Gröbner Bases for Linearized Polynomials

Margreta Kuijper and Anna-Lena Trautmann
Department of Electrical and Electronic Engineering
University of Melbourne, Australia.

Abstract

In this work we develop the theory of Gröbner bases for modules over the ring of univariate linearized polynomials with coefficients from a finite field.

1 Introduction

Gröbner bases [2] are a powerful conceptual and computational tool for modules over general multivariate polynomial rings. In particular, they also prove useful for modules over univariate polynomials with coefficients from a finite field. This motivates us to develop similar tools for modules over linearized polynomials, a special family of polynomials over a finite field, in an analogous manner. For more information on Gröbner bases for modules over finite field polynomial rings the interested reader is referred to [1].

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a prime power, and let $\mathbb{F}_{q^m}$ denote the extension field of extension degree m. A *linearized polynomial* over $\mathbb{F}_{q^m}$ is of the form

$$f(x) = \sum_{i=0}^{n} a_i x^{[i]}, \quad a_i \in \mathbb{F}_{q^m},$$

where $[i] := q^i$. If the base field needs to be specified, these polynomials are also called q-linearized. The name "linearized" stems from the fact that linearized polynomials function as q-linear maps. This class of polynomials was first investigated in [10] and later on by [3]. These polynomials have received a lot of interest in the past decades due to their application in rank-metric codes [3, 4] and related topics.

The set of linearized polynomials, equipped with normal polynomial addition $+$ and polynomial composition $\circ$, forms a non-commutative ring without zero-divisors (see e.g. [5]). We will denote this ring of q-linearized polynomials over $\mathbb{F}_{q^m}$ by $\mathcal{L}_q(x, q^m)$.

Due to the difference of composition (for linearized polynomials) and multiplication (for classical polynomials), the theory of bases in general, and Gröbner bases in particular, needs to be developed from scratch for the ring $\mathcal{L}_q(x, q^m)$.

The paper is structured as follows: In the next section we will investigate the structure of $\mathcal{L}_q(x, q^m)^\ell$ as a left module. In Section 3 we will derive the theory of Gröbner bases for submodules of $\mathcal{L}_q(x, q^m)^\ell$. We conclude this work in Section 4.

2 The Module $\mathcal{L}_q(x, q^m)^\ell$

As mentioned before, $\mathcal{L}_q(x, q^m)$ forms a ring with addition and composition. Hence $\mathcal{L}_q(x, q^m)^\ell$ forms a right or left module, which are different due to the non-commutativity of $\circ$. In this work we will consider $\mathcal{L}_q(x, q^m)^\ell$ as a left module and investigate its left submodules. The results then easily carry over to right modules.

Elements of $\mathcal{L}_q(x, q^m)^\ell$ are of the form

$$f := [f_1(x) \ \dots \ f_\ell(x)] = \sum_{i=1}^{\ell} f_i(x) e_i$$

where $f_i(x) = \sum_j f_{ij} x^{[j]} \in \mathcal{L}_q(x, q^m)$ and $e_1, \dots, e_\ell$ are the unit vectors of length ℓ. To avoid confusion we denote polynomials by $f(x)$, while vectors of polynomials are denoted by f. If we need to index polynomials, we use the notation $f_1(x), \dots, f_s(x)$, while for vectors of polynomials we will use the notation $f^{(1)}, \dots, f^{(s)}$. Analogous to polynomial multiplication on $\mathbb{F}_{q^m}[x]^\ell$ we define for $h(x) \in \mathcal{L}_q(x, q^m)$ the left operation

$$h(x) \circ f := [h(f_1(x)) \ \dots \ h(f_\ell(x))] = \sum_{i=1}^{\ell} h(f_i(x)) e_i.$$

The monomials of f are of the form $x^{[k]} e_i$ for all k such that $f_{ik} \neq 0$.

Definition 1. A subset $M \subseteq \mathcal{L}_q(x, q^m)^\ell$ is a *(left) submodule* of $\mathcal{L}_q(x, q^m)^\ell$ if it is closed under addition and composition with $\mathcal{L}_q(x, q^m)$ on the left.

Definition 2. Consider the non-zero elements $f^{(1)}, \dots, f^{(s)} \in \mathcal{L}_q(x, q^m)^\ell$. We say that $f^{(1)}, \dots, f^{(s)}$ are *linearly independent* if for any $a_1(x), \dots, a_s(x) \in \mathcal{L}_q(x, q^m)$

$$\sum_{i=1}^{s} a_i(x) \circ f^{(i)} = [\, 0 \ \dots \ 0 \,] \quad \Longrightarrow \quad a_1(x) = \cdots = a_s(x) = 0.$$

A generating set of a submodule $M \subseteq \mathcal{L}_q(x, q^m)^\ell$ is called a *basis* of M if all its elements are linearly independent.

