Computations of Gröbner bases over the free associative algebra using a new approach to the Letterplace paradigm

Grischa Studzinski
University of Passau
Innstraße 33
94032 Passau, Germany
grischa.studzinski@rwth-aachen.de

Benjamin Schnitzler
RWTH Aachen University
Templergraben 64
52062 Aachen, Germany
benjamin.schnitzler@rwth-aachen.de

Viktor Levandovskyy
RWTH Aachen University
Templergraben 64
52062 Aachen, Germany
viktor.levandovskyy@math.rwth-aachen.de

ABSTRACT

Recently, La Scala and Levandovskyy presented a one-to-one correspondence between two-sided ideals of the free algebra and ideals in a *Letterplace ring*, which is an infinitely generated commutative polynomial ring. This helps, among others, in dealing with modules over free algebra $\mathbb{K}\langle X\rangle$.
By performing practical computations over a commutative ring, one makes use of the experience, gathered in the past 40 years with the data structures as well as many fundamental algorithms. The basic idea behind the Gröbner basis computations in free algebra $\mathbb{K}\langle X\rangle$ utilizing the letterplace framework is to exploit the natural action of the monoid $\mathbb{N}$, which *shifts* places of monomials of the letterplace ring.

Using a separating invariant for the orbits of the shift action of $\mathbb{N}$, we derive a representation of monomials of the letterplace ring, which is invariant under the action of $\mathbb{N}$. In the paper the theoretical work is explained as well as an optimized way to compute Gröbner bases using this new representation. The memory usage throughout the computations with the new representation is significantly smaller, than with the original representation. Moreover, the effectiveness is demonstrated on some interesting examples.

In any Gröbner basis theory, criteria to avoid useless pairs in a Gröbner basis algorithm are of crucial importance.
We generalize the famous Gebauer-Möller's criterion to the non commutative setting, thus obtaining a procedure to reduce the set of critical pairs. However, applying this criterion in actual computations over $\mathbb{K}\langle X\rangle$ can be rather difficult. In contrast, by using the action of $\mathbb{N}$ by shift and the shift-invariant data representation in the letterplace paradigm, this criterion becomes easy to handle.

We illustrate that the letterplace approach is not only very effective when it comes down to practical computation, but also interesting for solving theoretical questions over free algebras, bringing new insights.

ISSAC2012 '12 Grenoble, France Europe

1. INTRODUCTION

With the recent work of Roberto La Scala and Viktor Levandovskyy a new way to compute Gröbner bases was born, where non commutative Gröbner bases of graded ideals in free algebras are computed via the *Letterplace correspondence*. The most important point for practical computer algebra is that the computations take place in a commutative ring, where the data structures as well as many fundamental algorithms have been deeply studied and enhanced in the past 40 years.
The basic idea, going back to Richard Feynman and Gian-Carlo Rota, is pleasingly simple: one enumerates the variables occurring in a monomial by their position in the monomial. Then one may commute the variables. However, practical use of the experimentational implementation of Viktor Levandovskyy has shown that the computation of a Gröbner basis is very expensive in terms of memory usage, because for each polynomial occurring during the computation one has to consider all of its "shifts" and since the shifts are needed for reduction as well, all of those need to be stored. So the idea arose to find a new way to compute critical pairs for s-polynomials and reduction.

The Letterplace ring has a very interesting structure, which is dominated by a monoid action of $\mathbb{N}$. This allows one often to use commutative methods "up to shifting".

In the following, we present our studies of this monoid action ultimativly leading to a representation of monomials invariant to the shifting. This helps a great deal in handling the Letterplace monomials, not only for Gröbner basis computations, but also for other things.

As an example for this we present a non commutative version of Gebauer-Möllers criterion and present the way to use it with the Letterplace setup. Since it is very easy to handle then, this allows us to speed up our computation.

We will always assume that the free algebra is endowed with a well ordering $<$.

2. THE LETTERPLACE RING AND THE SHIFT ACTION

2.1 The Letterplace paradigm

In this section we give a small introduction into the Letterplace realm. We follow ref->LaScalaLevandovskyy.

