



HAL
open science

Skew Reed Muller codes

Willi Geiselmann, Félix Ulmer

► **To cite this version:**

| Willi Geiselmann, Félix Ulmer. Skew Reed Muller codes. 2017. hal-01633128v2

HAL Id: hal-01633128

<https://hal.science/hal-01633128v2>

Preprint submitted on 13 Nov 2017 (v2), last revised 24 Feb 2018 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Skew Reed Muller codes

Willi Geiselmann and Felix Ulmer

ABSTRACT. We extend the classical Reed Muller codes by using non commutative iterated skew polynomial rings instead of classical commutative polynomial rings. This involves the construction of iterated skew polynomial rings and the definition of the notion of points and evaluation at those points for iterated skew polynomials. Our approach is based on the notion of a left module Gröbner basis in iterated skew polynomial rings.

1. Introduction

Let A be a ring with an automorphism θ , then a θ -derivation is a map $\delta : A \rightarrow A$ such that $\delta(a + b) = \delta(a) + \delta(b)$ and $\delta(ab) = \delta(a)b + \theta(a)\delta(b)$ for all a and b in A . In the following we denote $A^\theta \subset A$ the fixed field of θ and we will also use the notation a^θ for $\theta(a)$ and a^δ for $\delta(a)$.

Consider a ring A , an automorphism θ of A and a θ -derivation on A . On the set $\{a_n X^n + \dots + a_1 X + a_0 \mid a_i \in A \text{ and } n \in \mathbb{N}\}$ we consider the usual addition of polynomials and define a multiplication by the basic rule $Xa = \theta(a)X + \delta(a)$ for $a \in \mathbb{F}_q$ and extend this rule to all elements of R by associativity and distributivity. This defines the skew polynomial ring $A[X; \theta, \delta]$ (see [8]). The classical commutative polynomial ring corresponds to A commutative, $\theta = \text{id}$ and $\delta : a \mapsto 0$. By repeating this construction we obtain the iterated skew polynomial ring $R_\ell = (\dots(A[X_1; \theta_1, \delta_1])\dots)[X_\ell; \theta_\ell, \delta_\ell]$ in ℓ variables over A , which we simply note $R_\ell = A[X_1; \theta_1, \delta_1][X_2; \theta_2, \delta_2] \dots [X_\ell; \theta_\ell, \delta_\ell]$.

For a finite field \mathbb{F}_q and an automorphism $\theta \in \text{Aut}(\mathbb{F}_q)$ the univariate skew polynomial ring $\mathbb{F}_q[X; \theta]$ is a left and right euclidean ring (see [8]). There exists two generalizations of Reed-Solomon codes (Reed-Muller codes in one variable) to skew polynomial rings:

- (1) In [2] the evaluation of a skew polynomial $f \in \mathbb{F}_q[X; \theta]$ at a point $b \in \mathbb{F}_q$ is defined as the remainder $f(b)$ of a right division $f = q(X - b) + f(b)$ of f by $X - b$ in $\mathbb{F}_q[X; \theta]$ (cf. [7]). This allows for a direct generalization of Reed-Solomon codes using univariate skew polynomial ring.
- (2) Consider $q = p^m$ and $\theta : \mathbb{F}_q \rightarrow \mathbb{F}_q; y \mapsto y^p$ the Frobenius morphism. The map $\varphi : \mathbb{F}_q[X; \theta] \rightarrow \text{End}(\mathbb{F}_q)$, $\sum_{i=0}^m a_i X^i \mapsto \sum_{i=0}^m a_i \theta^i$ is a ring morphism. One can define the evaluation of a skew polynomial $f \in \mathbb{F}_q[X; \theta]$ at a point $b \in \mathbb{F}_q$ as $\varphi(f)(b)$, which corresponds to the evaluation of the linearized

2000 *Mathematics Subject Classification*. Primary 94B, 16Z; Secondary 13P.
Key words and phrases. Linear codes, skew polynomial rings, Gröbner base.

polynomial $\sum_{i=0}^m a_i X^i$ at b . This evaluation code leads to ‘‘Gabidulin codes’’ [6].

