Parametrised Gröbner-Shirshov Bases

PARAMETRISED GRÖBNER-SHIRSHOV BASES

K. Kalorkoti[1] and I. Stanciu[2]

Abstract: We consider the problem of describing Gröbner-Shirshov bases for free associative algebras in finite terms. To this end we consider parametrised elements of an algebra and give methods for working with them which under favourable conditions lead to a basis given by finitely many patterns. On the negative side we show that in general there can be no algorithm. We relate our study to the problem of verifying that a given set of words in certain groups yields Bokut' normal forms (or groups with a standard basis).

Key Words: Normal form, Gröbner-Shirsov bases, free associative algebra, group, HNN extension.

2000 Mathematics Subject Classification: 20F10; 16Z05; 68W30.

1. Introduction

Gröbner-Shirshov bases are a method for creating normal forms in various mathematical structures. In their historical survey Bokut' and Kolesnikov (2003) ascribe their origins to Shirshov (1962) for Lie polynomials and to Buchberger (1965) for commutative polynomials. In both cases we are given generators for an ideal and produce a basis that enables us to answer questions such as membership of the ideal. Although there is a uniformity in the basic ideas there is one significant difference between the commutative polynomial case and the non-commutative one. In the commutative case Hilbert's Basis Theorem assures us that there is a finite basis for every ideal and the sought after special basis is also finite (at least if we remove redundant members); this is not so for the non-commutative case. This difference raises the following questions for the non-commutative case:

1. How can we describe a Gröbner-Shirshov basis in finite terms?
2. How can we produce a Gröbner-Shirshov basis in finite time?
3. Given a proposed Gröbner-Shirshov basis how can we check if it is one in finite time?

An algorithm for producing a Gröbner-Shirshov basis is a finite description of the basis. However this is not amenable to algebraic operations on the members of the basis. Our aim is to produce a description that gives direct access to the format of the elements. In general there is no hope of answering the preceding questions in a constructive way. In this paper we focus on finitely generated free associative algebras and describe an approach based on parametrised elements that goes some way towards addressing the questions at least under favourable conditions. The methods discussed have a large algorithmic component but we show in §8.3 that they cannot be algorithmic in general, indeed even under some favourable assumptions (see also Lemma 4.1).

Bokut' (1966, 1967), see also Bokut' and Collins (1980), introduced a method for constructing normal forms for groups (called standard bases) built as a sequence of HNN extensions starting with a free group. These forms have proved very useful in simplifying the proofs of various results connected with decision problems in group theory, e.g., see Kalorkoti (1982). It is a straightforward matter to phrase the membership problem for a normal subgroup of a free group as a membership problem for an appropriate ideal in a free associative algebra. One motivation for the approach of this paper comes from an observation by Kalorkoti (2011) where it is shown that under some mild assumptions Bokut' normal forms are a Gröbner-Shirshov basis (Lemma 2.6 of

[1]School of Informatics, 10 Crichton Street, Edinburgh EH8 9AB, UK (kk@inf.ed.ac.uk)
[2]School of Informatics, address as above (s1235413@sms.ed.ac.uk)

the paper cited). These have the special form $U_i - V_i$, for $i \in I$, where each U_i, V_i is a parametrised word in the generators of the underlying group and their inverses. In many situations I is a finite set but each U_i, V_i represents infinitely many words determined by the parameters present and side conditions on them.

The method of Bokut' provides a way to identify a likely standard basis, it is then necessary to check certain conditions in order to verify that the proposed set is indeed a basis. The checking phase can involve quite detailed combinatorial analysis. The result cited above shows that if the proposed set is a standard basis then (subject to the mild assumptions) it is a Gröbner-Shirshov basis for the ideal in the corresponding free associative algebra and conversely. This opens the way to an alternative approach: we use the method of Bokut' to produce the proposed standard basis consisting of parametrised words as described above. We then use the method described in this paper to check if the proposed basis is a Gröbner-Shirshov basis. The methods described in this paper provide an approach but in general there cannot be an algorithm, as shown in §8.3. Our framework applies to general parametrised subsets of free associative algebras but our examples focus on the special case where elements are of the form $U - V$ where U, V are parametrised words.

2. Gröbner-Shirshov bases

In order to provide a context for the rest of the paper we give here a brief reminder of the key concepts of Gröbner-Shirshov bases for ideals of a free associative algebra $k\langle X\rangle$. We use X^* to denote the set of words over X and $\ell(W)$ to denote the length of a word W. We assume as given an admissible order[3] $<$ on X^*, i.e., a well-order such that if $U < V$ then $AUB < AVB$ for all $A, B, U, V \in X^*$. Thus every non-zero $f \in k\langle X\rangle$ has a largest word called the *leading word* and denoted by $\mathrm{lw}(f)$; the leading word of 0 is undefined. For non-zero fixed $f, g \in k\langle X\rangle$ we have two possible compositions:

1. If $W = \mathrm{lw}(f) = A\,\mathrm{lw}(g)B$ for some $A, B \in X^*$ then we define
$$(f, g)_W = f - \mathrm{lc}(f)/\mathrm{lc}(g))AgB.$$
This is called the *inclusion composition* of f and g w.r.t. W.

2. If $W = A\,\mathrm{lw}(f) = \mathrm{lw}(g)B$ for some $A, B \in X^*$ with $\ell(A) < \ell(\mathrm{lw}(g))$ and $\ell(B) < \ell(\mathrm{lw}(f))$ then we define
$$(f, g)_W = Af/\mathrm{lc}(f) - gB/\mathrm{lc}(g).$$
This is called the *intersection composition* of f and g w.r.t. W.

Note that if both compositions apply then $\mathrm{lw}(f) = \mathrm{lw}(g)$ and the compositions are the same up to a non-zero constant multiple. For the purposes of building a Gröbner-Shirshov basis non-zero constant multiples can be discarded and so we need only apply one of the two compositions.

Another important concept in Gröbner-Shirshov bases is that of reducing one element by another. If $f, g \in k\langle X\rangle$ are such that $\mathrm{lw}(f) = A\,\mathrm{lw}(g)B$ for some $A, B \in X^*$ then we write $f \to_g h$ where $h = f - \mathrm{lc}(f)/\mathrm{lc}(g)\,AgB$; i.e., h is the inclusion composition of f, g. The aim is to see if there is a sequence of reductions by elements of an ideal basis G that results in 0, for this is then a proof that f belongs to the ideal generated by G. The converse is true provided that G is a Gröbner-Shirshov basis, indeed this is one of various equivalent defining conditions for such bases and we will use this in the paper.

It is a simple matter to see that not every basis of an ideal is a Gröbner-Shirshov basis. Given a subset F of $k\langle X\rangle$ and an admissible order on X^* we have a method for building (at

[3]It is possible to work with other orders, see Chen and Zhong (2008), but this is rather exceptional.

least in principle) a Gröbner-Shirshov basis S for the ideal (F). We start by setting $S = F$ then consider in turn each possible composition $(f, g)_W$ and find a reduced form h for it w.r.t. S; i.e., reduce h as far as possible (there are no infinite reduction sequences since $<$ is a well order). If $h \neq 0$ we add it to S and iterate (each time considering only compositions that have not been considered before). Note that we need only find *one* possible reduced form h for $(f, g)_W$. This is because once h is added to S we have ensured that $(f, g)_W$ is trivial modulo S, i.e., reduces to 0 using members of S. For inclusion compositions the only situation where $(f, g)_W$ and $(g, f)_W$ are both defined is when $\mathrm{lw}(f) = \mathrm{lw}(g)$ and in this case the two compositions are the same up to a non-zero constant multiple. Thus only one composition needs to be considered, however the methods we describe in §8 do not use this optimisation for the sake of clearer exposition.

3. Notation

Throughout the paper X is a finite non-empty alphabet whose members are called letters. As mentioned above, we denote the set of all words over X by X^* and use $\ell(W)$ to denote the length of a word W. We will be working with parametrised words as defined below. Assume that we have fixed a subset P of X. Let $\mathcal{V}$ be a set of variables ranging over $\mathbb{N}$ (we include 0 in $\mathbb{N}$) and $\mathcal{F}$ a set of functions $f : \mathbb{N}^p \to \mathbb{N}$, where the arity p varies with f, and the parameters of f are variables from $\mathcal{V}$. Consider the first order logic expressions defined by

$$C := (v_1 > v_2) \mid \neg C \mid (C_1 \wedge C_2) \mid (C_1 \vee C_2) \mid \exists x\, C \mid \forall x\, C$$

where

- v_1, v_2 are of the form $n_0 + n_1 s_1 + \cdots + n_m s_m$ where $n_i \in \mathbb{Z}$, for $0 \leq i \leq m$, and $s_i \in \mathcal{V} \cup \mathcal{F}$, for $1 \leq i \leq m$.
- $x \in \mathcal{V}$.

Naturally operators such as $=, <, \leq, \geq$ can be expressed by the basic terms and we will use these in examples. Note that expressions are closed under negation. We will use $\mathrm{Var}(C)$ to denote the set of free variables that occur in C (i.e., those not under the scope of a quantifier). For example, $\mathrm{Var}((s > 1) \wedge \exists u \exists s(t = 2s - 3u)) = \{ s, t \}$. An expression of the form $C \wedge_{v \in \mathrm{Var}(C)} (v > 0)$ will be called a *defining condition*, we work with such conditions throughout the paper. An *assignment* $\mathbf{a}$ for C is a set of the form $\{ v_1 \leftarrow n_1, \ldots, v_m \leftarrow n_m \}$ where $v_1, \ldots, v_m \in \mathcal{V}$ with $\mathrm{Var}(C) \subseteq \{ v_1, \ldots, v_m \}$ and $n_1, \ldots, n_m$ strictly positive natural numbers. Such an assignment *satisfies* C if after replacing v_i with n_i, for $1 \leq i \leq m$, the resulting expression is true (as usual $\wedge$ is conjunction and $\vee$ is disjunction). We will use $\mathbf{V}(C)$ to denote the set of all assignments that satisfy C and involve only the variables in $\mathrm{Var}(C)$. For convenience we will use $\mathbf{tt}_V$ to denote $\wedge_{v \in V}(v > 0)$, where V is a set of variables; thus this condition is satisfied by all assignments that include its variables. If the set V is of no particular interest we will just write $\mathbf{tt}$. Requiring each number in an assignment to be strictly positive simplifies the analysis later on, if we want a variable to be 0 then we treat that as a special case. For a set of variables T the notation $\mathbf{V}_T(C)$ denotes all assignments in $\mathbf{V}(C)$ but each assignment $\{ v_1 \leftarrow n_1, \ldots, v_m \leftarrow n_m \}$ is replaced with $\{v_i \leftarrow n_i \mid 1 \leq i \leq n \text{ and } v_i \in T\}$. Let $T \subseteq \mathrm{Var}(C)$, $\{ t_1, \ldots, t_r \} = \mathrm{Var}(C) - T$ and define $C|_T = \exists t_1 \cdots \exists t_r\, C$ then it is clear that $\mathbf{V}_T(C) = \mathbf{V}(C|_T)$, assuming that C is a defining condition.

A *generalised word* over X is an expression of the form $x_1^{e_1} \cdots x_n^{e_n}$ where $x_i \in X$, for $1 \leq i \leq n$, and each e_i is either a natural number or a variable from $\mathcal{V}$ provided that $x_i \in P$. A *parametrised word* is an expression $[\![W]\!]_C$ where W is a generalised word and C is a defining condition, where $\mathrm{Var}(C)$ includes all the variables in the exponents of W (we allow the possibility that C has parameter variables that do not appear in W). If $E = [\![W]\!]_C$ is a parametrised word and $\mathbf{a}$ is an

assignment then $W(\mathbf{a})$ denotes the word obtained by replacing each variable with the value, if any, given by the assignment; we say that W is *evaluated at* $\mathbf{a}$ and also use $E(\mathbf{a})$ to denote $W(\mathbf{a})$. Note that throughout the paper we only use this notation when $\mathbf{a}$ contains all the variables that occur in W and so $W(\mathbf{a}) \in X^*$, in principle the definition applies more generally so that only some of the parameters become fixed. A parametrised word $E = [\![W]\!]_C$ denotes the set of words $\{W(\mathbf{a}) \mid \mathbf{a} \in \mathbf{V}(C)\} \subseteq X^*$. If s is a variable or a function we use $s(\mathbf{a})$ to denote the result of applying the assignment $\mathbf{a}$ to s or its arguments as appropriate. For the sake of convenience we set $n(\mathbf{a}) = n$, for all $n \in \mathbb{N}$.

For example, if $X = \{x, y\}$ with $P = \{y\}$ and s, t are variables from $\mathcal{V}$, then $[\![x^2y^sxy^t]\!]_C$ is a parametrised word of length $3+s+t$. The condition C can be any valid defining condition (e.g., $s > 0 \wedge t > 0$); naturally if C has no satisfying assignments then the parametrised word does not denote any members of X^*. We can put functions from $\mathcal{F}$ in exponents with the understanding that if $y^{f(s_1,\ldots,s_m)}$ occurs in W then this is shorthand for y^s where s is a new variable and we add $(s = f(s_1, \ldots, s_m)) \wedge (s > 0)$ to the defining condition. For example, $x^2y^{s+t+1}xy^{(s+1)^2}$ is a generalised word of length $4 + s + t + (s + 1)^2$, assuming that the displayed functions are in $\mathcal{F}$. A word $[\![W]\!]_C$ is *fixed* if none of its exponents involves a variable or a function in which case it denotes the singleton set $\{W\}$, if $\mathbf{V}(C) \neq \emptyset$, and the empty set otherwise. It is at times convenient to abuse notation and use U to denote the single member of $U = [\![W]\!]_C$ when W is fixed and $\mathbf{V}(C) \neq \emptyset$.