DEFINITION 2.1.
We call $X = x_1, \ldots, x_n$ *and* $P \subseteq \mathbb{N}_0$ *respectively the set of*

letters and places. We write for the elements of the product set $X \times P$: $x_i(j) := (x_i, j)$. Furthermore we denote by $\mathbb{K}[X|P]$ the polynomial ring in the commuting variables $x_i(j)$ and by $[X|P]$ the set of all monomials in $\mathbb{K}[X|P]$.
Let $\mu = (\mu_k)_{k\in\mathbb{N}}, \nu = (\nu_k)_{k\in\mathbb{N}}$ be two sequences of non-negative integers with finite support. We can consider (μ, ν) as a multidegree for the monomials $m = x_{i_1}(j_1)\dots x_{i_r}(j_r) \in [X|P]$.

Remark *2.2.*
If we define $\mathbb{K}[X|P]_{\mu,\nu}$ to be the homogeneous component of degree (μ, ν) we have $\mathbb{K}[X|P] = \bigoplus_{\mu,\nu} \mathbb{K}[X|P]_{\mu,\nu}$, so $\mathbb{K}[X|P]$ is a multigraded algebra. By putting $\mathbb{K}[X|P]_{*,\nu} = \bigoplus_{\mu} \mathbb{K}[X|P]_{\mu,\nu}$ and $\mathbb{K}[X|P]_{\mu,*} = \bigoplus_{\nu} \mathbb{K}[X|P]_{\mu,\nu}$ we obtain that $\mathbb{K}[X|P]$ is also multigraded with respect to letter or place multidegrees only.

Definition *2.3.*
For each monomial $m = x_{i_1}(j_1)\cdots x_{i_r}(j_r) \in [X|P]$ we define by $sh(m) = \min\{j_1, \dots, j_r\}$ the shift of m.
For each $s, r \in \mathbb{N}$ we denote by $s \cdot 1^r$ the place-multidegree $\nu = (\nu_k)_{k\in\mathbb{N}}$ such that

$$\nu_k = \begin{cases} 1, & \text{if } s \le k \le s + r - 1. \\ 0, & \text{otherwise.} \end{cases}$$

For $s = 0$ we write simply 1^r.
Define $V = \bigoplus_{n\in\mathbb{N}} \mathbb{K}[X|P]_{*,1^r}$, which is a subspace of $\mathbb{K}[X|P]^{(0)}$, the subspace of $\mathbb{K}[X|P]$ generated by all monomials with shift 0. Set $V' = \bigcup_{s\in\mathbb{N}} s \cdot V$, which is again a vector space.

Lemma *2.4.*
$\iota : \mathbb{K}\langle X\rangle \to V : x_{i_1}\cdots x_{i_r} \mapsto x_{i_1}(0)\cdots x_{i_r}(r-1)$ is an isomorphism of vector spaces, which preserves letter-multidegrees and hence total degrees of monomials.

This Lemma allows one to embed the free algebra into the Letterplace ring. Sadly, ι is not a ring homomorphism, since V is only a vectorspace and not a ring!
From now on we will additionally assume that the ordering $<$ on the free algebra and the one on the Letterplace ring $\prec$ are invariant under ι that is if $m < m'$ for two monomials $m, m' \in \mathbb{K}\langle X\rangle$ then $\iota(m) \prec \iota(m')$. For more details on this assumption we again refer to ref->LaScalaLevandovskyy
The next lemma shows the usefulness of V'.

Lemma *2.5.*
Let $m, m' \in \mathbb{K}\langle X\rangle$ and set $n = \iota(m)$, $n' = \iota(m')$. Then: $m|m' \Leftrightarrow \exists s \in \mathbb{N} : s \cdot n|n'$.

This indicates how to use the Letterplace ring for non commutative computations: If one considers the images of the monomials and all of their shifts, then a Gröbner basis can be found by applying the commutative version of Buchberger's algorithm and discard all the elements not needed. Let us put this in the correct terms. Therefor one needs the corresponding ideals and generating sets.