In both skew Reed-Solomon codes the lengths of the resulting code is smaller than the length for the corresponding Reed-Solomon codes in the commutative case. For Gabidulin codes this follows from the fact that the solution space of an operator $\sum_{i=0}^m a_i \theta^i$ is a vector space over \mathbb{F}_p , therefore the evaluation points need to be linearly independent over \mathbb{F}_p . This reduces the number of possible evaluation points, i.e. the length of the code. The vector space structure of the solution of an operator $\sum_{i=0}^m a_i \theta^i$ is also the reason why the notion of a rank distance is more appropriated than the notion of a hamming distance, when dealing with Gabidulin codes. A futur projet will be to generalize the notion of rank distance for the codes presented in this paper.

The paper is organized in the following way: In the first section we give some constructions of iterated skew polynomial rings. We then give a definition for an evaluation of a multivariate skew polynomial using left module Gröbner basis computations. In the third section we define skew Reed-Muller codes and provide some examples. In section 4 we extend the notion of skew Reed-Muller code to skew polynomial rings over chain rings.

2. Iterated skew polynomial rings

The construction of iterated skew polynomial rings is a difficult problem because little is known on the automorphism ring and the derivations of

$$R_\ell = (\cdots (A[X_1; \theta_1, \delta_1]) \cdots)[X_\ell; \theta_\ell, \delta_\ell].$$

Classical examples are quantum Weyl algebras where the ground ring A is central ([5], section 2.3.3), iterated skew polynomial rings of derivation type ([11]) and iterated skew polynomial rings whose variables commute ([4]). None of those examples turned out to be sufficiently general. In this paper our examples will be build using inner automorphisms and inner derivatives.

EXAMPLE 2.1. Consider a ring A and an invertible element ν in A . Then $\theta_\nu^A : A \rightarrow A; a \mapsto \nu^{-1} a \nu$ is an inner automorphism of A . The automorphism θ_ν^A is the identity on A if and only if ν is a central invertible element in A .

EXAMPLE 2.2. Consider a ring A , an automorphism $\theta \in \text{Aut}(A)$ and an element $\beta \in A$. The map $\delta_\beta^{A, \theta} : A \rightarrow A; a \mapsto \beta a - a^\theta \beta$ is an inner θ -derivation on A .

It is well known that skew polynomial rings that differ by inner derivations or inner automorphisms are isomorphic (see [1]), which explains why many different rings will lead to equivalent codes. A more general family of skew polynomial rings would probably lead to better codes.

EXAMPLE 2.3. Consider $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, $\theta_1 : \mathbb{F}_4 \rightarrow \mathbb{F}_4; y \rightarrow y^2$ the Frobenius automorphisms. We give an example of in iterated skew polynomial ring over \mathbb{F}_4 constructed using inner automorphisms and inner derivations. The parameters used are random but meet the definition 3.2 allowing to later compute a Gröbner basis over this ring.

(1) In the ring $R_1 = \mathbb{F}_4[X_1; \theta, \delta_1^{\mathbb{F}_4, \theta}]$ we have the commutation relation

$$X_1 \alpha = \theta(\alpha) X_1 + \delta_1^{\mathbb{F}_4, \theta}(\alpha) = \alpha^2 X_1 + (1 \cdot \alpha - \theta(\alpha) \cdot 1) = \alpha^2 X_1 + 1.$$

