}_x^{y_m}\} = \{\mathcal{L}_x^y \,/\, (\mathcal{L}_x^y, \mathcal{L}_y^x) \text{ is a pair of relative cycles, } y \in X \setminus \{x\}\},$$

then

$$\mathcal{L}_x = (x) \cdot \mathcal{L}_x^{y_1} \cdots \mathcal{L}_x^{y_m}.$$

3.1.28 Example. The square-free solution (X,r) defined in (3.6) is represented via the left action of $\mathcal{G}(X,r)$ on X by

$$\begin{cases} \mathcal{L}_{x_1} = (x_1)(x_2)(x_3x_4)(x_5x_6), \\ \mathcal{L}_{x_2} = (x_1)(x_2)(x_3x_4)(x_5x_6), \\ \mathcal{L}_{x_3} = (x_1x_2)(x_3)(x_4)(x_5x_6), \\ \mathcal{L}_{x_4} = (x_1x_2)(x_3)(x_4)(x_5x_6), \\ \mathcal{L}_{x_5} = (x_1x_4)(x_2x_3)(x_5)(x_6), \\ \mathcal{L}_{x_6} = (x_1x_4)(x_2x_3)(x_5)(x_6). \end{cases}$$

• **Graphs.**
The particular behaviour of square-free solutions of the YBE allow us to represent them by using graphs (cf. [39]), or more precisely, *pseudodigraphs* i.e., directed graphs for which parallel edges and loops are allowed. The pseudodigraph $\mathcal{T}(X,r)$ or, as we will refer from here on, the *graph* associated to each square-free solution (X,r) reflects the properties of (X,r), and it is useful for symbolic computation. Graph terminology used here can be found in [15, 16, et al.].

3.1.29 Definition. Let (X,r) be a square-free solution of the YBE. The *graph* $\mathcal{T}(X,r)$ *associated to* (X,r) is the pseudodigraph defined as follows:

- Set of vertices: X,
- Set of edges: for $a, x, y \in X$, there is an edge $x \xrightarrow{a} y$ from the vertex "x" to the vertex "y" if, and only if, $\mathcal{L}_a(x) = y$, or equivalently, if $ax = y* \in \Re(X,r)$.

3.1.30 Convention. *To draw the graph $\mathcal{T}(X,r)$, we shall consider:*

1. *We will rarely draw* loops *(closed edges) $x \xrightarrow{a} x$;*

2. *When $\mathcal{L}_a(x) = y$ and $\mathcal{L}_a(y) = x$, we will draw one edge in both directions $x \overset{a}{\leftrightarrow} y$ instead of two edges $x \overset{a}{\rightarrow} y$ and $x \overset{a}{\leftarrow} y$;*

3. *Notation $x \overset{\{a_1,\ldots,a_k\}}{\longrightarrow} y$ will be used whenever $\mathcal{L}_{a_i}(x) = y$ for all $i \in \{1,\ldots,k\}$, and we will draw $x \overset{\{a_1,\ldots,a_k\}}{\longleftrightarrow} y$ only if all a_i are edges in both directions, or equivalently, when $\mathcal{L}^x_{a_i} = \mathcal{L}^y_{a_i} = (xy)$, $1 \leq i \leq k$.*

Clearly the graph $\mathcal{T}(X,r)$ of a square-free solution (X,r) reflects the properties of the action of the Yang-Baxter group $\mathcal{G}(X,r)$ on X. In particular, each orbit $\mathcal{O}_y$ (with $y \in X$) corresponds to a connected component of $\mathcal{T}(X,r)$, more precisely, to that which contains the labelled vertex y.

3.1.31 Example. The graph $\mathcal{T}(X,r)$ associated to the square-free solution (X,r) defined in (3.6) is given by figure 3.1. We can observe that $\mathcal{T}(X,r)$ consists of two connected components, corresponding to the orbits

$$\mathcal{O}_{x_1} = \{x_1, x_2, x_3, x_4\}, \quad \mathcal{O}_{x_5} = \{x_5, x_6\}$$

under the left action $\mathcal{L}$ of $\mathcal{G}(X,r)$ on X.

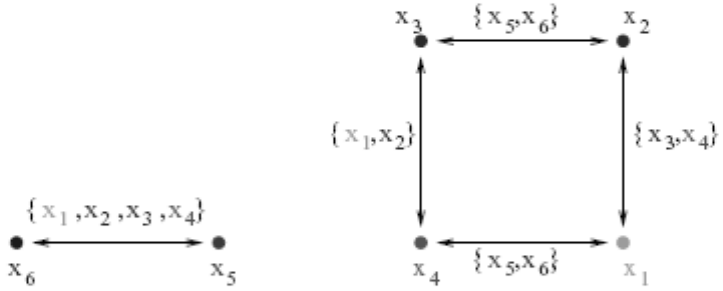


Figure 3.1: Graph of the square-free solution described in (3.6).

We propose the following definition for isomorphism between graphs associated to square-free solutions.

3.1.32 Definition. Let (X,r_X), (Y,r_Y) be square-free solutions of the YBE. We say that their associated graphs $\mathcal{T}(X,r_X)$, resp. $\mathcal{T}(Y,r_Y)$ are *isomorphic* if, and only if, there exists a bijective map $\phi : X \longrightarrow Y$ such that

$$x_1 \overset{a}{\rightarrow} x_2 \text{ is an edge of } \mathcal{T}(X,r_X) \iff \phi(x_1) \overset{\phi(a)}{\rightarrow} \phi(x_2) \text{ is an edge of } \mathcal{T}(Y,r_Y).$$

Note that this relation is an equivalence relation in the set of graphs of square-free solutions. We will prove later, in 3.2.5, that two square-free solutions (X,r_X) and (Y,r_Y) are isomorphic if, and only if, their graphs $\mathcal{T}(X,r_X)$ and $\mathcal{T}(Y,r_Y)$ are isomorphic.

3.1.3 Classification of square-free solutions

For a fixed finite set X, finding all solutions defined on X is a natural but difficult task in the study of the set-theoretic solutions of the YBE. One of the most relevant results appearing in the literature so far was found in [21], where the authors find all solutions defined on a set X with $|X| \leq 6$, by using a computer.

Given an arbitrary finite set X, the aim of classifying square-free solutions of the YBE defined on X is to find all possible square-free solutions (X, r) up to isomorphisms, or in other words, to give the set of representatives of all equivalence classes under the isomorphism relation $\sim$ (see 3.1.12). We will take into account (as it will be pointed out in 3.2.5) that two square-free solutions (X, r_1) and (X, r_2) are isomorphic if, and only if, they have isomorphic graphs $\mathcal{T}(X, r_1)$, $\mathcal{T}(X, r_2)$, or equivalently, if their sets of pairs of relative cycles $\mathcal{C}(X, r_1)$ and $\mathcal{C}(X, r_2)$ are the same after possibly re-indexing the variables of X for one of them.

If (X, r) is a square-free solution with $X = \{x_1, \ldots, x_n\}$, we denote by m the *maximum of lengths of all cycles* ocurring in $\mathcal{C}(X, r)$. A method to classify the square-free solutions defined on X, first proposed by T. Gateva-Ivanova, consists in splitting up the study in different cases depending on m. More precisely, it starts studying all possible square-free solutions with $\mathsf{m} = n - 1$, i.e., the square-free solutions $r : X^2 \longrightarrow X^2$ for which $(x_n)(x_{n-1}x_{n-2}\cdots x_1) \in \mathcal{C}(X, r)$. The following step consists in studying the case $\mathsf{m} = n-2$, and so on until $\mathsf{m} = 2$. Note that $\mathsf{m} = 1$ corresponds with the trivial solution $r = \mathrm{Id}_{X^2}$.

Next we will show some technical properties, useful in the computations required by this method of classifying square-free solutions.

3.1.33 Lemma. *Let (X, r) be a square-free solution of the YBE, and $a \neq x$ arbitrary elements of X, whose associated pair of relative cycles is $(\mathcal{L}_a^x = (x_1 x_2 \cdots x_m), \mathcal{L}_x^a)$ where $x = x_1$.*

1. *If $x_j x_i = x_k x_l \in \Re(X, r)$ for some $1 \leq k, l \leq m$, then*

$$x_{j+p} x_{i+p} = x_{k+p} x_{l+p} \in \Re(X, r), \ \forall\, p \geq 0;$$

2. *If $\mathcal{L}_a^x$ is an invariant cycle (i.e., for all x_i, $x_j \in \mathcal{L}_a^x$, it holds that $x_j x_i = x_k x_l \in \Re(X, r)$ for some x_k, $x_l \in \mathcal{L}_a^x$), and we know the relations*

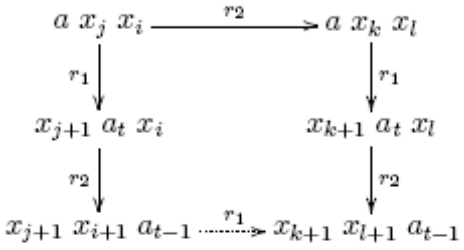
$$\begin{aligned} x_1 x_2 &= x_{k_2} x_{l_2} \in \Re(X, r) \\ &\vdots \\ x_1 x_m &= x_{k_m} x_{l_m} \in \Re(X, r), \end{aligned}$$

then

$$x_j x_i = x_{k_{i-j+1}+j-1} x_{l_{i-j+1}+j-1} \in \Re(X,r),\ \forall\, 1 \le i,j \le m.$$

where the indexes "s" of the variables x_s are taken modulo m.

Proof. Let us prove the statement 1. If we write $\mathcal{L}_x^a = (a_1 a_2 \cdots a_t)$ with $a_1 = a$, then from the dotted r_1-arrow of the YB diagram



it holds that $x_{j+1}x_{i+1} = x_{k+1}x_{l+1} \in \Re(X,r)$. Hence, the proof easily finishes using induction.

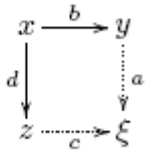
The statement 2 is a consequence of 1. Indeed,

$$x_1 x_{i-j+1} = x_{k_{i-j+1}} x_{l_{i-j+1}} \in \Re(X,r) \implies x_2 x_{i-j+2} = x_{k_{i-j+1}+1} x_{l_{i-j+1}+1}.$$

Repeating this process $j-2$ times we complete the proof. □

3.1.34 Lemma. *Let (X,r) be a square-free solution, and let a,b,c,d,x,y,z, $t \in X$ (not necessarily pairwise distinct).*

1. *If $ab = cd \in \Re(X,r)$, $\mathcal{L}_b(x) = y$, and $\mathcal{L}_d(x) = z$, then there exists $\xi \in X \setminus \{a,c\}$ such that $\mathcal{L}_a(y) = \xi$ and $\mathcal{L}_c(z) = \xi$. The square*

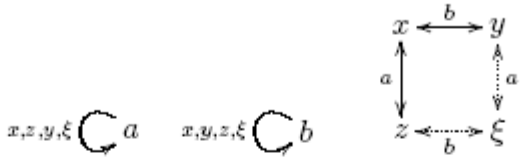


   is included in the graph $\mathcal{T}(X,r)$.

   Moreover, if $z \neq c$ then $\xi \neq c$, and analogously, if $y \neq a$ then $\xi \neq a$;

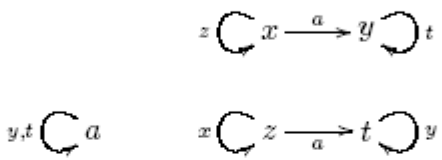
2. *If $y \notin \{a,x,z\}$, $z \notin \{b,x,y\}$, $ab = ba \in \Re(X,r)$, $\mathcal{L}_x^a = \mathcal{L}_z^a = (a)$, $\mathcal{L}_a^x = \mathcal{L}_a^z = (xz)$, $\mathcal{L}_x^b = \mathcal{L}_y^b = (b)$, and $\mathcal{L}_b^x = \mathcal{L}_b^y = (xy)$, then there*

exists $\xi \in X \setminus \{a, b, x, y, z\}$ *such that* $\mathcal{L}_y^a = \mathcal{L}_\xi^a = (a)$, $\mathcal{L}_a^y = \mathcal{L}_a^\xi = (y\xi)$, $\mathcal{L}_z^b = \mathcal{L}_\xi^b = (b)$, *and* $\mathcal{L}_b^z = \mathcal{L}_b^\xi = (z\xi)$, *i.e., the subgraph*



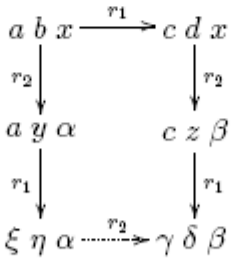
is included in $\mathcal{T}(X, r)$.

3. *If* $a \notin \{x, y, z, t\}$ *and* $ax = ya$, $az = ta$, $xz = zx \in \Re(X, r)$, *then* $yt = ty \in \Re(X, r)$, *i.e.,*



are arrows of $\mathcal{T}(X, r)$.

Proof. Let us prove 1. Let $\alpha, \beta, \xi, \gamma, \delta \in X$ such that $bx = y\alpha$, $dx = z\beta$, $ay = \xi\eta$, $cz = \gamma\delta \in \Re(X, r)$. From the YB diagram,



We have $\gamma = \xi$ and so, $cz = \xi\delta$. Since (X, r) is square-free, $\xi \neq c$ whenever $z \neq c$, and $\xi \neq a$ whenever $y \neq a$.

Now let us prove 2. Similarly as in 1, there exists $\xi \in X \setminus \{a, b\}$ such that $ay = \xi\eta$, $bz = \xi\delta$ and $\eta b = \delta a$ are in $\Re(X, r)$. From the last relation, $ab = \delta * \in \Re(X, r)$ and $ba = \eta * \in \Re(X, r)$, but since $ab = ba \in \Re(X, r)$, then $\delta = b$ and $\eta = a$. Hence, $ay = \xi a \in \Re(X, r)$ and $bz = \xi b \in \Re(X, r)$. Moreover $\xi \neq y$, because otherwise the relations $bz = yb$ and $bx = yb$ would

imply $y = x$. Analogously, $\xi \neq z$. Now, from the YB diagram

$$\begin{array}{ccc} a\ b\ y & \xrightarrow{r_2} & a\ x\ b \\ {\scriptstyle r_1}\downarrow & & \downarrow{\scriptstyle r_1} \\ b\ a\ y & & z\ a\ b \\ {\scriptstyle r_2}\downarrow & & \downarrow{\scriptstyle r_2} \\ b\ \xi\ a & \overset{r_1}{\dashrightarrow} & z\ b\ a \end{array}$$

we obtain that $b\xi = zb$. Therefore, $\mathcal{L}_z^b = \mathcal{L}_\xi^b = (b)$, $\mathcal{L}_b^z = \mathcal{L}_b^\xi = (z\xi)$. Similarly,

$$\begin{array}{ccc} a\ z\ b & \xrightarrow{r_1} & x\ a\ b \\ {\scriptstyle r_2}\downarrow & & \downarrow{\scriptstyle r_2} \\ a\ b\ \xi & & x\ b\ a \\ {\scriptstyle r_1}\downarrow & & \downarrow{\scriptstyle r_1} \\ b\ a\ \xi & \overset{r_2}{\dashrightarrow} & b\ y\ a \end{array}$$

implies $\mathcal{L}_y^a = \mathcal{L}_\xi^a = (a)$, $\mathcal{L}_a^y = \mathcal{L}_a^\xi = (y\xi)$. Finally, $\xi \neq x$ because otherwise, from $bx = zb \in \Re(X, r)$ and $bx = yb \in \Re(X, r)$, we would obtain that $y = z$ - a contradiction.
The assertion 3 follows from the YB diagram:

$$\begin{array}{ccc} a\ x\ z & \xrightarrow{r_2} & a\ z\ x \\ {\scriptstyle r_1}\downarrow & & \downarrow{\scriptstyle r_1} \\ y\ a\ z & & t\ a\ x \\ {\scriptstyle r_2}\downarrow & & \downarrow{\scriptstyle r_2} \\ y\ t\ a & \overset{r_1}{\dashrightarrow} & t\ y\ a \end{array}$$

□

In the next example we show how the previous properties can be applied in order to determine the classification of square-free solutions for a given finite set X.

3.1.35 Example. Let us classify all square-free solutions of the YBE defined on a set $X = \{x_1, x_2, x_3x_4\}$ of 4 elements by following the method explained above.

- In the case $\mathsf{m} = 3$ there is a cycle of length 3, namely, $(x_4)(x_3x_2x_1) \in \mathcal{C}(X, r)$. Note that the cycle $(x_3x_2x_1)$ is invariant (i.e., for all $i, j \in$

$\{1,2,3\}$, $r(x_jx_i) = x_kx_l$ for some $k,l \in \{1,2,3\}$). We distinguish three cases:

A) If $x_3x_1 = x_3* \in \Re(X,r)$, then by virtue of 5 in 3.1.19, $x_3x_3 = *x_1 \in \Re(X,r)$ - a contradiction.

B) If $x_3x_1 = x_2* \in \Re(X,r)$, then by the statement 1 of 3.1.33, we get $x_3x_1 = *x_2 \in \Re(X,r)$, which, together with $x_1x_2 = x_3* \in \Re(X,r)$, implies $x_3x_1 = x_2x_2 \in \Re(X,r)$ - a contradiction.

C) If $x_3x_1 = x_1* \in \Re(X$ relation $x_3x_1 = x_1x_1$ implies, by 3.1.33, t Therefore, $x_3x_1 = x_1$ 1 of 3.1.33, we have $x_3x_2 \in \Re(X,r)$. Th such that

C

, r), then $x_3x_1 = x_1x_3 \in \Re(X,r)$. Indeed, the is not possible, and $x_3x_1 = x_1x_2 \in \Re(X,r)$ hat $x_1x_2 = x_2x_3 \in \Re(X,r)$ - a contradiction. $x_3 \in \Re(X,r)$, and by virtue of the statement it holds $x_1x_2 = x_2x_1 \in \Re(X,r)$ and $x_2x_3 =$ as, there exists a square-free solution (X,r_1)

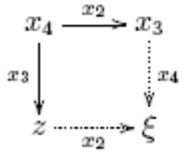
$(X,r_1) = \{(x_4)(x_3x_2x_1)\}$.

ossible cases:

X,r), then there are three possibilities: $x_4x_3 =$ $x_3 = x_2x_1 \in \Re(X,r)$ and $x_4x_3 = x_3x_4 \in$ rst two options are not possible. If we as- ne, we have by the property 5 of 3.1.19 that r) - a contradiction. Thus, $x_4x_3 = x_3x_4 \in$ e, the relation $x_1x_2 = **$ has to be the com- relations determine the square-free solution n terms of pairs of relative cycles by

$(X,r_2) = \{(x_4x_3)(x_2x_1)\}$.

r), then applying the property 1 of 3.1.34 to $x_2x_3 \in \Re(X,r)$, we get



$x_4\}$ satisfies $x_4x_3 = \xi* \in \Re(X,r)$ and $x_2z =$ hat $x_3x_4 = z* \in \Re(X,r)$ and $z \notin \{x_2,x_3\}$.

- If $m = 2$, there are two p

A) If $(x_4x_3)(x_2x_1) \in \mathcal{C}(X$ $x_1x_2 \in \Re(X,r)$, x_4 $\Re(X,r)$. But the fi sume e.g. the first o $x_2x_3 = x_1* \in \Re(X,$ $\Re(X,r)$ and therefo mutative one. These (X,r_2) represented i

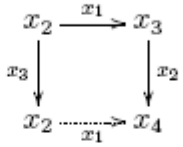
C

B) If $(x_4x_3)(x_2) \in \mathcal{C}(X,$ the relation $x_4x_2 =$

where $\xi \in X \setminus \{x_2,$ $\xi* \in \Re(X,r)$. Note t

B.1) If $\xi = x_3$, then z has to be x_4, otherwise $x_2x_1 = x_3* \in \Re(X,r)$ implies that $x_3x_2 = *x_1 \in \Re(X,r)$ - a contradiction. Thus, the relation $x_4x_3 = x_3*$ together with $x_3x_4 = x_4* \in \Re(X,r)$ (which implies $x_4x_3 = *x_4 \in \Re(X,r)$) provides the relation $x_3x_4 = x_4x_3 \in \Re(X,r)$. Looking at the remaining pairs of variables, we have three possibilities:

a) If $x_2x_1 = x_1x_3 \in \Re(X,r)$, then $x_3x_1 = x_1* \in \Re(X,r)$, but these relations do not provide any square-free solution, because if $x_3x_1 = x_1x_2 \in \Re(X,r)$, then from the dotted edge in the square



we get $x_1x_2 = x_4* \in \Re(X,r)$ - a contradiction; and similarly, the assumption of $x_3x_1 = x_1x_4 \in \Re(X,r)$ lead us to other contradiction.

b) The relation $x_2x_1 = x_1x_4 \in \Re(X,r)$ is not possible by reasons which are analogous to those in the previous case.

c) If $x_2x_1 = x_1x_2 \in \Re(X,r)$, then there are two possibilities:

c.i) If $x_3x_1 = x_1x_3 \in \Re(X,r)$, then $x_4x_1 = x_1x_4 \in \Re(X,r)$, and we obtain the square-free solution (X, r_3):

$$\mathcal{C}(X,r_3) = \{(x_4x_3)(x_2)\}.$$

c.ii) If $x_3x_1 = x_1x_4 \in \Re(X,r)$, then we can easily deduce that $x_4x_1 = x_1x_3 \in \Re(X,r)$. In this case we have the square-free solution (X, r_4):

$$\mathcal{C}(X,r_4) = \{(x_4x_3)(x_2), (x_4x_3)(x_1)\}.$$

B.2) If $\xi = x_1$, then $x_2z = x_1* \in \Re(X,r)$. Hence, $z \neq x_4$ and therefore, $z = x_1$. There are three cases:

a) If $x_3x_4 = x_1x_2 \in \Re(X,r)$, then $x_2x_4 = x_1* \in \Re(X,r)$ - a contradiction.

b) If $x_3x_4 = x_1x_3 \in \Re(X,r)$, then $x_4x_3 = x_3* \in \Re(X,r)$ - a contradiction.

c) If $x_3x_4 = x_1x_4 \in \Re(X,r)$, then $x_4x_4 = x_1* \in \Re(X,r)$ - a contradiction.

- The case $\mathsf{m} = 1$ provides the trivial solution (X, r_5), i.e.,

$$r_5(x_ix_j) = x_jx_i, \ \forall\, i,j.$$

3.2 Gluing solutions

In this section we first study the isomorphisms and automorphisms of square-free solutions. We use them later for devising effective methods to construct new solutions by gluing any two other solutions.

3.2.1 Isomorphisms and automorphisms of square-free solutions

Here we present the main results of the joint work [33], most of them obtained as generalizations of some previous results for automorphisms of square-free solutions proved in [25, Ch. 3]. As an improved alternative to the natural method of "checking the definition", we devise an algorithm to compute explicitly the automorphisms and the group of automorphism of square-free solutions, by introducing the notion of *star of a vertex*.

3.2.1 Lemma. *Let (X, r_X) and (Y, r_Y) be solutions. Let $\varphi : X \longrightarrow Y$ be a bijection. The following conditions are equivalent:*

a) φ is an isomorphism from (X, r_X) to (Y, r_Y);

b) for every $x \in X$ it hold

$$\varphi \circ \mathcal{L}_x = \mathcal{L}_{\varphi(x)} \circ \varphi \quad \text{and} \quad \varphi \circ \mathcal{R}_x = \mathcal{R}_{\varphi(x)} \circ \varphi;$$

c)

$$x_1 x_2 = \hat{x}_2 \check{x}_1 \in \Re(X, r_X) \iff \varphi(x_1)\varphi(x_2) = \varphi(\hat{x}_2)\varphi(\check{x}_1) \in \Re(Y, r_Y); \tag{3.7}$$

Proof. It is straightforward from Definition 3.1.12, since $\varphi \in \mathrm{Is}(X, Y)$ if, and only if, for all $x_1 x_2 = \hat{x}_2 \check{x}_1 \in \Re(X, r_X)$ it holds that

$$r_Y(\varphi(x_1)\varphi(x_2)) = \varphi(\hat{x}_2)\varphi(\check{x}_1).$$

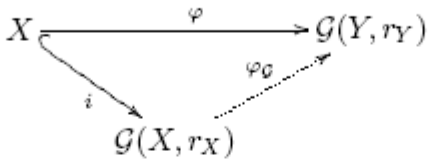
□

3.2.2 Proposition. *Any isomorphism $\varphi \in \mathrm{Is}(X, Y)$ of solutions (X, r_X), (Y, r_Y) can be extended to*

- *a semigroup isomorphism $\varphi_{\mathcal{S}} : \mathcal{S}(X, r_X) \longrightarrow \mathcal{S}(Y, r_Y)$ of their associated semigroups;*

- *a group isomorphism* $\varphi_{\mathcal{G}} : \mathcal{G}(X, r_X) \longrightarrow \mathcal{G}(Y, r_Y)$ *of their associated groups;*
- *an algebra isomorphism* $\varphi_{\mathcal{A}} : \mathcal{A}(k, X, r_X) \longrightarrow \mathcal{A}(k, Y, r_Y)$ *of their associated algebras.*

Proof. Let φ be an isomorphism from (X, r_X) to (Y, r_Y). Consider the diagram



where i denotes the inclusion map. From (3.7) in 3.2.1,

$$xa = a'x' \in \Re(X, r_X) \implies \varphi(x)\varphi(a) = \varphi(a')\varphi(x') \in \Re(Y, r_Y),$$

so there exists a group homomorphism

$$\begin{aligned} \varphi_{\mathcal{G}} : \mathcal{G}(X, r_X) &\longrightarrow \mathcal{G}(Y, r_Y) \\ x_{i_1} \cdots x_{i_s} &\mapsto \varphi(x_{i_1}) \cdots \varphi(x_{i_s}). \end{aligned}$$

Since $\varphi^{-1} \in \mathrm{Is}(Y, X)$, analogously one gets $(\varphi^{-1})_{\mathcal{G}} : \mathcal{G}(Y, r_Y) \longrightarrow \mathcal{G}(X, r_X)$, $(\varphi^{-1})_{\mathcal{G}}\ (y_{j_1} \cdots y_{j_t}) = \varphi^{-1}(y_{j_1}) \cdots \varphi^{-1}(y_{j_t})$. Since $(\varphi^{-1})_{\mathcal{G}} \circ \varphi_{\mathcal{G}} = \mathrm{Id}_{\mathcal{G}(X, r_X)}$ and $\varphi_{\mathcal{G}} \circ (\varphi^{-1})_{\mathcal{G}} = \mathrm{Id}_{\mathcal{G}(Y, r_Y)}$ we conclude that $\varphi_{\mathcal{G}}$ is a group isomorphism.
In a similar way, isomorphisms between the associated semigroups (and associated algebras) are constructed. □

3.2.3 Remark. By virtue of the statement 2 of 3.1.24 and 3.2.1, isomorphisms of square-free solutions may be characterized in a simpler way.
If (X, r_X), (Y, r_Y) are square-free solutions, then the bijection $\varphi : X \longrightarrow Y$ is an isomorphism if, and only if, for every $x \in X$ it holds

$$\varphi \circ \mathcal{L}_x = \mathcal{L}_{\varphi(x)} \circ \varphi. \tag{3.8}$$

Every isomorphism φ of two square-free solutions (X, r_X) and (Y, r_Y) is compatible with the Cyclic Condition (statement 6 of 3.1.19) in the sense that each pair of relative cycles of (X, r_X) is transformed under φ into a pair of relative cycles of (Y, r_Y) of the same lengths, and vice versa.

3.2.4 Lemma. *Let* (X, r_X) *and* (Y, r_Y) *be square-free solutions of the YBE, and let* $\varphi \in \mathrm{Is}(X, Y)$.

1. *There is an edge* $x_1 \stackrel{a}{\to} x_2$ *in the graph* $\mathcal{T}(X, r_X)$ *if, and only if,* $\varphi(x_1) \stackrel{\varphi(a)}{\to} \varphi(x_2)$ *is an edge of* $\mathcal{T}(Y, r_Y)$. *Furthermore, the following diagram*

$$\begin{array}{ccc} x_1 & \xrightarrow{\mathcal{L}_a} & x_2 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ \varphi(x_1) & \xrightarrow[\mathcal{L}_{\varphi(a)}]{} & \varphi(x_2) \end{array} \tag{3.9}$$

commutes, i.e., $\varphi(\mathcal{L}_a(x_1)) = \mathcal{L}_{\varphi(a)}(\varphi(x_1))$, *for all* $x_1, a \in X$.

2. *Let* $x \neq a \in X$. *The cycles* $\mathcal{L}_a^x = (x_1 x_2 \cdots x_k)$ *and* $\mathcal{L}_x^a = (a_1 a_2 \cdots a_m)$ *of* $\mathrm{Sym}(X)$ *are the pair of relative cycles associated to* $x, a \in X$ *if, and only if, the cycles*

$$\mathcal{L}_{\varphi(a)}^{\varphi(x)} = (\varphi(x_1)\varphi(x_2)\cdots\varphi(x_k)) \text{ and } \mathcal{L}_{\varphi(x)}^{\varphi(a)} = (\varphi(a_1)\varphi(a_2)\cdots\varphi(a_m))$$

of $\mathrm{Sym}(Y)$ *are the pair of relative cycles associated to* $\varphi(x), \varphi(a) \in Y$, *where* $x_1 = x$ *and* $a_1 = a$.