Theorem *2.6.*
Let I be a left ideal of $\mathbb{K}\langle X\rangle$ and put $I' = \iota(I)$. Define $J = \langle \bigcup_{s\in\mathbb{N}} s \cdot I' \rangle \subset \mathbb{K}[X|P]$. Then J is a shift-invariant ideal that is, if $s \cdot J^{(0)} = J^{(s)}$ for all $s \in \mathbb{N}$. Moreover, if I is graded then J is place-multigraded, that is $\boldsymbol{J} = \sum_{\nu} \boldsymbol{J}_{*,\nu}$, where $\boldsymbol{J}_{*,\nu} = \boldsymbol{J} \cap \mathbb{K}[X|P]_{*,\nu}$.

Definition *2.7.*
Let $J \subset \mathbb{K}[X|P]$ be an ideal. Then J is called shift-decomposable, if J is generated by $\bigcup_{s\in\mathbb{N}} J^{(s)}$.

Definition *2.8.*

- *Let $I \subset \mathbb{K}\langle X\rangle$ be a graded two-sided ideal. We denote by $\tilde{\iota}(I)$ the shift-invariant place-multigraded ideal $J \subset \mathbb{K}[X|P]$ generated by $\bigcup_{s\in\mathbb{N}} s \cdot \iota(I)$, and call J the Letterplace analogon of the ideal I.*
- *For a shift-invariant place-multigraded ideal $J \subset \mathbb{K}[X|P]$ we denote by $\tilde{\iota}^{-1}(J)$ the graded two-sided ideal $I = \iota^{-1}(J \cap V) \subset \mathbb{K}\langle X\rangle$.*
- *A graded ideal $J \subset \mathbb{K}[X|P]$ is called a Letterplace ideal if J is generated by $\bigcup_{s,d\in\mathbb{N}} s \cdot (J_d \cap V)$. In this case, J is shift-invariant and place-multigraded.*

Remark *2.9.*
The map $\iota : \mathbb{K}\langle X\rangle \to V$ induces a one-to-one correspondence $\tilde{\iota}$ between graded two-sided ideals I of the free associative algebra $\mathbb{K}\langle X\rangle$ and the Letterplace ideals J of the polynomial ring $\mathbb{K}[X|P]$.

The map $\tilde{\iota}$ identifies the corresponding ideals. Now what's about generating sets ans especially Gröbner bases?

Definition *2.10.*
Let J be a Letterplace ideal of $\mathbb{K}[X|P]$ and $H \subset \mathbb{K}[X|P]$. We say that H is a Letterplace basis of J if $H \subset \bigcup_{d\in\mathbb{N}} J_d \cap V$ and $\bigcup_{s\in\mathbb{N}} s \cdot H$ is a generating set of the ideal J.

Theorem *2.11.*
Let I be a graded two-sided ideal of $\mathbb{K}\langle X\rangle$ and put $J = \tilde{\iota}(I)$. Moreover, let $G \subset \bigcup_{d\in\mathbb{N}} I_d$ and define $H = \iota(G) \subset \bigcup_{d\in\mathbb{N}} J_d \cap V$. Then G is a generating set of I as a two-sided ideal if and only if H is a Letterplace basis of J.

Definition *2.12.*
Let J be an ideal of $\mathbb{K}[X|P]$ and $H \subset J$. Then H is called a (Gröbner) shift-basis of J if $\bigcup_{s\in\mathbb{N}} s \cdot H$ is a (Gröbner) basis of J.

Theorem *2.13.*
Let $I \trianglelefteq \mathbb{K}\langle X\rangle$ be a graded two-sided ideal and put $J = \tilde{\iota}(I)$. Moreover, let H be a Gröbner Letterplace basis of J and put $G = \iota^{-1}(H \cap V) \subset \bigcup_{d\in\mathbb{N}} I_d$. Then G is a Gröbnerbasis of I as a two-sided ideal.