(2) In the ring $R_2 = R_1[X_2; \theta_\alpha^{R_1}, \delta_{X_1+\alpha}^{R_1, \theta_\alpha^{R_1}}]$ we have the above commutation relation $X_1\alpha = \alpha^2X_1 + 1$ together with

$$\begin{aligned} X_2\alpha &= \theta_\alpha^{R_1}(\alpha)X_2 + \delta_{X_1+\alpha}^{R_1, \theta_\alpha^{R_1}}(\alpha) = \alpha X_2 + ((X_1 + \alpha)\alpha - \alpha^2(X_1 + \alpha)) \\ &= \alpha X_2 + X_1 + 1 \\ X_2X_1 &= \theta_\alpha^{R_1}(X_1)X_2 + \delta_{X_1+\alpha}^{R_1, \theta_\alpha^{R_1}}(X_1) \\ &= \alpha^2X_1\alpha X_2 + (X_1 + \alpha)\alpha - \alpha^2X_1\alpha(X_1 + \alpha) \\ &= \alpha^2X_1X_2 + \alpha X_2 + \alpha X_1^2 + \alpha X_1 \end{aligned}$$

(3) In the ring $R_3 = R_2[X_3; \theta_\alpha^{R_2}, \delta_{\alpha X_1}^{R_2, \theta_\alpha^{R_2}}]$ we have the above commutation relations together with

$$\begin{aligned} X_3\alpha &= \theta_\alpha^{R_2}(\alpha)X_3 + \delta_{\alpha X_1}^{R_2, \theta_\alpha^{R_2}}(\alpha) = \alpha X_3 + \alpha X_1 + \alpha \\ X_3X_1 &= \theta_\alpha^{R_2}(X_1)X_3 + \delta_{\alpha X_1}^{R_2, \theta_\alpha^{R_2}}(X_1) = \alpha^2X_1X_3 + \alpha X_3 \\ X_3X_2 &= \theta_\alpha^{R_2}(X_2)X_3 + \delta_{\alpha X_1}^{R_2, \theta_\alpha^{R_2}}(X_2) \\ &= X_2X_3 + (\alpha X_1 + \alpha)X_3 + (\alpha^2X_1 + \alpha^2)X_2 + \alpha^2X_1^2 + \alpha^2X_1 \end{aligned}$$

3. Left ideal Gröbner bases and skew Reed-Muller codes

In order to generalize Reed-Muller codes we need to define the evaluation of an element of an iterated skew polynomial ring. The evaluation of a classical polynomial $f \in \mathbb{F}_q[X_1, \dots, X_n]$ at the point $(\alpha_1, \dots, \alpha_n)$ can be seen as the remainder of successive divisions of f by $X_1 - \alpha_1, \dots, X_n - \alpha_n$, i.e.:

$$f = q_1(X_1 + \alpha_1) + \dots + q_n(X_n + \alpha_n) + f(\alpha_1, \dots, \alpha_n).$$

The result is independent of the order of the division, which corresponds to the fact that $\{X_1 - \alpha_1, \dots, X_n - \alpha_n\}$ is a Gröbner basis for the ideal generated by this set.

There exists several generalizations of the notion of Gröbner basis to various types of iterated skew polynomial rings in the literature.

We refer to [9] for the classical definition of a monomial ordering $<$ on \mathbb{N}^m . Classically a monomial ordering induces an ordering \prec on the set of monomials $\mathcal{M} = \{X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \dots X_m^{\alpha_m} \mid \alpha_i \in \mathbb{N}\}$ (note that the variables need to be in a precise order when dealing with a non commutative ring) via $X^\alpha \prec X^\beta$ if and only if $\alpha < \beta$. For any expression $f = \sum_{\alpha \in \mathbb{N}^m} c_\alpha X^\alpha$ where only finitely many constants c_α are nonzero, the monomial $X^\gamma = \max\{X^\alpha \mid c_\alpha \neq 0\}$ is called the leading monomial of f and c_α is called the leading coefficient of f , denoted respectively by $\text{lm}(f)$ and $\text{lc}(f)$. Then the least common multiple of X^α and X^β is defined as $\text{lcm}(X^\alpha, X^\beta) = X^\gamma$ where $\gamma_i = \max(\alpha_i, \beta_i)$. We will be interested in left ideals I of skew polynomial rings R

A Gröbner basis can be computed in Poincaré-Birkhoff-Witt extension (PBW) (see also [9], definition 1.2):