We extend the use of the notation $[\![\cdot]\!]_C$ to include tuples of generalised words: $[\![W_1, \ldots, W_r]\!]_C$. This notation denotes the set $\{(W_1(\mathbf{a}), \ldots, W_r(\mathbf{a})) \mid \mathbf{a} \in \mathbf{V}(C)\}$. The brackets provide a context that, unless otherwise indicated, delimits the scope of the variables in C. Thus the variable t in $[\![x^t]\!]_{t>0\wedge t<3}$ has no influence on the one in $[\![x^t]\!]_{t>0}$; the first parametrised word denotes the set $\{x, x^2\}$ and the second the set $\{x, x^2, x^3, \ldots\}$. By contrast $[\![x^s, x^t]\!]_{s=t+1\wedge s>0\wedge t>0}$ denotes the set $\{(x^2, x), (x^3, x^2), \ldots\}$.

We will at times wish to extend the scope of a variable so that it covers more than one word (or parametrised elements of $k\langle X\rangle$, see §7). A possible solution is to use the notion of an environment from computer science with local variables whose scope is delimited by the environment. In order to avoid excessive notation we will use the more compact $[\![\ ]\!]$ notation with the scope of parameter variables, when extended, being indicated by context just as is done in standard mathematical arguments.

4. Inclusion and intersection of words

We say that two words $[\![U]\!]_{C_U}$, $[\![V]\!]_{C_V}$ are *separated* if $\mathrm{Var}(C_U) \cap \mathrm{Var}(C_V) = \emptyset$, clearly this can always be ensured by using fresh parameter variables for $[\![V]\!]_{C_V}$, say. We assume throughout this section that $[\![U]\!]_{C_U}$, $[\![V]\!]_{C_V}$ are separated.

We will want to solve equations of the form: given $[\![W_1]\!]_{C_1}$ and $[\![W_2]\!]_{C_2}$ find all assignments $\mathbf{a} \in \mathbf{V}(C_1)$, $\mathbf{b} \in \mathbf{V}(C_2)$ such that $W_1(\mathbf{a}) = W_2(\mathbf{b})$. Assuming that the words are separated we have $\mathbf{V}(C_1 \wedge C_2) = \{\mathbf{a} \cup \mathbf{b} \mid \mathbf{a} \in \mathbf{V}(C_1) \text{ and } \mathbf{b} \in \mathbf{V}(C_2)\}$. We may therefore work with the pair $[\![W_1, W_2]\!]_{C_1\wedge C_2} = [\![W_1]\!]_{C_1} \times [\![W_2]\!]_{C_2}$ and consider the single variable equation $W_1(\mathbf{a}) = W_2(\mathbf{a})$. Since the words $[\![U]\!]_{C_U}$, $[\![V]\!]_{C_V}$ are assumed separated we replace the two defining conditions by the single one $C = C_U \wedge C_V$ and consider the pair $[\![U, V]\!]_C$. As discussed in §2, the following two problems are central to the construction of Gröbner-Shirshov bases:

Inclusion: Return all assignments $\mathbf{a}$ and quadruples of words $[\![A, B, U, V]\!]_Q$ such that $U(\mathbf{a}) = (AVB)(\mathbf{a})$.

Intersection: Return all assignments $\mathbf{a}$ and quadruples of words $[\![A, B, U, V]\!]_Q$ with $\ell(A(\mathbf{a})) < \ell(V(\mathbf{a}))$ and $\ell(B(\mathbf{a}))) < \ell(U(\mathbf{a})))$ such that $(AU)(\mathbf{a}) = (VB)(\mathbf{a})$.

By 'return all ...' we mean return finitely many quadruples of words $[\![A_1, B_1, U, V]\!]_{Q_1}, \ldots$ $[\![A_q, B_q, U, V]\!]_{Q_q}$ such that all the sought assignments $\mathbf{a}$ are members of $\cup_{i=1}^{q} \mathbf{V}(Q_i)$. Moreover given any $\mathbf{a} \in \mathbf{V}(Q_i)$, with $1 \leq i \leq q$, then $A = A_i$ and $B = B_i$ is a solution to $U(\mathbf{a}) = (AVB)(\mathbf{a})$, in the case of inclusion, or of $(AU)(\mathbf{a}) = (VB)(\mathbf{a})$, in the case of intersection.

Our subsequent analysis will show that this notion does indeed allow for all words to be characterised, we never need to use infinitely many quadruples or functions other than those in $\mathcal{F}$. We define

$$\mathrm{Inc}[\![U, V]\!]_C = \{[\![A_i, B_i, U, V]\!]_{Q_i} \mid 1 \leq i \leq q \text{ and } \mathbf{V}(Q_i) \neq \emptyset\}$$

where $[\![A_1, B_1, U, V]\!]_{Q_1}, \ldots [\![A_q, B_q, U, V]\!]_{Q_q}$ are the quadruples of words for the inclusion problem for $[\![U, V]\!]_C$. Likewise we define

$$\mathrm{Int}[\![U, V]\!]_C = \{[\![C_i, D_i, U, V]\!]_{R_i} \mid 1 \leq i \leq r \text{ and } \mathbf{V}(R_i) \neq \emptyset\}$$

where $[\![C_1, D_1, U, V]\!]_{R_1}, \ldots [\![C_r, D_r, U, V]\!]_{R_r}$ are the quaruples of words for the intersection problem for $[\![U, V]\!]_C$.

We have used quadruples $[\![A, B, U, V]\!]_C$ of words because the scope of the variables for $[\![U, V]\!]_C$ needs to cover the variables occurring in A, B. In the rest of the paper we will drop the final two words from quadruples of the form $[\![A, B, U, V]\!]_C$ in order to avoid repetition and clutter, but it must be understood that they are always present.

Note that if $U = 1$ or $V = 1$ then the intersection problem has no solutions. For the inclusion problem, if $U = 1$ then there is just one solution $A = B = 1$ provided $V = 1$ otherwise there is no solution. If $V = 1$ then A can be any prefix of U and B the rest of U. From now on we will assume without further comment that $U \neq 1$ and $V \neq 1$.

If U, V are both from X^* the two problems can clearly be solved algorithmically. We analyse the situation when at least one word is not from X^*. The quadruples of generalised words with the corresponding defining conditions can always be obtained. However the corresponding decision problem is undecidable in general even if the functions in $\mathcal{F}$ are computable, i.e., there is no algorithm to decide if $\mathrm{Inc}[\![U, V]\!]_C$ is empty and likewise for $\mathrm{Int}[\![U, V]\!]_C$.

Lemma 4.1 *There are polynomials M_1, M_2 with natural number coefficients such that the inclusion problem for words is undecidable with $\mathcal{F} = \{ M_1, M_2 \}$. Likewise there is a single polynomial M_1, with integer coefficients such that the intersection problem for words is undecidable with $\mathcal{F} = \{ M_1 \}$.*

Proof. Let S be a recursively enumerable non-recursive subset of $\mathbb{N}_{>0}$, where $\mathbb{N}_{>0}$ denotes the strictly positive natural numbers. By Matiyasevich (1970) there is a polynomial $M(t; s_1, \ldots, s_p)$ with integer coefficients such that $n \in S$ if and only if there is a $\mathbf{b} \in \mathbb{N}_{>0}^p$ such that $M(n; \mathbf{b}) = 0$.

For the inclusion problem set $M(t; s_1, \ldots, s_p) = M_+(t; s_1, \ldots, s_p) - M_-(t; s_1, \ldots, s_p)$ where M_+ and M_- have strictly positive coefficients or are 0. Set also $X = \{ x, y, z_1, \ldots, z_p \}$, $P = \{ y, z_1, \ldots, z_p \}$, $\mathcal{F} = \{ 1 + M_+, 1 + M_- \}$ and

$$U_n = [\![xy^{1+M_+(n;s_1,\ldots,s_p)} z_1^{s_1} \cdots z_p^{s_p} x]\!]_{s_1>0 \wedge \cdots \wedge s_p > 0},$$
$$V_n = [\![xy^{1+M_-(n;t_1,\ldots,t_p)} z_1^{t_1} \cdots z_p^{t_p} x]\!]_{t_1>0 \wedge \cdots \wedge t_p > 0}.$$

We claim that V_n is contained in U_n if and only if there is a $\mathbf{b} \in \mathbb{N}_{>0}$ such that $M(n; \mathbf{b}) = 0$. If this is the case then $M_+(n; \mathbf{b}) = M_-(n; \mathbf{b})$ and so the two words are equal upon setting appropriate values for the variables. Conversely suppose there exist words A_n, B_n and an assignment $\mathbf{a}$ such that $U_n(\mathbf{a}) = (A_n V_n B_n)(\mathbf{a})$. Since $U_n(\mathbf{a})$, $V_n(\mathbf{a})$ both start and end with x and have no

other occurrences of x it follows that $A_n(\mathbf{a}) = 1$ and $B_n(\mathbf{a}) = 1$. Thus $U_n(\mathbf{a}) = V_n(\mathbf{a})$ hence $s_i(\mathbf{a}) = t_i(\mathbf{a})$, for $1 \leq i \leq p$. It now follows easily that there is a $\mathbf{b} \in \mathbb{N}^p_{>0}$ such that $M(n; \mathbf{b}) = 0$.

We now deal with the intersection problem. Set $X = \{ x, y, z \}$, $P = \{ y \}$, $\mathcal{F} = \{ 1 + M^2 \}$ and

$$U_n = [\![xy^{1+M^2(n;s_1,\ldots,s_p)} z]\!]_{s_1>0\wedge\cdots\wedge s_p>0},$$
$$V = xyz.$$

We claim that the intersection happens if and only if $M(n; \mathbf{b}) = 0$ for some $\mathbf{b} \in \mathbb{N}^p_{>0}$. Suppose that there are words A_n, B_n and an $\mathbf{a}$ such that $A_n(\mathbf{a})U_n(\mathbf{a}) = V(\mathbf{a})B_n(\mathbf{a})$ with $\ell(A_n(\mathbf{a})) < \ell(V(\mathbf{a})) = 3$ and $\ell(B_n(\mathbf{a})) < \ell(U_n(\mathbf{a})) = 3 + M(n, s_1 \ldots, s_p)(\mathbf{a})^2$. It follows that $A_n(\mathbf{a})$ is either 1 or x or xy. The second and third possibilities lead to a contradiction and so $A_n(\mathbf{a}) = 1$. It now follows that we must have $M(n, s_1 \ldots, s_p)(\mathbf{a}) = 0$ and $B_n(\mathbf{a}) = 1$. Conversely if $M(n, \mathbf{b}) = 0$ then we have an assignment $\mathbf{a}$ such that $U_n(\mathbf{a}) = V = xyz$ and we take $A_n = B_n = 1$. □

A *syllable* is a word of the form x^e where $x \in X$ and $e \in \mathbb{N}$ or $e \in \mathcal{V}$ provided that $x \in P$. A generalised word $U = x_1^{e_1} \ldots x_n^{e_n}$ is said to be *collected* if $e_i \neq 0$, for $1 \leq i \leq n$, and $x_i \neq x_{i+1}$, for $1 \leq i \leq n-1$. By convention the empty word is collected and has 1 as its only syllable. The *first syllable* of U is $x_1^{e_1}$ and the *last syllable* is $x_n^{e_n}$. The empty word has 1 as its first and last syllables. Note that U and $U(\mathbf{a})$ have the same number of syllables, for all assignments $\mathbf{a}$, since by assumption no exponent evaluates to 0.

Let W be a collected word. The *P-partition* of W is defined as $W_0 \underline{x}_1^{u_1} W_1 \cdots W_{n-1} \underline{x}_n^{u_n} W_n$ where each $x_i \in P$ and each word W_j is free of letters from P. Moreover each u_i is either a variable from $\mathcal{V}$ or a strictly positive natural number. The *profile* of W is defined as

$$\mathrm{pr}(W) = (x_1^{u_1}, \ldots, x_n^{u_n})$$

The *length* of the profile of W, denoted by $\mathrm{lpr}(W)$, is n. We define $\mathrm{pr}(W)(\mathbf{a})$, for an assignment $\mathbf{a}$, in an analogous way to the definition for parametrised words. The *co-profile* of W is defined as:

$$\text{co-pr}(W) = (W_0, \ldots, W_n).$$

We will adopt the convention that an equality $W = W_0 \underline{x}_1^{u_1} W_1 \cdots W_{n-1} \underline{x}_n^{u_n} W_n$ means that the right hand side is the P-partition of the word W.

Lemma 4.2 *Let $U = U_0 \underline{x}_1^{u_1} \cdots \underline{x}_m^{u_m} U_m$ and $V = V_0 \underline{y}_1^{v_1} \cdots \underline{y}_n^{v_n} V_n$. We have the following cases.*

$$\mathrm{pr}(UV) = \begin{cases} (x_1^{u_1}, \ldots, x_{m-1}^{u_{m-1}}, x_m^{u_m+v_1}, y_2^{v_2}, \ldots, y_n^{v_n}), & \text{if } U_m = V_0 = 1 \text{ and } x_m = y_1; \\ (x_1^{u_1}, \ldots, x_m^{u_m}, y_1^{v_1}, \ldots, y_n^{v_n}), & \text{otherwise.} \end{cases}$$

Moreover $\mathrm{lpr}(UV) = \mathrm{lpr}(U) + \mathrm{lpr}(V) - 1$ *If* $U_m = V_0 = 1$ *and* $x_m = y_1$, *otherwise* $\mathrm{lpr}(UV) = \mathrm{lpr}(U) + \mathrm{lpr}(V)$.