Remark *2.14.*
So one computes a Gröbner Letterplace basis and once this is done, by discarding all elements not in V one gets the desired Gröbner basis. It is notable that any s-polynomial,

which will not lie in V can be discarded during the computation. Also, one only has to consider pairs of the form $(p_i, s \cdot p_j)$, because this are the only ones returning polynomials in V.
Although this allows one to do the computation more efficiently, the Letterplace structure allows to do the computation in a better way, as one may see in the next section.

2.2 A separating invariant

In commutative computer algebra one often uses exponent vectors to determine if a monomial divides another.

LEMMA *2.15.*
Take two monomials $m_1, m_2 \in \mathbb{K}[x1, \ldots, x_n]$ and say $m_1 = x_1^{a_1} \cdots x_n^{a_n} =: x^a$ and $m_1 = x_2^{b_1} \cdots x_n^{b_n} =: x^b$. Then
$m_1 | m_2 \quad \Leftrightarrow \quad a_i \leq b_i \; \forall i$.

Sadly this is not true for the free algebra and exponent vectors are generally not very useful. However, the Letterplace ring is commutative, so it is useful to study the exponent vectors. Since there are infinitely many variables we cut the exponent vector after the last non-zero entry (the support of a multidegree is always finite).

REMARK *2.16.*
Take $m \in V' \subset \mathbb{K}\langle x_1, \ldots, x_n \rangle$ of total degree d and shift s with exponent vector e. Then $e = (e_1, \ldots, e_{d+s})$, where e_i is a block of length n for all $1 \leq i < d$. If the length of e_d is smaller than n we add zeros (this will not change the corresponding monomial). Then:

- *For $1 \leq i < s$: e_i contains only zeros.*
- *For $s \geq i$: e_i contains exactly one 1 and $n-1$ zeros. Note that the 1 is on position j, if and only if $(x_j \mid i) | m$.*

LEMMA *2.17.*
Take $m, m' \in V'$ and $m' = s \cdot m$ for some $s \in \mathbb{N}$ with exponent vectors e and e' constructed as above. Say m is of total degree d and set $\tilde{e} = (e'_s, \ldots, e'_{s+d}$. Then $\tilde{e} = e$.

PROOF.
Denote by $\tilde{m}$ the monomial corresponding to $\tilde{e}$.
Since $shift(m') \geq s$ we have $e'_i = (0, \ldots, 0) \; \forall i < s$. It follows that $shift(\tilde{m}) = shift(m') - s$ and $s \cdot \tilde{m} = m'$, which already implies $\tilde{m} = m$ and thus $\tilde{e} = e$. □

DEFINITION *2.18.*
Let $m \in V'$ with total degree d and shift s and construct the exponent vector e as before. Set $\tilde{e} = (e_s, \ldots, e_{d+s}$. Construct another integer vector D as follows:
The first entry of D is the position of the 1 occurring in e_s. For $1 < i \leq d$ the $i-th$ entry equals the number of zeros between the 1 in e_{s+i} and the 1 in e_{s+i-1}. We call D a distance vector or dvec.

Denote by dv the map that assigns to each monomial $m \in V'$ its dvec.

THEOREM *2.19.*
The map dv is an invariant for the shift action, which separates the orbits. That is for all $m, m' \in V'$ we have: $m' = s \cdot m$ or $m = s \cdot m'$ for some $s \in \mathbb{N}$ if and only if $dv(m) = dv(m')$.

PROOF. " $\Rightarrow$ " : *Follows immediately by the previous Lemma, because the dvec ignores the shift of an monomial.*
" $\Leftarrow$ " : *It is sufficient to show that the restriction of dv to V is injectiv, which is clear by the remark above.* □

This leads to a way to decide whether or not $m | m'$ for monomials $m, m' \in \mathbb{K}\langle X \rangle$.

DEFINITION *2.20.*
For two dvecs d and d' we say that d is contained in d', if the $size(d') \geq size(d)$ and there exists i such that $d[1] = d'[i] + i*n - \sum_1^{i-1} d'[i]$ and $d[j] = d'[i+j-1]$ for $1 < j \leq size(d)$.