Proof. To prove the statement 1, use Eq. (3.8). Let us prove 2. Consider the relative cycles $\mathcal{L}_a^x = (x_1 x_2 \cdots x_k)$ and $\mathcal{L}_x^a = (a_1 a_2 \cdots a_m)$ with $x_1 = x$ and $a_1 = a$. As $a_j x_i = x_{i+1} a_{j-1} \in \Re(X, r_X)$ for all integers i, j (where x_i is $x_{i \,\mathrm{Mod}\, k}$ and a_j is $a_{j \,\mathrm{Mod}\, m}$). By virtue of (3.7) we have that

$$\varphi(a_j)\varphi(x_i) = \varphi(x_{i+1})\varphi(a_{j-1}) \in \Re(Y, r_Y).$$

Therefore, the cycles $\mathcal{L}_{\varphi(a)}^{\varphi(x)} = (\varphi(x_1)\varphi(x_2)\cdots\varphi(x_k))$, $\mathcal{L}_{\varphi(x)}^{\varphi(a)} = (\varphi(a_1)\varphi(a_2)\cdots\varphi(a_m))$, which have the same lengths of $\mathcal{L}_a^x$ and $\mathcal{L}_x^a$ respectively since φ is bijective, constitute the pair of relative cycles associated to $\varphi(a), \varphi(x)$. As $\varphi^{-1} \in \mathrm{Is}(Y, X)$, this also proves that if $\mathcal{L}_{\varphi(a)}^{\varphi(x)}$ and $\mathcal{L}_{\varphi(x)}^{\varphi(a)}$ are the pair of relative cycles associated to $\varphi(a), \varphi(x)$, then $\mathcal{L}_a^x$, $\mathcal{L}_x^a$ is the pair of relative cycles associated to a, x. □

In Theorem 3.2.5 we prove that isomorphisms of square-free solutions and isomorphisms of graphs of such solutions are equivalent notions.

3.2.5 Theorem. *Let* (X, r_X) *and* (Y, r_Y) *be square-free solutions, and let* $\varphi : X \longrightarrow Y$ *be a bijection. The following conditions are equivalent:*

1. $\varphi \in \mathrm{Is}(X, Y)$;
2. $\varphi \circ \mathcal{L}_x = \mathcal{L}_{\varphi(x)} \circ \varphi$, *for all* $x \in X$;
3. $x_1 x_2 = \hat{x_2}\check{x_1} \in \Re(X, r_X) \iff \varphi(x_1)\varphi(x_2) = \varphi(\hat{x_2})\varphi(\check{x_1}) \in \Re(Y, r_Y)$;

4. *there is a one-to-one map between the pairs of relative cycles of* (X, r_X) *and the pairs of relative cycles of* (Y, r_Y) *given by*

$$(\mathcal{L}_x^y, \mathcal{L}_y^x) \mapsto (\mathcal{L}_{\varphi(x)}^{\varphi(y)}, \mathcal{L}_{\varphi(y)}^{\varphi(x)});$$

5. φ *is an isomorphism between the graphs* $\mathcal{T}(X, r_X)$ *and* $\mathcal{T}(Y, r_Y)$.

Proof. The equivalence between 1 and 2 (resp. 1 and 3) is justified in 3.2.3 (resp. 3.2.1). Implication "1 $\Rightarrow$ 4" is directly deduced from the statement 2 of Lemma 3.2.4. For "4 $\Rightarrow$ 3", pick $a, x \in X$ and suppose that $\mathcal{L}_a^x = (x_1 x_2 \cdots x_k)$, $\mathcal{L}_x^a = (a_1 a_2 \cdots a_m)$ is the pair of relative cycles associated to $x = x_1$ and $a = a_1$. Since $\mathcal{L}_{\varphi(a)}^{\varphi(x)} = (\varphi(x_1)\varphi(x_2)\cdots\varphi(x_k))$, $\mathcal{L}_{\varphi(x)}^{\varphi(a)} = (\varphi(a_1)\varphi(a_2)\cdots\varphi(a_m))$ is the pair of relative cycles (associated to $\varphi(x), \varphi(a) \in Y$) it follows that

$$\varphi(a)\varphi(x) = \varphi(x_2)\varphi(a_m) \in \Re(Y, r_Y).$$

For the same reason, if $\varphi(a)\varphi(x) = \varphi(x_2)\varphi(a_m) \in \Re(Y, r_Y)$, then $ax = x_2 a_m \in \Re(X, r_X)$. The implication "1 $\Rightarrow$ 5" is just the statement 1 of Lemma 3.2.4. Now suppose that $\varphi : X \longrightarrow Y$ is an isomorphism between the graphs $\mathcal{T}(X, r_X)$ and $\mathcal{T}(Y, r_Y)$ and let us check the statement 2. Let $a, x_1 \in X$, and take $x_2 = \mathcal{L}_a(x_1)$. Since $x_1 \stackrel{a}{\to} x_2$ is an edge of $\mathcal{T}(X, r_X)$, $\varphi(x_1) \stackrel{\varphi(a)}{\to} \varphi(x_2)$ is an edge of $\mathcal{T}(Y, r_Y)$, so

$$(\mathcal{L}_{\varphi(a)} \circ \varphi)(x_1) = (\varphi \circ \mathcal{L}_a)(x_1).$$

□

3.2.6 Example. Let $X = \{x_1, \ldots, x_6\}$. Let (X, r_1) be the square-free solution given by the left action $\mathcal{L} : X \longrightarrow \mathrm{Sym}(X)$ given by

$$\begin{array}{ll} \mathcal{L}_{x_1} = \mathcal{L}_{x_3} = (x_1)(x_2x_4)(x_3)(x_5)(x_6), & \mathcal{L}_{x_5} = (x_1x_4)(x_2x_3)(x_5)(x_6), \\ \mathcal{L}_{x_2} = \mathcal{L}_{x_4} = (x_1x_3)(x_2)(x_4)(x_5)(x_6), & \mathcal{L}_{x_6} = (x_1x_2)(x_3x_4)(x_5)(x_6), \end{array}$$

and let (X, r_2) be the square-free solution given by $\mathcal{L}' : X \longrightarrow \mathrm{Sym}(X)$ as

$$\begin{array}{ll} \mathcal{L}'_{x_1} = \mathcal{L}'_{x_3} = (x_1)(x_2x_4)(x_3)(x_5)(x_6), & \mathcal{L}'_{x_5} = (x_1x_2)(x_3x_4)(x_5)(x_6), \\ \mathcal{L}'_{x_2} = \mathcal{L}'_{x_4} = (x_1x_3)(x_2)(x_4)(x_5)(x_6), & \mathcal{L}'_{x_6} = (x_1x_4)(x_2x_3)(x_5)(x_6). \end{array}$$

Their sets of pairs of relative cycles

$$\begin{array}{l} \mathcal{C}(X, r_1) = \{\, (x_4x_2)(x_3x_1), (x_6)(x_4x_3), (x_6)(x_2x_1), (x_5)(x_4x_1), (x_5)(x_3x_2)\}, \\ \mathcal{C}(X, r_2) = \{\, (x_4x_2)(x_3x_1), (x_6)(x_3x_2), (x_6)(x_4x_1), (x_5)(x_2x_1), (x_5)(x_4x_3)\}, \end{array}$$

are in a one-to-one correspondence $(\mathcal{L}_x^y, \mathcal{L}_y^x) \mapsto (\mathcal{L}_{\varphi(x)}^{\varphi(y)}, \mathcal{L}_{\varphi(y)}^{\varphi(x)})$, where $\varphi = (x_5 x_6) \in \mathrm{Sym}(X)$. Indeed, looking at figure 3.2 it is easy to recognize that $\mathcal{T}(X, r_1)$ and $\mathcal{T}(X, r_2)$ are isomorphic (note that we can redraw $\mathcal{T}(X, r_2)$ just drawing vertex x_3 in the place occupied by vertex x_2 and vice versa in order to obtain the same drawing as for $\mathcal{T}(X, r_1)$). Hence $(X, r_1) \sim (X, r_2)$.

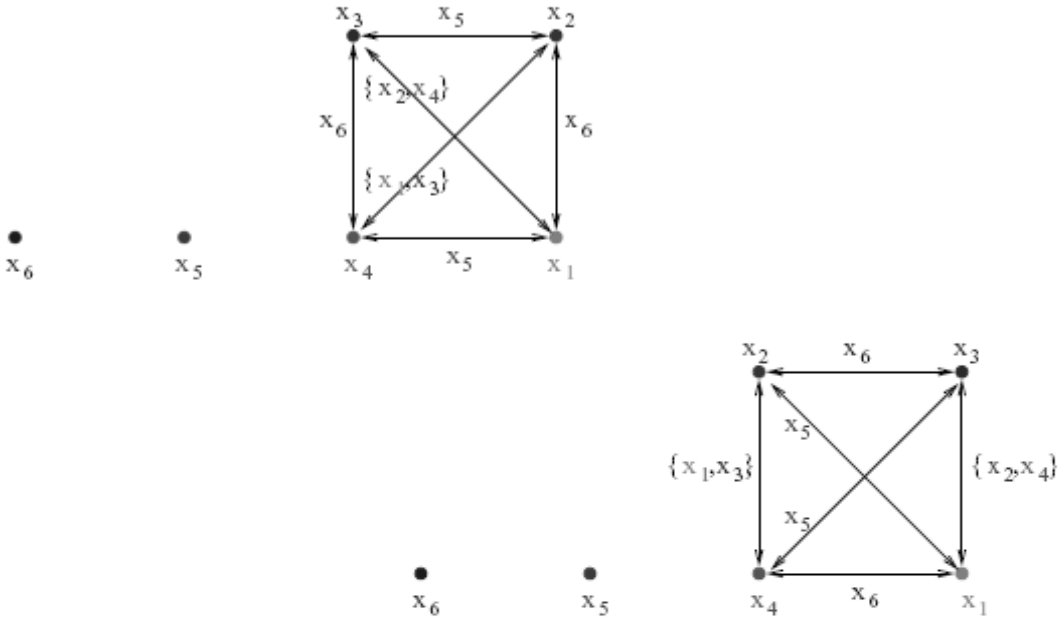


Figure 3.2: Graphs of the (isomorphic) solutions r_1, r_2 described in 3.2.6.

The question of effectively computing the set $\mathrm{Is}(X, Y)$ for two square-free solutions $(X, r_X), (Y, r_Y)$ explicitly given arises naturally. A first rough idea would consist in considering first the set of all bijective maps $\varphi : X \longrightarrow Y$ (which has $n!$ elements if $n = |X| = |Y|$) and then checking equality (3.8) for each φ. However, many of these last checks can be omitted since we can restrict the study to those φ satisfying certain conditions (see 3.2.14), which involves the notion of *star* of a vertex x of $\mathcal{T}(X, r_X)$.

3.2.7 Definition. Let (X, r) be a square-free solution of the YBE, and $x \in X$. We define the *star* of x as the set

$$\mathrm{Star}(x) = \{\mathcal{L}_a^x \,/\, a \in X \setminus \{x\}\} \subseteq \mathrm{Sym}(X),$$

where $\mathcal{L}_a^x$ denotes the first cycle in the pair $(\mathcal{L}_a^x, \mathcal{L}_x^a)$ of relative cycles associated to $a, x = x_1$ (see Cyclic Condition in 3.1.19).

3.2.8 Note. There can be elements $a \neq b \in X \setminus \{x\}$ giving the same cycle $\mathcal{L}_a^x = \mathcal{L}_b^x \in \mathrm{Star}(x)$. For example, for the square-free solution (X, r) with $X = \{x_1, \ldots, x_5\}$ given by

$$\mathcal{C}(X, r) = \{(x_5)(x_2x_1), (x_4x_3)(x_2x_1)\},$$

the star of x_1 consists of 2 elements

$$\mathrm{Star}(x_1) = \{\mathcal{L}_{x_2}^{x_1},\ \mathcal{L}_{x_3}^{x_1}\},$$

since $\mathcal{L}_{x_2}^{x_1} = (x_1)$ and $\mathcal{L}_{x_3}^{x_1} = \mathcal{L}_{x_4}^{x_1} = \mathcal{L}_{x_5}^{x_1} = (x_2x_1)$.

3.2.9 Definition. Let (X, r) be a square-free solution of the YBE, and $x \in X$. Assume that $\mathrm{Star}(x) = \{\mathcal{L}_{a_1}^x, \ldots, \mathcal{L}_{a_m}^x\}$, where $\mathcal{L}_{a_i}^x = (x_{i1}x_{i2}\cdots x_{ik_i})$ with $x_{i1} = x$. Let $\{v_{ij} \,/\, 1 \leq i \leq m, 2 \leq j \leq k_i\}$ be new variables. We define the *graph of the star of* x as the pseudodigraph $\mathcal{T}(\mathrm{Star}(x))$ determined by:

$$\begin{array}{ll} \text{Set of vertices of } \mathcal{T}(\mathrm{Star}(x)) : & \{x\} \cup \{v_{ij} \,/\, 1 \leq i \leq m, 2 \leq j \leq k_i\}. \\ \text{Set of edges of } \mathcal{T}(\mathrm{Star}(x)) : & \{x \xrightarrow{a_i} x, \text{ if there exists } i \text{ for which } k_i = 1\} \cup \\ & \{v_{ij} \xrightarrow{a_i} v_{ij+1} \,/\, 1 \leq i \leq m, 1 \leq j \leq k_i - 1\}, \end{array}$$

where v_{i1} denotes the vertex x.

Note that $\mathcal{T}(\mathrm{Star}_X(x))$ is, actually, a digraph with possibly a loop in the vertex x, corresponding to a cycle of type $\mathcal{L}_a^x = (x)$.

3.2.10 Example. Consider $X = \{x_1, \ldots, x_6\}$ and the square-free solution (X, r) defined as

$$\mathcal{C}(X, r) = \{(x_6)(x_5x_4),\ (x_6)(x_3x_2),\ (x_5)(x_1x_2x_3),\ (x_4)(x_3x_2x_1)\}.$$

whose graph is depicted in Fig. 3.3.

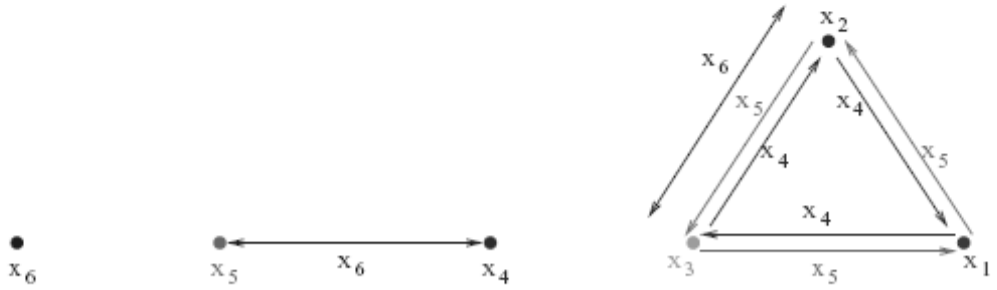


Figure 3.3: Graph of the solution in Example 3.2.10.

The graphs of the stars of all elements of X are represented in Fig. 3.4.

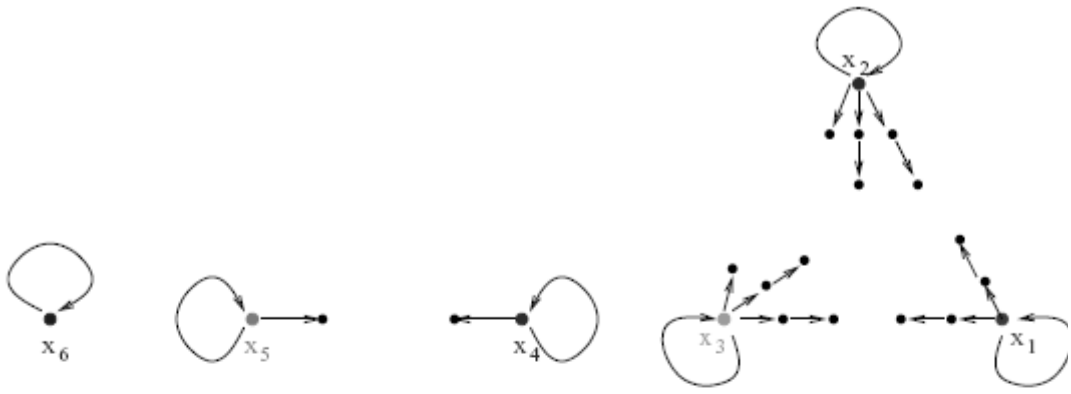


Figure 3.4: Stars of the elements of the solution in Example 3.2.10.

3.2.11 Definition. Let $(X, r_X), (Y, r_Y)$ be square-free solutions, and $x \in X$, $y \in Y$. Let $\mathrm{Star}_X(x)$ be the star of x with respect to (X, r_X), and $\mathrm{Star}_Y(y)$ the star of y with respect to (Y, r_Y). We say that $\mathrm{Star}_X(x)$ is equivalent to $\mathrm{Star}_Y(y)$ if, and only if, there exists a bijection $\phi : \mathrm{Star}_X(x) \longrightarrow \mathrm{Star}_Y(y)$ such that the lengths of $\mathcal{L}_a^x$ and $\phi(\mathcal{L}_a^x)$ are equal, for all $\mathcal{L}_a^x \in \mathrm{Star}_X(x)$.
We write $\mathrm{Star}_X(x) \sim \mathrm{Star}_Y(y)$ when $\mathrm{Star}_X(x)$ and $\mathrm{Star}_Y(y)$ are equivalent.

Note that $\sim$ is an equivalence relation.

3.2.12 Remark. It is easy to check that $\mathrm{Star}_X(x) \sim \mathrm{Star}_Y(y)$ if, and only if, their graphs $\mathcal{T}(\mathrm{Star}_X(x))$ and $\mathcal{T}(\mathrm{Star}_Y(y))$ are equivalent as *rooted pseudodigraphs* (pseudodigraphs with a distinguished vertex, the *root*), i.e., if there exists a bijection ϕ from the set of vertices of $\mathcal{T}(\mathrm{Star}_X(x))$ to the set of vertices of $\mathcal{T}(\mathrm{Star}_Y(y))$ such that $\phi(x) = y$ and for all vertices u, v of $\mathcal{T}(\mathrm{Star}_x(x))$, the number of edges from u to v is equal to the number of edges from $\phi(u)$ to $\phi(v)$.

3.2.13 Example. Taking $(X, r_X) = (Y, r_Y)$, in figure 3.4 we see that $\mathrm{Star}(x_2) \sim \mathrm{Star}(x_3)$, but $\mathrm{Star}(x_2)$ is not equivalent to $\mathrm{Star}(x_1)$. This fact proves that the elements of an orbit under the left action $\mathcal{L}$ of $G(X, r)$ on X do not have generally the same star.

3.2.14 Proposition. *Let $(X, r_X), (Y, r_Y)$ be square-free solutions of the YBE and $\varphi : X \longrightarrow Y$ a bijective map. Then,*

$$\varphi \in \mathrm{Is}(X, Y) \implies \mathrm{Star}_Y(\varphi(x)) \sim \mathrm{Star}_X(x), \ \forall\, x \in X.$$

Proof. Let $x \in X$. Suppose that $\varphi \in \mathrm{Is}(X,Y)$ and consequently that $\varphi^{-1} \in \mathrm{Is}(Y,X)$. From the statement 2 of 3.2.4, we can define the maps

$$\begin{array}{rcl} \phi_\varphi : \mathrm{Star}_X(x) \longrightarrow \mathrm{Star}_Y(\varphi(x)) & \qquad & \phi_{\varphi^{-1}} : \mathrm{Star}_Y(\varphi(x)) \longrightarrow \mathrm{Star}_X(x) \\ \mathcal{L}_a^x \mapsto \mathcal{L}_{\varphi(a)}^{\varphi(x)} & & \mathcal{L}_b^{\varphi(x)} \mapsto \mathcal{L}_{\varphi^{-1}(b)}^x, \end{array}$$

which are inverse of each other. Hence, ϕ_φ is a bijection. Since φ also preserves the lengths of cycles, $\mathrm{Star}_X(x) \sim \mathrm{Star}_Y(\varphi(x))$. □

The converse is not always true, as we show in 3.2.27.

In order to compute $\mathrm{Is}(X,Y)$ for square-free solutions (X,r_X) and (Y,r_Y) explicitly given, we first consider the set of bijections $\varphi : X \longrightarrow Y$ such that $\mathrm{Star}_Y(\varphi(x)) \sim \mathrm{Star}_X(x)$, $\forall\, x \in X$ and then, for each of these φ, we check equality (3.8) of 3.2.3. This is the idea used in Algorithm 20.

Algorithm 20 Isomorphisms of square-free solutions

Require: (X,r_X) and (Y,r_Y), square-free solutions of the YBE s.t. $|X| = |Y| = n$;
Ensure: $Isom$, the set of isomorphisms $\mathrm{Is}(X,Y)$;
  Initialization: Let $Isom := \emptyset$;
  $PossibleIsom := \{(y_1,\ldots,y_n) \in Y^n \,/\, i \neq j,\ y_i \neq y_j,\ \mathrm{Star}_Y(y_i) \sim \mathrm{Star}_X(x_i)\}$;
  while $(PossibleIsom \neq \emptyset)$ **do**
    Take $(y_1,\ldots,y_n) \in PossibleIsom$;
    Let $PossibleIsom := PossibleIsom \setminus \{(y_1,\ldots,y_n)\}$;
    Let $\varphi : X \longrightarrow Y$ defined as $\varphi(x_i) := y_i$, $\forall\, i \in \{1,\ldots,n\}$;
    if $\mathcal{L}_{y_i}(y_j) = \varphi(\mathcal{L}_{x_i}(x_j)), \forall\, i \neq j$ **then**
      $Isom := Isom \cup \{\varphi\}$;
    end if
  end while
  Return $Isom$.

3.2.15 Definition. A permutation $\tau \in \mathrm{Sym}(X)$ is called an *automorphism* of the solution (X,r) (or shortly, an *r-automorphism*) if $(\tau\times\tau)\circ r = r\circ(\tau\times\tau)$. The *group of r-automorphisms* of (X,r) will be denoted by $\mathrm{Aut}(X,r)$.

Note that $\mathrm{Aut}(X,r)$ is a subgroup of $\mathrm{Sym}(X)$.

3.2.16 Remark. Let (X,r) be a solution of the YBE. From the statement b) of 3.2.1, if $\tau \in \mathrm{Aut}(X,r)$, then

$$\mathcal{L}_x = \mathcal{L}_y \iff \mathcal{L}_{\tau(x)} = \mathcal{L}_{\tau(y)},$$

for $x, y \in X$.

3.2.17 Remark. As a consequence of 3.2.2, every automorphism τ of a solution (X,r) can be extended to

- a semigroup automorphism $\tau_{\mathcal{S}}$ of the associated semigroup $\mathcal{S}(X,r)$;
- a group automorphism $\tau_{\mathcal{G}}$ of the associated group $\mathcal{G}(X,r)$. Thus, we have an embedding $\mathrm{Aut}(X,r) \hookrightarrow \mathrm{Aut}(\mathcal{G}(X,r))$;
- an algebra automorphism $\tau_{\mathcal{A}}$ of the associated algebra $\mathcal{A}(\mathsf{k},X,r)$.

3.2.18 Example. Let $X = \{a, x_1, \ldots, x_n\}$ and r the square-free solution given by

$$\mathcal{L}_a = (a)(x_1 \cdots x_n), \quad \text{and} \quad \mathcal{L}_{x_i} = \mathrm{Id}_X, \ 1 \leq i \leq n.$$

Then, $\mathcal{L}_a$ is an automorphism of (X,r).

3.2.19 Example. Let $X = \{x_1, \ldots, x_{12}\}$ and (X,r) a square-free solution of which we know that $\{x_1, x_8\}$, $\{x_2, x_3, x_4\}$ and $\{x_5, x_6, x_7\}$ are sets of pairwise commutative variables, and

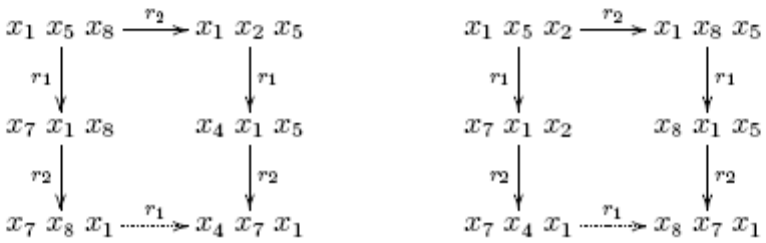
$$\begin{array}{ll} \mathcal{L}_{x_2}^{x_1} = \mathcal{L}_{x_3}^{x_1} = \mathcal{L}_{x_4}^{x_1} = (x_1), & \mathcal{L}_{x_1}^{x_2} = \mathcal{L}_{x_1}^{x_3} = \mathcal{L}_{x_1}^{x_4} = (x_4x_3x_2), \\ \mathcal{L}_{x_5}^{x_1} = \mathcal{L}_{x_6}^{x_1} = \mathcal{L}_{x_7}^{x_1} = (x_1), & \mathcal{L}_{x_1}^{x_5} = \mathcal{L}_{x_1}^{x_6} = \mathcal{L}_{x_1}^{x_7} = (x_7x_6x_5), \\ \mathcal{L}_{x_5}^{x_2} = \mathcal{L}_{x_5}^{x_8} = (x_8x_2), & \mathcal{L}_{x_2}^{x_5} = \mathcal{L}_{x_8}^{x_5} = (x_5) \end{array}$$

are relative cycles appearing in $\mathcal{C}(X,r)$.

With these hypotheses we will determine a square-free solution (X,r) of the YBE, and a particular automorphism satisfying a relation of symmetry in its associated graph $\mathcal{T}(X,r)$.

From the initial information for (X,r) we have the subgraph of (X,r) given in figure 3.5 where, as in all figures in this example, the continuous arrows correspond to x_1-edges.

Applying the YB diagrams



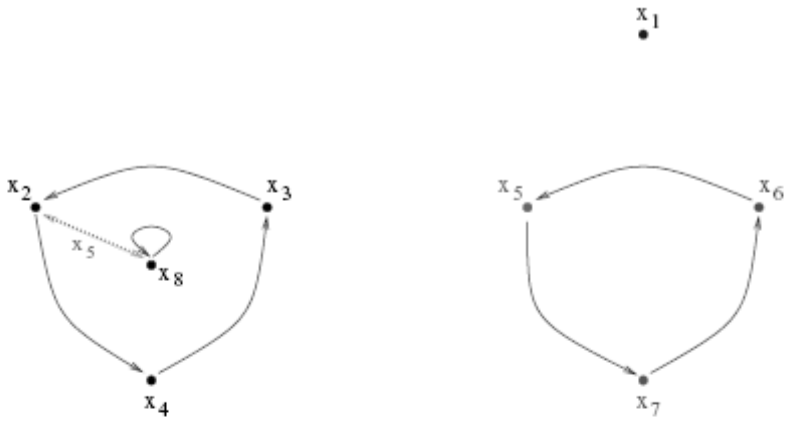


Figure 3.5: Subgraph of the square-free solution (X, r).

we obtain that $\mathcal{L}_{x_4}^{x_7} = \mathcal{L}_{x_8}^{x_7} = (x_7)$ and $\mathcal{L}_{x_7}^{x_4} = \mathcal{L}_{x_7}^{x_8} = (x_8x_4)$.
Analogously, we can obtain that $\mathcal{L}_{x_3}^{x_6} = \mathcal{L}_{x_8}^{x_6} = (x_6)$ and $\mathcal{L}_{x_6}^{x_3} = \mathcal{L}_{x_6}^{x_8} = (x_8x_3)$.
Now, by the statement 2 of 3.1.34, there exists $x_9 \in X \setminus \{x_3, x_4, x_6, x_7, x_8\}$ such that $\mathcal{L}_{x_3}^{x_7} = \mathcal{L}_{x_9}^{x_7} = (x_7)$, $\mathcal{L}_{x_7}^{x_3} = \mathcal{L}_{x_7}^{x_9} = (x_9x_3)$, $\mathcal{L}_{x_4}^{x_6} = \mathcal{L}_{x_9}^{x_6} = (x_6)$ and $\mathcal{L}_{x_6}^{x_4} = \mathcal{L}_{x_6}^{x_9} = (x_9x_4)$. It is also clear that x_9 is different from x_1, resp. x_5, because otherwise, $x_9x_7 = x_6x_1$, resp. $x_9x_6 = x_6x_5$ - a contradiction.
Applying the statement 2 of 3.1.34 two more times, there exist variables

$$x_{10} \in X \setminus \{x_1, x_2, x_4, x_5, x_6, x_7, x_8\},\ x_{11} \in X \setminus \{x_1, x_2, x_3, x_5, x_6, x_7, x_8\}$$

such that $\mathcal{L}_{x_4}^{x_5} = \mathcal{L}_{x_{10}}^{x_5} = (x_5)$, $\mathcal{L}_{x_5}^{x_4} = \mathcal{L}_{x_5}^{x_{10}} = (x_{10}x_4)$, $\mathcal{L}_{x_2}^{x_7} = \mathcal{L}_{x_{10}}^{x_7} = (x_7)$, $\mathcal{L}_{x_7}^{x_2} = \mathcal{L}_{x_7}^{x_{10}} = (x_{10}x_2)$, $\mathcal{L}_{x_3}^{x_5} = \mathcal{L}_{x_{11}}^{x_5} = (x_5)$, $\mathcal{L}_{x_5}^{x_3} = \mathcal{L}_{x_5}^{x_{11}} = (x_{11}x_3)$, $\mathcal{L}_{x_2}^{x_6} = \mathcal{L}_{x_{11}}^{x_6} = (x_6)$, and $\mathcal{L}_{x_6}^{x_2} = \mathcal{L}_{x_6}^{x_{11}} = (x_{11}x_2)$.
Besides, x_9, x_{10}, x_{11} are pairwise distinct (if, for example, $x_{10} = x_9$, then $x_9x_7 = x_7x_2$ - a contradiction since $x_9x_7 = x_7x_3$). Hence, $x_9 \neq x_i$, for all $1 \leq i \leq 11$, $i \neq 2$, $x_{10} \neq x_i$, for all $1 \leq i \leq 11$, $i \neq 3$, $x_{11} \neq x_i$, for all $1 \leq i \leq 11$, $i \neq 4$.
Figure 3.6 represents a subgraph of the solution (X, r), according with the information we have determined so far. We distinguish two cases:

A) If $x_9 = x_2$, from $x_6x_9 = x_4x_6$ and $x_6x_2 = x_{11}x_6$ then $x_{11} = x_4$. Hence, $x_{10} = x_3$, since $x_5x_{11} = x_3x_5$ and $x_5x_4 = x_{10}x_5$. Figure 3.7 represents this situation.