Proof. Apart from the first case the syllables of the profile of UV are either separated by $U_n V_0$ or $x_m \neq y_1$. The second part follows from the expression for $\mathrm{pr}(UV)$. □

Note that evaluating words at an assignment has no effect on which case holds in the preceding lemma. We will be applying the lemma to analyse the equations $U(\mathbf{a}) = (AVB)(\mathbf{a})$ and $(AU)(\mathbf{a}) = (VB)(\mathbf{a})$ for an assignment $\mathbf{a}$. We can reduce the number of cases to be considered by observing that the equations can be written as $U^R(\mathbf{a}) = (B^R V^R A^R)(\mathbf{a})$ and $(U^R A^R)(\mathbf{a}) = (B^R V^R)(\mathbf{a})$ where W^R denotes the reversed version of W.

Lemma 4.3 *Let* $\mathbf{a}$ *be an assignment. Then* $U(\mathbf{a}) = V(\mathbf{a})$ *if and only if* $\mathrm{pr}(U)(\mathbf{a}) = \mathrm{pr}(V)(\mathbf{a})$ *and* $\text{co-pr}(U) = \text{co-pr}(V)$.

Proof. Set $U = U_0\underline{x}_1^{u_1}U_1\cdots U_{m-1}\underline{x}_m^{u_m}U_m$ and $V = V_0\underline{y}_1^{v_1}V_1\cdots V_{n-1}\underline{y}_n^{v_n}V_n$. Suppose $U(\mathbf{a}) = V(\mathbf{a})$ so that $U_0x_1^{u_1(\mathbf{a})}U_1\cdots U_{m-1}x_m^{u_m(\mathbf{a})}U_m = V_0y_1^{v_1(\mathbf{a})}V_1\cdots V_{n-1}y_n^{v_n(\mathbf{a})}V_n$. By the assumption on assignments and the definition of a profile $u_i(\mathbf{a}) \neq 0$, for $1 \leq i \leq m$, and $v_j(\mathbf{a}) \neq 0$, for $1 \leq j \leq n$. Moreover each U_i is free of letters from P and likewise for each V_j. It follows that $U_0 = V_0$ and hence $x_1 = y_1$ with $u_1(\mathbf{a}) = v_1(\mathbf{a})$. A simple induction completes the proof. The converse is immediate. □

5. The inclusion problem

Throughout this and the next section we consider the separated words $[\![U]\!]_{C_U}$, $[\![V]\!]_{C_V}$ and set

$$U = U_0\underline{x}_1^{u_1}U_1\cdots U_{m-1}\underline{x}_m^{u_m}U_m,$$
$$V = V_0\underline{y}_1^{v_1}V_1\cdots V_{n-1}\underline{y}_n^{v_n}V_n,$$

so that $\mathrm{lpr}(U) = m$ and $\mathrm{lpr}(V) = n$. Also

$$A = A_0\underline{z}_1^{a_1}A_1\cdots A_{s-1}\underline{z}_s^{a_s}A_s,$$
$$B = B_0\underline{w}_1^{b_1}B_1\cdots B_{t-1}\underline{w}_t^{b_t}B_t.$$

so that $s = \mathrm{lpr}(A)$ and $t = \mathrm{lpr}(B)$. We will assume that the variables in A, B are distinct from each other as well as those in U, V.

In order for $U(\mathbf{a}) = (AVB)(\mathbf{a})$ to hold we must have $\mathrm{pr}(U(\mathbf{a})) = \mathrm{pr}((AVB)(\mathbf{a}))$. It follows from Lemma 4.2 that m is one of $n+s+t$, $n+s+t-1$ or $n+s+t-2$ depending on which cases of Lemma 4.2 hold for AV and for $(AV)B$. Once we assume which pair of cases holds we can determine if the equation for m is at all possible and if so we analyse the equation $U(\mathbf{a}) = (AVB)(\mathbf{a})$. We consider two cases, the rest are similar.

Case I: First assume that the second case of Lemma 4.2 holds for both AU and for $(AU)V$ so that for an inclusion we must have $m = n+s+t$. Assume this equality holds. It follows that $\mathrm{pr}(A) = (x_1^{a_1}, \ldots, x_s^{a_s})$ and $\mathrm{pr}(B) = (x_{m-t+1}^{b_1}, \ldots, x_m^{b_t})$. Once this choice is made the equation $U(\mathbf{a}) = (AVB)(\mathbf{a})$ becomes

$$U_0x_1^{u_1(\mathbf{a})}U_1\cdots U_{m-1}x_m^{u_m(\mathbf{a})}U_m = A_0x_1^{a_1(\mathbf{a})}A_1\cdots x_s^{a_s(\mathbf{a})}A_sV_0y_1^{v_1(\mathbf{a})}V_1\cdots V_{n-1}y_n^{v_n(\mathbf{a})}V_nB_0x_{m-t+1}^{b_1(\mathbf{a})}\cdots x_m^{b_t(\mathbf{a})}B_t$$

By Lemma 4.3 the equation cannot hold unless $y_1 = x_{s+1}, \ldots, y_n = x_{s+n}$. Assuming this is the case then it follows from Lemma 4.3 that

$$U_i = \begin{cases} A_i, & \text{for } 0 \leq i \leq s-1; \\ A_sV_0, & \text{for } i = s; \\ V_{i-s}, & \text{for } s+1 \leq i \leq s+n-1; \\ V_nB_0, & \text{for } i = s+n; \\ B_{i-s-n}, & \text{for } s+n+1 \leq i \leq m \end{cases}$$

In addition

$$u_i(\mathbf{a}) = \begin{cases} a_i(\mathbf{a}), & \text{for } 1 \leq i \leq s; \\ v_{i-s}(\mathbf{a}), & \text{for } s+1 \leq i \leq s+n; \\ b_{i-s-n}(\mathbf{a}), & \text{for } s+n+1 \leq i \leq m; \end{cases}$$

The equalities for the U_i are easy to check, the only decision part is to check if there are words A_s, B_0 such that $A_sV_0 = U_s$ and $V_nB_0 = U_{s+n}$. Since V_0, V_n, U_s and U_{s+n} are fixed the problem is straightforward. Thus this part either shows that the inclusion is not possible or yields unique values for the subwords $U_0, \ldots, U_m$ and $V_0, \ldots, V_n$. For the defining condition, for a choice of s and t, we use

$$C \wedge \bigwedge_{1\leq i\leq s}(a_i = u_i) \bigwedge_{s+1\leq i\leq s+n}(v_{i-s} = u_i) \bigwedge_{s+n+1\leq i\leq m}(b_{i-s-n} = u_i) \bigwedge_{1\leq i\leq s}(a_i > 0) \bigwedge_{1\leq i\leq t}(b_i > 0).$$

The last two conjuncts can be omitted since C asserts that $u_i > 0$, for $1 \leq i \leq m$.

Case II: Assume now that the second and first cases of Lemma 4.2 hold for AV and for $(AV)B$ respectively so that $m = n + s + t - 1$. Assume that this equality is possible. Since case 2 of Lemma 4.2 holds for AV it follows that $A_sV_0 \neq 1$ or $z_s \neq y_1$. Since case 1 holds for $(AV)B$ it follows that $V_n = 1$, $B_0 = 1$ and $y_n = w_1$. the equation $U(\mathbf{a}) = (AVB)(\mathbf{a})$ becomes

$$U_0x_1^{u_1(\mathbf{a})}U_1\cdots U_{m-1}x_m^{u_m(\mathbf{a})}U_m = A_0z_1^{a_1(\mathbf{a})}A_1\cdots A_{s-1}z_s^{a_s(\mathbf{a})}A_sV_0y_1^{v_1(\mathbf{a})}V_1y_2^{v_2(\mathbf{a})}V_2\cdots V_{n-1}y_n^{v_n(\mathbf{a})+b_1(\mathbf{a})}B_1w_2^{b_2(\mathbf{a})}B_2\cdots B_{t-1}w_t^{b_t(\mathbf{a})}B_t.$$

Once again we obtain equalities for the U_i which can be checked easily as well as for the x_i. (If $A_sV_0 = 1$ then we require that $x_s \neq x_{s+1}$.) Assuming these hold we deduce that

$$u_i(\mathbf{a}) = \begin{cases} a_i(\mathbf{a}), & \text{for } 1 \leq i \leq s; \\ v_{i-s}(\mathbf{a}), & \text{for } s+1 \leq i \leq n+s-1; \\ v_n(\mathbf{a}) + b_1(\mathbf{a}) & \text{for } i = n+s; \\ b_{i-n-s+1}(\mathbf{a}), & \text{for } n+s+1 \leq i \leq m. \end{cases}$$

For the defining condition we use

$$C\wedge \bigwedge_{1\leq i\leq s}(a_i = u_i) \bigwedge_{s+1\leq i\leq n+s-1}(v_{i-s} = u_i) \wedge (v_n + b_1 = u_{n+s}) \bigwedge_{n+s+1\leq i\leq m}(b_{i-n-s+1} = u_i) \bigwedge_{1\leq i\leq s}(a_i > 0) \bigwedge_{1\leq i\leq t}(b_i > 0).$$

As above, the last two conjuncts can be omitted

6. The intersection problem

We continue to use the notation of the previous section for U, V, A and B. In order for $(AU)(\mathbf{a}) = (VB)(\mathbf{a})$ to hold we must have $\mathrm{pr}((AU)(\mathbf{a})) = \mathrm{pr}((UB)(\mathbf{a}))$. It follows from Lemma 4.2 that $s + m$ is one of $n + t + 1$, $n + t$, or $n + t - 1$ depending on which cases of Lemma 4.2 hold for AU and for VB. Once we assume which pair of cases holds we can determine if the equation for $s + m$ is at all possible and if so we analyse the equation $(AU)(\mathbf{a}) = (VB)(\mathbf{a})$.

6.1 Proof that $s \leq n$ is necessary

We will prove that if $s > n$ then $\ell(A) > \ell(V)$ and so the intersection is not possible. Assume that $s > n$ in this section. Given that the P-partition of a word W is $W_0\underline{x}_1^{u_1}W_1\cdots W_{m-1}\underline{x}_m^{u_m}W_m$ define its *P_i-partition* to be $W_0\underline{x}_1^{u_1}W_1\cdots W_{i-1}\underline{x}_i^{u_i}W_i$, for $1 \leq i \leq m$. Obviously two words W and W' are equal if and only if their profile lengths are the same and their P_i-partitions are equal for all i with $1 \leq i \leq \mathrm{lpr}(W)$.

If $AU(\mathbf{a}) = VB(\mathbf{a})$ then the P_n-partition of $AU(\mathbf{a})$ is $A_0 z_1^{a_1(\mathbf{a})} A_1 \cdots A_{n-1} z_n^{a_n(\mathbf{a})} A_n$. If the first case of Lemma 4.2 holds for VB, then its P_n-partition is $V_0 y_1^{v_1(\mathbf{a})} V_1 \cdots V_{n-1} y_n^{v_n(\mathbf{a})+b_1(\mathbf{a})} B_1$ otherwise it is $V_0 y_1^{v_1(\mathbf{a})} V_1 \cdots V_{n-1} y_n^{v_n(\mathbf{a})} V_n B_0$. Since the P_n-partitions of AU and VB are equal, we have

1. $V_i = A_i$ for $0 \le i \le n-1$
2. $v_i(\mathbf{a}) = a_i(\mathbf{a})$ for $0 \le i \le n-1$
3. $v_n(\mathbf{a}) \le a_n(\mathbf{a})$
4. $\ell(V_n) \le \ell(A_n)$

Therefore,

$$\begin{aligned}
\ell(V) &= \sum_{i=1}^{n} v_i(\mathbf{a}) + \sum_{i=0}^{n} \ell(V_i) \\
&= \sum_{i=1}^{n-1} v_i(\mathbf{a}) + \sum_{i=0}^{n-1} \ell(V_i) + v_n(\mathbf{a}) + \ell(V_n) \\
&= \sum_{i=1}^{n-1} a_i(\mathbf{a}) + \sum_{i=0}^{n-1} \ell(A_i) + v_n(\mathbf{a}) + \ell(V_n) \\
&\le \sum_{i=1}^{n-1} a_i(\mathbf{a}) + \sum_{i=0}^{n-1} \ell(A_i) + a_n(\mathbf{a}) + \ell(A_n) \\
&= \ell(A).
\end{aligned}$$

This contradicts the requirement that $\ell(A) < \ell(V)$, so the intersection is not possible if $s > n$.

6.2 Analysis of intersection

Just as for the inclusion problem, we illustrate the intersection problem with two cases, the rest are similar.

Case I: First assume that the second case of Lemma 4.2 holds for both AU and for VB so that $s + m = n + t$. As before, once a choice for s is made this fixes t and the equation $(AU)(\mathbf{a}) = (VB)(\mathbf{a})$ becomes

$$\begin{aligned}
A_0 z_1^{a_1(\mathbf{a})} A_1 \cdots A_{s-1} z_s^{a_s(\mathbf{a})} A_s U_0 x_1^{u_1(\mathbf{a})} U_1 \cdots U_{m-1} x_m^{u_m(\mathbf{a})} U_m = \\
V_0 y_1^{v_1(\mathbf{a})} V_1 \cdots V_{n-1} y_n^{v_n(\mathbf{a})} V_n B_0 w_1^{b_1(\mathbf{a})} B_1 \cdots B_{t-1} w_t^{b_t(\mathbf{a})} B_t,
\end{aligned}$$

It follows from §6.1 that $s \le n$. Note that $t = s + m - n \le m$. If $s < n$ then $t < m$ and we have the following equations:

1. $A_i = V_i$, for $0 \le i \le s-1$.
2. $A_s U_0 = V_s$.
3. $U_i = V_{i+s}$, for $1 \le i \le n-s-1$.
4. $U_{n-s} = V_n B_0$.
5. $U_i = B_{i-n+s}$ for $n-s+1 \le i \le m$.