REMARK *2.21.*
By construction of the dvecs we have $dv(m)$ is contained in $dv(m')$ if and only if $m | m' \qquad \forall m, m' \in \mathbb{K}[X|P]$.

COROLLARY *2.22.*
Take two monomials $m, m' \in \mathbb{K}\langle X \rangle$ and set $n = \iota(m), n' = \iota(m')$ and name the dvecs d and d' respectively. Then:
$m | m' \quad \Leftrightarrow \quad d$ is contained in d'

PROOF.
$m | m' \quad \Leftrightarrow \quad \exists s \in \mathbb{N} : \; s \cdot n | n'$. Since dvecs ignore the shift this proves the claim. □

REMARK *2.23.*
This leads to a practical way to conclude if $m | m'$ by just comparing the dvecs. The nice thing about this procedure is that one gets the shift s directly and can use $s \cdot n$ say for reduction of n' (or their polynomials respectively).

This directly improves the algorithm, since one has not to consider all of the shifts of n, but just those witch are really needed.

3. GEBAUER-MÖLLER'S CRITERION

That the practical use of criteria to reduce the set of critical pairs is very effective is a well-known fact in commutative as well as non commutative Gröbner basis theory. Over commutative rings it has been proven that Gebauer-Möller's criterion is of utter importance. So it makes sense to study its value from a non commutative point of view as well.

For this section we will assume that each set $P \subset \mathbb{K}\langle X \rangle$ is interreduced, meaning $\forall p, q \in P, p \neq q : \mathbf{lm}(p) \nmid \mathbf{lm}(q)$ and that each $p \in P$ is monic.

3.1 The non commutative theory

In the non commutative version of Buchberger's algorithm constructs s-polynomials from so-called obstructions that is a six-tupel $(l, p, r; \lambda, q, \rho)$ with $l, r, \lambda, \rho \in \mathbb{K}\langle X \rangle$, $p, q \in P$ and $\mathbf{lm}(lpr) = \mathbf{lm}(\lambda, q, \rho)$.
There is a theorem which states that only those pairs need to be considered, which leading monomials involve an overlap, that is $\mathbf{lm}(p) = ab$ and $\mathbf{lm}(q) = bc$ for some monomials a, b, c. Therefor one only has to consider pairs $\pi = (1, p_i, r; \lambda, p_j, 1)$, such that $\mathbf{lm}(p_i r) = \mathbf{lm}(\lambda p_j)$. For more details we refer to reference->diplomarbeit?

DEFINITION *3.1.*
For an obstruction $\pi = (1, p_i, r; \lambda, p_j, 1)$ we denote by $\mathbf{cm}(\pi) := \mathbf{lm}(p_i r) = \mathbf{lm}(p_i) r = \lambda \mathbf{lm}(p_j)$ the common multiple of p_i and p_j with respect to the overlap considered in π.

We now have the following setup: Consider a set of polynomials P, say the generating system. We want to construct the set of all critical pairs $\pi(P)$. This set is usually constructed by searching for overlaps in the leading monomials. We want to apply the criteria to $\pi(P)$ to reduce its size.

THEOREM *3.2.*
Assume we have a set of polynomials P, its set of critical pairs $\pi(P)$ a pair $\pi = (1, p_i, r_i; \lambda_k, p_k, 1) \in \pi(P)$.

1. *If there exists a pair $\pi_1 = (1, p_j, r_j; \lambda'_k, p_k, 1) \in \pi(P) \setminus \{\pi\}$, such that $\mathbf{cm}(\pi_1)$ divides $\mathbf{cm}(\pi)$ from the right, then the s-polynomial $s(\pi)$ of π will reduce to zero.*
2. *If there are two pairs $\pi_1 = (1, p_i, r'_i; \lambda_j, p_j, 1), \pi_2 = (1, p_j, r_j; \lambda'_k, p_k, 1) \in \pi(P) \setminus \{\pi\}$, such that $\mathbf{lm}(p_j) | \mathbf{cm}(\pi)$, then the s-polynomial $s(\pi)$ of π will reduce to zero.*

PROOF.