DEFINITION 3.1. (see [10], definition 3.2.1) Let A and R be two associative rings with $A \subset R$. The ring R is called a (finite) Poincaré-Birkhoff-Witt PBW extension (**PBW extension**) of A if there exist X_1, X_2, \dots, X_n in R such that

- (1) the monomials $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ form a base for R as a free left A -module, where i_1, \dots, i_n are in \mathbb{N} ;
- (2) $X_i a - a X_i = [X_i, a] \in A$ for each $i \in \{1, \dots, n\}$ and any $a \in A$;

(3) $X_i X_j - X_j X_i = [X_i, X_j] \in A + AX_1 + \dots + AX_n$ for all i, j in $\{1, \dots, n\}$.

We write $R = A \langle X_1, \dots, X_n \rangle$.

In [9, 10] algorithms are given for computing Gröbner bases of a left ideal I in solvable polynomial algebras and skew solvable polynomial rings. We will work with the following slight generalization of the last definition

DEFINITION 3.2. Let $R_\ell = (\dots A[X_1; \theta_1, \delta_1]) \dots [X_n; \theta_n, \delta_n]$ be an iterative skew polynomial ring in $n \in \mathbb{N}$. We call the ring **left-lex-solvable**, for the lexicographical order $1 \prec X_1 \prec \dots \prec X_n$, if

- (1) for any $a \in A$ and any $i \in \{1, \dots, n\}$, $X_i a = b X_i + p_{i,a}$ where $b \in A$ and $p_{i,a} \in R_{i-1}$;
- (2) for all $j < i$ in $\{1, \dots, n\}$, $X_i X_j = b X_j X_i + p_{i,j}$ where $b \in A$ and all monomials in $p_{i,j}$ are $\prec X_i X_j$.

Suppose now that R is a left-lex-solvable iterated polynomial ring in the (non commuting) variables X_1, \dots, X_m . We say that $X^\alpha \in \mathcal{M}$ is divisible by X^β if $X^\alpha = \text{lm}(X^\omega X^\beta)$ for some $X^\omega \in \mathcal{M}$ (note that $X^\omega X^\beta$ may no longer be a monomial, but that the non leading monomials of $X^\omega X^\beta$ are $\prec X^\alpha$).

We follow the definition of an S -polynomial of ([9], definition 2.5). If $X^\gamma = \text{lm}(\text{lcm}(X^\alpha X^\beta))$, $t_f = X^{\gamma-\alpha}$ and $t_g = X^{\gamma-\beta}$, then

$$\text{SPoly}(f, g) = t_f f - c t_g g, \text{ where } c = \frac{\text{lc}(t_f f)}{\text{lc}(t_g g)}$$

If the iterative skew polynomial ring R_ℓ is left-lex-solvable, then, according to ([9], section 2.2) the classical Buchberger algorithm, applied to the above S -polynomials using a lexicographic order $X_1 \prec \dots \prec X_\ell$, produces a left Gröbner basis of any left ideal $I \subset R$. For a given Gröbner basis G of a left ideal $I \subset R$ we denote $\text{rem}(f, G)$ the unique polynomial $r \in R$ in the decomposition $f = (\sum_j q_j \cdot g_i) + r$.

DEFINITION 3.3. Let F be a field, R an left-finitely generated algebra over F and \prec an admissible ordering on R . We call a left Gröbner basis $\mathcal{B}_I = \{g_1, \dots, g_k\}$ of a left ideal $I \subset R$ an evaluation base if

- (1) $I = (g_1, \dots, g_k) \neq \{1\}$ (we exclude the “always zero” evaluation which is of no interest for Reed-Muller type codes).
- (2) the right reduction $f = \text{rem}(f, \mathcal{B}_I)$ of any $f \in R$ by \mathcal{B}_I belongs to F .

PROPOSITION 3.4. Let F be a field, R a skew solvable polynomial ring over F generated by X_1, \dots, X_n and \prec an admissible monomial ordering. If the ordering \prec is a well ordering, then any reduced evaluation base \mathcal{B}_I is of the form

$$(X_1 - \alpha_1, X_2 - \alpha_2, \dots, X_n - \alpha_n)$$

where $\alpha_i \in F$.