   Now, applying the statement 3 of 3.1.34 with the relations $x_6x_3 = x_8x_6$, $x_6x_4 = x_2x_6$ and $x_3x_4 = x_4x_3$, we get that $x_8x_2 = x_2x_8$. Similarly, it holds that $x_8x_3 = x_3x_8$ and $x_8x_4 = x_4x_8$.

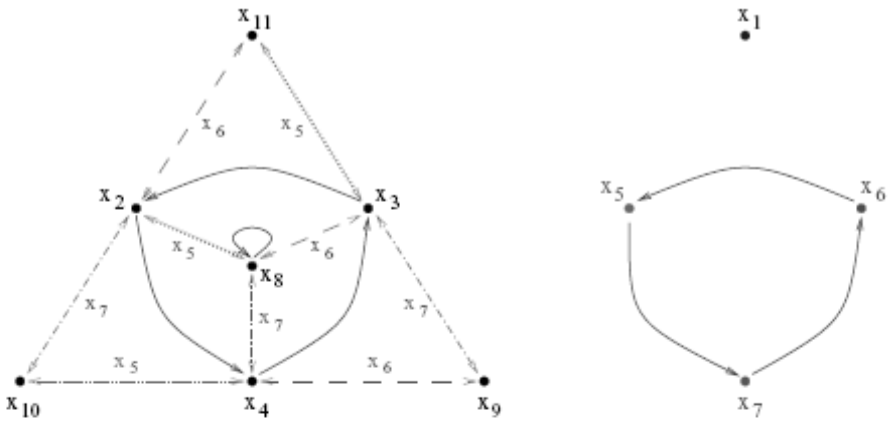


Figure 3.6: Subgraph of the square-free solution (X, r)

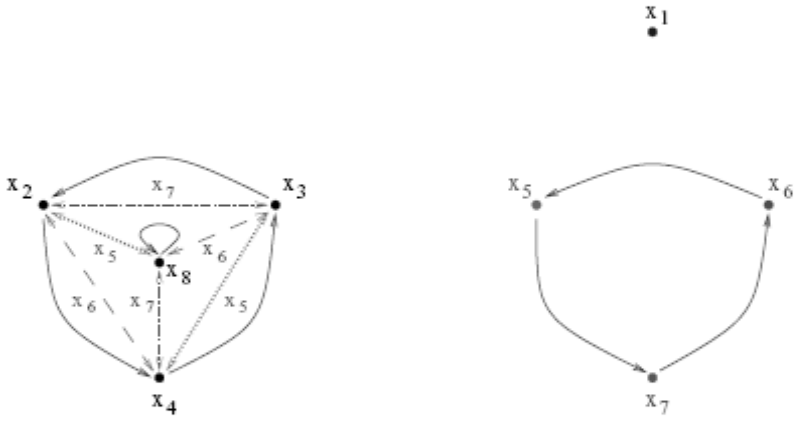


Figure 3.7: Subgraph of the square-free solution (X, r) in case A).

In this case, $Y = \{x_1, \ldots, x_8\}$ and r_Y given by

$$\begin{aligned}
\mathcal{L}_{x_1} &= (x_8)(x_7x_6x_5)(x_4x_3x_2)(x_1),\\
\mathcal{L}_{x_5} &= (x_8x_2)(x_7)(x_6)(x_5)(x_4x_3)(x_1),\\
\mathcal{L}_{x_6} &= (x_8x_3)(x_7)(x_6)(x_5)(x_4x_2)(x_1),\\
\mathcal{L}_{x_7} &= (x_8x_4)(x_7)(x_6)(x_5)(x_3x_2)(x_1),\\
\mathcal{L}_{x_2} &= \mathcal{L}_{x_3} = \mathcal{L}_{x_4} = \mathcal{L}_{x_8} = \mathrm{Id}_Y,
\end{aligned} \tag{3.10}$$

is a square-free solution, or equivalently, an r-invariant subset of the square-free solution (X, r) (see definition in 3.2.28). Its graph can be drawn as in Fig. 3.8.

Note that $\mathcal{L}_{x_1} \in \mathrm{Aut}(Y, r_Y)$.

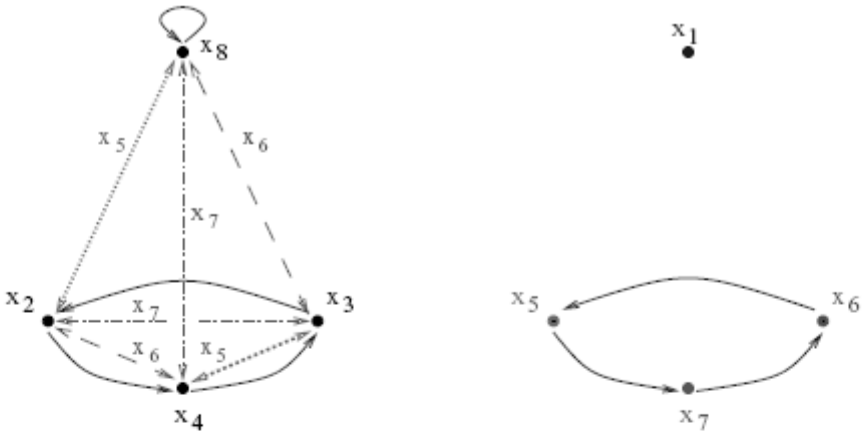
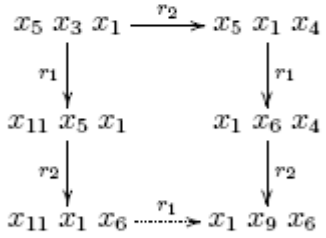


Figure 3.8: Graph of the square-free solution given in (3.10).

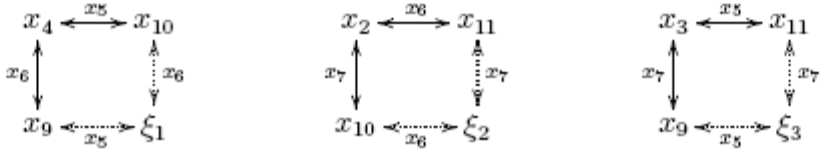
B) If $x_9 \neq x_2$, applying similar arguments than in the previous case, it follows that $x_{10} \neq x_3$ and $x_{11} \neq x_4$.

From the YB diagram



$x_{11}x_1 = x_1x_9$, and similarly, $x_{10}x_1 = x_1x_{11}$ and $x_9x_1 = x_1x_{10}$. So, $\mathcal{L}_{x_1}^{x_9} = \mathcal{L}_{x_1}^{x_{10}} = \mathcal{L}_{x_1}^{x_{11}} = (x_{11}x_{10}x_9)$ and $\mathcal{L}_{x_9}^{x_1} = \mathcal{L}_{x_{10}}^{x_1} = \mathcal{L}_{x_{11}}^{x_1} = (x_1)$.

Applying the statement 3 of 3.1.34 several times, we obtain that x_8, x_9, x_{10} and x_{11} are pairwise commutative. Now, applying 2 of 3.1.34,



there exists ξ_1, ξ_2, ξ_3, each of them different from all x_i's, such that

$$\begin{array}{ll}
\mathcal{L}_{x_9}^{x_5} = \mathcal{L}_{\xi_1}^{x_5} = (x_5), & \mathcal{L}_{x_5}^{x_9} = \mathcal{L}_{x_5}^{\xi_1} = (x_9\xi_1), \\
\mathcal{L}_{x_{10}}^{x_6} = \mathcal{L}_{\xi_1}^{x_6} = (x_6), & \mathcal{L}_{x_6}^{x_{10}} = \mathcal{L}_{x_6}^{\xi_1} = (x_{10}\xi_1), \\
\mathcal{L}_{x_{10}}^{x_6} = \mathcal{L}_{\xi_2}^{x_6} = (x_6), & \mathcal{L}_{x_6}^{x_{10}} = \mathcal{L}_{x_6}^{\xi_2} = (x_{10}\xi_2), \\
\mathcal{L}_{x_{11}}^{x_7} = \mathcal{L}_{\xi_2}^{x_7} = (x_7), & \mathcal{L}_{x_7}^{x_{11}} = \mathcal{L}_{x_7}^{\xi_2} = (x_{11}\xi_2), \\
\mathcal{L}_{x_9}^{x_5} = \mathcal{L}_{\xi_3}^{x_5} = (x_5), & \mathcal{L}_{x_5}^{x_9} = \mathcal{L}_{x_5}^{\xi_3} = (x_9\xi_3), \\
\mathcal{L}_{x_{11}}^{x_7} = \mathcal{L}_{\xi_3}^{x_7} = (x_7), & \mathcal{L}_{x_7}^{x_{11}} = \mathcal{L}_{x_7}^{\xi_3} = (x_{11}\xi_3).
\end{array}$$

Hence, from the uniqueness of the pairs of relative cycles, $\xi_1 = \xi_2 = \xi_3$. Let $x_{12} = \xi_1$. The information about (X, r) we have so far is represented in figure 3.9.

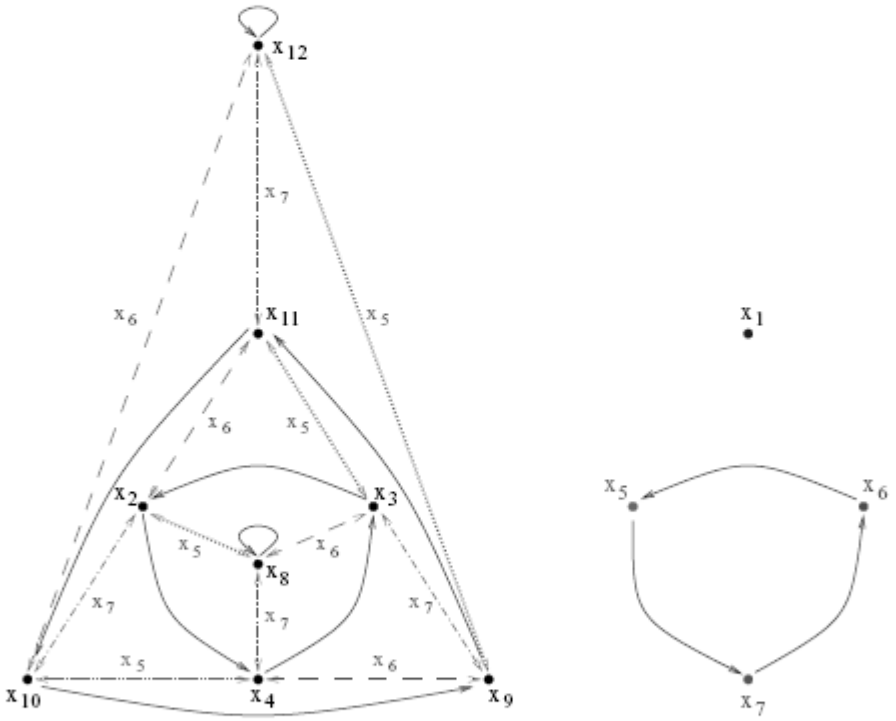


Figure 3.9: Subgraph of the square-free solution (X, r) in case B).

From 3 of 3.1.34 and the commutativity of x_8 with x_9, x_{10}, x_{11} it follows that x_{12} commutes with x_2, x_3, x_4.

Now, it can easily be checked that the only relation for x_{12} and x_1 is $x_{12}x_1 = x_1x_{12}$. Hence, using the statement 3 of 3.1.34, we obtain that $x_2x_9 = x_9x_2$, $x_3x_{10} = x_{10}x_3$ and $x_4x_{11} = x_{11}x_4$.

At this point, $\mathcal{L}_{x_8}(x_4)$ can be either x_2, or x_3 or x_4, but one can check that two first are not possible, and that the last one leads us to $x_8x_4 = x_4x_8$. With this commutative relation, we can apply 3 of 3.1.34 in order to obtain that $\{x_3, x_9\}$, $\{x_{11}, x_{12}\}$ and $\{x_2, x_{10}\}$ are sets of pairwise commutative variables. Similarly, one can check that $x_8x_3 = x_3x_8$, $x_8x_2 = x_2x_8$, and applying 3 of 3.1.34, that $\{x_4, x_9\}$, $\{x_{10}, x_{12}\}$, $\{x_2, x_{11}\}$, $\{x_3, x_{11}\}$ and $\{x_9, x_{12}\}$ are sets of pairwise commutative variables.

Therefore, in this case we obtain a complete description of the square-free solution (X, r) [3]

$$\begin{aligned}
&\mathcal{L}_{x_i} = \mathrm{Id}_X,\ i \in \{2,3,4,8,9,10,11,12\},\\
&\mathcal{L}_{x_1} = (x_{12})(x_{11}x_{10}x_9)(x_8)(x_7x_6x_5)(x_4x_3x_2)(x_1),\\
&\mathcal{L}_{x_5} = (x_{12}x_9)(x_{11}x_3)(x_{10}x_4)(x_8x_2)(x_7)(x_6)(x_5)(x_1),\\
&\mathcal{L}_{x_6} = (x_{12}x_{10})(x_{11}x_2)(x_9x_4)(x_8x_3)(x_7)(x_6)(x_5)(x_1),\\
&\mathcal{L}_{x_7} = (x_{12}x_{11})(x_{10}x_2)(x_9x_3)(x_8x_4)(x_7)(x_6)(x_5)(x_1),
\end{aligned} \tag{3.11}$$

whose graph can be drawn as in figure 3.10.

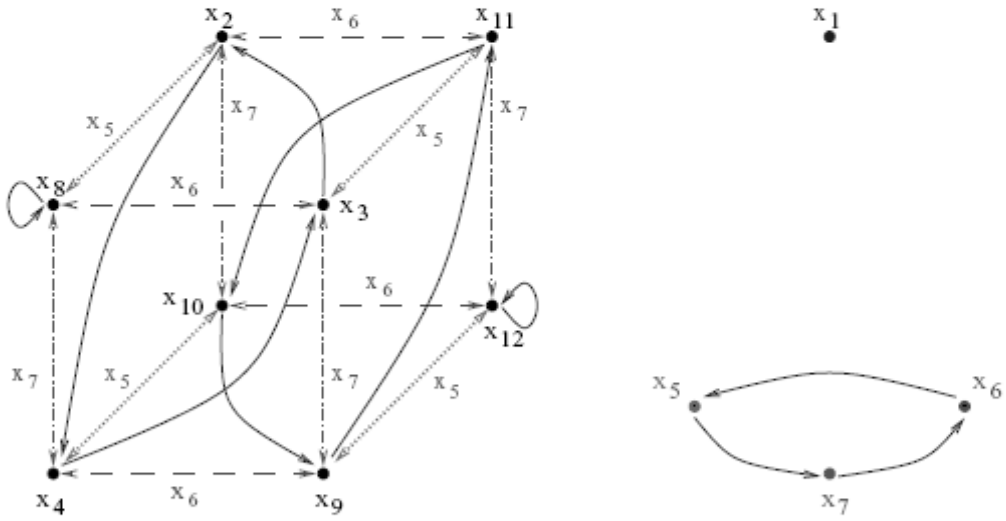


Figure 3.10: Graph of the square-free solution given in (3.11).

Note that $\mathcal{L}_{x_1} \in \mathrm{Aut}(X, r)$, which is represented in the figure by continuous arrows, behaves as a symmetry with respect to the axe $\overline{x_8x_{12}}$ in the *cubic* connected component.

[3] The square-free solution (X, r) is the so-called *Crystal solution*. The reason for this name may be its graph (see Fig. 3.10), which looks like the structure of a molecule of a crystal.

The next result is a direct consequence of 3.2.5.

3.2.20 Theorem. *Let (X,r) be a square-free solution of the YBE with graph $\mathcal{T} = \mathcal{T}(X,r)$. Let $\tau \in \mathrm{Sym}(X)$. The following conditions are equivalent:*

1. *τ is an r-automorphism;*
2. *For any $a \in X$, $\tau \circ \mathcal{L}_a = \mathcal{L}_{\tau(a)} \circ \tau$, or equivalently,*
$$\tau \circ \mathcal{L}_a \circ \tau^{-1} = \mathcal{L}_{\tau(a)}; \tag{3.12}$$
3. *There is an edge $x \xrightarrow{a} y$ in $\mathcal{T}$ if, and only if, $\tau(x) \xrightarrow{\tau(a)} \tau(y)$ occurs in $\mathcal{T}$, or equivalently, τ defines an isomorphism from $\mathcal{T}$ onto itself.*

The next result is a consequence of the second equivalent statement of the Theorem 3.2.20.

3.2.21 Corollary. $\mathrm{Aut}(X,r)$ *is a subgroup of the normalizer* $\mathrm{Nor}_{\mathrm{Sym}(X)}\mathcal{G}_{\mathcal{L}}$ *of the group* $\mathcal{G}_{\mathcal{L}} = \mathcal{L}(\mathcal{G}(X,r))$.

In general $\mathrm{Nor}_{\mathrm{Sym}(X)}\mathcal{G}_{\mathcal{L}}$ is greater than $\mathrm{Aut}(X,r)$. This fact is shown in the following example.

3.2.22 Example. Consider the solution (X,r), where $X = \{x_1,\ldots,x_6\}$ and

$$\mathcal{L}_{x_1} = \mathcal{L}_{x_2} = \mathcal{L}_{x_3} = \mathcal{L}_{x_4} = \mathrm{Id}_X,$$
$$\mathcal{L}_{x_5} = (x_1x_3)(x_2x_4)(x_5)(x_6), \quad \mathcal{L}_{x_6} = (x_1x_2)(x_3x_4)(x_5)(x_6).$$

The graph $\mathcal{T}(X,r)$ is depicted in Fig. 3.11. The group $\mathcal{G}_{\mathcal{L}} = \mathcal{L}(\mathcal{G}(X,r)) \subseteq$

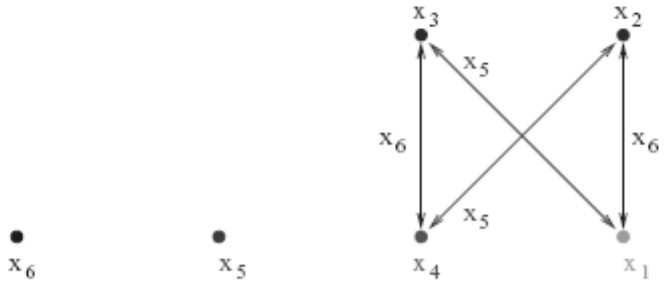


Figure 3.11: Graph of the solution of 3.2.22.

$\mathrm{Sym}(X)$ is the group generated by $\{\mathcal{L}_{x_5}, \mathcal{L}_{x_6}\}$, with relations

$$\{\mathcal{L}_{x_5}^2 = \mathcal{L}_{x_6}^2 = \mathrm{Id}_X,\ \mathcal{L}_{x_5}\mathcal{L}_{x_6} = \mathcal{L}_{x_6}\mathcal{L}_{x_5}\}.$$

Hence, $\mathcal{G}_{\mathcal{L}}$ is isomorphic to the *Klein's group* $\mathbb{Z}_2 \times \mathbb{Z}_2$.
The permutation $\tau = (x_1x_3)(x_2x_4)(x_5x_6) \in \mathrm{Sym}(X)$ is in $\mathrm{Nor}_{\mathrm{Sym}(X)}\mathcal{G}_{\mathcal{L}}$ since it satisfies the equalities:

$$\tau \circ \mathcal{L}_{x_5} \circ \tau^{-1} = \mathcal{L}_{x_5}, \tag{3.13}$$

$$\tau \circ \mathcal{L}_{x_6} \circ \tau^{-1} = \mathcal{L}_{x_6}. \tag{3.14}$$

The assignement $\tau(x_5) = x_6$ and (3.13) show that τ does not satisfy the necessary condition $\tau \circ \mathcal{L}_{x_5} = \mathcal{L}_{\tau(x_5)} \circ \tau$ for being an automorphism. Therefore, $\mathrm{Aut}(X, r) \subsetneq \mathrm{Nor}_{\mathrm{Sym}(X)}(\mathcal{G}_{\mathcal{L}})$.

As a particular case of 3.2.14, we have:

3.2.23 Proposition. *Let (X, r) be a square-free solution and $\tau \in \mathrm{Sym}(X)$. Then*

$$\tau \in \mathrm{Aut}(X, r) \implies \mathrm{Star}(\tau(x)) \sim \mathrm{Star}(x), \ \forall\, x \in X.$$

To compute the group $\mathrm{Aut}(X, r)$ we can proceed in an analogous way as that for $\mathrm{Is}(X, Y)$ (see Algorithm 20), since it is a particular case.

3.2.24 Example. Consider the square-free solution (X, r) given in Example 3.2.22. Let us compute $\mathrm{Aut}(X, r)$ following the spirit of 3.2.23.
Suppose that $\tau \in \mathrm{Aut}(X, r)$. By 3.2.23, $\mathrm{Star}(\tau(x_6)) \sim \mathrm{Star}(x_6)$. Hence, looking at Fig. 3.12, there are two possible cases: $\tau(x_6) = x_6$ or $\tau(x_6) = x_5$.

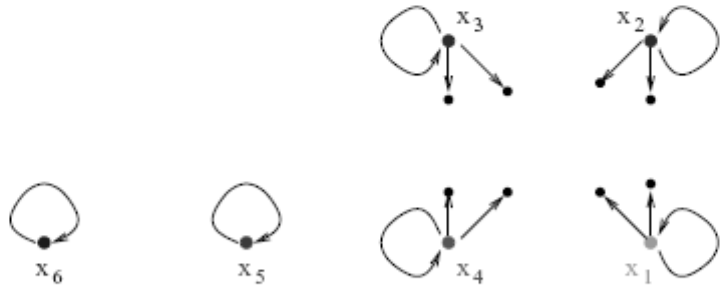


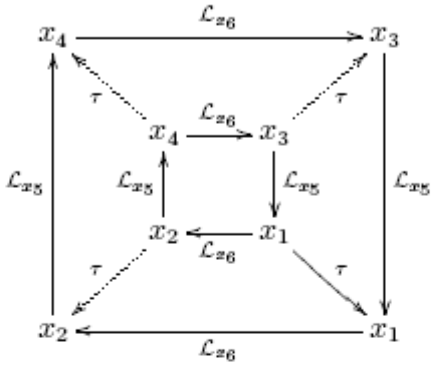
Figure 3.12: Stars corresponding to the square-free solution given in 3.2.22.

A) If $\tau(x_6) = x_6$, then $\tau(x_5) = x_5$ (for the same reason). Since

$$\mathrm{Star}(x_1) \sim \mathrm{Star}(x_2) \sim \mathrm{Star}(x_3) \sim \mathrm{Star}(x_4),$$

there are four possible cases:

A.1.) If $\tau(x_1) = x_1$, then applying diagram (3.9) of 3.2.4 to the relations $x_6x_4 = x_3*$, $x_5x_3 = x_1*$, $x_6x_1 = x_2*$ and $x_5x_2 = x_4*$ of $\Re(X, r)$, we obtain the images under τ of all the elements:



Hence, $\tau = \mathrm{Id}_X$.

Considering analogous diagrams we can easily determine τ in each of the following situations.

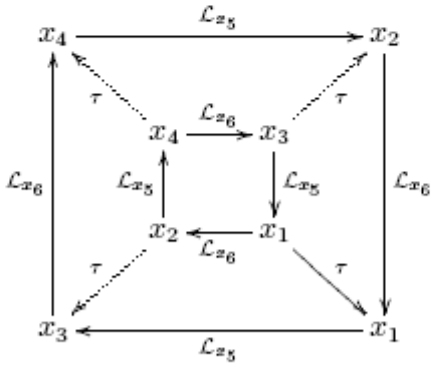
A.2.) If $\tau(x_1) = x_2$, then $\tau = (x_1x_2)(x_3x_4)(x_5)(x_6)$.

A.3.) If $\tau(x_1) = x_3$, then $\tau = (x_1x_3)(x_2x_4)(x_5)(x_6)$.

A.4.) If $\tau(x_1) = x_4$, then $\tau = (x_1x_4)(x_2x_3)(x_5)(x_6)$.

B) If $\tau(x_6) = x_5$, then $\tau(x_5) = x_6$. There are the same possibilities for $\mathrm{Star}(x_1)$ as in case A.

B.1.) If $\tau(x_1) = x_1$, then applying diagram (3.9) of 3.2.4



we obtain that $\tau = (x_1)(x_2)(x_2x_3)(x_5x_6)$.

B.2.) If $\tau(x_1) = x_2$, then $\tau = (x_1x_2x_4x_3)(x_5x_6)$.

B.3.) If $\tau(x_1) = x_3$, then $\tau = (x_1x_3x_4x_2)(x_5x_6)$.

B.4.) Finally, if $\tau(x_1) = x_4$, then $\tau = (x_1x_4)(x_2)(x_3)(x_5x_6)$.

Each $\tau \in \mathrm{Sym}(X)$ previously obtained is an automorphism of (X, r). Therefore,

$$\mathrm{Aut}(X,r) = \left\{ \begin{array}{ll} \tau_1 = \mathrm{Id}_X, & \tau_5 = (x_1)(x_2x_3)(x_4)(x_5x_6), \\ \tau_2 = (x_1x_2)(x_3x_4)(x_5)(x_6), & \tau_6 = (x_1x_2x_4x_3)(x_5x_6) \\ \tau_3 = (x_1x_3)(x_2x_4)(x_5)(x_6), & \tau_7 = (x_1x_3x_4x_2)(x_5x_6) \\ \tau_4 = (x_1x_4)(x_2x_3)(x_5)(x_6), & \tau_8 = (x_1x_4)(x_2)(x_3)(x_5x_6) \end{array} \right\},$$

which is not an abelian group since $\tau_5\tau_2 = \tau_7 \neq \tau_6 = \tau_2\tau_5$. Thus, there are two possibilities for $\mathrm{Aut}(X, r)$: to be (isomorphic to) either the *Dihedral group*

$$\mathfrak{D}_8 = \{\ e,\ x,\ x^2,\ x^3,\ y,\ xy,\ x^2y,\ x^3y\ \},$$

where

$$\begin{array}{l} x^iy = yx^{4-i},\ \forall\ 1 \leq i \leq 3, \\ o(x) = o(x^3) = 4, \\ o(x^2) = o(y) = o(xy) = o(x^2y) = o(x^3y) = 2, \end{array} \tag{3.15}$$

(denoting by $o(a)$ the order of an element $a \in G$ in the group G), or to be the group of *Quaternions*:

$$\mathfrak{Q} = \{\ e,\ -e,\ i,\ -i,\ j,\ -j,\ k,\ -k\ \},$$

with

$$\begin{array}{l} i^2 = j^2 = k^2 = -e,\ ij = k,\ jk = i,\ ki = j, \\ o(-e) = 2,\ \ o(i) = o(-i) = o(j) = o(-j) = o(k) = o(-k) = 4. \end{array}$$

In our case,

$$o(\tau_2) = o(\tau_3) = o(\tau_4) = o(\tau_5) = o(\tau_8) = 2, \quad o(\tau_6) = o(\tau_7) = 4.$$

Thus,

$$\mathrm{Aut}(X,r) \cong \mathfrak{D}_8.$$

In fact, $x := \tau_6$ and $y := \tau_5$ satisfy all the relations (3.15). Hence, $\mathrm{Aut}(X, r)$ is the group generated by $\{\tau_5, \tau_6\}$ with relations

$$\{\tau_6^4 = \tau_5^2 = \mathrm{Id}_X,\ \tau_6\tau_5 = \tau_5\tau_6^3\}.$$

3.2.25 Example. Consider the square-free solution (X, r) given by $X = \{x_1, \ldots, x_6\}$ and relations

$$\mathcal{C}(X,r) = \{(x_6x_5)(x_4x_3x_2x_1),\ (x_4x_2)(x_3x_1)\}.$$

Its group of automorphisms is

$$\mathrm{Aut}(X,r)=\left\{\begin{array}{ll}\tau_1=\mathrm{Id}_X, & \tau_5=(x_1x_3)(x_2x_4)(x_5)(x_6),\\ \tau_2=(x_1)(x_2)(x_3)(x_4)(x_5x_6), & \tau_6=(x_1x_3)(x_2x_4)(x_5x_6)\\ \tau_3=(x_1x_2x_3x_4)(x_5)(x_6), & \tau_7=(x_1x_4x_3x_2)(x_5)(x_6)\\ \tau_4=(x_1x_2x_3x_4)(x_5x_6), & \tau_8=(x_1x_4x_3x_2)(x_5x_6)\end{array}\right\},$$

which is abelian. Therefore, $\mathrm{Aut}(X,r)$ is either isomorphic to $\mathbb{Z}_8$, or to $\mathbb{Z}_4\times\mathbb{Z}_2$, or to $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$. Since $o(\tau_2)=o(\tau_5)=o(\tau_6)=2$ and $o(\tau_3)=o(\tau_4)=o(\tau_7)=o(\tau_8)=4$, $\mathrm{Aut}(X,r)$ is the group generated by $\{\tau_2,\tau_3\}$ with relations

$$\{\tau_2^2=\tau_3^4=\mathrm{Id}_X,\ \tau_2\tau_3=\tau_3\tau_2\}$$

Therefore, $\mathrm{Aut}(X,r)\ \cong\ \mathbb{Z}_4\times\mathbb{Z}_2$.