1. *We first note that $\mathbf{lm}(p_j) r_j = \mathbf{lm}(p_j r_j) = \mathbf{lm}(\lambda'_k p_k) = \lambda'_k \mathbf{lm}(p_k)$ and $\tilde{l}\mathbf{lm}(p_j) r_j = \tilde{\lambda}\lambda'_k \mathbf{lm}(p_k) = \lambda_k \mathbf{lm}(p_k) = \mathbf{lm}(p_i) r_i$ for some monomials $\tilde{l}, \tilde{\lambda}$. This already implies $\tilde{l} = \tilde{\lambda}$ and $\tilde{\lambda}\lambda' = \lambda_k$.*
   We then have $s(\pi) = p_i r_i - (\lambda_k \mathbf{lm}(p_k) + \lambda_k \mathbf{tail}(p_k)) \to p_i r_i - (-\tilde{l}\mathbf{tail}(p_j) r_j + \tilde{(\lambda)}\lambda' \mathbf{tail}(p_k)) = p_i r_i - \tilde{l}(-s(\pi_1)) \to 0$.
2. *Because of the assumptions we have $\mathbf{lm}(f_j) = abc$, $\mathbf{lm}(f_k) = bct_k$ and $\mathbf{lm}(f_i) = t_i ab$ for some monomials a, b, c, t_i, t_k. Because the set of polynomials is interreduced none of the leading monomials can divide the overlap cofactors. This implies $\lambda_k = t_i a$ and $r_i = ct_k$. Moreover, the existence of π_1 and π_2 and the form of the leading monomials imply that there exist pairs $\pi'_1 = (1, p_i, c; t_i, p_j, 1)$ and $\pi'_2 = (1, p_j, t_k; a, p_k, 1)$*
   Then $s(\pi) = p_i ct_k - t_i a p_k = t_i abct_k + \mathbf{tail}(p_i) ct_k - t_i abct_k - t_i a \mathbf{tail}(p_k) \to$
   $-t_i \mathbf{tail}(p_j) t_k + \mathbf{tail}(p_i) ct_k + t_i \mathbf{tail}(p_j) t_k - t_i a \mathbf{tail}(p_k) = -s(\pi'_1) t_k - t_i s(\pi'_s) \to 0$

REMARK *3.3.*
One can apply these criteria in a straight forward way: If the set of critical pairs during some step of Buchberger's algorithm has been constructed, then one can just check the pairs and search for redundant ones. However, to decide if a monomial divides another is not as easy as in the commutative case. Again, dvecs can come in handy and one can use the procedure presented above.

3.2 Translation to Letterplace

Our final goal now is to translate the criteria into the Letterplace realm. This is done quite easily.

THEOREM *3.4.*
Assume we have a pair $\pi = (p_i, s \cdot p_k)$.

1. *If there exists a pair $\pi_1 = (p_j, s \cdot p_k) \neq \pi$, such that $\mathbf{lcm}(p_j, s \cdot p_k)$ divides $\mathbf{lcm}(p_i, s \cdot p_k)$, then the s-polynomial $s(\pi)$ of π will reduce to zero.*
2. *If there are two pairs $\pi_1 = (p_i, s' \cdot p_j)$ and $\pi_2 = (p_j, s'' \cdot p_k)$, such that $\mathbf{lm}(s' \cdot p_j) | \mathbf{lcm}(p_i, s \cdot p_k)$, then the s-polynomial $s(\pi)$ of π will reduce to zero.*

REMARK *3.5.*
In 1.: Since we assume that the shift of p_k is the same for π and π_1 the condition, that $\mathbf{cm}(\pi_1)$ divides $\mathbf{cm}(\pi)$ from the right, is always satisfied.
In 2.: We have $s'' = s - s'$. This follows immediately from the non commutative proof and the form of the overlap.
If the shifts are known one can simply apply commutative methods to check the divisibility. For condition one this is especially easy, since the shift is known from the pair we check.

4. IMPLEMENTATION AND TIMINGS