These allow for finitely many solutions giving us finitely many pairs of candidates for A, B. If $s = n$ then $t = m$ and the equations become:

1. $A_i = V_i$, for $0 \leq i \leq n-1$.
2. $A_n U_0 = V_n B_0$.
3. $U_i = B_i$, for $1 \leq i \leq m$.

The equation $A_n U_0 = V_n B_0$ is similar to intersection except that there is no immediate requirement for the lengths of A_n, B_0 to be smaller than those of V_n, U_0 respectively. Even so an upper bound on their lengths will follow from the requirement on the lengths of A, B given below, so again we obtain finitely many pairs of candidates for A, B. Assuming the equations hold we must then have $a_i(\mathbf{a}) = v_i(\mathbf{a})$, for $1 \leq i \leq s$, and

$$u_{i-s}(\mathbf{a}) = \begin{cases} v_i(\mathbf{a}), & \text{for } s+1 \leq i \leq n; \\ b_{i-n}(\mathbf{a}), & \text{for } n+1 \leq i \leq s+m. \end{cases}$$

We also need to ensure the length conditions on A and B which state

$$\sum_{i=1}^{s} a_i(\mathbf{a}) + \sum_{i=0}^{s} \ell(A_i) < \sum_{i=1}^{n} v_i(\mathbf{a}) + \sum_{i=0}^{n} \ell(V_i),$$
$$\sum_{i=1}^{t} b_i(\mathbf{a}) + \sum_{i=0}^{t} \ell(B_i) < \sum_{i=1}^{m} u_i(\mathbf{a}) + \sum_{i=0}^{n} \ell(U_i).$$

If $s = n$ the conditions are equivalent to

$$\ell(A_n) < \ell(V_n), \qquad \ell(B_0) < \ell(U_0),$$

which give us the claimed bounds for the lengths of A_n and B_0 (in fact we only use one inequality since $A_n U_0 = V_n B_0$ so that, e.g., $\ell(B_0) = \ell(A_n) + \ell(U_0) - \ell(V_N)$.) If $s < n$ the conditions are equivalent to

$$0 < \sum_{i=s+1}^{n} v_i(\mathbf{a}) + \sum_{i=s+1}^{n} \ell(V_i), \qquad 0 < \sum_{i=1}^{n-s} u_i(\mathbf{a}) + \sum_{i=1}^{n-s} \ell(U_i).$$

These hold automatically since all summands are nonnegative and $v_n(\mathbf{a}) > 0$, $u_1(\mathbf{a}) > 0$. (Recall that for this case we do not need bounds on $\ell(A_n)$ and $\ell(B_n)$.) We can now write down the defining condition (which is the same for all pairs) just as before.

Case II: Suppose now, that the first case of Lemma 4.2 holds for both AU and for VB so that $s + m = n + t$. As before, once a choice for s is made this fixes t. As the first case of the lemma holds this gives the following:

1. $A_s = 1$ and $U_0 = 1$
2. $V_n = 1$ and $B_0 = 1$
3. $z_s = x_1$
4. $y_n = w_1$

The equation $AU(\mathbf{a}) = VB(\mathbf{a})$ becomes:

$$A_0 z_1^{a_1(\mathbf{a})} A_1 \cdots A_{s-1} z_s^{a_s(\mathbf{a})+u_1(\mathbf{a})} U_1 x_2^{u_2(\mathbf{a})} \cdots U_{m-1} x_m^{u_m(\mathbf{a})} U_m = V_0 y_1^{v_1(\mathbf{a})} V_1 \cdots V_{n-1} y_n^{v_n(\mathbf{a})+b_1(\mathbf{a})} B_1 w_2^{b_2(\mathbf{a})} \cdots B_{t-1} w_t^{b_t(\mathbf{a})} B_t,$$

Suppose first that $s < n$. Then $t < m$ and we have the following equations:

1. $A_i = V_i$ for $0 \leq i \leq s-1$.
2. $U_i = V_{i+s-1}$ for $1 \leq i \leq n-s$.
3. $U_i = B_{i+s-n}$ for $n-s+1 \leq i \leq m$.

The equations allow for at most one solution. The equations for the exponents are:

1. $a_i(\mathbf{a}) = v_i(\mathbf{a})$, for $1 \leq i \leq s-1$.
2. $a_s(\mathbf{a}) + u_1(\mathbf{a}) = v_s(\mathbf{a})$.
3. $u_i(\mathbf{a}) = v_{s-1+i}(\mathbf{a})$, for $2 \leq i \leq n-s$.
4. $u_{n-s+1}(\mathbf{a}) = v_n(\mathbf{a}) + b_1(\mathbf{a})$.
5. $u_i(\mathbf{a}) = b_{i-n+s}(\mathbf{a})$. for $n-s+2 \leq i \leq m$.

We must also check the equalities for lengths, i.e., $\ell(A) < \ell(V)$ and $\ell(B) < \ell(U)$. These reduce to

$$a_s(\mathbf{a}) < \sum_{i=s}^{n} v_i(\mathbf{a}) + \sum_{i=s}^{n-1} \ell(V_i), \qquad b_1(\mathbf{a}) < \sum_{i=1}^{n-s+1} u_i(\mathbf{a}) + \sum_{i=1}^{n-s} \ell(U_i),$$

which follow from the second and fourth equations above.

Suppose now that $s = n$, so that $m = t$. Recall that we are trying to solve the equation:

$$A_0 z_1^{a_1} A_1 \cdots A_{n-1} z_n^{a_n+u_1} U_1 x_2^{u_2} \cdots U_{m-1} x_m^{u_m} U_m = V_0 y_1^{v_1} V_1 \cdots V_{n-1} y_n^{v_n+b_1} B_1 w_2^{b_2} \cdots B_{t-1} w_m^{b_m} B_m,$$

We obtain the following equations:

1. $A_i = V_i$ for $0 \leq i \leq n-1$
2. $U_i = B_i$ for $1 \leq i \leq m$

These allow for only one solution. The equations for the exponents are given by

1. $a_i(\mathbf{a}) = v_i(\mathbf{a})$ for $1 \leq 1 \leq n-1$
2. $a_s(\mathbf{a}) + u_1(\mathbf{a}) = v_s(\mathbf{a}) + b_1(\mathbf{a})$
3. $u_i(\mathbf{a}) = b_i(\mathbf{a})$ for $2 \leq i \leq m$

The inequalities $\ell(A) < \ell(V)$ and $\ell(B) < \ell(U)$ reduce to

$$a_s(\mathbf{a}) < v_s(\mathbf{a}), \qquad b_1(\mathbf{a}) < u_1(\mathbf{a}).$$

The defining condition now follows easily.

7. Parametrised elements of a free associative algebra

Consider now the free associative algebra $k\langle X\rangle$ over a field k. A parametrised element[4] of $k\langle X\rangle$ is an expression $[\![f]\!]_{C_f}$ where f is a k-linear combination of parametrised words over X and C_f is a defining condition such that $\mathrm{Var}(C_f)$ includes all the variables that occur as exponents in the words of f. Just as for parametrised words, we allow the possibility that C_f has parameter variables that do not appear in f. During discussions it is often convenient to use the phrase 'f with condition C_f' to denote $[\![f]\!]_{C_f}$.

For an assignment $\mathbf{a} \in C_f$ we define $f(\mathbf{a})$ to be the element of $k\langle X\rangle$ obtained by evaluating each word of f at $\mathbf{a}$. Just as for parametrised words, $[\![f]\!]_{C_f}$ denotes the set of elements $\{f(\mathbf{a}) \mid \mathbf{a} \in \mathbf{V}(C_f)\} \subseteq k\langle X\rangle$. If $S = \{[\![f_i]\!]_{C_i} \mid i \in I\}$ is a set of parametrised elements then it denotes the subset $\cup_{i\in I}\{f_i(\mathbf{a}) \mid \text{for all } \mathbf{a} \in \mathbf{V}(C_i)\}$ of $k\langle X\rangle$. An element $[\![f]\!]_{C_f}$ is fixed if f does not involve any parameter variables. For the sake of uniformity we will regard all elements of $k\langle X\rangle$ as presented in the form $[\![f]\!]_{C_f}$ where C_f is any condition with $\mathbf{V}(C_f) \neq \emptyset$, e.g. $C_f = (s > 0)$. For such elements we will regard f and $[\![f]\!]_{C_f}$ as being the same.

We follow the same convention as for words for a notation such as $[\![f, g]\!]_C$. We say that f, g are *separated* if $\mathrm{Var}(C_f) \cap \mathrm{Var}(C_g) = \emptyset$. As already observed, this can always be achieved by using fresh variables for g and C_g, say. Just as before, if $[\![f]\!]_{C_f}$, $[\![g]\!]_{C_g}$ are separated then we can take a single common defining condition for them, namely $C_f \wedge C_g$. Let $\mathbf{V}_f(C)$ denote $\mathbf{V}_T(C)$ for a condition C where T is the set of parameter variables that occur in f. Then we have $\mathbf{V}_f(C_f) = \mathbf{V}_f(C_f \wedge C_g)$ provided $[\![f]\!]_{C_f}$ and $[\![g]\!]_{C_g}$ are separated; so under this assumption we have $\{f(\mathbf{a}) \mid \mathbf{a} \in \mathbf{V}_f(C_f)\} = \{f(\mathbf{a}) \mid \mathbf{a} \in \mathbf{V}(C_f)\} = \{f(\mathbf{a}) \mid \mathbf{a} \in \mathbf{V}(C_f \wedge C_g)\}$. In examples it will be convenient to abuse notation slightly and denote $\mathbf{V}_f(C)$ by a first order formula that defines it. For example, if $f = zy^s - y^t z$ and $C = (s = u \wedge s > 0 \wedge t > 0 \wedge u > 0)$ then we write $\mathbf{V}_f(C) = (s > 0 \wedge t > 0)$ rather than the more cumbersome $\mathbf{V}_f(C) = \{\{s \leftarrow s_1, t \leftarrow t_1\} \mid s_1 > 0 \wedge t_1 > 0\}$.

Recall from §2, that in order to construct a Gröbner-Shirshov basis for a two-sided ideal of $k\langle X\rangle$ we assume as given an admissible order $<$ on X^*. We will assume that the order is such that given two parametrised words U, V we can construct a defining condition $C_{U,V}$ of equalities and inequalities such that $U(\mathbf{a}) < V(\mathbf{a})$ if and only if $\mathbf{a} \in \mathbf{V}(C_{U,V})$. It is of course always possible to construct such a condition $E_{U,V}$ with the property that $U(\mathbf{a}) = V(\mathbf{a})$ if and only if $\mathbf{a} \in \mathbf{V}(E_{U,V})$. The assumption is not so restrictive, e.g., the total degree then lexicographic order has the required property. (In all our examples we will use the total degree then lexicographic order with letters ordered as in the alphabet, so $x < y < z$.) For example consider $U = [\![xy^{u_1}x^{u_2}]\!]_{C_U}$ and $V = [\![xy^{v_1}x^{v_2}]\!]_{C_V}$ then $U(\mathbf{a}) < V(\mathbf{a})$ if and only if

1. $u_1(\mathbf{a}) + u_2(\mathbf{a}) < v_1(\mathbf{a}) + v_2(\mathbf{a})$, or
2. $u_1(\mathbf{a}) + u_2(\mathbf{a}) = v_1(\mathbf{a}) + v_2(\mathbf{a})$ and $u_1(\mathbf{a}) < v_1(\mathbf{a})$.

Thus the required condition is $C_U \wedge C_V \wedge (C_1 \vee C_2)$ where $C_1 = (u_1 + u_2 < v_1 + v_2)$ and $C_2 = (u_1 + u_2 = v_1 + v_2) \wedge (u_1 < v_1)$. A key problem we must address in building the Gröbner-Shirshov basis of a set of parametrised elements is how to find the leading word of an element.

Consider a parametrised element $[\![f]\!]_C$. For each non-empty subset E of the set of words that occur in f we can create a condition C_E with the property that for all $\mathbf{a} \in \mathbf{V}(C_E)$ and words U, V that occur in f we have $U(\mathbf{a}) = V(\mathbf{a})$, if U, V are both from E, while $U(\mathbf{a}) \neq V(\mathbf{a})$, if only one of U, V is from E. Choose a representative W_E of the subset E and create a condition L_{f,W_E} such that for all words V that occur in f but do not belong to E we have $W(\mathbf{a}) > V(\mathbf{a})$

[4] An alternative name is *parametrised non-commutative polynomial* but this is somewhat unwieldy.

if and only if $\mathbf{a} \in \mathbf{V}(L_{f,W})$. Set

$$f_E = \Big(\sum_{U \in E} \mathrm{coeff}(U, f) \Big) W_E + \sum_{V \notin E} \mathrm{coeff}(V, f) V,$$

where $\mathrm{coeff}(W, f)$ denotes the coefficient of a word W in f. Clearly $f(\mathbf{a}) = f_E(\mathbf{a})$, for all $\mathbf{a} \in \mathbf{V}(C_E)$. We define

$$\begin{aligned} \mathrm{LW}[\![f]\!]_C = \{ [\![W_E, f_E]\!]_{C \wedge C_E \wedge L_{f_E, W_E}} \mid & \text{ for all non-empty subsets } E \text{ of the} \\ & \text{words in } f \text{ s.t. } \mathrm{coeff}(W_E, f_E) \neq 0 \text{ and} \\ & \mathbf{V}(C \wedge C_E \wedge L_{f_E, W_E}) \neq \emptyset \}. \end{aligned}$$

It follows that for all $\mathbf{a} \in \mathbf{V}(C)$ we have $\mathrm{lw}(f(\mathbf{a})) = W_E(\mathbf{a})$ if and only if $\mathbf{a} \in \mathbf{V}(C \wedge C_E \wedge L_{f_E, W_E})$. Note that for such an $\mathbf{a}$ we have $f(\mathbf{a}) \neq 0$. It is possible to have $U(\mathbf{a}) = V(\mathbf{a})$ for distinct words of f_E so long as neither of them is from E. We extend the notation LW to sets of elements in the obvious way.