3.2.26 Example. Consider the square-free solution (X,r) with $X=\{x_1,\ldots,x_8\}$ and set of pairs of relative cycles

$$\mathcal{C}(X,r)=\{(x_8x_6x_7)(x_5),\ (x_8x_6x_7)(x_4),\ (x_5)(x_3x_2x_1),\ (x_4)(x_3x_1x_2)\}.$$

The group of automorphisms $\mathrm{Aut}(X,r)$ of (X,r) consists of

$$\begin{array}{ll}\tau_1=\mathrm{Id}_X, & \tau_{10}=(x_1x_2x_3)(x_4)(x_5)(x_6)(x_7)(x_8)\\ \tau_2=(x_1)(x_2)(x_3)(x_4)(x_5)(x_6x_7x_8), & \tau_{11}=(x_1x_2x_3)(x_4)(x_5)(x_6x_7x_8)\\ \tau_3=(x_1)(x_2)(x_3)(x_4)(x_5)(x_6x_8x_7), & \tau_{12}=(x_1x_2x_3)(x_4)(x_5)(x_6x_8x_7)\\ \tau_4=(x_1)(x_2x_3)(x_4x_5)(x_6)(x_7)(x_8), & \tau_{13}=(x_1x_3x_2)(x_4)(x_5)(x_6)(x_7)(x_8)\\ \tau_5=(x_1)(x_2x_3)(x_4x_5)(x_6x_7x_8), & \tau_{14}=(x_1x_3x_2)(x_4)(x_5)(x_6x_7x_8)\\ \tau_6=(x_1)(x_2x_3)(x_4x_5)(x_6x_8x_7), & \tau_{15}=(x_1x_3x_2)(x_4)(x_5)(x_6x_8x_7)\\ \tau_7=(x_1x_2)(x_3)(x_4x_5)(x_6)(x_7)(x_8), & \tau_{16}=(x_1x_3)(x_2)(x_4x_5)(x_6)(x_7)(x_8)\\ \tau_8=(x_1x_2)(x_3)(x_4x_5)(x_6x_7x_8), & \tau_{17}=(x_1x_3)(x_2)(x_4x_5)(x_6x_7x_8)\\ \tau_9=(x_1x_2)(x_3)(x_4x_5)(x_6x_8x_7), & \tau_{18}=(x_1x_3)(x_2)(x_4x_5)(x_6x_8x_7)\end{array}$$

Since $\tau_4\tau_{10}=\tau_{16}\neq\tau_7=\tau_{10}\tau_4$, $\mathrm{Aut}(X,r)$ is a non abelian group of order 18. Therefore, it can be (isomorphic to) $\mathfrak{D}_{18}$, or $\mathfrak{D}_6\times\mathbb{Z}_3$, or $(\mathbb{Z}_3\times\mathbb{Z}_3)\rtimes\mathbb{Z}_2$ where $\rtimes$ denotes the semidirect product (see [20, Ch. 5.3] for a table of classification of groups of orders up to 20). But

$$\mathrm{Aut}(X,r)=\left\{\begin{array}{ll}\mathrm{Id}_{\{x_i\}_{i=1}^5}, & (x_1x_2x_3)(x_4)(x_5)\\ (x_1)(x_2x_3)(x_4x_5), & (x_1x_3x_2)(x_4)(x_5)\\ (x_1x_2)(x_3)(x_4x_5), & (x_1x_3)(x_2)(x_4x_5)\end{array}\right\}\times\left\{\begin{array}{l}\mathrm{Id}_{\{x_i\}_{i=6}^8}\\ (x_6x_7x_8)\\ (x_6x_8x_7)\end{array}\right\}\cong\mathfrak{D}_6\times\mathbb{Z}_3,$$

which can be presented as the group generated by $\{\tau_2,\tau_4,\tau_{10}\}$ with relations

$$\left\{\begin{array}{ll}\tau_2^3=\tau_4^2=\tau_{10}^3=\mathrm{Id}_X, & \tau_{10}\tau_4=\tau_4\tau_{10}^2\\ \tau_2\tau_4=\tau_4\tau_2, & \tau_4\tau_{10}=\tau_{10}\tau_4\end{array}\right\}.$$

3.2.27 Remark. The converse of 3.2.23 is not always true, as it shows the following example. Let $X = \{a, b, c, x_1, x_2, x_3\}$ and r be the square-free solution given by

$$\mathcal{C}(X, r) = \{\ (a)(x_1x_2x_3),\ (b)(x_1x_2x_3),\ (c)(x_3x_2x_1)\}.$$

Let $\tau = (a)(bc)(x_1)(x_2)(x_3) \in \mathrm{Sym}(X)$. The stars of all elements of X verify $\mathrm{Star}(x) \sim \mathrm{Star}(\tau(x))$. However, $\tau \notin \mathrm{Aut}(X, r)$ since

$$(\tau \circ \mathcal{L}_b)(x_1) = x_2 \neq x_3 = (\mathcal{L}_{\tau(b)} \circ \tau)(x_1).$$

3.2.2 Extensions of solutions

The aim of this section is to find methods (see e.g. Algorithms 21 and 22) for constructing new solutions by gluing two already known solutions. The study of *extensions* of solutions is necessary not only for constructing new solutions, but also for understanding their structure. The main results of this section are also shown in [33].

We first recall some definitions which can be found in [21].

3.2.28 Definition. [21] Let (Z, r) be a solution

1. A non-empty set $Y \subseteq Z$ is said to be an r-*invariant* subset of Z if $r(Y \times Y) \subseteq Y \times Y$.

2. (Z, r) is *decomposable* if there exist two non-empty r-invariant subsets X and Y of Z such that $Z = X \cup Y$ is a disjoint union. Otherwise, (X, r) is said to be *indecomposable*.

Clearly, the trivial solution (X, r) is decomposable when $|X| \geq 2$.

3.2.29 Remark. Note that the nondegeneracy of a solution (resp. square-free solution) (Z, r), together with the finiteness of the set Z, implies that each r-invariant subset Y is nondegenerate, and hence, the restriction $r_{|Y\times Y}$ of r to $Y \times Y$ provides a solution (resp. square-free solution) $(Y, r_{|Y\times Y})$.

Moreover, if (Z, r) is a solution and Z decomposes into the r-invariant subsets X, Y, then the restriction maps $\mathcal{L}_{x|X}, \mathcal{R}_{x|X}, \mathcal{L}_{y|X}, \mathcal{R}_{y|X}$ are permutations of X for all $x \in X$, $y \in Y$, and analogously, $\mathcal{L}_{y|Y}, \mathcal{R}_{y|Y}, \mathcal{L}_{x|Y}, \mathcal{R}_{x|Y}$ are elements of $\mathrm{Sym}(Y)$. Indeed, since $(X, r_{|X\times X})$ and $(Y, r_{|Y\times Y})$ are solutions, $\mathcal{L}_{x|X}, \mathcal{R}_{x|X} \in \mathrm{Sym}(X)$ and $\mathcal{L}_{y|Y}, \mathcal{R}_{y|Y} \in \mathrm{Sym}(Y)$. Moreover, the epimorphic image of the map $\mathcal{L}_{y|X} : X \longrightarrow Z$ is exactly X, otherwise, if there exists $x \in X$ such that $\mathcal{L}_y(x) \in Y$, then, as $\mathcal{L}_{y|Y} \in \mathrm{Sym}(Y)$, there exists $y_1 \in Y$ for which

$\mathcal{L}_y(x) = \mathcal{L}_y(y_1)$, but from injectiveness of $\mathcal{L}_y : Z \longrightarrow Z$ it follows that $x = y_1$ - a contradiction. Hence, $\mathcal{L}_{y_{|X}} \in \mathrm{Sym}(X)$. Similar ideas can be used for the remaining restriction maps.

From Remark 3.2.29, one can prove the following fact.

3.2.30 Lemma. [21] *If a solution (Z, r) can be decomposed into the (non-degenerate) r-invariant subsets X, Y, then r induces bijections $r_{|X\times Y} : X \times Y \longrightarrow Y \times X$, and $r_{|Y\times X} : Y \times X \longrightarrow X \times Y$. Moreover, $r^{-1}_{|X\times Y} = r_{|Y\times X}$.*

From the following result we obtain that for any solution (X, r), every orbit $\mathcal{O}_y$ ($y \in X$) under the left action of the associated group $\mathcal{G}(X, r)$ on X is an r-invariant subset of X and hence, $(\mathcal{O}_y, r_{|\mathcal{O}_y\times\mathcal{O}_y})$ is a solution.

3.2.31 Lemma. *Let (X, r) be a solution, written as $r(yz) = \mathcal{L}_y(z)\mathcal{R}_z(y)$. For all $y, z \in X$ it holds*

1. *$\mathcal{L}_y(\mathcal{O}_z) \subseteq \mathcal{O}_z$ and $\mathcal{R}_z(\mathcal{O}_y) \subseteq \mathcal{O}_y$;*
2. *$r(\mathcal{O}_y \times \mathcal{O}_z) \subseteq \mathcal{O}_z \times \mathcal{O}_y$;*
3. *$\mathcal{O}_y$ is r-invariant,*

where $\mathcal{O}_y$ denotes the orbit of $y \in X$ under the left action of $\mathcal{G}(X, r)$ on X.

Proof. Obviously $\mathcal{L}_y(\mathcal{O}_z) \subseteq \mathcal{O}_z$. From involutiveness of r, for all $t, z \in X$ we have

$$(t, z) \xrightarrow{r} (\mathcal{L}_t(z), \mathcal{R}_z(t)) \xrightarrow{r} (\mathcal{L}_{\mathcal{L}_t(z)}\mathcal{R}_z(t), \mathcal{R}_{\mathcal{R}_z(t)}\mathcal{L}_t(z)) = (t, z),$$

Therefore, $t = \mathcal{L}_g(\mathcal{R}_z(t))$ for some $g \in \mathcal{G}(X, r)$. Thus, for all $t \in \mathcal{O}_y$, namely $t = \mathcal{L}_h(y)$ with $h \in \mathcal{G}(X, r)$, it holds that

$$\mathcal{R}_z(t) = ((\mathcal{L}_g)^{-1} \circ \mathcal{L}_h)(y) = \mathcal{L}_{g^{-1}h}(y).$$

Hence, $\mathcal{R}_z(\mathcal{O}_y) \subseteq \mathcal{O}_y$. It clearly follows that $r(\mathcal{O}_y \times \mathcal{O}_z) \subseteq \mathcal{O}_z \times \mathcal{O}_y$, and in particular, $r(\mathcal{O}_y \times \mathcal{O}_y) \subseteq \mathcal{O}_y \times \mathcal{O}_y$. □

3.2.32 Remark. A solution (X, r) is decomposable if, and only if, the associated group $\mathcal{G}(X, r)$ acts non-transitively on X via the left action $\mathcal{L}$ (see [21]). W. Rump proved that every solution (X, r) is decomposable, provided that (X, r) is square-free (cf. [40]).

The first part of the following result appears in [40].

3.2.33 Corollary. *Every solution (X,r) of the YBE can be decomposed into a finite disjoint union of r-invariant subsets. More precisely,*

$$X = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_k,$$

where $\mathcal{O}_1, \ldots, \mathcal{O}_k$ are the orbits under the left action $\mathcal{L}$ of the associated group $\mathcal{G}(X,r)$ on X. Hence, (X,r) induces solutions $(\mathcal{O}_i, r_{|\mathcal{O}_i \times \mathcal{O}_i})$, for all $1 \leq i \leq k$.
Furthermore, if (X,r) is square-free, then $k \geq 2$, and therefore, $\mathcal{G}(X,r)$ acts non-transitively on X and the induced solutions $(\mathcal{O}_i, r_{|\mathcal{O}_i \times \mathcal{O}_i})$ are also square-free.

Proof. Lemma 3.2.31 proves the first part of the result. Since every square-free solution is decomposable, we can deduce the second part. Indeed, if the square-free solution (X,r) decomposes into the r-invariant subsets X_1, X_2, then we can write

$$X = X_1 \cup X_2 \subseteq (\bigcup_{y \in X_1} \mathcal{O}_y) \cup (\bigcup_{z \in X_2} \mathcal{O}_z), \tag{3.16}$$

where $\mathcal{O}_x$ denotes the orbit of the element $x \in X$ under the left action $\mathcal{L}$ of $\mathcal{G}(X,r)$ on X. Let us check that $\mathcal{O}_y \subseteq X_1$, for all $y \in X_1$. Note that it is enough to prove that $\mathcal{L}_x(x_1) \in X_1$ for all $x \in X$ and $x_1 \in X_1$ because in that case, $\mathcal{L}_g(y) \in X_1$ for all $g \in \mathcal{G}(X,r)$ and $y \in X_1$, and hence, $\mathcal{O}_y \subseteq X_1$. So, pick arbitrary elements $x \in X$, $x_1 \in X_1$. There are two possible cases: $x \in X_1$ or $x \in X_2$, but by virtue of 3.2.29, in both it holds that $\mathcal{L}_x(x_1) \in X_1$. Similarly, we can prove that $\mathcal{O}_z \subseteq X_2$ for all $z \in X_2$. Thus, we obtain that

$$X_1 = \bigcup_{y \in X_1} \mathcal{O}_y \quad \text{and} \quad X_2 = \bigcup_{z \in X_2} \mathcal{O}_z,$$

where each union consists of at least one orbit since X_1 and X_2 are non-empty sets. Finally, from (3.16) and finiteness of the set X we conclude that

$$X = (\bigcup_{i=1}^{k} \mathcal{O}_{y_i}) \cup (\bigcup_{j=1}^{l} \mathcal{O}_{z_j})$$

where $y_i \in X_1$, $z_j \in X_2$, $k \geq 1$ and $l \geq 1$. □

3.2.34 Example. Consider the square-free solution (X,r) described in Example 3.1.31. Since the orbits of (X,r) are $X_1 = \{x_5, x_6\}$ and $X_2 = \{x_1, \ldots, x_4\}$, (X,r) decomposes into the r-invariant subsets X_1, X_2. Hence, (X,r) induces the square-free solutions (X_1, r_1) and (X_2, r_2), where r_1 is the trivial solution and r_2 is given by $\mathcal{C}(X_2, r_2) = \{(x_4 x_3)(x_2 x_1)\}$ (see Fig. 3.13).

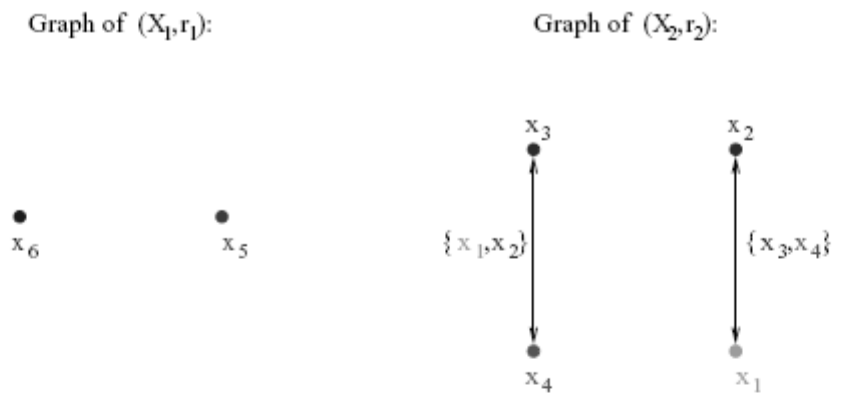


Figure 3.13: Graphs of the solutions constructed from the orbits of the solution of Fig. 3.1.

3.2.35 Definition. [21] Let (X,r_X), (Y,r_Y) be solutions. A solution (Z,r) is a *union* of (X,r_X) and (Y,r_Y), or an *extension* of X by Y, if $X\cap Y=\emptyset$, $Z=X\cup Y$ as sets, $r_{|X\times X}=r_X$ and $r_{|Y\times Y}=r_Y$.
The set of all extensions of X by Y is denoted by $\mathrm{Ext}(X,Y)$. Clearly, $\mathrm{Ext}(Y,X)=\mathrm{Ext}(X,Y)$. We will often denote $\mathrm{Ext}(X,Y)$ by $\mathrm{Ext}(X,r_X,Y,r_Y)$ (for emphasizing the extended solutions (X,r_X), (Y,r_Y)).

Note that a solution (Z,r) is decomposable into the r-invariant subsets X,Y of Z if, and only if, $Z\in\mathrm{Ext}(X,r_{|X\times X},Y,r_{|Y\times Y})$.

3.2.36 Remark. Let (Z,r), (X,r_X), (Y,r_Y) be solutions. If $Z\in\mathrm{Ext}(X,Y)$, then

1) by virtue of 3.2.30, (Z,r) is uniquely determined by the map $r_{|X\times Y}$ (or equivalently, by $r_{|Y\times X}$);

2) from 3.1.21 and 3.2.29, writing r as $r(z_1,z_2)=(\mathcal{L}_{z_1}(z_2),\mathcal{R}_{z_2}(z_1))$, we have that the assignments $x\mapsto\mathcal{L}_{x|Y}$, $y\mapsto\mathcal{R}_{y|X}^{-1}$ for $x\in X$, $y\in Y$ give left actions of $\mathcal{G}(X,r_X)$ on Y and of $\mathcal{G}(Y,r_Y)$ on X, respectively;

3) (X,r_X) and (Y,r_Y) are square-free if, and only if, (Z,r) is square-free.

Next we find a suitable bijection $r_{|X\times Y}:X\times Y\longrightarrow Y\times X$, constructed by using automorphisms, which (uniquely) determines an extension (Z,r) of two disjoint solutions (X,r_X), (Y,r_Y). The solution (Z,r) obtained by this method is an example of the so-called *(generalized) twisted unions* studied e.g. in [21, 40].

3.2.37 Proposition. [25] *Let (X, r_X) and (Y, r_Y) be solutions such that $X \cap Y = \emptyset$, and let $\tau_X \in \mathrm{Aut}(X, r_X)$ and $\tau_Y \in \mathrm{Aut}(Y, r_Y)$. If $Z = X \cup Y$ and*

$$\begin{array}{rcll} r : Z \cup Z & \longrightarrow & Z \cup Z & \\ (x_1, x_2) & \mapsto & r_X(x_1, x_2), & (x_1, x_2) \in X \times X, \\ (y_1, y_2) & \mapsto & r_Y(y_1, y_2), & (y_1, y_2) \in Y \times Y, \\ (x, y) & \mapsto & (\tau_Y^{-1}(y), \tau_X^{-1}(x)), & (x, y) \in X \times Y, \\ (y, x) & \mapsto & (\tau_X(x), \tau_Y(y)), & (y, x) \in Y \times X, \end{array} \tag{3.17}$$

then (Z, r) is a solution, and therefore, $Z \in \mathrm{Ext}(X, Y)$.

Proof. It can easily be proved that r is bijective, involutive and nondegenerate. Finally, let us check the YB condition for all $(z_1, z_2, z_3) \in Z \times Z \times Z$. There are eight possible cases:

1) $(z_1, z_2, z_3) \in X \times X \times X$,
2) $(z_1, z_2, z_3) \in X \times X \times Y$,
3) $(z_1, z_2, z_3) \in X \times Y \times X$,
4) $(z_1, z_2, z_3) \in Y \times X \times X$,
5) $(z_1, z_2, z_3) \in Y \times Y \times Y$,
6) $(z_1, z_2, z_3) \in Y \times Y \times X$,
7) $(z_1, z_2, z_3) \in Y \times X \times Y$,
8) $(z_1, z_2, z_3) \in X \times Y \times Y$.

The cases 1) and 5) are obvious since (X, r_X) and (Y, r_Y) are solutions. The proofs for the cases 6), 7) and 8) are similar to the proofs for 2), 3) and 4), respectively. For the case 2), consider the YB diagram

$$\begin{array}{ccc} x_1\ x_2\ y & \xrightarrow{r_2} & x_1\ \tau_Y^{-1}(y)\ \tau_X^{-1}(x_2) \\ \downarrow{\scriptstyle r_1} & & \downarrow{\scriptstyle r_1} \\ \mathcal{L}_{x_1}(x_2)\ \mathcal{R}_{x_2}(x_1)\ y & & \tau_Y^{-1}\tau_Y^{-1}(y)\ \tau_X^{-1}(x_1)\ \tau_X^{-1}(x_2) \\ \downarrow{\scriptstyle r_2} & & \vdots{\scriptstyle r_2} \\ \mathcal{L}_{x_1}(x_2)\ \tau_Y^{-1}(y)\ \tau_X^{-1}\mathcal{R}_{x_2}(x_1) & \xrightarrow{r_1} & \tau_Y^{-1}\tau_Y^{-1}(y)\ \tau_X^{-1}\mathcal{L}_{x_1}(x_2)\ \tau_X^{-1}\mathcal{R}_{x_2}(x_1) \end{array}$$

which holds if, and only if,

$$r(\tau_X^{-1}(x_1), \tau_X^{-1}(x_2)) = (\tau_X^{-1}\mathcal{L}_{x_1}(x_2), \tau_X^{-1}\mathcal{R}_{x_2}(x_1)).$$

But this condition is satisfied since $\tau_X^{-1} \in \mathrm{Aut}(X, r_X)$. The cases 3) and 4) may similarly be proved. Hence, (Z, r) is a solution of the YBE which extends (X, r_X) and (Y, r_Y). □

3.2.38 Remark. Following the terminology of 3.2.37, if we assume that (X, r_X) and (Y, r_Y) are square-free and that the automorphisms τ_X and τ_Y are given by their decompositions into a product of disjoint cycles (considering also the cycles of length 1) as

$$\begin{array}{l} \tau_X = C_1 \cdots C_r, \text{ where } C_i = (x_1^i \cdots x_{r_i}^i) \text{ for all } 1 \leq i \leq r, \\ \tau_Y^{-1} = C_1' \cdots C_s', \text{ where } C_j' = (y_1^j \cdots y_{s_j}^j) \text{ for all } 1 \leq j \leq s, \end{array}$$

then the (square-free) solution r given in the formula (3.17) can be described by the set of pairs of relative cycles as

$$\mathcal{C}(Z,r) = \mathcal{C}(X,r_X) \cup \mathcal{C}(Y,r_Y) \cup \{\, \sigma_{ij} = C_i C'_j \,/\, 1 \leq i \leq r,\ 1 \leq j \leq s\}.$$

In this set up, each σ_{ij} represents the relations

$$y_l^j x_k^i = \sigma_{ij}(x_k^i)\sigma_{ij}^{-1}(y_l^j), \quad x_k^i y_l^j = \sigma_{ij}(y_l^j)\sigma_{ij}^{-1}(x_k^i),$$

for all $1 \leq l \leq s_j$ and $1 \leq k \leq r_i$.

From 3.2.37 and 3.2.38 we devise Algorithm 21 which returns an extension (Z,r) of two square-free solutions (X,r_X), (Y,r_Y).

Algorithm 21 Gluing square-free solutions by using automorphisms

Require: (X,r_X) and (Y,r_Y), two square-free solutions of the YBE, $\tau_X \in \mathrm{Aut}(X,r_X)$ and $\tau_Y \in \mathrm{Aut}(Y,r_Y)$;

Ensure: (Z,r) a new square-free solution with $Z = X \cup Y$ such that $r_{|X\times X} = r_X$ and $r_{|Y\times Y} = r_Y$;

Let $\tau_X = C_1 \cdots C_r$ and $\tau_Y = c_1 \cdots c_s$ the decompositions of τ_X and τ_Y into a product of disjoint cycles of lengths ≥ 1;

If $c_j = (y_1^j \cdots y_{s_j}^j)$ for $1 \leq j \leq s$, let $\tau_Y^{-1} := C'_1 \cdots C'_s$, with $C'_j := (y_{s_j}^j \cdots y_1^j)$;

Let $Z := X \cup Y$;

$\mathcal{C}(Z,r) := \mathcal{C}(X,r_X) \cup \mathcal{C}(Y,r_Y) \cup \{\, \sigma_{ij} = C_i C'_j \,/\, 1 \leq i \leq r,\ 1 \leq j \leq s\}$;

Return $\mathcal{C}(Z,r)$.

3.2.39 Example. Let (X,r_X) be the square-free solution

$$\mathcal{C}(X,r_X) = \{(x_6)(x_3x_2x_1),\ (x_5x_4)(x_3x_2x_1)\}, \tag{3.18}$$

whose graph is represented by Fig. 3.14, and let (Y,r_Y) be the square-free solution given by

$$\mathcal{C}(Y,r_Y) = \{(y_9y_7)(y_5y_4y_3y_2y_1),\ (y_8y_6)(y_5y_1y_2y_3y_4)\}, \tag{3.19}$$

represented in Fig. 3.15.

Let

$$\tau_X = (x_1x_2x_3)(x_4x_5)(x_6) \in \mathrm{Aut}(X,r_X),$$
$$\tau_Y = \tau_Y^{-1} = (y_1)(y_2)(y_3)(y_4)(y_5)(y_6y_8)(y_7y_9) \in \mathrm{Aut}(Y,r_Y).$$

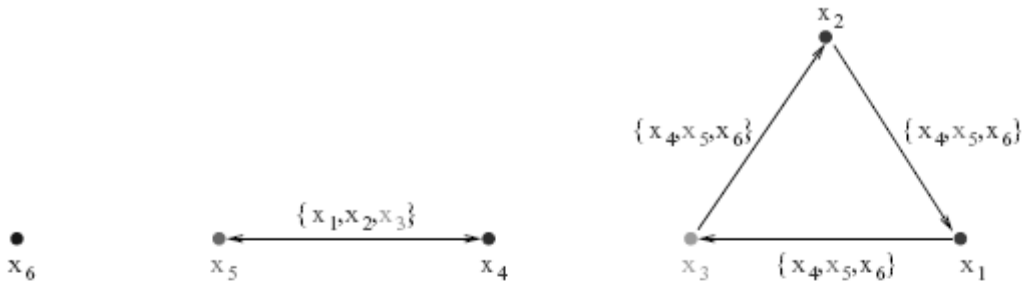


Figure 3.14: Graph of the solution given by (3.18).

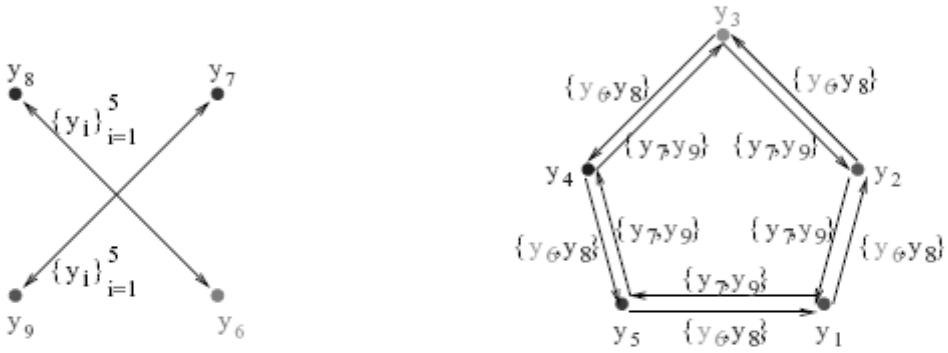


Figure 3.15: Graph of the solution given by (3.19).

Following Algorithm 21, the set of relations $\{C_iC'_j \,/\, 1 \leq i \leq 3,\ 1 \leq j \leq 7\}$ consists of

$$\begin{array}{lll} (x_1x_2x_3)(y_i),\ 1 \leq i \leq 5, & (x_1x_2x_3)(y_6y_8), & (x_1x_2x_3)(y_7y_9), \\ (x_4x_5)(y_i),\ 1 \leq i \leq 5, & (x_4x_5)(y_6y_8), & (x_4x_5)(y_7y_9), \\ (x_6)(y_i),\ 1 \leq i \leq 5, & (x_6)(y_6y_8), & (x_6)(y_7y_9). \end{array}$$

Hence,

$$\mathcal{C}(Z,r) = \left\{ \begin{array}{ll} (y_9y_7)(y_5y_4y_3y_2y_1), & (y_9y_7)(x_6) \\ (y_9y_7)(x_5x_4), & (y_9y_7)(x_3x_1x_2) \\ (y_8y_6)(y_5y_1y_2y_3y_4), & (y_8y_6)(x_6) \\ (y_8y_6)(x_5x_4), & (y_8y_6)(x_3x_1x_2) \\ (y_i)(x_6),\ \ 1 \leq i \leq 5 & (y_i)(x_5x_4),\ \ 1 \leq i \leq 5 \\ (y_i)(x_3x_1x_2),\ \ 1 \leq i \leq 5 & (x_6)(x_3x_2x_1) \\ (x_5x_4)(x_3x_2x_1) & \end{array} \right\} \tag{3.20}$$

defines a square-free solution on $Z = \{x_i\}_{i=1}^{6} \cup \{y_i\}_{i=1}^{9}$, whose graph is represented in Fig. 3.16.

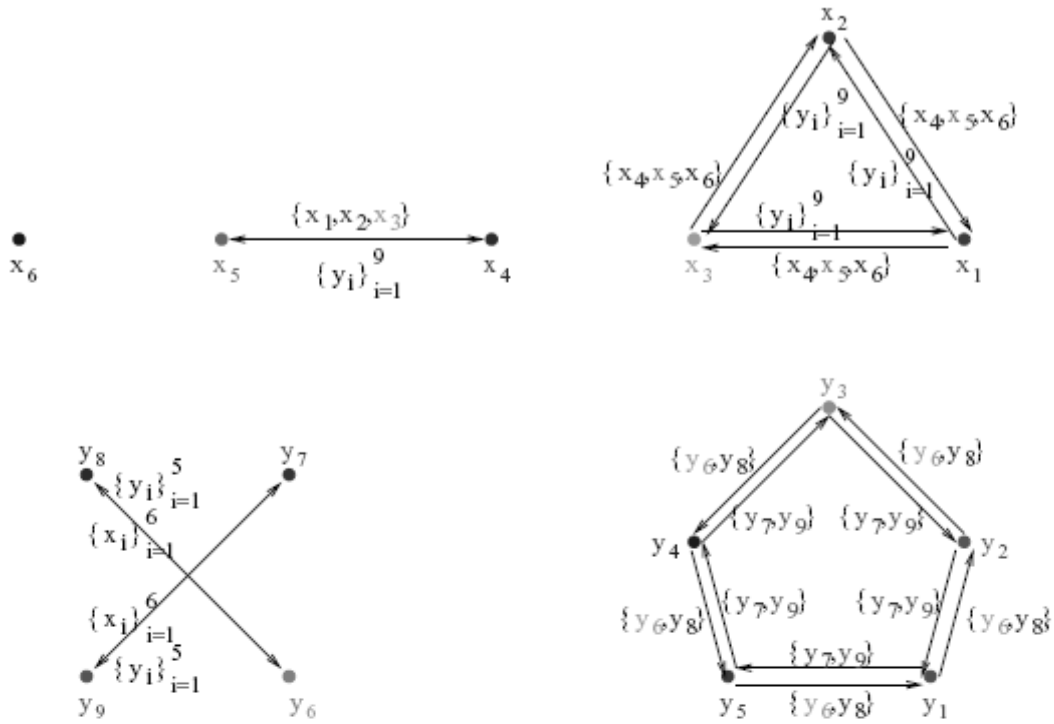


Figure 3.16: Graph of the solution given by (3.20).