One can easily see that

$$B = \{xe_1, xe_2 \dots, xe_\ell\}$$

is a basis of $\mathcal{L}_q(x, q^m)^\ell$, thus $\mathcal{L}_q(x, q^m)^\ell$ is a *free* and *finitely generated* module.

We need the notion of monomial order for the subsequent results, which we will define in analogy to [1, Definition 3.5.1].

Definition 3. A *monomial order* $<$ on $\mathcal{L}_q(x, q^m)^\ell$ is a total order on $\mathcal{L}_q(x, q^m)^\ell$ that fulfills the following two conditions:

- $x^{[k]} e_i < x^{[j]} \circ (x^{[k]} e_i)$ for any monomial $x^{[k]} e_i \in \mathcal{L}_q(x, q^m)^\ell$ and $j \in \mathbb{N}_{>0}$.
- If $x^{[k]} e_i < x^{[k']} e_{i'}$, then $x^{[j]} \circ (x^{[k]} e_i) < x^{[j]} \circ (x^{[k']} e_{i'})$ for any monomials $x^{[k]} e_i, x^{[k']} e_{i'} \in \mathcal{L}_q(x, q^m)^\ell$ and $j \in \mathbb{N}_0$.

An example of a monomial order on $\mathcal{L}_q(x, q^m)^\ell$ is the weighted term-over-position monomial order in [8]. In the following we will not fix a monomial order. The results are general and hold for any chosen monomial order.

Definition 4. We can order all monomials of an element $f \in \mathcal{L}_q(x, q^m)^\ell$ in decreasing order with respect to some monomial order. Rename them such that $x^{[i_1]}e_{j_1} > x^{[i_2]}e_{j_2} > \dots$. Then

1. the *leading monomial* $\mathrm{lm}(f) = x^{[i_1]}e_{j_1}$ is the greatest monomial of f.
2. the *leading position* $\mathrm{lpos}(f) = j_1$ is the vector coordinate of the leading monomial.
3. the *leading term* $\mathrm{lt}(f) = f_{j_1,i_1}x^{[i_1]}e_{j_1}$ is the complete term of the leading monomial.

In order to define minimality for submodule bases we need the following notion of reduction, in analogy to [1, Definition 4.1.1].

Definition 5. Let $f, h \in \mathcal{L}_q(x, q^m)^\ell$ and let $F = \{f^{(1)}, \dots, f^{(s)}\}$ be a set of non-zero elements of $\mathcal{L}_q(x, q^m)^\ell$. We say that *$f$ reduces to h modulo F in one step* if and only if

$$h = f - ((b_1x^{[a_1]}) \circ f^{(1)} + \dots + (b_kx^{[a_k]}) \circ f^{(k)})$$

for some $a_1, \dots, a_k \in \mathbb{N}_0$ and $b_1, \dots, b_k \in \mathbb{F}_{q^m}$, where

$$\mathrm{lm}(f) = x^{[a_i]} \circ \mathrm{lm}(f^{(i)}), \quad i = 1, \dots, k, \quad \text{and}$$

$$\mathrm{lt}(f) = (b_1x^{[a_1]}) \circ \mathrm{lt}(f^{(1)}) + \dots + (b_kx^{a_{[k]}}) \circ \mathrm{lt}(f^{(k)}).$$

We say that f is *minimal* with respect to F if it cannot be reduced modulo F.

Definition 6. A module basis B is called *minimal* if all its elements b are minimal with respect to $B\backslash\{b\}$.

Proposition 7. *[7] Let B be a basis of a module $M \subseteq \mathcal{L}_q(x, q^m)^\ell$. Then B is a minimal basis if and only if all leading positions of the elements of B are distinct.*

Proof. Let B be minimal. If two elements of B have the same leading position, the one with the greater leading monomial can be reduced modulo the other element, which contradicts the minimality. Hence, no two elements of a minimal basis can have the same leading position.

The other direction follows straight from the definition of reducibility and minimality of a basis, since if the leading positions of all elements are different, none of them can be reduced modulo the other elements. □

The property outlined in the following theorem is called the *Predictable Leading Monomial (PLM) property*, a terminology that was introduced in [6] for modules in $\mathbb{F}_q[x]^\ell$ with respect to multiplication. For linearized polynomials it was formulated and proven in [9].