We consider now the process of reducing one element by another (see §2). For parametrised and separated elements $[\![f']\!]_{C_{f'}}$, $[\![g]\!]_{C_g}$ we try to remove the leading word identified by each member $[\![U, f]\!]_D$ of $\mathrm{LW}[\![f']\!]_{C_{f'}}$ by using each $[\![V, g]\!]_E$ from $\mathrm{LW}[\![g]\!]_{C_g}$. For a given $[\![U, f]\!]_D$ and $[\![V, g]\!]_E$ set $C = D \wedge E$. If $\mathrm{Inc}[\![U, V]\!]_C = \emptyset$ we discard $[\![V, g]\!]_E$ and move on since no reduction is possible. Assume now that $\mathrm{Inc}[\![U, V]\!]_C = \{ [\![A_i, B_i]\!]_{C_i} \mid 1 \leq i \leq m \}$ with $m \geq 1$ (recall that each element of $\mathrm{Inc}[\![U, V]\!]_C$ is a quadruple $[\![A, B, U, V]\!]_D$ but we have adopted the convention of dropping the last two elements as they are clear from the context). Fix i and set $h_i = f - \mathrm{coeff}(U, f)/\mathrm{coeff}(V, g)\, A_i g B_i$. It follows that $f'(\mathbf{a}) = f(\mathbf{a}) \to_{g(\mathbf{a})} h_i(\mathbf{a})$ for all $\mathbf{a} \in \mathbf{V}(C_i)$. We will summarise this by saying that $f \to_g h_i$ with condition C_i. The reduction has shown that the elements of $[\![h_i]\!]_{C_i}$ are also in the ideal and each has smaller leading word than the element of $[\![f]\!]_{C_i}$ from which it was obtained by the reduction. Suppose now that $f \to_g h_j$ with condition C_j for $j \neq i$. If $\mathbf{V}(C_j) \subseteq \mathbf{V}(C_i)$ then the second reduction is unnecessary since all fixed elements that can be reduced by it are already reduced by the first one (possibly to different fixed elements of course).

The preceding paragraph motivates and justifies the following notion. Assume the elements of $\mathrm{Inc}[\![U, V]\!]_C$ have been enumerated in some order as $[\![A_i, B_i]\!]_{C_i}$ for $1 \leq i \leq m$. Consider the partial order $\prec$ on $\mathrm{Inc}[\![U, V]\!]_C$ defined by

$$[\![A_i, B_i]\!]_{C_i} \prec [\![A_j, B_j]\!]_{C_j} \iff \mathbf{V}(C_i) \subset \mathbf{V}(C_j) \text{ or } (\mathbf{V}(C_i) = \mathbf{V}(C_j) \text{ and } i < j).$$

A few words are necessary to explain the meaning of $\mathbf{V}(C_i) \subset \mathbf{V}(C_j)$: the variables involved in each of the conditions $C_1, \ldots, C_m$ are assumed to be the same so that an assignment is of the form $\{s_1 \leftarrow v_1, \ldots, s_n \leftarrow v_n\}$ and the containment $\mathbf{V}(C_i) \subset \mathbf{V}(C_j)$ makes sense. Let M be the set of maximal elements under this order and find a subset T of M such that $\cup_{S \in T} \mathbf{V}(S) = \cup_{S \in M} \mathbf{V}(S)$. In carrying out reductions we need only consider the members of T. Note that if $\cup_{S \in T} \mathbf{V}_f(S) = \mathbf{V}(C_f)$ then all fixed words defined by f have been reduced. Otherwise those in $\mathbf{V}(C_f) - \cup_{S \in T} \mathbf{V}_f(S)$ either cannot be reduced or must be reduced using a different element of $\mathrm{LW}[\![g]\!]_{C_g}$. We call S a *cover* for $\mathrm{Inc}[\![U, V]\!]_C$. If $M = \{ [\![A'_i, B'_i]\!]_{C'_i} \mid 1 \leq i \leq r \}$ we can take $S = \{ [\![A'_i, B'_i]\!]_{C'_i} \mid 1 \leq i \leq s \}$ where s is minimal such that $\cup_{1 \leq i \leq s} \mathbf{V}(C'_i) = \cup_{1 \leq i \leq r} \mathbf{V}(C'_i)$, this does not necessarily contain the fewest sets and might include redundant ones. Note, finally, that this approach is simply a heuristic aimed at avoiding unnecessary extra reductions.

As an example set $F = [\![xy^s - xy]\!]_{s>0}$ and $G = [\![xy^t - x]\!]_{t>1}$. The discussion will be made clearer by setting $f = xy^s - xy$ and $C_f = (s > 0)$. As usual, we assume a total degree then

lexicographic order with $x < y$ so that

$$\mathrm{LW}\, F = \{\, [\![xy^s, xy^s - xy]\!]_{s>1} \,\},$$
$$\mathrm{LW}\, G = \{\, [\![xy^t, xy^t - x]\!]_{t>1} \,\}.$$

Note that $\mathrm{lw}(f)$ is undefined for $s = 1$ since then the corresponding element is 0. We aim to reduce F using G (more accurately elements of F by elements of G). Thus we need to solve $xy^s = Axy^tB$ with the condition $s > 1 \wedge t > 1$, this yields

$$\mathrm{Inc}[\![xy^s, xy^t]\!]_{s>1\wedge t>1} = \{\, [\![1, y^{s-t}]\!]_{s>t\wedge s>1\wedge t>1}, [\![1,1]\!]_{s=t\wedge s>1\wedge t>1} \,\}.$$

The second case cannot be included in the first one because we assume that all parameters are strictly positive. Now

$$\mathbf{V}_f(s > t \wedge s > 1 \wedge t > 1) = (s > 2),$$
$$\mathbf{V}_f(s = t \wedge s > 1 \wedge t > 1) = (s > 1),$$

Thus $\{\, [\![1,1]\!]_{s=t\wedge s>1\wedge t>1} \,\}$ is a cover for $\mathrm{Inc}[\![xy^s, xy^t]\!]_{s>1\wedge t>1}$, indeed the only one, and so we employ the reduction $xy^s - xy \to_{xy^t - x} -xy + x$ with the condition $s = t \wedge s > 1 \wedge t > 1$. Since $\mathbf{V}_f(s = t \wedge s > 1 \wedge t > 1) \subsetneq \mathbf{V}(C_f)$ we should check $\mathrm{LW}\, G$ for any other possible elements with which to reduce f with the condition $C_f \wedge \neg\exists t(s = t \wedge s > 1 \wedge t > 1)$, i.e., $s = 1$. Since $\mathrm{LW}\, G$ has no further elements no reduction is possible; the general algorithm would simply add any such irreducible parametrised element to the basis being constructed. Here we can see that there is only one element and it is equal to 0 so we can dispense with it.

To sum up, what this has shown is that every element from the set $\{\, xy^2 - xy,\ xy^3 - xy,\ xy^4 - xy, \ldots\}$ can be reduced to $-xy+x$ by using the corresponding element from the set $\{\, xy^2 - x,\ xy^3 - x,\ xy^4 - x, \ldots\}$. In fact all elements except $xy^2 - xy$ can be reduced to 0 since $xy^s - xy \to_{xy^t - x} 0$ with condition $(s > t \wedge s > 1 \wedge t > 1 \wedge t = s - 1)$. From the perspective of building a Gröbner-Shirshov basis this is not important as we must account for the exceptional case $xy^2 - xy$ which reduces only to $-xy + x$. Pursuing this we have $\mathrm{LW}[\![-xy + x]\!]_{\mathbf{tt}} = \{\, [\![xy, -xy + x]\!]_{\mathbf{tt}} \,\}$. But now $\mathrm{Inc}[\![xy, xy^t]\!]_{t>1} = \emptyset$ and so no reduction is possible. Thus in order to obtain a Gröbner-Shirshov basis for the ideal generated by the elements of F we must enlarge the basis to

$$\{[\![xy^s - xy]\!]_{s>0}, [\![\, xy^t - x]\!]_{t>1}, -xy + x \,\}.$$

We must also consider any intersection composition between F and G. Indeed in order to complete the construction of the Gröbner-Shirshov basis we must also consider all possible compositions between the remaining pairs. We will not pursue this here since a complete example will be given in §8.1.

8. Parametrised Gröbner-Shirshov bases

Given a set G of parametrised words, we construct a Gröbner-Shirshov basis S for the ideal generated by G by the process in Figure 1 (scope is indicated by indentation). The method is a direct analogue of the one for fixed elements outlined in §2 however we have to keep track of the defining condition of each word and, in the relevant parts, of the defining condition for the leading word. Note that even if G is finite the process does not necessarily terminate, though it will in favourable cases, but creates a Gröbner-Shirshov basis in the limit provided the method Reduce terminates (we discuss this in §8.2). In any implementation we would treat the returned result as a stream. The phrase 'Separate $[\![V, g]\!]_{E_g}$ from $[\![U, f]\!]_{E_f}$' simply means that we ensure that the parameter variables occurring in $[\![V, g]\!]_{E_g}$ are distinct from those in $[\![U, f]\!]_{E_f}$ by using fresh ones if necessary. Note that the method Reduce_Param of Figure 2 uses the parameter

GS-Basis(G)
  $S \leftarrow G$
  $Pairs \leftarrow \emptyset$
  for $[\![U, f]\!]_{E_f} \in \mathrm{LW}\, S$ **do**
    for $[\![V, g]\!]_{E_g} \in \mathrm{LW}\, S$ **do**
      Separate $[\![V, g]\!]_{E_g}$ from $[\![U, f]\!]_{E_f}$ ▷ Keep the same names.
      $Pairs \leftarrow Pairs \cup \{ ([\![U, f]\!]_{E_f}, [\![V, g]\!]_{E_g}) \}$
  while $Pairs \neq \emptyset$ **do**
    $Comps \leftarrow \emptyset$
    for $([\![U, f]\!]_{E_f}, [\![V, g]\!]_{E_g}) \in Pairs$ **do**
      for $[\![A, B]\!]_Q \in \mathrm{Inc}[\![U, V]\!]_{E_f \wedge E_g}$ **do** ▷ Inclusion compositions.
        $inc \leftarrow f - \mathrm{coeff}(U, f)/\mathrm{coeff}(V, g) AgB$
        if $inc \neq 0$ **then**
          $Comps \leftarrow Comps \cup \{ [\![inc]\!]_Q \}$
      for $[\![A, B]\!]_Q \in \mathrm{Int}[\![U, V]\!]_{E_f \wedge E_g}$ **do** ▷ Intersection compositions.
        if $A \neq 1$ **and** $B \neq 1$ **then** ▷ Otherwise essentially the same as an inclusion.
          $int \leftarrow Af/\mathrm{coeff}(U, f) - gB/\mathrm{coeff}(V, g)$
          if $int \neq 0$ **then**
            $Comps \leftarrow Comps \cup \{ [\![int]\!]_Q \}$
    for $[\![h]\!]_{C_h} \in Comps$ **do**
      $Redns \leftarrow \textsc{Reduce}([\![h]\!]_{C_h}, S)$
    for $[\![U, f]\!]_{E_f} \in \mathrm{LW}\, S$ **do**
      for $[\![V, g]\!]_{E_g} \in \mathrm{LW}\, Redns$ **do** ▷ Add all new pairs to $Pairs$.
        Separate $[\![V, g]\!]_{E_g}$ from $[\![U, f]\!]_{E_f}$ ▷ Keep the same names.
        $Pairs \leftarrow Pairs \cup \{ ([\![U, f]\!]_{E_f}, [\![V, g]\!]_{E_g}), ([\![V, g]\!]_{E_g}, [\![U, f]\!]_{E_f}) \}$
    for $F \in Redns$ **do** $S \leftarrow S \cup \{ F \}$ ▷ Add (non-zero) reduced elements to basis.
  return S

Figure 1: Creating a parametrised Gröbner-Shirshov basis.

variable R to collect the set of all possible non-zero reductions of the parameter element $[\![f]\!]_{C_f}$; if all reductions are 0 then the empty set is returned. In this method we also use **ff** to stand for any condition that is not satisfied by any assignment, e.g., $(0 = 1)$. The symbol ▷ is used to indicate the start of a comment.

A subset S of $k\langle X\rangle$ is a Gröbner-Shirshov basis for the ideal it generates if and only if every composition of all pairs of elements form S reduces to 0 with respect to S. We can adapt this to the parametrised situation to produce the process in Figure 3.