PROOF. For an evaluation base \mathcal{B}_I each generator X_i must reduce to $\alpha_i \in F$: $X_i = (\sum_{g_i \in \mathcal{B}_I} h_i g_i) + \alpha_i \in F$. Therefore $X_i - \alpha_i = (\sum_{g_i \in \mathcal{B}_I} h_i g_i) \in I$. Assume that $X_1 \prec \dots \prec X_n$ and proceed by induction on i :

- (1) Since \prec is a well ordering and $1 \notin \mathcal{B}_I$, the monomial X_1 is minimal among the leading monomials in \mathcal{B}_I and therefore $X_1 - \alpha_1$ must belong to the Gröbner basis \mathcal{B}_I .

- (2) Suppose that $X_1 - \alpha_1, \dots, X_i - \alpha_i$ belongs to \mathcal{B}_I . A reduced evaluation base \mathcal{B}_I cannot contain any other monomial divisible by X_1, \dots, X_i , and X_{i+1} is a minimal leading monomial among the other polynomials of \mathcal{B}_I . Suppose that $X_j \in \{X_1, \dots, X_i\}$ divides the monomial X_{i+1} , then $X_{i+1} = MX_i$ for some monomial M which must contain a variable in $\{X_{i+1}, \dots, X_n\}$. Reordering the variables in MX_i we obtain a leading term containing X_i and therefore a contradiction. Therefore $X_{i+1} - \alpha_{i+1}$ belongs to \mathcal{B}_I .

Therefore \mathcal{B}_I contains $X_1 - \alpha_1, \dots, X_n - \alpha_n$. Since the base is reduced it can only contain those polynomials, showing that for a lexicographic order a reduced Gröbner basis of an evaluation ideal is always of the form $(X_1 - \alpha_1, X_2 - \alpha_2, \dots, X_n - \alpha_n)$. \square

EXAMPLE 3.5. In example 2.3 we constructed the iterate skew polynomial ring

$$R_3 = \mathbb{F}_4[X_1; \theta, \delta_1^{\mathbb{F}_4, \theta}][X_2; \theta_\alpha^{R_1}, \delta_{X_1 + \alpha}^{R_1, \theta_\alpha^{R_1}}][X_3; \theta_\alpha^{R_2}, \delta_{\alpha X_1}^{R_2, \theta_\alpha^{R_2}}]$$

For this ring and the lexicographic order $X_3 > X_2 > X_1$ only 28 ideals of the form $(X_1 - \alpha_1, X_2 - \alpha_2, X_3 - \alpha_3)$ are distinct from $(1) = R_3$. For example (X_1, X_2, X_3) is a Gröbner basis, but for $(X_1, X_2, X_3 - 1)$ the Gröbner basis turns out to be (1) since $(\alpha^2 X_3 + \alpha)X_1 + (\alpha X_1 + 1)(X_3 - 1) = 1$.

DEFINITION 3.6. \mathbb{F}_q Consider an iterated skew polynomial ring

$$R_\ell = \mathbb{F}_q[X_1; \theta_1, \delta_1][X_2; \theta_2, \delta_2] \dots [X_\ell; \theta_\ell, \delta_\ell]$$

over a finite field \mathbb{F}_q , and $<$ an admissible ordering on R and a list $\mathcal{B}_{I_1}, \dots, \mathcal{B}_{I_n}$ of Gröbner basis I which are evaluation bases for R_ℓ . If the space W of polynomials of order less than a given bound is of dimension r , then a **skew Reed Muller encoding** of length n of $f \in W$ is given by

$$(\text{red}(f, \mathcal{B}_{I_1}), \dots, \text{red}(f, \mathcal{B}_{I_n})) \in \mathbb{F}_q^n.$$