Theorem 8 (PLM property,[9]). *Let M be a module in $\mathcal{L}_q(x, q^m)^\ell$ with minimal basis $B = \{b^{(1)}, \ldots, b^{(k)}\}$. Then for any $0 \neq f \in M$, written as*

$$f = a_1(x) \circ b^{(1)} + \cdots + a_k(x) \circ b^{(k)},$$

where $a_1(x), \ldots, a_k(x) \in \mathcal{L}_q(x, q^m)$, we have

$$\mathrm{lm}(f) = \max_{1 \leq i \leq k; a_i(x) \neq 0} \{\mathrm{lm}(a_i) \circ \mathrm{lm}(b^{(i)})\}$$

where (with slight abuse of notation) $\mathrm{lm}(a_i(x))$ denotes the term of $a_i(x)$ of highest q-degree.

3 Gröbner Bases for Submodules of $\mathcal{L}_q(x, q^m)^\ell$

We will now investigate a special family of bases, called Gröbner bases, for submodules of $\mathcal{L}_q(x, q^m)^\ell$.

Definition 9. Let $M \subseteq \mathcal{L}_q(x, q^m)^\ell$ be a submodule. A subset $B \subset M$ is called a *Gröbner basis* of M if the leading terms of B span a left module that contains all leading terms of M.

It is well-known that a Gröbner basis of a module M in $\mathbb{F}_q[x]^\ell$ (equipped with normal multiplication) generates M. We will now show the analog for linearized polynomials.

Theorem 10. *Let M be a module in $\mathcal{L}_q(x, q^m)^\ell$ with Gröbner basis B. Then B generates M.*

Proof. Let $f \in M$ and $B = \{b^{(1)}, \ldots, b^{(k)}\} \subset \mathcal{L}_q(x, q^m)^\ell$. Since B is a Gröbner basis there exist $h_1(x), \ldots, h_k(x) \in \mathcal{L}_q(x, q^m)$ such that

$$\mathrm{lt}(f) = \sum_{j=1}^{k} h_j(\mathrm{lt}(b^{(j)})).$$

One sees that $\mathrm{lt}(f)$ can only be a combination of the elements of the Gröbner basis that have the same leading position as f. Without loss of generality assume that this is the case for $b^{(1)}, \ldots, b^{(k')}, k' \leq k$. Then

$$\mathrm{lt}(f) = \sum_{j=1}^{k'} h_j(\mathrm{lt}(b^{(j)})) = \sum_{j=1}^{k'} h_j(b^{(j)}_{m_j} x^{[m_j]} e_{\mathrm{lpos}(f)}),$$

where $b^{(j)}_{m_j} x^{[m_j]} e_{\mathrm{lpos}(f)}$ is the leading term of $b^{(j)}$. Denote $m_- := \min\{m_j \mid j = 1, \ldots, k'\}$. Then

$$\mathrm{lt}(f) = \sum_{j=1}^{k'} h_j(b^{(j)}_{m_j} x^{[m_j - m_-]}(x^{[m_-]} e_{\mathrm{lpos}(f)}))$$

$$= \left(\sum_{j=1}^{k'} h_j(b^{(j)}_{m_j} x^{[m_j - m_-]}) \right) \circ (x^{[m_-]} e_{\mathrm{lpos}(f)})$$

and thus $x^{[m-]}e_{\mathrm{lpos}(f)}$ symbolically divides $\mathrm{lt}(f)$. Furthermore, there exists $1 \leq i \leq k'$ such that $x^{[m-]}e_{\mathrm{lpos}(f)} = \mathrm{lm}(b^{(i)})$.

Now reduce f modulo G until it is minimal and call the resulting vector $r \in \mathcal{L}_q(x, q^m)^\ell$. Hence there exist $h_1(x), \ldots, h_k(x) \in \mathcal{L}_q(x, q^m)$ such that

$$f - r = \sum_{i=1}^{k} h_i(b^{(i)})$$

which implies that $f - r \in M$. If $r = 0$, then $f = \sum_{i=1}^{k} h_i(b^{(i)})$. We will now show by contradiction that $r \neq 0$ is not possible. If $r \neq 0$ then $r = f - \sum_{i=1}^{k} h_i(b^{(i)}) \in M$, since $f \in M$. Then, by the first part of the proof, there exists $h(x) \in \mathcal{L}_q(x, q^m)$ and $1 \leq i \leq k$ such that

$$\mathrm{lt}(r) = h(\mathrm{lm}(g_i))$$

which means that r could be further reduced modulo G, which contradicts the minimality assumption. Thus, we have shown that any $f \in M$ can be generated by the elements of B. □

Thus, we have shown that any Gröbner basis of a module is actually a basis of this module. Clearly, the other way around is not true, i.e. not every basis is a Gröbner basis, but for minimal bases the reverse implication also holds, as shown in the following.