8.1 An example

Suppose $F_1 = [\![f_1]\!]_{s>0}$ and $F_2 = [\![f_1]\!]_{t>0}$ where

$$f_1 = xy^s - z,$$
$$f_2 = y^t x - z,$$

Consider the ideal generated by $G = \{ F_1, F_2 \}$, i.e., $(xy^s - z, y^t x - z; s, t > 0)$. As usual in this paper, we order words by length and then lexicographically with $x < y < z$. We proceed to illustrate the method for finding a Gröbner-Shirshov basis (with some obvious shortcuts). One difference between this example and the methods shown in Figures 1, 2 is that whenever

```
REDUCE(⟦f⟧_{C_f}, S)
  if V(C_f) = ∅ then return ∅
  else if f is fixed then
    return REDUCE_FIXED(f, S)
  else
    R ← ∅
    REDUCE_PARAM(⟦f⟧_{C_f}, S, R)
    return R

REDUCE_FIXED(f, S)
  if f = 0 then return ∅
  else
    red ← TRUE
    h ← f
    while red do
      red ← FALSE
      U ← lw(h)
      for ⟦V, g⟧_{E_g} ∈ LW S do    ▷ Look for a way to reduce f.
        if Inc⟦U, V⟧_{E_g} ≠ ∅ then red ← TRUE; exit for loop    ▷ Found one.
      if red then    ▷ Carry out a reduction step when possible.
        pick any ⟦A, B⟧_Q from Inc⟦U, V⟧_{E_g}
        pick any a from V(Q)
        h ← h − coeff(U, h)/coeff(V, g(a))A(a)g(a)B(a)
    if h ≠ 0 then return { h }
    else return ∅

REDUCE_PARAM(⟦f⟧_{C_f}, S, R)
  if f = 0 or V(C_f) = ∅ then return R
  else
    for ⟦U, h⟧_{D_h} ∈ LW⟦f⟧_{C_f} do
      Done ← ff
      for ⟦V, g⟧_{E_g} ∈ LW S do
        if V_h(Done) ≠ V(D_h) then    ▷ Check if all elements in ⟦h⟧_{D_h} have been reduced.
          if Inc⟦U, V⟧_{D_h ∧ E_g} ≠ ∅ then
            choose a cover T for Inc⟦U, V⟧_{D_h ∧ E_g}
            for ⟦A, B⟧_Q ∈ T do
              Done ← Done ∨ Q
              inc ← h − coeff(U, h)/coeff(V, g)AgB
              REDUCE_PARAM(⟦inc⟧_Q, S, R)
      if V(D_h ∧ ¬(Done|_h)) ≠ ∅ then    ▷ Put into R all irreducible elements from ⟦h⟧_{D_h}.
        R ← R ∪ { ⟦h⟧_{D_h ∧ ¬(Done|_h)} }
    return R
```

Figure 2: Reducing a parametrised element with respect to a set.

```
GS-Basis-Check(S)
  Pairs ← ∅
  for ⟦U, f⟧_{E_f} ∈ LW S do
    for ⟦V, g⟧_{E_g} ∈ LW S do
      Separate ⟦V, g⟧_{E_g} from ⟦U, f⟧_{E_f}     ▷ Keep the same names.
      Pairs ← Pairs ∪ { (⟦U, f⟧_{E_f}, ⟦V, g⟧_{E_g}) }
  while Pairs ≠ ∅ do
    Comps ← ∅
    for (⟦U, f⟧_{E_f}, ⟦V, g⟧_{E_g}) ∈ Pairs do
      remove (⟦U, f⟧_{E_f}, ⟦V, g⟧_{E_g}) from Pairs
      for ⟦A, B⟧_Q ∈ Inc⟦U, V⟧_{E_f ∧ E_g} do
        inc ← f − coeff(U, f)/ coeff(V, g) AgB
        if inc ≠ 0 then Comps ← Comps ∪ { ⟦inc⟧_Q }
      for ⟦A, B⟧_Q ∈ Int⟦U, V⟧_{E_f ∧ E_g} do
        if A ≠ 1 or B ≠ 1 then
          int ← Af/ coeff(U, f) − gB/ coeff(V, g)
          if int ≠ 0 then Comps ← Comps ∪ { ⟦int⟧_Q }
    for ⟦U, f⟧_{E_f} ∈ Comps do
      if Reduce(⟦f⟧_{E_f}, S) ≠ ∅ then return False
  return True
```

Figure 3: Checking a parametrised set to see if it is a Gröbner-Shirshov basis.

a non-zero element cannot be further reduced we add it to the basis straight away. This is an optimisation that would be applied to any implementation of the methods, it is not shown in the figures for the sake of simplicity.

We start by setting $S \leftarrow G$. Thus

$$\mathrm{LW}\, S = \{\, [\![xy^s, xy^s - z]\!]_{s>0}, [\![y^t x, y^t x - z]\!]_{t>0} \,\},$$

and

$$\begin{aligned} \mathit{Pairs} = \{\, &([\![xy^s, xy^s - z]\!]_{s>0}, [\![xy^t, xy^t - z]\!]_{t>0}),\ ([\![xy^s, xy^s - z]\!]_{s>0}, [\![y^t x, y^t x - z]\!]_{t>0}) \\ &([\![y^t x, y^t x - z]\!]_{t>0}, [\![xy^s, xy^s - z]\!]_{s>0}),\ ([\![y^s x, y^s x - z]\!]_{s>0}, [\![y^t x, y^t x - z]\!]_{t>0}) \,\}. \end{aligned}$$

Considering the first pair, an intersection $Axy^s = xy^t B$ with $A \neq 1$ is not possible so any intersection is the same as an inclusion (similarly for $xy^s A = Bxy^t$). For inclusion, let $U = xy^s$, $V = xy^t$ then we have two solutions (i) $A = 1$, $B = 1$ with condition $s = t$ and (ii) $A = 1$, $B = y^{s-t}$ with the condition $s > t$. For the first case the composition is 0 so it is discarded. For the second case the result of composing $xy^s - z$ and $xy^t - z$ is $zy^{s-t} - z$ with condition $s > t$. This new element cannot be reduced by S, so we add it to the basis but we rename $s - t$ as u and so add $f_3 = zy^u - z$ for $u > 0$ to the basis. Hence we now have

$$S = \{\, [\![xy^s - z]\!]_{s>0}, [\![y^t x - z]\!]_{t>0}, [\![zy^u - z]\!]_{u>0} \,\}$$

At this point the set *Pairs* is updated by removing the considered pair and including all pairs formed with f_3 as one entry and one of f_1, f_2, f_3 as the other entry but to save space we will not show this.

Applying the same reasoning to the pairs formed from f_2 in both entries, we see that $f_4 = y^v z - z$, for $v > 0$ is also in the basis. Thus the basis so far is

$$S = \{\, [\![xy^s - z]\!]_{s>0}, [\![y^t x - z]\!]_{t>0}, [\![zy^u - z]\!]_{u>0}, [\![y^v z - z]\!]_{v>0} \,\}$$

We now consider the possible compositions between $f_1 = xy^s - z$, $f_2 = y^t x - z$. Inclusion is not possible, so we only have to deal with the intersection composition between xy^s and $y^t x$. Assume first that that we want to solve $Axy^s = y^t xB$. The intersection is possible only with $A = y^t$ and $B = y^s$ where $s, t > 0$. The result of the composition is $f = Af_1 - f_2 B = zy^s - y^t z$. Now

$$\mathrm{LW}[\![f]\!]_{s>0\wedge t>0} = \{\, [\![zy^s, f]\!]_{s\geq t\wedge s>0\wedge t>0}, [\![y^t z, f]\!]_{t>s\wedge s>0\wedge t>0}\}$$

We can reduce $[\![f]\!]_{s\geq t\wedge s>0\wedge t>0}$ by $g_1 = zy^u - z$ to obtain

$$f \to_{g_1} = \begin{cases} z - y^t z, & \text{with condition } Q_1 = (s = u \wedge s \geq t \wedge s > 0 \wedge t > 0 \wedge u > 0); \\ zy^{s-u} - y^t z, & \text{with condition } Q_2 = (s > u \wedge s \geq t \wedge s > 0 \wedge t > 0 \wedge u > 0). \end{cases}$$

Clearly $\mathbf{V}_f(Q_1) = (s \geq t \wedge s > 0 \wedge t > 0)$ and $\mathbf{V}_f(Q_2) = (s \geq t \wedge s > 1 \wedge t > 0)$ thus $\mathbf{V}_f(Q_2) \subset \mathbf{V}_f(Q_1)$. Therefore, we choose to reduce f to $f_1 = -y^t z + z$ with $t > 0$. Now, f_1 can be reduced by $g_2 = y^u z - z$ to obtain:

$$f_1 \to_{g_2} = \begin{cases} 0, & \text{with condition } Q_1 = (t = u \wedge t > 0 \wedge u > 0); \\ -y^{t-u} z + z, & \text{with condition } Q_2 = (t > u \wedge t > 0 \wedge u > 0). \end{cases}$$

Here, we have $\mathbf{V}_{f_1}(Q_1) = (s > 0)$ and $\mathbf{V}_{f_1}(Q_2) = (s > 1)$ thus $\mathbf{V}_{f_1}(Q_2) \subset \mathbf{V}_{f_1}(Q_1)$, so we reduce f_1 to 0, i.e., the process works in the same way as intuition.

Now we consider reducing the second element of $\mathrm{LW}[\![f]\!]_{s>0\wedge t>0}$, i.e., $[\![-y^t z + zy^s]\!]_{t>s\wedge s>0\wedge t>0}$. This reduces to $[\![zy^s - z]\!]_{s>0}$ via $[\![y^v z - z]\!]_{v>0}$ and then to 0 via $[\![zy^u - z]\!]_{u>0}$.

To complete the possible inclusions between f_1 and f_2 we must also solve the equation $xy^s A = By^t x$. First assume that $s = t$, then we have the solutions $A = B = x$ and $A = y^a x$, $B = xy^a$ where $0 < a < s - 1$. Taking $A = B = x$ the result of the intersection composition is $-zx + xz$. As this cannot be further reduced, we add it to the basis. Now for $A = y^a x$, $B = xy^a$ the composition is $-zy^a x + xy^a z$ and this reduces to 0 via $[\![zy^u - z]\!]_{u>0}$, $[\![y^v z - z]\!]_{v>0}$ and $-zx + xz$.

For $s \neq t$ we have the following possibilities: in general we set $A = y^a x$, $B = xy^b$ with $0 < a < t - 1$, $0 < b < s - 1$ and $s + a = b + t$. For the case $s > t$ we also have the solution $A = x$, $B = xy^{s-t}$ while for $t > s$ we have $A = y^{t-s} x$, $B = x$. For $s > t$ and $A = x$, $B = xy^{s-t}$ we obtain the composition $f = xy^{s-t} z - zx$. We can rename f to $xy^s z - zx$, with the condition $s > 0$. Then we reduce f by $g_1 = y^t z - z$ to obtain

$$f \to_{g_1} = \begin{cases} -zx + xz, & \text{with condition } Q_1 = (s = t \wedge t > 0 \wedge s > 0); \\ xy^{s-t} z - zx, & \text{with condition } Q_2 = (s > t \wedge t > 0 \wedge s > 0). \end{cases}$$

We have $\mathbf{V}_f(Q_1) = (s > 0)$ and $\mathbf{V}_f(Q_2) = (s > 1)$ thus $\mathbf{V}_f(Q_2) \subset \mathbf{V}_f(Q_1)$, so we reduce f to $f_1 = -zx + xz$. We now call the procedure REDUCE_FIXED to reduce f_1 to 0 as it is already in the basis. A similar analysis applies when $t > s$. In the general case $A = y^a x$, $B = xy^b$ the composition is $[\![xy^b z - zy^a x]\!]_{a>0\wedge b>0}$ and this reduces to 0 via $[\![zy^u - z]\!]_{u>0}$, $[\![y^v z - z]\!]_{v>0}$ and $-zx + xz$. Therefore, *Pairs* is updated and the basis so far is given by

$$S = \{\, [\![xy^s - z]\!]_{s>0}, [\![y^t x - z]\!]_{t>0}, [\![zy^u - z]\!]_{u>0}, [\![y^v z - z]\!]_{v>0}, -zx + xz \,\}.$$

It is worth noting here that the reduction of $[\![xy^b z - zy^a x]\!]_{a>0\wedge b>0}$ falls into two cases: one where $a < b$ so that the leading word is $xy^b z$ and the other where $a \geq b$ giving $zy^a x$ as the leading word. Furthermore if, in the case of $b > a$ we reduce first by $[\![xy^s - z]\!]_{s>0}$ followed by $[\![zy^u - z]\!]_{u>0}$ then we obtain $z^2 - zx$ which cannot be reduced and would thus be put in the basis (see below). Similarly if, in the case $a \geq b$, we reduce first by $[\![y^t x, y^t x - z]\!]_{t>0}$ followed by $[\![xy^s - z]\!]_{s>0}$ then we obtain $xz - z^2$ which reduces to $zx - z^2$ via $-zx + xz$.

Consider now the elements $f_1 = xy^s - z$ and $f_3 = zy^u - z$. In this case, neither intersection nor inclusion is possible so we move on and look at the first and the fourth elements: $f_1 = xy^s - z$ and $f_4 = y^v z - z$. Here inclusion is not possible so we consider intersection. The equation $Axy^s = y^v zB$ has no solutions, so we move on to the equation $xy^s A = By^v z$. If $s = v$ then, as before, this splits into the special case and $A = z$, $B = x$ and the general one $A = y^a z$, $B = xy^a$ with $0 < a < s - 1$. For the case $A = z$, $B = x$ the composition is $f = -z^2 + xz$ which cannot be further reduced, so it is added to the basis. For the case $A = y^a z$, $B = xy^a$ the composition is $-zy^a z + xy^a z$ and this reduces to $-z^2 + xz$ via $[\![y^v z - z]\!]_{v>0}$ applied twice.