The following result, due to Majid and Gateva-Ivanova, gives a necessary and sufficient condition for obtaining an extension of two disjoint solutions (X, r_X) and (Y, r_Y) in terms of their Yang-Baxter groups. Moreover, since all square-free solutions are decomposable, it covers all possible constructions of solutions restricted to the square-free case.

3.2.40 Theorem. (cf. [40]) *Let (X, r_X), (Y, r_Y) be disjoint solutions with associated groups $\mathcal{G}(X, r_X)$ and $\mathcal{G}(Y, r_Y)$ respectively. Suppose that $Z = X \cup Y$ and that the bijective map $r : Z \times Z \longrightarrow Z \times Z$ is an extension of r_X and r_Y. Then, (Z, r) is a solution if, and only if, $(\mathcal{G}(X, r_X), \mathcal{G}(Y, r_Y))$ is a matched pair of groups, in the sense of Majid* [67].

Next we consider a special case of *one-sided* extensions.

3.2.41 Definition. [21] An element $Z \in \mathrm{Ext}(X, Y)$ is a *left* (resp. *right*) *extension of Y by X* if $r(y, x) = (\mathcal{L}_y(x), y)$ (resp. $r(y, x) = (x, \mathcal{R}_x(y))$). The set of the left (resp. right) extensions of Y by X will be denoted by $Ext_-(Y, X)$ (resp. $\mathrm{Ext}_+(Y, X)$).

We will often denote $\mathrm{Ext}_-(Y, X)$ (resp. $\mathrm{Ext}_+(Y, X)$) by $\mathrm{Ext}_-(Y, r_Y, X, r_X)$

(resp. $\mathrm{Ext}_+(Y, r_Y, X, r_X)$) (for emphasizing the solutions (X, r_X), (Y, r_Y)).

3.2.42 Proposition. *Let $Z \in \mathrm{Ext}(X, Y)$ (recall from 3.2.30 that the restriction maps $\mathcal{L}_{y|X}$, $\mathcal{R}_{y|X}$, $\mathcal{L}_{x|Y}$ and $\mathcal{L}_{x|Y}$ are bijections).*

1) If $Z \in \mathrm{Ext}_-(Y, X)$, then

$$\mathcal{L}_{y|X} = \mathcal{R}_{y|X}^{-1} \quad \text{and} \quad r(x, y) = (y, \mathcal{L}_y^{-1}(x)), \quad \forall\, x \in X,\ y \in Y; \tag{3.21}$$

2) $\mathrm{Ext}_-(Y, X) = \mathrm{Ext}_+(X, Y)$;

3) If $Z \in \mathrm{Ext}_+(Y, X)$, then

$$\mathcal{L}_{x|Y} = \mathcal{R}_{x|Y}^{-1} \quad \text{and} \quad r(x, y) = (\mathcal{R}_x^{-1}(y), x) \quad \forall\, x \in X,\ y \in Y;$$

4) Suppose that $Z \in \mathrm{Ext}_-(Y, X)$ or $Z \in \mathrm{Ext}_+(Y, X)$. If (X, r_X) is square-free, then

$$\mathcal{R}_x = \mathcal{L}_x^{-1} : Z \longrightarrow Z, \quad \forall\ x \in X$$

and simmetrically, if (Y, r_Y) is square-free, then

$$\mathcal{R}_y = \mathcal{L}_y^{-1} : Z \longrightarrow Z, \quad \forall\ y \in Y.$$

Proof. The statement 1) follows from involutiveness of r:

$$(y, x) \xrightarrow{r} (\mathcal{L}_y(x), y) \xrightarrow{r} (\mathcal{L}_{\mathcal{L}_y(x)}(y), \mathcal{R}_y\mathcal{L}_y(x)) = (y, x).$$

The statement 2) is a direct consequence of 1). The proof of 3) is analogous to the one of 1). Finally, since $\mathcal{R}_{x|Y} = \mathcal{L}_{x|Y} = \mathrm{Id}_Y$ when $Z \in \mathrm{Ext}_-(Y, X)$ (and $\mathcal{L}_{x|Y} = \mathcal{R}_{x|Y}^{-1}$ when $\mathrm{Ext}_+(Y, X)$), square-freeness of (X, r_X) implies $\mathcal{R}_x = \mathcal{L}_x^{-1}$ as permutations of Z, which proves 4). □

From the following result we obtain a group-theoretic description of $\mathrm{Ext}_-(Y, X)$.

3.2.43 Theorem. *Let (X, r_X) and (Y, r_Y) be disjoint solutions.*

1. *If $Z \in Ext_-(Y, X)$, then for all $y \in Y$, $\mathcal{L}_{y|X} \in \mathrm{Aut}(X, r_X)$;*
2. *If $(Z, r) \in Ext_-(Y, X)$, then the assignment*

$$y \to \mathcal{L}_{y|X}, \text{ for } y \in Y$$

can be extended uniquely to a canonical group homomorphism

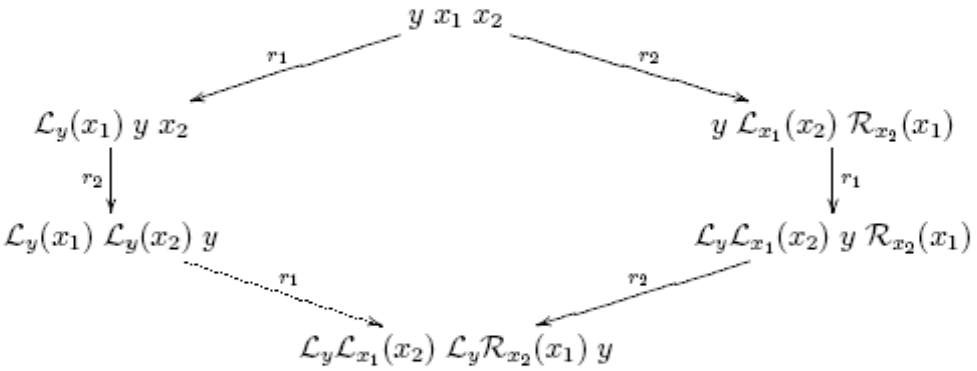
$$\varphi_Z : \mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r_X).$$

3. *Conversely, if* $\varphi : \mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r_X)$ *is a group homomorphism, then there is a unique solution* $(Z, r_\varphi) \in Ext_-(Y, X)$*, canonically determined by* φ*. Namely, for the disjoint union* $Z = Y \cup X$*, the map* $r_\varphi : Z \times Z \longrightarrow Z \times Z$ *extends* r_Y *and* r_X*, and it is defined on* $Y \times X$*, and* $X \times Y$*, respectively, as:*

$$r_\varphi(y, x) = (\varphi(y)(x), y), \quad r_\varphi(x, y) = (y, \varphi(y)^{-1}(x)), \tag{3.22}$$

for all $x \in X$*,* $y \in Y$*.*

Proof. Let us prove 1. Let $y \in Y$. We already know that $\mathcal{L}_{y|X} \in \mathrm{Sym}(X)$. Let us check that $\mathcal{L}_{y|X}$ is an r_X-automorphism. From statement 1 of 3.2.42 and the YB diagram



we get $r(\mathcal{L}_y(x_1), \mathcal{L}_y(x_2)) = (\mathcal{L}_y\mathcal{L}_{x_1}(x_2), \mathcal{L}_y\mathcal{R}_{x_2}(x_1))$. Hence, $\mathcal{L}_{y|X} \in \mathrm{Aut}(X, r_X)$.

The statement 2 is a consequence of property 2) of 3.2.36 since, by (3.21), $\mathcal{L}_{y|X} = \mathcal{R}_{y|X}^{-1}$ for all $y \in Y$.

Finally, let us check 3. Defined as in (3.22), r_φ is bijective and involutive. Nondegeneracy is clear since the maps $\mathcal{L}_{x|X}, \mathcal{L}_{y|X} = \varphi(y) : X \longrightarrow X$ and $\mathcal{L}_{x|Y} = \mathrm{Id}_Y, \mathcal{L}_{y|Y} : Y \longrightarrow Y$ are bijections for all $x \in X$, $y \in Y$. Let us check the YB condition for all $(z_1, z_2, z_3) \in Z \times Z \times Z$. There are eight possible cases as in the proof of 3.2.37. The YB condition holds in the cases 1) and 5) since (X, r_X) and (Y, r_Y) are solutions. The cases 3) and 4) can be reduced to the case 2) since $(x_1, y, x_2) = r_2(x_1, \varphi(y)(x_2), y)$ and $(y, x_1, x_2) = r_2r_1(\varphi(y)(x_1), \varphi(y)(x_2), y)$ for all $x_1, x_2 \in X$, $y \in Y$. Symmetrically, the

cases 7) and 8) can be reduced to the case 6). Let us check the case 2).

$$\begin{array}{ccc}
x_1\ x_2\ y & \xrightarrow{\quad r_2 \quad} & x_1\ y\ \varphi(y)^{-1}(x_2) \\
\downarrow r_1 & & \downarrow r_1 \\
\mathcal{L}_{x_1}(x_2)\ \mathcal{R}_{x_2}(x_1)\ y & & y\ \varphi(y)^{-1}(x_1)\ \varphi(y)^{-1}(x_2) \\
\downarrow r_2 & & \vdots\, r_2 \\
\mathcal{L}_{x_1}(x_2)\ y\ \varphi(y)^{-1}\mathcal{R}_{x_2}(x_1) & \xrightarrow{r_1} & y\ \varphi(y)^{-1}\mathcal{L}_{x_1}(x_2)\ \varphi(y)^{-1}\mathcal{R}_{x_2}(x_1)
\end{array}$$

The previous diagram is satisfied if, and only if,

$$r_X(\varphi(y)^{-1}(x_1), \varphi(y)^{-1}(x_2)) = (\varphi(y)^{-1}\mathcal{L}_{x_1}(x_2), \varphi(y)^{-1}\mathcal{R}_{x_2}(x_1)),$$

which is true since $\varphi(y)^{-1} \in \mathrm{Aut}(X, r_X)$. Finally, we check the YB condition for the case 6). For $y_1, y_2 \in Y$, $x \in X$,

$$\begin{array}{ccc}
y_1\ y_2\ x & \xrightarrow{\quad r_2 \quad} & y_1\ \varphi(y_2)(x)\ y_2 \\
\downarrow r_1 & & \downarrow r_1 \\
\mathcal{L}_{y_1}(y_2)\ \mathcal{R}_{y_2}(y_1)\ x & & \varphi(y_1)\varphi(y_2)(x)\ y_1\ y_2 \\
\downarrow r_2 & & \downarrow r_2 \\
\mathcal{L}_{y_1}(y_2)\ \varphi(\mathcal{R}_{y_2}(y_1))(x)\ \mathcal{R}_{y_2}(y_1) & \xrightarrow{r_1} & \varphi(y_1)\varphi(y_2)(x)\ \mathcal{L}_{y_1}(y_2)\ \mathcal{R}_{y_2}(y_1)
\end{array}$$

This diagram holds if, and only if,

$$r_\varphi(\mathcal{L}_{y_1}(y_2), \varphi(\mathcal{R}_{y_2}(y_1))(x)) = (\varphi(y_1)\varphi(y_2)(x), \mathcal{L}_{y_1}(y_2)),$$

or equivalently, if

$$(\varphi(\mathcal{L}_{y_1}(y_2))\varphi(\mathcal{R}_{y_2}(y_1))(x), \mathcal{L}_{y_1}(y_2)) = (\varphi(y_1)\varphi(y_2)(x), \mathcal{L}_{y_1}(y_2)).$$

The previous equality is satisfied since $y_1 y_2 = \mathcal{L}_{y_1}(y_2)\mathcal{L}_{y_2}^{-1}(y_1)$ in $G(Y, r_Y)$ and φ is a group homomorphism. □

3.2.44 Definition. We call the extension $(Z, r_\varphi) \in Ext_-(Y, X)$, given in Theorem 3.2.43, *the left extension of Y by X associated to φ*, and we shall often denote it by Z_φ. Symmetrically, $\varphi_Z \in \mathrm{Hom}(\mathcal{G}(Y, r_Y), \mathrm{Aut}(X, r_X))$ is called *the group homomorphism associated to the left extension* (Z, r_Z).

The result 3.2.45, which gives a complete description of $\mathrm{Ext}_-(Y, r_Y, X, r_X)$, can be regarded as a refined version of [21, Prop. 2.18], since our characterization is given in terms of group homomorphisms $\mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r_X)$, instead of $\mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Sym}(X)$ (left actions).

3.2.45 Corollary. *Let (X, r_X) and (Y, r_Y) be disjoint solutions. There exists a one-to-one canonical correspondence*

$$\begin{aligned} \mathrm{Hom}(\mathcal{G}(Y, r_Y), \mathrm{Aut}(X, r_X)) &\longleftrightarrow \mathrm{Ext}_-(Y, X), \\ \varphi &\to Z_\varphi \\ \varphi_Z &\leftarrow (Z, r_Z), \end{aligned}$$

where Z_φ and φ_Z are as in Theorem 3.2.43.

Note that the solution (Z, r) given by $r_{|X\times X} = r_X$, $r_{|Y\times Y} = r_Y$ and $r_{|X\times Y}$ the flip map $r(x, y) = (y, x)$, is always an element of $\mathrm{Ext}_-(Y, X)$. Indeed, it is the solution Z_φ associated to the group homomorphism $\varphi : \mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r)$; $y \mapsto \mathrm{Id}_X$, for all $y \in Y$.

3.2.46 Remark. (cf. [21]) If $Z \in \mathrm{Ext}_-(Y, X)$, then its associated group $\mathcal{G}(Z, r)$ is isomorphic to the semidirect product $\mathcal{G}(Y, r_Y) \ltimes \mathcal{G}(X, r_X)$ of the groups of (X, r_X) and (Y, r_Y), formed using the left action of $\mathcal{G}(Y, r_Y)$ on X via $y \to \mathcal{R}_{y|X}^{-1}$.

In the spirit of 3.2.45 we devise Algorithm 22 to compute $\mathrm{Ext}_-(Y, X)$. For two solutions (X, r_X), (Y, r_Y) with $Y = \{y_1, \ldots, y_n\}$, each group homomorphism $\varphi : \mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r_X)$ is uniquely determined by an n-tuple $(\tau_{y_1}, \ldots, \tau_{y_n}) \in (\mathrm{Aut}(X, r_X))^n$, just setting $\varphi(y_i) = \tau_{y_i}$. Amongst all possible such n-tuples we will look for those satisfying

$$\tau_{y_i} \circ \tau_{y_j} = \tau_{\mathcal{L}_{y_i}(y_j)} \circ \tau_{\mathcal{R}_{y_j}(y_i)}, \ \forall\, y_i y_j = \mathcal{L}_{y_i}(y_j)\mathcal{R}_{y_j}(y_i) \in \Re(Y, r_Y). \tag{3.23}$$

Algorithm 22 Left extensions

Require: (X, r_X) and (Y, r_Y), solutions of the YBE, with $Y = \{y_1, \ldots, y_n\}$;
Ensure: Ext_YX, the set of left extensions of Y by X;

Initialization: Let φ be an empty list;
Let $\{\tau_1, \ldots, \tau_m\}$ be the group $\mathrm{Aut}(X, r_X)$ (computed using, e.g., Algorithm 20 if (X, r_X) is square-free);
Leftext(φ,0); {call to Algorithm 23}
Return Ext_YX.

In order to construct a more efficient method for obtaining (some) elements $Z \in \mathrm{Ext}(X, r_X, Y, r_Y)$, we may consider only the group homomorphisms $\mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r_X)$ which act as a constant on each $\mathcal{G}(Y, r_Y)$-orbit of (Y, r_Y).

Algorithm 23 Leftext

Require: φ, a list of elements of $\mathrm{Aut}(X, r_X)$ and $card\varphi$, the number of elements of φ;

if $(card\varphi = n)$ **then**

Let $r_\varphi : X \cup Y \longrightarrow X \cup Y$, such that $r_{\varphi|X\times X} := r_X$, $r_{\varphi|Y\times Y} =: r_Y$, $r_\varphi(y_j, x) := (\varphi[j](x), y_j)$, $r_\varphi(x, y_j) := (y_j, \varphi[j]^{-1}(x))$, for all $x \in X$, $1 \leq j \leq n$;

Let Ext_YX := Ext_$YX \cup \{r_\varphi\}$;

else

Let $\varphi' := \varphi$;

for i from 1 to m **do**

Let φ be the list $\varphi' \cup \tau_i$ and $card\varphi$, the number of elements of φ;

$Re := \{y_k y_l = y_s y_t \in \Re(Y, r_Y)/y_{card\varphi} \in \{y_k, y_l, y_s, y_t\}, 1 \leq k, l, s, t \leq card\varphi\}$;

Continue:= Yes;

while (Continue = Yes and $Re \neq \emptyset$) **do**

Take $y_k y_l = y_s y_t \in Re$;

$Re := Re \setminus \{y_k y_l = y_s y_t\}$;

if $\varphi[k] \circ \varphi[l] \neq \varphi[s] \circ \varphi[t]$ **then**

Continue:= No;

end if

end while

if Continue=Yes **then**

Leftext(φ,$card\varphi$); {call to Algorithm 23}

end if

end for

end if

3.2.47 Corollary. *Let (X, r_X) and (Y, r_Y) be disjoint solutions. Let $Y = \bigcup_{i=1}^{s} \mathcal{O}_i$ be the decomposition of Y into disjoint $\mathcal{G}(Y, r_Y)$-orbits (i.e., under the left action $\mathcal{L}_Y$ of $\mathcal{G}(Y, r_Y)$ on Y), and $\tau_1, \cdots \tau_s$ an s-tuple of (not necessarily pairwise distinct) elements of $\mathrm{Aut}(X, r_X)$. Then the assignment*

$$\varphi : y_i \to \tau_i, \quad \text{for all } y_i \in \mathcal{O}_i,\ 1 \leq i \leq s$$

can be extended to a group homomorphism $\varphi : \mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r_X)$ if, and only if,

$$\tau_i \circ \tau_j = \tau_j \circ \tau_i,\ \forall\, 1 \leq i < j \leq s. \tag{3.24}$$

In that case, $Z_\varphi \in \mathrm{Ext}_-(Y, X)$ (defined as in 3.2.44).

In the particular case that $\mathrm{Aut}(X, r_X)$ is abelian, this method provides $|\mathrm{Aut}(X, r_X)|^s$ elements Z_φ of $\mathrm{Ext}_-(Y, X)$.

Proof. The assignments $\varphi : y_i \to \tau_i$, for all $y_i \in \mathcal{O}_i$ and $1 \leq i \leq s$ can be extended to a group homomorphism $\varphi : \mathcal{G}(Y, r_Y) \longrightarrow \mathrm{Aut}(X, r_X)$ if, and only if,

$$\varphi(a) \circ \varphi(b) = \varphi(c) \circ \varphi(d), \quad \forall\, ab = cd \in \Re(Y, r_Y) \tag{3.25}$$

If $a \in \mathcal{O}_i$ and $b \in \mathcal{O}_j$, then from 3.2.31 we know that $c = \mathcal{L}_a(b) \in \mathcal{O}_j$ and $d = \mathcal{R}_b(a) \in \mathcal{O}_i$, and therefore, $\varphi(a) = \varphi(d) = \tau_i$ and $\varphi(b) = \varphi(c) = \tau_j$. Hence, condition (3.2.47) is equivalent to

$$\tau_i \circ \tau_j = \tau_j \circ \tau_i, \qquad \forall\, 1 \leq i, j \leq s.$$

Finally, due to "symmetry" of the previous equation, note that the integers i, j can be assumed to satisfy the less restrictive condition $1 \leq i < j \leq s$. □

As previously, we can devise an algorithm to obtain left extensions of Y by X given two solutions (X, r_X),(Y, r_Y). The drawback with respect to Algorithm 22 is that, obviously, we do not necessarily obtain the complete set $\mathrm{Ext}_-(Y, X)$. However, the size $s \leq n = |Y|$ of the tuples $(\tau_1, \ldots, \tau_s) \in (\mathrm{Aut}(X, r_X))^s$ can have positive repercussions on the computation time. Note that the condition (3.23) is translated into (3.24), which does not depend on the relations of the solution (Y, r_Y). Assuming that $\mathrm{Aut}(X, r_X) = \{\tau_1, \ldots, \tau_m\}$, in Algorithm 24 and 25 we introduce a global variable, a symmetric $(m \times m)$-matrix called *MatrixComm*, in order to avoid repeating checks of condition (3.24) (when, for example, $m << s$) . This matrix, defined for

all $1 \leq i, j \leq m$ by

$$MatrixComm[i,j] = MatrixComm[j,i] = \begin{cases} 1, \text{ if } \tau_i \circ \tau_j = \tau_j \circ \tau_i \\ -1, \text{ if } \tau_i \circ \tau_j \neq \tau_j \circ \tau_i \\ 0, \text{ if there is no information about commutativity of } \tau_i, \tau_j \end{cases}$$

will be completed (replacing the zeros by either 1, or -1) as the algorithm runs.

Algorithm 24 Left extensions (acting as constants on the $\mathcal{G}(Y, r_Y)$-orbits)

Require: (X, r_X) and (Y, r_Y), solutions of the YBE, where $Y = \bigcup_{i=1}^{s} \mathcal{O}_i$ is the decomposition of Y into disjoint $\mathcal{G}(Y, r_Y)$-orbits;

Ensure: The subset ext_YX of Ext_(Y, X) consisting of all possible left extensions (Z, r) of Y by X determined by $r(y, x) = (\tau_i(x), y)$ (with $\tau_i \in \mathrm{Aut}(X, r_X)$), for all $x \in X$, $y \in \mathcal{O}_i$ and $1 \leq i \leq s$;

Initialization: Let φ be an empty list, $ext\_YX = \emptyset$;

Let $\{\tau_1, \ldots, \tau_m\}$ be the group $\mathrm{Aut}(X, r_X)$ (see Algorithm 20 if (X, r_X) is square-free);

Let $MatrixComm$ be a matrix of size $m \times m$ with all entries equal to 0, except $MatrixComm[i,i] := 1$, for $1 \leq i \leq m$;

Leftextorbits(φ,0); {call to Algorithm 25}

Return ext_YX.

3.3 Yang-Baxter Algebras and equivalent structures

In this section we first recall some results of T. Gateva-Ivanova and M. Van den Bergh [42], who discovered close relations amongst square-free solutions of the YBE and some mathematical objects which appeared earlier in very different contexts: the *semigroups of I-type*, the *semigroups of skew-polynomial type* and the *Bieberbach groups*. In particular, a result recently proved by T. Gateva-Ivanova [40] is emphasized. This result states that square-free solutions of the YBE, semigroups of skew-polynomial type and semigroups of I-type are equivalent notions. We also justify that Yang-Baxter Algebras have PBW bases and we show how some Linear Programming problems describe the behaviour of semigroups of skew-polynomial type.

Algorithm 25 Leftextorbits

Require: φ, a list of elements of $\mathrm{Aut}(X, r_X)$ and $card\varphi$, the number of elements of φ;

if $(card\varphi = s)$ **then**

Let $r_\varphi : X \cup Y \longrightarrow X \cup Y$, such that $r_{\varphi|X\times X} := r_X$, $r_{\varphi|Y\times Y} =: r_Y$, $r_\varphi(y,x) := (\varphi[i](x), y)$, $r_\varphi(x,y) = (y, \varphi[i]^{-1}(x))$, for all $x \in X$, $y \in \mathcal{O}_i$ and $1 \leq i \leq s$;

Let $ext\_YX := ext\_YX \cup \{r_\varphi\}$;

else

Let $\varphi' := \varphi$;

for i from 1 to m **do**

Continue:= Yes; $j := 1$;

while (Continue = Yes and $j \leq card\varphi$) **do**

Let k be the index such that $\varphi[j] = \tau_k$;

if $MatrixComm[i,k] = -1$ **then**

Continue:= No;

else

if $MatrixComm[i,k] = 0$ **then**

if $\tau_i \circ \tau_k \neq \tau_k \circ \tau_i$ **then**

Continue:=No;

$MatrixComm[i,k] := -1$; $MatrixComm[k,i] := -1$;

else

$MatrixComm[i,k] := 1$; $MatrixComm[k,i] := 1$;

end if

end if

end if

$j := j + 1$;

end while

if Continue=Yes **then**

Let φ be the list $\varphi' \cup \tau_i$ and $card\varphi$, the number of elements of φ;

Leftextorbits(φ,$card\varphi$); {call to Algorithm 25}

end if

end for

end if

The notion of semigroup of skew-polynomial type comes from [35, 36], where the author introduces and studies the so-called *skew-polynomial rings with binomial relations*, or *binomial skew-polynomial rings*. The binomial skew-polynomial rings are a restricted class of the skew-polynomial rings considered in an earlier work by Artin and Schelter (cf. [4]). In [35, 36, 40], T. Gateva-Ivanova proves that skew-polynomial rings with binomial relations are left and right Noetherian, satisfy the Cyclic Condition (see property 6 in 3.1.19). Besides, the binomial skew-polynomial rings provide a new class of *Artin-Schelter regular rings* of arbitrary global dimension.

Together with these results on skew-polynomial rings with binomial relations appeared the notion of semigroups of skew-polynomial type (also called *binomial semigroups* in e.g. [53]), whose algebraic structure was studied in [42, 43, 53, et al.].

3.3.1 Definition. A semigroup $\mathcal{S}$ is called a *semigroup of skew-polynomial type* (or a *skew-polynomial semigroup*) if it has a *finite standard presentation* as a group generated by a totally ordered set of generators $X = \{x_1 \prec \cdots \prec x_n\}$ $(n \geq 2)$ with $\binom{n}{2}$ square-free defining relations

$$\Re = \{x_j x_i = x_{i'} x_{j'} \,/\, 1 \leq i < j \leq n, 1 \leq i' < j' \leq n\}$$

such that:

each monomial $x_i x_j$ with $i \neq j$ occurs in exactly one relation of $\Re$, and no monomial $x_i x_i$ occurs in any relation of $\Re$;

if $x_j x_i = x_{i'} x_{j'} \in \Re$ with $j > i$, then $i' < j'$ and $j > i'$ (this also implies $i < j'$, see [36, 40]);

the monomials $x_k x_j x_i$ for all $1 \leq i < j < k \leq n$ do not give rise to new relations in $\mathcal{S}$, or equivalently (by 1.1.25), the set $G = \{x_j x_i - x_{i'} x_{j'} \,/\, x_j x_i = x_{i'} x_{j'} \in \Re\}$ is a two-sided Gröbner basis for ${}_{k\langle X\rangle}\langle G\rangle_{k\langle X\rangle}$ with respect to any monomial order on $\langle X\rangle$ such that $x_{i'} x_{j'} \prec x_j x_i$, for all $1 \leq i < j \leq n$ (e.g., the degree lexicographical order $\preceq_{deglex}$ on $\langle X\rangle$).

3.3.2 Example. Let (X, r) be the square-free solution of the YBE given by

$$\begin{aligned}\mathcal{C}(X,r) = \{&(x_{12}x_{11})(x_7x_8x_9x_{10}),\ (x_{12}x_{11})(x_1x_2x_3x_4x_5x_6),\ (x_{10}x_8)(x_9x_7),\\ &(x_{10}x_9x_8x_7)(x_6x_5x_4x_3x_2x_1),\ (x_6x_4x_2)(x_5x_3x_1)\}.\end{aligned}$$

(see its graph in figure 3.17). In 3.3.18, we compute the order $\preceq$ on X

$$x_1 \prec x_3 \prec x_5 \prec x_2 \prec x_4 \prec x_6 \prec x_7 \prec x_9 \prec x_8 \prec x_{10} \prec x_{11} \prec x_{12}$$

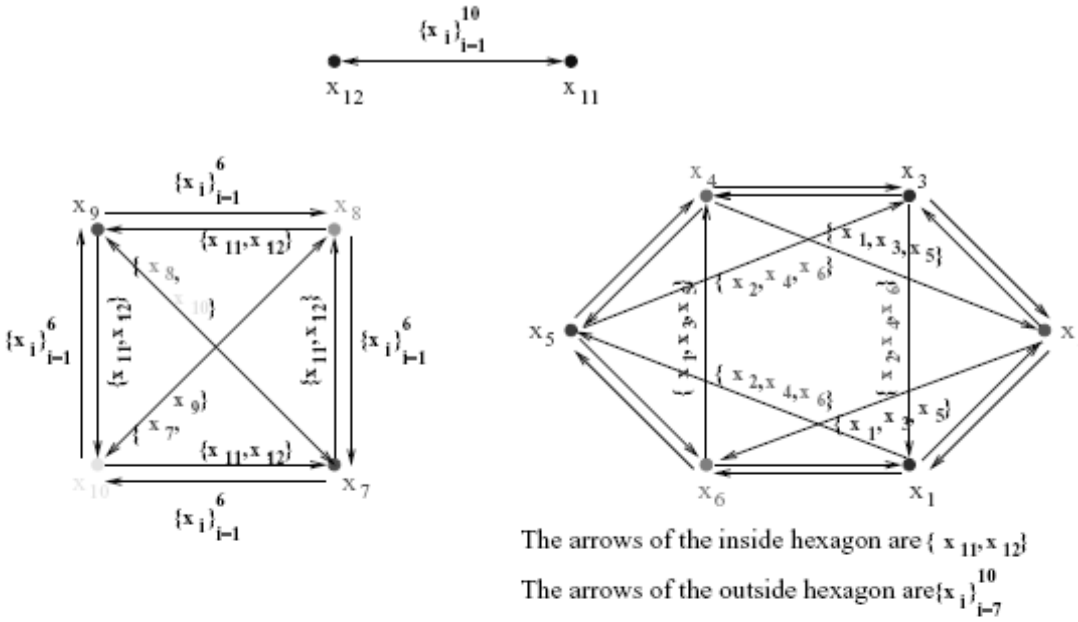


Figure 3.17: Graph of the square-free solution given in 3.3.2.

which satisfies condition 2) of 3.3.1 (renaming previously the variables $x_i's$ in such a way that they follow this order). Consider the set of relations of $\Re(X,r)$, each of them written as in 2). One can check that condition 1) and 3) also hold. Hence, the Yang-Baxter semigroup $\mathcal{S}(X,r)$ is a semigroup of skew-polynomial type.