The resulting code is a linear code with parameters $[n, r]$

In order to verify that this gives an \mathbb{F}_q -linear code we need to show that

$$\mathcal{C} = \{(\text{rem}(f, \mathcal{B}_{I_1}), \dots, \text{rem}(f, \mathcal{B}_{I_n})) \mid f \in W\}$$

is a subspace of \mathbb{F}_q^n . In order to see this we note that for all s in $\{1, \dots, \ell\}$, for all f in R_ℓ with $f = (\sum_{g_i \in \mathcal{B}_{I_s}} h_i g_i) + \text{rem}(\tilde{f}, \mathcal{B}_{I_s})$, all \tilde{f} in R_ℓ with $\tilde{f} = (\sum_{g_i \in \mathcal{B}_{I_s}} \tilde{h}_i g_i) + \text{rem}(\tilde{f}, \mathcal{B}_{I_s})$ and all λ in \mathbb{F}_q we have:

$$(3.1) \quad \lambda f = \left(\sum_{g_i \in \mathcal{B}_{I_s}} \lambda h_i g_i \right) + \lambda \cdot \text{rem}(f, \mathcal{B}_{I_s})$$

$$(3.2) \quad \tilde{f} + f = \left(\sum_{g_i \in \mathcal{B}_{I_s}} (\tilde{h}_i + h_i) g_i \right) + \text{rem}(\tilde{f}, \mathcal{B}_{I_s}) + \text{rem}(f, \mathcal{B}_{I_s}).$$

The result now follows from the uniqueness of the reduction by a Gröbner basis. We note that, even if the evaluation map is a ring homomorphism

$$R_\ell \rightarrow \mathbb{F}_q; f \mapsto \text{rem}(\tilde{f}, \mathcal{B}_{I_s}),$$

the fact that we obtain a linear code over \mathbb{F}_q relies only on the fact that the map $R_\ell \rightarrow \mathbb{F}_q; f \mapsto \text{rem}(\tilde{f}, \mathcal{B}_{I_s})$ is an \mathbb{F}_q -linear map.

EXAMPLE 3.7. In example 2.3 we constructed the iterate skew polynomial ring

$$R_3 = \mathbb{F}_4[X_1; \theta, \delta_1^{\mathbb{F}_4, \theta}][X_2; \theta_\alpha^{R_1}, \delta_{X_1+\alpha}^{R_1, \theta_\alpha^{R_1}}][X_3; \theta_\alpha^{R_2}, \delta_{\alpha X_1}^{R_2, \theta_\alpha^{R_2}}]$$

While classical Reed-Muller codes are of length 64, for this ring and the lexicographic order $X_3 > X_2 > X_1$ we obtain 28 evaluation points with Gröbner bases of the form $(X_1 - \alpha_1, X_2 - \alpha_2, X_3 - \alpha_3)$ distinct from $(1) = R_3$ (the indicated distance is the hamming distance):

- (1) Considering the vector space of all polynomials of degree 1 we obtain a $[28, 4, 12]_4$.
- (2) Considering the vector space of all polynomials of degree 2 we obtain a $[28, 10, 6]_4$.
- (3) Considering the vector space of all polynomials of degree 3 we obtain a $[28, 17, 3]_4$.

4. Skew Reed-Muller codes over finite chain rings

In order to define skew Reed-Muller codes over finite chain rings we need to define the notion of a Gröbner basis to finite chain rings. We do that by following [3]. In a finite chain ring A the unique maximal ideal is generated by an element ω of nilpotency index ℓ (i.e. ℓ is the smallest integer such that $\omega^\ell = 0$) any element a can be written in the form $\mu_a \omega^{\ell_a}$ where $0 \leq \ell_a \leq \ell - 1$ and μ_a is a invertible element of A , unique modulo $\omega^{\ell - \ell_a}$.