Suppose now that $s \neq v$. First, let $s > v$; we have the special solution $A = z$, $B = xy^{s-v}$ to obtain $f = xy^{s-v}z - z^2$, which we rename $f = xy^s z - z^2$, with condition $s > 0$. We can reduce f by $g_1 = xy^t - z$ to obtain:

$$f \to_{g_1} = \begin{cases} 0, & \text{with condition } Q_1 = (s = t \wedge t > 0 \wedge s > 0); \\ zy^{s-t}z - z^2, & \text{with condition } Q_2 = (s > t \wedge t > 0 \wedge s > 0). \end{cases}$$

Again, we have $\mathbf{V}_f(Q_2) \subset \mathbf{V}_f(Q_1)$, so we proceed to reduce f to 0. A similar analysis applies for the special solution when $s < v$ and the solution $A = y^{v-s}z$, $B = x$. We also have the general solution $A = y^a z$, $B = xy^b$ with $s + a = v + b$, $0 < a < v - 1$ and $0 < b < s - 1$. The composition is $[\![xy^b z - zy^a z]\!]_{a>0 \wedge b>0}$ which reduces to 0 via $[\![y^v z - z]\!]_{v>0}$ and $-z^2 + xz$. Therefore, *Pairs* is updated and the basis so far is given by

$$S = \{[\![xy^s - z]\!]_{s>0}, [\![y^t x - z]\!]_{t>0}, [\![zy^u - z]\!]_{u>0}, [\![y^v z - z]\!]_{v>0}, -zx + xz, -z^2 + xz\}.$$

In fact all other compositions reduce to 0 and so this is a Gröbner-Shirshov basis for the ideal $(xy^s - z, y^t x - z; s, t > 0)$ with words ordered by length and then lexicographically with $x < y < z$.

8.2 The method REDUCE

In the standard situation where we are reducing a fixed element of $k\langle X\rangle$ reduction is guaranteed to terminate since each step produces a fixed word by replacing the leading word with one or more smaller fixed words and the order on words is a well order. However in the parametrised situation we do not have a guarantee of termination. As an example, consider $[\![xy^s - x]\!]_{s>1}$ and $[\![xy - x]\!]_{\mathbf{tt}}$. We have the following sequence of reductions:

$$\begin{aligned} xy^s - x &\to_{xy-x} xy^{s-1} - x \quad \text{with condition } s > 1 \\ &\to_{xy-x} xy^{s-2} - x \quad \text{with condition } s > 2 \\ &\vdots \end{aligned}$$

Of course once we give s a value the sequence reaches $xy - x$ after $s - 1$ steps and goes to 0 in one more step. Moreover it takes exactly this many steps, i.e., there is no upper bound independent of s. In this simple example it is clear that the sequence will not terminate (with s an unassigned variable) because $[\![xy^{s-1} - x]\!]_{s>1}$ is just $[\![xy^s - x]\!]_{s>2}$ and so we are in a cycle with the lower bound on s increasing each time. Naturally in this case we can detect the cycle and simply add $[\![xy^s - x]\!]_{s>1}$ to the basis. However non-termination need not always be due to such cycles. For example, consider $f = [\![x^{s_1}y^{s_2} - x^{s_2}y^{s_2}z^{s_2}]\!]_{s_1>0 \wedge s_2>0 \wedge s_1>2s_2}$ and $g = [\![x^{t_1}y^{t_2} - x^{t_2}y^{t_2}z^{t_2}x^{t_2}y^{t_2}]\!]_{t_1>0 \wedge t_2>0 \wedge t_1>4t_2}$. One possible reduction is to set $t_1 = s_1$ and $t_2 = s_2$. For the inclusion composition we have $x^{s_1}y^{s_2} = 1\, x^{s_1}y^{s_2}\, 1$, so we obtain

$$f' = [\![x^{s_2}y^{s_2}z^{s_2}x^{s_2}y^{s_2} - x^{s_2}y^{s_2}z^{s_2}]\!]_{s_2>0}$$

Again we can reduce by g. Setting $t_1 \leq s_2$ and $t_2 \leq s_2$ we obtain $x^{s_2}y^{s_2}z^{s_2}x^{s_2}y^{s_2} = Ax^{t_1}y^{t_2}B$ with $A = x^{s_2-t_1}$ and $B = y^{s_2-t_2}z^{s_2}x^{s_2}y^{s_2}$. Applying the reduction we obtain

$$f'' = [\![x^{s_2+t_2-t_1}y^{t_2}z^{t_2}x^{t_2}y^{s_2}z^{s_2}x^{s_2}y^{s_2} - x^{s_2}y^{s_2}z^{s_2}]\!]_{s_2>0\wedge t_1>0\wedge t_2>0\wedge t_1\leq s_2\wedge t_2\leq s_2\wedge t_1>4t_2}.$$

This process can be carried on indefinitely with the leading word of the new element growing each time.

8.3 Non-existence of an algorithm for the method REDUCE

Let us assume that we have an algorithm for deciding if $\mathrm{Inc}[\![U, V]\!]_C$ is empty likewise for $\mathrm{Int}[\![U, V]\!]_C$ so that Lemma 4.1 is not a barrier to producing an algorithm for method REDUCE. Nevertheless, the preceding observations suggest that in general we cannot hope to detect non-termination, this is indeed the case. We will work with Turing machines that, by default, have a two way infinite tape and quintuples as instructions. We assume that the tape alphabet consists of $0, 1, \ldots, m-1$ where 0 denotes the blank symbol. The states are $0, 1, \ldots, n-1$ where 0 is a halting state. When denoting configurations we underline the state. For a machine T and configurations C, C' we use $C \Rightarrow_T C'$ (respectively $C \Rightarrow_T^* C'$) to indicate that T transforms C to C' in one move (respectively zero or more moves). Let $C = \ldots b_2b_1b_0\underline{q}ac_0c_1c_2\ldots$ be a configuration (the state is underlined) and set $\alpha = \sum_{i=0}^{\infty} b_im^i$, $\beta = \sum_{i=0}^{\infty} c_im^i$; both sums are finite since all but finitely many symbols are blank. We encode the configuration as (α, q, a, β). The move function of T is simply described: if T has no quintuple starting with (q, a) the machine halts, i.e., the configuration is terminal. Otherwise set $\alpha = \alpha'm + b$, $\beta = \beta'm + c$ where $0 \leq a, b < m$ then

$$(\alpha, q, a, \beta) \Rightarrow_T \begin{cases} (\alpha m + a', q', c, \beta'), & \text{if } (q, a, q', a', R) \text{ is a quintuple of } T; \\ (\alpha', q', b, \beta m + a), & \text{if } (q, a, q', a', L) \text{ is a quintuple of } T; \end{cases}$$

Clearly the encoded version mimics the computation of the given machine faithfully. Moreover, every quadruple (α, q, a, β) with $\alpha, \beta \in \mathbb{N}$, $0 \leq q < n$ and $0 \leq a < m$ corresponds to a configuration of T. Consider now the free algebra $\mathbb{Q}\langle w, x, y, z, u, v\rangle$. We could encode the configuration (α, q, a, β) as $wx^\alpha y^q z^a u^\beta v$ but as we do not allow parameter variables to be 0 we use

$$\phi(C) = wx^{1+\alpha}y^{1+q}z^{1+a}u^{1+\beta}v$$

instead. The reason for the presence of w, v is that for a pair of such words there is a composition of inclusion or intersection if and only if they are equal, this is critical to the proof of Lemma 8.1 below. The nature of the words we use also ensures the assumption at the start of this section regarding $\mathrm{Inc}[\![U, V]\!]_C$ and $\mathrm{Int}[\![U, V]\!]_C$.

Clearly there is a first order logic formula $M(s, q, a, t, s', q', a', t')$ with the displayed free variables such that the formula is true if and only if $C = (s, q, a, t)$, $C' = (s', q', a', t')$ are configurations and $C \Rightarrow_T C'$. We will denote the formula by $M(C, C')$ for brevity. It will be convenient to work only with certain configurations. We assume that we have identified a set of configurations that we will call *standard* with the property that if $C \Rightarrow_T C'$ then C is standard if and only if C' is standard.

We consider the ideal

$$I = (\{\phi(C) - \phi(C') \mid \ C \text{ is standard and } C \Rightarrow C'\})$$

of $\mathbb{Q}\langle w, x, y, z, u, v\rangle$. As usual, we use the total degree then lexicographic order on $\{ w, x, y, z, u, v \}^*$. Two configurations C_1, C_2 are said to *conflow* if there is a configuration C such that $C_1 \Rightarrow_T^* C$ and $C_2 \Rightarrow_T^* C$.

Lemma 8.1 *$S = \{\phi(C) - \phi(C') \mid C \neq C'$ are standard and conflow$\}$ is a Gröbner-Shirshov basis for I.*

PROOF. Cleary $I \subseteq (S)$. For the reverse inclusion, assume that C_1, C_2 are distinct and standard and $C_1 \Rightarrow_T^* C$ in s_1 steps while $C_2 \Rightarrow_T^* C$ in s_2 steps with $s_1 + s_2$ minimal. We use induction on $s_1 + s_2$ to show that $\phi(C_1) - \phi(C_2) \in I$. Since $C_1 \neq C_2$ we have $s_1 + s_2 > 0$. If $s_1 + s_2 = 1$ then either $C_1 \Rightarrow_T C_2$ or $C_2 \Rightarrow_T C_1$ and so either $\phi(C_1) - \phi(C_2)$ or $\phi(C_2) - \phi(C_1)$ is in the basis of I. Otherwise we may assume without loss of generality that $s_1 > 0$ and so $C_1 \Rightarrow_T C'$; hence C' is standard and $C' \Rightarrow_T^* C$ in $s_1 - 1$ steps. It follows from the induction hypothesis that $\phi(C') - \phi(C_2) \in I$. By the definition of I, we have $\phi(C_1) - \phi(C') \in I$ and so $\phi(C_1) - \phi(C_2) \in I$ as claimed. Thus $(S) \subseteq I$ and so $I = (S)$.

It remains to show that S is a Gröbner-Shirshov basis, we do this by showing that all compositions of members of S reduce to 0 w.r.t. S. Consider $\phi(C_1) - \phi(C_1'), \phi(C_2) - \phi(C_2') \in S$. As observed above two words $\phi(C)$, $\phi(C')$ do not have a composition of inclusion or intersection unless they are equal. It follows that there is a composition (only one type need be considered) between $\phi(C_1) - \phi(C_1')$ and $\phi(C_2) - \phi(C_2')$ if and only if $\mathrm{lw}(\phi(C_1) - \phi(C_1')) = \mathrm{lw}(\phi(C_2) - \phi(C_2'))$. Suppose that $\phi(C_1) = \phi(C_2)$ are the leading words, then the composition is $\phi(C_2') - \phi(C_1')$. Now C_1 and C_1' conflow and similarly for C_2 and C_2'. Since $C_1 = C_2$ it follows that C_1' and C_2' conflow and so $\phi(C_2') - \phi(C_1') \in S$. The other cases are similar. □

Lemma 8.2 *For all distinct configurations C_1, C_2 we have $\phi(C_1) - \phi(C_2) \in I$ if and only if C_1, C_2 conflow and are both standard.*

PROOF. Suppose that $\phi(C_1) - \phi(C_2) \in I$. Let S be the Gröbner-Shirshov basis for I defined in Lemma 8.1 so that $\phi(C_1) - \phi(C_2) \to_S 0$ in s steps (necessarily $s > 0$). We use induction on s to show that C_1, C_2 conflow and are both standard. If $s = 1$ the claim is immediate by definition of S. Assume w.l.o.g. that $\mathrm{lw}(\phi(C_1) - \phi(C_2)) = \phi(C_1)$ so that $\phi(C_1) - \phi(C_1') \in S$ for some C_1'. It follows that C_1 is standard and $\phi(C_1) - \phi(C_2) \to_{\phi(C_1) - \phi(C_1')} \phi(C_1') - \phi(C_2) \to_S 0$. By induction C_1' and C_2 are standard and conflow. But C_1 and C_1' conflow since $\phi(C_1) - \phi(C_1') \in S$ and so C_1 and C_2 conflow. For the converse, we have $\phi(C_1) - \phi(C_2) \in S \subseteq I$ by Lemma 8.1. □

A *final* set of standard configurations of T is a set F such that:

1. If $C \in F$ then C is standard and either C is terminal or $C \Rightarrow_T C$.
2. For all standard configurations C' there is a configuration $C \in F$ such that $C' \Rightarrow_T^* C$.

(There is no guarantee that a final set exists.) For $C \in F$ set

$$[C]_T = \{C' \mid C' \Rightarrow_T^* C \text{ and } C' \notin F\}.$$

Lemma 8.3 *Suppose T has a set F of final configurations and let I be the ideal defined above. Assume that the admissible order on $\{w, x, y, z, u, v\}^*$ is such that whenever $C' \Rightarrow_T^* C$ with $C \in F$ we have $\phi(C') \geq \phi(C)$. Then*

$$S = \bigcup_{C \in F} \{\phi(C') - \phi(C) \mid C' \in [C]_T\}$$

is a Gröbner-Shirshov basis for I.