3.3.3 Remarks. Let $\mathcal{S}$ be a semigroup of skew-polynomial type generated by X and with defining relations $\Re$. For any field k, let $\mathcal{A} = \mathsf{k}[\mathcal{S}]$ be the associated semigroup algebra, i.e., $\mathcal{A} = \mathsf{k}\langle X\rangle / I_{\Re}$, where $I_{\Re}$ denotes the two-sided ideal of $\mathsf{k}\langle X\rangle$

$$I_{\Re} = {}_{\mathsf{k}\langle X\rangle}\langle xy - \hat{y}\check{x} \;/\; xy = \hat{y}\check{x} \in \Re\rangle_{\mathsf{k}\langle X\rangle}.$$

The semigroup algebra $\mathcal{A}$ is a *binomial skew-polynomial ring* in the sense of [35, 36, 37], i.e., $\mathcal{A}$ is a graded standard finitely presented algebra $\mathcal{A} = \mathsf{k}\langle X\rangle / I_{\Re}$ such that the set of defining relations $\Re$ has the form

$$\Re = \{x_j x_i = c_{ij} u_{ij} \;/\; 1 \leq i < j \leq n\}$$

where $c_{ij} \in \mathsf{k} \setminus \{0\}$ and u_{ij} is a standard monomial of degree 2 satisfying $u_{ij} \prec x_j x_i$ for all $1 \leq i < j \leq n$, and the set

$$F = \{x_j x_i - c_{ij} u_{ij} \;/\; 1 \leq i < j \leq n\}$$

is the reduced Gröbner basis for the two-sided ideal ${}_{k\langle X\rangle}\langle F\rangle_{k\langle X\rangle}$ (for the degree lexicographical order $\preceq_{deglex}$ on $\langle X\rangle$).

- It is shown in [35, 36] that assuming 2) and 3), the condition 1) is necessary and sufficient for $\mathcal{A}$ to be (left and right) Noetherian.
- Condition 3) implies that $\mathcal{S}$ can be identified as a set with the set of ordered monomials:
$$\{x_1^{\alpha_1}\cdots x_n^{\alpha_n} \,/\, (\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n\},$$
which forms a PBW basis of $\mathcal{A}$ (see 1.2.4).
- Definition 3.3.1 is symmetric in the sense that $\mathcal{S}$ is a semigroup of skew-polynomial type if, and only if, its opposite semigroup $\mathcal{S}^{\rm op}$ is of skew-polynomial type.

Every semigroup of skew-polynomial type $\mathcal{S}$ defines a square-free solution via the set of relations.

3.3.4 Theorem. [42] *Let $\mathcal{S}$ be a semigroup of skew-polynomial type for a finite set of generators X and the set of relations $\Re$, and consider the map*

$$\begin{aligned} r_{\mathcal{S}} : X^2 &\longrightarrow X^2 \\ x_ix_i &\mapsto x_ix_i, \quad 1\le i\le n, \\ x_jx_i &\leftrightarrow x_{i'}x_{j'}, \quad \text{if } x_jx_i = x_{i'}x_{j'}\in\Re. \end{aligned}$$

Then, $(X, r_{\mathcal{S}})$ is a square-free solution of YBE.

The notions of I- structure, and algebras and modules of I-type, were introduced and studied by J. Tate and M. Van den Bergh in their work about *Sklyanin* algebras (cf. [80]). The I-structure on an algebra $\mathcal{A}$ implies that $\mathcal{A}$ has the Hilbert series of the commutative polynomial ring in n variables, and that $\mathcal{A}$ satisfies nice homological properties, like to be a Koszul algebra, an Artin-Schelter regular algebra, etc. Besides, the I-type condition is a technical property, useful for computations. The notion of semigroup of I-type was formally introduced in [42], and it is analogous to the above-mentioned algebraic structures of I-type. In fact, the semigroup algebra of a semigroup of I-type over a field is an algebra of I-type. T. Gateva-Ivanova and M. Van den Bergh showed the equivalence of the notions of square-free solutions of the YBE and semigroups of I-type.

3.3.5 Definition. Let $\mathcal{S}$ be a semigroup generated by $X = \{x_1,\ldots,x_n\}$, and $\mathcal{U} = [u_1,\ldots,u_n]$ the free abelian semigroup generated by $\{u_1,\ldots,u_n\}$.

$\mathcal{S}$ is of *left I-type* if there exists a bijection $v : \mathcal{U} \longrightarrow \mathcal{S}$, called *left I-structure*, such that

i) $v(1) = 1$;
ii) $\{v(u_1 a), \ldots, v(u_n a)\} = \{x_1 v(a), \ldots, x_n v(a)\}$, for all $a \in \mathcal{U}$.

Note that if $\mathcal{S}$ is a semigroup of left I-type, then

$$\forall\, a \in \mathcal{U},\ \forall\, i \in \{1, \ldots, n\},\ \exists!\ x_{a,i} \in X \text{ s.t. } v(u_i a) = x_{a,i} v(a), \tag{3.26}$$

and $\{x_{a,i} \,/\, 1 \leq i \leq n\} = X$.
The definition and the properties of semigroups of *right I-type* are analogous.

3.3.6 Example. [42] Let $\mathcal{S}$ be the semigroup generated by $\{x, y\}$ with defining relations $\{x^2 = y^2\}$. Consider the doubly infinity graph shown in Fig. 3.18. For each $(\alpha, \beta) \in \mathbb{N}^2$, there exists a unique reduced directed *path* from

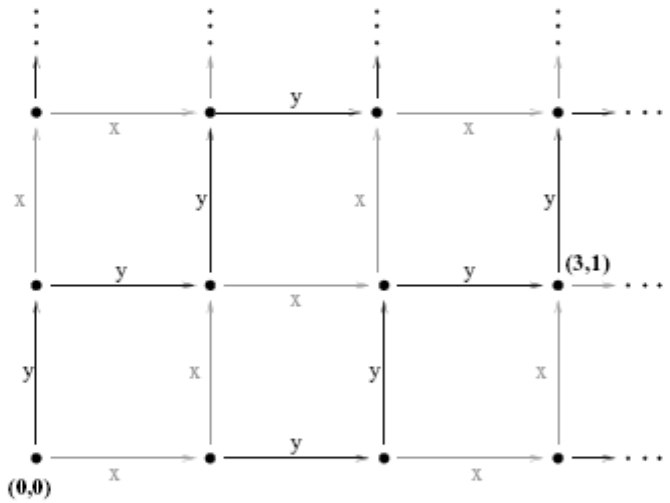


Figure 3.18: Graph representing the semigroup generated by $\{x, y\}$ with set of defining relations $\{x^2 = y^2\}$ described in 3.3.6

$(0, 0)$ to (α, β), which joins $(0, 0)$ with (α, β). For example, all possible ways to connect $(0, 0)$ with $(3, 1)$ are x^2yx, y^3x, yx^3, yxy^2 (see figure above), but all of them give the same reduced path since $x^2 = y^2$ in $\mathcal{S}$. Hence, the map

$$\begin{aligned} v : \mathcal{U} = [u_1, u_2] &\longrightarrow \mathcal{S} \\ (u_1^\alpha, u_2^\beta) &\mapsto v(u_1^\alpha, u_2^\beta) := \text{path from } (0,0) \text{ to } (\alpha, \beta) \end{aligned}$$

is well-defined and it makes $\mathcal{S}$ be of *I-type*.

The following result gives the equivalence of the notions of square-free solutions of the YBE and semigroups of left I-type.

3.3.7 Theorem. [42].

1. *Let $\mathcal{S}$ be a semigroup of left I-type, with left I-structure $v : [u_1, \ldots, u_n] \longrightarrow \mathcal{S}$, and let $r : X^2 \longrightarrow X^2$ be the map defined as*

$$r : x_{u_i,j}\, x_{1,i} \longleftrightarrow x_{u_j,i}\, x_{1,j}$$

Then, (X, r) is a square-free solution.

2. *Conversely, let (X, r) be a square-free solution and $\mathcal{S} = \mathcal{S}(X, r)$ the Yang-Baxter semigroup. Then $\mathcal{S}$ is of left I-type. More precisely, there exists a unique left (and right) I-structure $v : \mathcal{U} \longrightarrow \mathcal{S}$ satisfying $v(u_i) = x_i$, for all $1 \leq i \leq n$.*

3.3.8 Note. The map r in the statement 1 is defined for all pair in X^2 since, from bijectiv ness of v and Eq. (3.26), it follows that $X = \{x_{x_{1,k}}\}_{k=1}^n$ and $X = \{x_{u_i,k}\}_{k=1}^n$ for every u_i.

3.3.9 Remark. Since the Yang-Baxter semigroup $\mathcal{S}(X, r)$ of a square-free solution (X, r) is of (left and right) I-type, the Yang-Baxter Algebra $\mathcal{A}(\mathsf{k}, X, r)$, which is exactly the semigroup algebra $\mathsf{k}[\mathcal{S}(X, r)]$ associated to $\mathcal{S}(X, r)$, is an algebra of I-type for any field k (cf. [80]).

From the previous remark, the already known algebraic and homological properties of algebras of I-type are satisfied, in particular, by every Yang-Baxter Algebra $\mathcal{A}(\mathsf{k}, X, r)$. Some of these properties, picked up from [40, 42], are collected in the following result.

3.3.10 Theorem. [40, 42] *Let (X, r) be a square-free solution and let $\mathcal{S}(X, r)$, $\mathcal{G}(X, r)$ and $\mathcal{A}(k, X, r)$ be the associated Yang-Baxter semigroup, Yang-Baxter group and Yang-Baxter Algebra for any field k, respectively. Then the following conditions hold.*

1) $\mathcal{S}(X, r)$ is (left and right) cancelative and $\mathcal{G}(X, r)$ is its group of quotients;

2) $\mathcal{S}(X, r)$ is a Noetherian semigroup and $\mathcal{A}(k, X, r)$ is a Noetherian domain;

3) The Hilbert series of $\mathcal{A} = \mathcal{A}(k, X, r)$ is $H_{\mathcal{A}}(t) = \frac{1}{(1-t)^n}$;

4) $\mathcal{A}(k, X, r)$ is Koszul;

5) $\mathcal{A}(k, X, r)$ satisfies the Auslander condition;

6) $\mathcal{A}(k, X, r)$ is Cohen-Macaulay;

7) $\mathcal{A}(k, X, r)$ *is an Artin-Schelter regular ring of global dimension* n;

8) *The Koszul dual* $\mathcal{A}^!$ *of* $\mathcal{A} = \mathcal{A}(k, X, r)$ *is a Frobenius algebra;*

9) $\mathcal{S}(X, r)$ *satisfies a semigroup identity and* $\mathcal{A}(k, X, r)$ *satisfies a polynomial identity;*

10) $\mathcal{A}(k, X, r)$ *is catenary.*

3.3.11 Note. (cf. [40]) The proofs of the statements from 1) to 7) can be found in [42], where *Cohen-Macaulay* algebras and *Auslander condition* are defined in [63], and the notion of *Artin-Schelter regular ring* can be viewed in [4]. We can find the statement 8) in [37], whereas 9) is a consequence of a more general result shown in [43], in which certain semigroup algebras satisfy a polynomial identity. See [78] for the statement 10).

Theorem 3.3.4 and the Cyclic Condition (satisfied also by skew-polynomial semigroups) gave rise to a conjecture of T. Gateva-Ivanova, first reported in a talk at the *International Conference in Ring Theory* (Miskolc, 1996), which stated that every square-free solution can be obtained from a semigroup of skew-polynomial type. This conjecture, enunciated next, was recently proved in [40].

3.3.12 Proposition. [40] *Let* (X, r) *be a square-free solution of the YBE with* $|X| = n$, *then the set* X *can be ordered so that the associated semigroup* $\mathcal{S}(X, r)$ *is of skew-polynomial type. More precisely, the set* X *may be totally ordered in such a way that*

$$\forall\, x_j x_i = x_{i'} x_{j'} \in \Re(X, r) \text{ with } j > i \implies \begin{cases} i' < j' \\ j > i' \\ i < j' \end{cases} \tag{3.27}$$

(the last inequality, $i < j'$, *can be deduced from the first and second ones, see 3.3.1, cf. [36]), and therefore, the monomials* $x_k x_j x_i$ *for all* $1 \leq i < j < k \leq n$ *do not give rise to new relations in* $\mathcal{S}$.

As a consequence of 3.3.12 we prove, by an alternative way to that followed by Gateva-Ivanova in [40], that the set of standard monomials constitute a k-basis of the Yang-Baxter Algebra $\mathcal{A}(\mathsf{k}, X, r)$ associated to any square-free solution (X, r).

3.3.13 Proposition. *Let* (X, r) *be a square-free solution with* $X = \{x_1, \ldots, x_n\}$. *Then, the Yang-Baxter Algebra* $\mathcal{A}(k, X, r)$ *has a PBW basis, i.e., the set of standard monomials*

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \,/\, (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$$

is a k-basis of $\mathcal{A}(k, X, r)$.

Proof. By 3.3.12, we can assume the existence of an order $\preceq$ on $X = \{x_1 \prec \cdots \prec x_n\}$ satisfying (3.27). Then, the reduction system

$$Q = \{(x_j x_i, x_{i'} x_{j'}) \,/\, x_j x_i = x_{i'} x_{j'} \in \Re(X, r),\ 1 \leq i < j \leq n\}$$

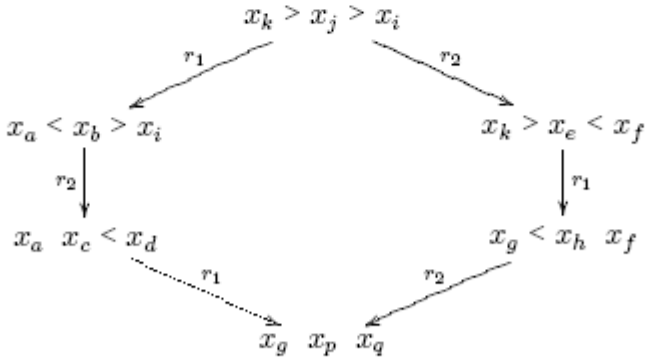
is compatible with the monomial order $\preceq_{deglex}$ on $\langle X \rangle$. From Theorem 1.2.4, it is enough to prove that $G = \{x_j x_i - x_{i'} x_{j'}\}_{j>i}$ is a two-sided Gröbner basis for the two-sided ideal I_Q generated by Q, or equivalently, by virtue of 1.1.25, that all ambiguities of Q are resolvable. Note that all ambiguities of Q are overlap ambiguities. If we denote $\sigma_{ji} = (x_j x_i, x_{i'} x_{j'})$ for all $1 \leq i < j \leq n$ where $r(x_j x_i) = x_{i'} x_{j'}$, then the overlaps of Q are

$$(\sigma_{kj}, \sigma_{ji}, x_k, x_j, x_i), \quad \forall\, 1 \leq i < j < k \leq n.$$

Let us pick $i < j < k$. Writing

$$\begin{array}{lll}
x_k x_j = x_a x_b, & k > j & \Longrightarrow\ a < b,\ k > a,\ j < b \\
x_b x_i = x_c x_d, & b > j > i & \Longrightarrow\ c < d,\ b > c,\ \ i < d \\
x_j x_i = x_e x_f, & j > i & \Longrightarrow\ e < f,\ j > e,\ \ i < f \\
x_k x_e = x_g x_h, & k > j > e & \Longrightarrow\ g < h,\ k > g,\ e < h \\
x_a x_c = x_l x_m, & & \\
x_h x_f = x_p x_q, & &
\end{array} \tag{3.28}$$

we get from the YB diagram



that $l = g$, $m = p$, $d = q$. Note that $a \neq c$. Otherwise, from the second relation of (3.28), it would follow that $x_a x_b = *x_i$ which implies, together with the first relation, that $i = j$ - a contradiction. Thus, there are two cases:

A) If $a < c$, then $h > f$. Indeed, if we assume that $h = f$ then, from square-freeness of (X, r) we have that $h = f = p = m = q = d$, and

therefore, from the fourth and fifth relation of (3.28) it follows that $k = a$ - a contradiction with the first relation of (3.28) and the statement 4 of 3.1.19. Similarly, if we assume that $h < f$, then $m = p > q = d > c$ - a contradiction, because $a < c$ implies $c > m$. Thus, if $a < c$ then $g > p$ and $h > f$. Therefore, $p < d$. Since $r_1^{-1} = r_1$, the YB condition can be rewritten as $r_2 r_1 = r_1 r_2 r_1 r_2$. Hence,

$$r_{x_a \sigma_{bi}}(x_a x_b x_i) = (r_{\sigma_{gp} x_f} \circ r_{x_g \sigma_{hf}} \circ r_{\sigma_{ke} x_f})(x_k x_e x_f)$$

(see the notation in Chapter 1), i.e. the ambiguity $(\sigma_{kj}, \sigma_{ji}, x_k, x_j, x_i)$ is resolvable.

B) If $a > c$, then $l = g < m = p$. Let us distinguish different cases depending on h and f. First note that $h \neq f$ because otherwise, from the fourth relation of (3.28) we get $x_e x_f = x_k *$, which implies, together with the third relation, that $k = j$ - a contradiction.

B1) If $h < f$, then $p > q$. Therefore,

$$(r_{x_g \sigma_{pq}} \circ r_{\sigma_{ae} x_d} \circ r_{x_a \sigma_{bi}})(x_a x_b x_i) = r_{\sigma_{ke} x_f}(x_k x_e x_f).$$

B2) If $h > f$, then $p < q$. Thus,

$$(r_{\sigma_{ae} x_d} \circ r_{x_a \sigma_{bi}})(x_a x_b x_i) = (r_{x_g \sigma_{hf}} \circ r_{\sigma_{ke} x_f})(x_k x_e x_f).$$

□

From 3.3.4, 3.3.7 and 3.3.12 it follows that the three notions (square-free solutions of the YBE, semigroups of skew-polynomial type and semigroups of I-type) are equivalent.

3.3.14 Theorem. [40] *Let X be a set with $n \geq 1$ elements and $r : X^2 \longrightarrow X^2$ a square-free involutive bijection. Let $\mathcal{S}(X, r)$, resp. $\mathcal{A}(k, X, r)$ with an arbitrary field k, be the semigroup, resp. the algebra, associated to (X, r). Then the following conditions are equivalent:*

1. *(X, r) is a nondegenerate set-theoretic solution of the YBE;*
2. *$\mathcal{S}(X, r)$ is a semigroup of I-type;*
3. *There exists an order $\preceq$ on X such that $\mathcal{S}(X, r)$ is a semigroup of skew-polynomial type;*
4. *There exists an order on X such that if $X = \{x_1 \prec \cdots \prec x_n\}$, then for any field k, $\mathcal{A}(k, X, r)$ has a PBW basis. More precisely, the set of ordered monomials*

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \,/\, (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$$

is a k-basis of $\mathcal{A}(k, X, r)$.

Moreover, any of these conditions implies that the solution (X, r) is decomposable.

3.3.1 Computing orders for skew-polynomial structures

The main result in this subsection establishes a complete computational description of the condition 2) of 3.3.1 satisfied by the skew-polynomial semigroups, by using certain LP (*Linear Programming*) problems. We show that for a finite set X with $|X| = n \geq 2$ and a set $\Re$ of $\binom{n}{2}$ square-free defining relations the existence of an order on X satisfying such condition is equivalent to the solvability of (at least) one of the LP problems described in 3.3.16, or in other words, to the existence of a non-empty feasible region ϕ_l. Once we formulate the above-mentioned LP problems, we can solve them by using any software which includes the *Simplex Algorithm*.

This result was first proved in [25] and it was useful to check the assertion 3.3.12 (when it still was a conjecture) for explicit examples of square-free solutions, that is, we used it to empirically confirm that square-free solutions of the YBE provide semigroups of skew-polynomial type.

Moreover, with the following method we obtain all possible orders on X for which the Yang-Baxter semigroup $\mathcal{S}(X, r)$ of an arbitrary square-free solution (X, r) is of skew-polynomial type.

3.3.15 Notation. *Let X be a finite set of order $n \geq 2$ and $r : X^2 \longrightarrow X^2$ a square-free involutive bijection such that $r(xy) \neq xy$ for all $x \neq y \in X$. Note that the set of relations $\Re(X, r)$ (in which we will not consider the relations $x_i x_i = x_i x_i$ for all $x_i \in X$) has $\frac{n(n-1)}{2}$ elements.*
Each relation of $\Re(X, r)$ can be written in two ways, either $x_j x_i = x_{i'} x_{j'}$ or $x_{i'} x_{j'} = x_j x_i$, when $r(x_j x_i) = x_{i'} x_{j'}$, $x_i \neq x_j$. Thus, we can distinguish different sets $\{\Re_l\}_l$ of ordered relations, where each set $\Re_l$ consists of all the $\frac{n(n-1)}{2}$ relations of $\Re(X, r)$ with a fixed way of writing each relation. Note that there are exactly $2^{\frac{n(n-1)}{2}}$ different sets of ordered relations.
For instance, for the square-free solution of 3 variables given by $\mathcal{C}(X, r) = \{(x_3)(x_2 x_1)\}$. The sets

$$\Re_1 = \{\, x_3x_2 = x_1x_3,\ x_3x_1 = x_2x_3,\ x_2x_1 = x_1x_2\},$$
$$\Re_2 = \{\, x_1x_3 = x_3x_2,\ x_3x_1 = x_2x_3,\ x_2x_1 = x_1x_2\}$$

are two (of the 8) different sets of ordered relations *of (X, r).*

3.3.16 Theorem. *Let X be a finite set of order $n \geq 2$ and $r : X^2 \longrightarrow X^2$ a square-free involutive bijection such that $r(xy) \neq xy$ for all $x \neq y \in X$. Let $\{\Re_l\}_l$ be all sets of ordered relations (described in 3.3.15).*

For each $\Re_l$, consider the LP problem:

$$\begin{array}{l}\textbf{minimize} \qquad \varphi(\omega) = \omega_1 + \cdots + \omega_n, \\ \textbf{subject to :} \\ \phi_l \equiv \left\{ \begin{array}{ll} \omega_k \geq 1, & 1 \leq k \leq n; \\ \left.\begin{array}{l} \text{a) } \langle\, \omega\,,\, \epsilon_j - \epsilon_i \,\rangle \;\geq 1 \\ \text{b) } \langle\, \omega\,,\, \epsilon_{j'} - \epsilon_{i'} \,\rangle \geq 1 \\ \text{c) } \langle\, \omega\,,\, \epsilon_j - \epsilon_{i'} \,\rangle \;\geq 1 \\ \text{d) } \langle\, \omega\,,\, \epsilon_{j'} - \epsilon_i \,\rangle \;\geq 1 \end{array}\right\} \text{ if } (i',j') \neq (i,j) & \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} \forall\, x_j x_i = x_{i'} x_{j'} \in \Re_l \end{array}\right. \end{array} \tag{3.29}$$

where ϵ_i is the element $(0,\ldots,\overset{i}{1},\ldots,0) \in \mathbb{N}^n$, the components of $\omega \in \mathbb{N}^n$ are denoted by $(\omega_1,\ldots,\omega_n)$, and the operation $\langle -,- \rangle$ denotes the scalar product on $\mathbb{N}^n \times \mathbb{N}^n$, given by $\langle u,v\rangle = \sum_{i=1}^n u_i v_i$, for $u = (u_1,\ldots,u_n), v = (v_1,\ldots,v_n) \in \mathbb{N}^n$.

Then, there exists a set of ordered relations $\Re_l$ for which the problem (3.29) has a solution if, and only if, there exists a total order $\preceq$ on $X = \{x_1,\ldots,x_n\}$ such that

$$\forall\, x_j x_i = x_{i'} x_{j'} \in \Re(X,r) \text{ with a}')\ x_j \succ x_i, \text{ then } \left\{ \begin{array}{ll} \text{b}') & x_{i'} \prec x_{j'} \\ \text{c}') & x_j \succ x_{i'} \\ \text{d}') & x_i \prec x_{j'} \end{array}\right.$$

Proof. Suppose that there exists a set $\Re_l$ so that the LP problem (3.29) has a solution, that is, there exists an element ω in the feasible region ϕ_l. Let $\preceq_\omega$ be the order on X defined as in Appendix A. Take $x_j x_i = x_{i'} x_{j'}$ in $\Re(X,r)$ and suppose, without loss of generality, that it appears in $\Re_l$ written in this way. From condition a) of (3.29) and bilinearity of $\langle -,- \rangle$, it follows

$$\langle \omega, \epsilon_j \rangle - \langle \omega, \epsilon_i \rangle > 0 \;\Rightarrow\; \langle \omega, \epsilon_j \rangle > \langle \omega, \epsilon_i \rangle \;\Rightarrow\; x_j \succ_\omega x_i.$$

Moreover, if $(i',j') = (i,j)$, or equivalently if x_j and x_i commute, the conditions b'), c') and d') are clear. If, instead, $(i,j) \neq (i',j')$, then the conditions b), c), resp. d) imply b'), c'), resp. d'), similarly as a) implies a').

Conversely, suppose that there exists a total order $\preceq$ on X satisfying conditions from a') to d'). Then, $x_{\sigma(1)} \prec x_{\sigma(2)} \cdots \prec x_{\sigma(n)}$ for some permutation σ on $\{1,\ldots,n\}$. So,

$$x_j \succ x_i \Longrightarrow \sigma^{-1}(j) > \sigma^{-1}(i),$$

or equivalently, taking $\omega = (\sigma^{-1}(1),\ldots,\sigma^{-1}(n)) \in (\mathbb{N}^+)^n$,

$$x_j \succ x_i \Longrightarrow \omega_j > \omega_i. \tag{3.30}$$

Let

$$\Re_l = \{\, x_j x_i = x_{i'} x_{j'} \in \Re(X,r) \,/\, x_j \succ x_i \}.$$

For each relation $x_j x_i = x_{i'} x_{j'}$ with $x_j \succ x_i$, from (3.30) it follows that

$$\langle \omega, \epsilon_j - \epsilon_i \rangle = \langle \omega, \epsilon_j \rangle - \langle \omega, \epsilon_i \rangle = \omega_j - \omega_i > 0.$$

So condition a) is true since $\langle \omega, \epsilon_j - \epsilon_i \rangle$ is an integer. Similarly, if $(i,j) \neq (i',j')$ then the conditions b'), c') and d') imply b), c) and d). Therefore, $\omega \in \phi_l$ is a solution of the LP problem (3.29) applied on $\Re_l$. □

From 3.3.12 and 3.3.16, it follows that for each square-free solution (X,r) there exists an (optimal) solution $\omega \in \mathbb{N}^n$ for at least one of the LP problems (3.29), and so, there exists an order $\preceq_\omega$ on X which provides a skew-polynomial structure for the Yang-Baxter semigroup $\mathcal{S}(X,r)$.

3.3.17 Corollary. *If (X,r) is a square-free solution of the YBE, then there exists a set of ordered relations $\Re_l$ for which the LP problem (3.29) has a solution ω, and therefore, the induced order $\preceq_\omega$ on X (see A.1.1) provides (renaming the variables if necessary) a skew-polynomial structure for the Yang-Baxter semigroup $\mathcal{S}(X,r)$.*
Furthermore, all possible orders on $X = \{x_1 \prec \cdots \prec x_n\}$ such that $\mathcal{S}(X,r)$ is of skew-polynomial type are exactly the orders $\preceq_\omega$ on X obtained from solving the family of LP problems (3.29) stated in 3.3.16.

Proof. Let us check the second part. Let $\preceq_\omega$ be the order induced (as in A.1.1) by a solution ω of the LP problem stated on a set of ordered relations R_l, and suppose, without loss of generality, that X is ordered by $x_{\sigma(1)} \prec_\omega x_{\sigma(2)} \cdots \prec_\omega x_{\sigma(n)}$ for some permutation σ on $\{1,\ldots,n\}$. Taking $y_i := x_{\sigma(i)}$ for all $1 \leq i \leq n$, it follows that

$$X = \{y_1 \prec_\omega \cdots \prec_\omega y_n\}$$

and $\mathcal{S}(X,r)$ is of skew-polynomial type. Moreover, if $\preceq$ is an order on $X = \{x_1 \prec \cdots \prec x_n\}$ so that $\mathcal{S}(X,r)$ is of skew-polynomial type and we consider

$$R_l = \{x_j x_i = x_{i'} x_{j'} \in \Re(X,r) \,/\, j > i\},$$

then $\omega = (1,2,\ldots,n)$ is a solution (the optimal one) of the LP problem (3.29) stated for R_l, and $\preceq = \preceq_\omega$ on X. □

From these results we devise Algorithm 26, which stops when it finds a solution for one of the LP problems described in (3.29). This algorithm can be obviously modified in order to compute all possible orders for which the Yang-Baxter semigroup $\mathcal{S}(X,r)$ associated to a square-free solution (X,r) is of skew-polynomial type (just removing the variable *Found*).

Algorithm 26 Orders for skew-polynomial structures

Require: (X, r), a square-free solution of the YBE;
Ensure: A order $\preceq_\omega$ on X such that $\mathcal{S}(X, r)$ is of skew-polynomial type;

Initialization: $Relsets := \{\Re_l\}_l$ (described in 3.3.15) and $Found$:=No;
while $Relsets$ is non-empty and $Found$=No **do**
Take $\Re_l \in Relsets$;
$Relsets := Relsets \setminus \Re_l$;
For $\Re_l$, consider the LP problem

$$\begin{array}{l} \textbf{minimize} \qquad \varphi(\omega) = \omega_1 + \cdots + \omega_n, \\ \textbf{subject to :} \end{array}$$

$$\phi_l \equiv \left\{ \begin{array}{ll} \omega_k \geq 1, & 1 \leq k \leq n; \\ \left.\begin{array}{l} \text{a) } \langle\, \omega\ ,\ \epsilon_j - \epsilon_i \,\rangle \ \geq 1 \\ \text{b) } \langle\, \omega\ ,\ \epsilon_{j'} - \epsilon_{i'} \,\rangle \geq 1 \\ \text{c) } \langle\, \omega\ ,\ \epsilon_j - \epsilon_{i'} \,\rangle \ \geq 1 \\ \text{d) } \langle\, \omega\ ,\ \epsilon_{j'} - \epsilon_i \,\rangle \ \geq 1 \end{array}\right\} & \text{if } (i', j') \neq (i, j) \end{array} \right\} \forall\, x_j x_i = x_{i'} x_{j'} \in \Re_l;$$

if there exists a solution $\omega \in (\mathbb{N}^+)^n$ **then**

$$\text{Let } x_i \prec_\omega x_j \iff \begin{cases} \langle \omega, \epsilon_i \rangle < \langle \omega, \epsilon_j \rangle \\ \text{or} \\ \langle \omega, \epsilon_i \rangle = \langle \omega, \epsilon_j \rangle \text{ and } i < j; \end{cases}$$

$Found$:=Yes;
end if
end while
Return $\preceq_\omega$.