EXAMPLE 4.1. The ring $A = \mathbb{F}_4[z]/(z^2)$ is a chain ring of order 16. The unique maximal ideal of A is (z) whose nilpotency index is $\ell = 2$. The invertible elements of A are

$$\{\alpha, z + \alpha, \alpha z + \alpha, \alpha^2 z + \alpha, 1, z + 1, \alpha z + 1, \alpha^2 z + 1, \alpha^2, z + \alpha^2, \alpha z + \alpha^2, \alpha^2 z + \alpha^2\}$$

We can construct an iterated skew polynomial ring using inner automorphisms and inner derivations in the same way than in example 2.3. Two simple examples that we will use later are

- (1) The ring homomorphism $\theta_3 : A \rightarrow A$ defined by $a \mapsto a$ and $z \mapsto \alpha^2 z$ is an automorphism of order 3 of A . In the ring $R_{2,3} = A[X_1; \theta_3][X_2]$ we have the commutation relation

$$X_1 \alpha = \theta_3(\alpha) X_1 = \alpha X_1; X_1 z = \theta_3(z) X_1 = \alpha^2 z X_1$$

and X_2 is a central element.

- (2) The ring homomorphism $\theta_2 : A \rightarrow A$ defined by $a \mapsto a^2$ and $z \mapsto \alpha z$ is an automorphism of order 2 of A . In the ring $R_{2,2} = A[X_1; \theta][X_2]$ we have the commutation relation

$$X_1 \alpha = \theta_2(\alpha) X_1 = \alpha^2 X_1; X_1 z = \theta_2(z) X_1 = \alpha z X_1$$

and X_2 is a central element.

We follow the definition of an S -polynomial in ([3], definition 3.4). Suppose now that R is a left-lex-solvable iterated polynomial ring in the (non commutating) variables $X_1 \dots, X_m$ over a finite commutative chain ring A . Recall that $\text{lcm}(X^\alpha, X^\beta) = X^\gamma$ where $\gamma_i = \max(\alpha_i, \beta_i)$ and that $X^\alpha \in \mathcal{M}$ is divisible by X^β if $X^\alpha = \text{lm}(X^\omega X^\beta)$ for some $X^\omega \in \mathcal{M}$ (note that the product of monomial $X^\omega X^\beta$ may no longer be a monomial, but that the non leading monomials of $X^\omega X^\beta$ are $\prec X^\alpha$ in a left-lex-solvable iterated polynomial ring).

Adapting ([3], definition 3.2) to the non commutative situation we define that the polynomial g reduces the monomial $\mu_f \omega^{\ell_f} X^\alpha$ if

- (1) $\text{lm}(g) = X^\beta$ with $\beta < \alpha$.
- (2) if $\text{lc}(X^{\alpha-\beta}g) = \mu_g \omega^{\ell_g}$ with $\ell_g < \ell_f$.

The corresponding reduction step is the result of

$$\mu_f \omega^{\ell_f} X^\alpha - \mu_f \mu_g^{-1} \omega^{\ell_f - \ell_g} X^{\alpha - \beta} g$$

We say that a polynomial g reduces a polynomial f if g reduces $\text{lt}(f)$.

Let f and g be two non zero polynomials whose leading monomials are X^α and X^β . If $X^\gamma = \text{lm}(\text{lcm}(X^\alpha, X^\beta))$, $a_f = \text{lc}(X^{\gamma-\alpha}f) = \mu_f \omega^{\ell_f}$, $b_g = \text{lc}(X^{\gamma-\beta}g) = \mu_g \omega^{\ell_g}$ and $\ell_{f,g} = \max\{\ell_f, \ell_g\}$. We follow the definition of an S -polynomial of ([3], definition 3.4):

$$\text{SPoly}(f, g) = \mu_f^{-1} \omega^{\ell_{f,g} - \ell_f} X^{\gamma - \alpha} f - \mu_g^{-1} \omega^{\ell_{f,g} - \ell_g} X^{\gamma - \beta} g$$

According to [3] we also need the notion of an A -polynomial. Consider f with $\text{lc}(f) = \mu_a \omega^{\ell_a}$ with $\ell_a > 0$ (i.e. a non invertible zero divisor):

$$\text{APoly}(f) = \omega^{\ell - \ell_a} f$$

A base of an ideal is a Gröbner basis if all S -polynomials between the elements of the base and all A -polynomials of the elements of the base reduce to zero.