Theorem 11. *Any minimal basis B of a module $M \subseteq \mathcal{L}_q(x, q^m)^\ell$ is a minimal Gröbner basis of M.*

Proof. Let $f \in M$. Since any minimal basis of a module in $\mathcal{L}_q(x, q^m)^\ell$ has at most ℓ elements, we can assume $B = \{b^{(1)}, \ldots, b^{(\ell')}\}$, where $\ell' \leq \ell$. There exist $a_1(x), \ldots, a_{\ell'}(x) \in \mathcal{L}_q(x, q^m)$ such that $\sum_i a_i(x) \circ b^{(i)} = f$. Then by Theorem 8

$$\mathrm{lm}(f) = \max_{1 \leq i \leq \ell'; a_i \neq 0} \{\mathrm{lm}(a_i) \circ \mathrm{lm}(b^{(i)})\},$$

i.e. $\mathrm{lm}(f)$ and thus also $\mathrm{lt}(f)$ is in the module spanned by all $\mathrm{lm}(b^{(i)})$, $i = 1, \ldots, \ell'$. □

Finally, we show the existence of Gröbner bases of modules in $\mathcal{L}_q(x, q^m)^\ell$.

Theorem 12. *For any module $M \subseteq \mathcal{L}_q(x, q^m)^\ell$ there exists a finite minimal Gröbner basis.*

Proof. Without restriction assume that M contains elements with leading position i for all $i \in \{1, \ldots, \ell\}$. Define $f_{\min,i}$ as the (non-unique) $f \in M$ with $\mathrm{lpos}(f) = i$ whose leading monomial is minimal, for $i = 1, \ldots, \ell$. Then $B = \{f_{\min,1}, \ldots, f_{\min,\ell}\}$ forms a Gröbner basis of M, since any leading term of M is an element of the module generated by the leading terms of B. To see this, denote an arbitrary leading term of M by $c_i x^{[j_i]} e_i$ and $\mathrm{lt}(f_{\min,i}) = c_m x^{[j_m]} e_i$; then $j_i \geq j_m$ and

$$c_i x^{[j_i]} e_i = \left(\frac{c_i}{c_m^{[j_i - j_m]}} x^{[j_i - j_m]} \right) \circ \mathrm{lt}(f_{\min,i}).$$

Clearly, B is finite and the leading positions of all its elements are distinct. □

4 Conclusion

Gröbner bases for modules over $\mathbb{F}_q[x]$ are well-known and have been extensively studied. In this work we have translated some of the definitions and results of Gröbner bases from the polynomial ring $\mathbb{F}_q[x]$, equipped with multiplication, to the linearized polynomial ring $\mathcal{L}_q(x, q^m)$, equipped with composition. It turns out, that, despite the different operation used in the ring of linearized polynomials, all results covered in this work hold in both settings.

References

[1] W. W. Adams and P. Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1994.

[2] B. Buchberger. Gröbner bases: an introduction. In *Automata, languages and programming (Vienna, 1992)*, volume 623 of *Lecture Notes in Comput. Sci.*, pages 378–379. Springer, Berlin, 1992.

[3] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[4] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[5] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[6] M. Kuijper and K. Schindelar. Minimal Gröbner bases and the predictable leading monomial property. *Linear Algebra and its Applications*, 434(1):104–116, 2011.

[7] M. Kuijper and A.-L. Trautmann. Iterative list-decoding of Gabidulin codes via Gröbner based interpolation. In *arXiv:1405.7152 [cs.IT]*, 2014.

[8] M. Kuijper and A.-L. Trautmann. List decoding Gabidulin codes via interpolation and the Euclidean algorithm. In *arXiv:1404.5716 [cs.IT]*, 2014.

[9] M. Kuijper and A.-L. Trautmann. The predictable leading monomial property for linearized polynomials and Gabidulin list-decoding. In *preprint*, 2014.

[10] O. Ore. On a Special Class of Polynomials. *Transactions of the American Mathematical Society*, 35:559–584, 1933.