3.3.18 Example. We continue working with the square-free solution (X, r) given in Example 3.3.2:

$$\mathcal{C}(X,r) = \{(x_{12}x_{11})(x_7x_8x_9x_{10}),\ (x_{12}x_{11})(x_1x_2x_3x_4x_5x_6),\ (x_{10}x_8)(x_9x_7),\\ (x_{10}x_9x_8x_7)(x_6x_5x_4x_3x_2x_1),\ (x_6x_4x_2)(x_5x_3x_1)\},$$

One of the sets of ordered relations gives the LP problem

$$\text{minimize} \sum_{k=1}^{12} w_k$$

subject to:
$\{\ 1 \leq w_1,\ 1 \leq w_2,\ 1 \leq w_3,\ 1 \leq w_4,\ 1 \leq w_5,\ 1 \leq w_6,\ 1 \leq w_7,\ 1 \leq w_8,\ 1 \leq w_9,\ 1 \leq w_{10}, 1 \leq w_{11},\ 1 \leq w_{12},\ 1 \leq w_{11} - w_{10},\ 1 \leq w_{12} - w_9,\ 1 \leq w_{12} - w_{10},\ 1 \leq w_{11} - w_7, 1 \leq w_{12} - w_{11},\ 1 \leq w_{12} - w_7,\ 1 \leq w_{12} - w_5,\ 1 \leq w_{12} - w_6,\ 1 \leq w_{11} - w_1,\ 1 \leq w_{12} - w_1, 1 \leq w_{11} - w_6,\ 1 \leq w_{11} - w_8,\ 1 \leq w_{11} - w_9,\ 1 \leq w_{12} - w_8,\ 1 \leq w_{11} - w_2,\ 1 \leq w_{11} - w_4, 1 \leq w_{12} - w_3,\ 1 \leq w_{11} - w_3,\ 1 \leq w_{12} - w_2,\ 1 \leq w_{11} - w_5,\ 1 \leq w_{12} - w_4,\ 1 \leq w_{10} - w_8, 1 \leq w_{10} - w_9,\ 1 \leq w_8 - w_7,\ 1 \leq w_{10} - w_7,\ 1 \leq w_8 - w_9,\ 1 \leq w_7 - w_2,\ 1 \leq w_{10} - w_2, 1 \leq w_{10} - w_3,\ 1 \leq w_7 - w_3,\ 1 \leq w_{10} - w_4,\ 1 \leq w_{10} - w_6,\ 1 \leq w_7 - w_5,\ 1 \leq w_{10} - w_5, 1 \leq w_7 - w_6,\ 1 \leq w_7 - w_4,\ 1 \leq w_9 - w_4,\ 1 \leq w_9 - w_6,\ 1 \leq w_9 - w_5,\ w_7 - w_8 \leq 1, w_9 - w_8 \leq 1,\ w_7 - w_{10} \leq 1,\ 1 \leq w_9 - w_7,\ w_9 - w_{10} \leq 1,\ 1 \leq w_7 - w_1,\ 1 \leq w_{10} - w_1, 1 \leq w_8 - w_4,\ 1 \leq w_8 - w_6,\ 1 \leq w_8 - w_5,\ 1 \leq w_9 - w_1,\ 1 \leq w_9 - w_3,\ 1 \leq w_9 - w_2, 1 \leq w_8 - w_1,\ 1 \leq w_8 - w_2,\ 1 \leq w_8 - w_3,\ 1 \leq w_4 - w_5,\ 1 \leq w_4 - w_3,\ w_1 - w_2 \leq 1, w_5 - w_2 \leq 1,\ 1 \leq w_5 - w_3,\ w_5 - w_6 \leq 1,\ w_1 - w_4 \leq 1,\ w_5 - w_4 \leq 1,\ w_1 - w_6 \leq 1, 1 \leq w_6 - w_2,\ 1 \leq w_6 - w_4,\ 1 \leq w_2 - w_1,\ 1 \leq w_6 - w_1,\ 1 \leq w_6 - w_5,\ 1 \leq w_2 - w_3, 1 \leq w_6 - w_3,\ 1 \leq w_2 - w_5,\ 1 \leq w_3 - w_1,\ w_3 - w_2 \leq 1,\ 1 \leq w_4 - w_1,\ 1 \leq w_4 - w_2, w_3 - w_4 \leq 1,\ 1 \leq w_5 - w_1\ \}.$

Running the Simplex Algorithm we obtain $\omega = (1, 4, 2, 5, 3, 6, 7, 9, 8, 10, 11, 12)$. Hence,

$$x_1 \prec_\omega x_3 \prec_\omega x_5 \prec_\omega x_2 \prec_\omega x_4 \prec_\omega x_6 \\ \prec_\omega x_7 \prec_\omega x_9 \prec_\omega x_8 \prec_\omega x_{10} \prec_\omega x_{11} \prec_\omega x_{12}$$

is an order for which the Yang-Baxter semigroup $\mathcal{S}(X, r)$ is of skew-polynomial type, just setting $X = \{y_1 \prec \cdots \prec y_n\}$, where $y_1 := x_1$, $y_2 := x_3$, $y_3 := x_5$, and so on.

3.3.19 Notes.

1. The conditions $\omega_k \geq 1$, $\forall\, k$ are included in the LP problem (3.29) just to assure that the ω_k's are bounded. If ω_k´s were bounded by any other integer, we would obtain the same order on X.

2. We have encoded a recursive version of Algorithm 26 in *Maple* (see the attached library in [32]) which for every square-free solution (X, r) computes the (optimal) solutions ω's of the LP problems described in 3.3.16, and hence, it gives all possible ways of ordering the set X such that $\mathcal{S}(X, r)$ is of skew-polynomial type.

Appendix A

Orders

In this appendix, we list all the orders used throughout the three chapters. The set X is supposed to be finite, namely $X = \{x_1, \ldots, x_n\}$.

A.1 Orders on X

A.1.1 The order $\preceq_\omega$ defined on X by

$$x_i \prec_\omega x_j \iff \begin{cases} \langle \omega, \epsilon_i \rangle < \langle \omega, \epsilon_j \rangle \\ \text{or} \\ \langle \omega, \epsilon_i \rangle = \langle \omega, \epsilon_j \rangle \text{ and } i < j, \end{cases}$$

is a total order.

A.2 Orders on the free monoid $\langle X \rangle$

A.2.1 The *lexicographical order* $\preceq_{lex}$ *defined on* $\langle X \rangle$ is given for every $u = x_{i1} \cdots x_{is}$, $v = x_{j1} \cdots x_{jt} \in \langle X \rangle$, by

$$u \prec_{lex} v \iff \begin{cases} s \leq t \text{ and } i_k = j_k, \forall\, k \leq s \\ \text{or} \\ \exists\, r \leq \min\{s,t\} \text{ s.t. } i_r < j_r \text{ and } i_k = j_k, \forall\, k \leq r. \end{cases}$$

A.2.2 The *degree lexicographical order* $\preceq_{deglex}$ *on* $\langle X \rangle$ is defined as

$$u \prec_{deglex} v \iff \begin{cases} \deg(u) < \deg(v) \\ \text{or} \\ \deg(u) = \deg(v) \text{ and } u \preceq_{lex} v, \end{cases}$$

where $\deg(u)$ denotes the length (i.e., the number of letters) of the word u.

The order $\preceq_{deglex}$ is a monomial order, whereas $\preceq_{lex}$ is not.

A.2.3 Let $\preceq$ be an admissible order in $\mathbb{N}^n$. Then the order $\preceq$ defined on $\langle X\rangle$ as

$$M_1 \prec M_2 \iff \begin{cases} \mathrm{mdeg}(M_1) \prec \mathrm{mdeg}(M_2) \\ \text{or} \\ \mathrm{mdeg}(M_1) = \mathrm{mdeg}(M_2) \text{ and } \nu(M_1) < \nu(M_2), \end{cases} \tag{A.1}$$

where $\mathrm{mdeg}(M)$ and $\nu(M)$ are the multidegree and the misordering index, respectively, of M is a monomial order on $\langle X\rangle$ (see [13, Prop. 2.2]).

A.3 Orders on the free algebra $\mathsf{k}\langle X\rangle$

A.3.1 Just as it appears, e.g., in [57], it is possible to extend a monomial order $\preceq$ on $\langle X\rangle$ to a partial order on the free algebra $\mathsf{k}\langle X\rangle$ satisfying the d.c.c.. This new order, denoted also by $\preceq$, is defined by putting $0 \prec f$, for all $f \in \mathsf{k}\langle X\rangle \setminus \{0\}$, and

$$f \prec g \iff \begin{cases} \mathrm{lm}\,(f) \prec \mathrm{lm}\,(g) \\ \text{or} \\ \mathrm{lm}\,(f) = \mathrm{lm}\,(g) \text{ and } f - \mathrm{lt}\,(f) \prec g - \mathrm{lt}\,(g), \end{cases} \tag{A.2}$$

for any $f, g \in \mathsf{k}\langle X\rangle \setminus \{0\}$, $f \neq g$.

A.4 Orders on $\mathbb{N}^n$ $(n \geq 1)$

A.4.1 The *reverse lexicographical order* $\preceq_{revlex}$ on $\mathbb{N}^n$ with $\epsilon_1 \prec_{revlex} \cdots \prec_{revlex} \epsilon_n$, defined for $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ as

$$\alpha \prec_{revlex} \beta \iff \exists\, j \in \{1, \ldots, n\} \text{ such that } \alpha_j > \beta_j \text{ and } \alpha_i = \beta_i,\ \forall\, i < j,$$

is a monoid total order, but it is not admissible since condition $0 \preceq \alpha$ is not satisfied for all $\alpha \in \mathbb{N}^n$ (note, for example, that $\epsilon_n \prec_{revlex} 0$).
There is also a reverse lexicographical order with $\epsilon_1 \succ_{revlex} \cdots \succ_{revlex} \epsilon_n$, obtained by replacing "$i < j$" by "$i > j$" in the definition above.

A.4.2 The *lexicographical order* $\preceq_{lex}$ on $\mathbb{N}^n$ with $\epsilon_1 \prec_{lex} \cdots \prec_{lex} \epsilon_n$ is the admissible order defined for every $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ by

$$\alpha \prec_{lex} \beta \iff \exists\, j \in \{1, \ldots, n\} \text{ such that } \alpha_j < \beta_j \text{ and } \alpha_i = \beta_i,\ \forall\, i > j.$$

The lexicographical order with $\epsilon_1 \succ_{lex} \cdots \succ_{lex} \epsilon_n$ can be defined similarly, just replacing "$i > j$" by "$i < j$".

A.4.3 Let $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{N}^n$. The *$\omega$-weighted lexicographical order* $\preceq_\omega$ on $\mathbb{N}^n$ is the admissible order given, for every $\alpha, \beta \in \mathbb{N}^n$, by

$$\alpha \prec_\omega \beta \iff \begin{cases} |\alpha|_\omega < |\beta|_\omega \\ \text{or} \\ |\alpha|_\omega = |\beta|_\omega \text{ and } \alpha \prec_{lex} \beta, \end{cases}$$

where $|\alpha|_\omega$ denotes the scalar product $\langle \omega, \alpha \rangle = \sum_{i=1}^n \alpha_i \omega_i$.

A.4.4 The *degree lexicographical order* $\preceq_{deglex}$ on $\mathbb{N}^n$ is the admissible order $\preceq_\omega$ with $\omega = (1, \ldots, 1) \in \mathbb{N}^n$.

A.4.5 Let $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{N}^n$. The *$\omega$-weighted reverse lexicographical order* $\preceq_{\omega revlex}$ on $\mathbb{N}^n$ is the admissible order defined for every $\alpha, \beta \in \mathbb{N}^n$ as

$$\alpha \prec_{\omega revlex} \beta \iff \begin{cases} |\alpha|_\omega < |\beta|_\omega \\ \text{or} \\ |\alpha|_\omega = |\beta|_\omega \text{ and } \alpha \prec_{revlex} \beta. \end{cases}$$

A.4.6 The *degree reverse lexicographical order* $\preceq_{revdeglex}$ on $\mathbb{N}^n$ is the admissible order defined as the order $\preceq_{\omega revlex}$ where $\omega = (1, \ldots, 1) \in \mathbb{N}^n$.

A.4.7 Let $\preceq_m$, resp. $\preceq_n$, be an admissible order on $\mathbb{N}^m$, resp. on $\mathbb{N}^n$.

- The *elimination order $\preceq^*$ with the second component larger than the first*, defined as

$$(\alpha, \beta) \prec^* (\gamma, \delta) \iff \begin{cases} \beta \prec_n \delta \\ \text{or} \\ \beta = \delta \text{ and } \alpha \prec_m \gamma, \end{cases}$$

- and the *elimination order $\preceq_*$ with the first component larger than the second*, defined as

$$(\alpha, \beta) \prec_* (\gamma, \delta) \iff \begin{cases} \alpha \prec_m \gamma \\ \text{or} \\ \alpha = \gamma \text{ and } \beta \prec_n \delta \end{cases}$$

for $\alpha, \gamma \in \mathbb{N}^m$, $\beta, \delta \in \mathbb{N}^n$, are admissible orders on $\mathbb{N}^{m+n}$.

Both elimination orders are crucial in *Elimination Theory*, which has been used in different contexts (in [1, 18] when the underlying ring is the commutative polynomial ring, or in [13] for left PBW rings).

A.4.8 Let $\preceq_1, \ldots, \preceq_m$ be orders on $\mathbb{N}^{n_1}, \ldots, \mathbb{N}^{n_m}$, respectively, and let σ be a permutation of m elements. The *generalized elimination order* $\preceq^*_\sigma$ (with

the $\sigma(1)$-component larger than the $\sigma(2)$-component, etc.) is defined on $\mathbb{N}^{n_1+\cdots+n_m}$ as

$$(\alpha^1,\ldots,\alpha^m) \prec^*_\sigma (\beta^1,\ldots,\beta^m) \iff \left\{\begin{array}{l}\exists\, j\in\{1,\ldots,m\} \text{ s.t. } \alpha^{\sigma(j)} \prec_{\sigma(j)} \beta^{\sigma(j)} \\ \text{and } \alpha^{\sigma(i)} = \beta^{\sigma(i)}, \forall\, i<j\end{array}\right\},$$

for $\alpha^k, \beta^k \in \mathbb{N}^{n_k}$, $1 \le k \le m$.

Lemma. Let $\preceq_1,\ldots,\preceq_m$ be orders on $\mathbb{N}^{n_1},\ldots,\mathbb{N}^{n_m}$, respectively, and let σ be a permutation of m elements.

- If $\preceq_k$ is a partial (resp. total) order for $1 \le k \le m$, then $\preceq^*_\sigma$ is also a partial (resp. total) order on $\mathbb{N}^{n_1+\cdots+n_m}$;
- If $\preceq_k$ is a monoid order for $1 \le k \le m$, then $\preceq^*_\sigma$ is also a monoid order;
- If $\preceq_k$ is an admissible order for $1 \le k \le m$, then $\preceq^*_\sigma$ is also an admissible order.

Note. The lemma may easily be proved by mimicking the well-known proof for the case $m = 2$. Note that for $m = 2$ and $\sigma = \mathrm{Id}$, the order $\preceq^*_\sigma$ is exactly the elimination order $\preceq_*$ with the first component larger than the second, whilst if $m = 2$ and σ is the permutation given by $\sigma(j) = 3-j$ for $1 \le j \le m$, then $\preceq^*_\sigma$ becomes the elimination order $\preceq^*$ with the second component larger than the first (see A.4.7).

A.4.9 Let $\preceq$ be an order on $\mathbb{N}^n$. The *opposite order* of $\preceq$, denoted by $\preceq^{\mathrm{op}}$, is defined for any $\alpha, \beta \in \mathbb{N}^n$ by

$$\alpha \preceq^{\mathrm{op}} \beta \iff \alpha^{\mathrm{op}} \preceq \beta^{\mathrm{op}},$$

where $\alpha^{\mathrm{op}} = (\alpha_n,\ldots,\alpha_1)$, for all $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$.
It is obvious that if "$\preceq$" is an admissible order, then so is "$\preceq^{\mathrm{op}}$".

A.4.10 Let $\preceq$ be an order on $\mathbb{N}^n$. The *up-component composition order* in $\mathbb{N}^{2n}$, denoted by $\preceq^c$, is defined as

$$(\alpha,\beta) \prec^c (\gamma,\delta) \Leftrightarrow \begin{cases}\alpha+\beta^{\mathrm{op}} \prec \gamma+\delta^{\mathrm{op}}, \text{ or} \\ \alpha+\beta^{\mathrm{op}} = \gamma+\delta^{\mathrm{op}} \text{ and } \beta^{\mathrm{op}} \prec \delta^{\mathrm{op}}.\end{cases}$$

The *down-component composition order* $\preceq_c$ is defined as

$$(\alpha,\beta) \prec_c (\gamma,\delta) \Leftrightarrow \begin{cases}\alpha+\beta^{\mathrm{op}} \prec \gamma+\delta^{\mathrm{op}}, \text{ or} \\ \alpha+\beta^{\mathrm{op}} = \gamma+\delta^{\mathrm{op}} \text{ and } \alpha \prec \gamma.\end{cases}$$

It is a straightforward calculation to check that if "$\preceq$" is an admissible order on $\mathbb{N}^n$, then both composition orders "$\preceq^c$" and "$\preceq_c$"are admissible orders on $\mathbb{N}^{2n}$ (the proof may be found in [24]).

A.5 Orders on the set $\mathbb{N}^{n,(s)}$ $(n, s \geq 1)$

A.5.1 The order $\leq^{n,(s)}$, defined as

$$\begin{aligned}(\alpha, i) \leq^{n,(s)} (\beta, j) &\iff (\beta, j) \in (\alpha, i) + \mathbb{N}^n, \\ &\iff i = j \text{ and } \alpha_k \leq \beta_k, \ \forall\, 1 \leq k \leq n,\end{aligned}$$

for (α, i), $(\beta, j) \in \mathbb{N}^{n,(s)}$, is a partial order on $\mathbb{N}^{n,(s)}$.

A.5.2 Let "$\preceq$" be an admissible order on $\mathbb{N}^n$.

- The *Term Over Position order* (or TOP *order*) (with $\exp(\boldsymbol{e_1}) > \exp(\boldsymbol{e_2}) > \cdots > \exp(\boldsymbol{e_s})$), defined as

$$(\alpha, i) \prec_{TOP} (\beta, j) \iff \begin{cases} \alpha \prec \beta \\ \text{or} \\ \alpha = \beta \text{ and } i > j, \end{cases}$$

- and the *Position Over Term order* (or POT *order*) (with $\exp(\boldsymbol{e_1}) > \exp(\boldsymbol{e_2}) > \cdots > \exp(\boldsymbol{e_s})$), given by

$$(\alpha, i) \prec_{POT} (\beta, j) \iff \begin{cases} i > j \\ \text{or} \\ i = j \text{ and } \alpha \prec \beta, \end{cases}$$

are admissible order on $\mathbb{N}^{n,(s)}$.

Both orders TOP and POT can also be defined with $\exp(\boldsymbol{e_1}) < \exp(\boldsymbol{e_2}) < \cdots < \exp(\boldsymbol{e_s})$, just replacing "$i < j$" by "$i > j$" in the definitions above.

Appendix B

Resumen en español

El célebre teorema de Poincaré-Birkhoff-Witt establece que si $\{x_1, \ldots, x_n\}$ es una k-base del álgebra de Lie $\mathfrak{g}$, entonces el conjunto de monomios estándar

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n}\}_{\alpha_1,\ldots,\alpha_n \in \mathbb{N}}$$

es una k-base del álgebra envolvente universal $U(\mathfrak{g})$. Esta propiedad, que las álgebras envolventes universales comparten con muchas otras álgebras asociativas, es una de las razones por las que la mayoría de los algoritmos utilizados en los anillos de polinomios conmutativos también funcionan en un contexto no necesariamente conmutativo. De hecho, a pesar de que la teoría de bases de Gröbner ha sido extendida a álgebras que no poseen bases de monomios estándar (véanse los trabajos de Mora en el álgebra libre [70, 71, 73]), parece que los mejores resultados desde un punto de vista computacional se obtienen en álgebras donde una de estas bases, también llamadas *bases PBW*, existe (ver [3, 8, 9, 10, 11, 12, 13, 23, 30, 31, 44, 54, 59, 60, 61, 62, 64, 65, 72, et.al.]).

El objetivo de este trabajo es estudiar, desde un punto de vista computacional, la clase de las álgebras en las que existe una base PBW. Más concretamente, nos centramos en álgebras que además son finitamente presentadas por un conjunto finito de generadores $X = \{x_1, \ldots, x_n\}$ y un conjunto de relaciones $Q \subseteq \langle X \rangle \times \mathsf{k}\langle X \rangle$ finito (el llamado *sistema de reducción*). Como demostramos en el primer capítulo, cuando $Q = \{(W_\sigma, f_\sigma)\}_\sigma$ es un sistema de reducción completo (en el sentido de [57]) compatible con algún orden monomial en $\langle X \rangle$ y todos los W_σ están desordenados, el conjunto de monomios estándar en los generadores $\{x_1, \ldots, x_n\}$ es una base PBW del álgebra $\mathsf{k}\langle X \rangle / I_Q$ (donde I_Q denota al ideal bilátero generado por Q) si, y sólo si, todo monomio $x_j x_i$ con $i < j$ es el término principal de una relación de Q. Nótese que esto último se puede comprobar de forma efectiva.

Nuestros principales casos de estudio son la clase de las *G-Álgebras*, que es seguramente la clase de álgebras más profusamente estudiada en la literatura sobre métodos efectivos en álgebras asociativas, y la clase de las *Álgebras de Yang-Baxter*, mucho menos conocidas al menos en sus aspectos computacionales. La primera es la clase de álgebras que introdujeron Kandri-Rody y Weispfenning en su trabajo [54], y cuya teoría ha sido recientemente desarrollada en [13, 59, 60, 64, 65]. La segunda es la clase de las álgebras que surgen de las soluciones de tipo conjuntista de la ecuación de Yang-Baxter, concretamente de las soluciones involutivas no-degeneradas libres de cuadrados. Recientemente se ha probado que el semigrupo asociado a estas álgebras es de tipo skew-polinomial (ver [40]) y, por tanto, encajan en nuestro esquema computacional.

Este trabajo está organizado de la siguiente manera.

El primer capítulo recoge las nociones y resultados básicos sobre sistemas de reducción y ambigüedades de reducción, incluyendo el lema del diamante de Bergman y un algoritmo de reducción adaptado, que efectúa una división bilátera en el álgebra libre:

Algoritmo 1. Reducción en $\mathsf{k}\langle X\rangle$

Require: $f \in \mathsf{k}\langle X\rangle$, y un sistema de reducción Q, compatible con un orden monomial $\preceq$ en $\langle X\rangle$;
Ensure: $q, r \in \mathsf{k}\langle X\rangle$ tales que

1. $f = q + r$, donde
2. $q = \sum_{\sigma\in Q} q_\sigma(W_\sigma - f_\sigma)$, con

$$q_\sigma = \sum_{\text{i; finite}} \lambda_{\sigma,i}(A_{\sigma,i} \otimes B_{\sigma,i}), \text{ y } A_{\sigma,i}W_\sigma B_{\sigma,i} \preceq \operatorname{lm}(f),$$

3. si $r \neq 0$, entonces $r \in \mathsf{k}\langle X\rangle_{\text{irr}}$ y $\operatorname{lm}(r) \preceq \operatorname{lm}(f)$;

Initialization: $p := f$, $q := 0$, $r := 0$;
while $p \neq 0$ **do**
  if $\operatorname{lm}(p) \notin \langle X\rangle_{\text{irr}}$ **then**
    Sean $A, B \in \langle X\rangle$ y $\sigma = (W_\sigma, f_\sigma) \in Q$ tales que $\operatorname{lm}(p) = AW_\sigma B$;
    $p := p - \operatorname{lc}(p)(A \otimes B)(W_\sigma - f_\sigma)$;
    $q := q + \operatorname{lc}(p)(A \otimes B)(W_\sigma - f_\sigma)$;
  else

$p := p - \mathrm{lt}\,(p)$;
$r := r + \mathrm{lt}\,(p)$;
end if
end while
Devuelve q, r.

En este capítulo también se recoge la equivalencia entre los conceptos de base de Gröbner bilátera en el álgebra libre y sistema de reducción completo, que nos permitirá probar en el capítulo 2 que las *condiciones de no-degeneración* de Levandovskyy (ver [61]) planteadas en cualquier G-Álgebra, pongamos $\mathsf{k}\langle X\rangle/I_Q$, equivalen a que las ambigüedades de solapamiento de Bergman sean resolubles (ver [7]), o equivalentemente, a que el sistema de reescritura noetheriano Q' (ver [57]) que se obtiene de Q sea completo:

1.1.25 Teorema.
Sea $\preceq$ un orden monomial en $\langle X\rangle$. Sea G un sistema generador bilátero de un ideal bilátero I de $k\langle X\rangle$ y consideremos el sistema de reducción $Q = \{(\mathrm{lm}\,(g), \mathrm{lm}\,(g) - \mathrm{lc}\,(g)^{-1}g)\}_{g\in G}$ de $k\langle X\rangle$.
Las siguientes condiciones son equivalentes:

1. *G es una base de Gröbner bilátera de I;*
2. *$\mathrm{L}\,(G)\bigcap\langle X\rangle = \mathrm{M}\,(I)$;*
3. *$\langle X\rangle_{\mathrm{irr}} = \langle X\rangle \setminus \mathrm{M}\,(I)$;*
4. *Todas las ambigüedades de Q son resolubles;*
5. *Todas las ambigüedades de Q son resolubles respecto a $\preceq$;*
6. *Todos los elementos de $k\langle X\rangle$ son de reducción única bajo Q;*
7. *El conjunto $\{M + I \,/\, M \in \langle X\rangle_{\mathrm{irr}}\}$ es una k-base del álgebra $k\langle X\rangle/I$;*
8. *$k\langle X\rangle = k\langle X\rangle_{\mathrm{irr}} \bigoplus I$, o equivalentemente, $k\langle X\rangle_{\mathrm{irr}} \bigcap I = \{0\}$;*
9. *$k\langle X\rangle/I \cong k\langle X\rangle_{\mathrm{irr}}$;*
10. *Q es completo, or equivalentemente, noetheriano;*
11. *Todo $f \in I$ tiene una única forma normal ${}^{Q}\overline{f}$, que es 0;*

---

12. *Para todo* $f \in k\langle X\rangle \setminus \{0\}$, $f \in I$ *si, y sólo si,* f *se puede expresar como*

$$f = \sum_{g \in G} q_g g, \text{ with } q_g = \sum_{\text{finite}} \lambda_{i,g}(A_{i,g} \otimes B_{i,g}),$$

y $\operatorname{lm}(f) = \max_{\preceq}\{A_{i,g}\operatorname{lm}(g)B_{i,g}\}_{i,g}$;

13. *Para todo* $f \in I$, $f \to_Q 0$, *o equivalentemente, para todo* $f \in k\langle X\rangle$,

$$f \in I \iff f \to_Q 0;$$

14. *Todo* $f \in k\langle X\rangle$ *tiene una única forma normal* $\overline{f}^Q$;

15. $S(\sigma, \tau, A, B, C) \to_Q 0$, *para todo S-polinomio* $S(\sigma, \tau, A, B, C)$;

En la última sección del capítulo 1 probamos nuestra caracterización de las álgebras con base PBW:

1.2.4 Teorema. *Sea* $X = \{x_1, \ldots, x_n\}$ *y* Q *un sistema de reducción de* $k\langle X\rangle$, *compatible con un orden monomial* $\preceq$ *en* $\langle X\rangle$, *de manera que todo* W_σ *sea desordenado, e.d.,*

$$\forall\, \sigma = (W_\sigma, f_\sigma) \in Q,\ W_\sigma = Ax_jx_iB, \text{ para algún } A, B \in \langle X\rangle, j > i. \quad \text{(B.1)}$$

Consideremos las siguientes afirmaciones:

1. $k\langle X\rangle/I_Q$ *es una* k*-algebra con una base PBW. Más concretamente,* $\{X^\alpha\}_{\alpha\in\mathbb{N}^n}$ *es una* k*-base de* R, *donde* X^α *denota* $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ *y* $X_i = x_i + I_Q$;

2. $\{x_jx_i \,/\, 1 \le i < j \le n\} \subseteq \{W_\sigma \,/\, \sigma \in Q\}$, *o equivalentemente,* $\langle X\rangle_{\text{irr}} = \{x^\alpha \,/\, \alpha \in \mathbb{N}^n\}$;

3. *El conjunto* $G = \{W_\sigma - f_\sigma\}_{\sigma\in Q}$ *es una base de Gröbner bilátera de* I_Q, *o equivalentemente,* Q *es completo.*

Entonces,

A) Si 2 es cierta, entonces 1 es equivalente a 3.

B) Asumiendo 3, las afirmaciones 1 y 2 son equivalentes.

C) Si además Q *no tiene ambigüedades de inclusión, entonces en A) y B) la condición 2 puede ser reemplazada por:*

2'. $\{W_\sigma \,/\, \sigma \in Q\} = \{x_jx_i \,/\, 1 \le i < j \le n\}$.