PROOF. First we note that $S \subseteq I$ by Lemma 8.2. By Lemma 8.1 we need only show that $\phi(C_1) - \phi(C_2) \to_S 0$ where $C_1 \neq C_2$ are standard and conflow. We have $C_1 \Rightarrow_T^* C$ and $C_2 \Rightarrow_T^* C$ for some $C \in F$. Thus $\phi(C_1) - \phi(C), \phi(C_2) - \phi(C) \in S$ and the leading words are $\phi(C_1)$, $\phi(C_2)$ respectively. We may assume without loss of generality that $\mathrm{lw}(\phi(C_1) - \phi(C_2)) = \phi(C_1)$. Now

$$\phi(C_1) - \phi(C_2) \to_{\phi(C_1)-\phi(C)} \phi(C) - \phi(C_2) \to_{\phi(C_2)-\phi(C)} 0.$$

Thus S is a Gröbner-Shirshov basis for I. □

Now let T' be any Turing machine with a one way infinite tape (to the right) whose halting problem on the empty tape is undecidable. We employ the following standard construction to obtain a two way infinite tape machine T whose overall behaviour is to treat its input word w as a counter (in unary) and simulate T' with an empty tape until the counter reaches 0 or the simulation halts. If the first case happens we clear the tape and keep moving right forever in state 1. If the latter happens we clear the tape and enter state 0 (a special halting state).

We give the construction of T in more detail for the sake of readers who are not familiar with Turing machines. In the description we will use some non-numeric tape symbols since these are more meaningful, they should be seen as names for some appropriate number in the range $1, \ldots, m-1$ where m is the total number tape symbols (recall that 0 is reserved for the blank symbol). Similar remarks apply to states. T has an initial start state q_I and is always started with the configuration $q_I w$ where w is a sequence of 1's. We will simulate T' in a portion of the tape of T delimited by the special symbols \$ and]. We ensure that within this portion only a reserved set Σ of symbols is used. This set includes 0 (the blank symbol) but is otherwise disjoint from all other symbols used. The behaviour of T is as follows.

1. If the square to the left of the one scanned by q_I is blank (i.e., 0) then place a special end marker symbol [and move right in a state q_b, skipping 1, till the first blank is seen. If any other symbol is seen during this preparatory phase then enter the state q_H and halt.

2. Overwrite the found blank symbol with a new symbol \$, enter a state $q_{\$}$. If the next symbol is blank move right and enter state $q_{\$\$}$. If the next symbol is blank then replace it with], move left and enter a new state q_S; this initialises the step by step simulation of T' on its empty tape. Otherwise enter the state q_H and halt.

3. Simulate T' on the part of the tape between \$ and] one step at a time.

   (a) If] is seen during the simulation first check that the next square to the right is blank. If so, replace] with a blank (i.e., 0) and print] one square to the right (i.e., make space available to continue) then resume the simulation. If the symbol to the right of] is not blank then enter the state q_H and halt.

   (b) After each simulation step, search for the first 1 to the left of \$ skipping over any 0 symbols seen. If 1 is found then replace it with 0 and resume the simulation of T'. If there is no occurrence of 1 and [is not found the machine moves to the left forever staying in a state q_L different from 0 and 1. Otherwise delete [and enter the state q_d which deletes any symbol from $\Sigma \cup \{1, \$\}$ and moves right seeking]. If] is found then delete it and change to a state 1 which keeps moving right so long as a blank is seen. If any other symbol is found then enter state q_H and halt.

4. If the simulation of T' halts before the counter reaches 0 (i.e., the relevant portion of the tape is all blanks) then seek [. If it is not found then move to the left for ever (the state is irrelevant but is different from 0 and 1). Otherwise delete [and all symbols in $\Sigma \cup \{1, \$\}$ from here up to] then enter the halting state 0. If any other symbol is seen then enter state q_H and halt.

It is clear from the design of T that for a given configuration C we can decide if $C \to \underline{0}0$ or $C \to \underline{1}0$. We take the set of all such configurations to be the standard ones, in particular we can decide if C is standard. There is thus a total computable function γ from configurations to $\mathbb{N}$ such that

$$\gamma(C) = \begin{cases} 0, & \text{if } C \Rightarrow^* \underline{0}0; \\ 1, & \text{if } C \Rightarrow^* \underline{1}0; \\ 2, & \text{otherwise;} \end{cases}$$

We denote the halting configuration $\underline{0}0$, encoded as $(0,0,0,0)$, by H and the non-terminating configuration $\underline{1}0$, encoded as $(0,1,0,0)$, by L. We can test if $C = (\alpha, q, a, \beta)$ is a configuration by the first order formula

$$\mathrm{con}(C) = \alpha \geq 0 \wedge (q \geq 0 \wedge q < n) \wedge (a \geq 0 \wedge a < m) \wedge \beta \geq 0.$$

Set

$$S = \{\, [\![\phi(C) - \phi(H)]\!]_{\mathrm{con}(C) \wedge \gamma(C)=0}, [\![\phi(C) - \phi(L)]\!]_{\mathrm{con}(C) \wedge \gamma(C)=1} \,\},$$
$$J = (S).$$

The set S can be expressed without the use of γ but at the expense of using infinitely many parametrised words as follows. We can express the condition that $C = (\alpha, q, a, \beta)$ is a configuration and $C \Rightarrow_T^* H$ in s steps by the first order formula

$$\mathcal{H}_s(C) = \mathrm{con}(C) \wedge \exists C_1, \ldots, C_s \left(C = C_1 \wedge \bigwedge_{0 \leq i \leq s-1} M(C_i, C_{i+1}) \wedge C_s = H \right).$$

Of course it is possible that $C \Rightarrow_T^* H$ in fewer or more than s steps as well as exactly s steps. By replacing H with L in the formula above we obtain a formula $\mathcal{L}_s$ for the condition that C is a configuration and $C \Rightarrow_T^* L$ in s steps. Clearly

$$S = \{ [\![\phi(C) - \phi(H)]\!]_{\mathcal{H}_s(C)}, [\![\phi(C) - \phi(L)]\!]_{\mathcal{L}_s(C)} \mid s \geq 0 \}.$$

Lemma 8.4 *$I = J$ and S is a recursive Gröbner-Shirsov basis for I.*

Proof. Recall that we order the words of $\{\, w, x, y, z, u, v \,\}^*$ first by size and then lexicographically (the order of the letters can be arbitrary). If $C \Rightarrow_T^* H$ then necessarily $\phi(C) \geq \phi(H)$ since the entries of C are at least 0 and the entries of H are all equal to 0 (of course in the exponents of the encoding words we add 1 to everything). Furthermore, if $C \Rightarrow_T^* L$ then the state of C cannot be 0 thus the state is at least 1 while all other entries are at least 0, hence $\phi(C) \geq \phi(L)$. Since $\{\, H, L \,\}$ is a final set of standard configurations for T, it follows from Lemma 8.3 that S is a Gröbner-Shirsov basis for I and hence $I = J$. Given a configuration C we have $\phi(C) - \phi(L) \in S$ if and only if $\phi(C) - \phi(H) \notin S$. Now $\phi(C) - \phi(H) \in S$ if and only if $C \Rightarrow_T^* H$ and this is decidable. □

Consider the method Reduce where the given basis (i.e., the second parameter S) is a Gröbner-Shirshov basis for an ideal I. An algorithm for the method is one that terminates on all inputs and returns 0 when the element $[\![f]\!]_{C_f}$ to be reduced is in I, i.e., $\{f(\mathbf{a}) \mid \mathbf{a} \in \mathbf{V}(C_f)\} \subseteq I$. Otherwise one or more non-zero parametrised elements $[\![g]\!]_{C_g}$ are returned such that $f \to_S g$ with condition C_g where $\{g(\mathbf{a}) \mid \mathbf{a} \in \mathbf{V}(C_g)\} \cap I = \emptyset$. In fact the next Lemma shows that there is no algorithm even for deciding just the first condition that $[\![f]\!]_{C_f}$ is in I

Theorem 8.1 *There is no algorithm for the method* REDUCE *even when S is a recursive Gröbner-Shirsov basis.*

PROOF. Consider configurations C of the Turing machine T that are of the form $q_I 1^*$. In encoded form these are $(0, q_I, 0, 0)$ or $(0, q_I, 1, (m^s - 1)/(m - 1))$ for $s \geq 0$ and can be classified by the first order formula

$$\mathcal{I}(\alpha, q, a, \beta) = \big(\alpha = 0 \wedge q = q_I \wedge ((a = 0 \wedge \beta = 0) \vee (a = 1 \wedge \exists s\, (m-1)\beta = m^s - 1))\big)$$

Now $[\![\phi(C) - \phi(L)]\!]_{\mathcal{I}(C)} \to_S 0$ if and only if T does not halt on any such C which is equivalent to T' not halting on the empty tape. If we have an algorithm for REDUCE that terminates on all inputs then we can solve the halting problem for T' on the empty tape which is a contradiction. □

We end this section with two remarks. If, in the definition of S, we allow only first order formulae without auxiliary functions (i.e., we do not allow the function γ) then S consists of infinitely many parametrised words; it would be interesting to know if there is an example with finitely many such words. In our encoding of Turing machines we could have gone further and encoded configurations as pairs of natural numbers to obtain Modular machines, see Aaanderaa and Cohen (1980a, 1980b). The gain is that we need only work with the free associative algebra $\mathbb{Q}\langle w, x, y, v\rangle$ but at the expense of some complications in the construction.

9. Concluding remarks

We have described an approach to working with parametrised sets of words with the aim of obtaining, at least in some circumstances, a finite description of a Gröbner-Shirshov basis for the ideal they generate. On the one hand we have shown an example where this works well. On the other hand we have shown that in general there can be no algorithm for the reduction process. However, this negative result does not hold if all the parameter variables are bounded from above as then all reductions must terminate. Thus one possible approach to checking a proposed Gröbner-Shirshov basis G is to put a bound on the unbounded variables (all other decision problems in the methods are decidable since we are dealing with a finite domain). Any compositions that fail to reduce to 0 are either counterexamples to G being a Gröbner-Shirshov basis or show that we need to increase the bound on the variables. Similar remarks apply to constructing a basis. This approach does not of course provide an algorithm but a tool to help investigation.

Furthermore the negative results do not apply in the case of finitely many parametrised words whose conditions have only finitely many assignments, assuming that these can be found algorithmically. Thus the methods can be used as algorithms in the case of a large number of finitely many fixed words that can be described succinctly by patterns.

It would be of interest to have at least a partial characterisation of sets of parametrised elements for which we can indeed obtain a parametrised Gröbner-Shirshov basis following the methods discussed here. The discussion in the introduction shows that this remains of interest in the special case when all elements are of the form $U - V$ where U, V are parametrised words. Despite a fair amount of effort we only have some very limited success which is not discussed in this paper.

Finally, in the introduction, we motivated part of our study with reference to applying our methods to verifying proposed standard bases (or Bokut' normal forms). We have not attempted to include an example of such a verification as it would be too complicated without machine assistance, an approach that we hope to pursue in the future. Before this research was conducted the second author implemented Gröbner-Shirshov bases for fixed words in the

Axiom computer algebra system (available as open source at http://www.axiom-developer.org and https://github.com/daly/axiom). He used this system to check bases obtained from Bokut' normal forms by the first author, Kalorkoti (2011), for particular modular machines. Extending the system to parametrised words would be a major effort.

BIBLIOGRAPHY

Aanderaa, S., Cohen, D. E. (1980a). Modular machines, the word problem for finitely presented groups and Collins' theorem, *Word problems II, the Oxford book* (ed. S. I. Adian, W. W. Boone, G. Higman, North-Holland, Amsderdam), pp. 1–16.

Aanderaa, S., Cohen, D. E. (1980b). Modular machines and the Higman–Clapham–Valiev embedding theorem, *Word problems II, the Oxford book* (ed. S. I. Adian, W. W. Boone, G. Higman, North-Holland, Amsderdam, 1980), pp. 17–28.

Bokut', L. A. (1966). On a property of the Boone groups (in Russian). *Algebra i Logika*, 5:5–23.

Bokut', L. A. (1967). On a property of the Boone groups (in Russian). *Algebra i Logika*, 6:15–24.

Bokut', L. A., Collins, D. J. (1980). Malcev?s problem and groups with a normal form. In: Adian, A. I., Boone, W., Higman, G., eds. *Word Problems II.* Studies in Logic and the Foundations of Mathematics. Vol. 95. North-Holland.

Bokut', L.A., Kolesnikov, P.S. (2003). Gröbner-Shirshov Bases from their Incipiency to the Present, J. of Math. Sciences, Vol. 116, No. 1, pp. 2894–2916.

Buchberger, B. (1965). An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal [in German], Ph.D. thesis, University of Innsbruck, Austria.

Chen, Y., Zhong, C. (2008). Gröbner-Shirshov basis for HNN extensions of groups and for the alternating group. Communications in Algebra 36:94–103.

Kalorkoti, K. (1982). Decision problems in group theory, *Proceedings of the London Mathematical Society*, vol. 44, no. 3, 312–332.

Kalorkoti, K. (2011). Sufficiency Conditions for Bokut' Normal Forms, *Communications in Algebra*, 39:8, 2862-2873

Matiyasevich, Y.V. (1970). Enumerable sets are Diophantine. Doklady Akademii Nauk SSSR (in Russian) 191: 279–282. English translation in Soviet Mathematics 11 (2), pp. 354–357.

Shirsov, S.I. (1962), Some algorithmic problems for Lie algebras, *Sib. Mat. Zh.*, **3**, 292–296.