Justificamos además, usando una técnica que desarrollamos en detalle en el capítulo 2, por qué el algoritmo de reducción también proporciona una división bilátera en un álgebra con base PBW:

1.2.11 Teorema. *Sea $\preceq$ un orden admisible en $\mathbb{N}^n$, y sea $R = k\langle X\rangle/I_Q$, donde $Q = \{(x_j x_i, f_{ji}) \,/\, 1 \leq i < j \leq n\}$ es un sistema de reducción completo con respecto al orden monomial $\preceq$ en $\langle X\rangle$ inducido por $\preceq$ en $\mathbb{N}^n$.*
Sea $\{G_1, \ldots, G_s\} \subseteq R \setminus \{0\}$. Todo elemento $F \in R \setminus \{0\}$ se puede expresar como

1. *$F = \sum_{i=1}^{s} P_i G_i + F'$ con $F' \in R$, $P_i \in R \otimes_k R^{\mathrm{op}}$, de tal manera que*
2. *$\exp_R(P_i G_i) \preceq \exp_R(F)$, para todo $1 \leq i \leq s$;*
3. *si $F' \neq 0$, entonces $\exp_R(F') \preceq \exp_R(F)$ y existe un polinomio estándar $f' \in k\langle X\rangle$ tal que $F' = f' + I_Q$ y*

$$x^\alpha \notin L(\{g_1, \ldots, g_s\}),\ \forall\, x^\alpha \text{ monomio de } f',$$

donde $G_i = g_i + I_Q$, para ciertos $g_i \in k\langle X\rangle$.

En el capítulo 2 analizamos nuestro primer ejemplo de álgebra con base PBW: la clase de las G-Álgebras (conocidas también como *álgebras polinomiales solubles* en [54, 59, et.al.] y como *álgebras PBW* en [9, 13, 30, 65, et.al.]). Estas álgebras vienen definidas, además de por tener una base PBW, por la propiedad de que el *exponente* del *skew-conmutador* $p_{ij} = x_j x_i - c_{ij} x_i x_j$ está acotado por el *exponente* del producto $x_i x_j$, que es $(0, \ldots, \overset{-i-}{1}, \ldots, \overset{-j-}{1}, \ldots, 0)$ para todo $1 \leq i < j \leq n$. La clase de las G-Álgebras incluye las álgebras envolventes universales de las álgebras de Lie finito-dimensionales, extensiones de Ore iteradas, una gran variedad de cuánticos ($M_q(2)$, los espacios cuánticos, etc.) y es cerrada al tomar álgebras opuestas y productos tensoriales, como mostramos en la segunda sección de este capítulo.
En las primeras cuatro secciones del capítulo 2 resumimos las nociones básicas de la teoría de bases de Gröbner en el contexto de las G-Álgebras. Seguimos la notación y terminología de [13]. En la cuarta sección, en la que recogemos algunas de las aplicaciones clásicas de las bases de Gröbner, contribuímos con un algoritmo para calcular la codimensión de un submódulo a izquierda, a derecha o bilátero $M \subseteq R^s$ cuando R es una G-Álgebra en caso de ser M cofinito (algoritmos 8 y 9).
En la quinta sección proponemos un nuevo método, que mostramos por primera vez en [28], para manejar de forma efectiva bimódulos usando directamente sus sistemas generadores biláteros como datos de entrada.

Algoritmo 8. Módulo cofinito

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}\} \subseteq R^s$, un sistema generador del módulo $M \subseteq R^s$ ($M = {}_R\langle F\rangle$ o $M = {}_R\langle F\rangle_R$);

Ensure: *cofinite*= FALSE, si M no es un módulo cofinito, y *cofinite*= TRUE, en otro caso. Si se cumple esto último entonces devuelve el valor de $\mathrm{codim}_k(M)$ en la variable *codimension*;

Initialization: *cofinite*:=TRUE, $i := 1$, $k := 1$;

Calcular una base de Gröbner $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$ for M;

while *cofinite*= TRUE y $k \leq s$ y $i \leq n$ **do**

  if $\nexists \exp(\boldsymbol{g}) \in G$ tal que $\exp(\boldsymbol{g}) = (\nu\epsilon_i, k)$ para algún $\nu \in \mathbb{N}$ **then**

    cofinite :=FALSE;

  else

    if $i = n$ **then**

      $k := k + 1$; $i := 1$;

    else

      $i := i + 1$;

    end if

  end if

end while

if *cofinite* = TRUE **then**

  Calcular una base de Gröbner minimal G' a partir de G;

  codimension:= 0;

  for $k = 1$ to s **do**

    Para $1 \leq i \leq n$, sea $(\alpha^{ik}, k) \in \mathrm{Exp}(G')$ tal que

    $\alpha^{ik} = (0, \ldots, \overset{-i-}{\nu_{ik}}, \ldots, 0)$ para algún $\nu_{ik} \in \mathbb{N}$;

    $(\beta_1, \ldots, \beta_n) := (0, \ldots, 0)$;

    Codimensión(n,k); {Llamada al algoritmo 9}

  end for

end if

Devuelve *cofinite* y, si *cofinite* = TRUE, devuelve también *codimension*.

Algoritmo 9. Codimensión

Require: n_{coord} un entero positivo, y $k \in \{1, \ldots, s\}$;

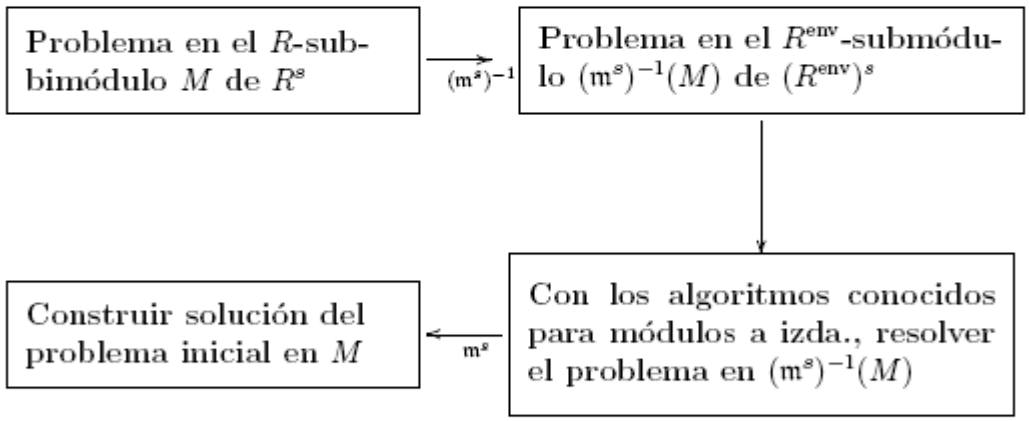
if $n_{coord} = 1$ **then**

  $\beta_1 := 0$;

  while $\forall \boldsymbol{g} \in G$ con $\mathrm{level}(\boldsymbol{g}) = k$, existe $l_{\boldsymbol{g}} \in \{1, \ldots, n\}$ tal que la $l_{\boldsymbol{g}}$-ésima componente de $\overline{\exp(\boldsymbol{g})}$ es estrictamente mayor que que la $l_{\boldsymbol{g}}$-ésima

componente de $(\beta_1, \ldots, \beta_n)$ (punto actual) do
codimension:= *codimension* + 1;
$\beta_1 := \beta_1 + 1$;
end while
else
for all $j = 0$ to $(\alpha_{n_{coord}\,k} - 1)$ **do**
Codimensión($n_{coord} - 1$,k); {Llamada al algoritmo 9}
$\beta_{n_{coord}} := \beta_{n_{coord}} + 1$;
end for
end if

La ventaja de utilizar la nueva técnica para manejar bimódulos estriba en que se evitan pasos iniciales innecesarios para transformar los datos biláteros en entradas a izquierda o a derecha. Un esquema de este método es el siguiente:



(B.2)

Aplicamos este método para calcular bases de Gröbner biláteras de bimódulos sobre una G-Álgebra de manera alternativa a la del método de Clausura a Derecha de Kandri-Rody y Weispfenning (ver [54]). Este nuevo algoritmo llama una sóla vez al algoritmo de Buchberger a izquierda en lugar del, a priori desconocido, número de llamadas típico del método de Clausura a Derecha.

Algoritmo 10. Bases de Gröbner biláteras

Require: $F = \{\boldsymbol{f_1}, \ldots, \boldsymbol{f_t}\} \subseteq R^s \setminus \{0\}$;

Ensure: $G = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_r}\}$, una base de Gröbner bilátera de ${}_R\langle F\rangle_R$ tal que $F \subseteq G$;

Initialization: $B := \{\boldsymbol{f_i} \otimes \mathbf{1}\}_{i=1}^{t} \cup \{\boldsymbol{x^{(e_j,k)}} \otimes \mathbf{1} - \mathbf{1} \otimes \boldsymbol{x^{(e_j,k)}}\}_{1\leq j\leq n,\ 1\leq k\leq s}$;

Usando el algoritmo de Buchberger a izquierda, calcular una base de Gröbner a izquierda G' en el módulo libre $(R^{\mathrm{env}})^s$ para B;

Si $G' = \{\boldsymbol{g'_1}, \ldots, \boldsymbol{g'_{t'}}\}$ con $\boldsymbol{g'_i} = (\sum_{j\in\mathfrak{I}_i} p_{ij}^1 \otimes q_{ij}^1, \ldots, \sum_{j\in\mathfrak{I}_i} p_{ij}^s \otimes q_{ij}^s)$, poner $\boldsymbol{g_i} := (\sum_{j\in\mathfrak{I}_i} p_{ij}^1 q_{ij}^1, \ldots, \sum_{j\in\mathfrak{I}_i} p_{ij}^s q_{ij}^s)$;

$G := \emptyset$;

for all $i = 1$ to t' **do**
  if $\boldsymbol{g_i} \neq 0$ **then**
    $G := G \cup \{\boldsymbol{g_i}\}$;
  end if
end for
Devuelve G.

Posteriormente llevamos a cabo una comparación entre este algoritmo y el método de Clausura a Derecha discutiendo varios ejemplos explícitos.

En la sexta sección la técnica mostrada en la sección anterior para manejar bimódulos se aplica esta vez para calcular el *bimódulo de sicigias*, introducido por Mora ([71]) para ideales biláteros homogéneos en el contexto de estructuras graduadas no conmutativas, y luego, independientemente, los autores ([27, 30]) para bimódulos no necesariamente homogéneos sobre una G-Álgebra. Mostramos que los bimódulos de sicigias, que pueden ser vistos como la contrapartida bilátera de los módulos de sicigias a izquierda, son útiles resolviendo algunos problemas computacionales cuando se tienen datos de entrada biláteros, como el cálculo de intersecciones finitas de sub-bimódulos de R^s, presentaciones y resoluciones libres de sub-bimódulos de R^s, ideales de división biláteros de R, etc. En el caso en que los bimódulos estén generados por elementos del *centralizador*, mostramos cómo se mejoran algunos de estos resultados y se simplifican muchos cálculos.

En la última sección presentamos un algoritmo para calcular una presentación de $\mathrm{Tor}_k(M, N)$ en el contexto de las G-Álgebras.

En el capítulo 3 nos centramos en nuestro segundo ejemplo de álgebras con base PBW: las Álgebras de Yang-Baxter. Estas álgebras se definen a partir de soluciones de tipo conjuntista involutivas, no-degeneradas y libres de cuadrados de la ecuación de Yang-Baxter, a las que denominaremos de aquí en adelante *soluciones libres de cuadrados*. Si $X = \{x_1, \ldots, x_n\}$, entonces la

biyección $r : X \times X \longrightarrow X \times X$ es una solución de tipo conjuntista de la ecuación de Yang-Baxter si

$$(r \times Id)(Id \times r)(r \times Id) = (Id \times r)(r \times Id)(Id \times r).$$

En el caso de ser además, involutiva, no-degenerada y libre de cuadrados, el conjunto de monomios estándar en X es una k-base del álgebra generada por X con relaciones $\{x_j x_i - r(x_j x_i)\}_{1 \leq i < j \leq n}$, como se prueba, de manera alternativa a como lo hace la autora de [40], en:

3.3.13 Proposición. *Sea (X, r) una solución libre de cuadrados, donde $X = \{x_1, \ldots, x_n\}$. Entonces, el álgebra de Yang-Baxter $\mathcal{A}(k, X, r)$ tiene una base PBW. Más concretamente, el conjunto de monomios estándar*

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \ / \ (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$$

es una k-base de $\mathcal{A}(k, X, r)$.

Como mostramos a lo largo de todo el capítulo, se puede usar una aproximación combinatoria con objeto de desarrollar métodos algorítmicos en el contexto de las soluciones de tipo conjuntista de la ecuación de Yang-Baxter. Después de exhibir distintas formas de representar y clasificar las soluciones libres de cuadrados, entre las que destacamos la representación mediante grafos, centramos nuestra atención en los isomorfismos y automorfismos de soluciones siguiendo esta aproximación combinatoria-computacional. Basándonos en la noción de *estrella* de un elemento, encontramos un método para calcular el conjunto de isomorfismos entre dos soluciones. Este resultado puede verse como una generalización del que probamos en [25, 33] para el cálculo del grupo de automorfismos. La utilidad de calcular el grupo de automorfismos de una solución se justifica al final de la segunda sección, donde desarrollamos algoritmos que requieren de dichos automorfismos para calcular nuevas soluciones pegando dos soluciones existentes. Uno de ellos es el que se detalla a continuación.

Algoritmo 21. Pegado de soluciones libres de cuadrados usando automorfismos

Require: (X, r_X) y (Y, r_Y), dos soluciones libres de cuadrados de la ecuación de Yang-Baxter, $\tau_X \in \mathrm{Aut}(X, r_X)$ y $\tau_Y \in \mathrm{Aut}(Y, r_Y)$;

Ensure: (Z, r) una nueva solución libre de cuadrados, donde $Z = X \cup Y$ y tal que $r_{|X \times X} = r_X$ y $r_{|Y \times Y} = r_Y$;

Sean $\tau_X = C_1 \cdots C_r$ y $\tau_Y = c_1 \cdots c_s$ las descomposiciones de τ_X y τ_Y como producto de ciclos disjuntos de longitud ≥ 1;

Si $c_j = (y_1^j \cdots y_{s_j}^j)$ para $1 \leq j \leq s$, sea $\tau_Y^{-1} := C_1' \cdots C_s'$, con $C_j' := (y_{s_j}^j \cdots y_1^j)$;
Sea $Z := X \cup Y$;
$\mathcal{C}(Z, r) := \mathcal{C}(X, r_X) \cup \mathcal{C}(Y, r_Y) \cup \{ \sigma_{ij} = C_i C_j' \,/\, 1 \leq i \leq r,\ 1 \leq j \leq s\}$;
Devuelve $\mathcal{C}(Z, r)$.

Además, encontramos una correspondencia bijectiva entre las extensiones a izquierda de dos soluciones (X, r_X), (Y, r_Y) y los morfismos que van desde el grupo $\mathcal{G}(Y, r_Y)$ asociado a la solución (Y, r_Y) al grupo de automorfismos $\mathrm{Aut}(X, r_X)$ de (X, r_X).
En la última sección discutimos la equivalencia, probada por T. Gateva-Ivanova y M. van den Bergh ([40, 42]), entre soluciones libres de cuadrados de la ecuación de Yang-Baxter, semigrupos de tipo skew-polinomial y semigrupos de tipo I. Es en este contexto donde usamos la teoría de los sistemas de reducción recogida en el primer capítulo para probar de manera alternativa a como se hace en [40] que el álgebra de Yang-Baxter $\mathcal{A}(\mathsf{k}, X, r)$ asociada a una solución libre de cuadrados (X, r) es un álgebra con una base PBW. Finalmente, mostramos cómo el comportamiento de los semigrupos de tipo skew-polinomial puede ser determinado completamente por una familia de problemas de programación lineal.

A lo largo de los capítulos 2 y 3 ilustramos los conceptos teóricos con ejemplos explícitos. Para efectuar los cálculos hemos codificado sendas bibliotecas de programas, que se incluyen en el CD adjunto (ver también [32]), utilizando el paquete de cálculo simbólico *Maple*. Este software debe considerarse como parte de esta tesis doctoral.
La biblioteca que corresponde a las G-Álgebras incluye desde la aritmética básica entre elementos en una G-Álgebra hasta todos los algoritmos listados en el capítulo 2. La biblioteca de métodos que atañen a las soluciones de tipo conjuntista incluye algoritmos que nos permiten reconocer si una serie de relaciones determinan una solución libre de cuadrados, calcular todos los órdenes $\preceq$ en $X = \{x_1 \prec \cdots \prec x_n\}$ posibles (reindexando las variables si fuese necesario) tal que el semigrupo de Yang-Baxter $\mathcal{S}(X, r)$ es de tipo skew-polinomial, verificar si una biyección es un automorfismo de una solución libre de cuadrados, calcular el grupo de automorfismos de cualquier solución libre de cuadrados, pegar dos soluciones libres de cuadrados para obtener una nueva, etc.

Para facilitar la lectura, al final del trabajo se incluye un apéndice con definiciones y ejemplos de los órdenes (monomiales, admisibles, etc.) usados a lo largo de los tres capítulos.

Índice en español

Bibliography

[1] Adams, W. and Loustaunau, P., An Introduction to Gröbner Bases. AMS, Providence ri, 1994.

[2] Apel, J., *Computational Ideal Theory in Finitely Generated Extension Rings*, Theor. Comput. Sci. **244** (2000) 1-2, 1–33.

[3] Apel, J. and Lassner, W., *An algorithm for calculations in enveloping fields of Lie algebras*, Proc. Conf. Comp. Alg., Dubna (1985), 231–241.

[4] Artin, M. and Schelter, W., *Graded algebras of global dimension 3*, Adv. in Math. **66** (1987), 171–216.

[5] Becker, T. and Weispfenning, V., Gröbner Bases: a computational approach to commutative algebra. Springer, 1993.

[6] Benkart, G. and Roby, T., *Down-up algebras*, J. Algebra **209** (1998) 1, 305–344.

[7] Bergman, G., *The diamond lemma in ring theory*, Adv. Math. **29** (1978), 178–218.

[8] Bueso, J.L., Castro, F., Gómez Torrecillas, J. and Lobillo, F.J., *Computing the Gelfand Kirillov dimension*, sac Newsletter **1** (1996), 39–52.

[9] Bueso, J.L., Castro, F., Gómez Torrecillas, J. and Lobillo, F.J., *An introduction to effective calculus in quantum groups*, Lect. Notes Pure App. Math. **197** (1998), 55–83.

[10] Bueso, J.L., Castro, F., Gómez Torrecillas, J. and Lobillo, F.J., *Test de primalité dans une extension de Ore itérée*, c.r. Acad. Sci. Paris Sér. I Math. **328** (1999), 459–462.

[11] Bueso, J.L., Castro, F., Gómez Torrecillas, J. and Lobillo, F.J., *Primality test in iterated Ore extensions*, Comm. in Algebra **29** (2001), 1357–1371.

[12] Bueso, J.L., Gómez Torrecillas, J. and Lobillo, F.J., *Homological computations in PBW modules*, Alg. Rep. Theory **4** (2001), 201–218.

[13] Bueso, J.L., Gómez Torrecillas, J. and Verschoren, A., Algorithmic Methods in Noncommutative Algebra: Applications to Quantum Groups. Kluwer, 2003.

[14] Caboara, M. and Traverso, C., *Efficient algorithms for ideal operations* (extended abstract). Proc. of the International Symposium on Symbolic and Algebraic Computation issac'98. acm Press (1998), 147–152.

[15] Chartrand, G. and Oellermann, O., Applied and Algorithmic Graph Theory. MacGraw-Hill, 1993.

[16] Christofides, N., Graph Theory: An Algorithmic Approach. Academic Press, 1975.

[17] CoCoA Team. CoCoA System: Computations in Commutative Algebra. Available at: `http://cocoa.dima.unige.it`.

[18] Cox, D., Little, J. and O'Shea, D., Ideals, Varieties, and Algorithms. Springer Verlag, New York, 1992.

[19] Drinfeld, V., *On some unsolved problems in quantum group theory*, Lect. Notes in Math. **1510** (1992), 1–8.

[20] Dummit, D. and Foote, R., Abstract algebra. Prentice-Hall, 1991.

[21] Etingof, P., Schedler, T. and Soloviev, A., *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), 169–209.

[22] Gago Vargas, J., *Bases for projective modules in $A_n(k)$*, J. Symb. Comput. **36** (2003), 845–853.

[23] Galligo, A., *Algorithmes de cacul de bases standard* (preprint). Niza, 1982.

[24] García Román, M.S., Álgebra efectiva en grupos cuánticos (Minor thesis, in Spanish). University of La Laguna, Spain, 2000.

[25] García Román, M.S., Set-theoretic solutions of the Yang-Baxter equation (Master thesis, *International Advanced Master Degree in Noncommutative Algebra and Geometry*). University of Antwerp, Belgium, 2003.

[26] García Román, M. and García Román, M.S., *A new algorithm to compute two-sided Gröbner bases*, Proc. of the 7th Spanish Meeting on Computer Algebra and Applications EACA-2001 (J. Rubio ed.). ACM SIGSAM Bull. 35 (2001), 4.

[27] García Román, M. and García Román, M.S., *Syzygy bimodules and first applications*, Proc. of the 9th Spanish Meeting on Computer Algebra and Applications EACA-2004 (González Vega, L,. and Recio, T. eds.), Santander, Spain, 2004, 143–147.

[28] García Román, M. and García Román, M.S., *New methods on bimodules* (poster), presented in ISSAC-2004, Santander, Spain, 2004.

[29] García Román, M. and García Román, M.S., *Sygygy Bimodules and simplified computations using centralizers* (electronic), Proc. of the Effective Methods in Algebraic Geometry MEGA-2005, Sardinia, Italy, 2005.

[30] García Román, M. and García Román, M.S., *Gröbner bases and syzygies on bimodules over PBW algebras*, J. Symb. Comput. 40 (2005), 1039–1052.

[31] García Román, M. and García Román, M.S., *Effective computation of* $\mathrm{Tor}_k(M,N)$ (preprint accepted for publication), `arXiv.math.KT/0412326`.

[32] García Román, M. and García Román, M.S., *Computations in G-Algebras and Yang-Baxter Algebras* (electronic library in Maple), `http://webpages.ull.es/users/sgarcia/`.

[33] García Román, M.S. and Gateva-Ivanova, T., *Isomorphisms and automorphisms of square-free solutions of the YBE* (preprint). La Laguna, Spain, 2004.

[34] Gateva-Ivanova, T., *On the Noetherianity of Some Associative Finitely Presented Algebras*, J. Algebra 138 (1991), 13–35.

[35] Gateva-Ivanova, T., *Noetherian properties of skew polynomial rings with binomial relations*, Trans. Amer. Math. Soc. **343** (1994), 203–219.

[36] Gateva-Ivanova, T., *Skew polynomial rings with binomial relations*, J. Algebra **185** (1996), 710–753.

[37] Gateva-Ivanova, T., *Regularity of the skew polynomial rings with binomial relations* (preprint). 1996.

[38] Gateva-Ivanova, T., *Set theoretic solutions of the Yang-Baxter equation*, Mathematics and education in Mathematics, Proc. of the Twenty Ninth Spring Conference of the Union of Bulgarian Mathematicians, Lovetch (2000), 107–117.

[39] Gateva-Ivanova, T., *Set-theoretic solutions of the Yang-Baxter Equation*, Proc. of the International Conference on Algebras, Modules and Rings, Lisboa (2003).

[40] Gateva-Ivanova, T., *A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation*, J. Math. Phys. **45** (2004) 10, 3828–3858.

[41] Gateva-Ivanova, T., *Regularity of skew-polynomial rings and regular solutions of set-theoretic YBE*, Proc. of AGAAP (Algebraic Geometry, Algebra and Aplications), Borovetz-Bulgaria 2004, Serdica Mathematical Journal (to appear).

[42] Gateva-Ivanova, T. and Van den Bergh, M., *Semigroups of I-type*, J. Algebra **206** (1998), 97–112.

[43] Gateva-Ivanova, T., Jespers, E. and Okninski, J., *Quadratic algebras of skew polynomial type and underlying semigroups* (preprint). 2001.

[44] Gómez Torrecillas, J. and Lobillo, F.J., *Global homological dimension of multifiltered rings and quantized enveloping algebras*, J. Algebra **225** (2000) 2, 522–533.

[45] Green, E., *Noncommutative Groebner bases and projective resolutions*, Computational methods for representations of groups and algebras. Proc. of the Euroconference in Essen, Germany, April 1-5, 1997 (P. Draexler ed.). Basel: Birkhauser. Prog. Math. 173, 29–60 (1999).

[46] Greuel, G-M. and Pfister, G., A Singular Introduction to Commutative Algebra. Springer, Heidelberg, 2002.

[47] G.-M. Greuel, G. Pfister, and H. Schönemann., Singular 3.0.0. A Computer Algebra System for Polynomial Computations (computer program). Centre for Computer Algebra, University of Kaiserslautern (2001). `http://www.singular.uni-kl.de`.

[48] Havlicek, M., Klimyk, A. and Posta, S., *Central elements of the algebras $U'_q(\mathrm{so}_m)$ and $U'_q(\mathrm{iso}_m)$* (preprint), `arXiv.math.QA/9911130`.

[49] Humphreys, J. E., Introduction to Lie Algebras and Representation Theory. Springer, New York, 1972.

[50] Isaev, A., Pyatov, P. and Rittenberg, V., *Diffusion algebras* (preprint), `arXiv.math.QA/0103603`.

[51] Iorgov, N., *On the Center of q-Deformed Algebra $U'_q(\mathrm{iso}_3)$ Related to Quantum Gravity at q a Root of* 1, Proc. of IV Int. Conf. Symmetry in Nonlinear Mathematical Physics, Kyiv, Ukraine, 2001.

[52] Jacobson, N., Lie Algebras. John Wiley, New York, 1962.

[53] Jespers, E. and Okninski, J., *Binomial Semigroups*, J. Algebra **202** (1998), 250–275.

[54] Kandri-Rody, A. and Weispfenning, V., *Noncommutative Gröbner bases in algebras of solvable type*, J. Symb. Comput. **9** (1990), 1–26.

[55] Kassel, C., Quantum Groups. Springer, New York, 1995.

[56] Klimyk, A. and Schmüdgen, K., Quantum groups and their representations. Springer, 1997.

[57] Kobayashi, Y., *Gröbner Bases of Associative Algebras and the Hochschild Cohomology*, Trans. Amer. Math. Soc. (electronic), posted July 16, 2004.

[58] Kostrikin, A.I. and Manin, Y.I., Linear algebra and geometry. Gordon and Breach Science, 1989.

[59] Kredel, H., Solvable Polynomial Rings. Shaker, 1993.

[60] Levandovskyy, V., *On Gröbner bases for noncommutative G-algebras*, Proc. of the 8th Rhine Workshop on Computer Algebra (H. Kredel and W.K. Seiler eds.), Mannheim, Germany, 2002.

[61] Levandovskyy, V., *PBW Bases, Non-Degeneracy Conditions and Applications*, Proc. of the ICRA X conference (R.-O. Buchweitz and H. Lenzing eds.), Toronto, Canada. Fields Institute Communications **43** (2003).

[62] Levandovskyy, V. and Schönemann, H., *Plural - a computer algebra system for noncommutative polynomial algebras*, Proc. of the International Symposium on Symbolic and Algebraic Computation issac-2003, acm Press, 2003.

[63] Levasseur, T., *Some properties of non-commutative regular rings*, Glasgow Math. J. **34** (1992), 277–300.

[64] Li, H., Non-commutative Gröbner Bases and Filtered-Graded Transfer, Lect. Notes in Math. 1795. Springer, 2002.

[65] Lobillo, F.J., *Métodos algebraicos y efectivos en grupos cuánticos* (PhD thesis, in Spanish). University of Granada, Spain, 1998.

[66] Lu, J., Yan, M. and Zhu, Y., *On the set-theoretical Yang-Baxter equation*, Duke Math. J. **104** (2000), 1–18.

[67] Majid, S., Foundations of the Quantum Groups. Cambridge University Press, 1995.

[68] Manin, Yu I., Quantum groups and non-commutative geometry. Les publications CRM, Université de Montreal, 1988.

[69] McConnell, J.C. and Robson, J.C., Non-commutative noetherian rings. John Wiley and Sons, Chichester, 1987.

[70] Mora, T., *Gröbner bases for non-commutative polynomial rings*, Proc. aaecc 3, Lect. N. in Comp. Sci. **229** (1986), 353–362.

[71] Mora, T., *Seven variations on standard bases* (preprint), Univ. Genoa, 1988 (accesible in `http://www.disi.unige.it/person/MoraF/publications.html`).

[72] Mora, T., *Gröbner bases in non-commutative algebras*, Proc. of the issac'88 Conference, Lect. N. Comp. Sci. **358** (1989) 1, 150–161.

[73] Mora, T., *An introduction to commutative and noncommutative Gröbner bases*, Theor. Comput. Sci. **134** (1994) 1, 131–173.

[74] Newman, M.H.A., *On theories with a combinatorial definition of "equivalence"*, Ann. of Math. **43** (1942), 223–243.

[75] Odesskii, A., *On the set-theoretical Yang-Baxter equation* (preprint). 2002.

[76] Pesch, M., *Two-sided Gröbner bases in iterated Ore extensions*, Symbolic rewriting techniques. Papers from the workshop held in Ascona, Switzerland, April 30 - May 4, 1995. Prog. Comput. Sci. Appl. Log. **15** (1998) 225–243 .

[77] Rotman, J., An introduction to homological algebra. Academic Press, 1979.

[78] Schelter, W., *Noncommutative affine rings with polynomial identity are catenary*, J. Algebra **51** (1978), 12–18.

[79] Smith, G., *Computing global extension modules*, J. Symb. Comput. **29** (2000) 4-5, 729–746.

[80] Tate, J. and Van der Bergh, M., *Homological properties of Sklyanin algebras*, Invent. Math. **124** (1996), 619–647.

[81] Weinstein, P. and Xu, P., *Classical solutions of the quantum Yang-Baxter equation*, Comm. Math. Phys. **148** (1992), 309–343.

Index

List of Symbols