Similarly to $\mathbb{Z}[X]$ where $(X, 2)$ is a maximal ideal, the maximal ideals in an iterated skew polynomial ring are no longer all of the form $(X_1 - \alpha_1, \dots, X_\ell - \alpha_\ell)$.

EXAMPLE 4.2. Consider $A = \mathbb{F}_4[z]/(z^2)$ and $R_{2,2} = A[X_1; \theta_2][X_2]$ as defined in example 4.1. With lex order $X_2 > X_1$ there are 88 evaluation points with Gröbner bases of the form $(X_1 - \alpha_1, X_2 - \alpha_2)$ and 12 additional evaluation points with Gröbner bases $(X_1 - \alpha_1, X_2 - \alpha_2, z)$. For example the Gröbner basis of $(X_1 - 1, X_2 - z)$ is $(X_1 - 1, X_2, z)$.

Using only the 88 evaluation points whose Gröbner bases are of the special form $(X_1 - \alpha_1, X_2 - \alpha_2)$ we obtain the following skew Reed-Muller codes (the indicated distance is the hamming distance):

- (1) Considering the left A -module of all polynomials of degree 1 we obtain a $[88, 3]$ code over A which maps, using the mapping $A \rightarrow \mathbb{F}_4^2$ given by $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$, to a $[176, 6, 88]_4$ code.
- (2) Considering the left A -module of all polynomials of degree 2 we obtain a $[88, 6]$ code over A which maps to a $[176, 12, 16]_4$ code.
- (3) Considering the left A -module of all polynomials of degree 3 we obtain a $[88, 9]$ code over A which maps to a $[176, 18, 8]_4$ code.

Using all 96 evaluation points, including those with Gröbner bases of the form $(X_1 - \alpha_1, X_2 - \alpha_2, z)$ we obtain the following skew Reed-Muller codes (the indicated distance is the hamming distance):

- (1) Considering the left A -module of all polynomials of degree 1 we obtain a $[96, 3]$ code over A which maps, under the above mapping, to a $[192, 6, 96]_4$ code.
- (2) Considering the left A -module of all polynomials of degree 2 we obtain a $[96, 6]$ code over A which maps to a $[192, 12, 16]_4$ code.
- (3) Considering the left A -module of all polynomials of degree 3 we obtain a $[96, 9]$ code over A which maps to a $[192, 18, 8]_4$ code.

EXAMPLE 4.3. Consider $A = \mathbb{F}_4[z]/(z^2)$ and $R_{2,3} = A[X_1; \theta_3][X_2]$ as defined in example 4.1. With lex order $X_2 > X_1$ there are 112 evaluation points with Gröbner basis of the form $(X_1 - \alpha_1, X_2 - \alpha_2)$ and 12 additional evaluation points with Gröbner bases of the form $(X_1 - \alpha_1, X_2 - \alpha_2, z)$. For example the points $(X_1 - a, X_2 - a, z)$ or $(X_1 - 1, X_2, z)$. Using only the 112 evaluation points with Gröbner bases of the form $(X_1 - \alpha_1, X_2 - \alpha_2)$ we obtain the following skew Reed-Muller codes (the indicated distance is the hamming distance):

- (1) Considering the vector space of all polynomials of degree 1 we obtain a $[112, 3]$ code over A which, under the mapping $A \rightarrow \mathbb{F}_4^2$ with $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$, map to a $[224, 6, 96]_4$ code.
- (2) Considering the vector space of all polynomials of degree 2 we obtain a $[112, 6]$ code over A which under the mapping $A \rightarrow \mathbb{F}_4^2$ with $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$, map to a $[224, 12, 64]_4$ code.
- (3) Considering the vector space of all polynomials of degree 3 we obtain a $[112, 10]$ code over A which under the mapping $A \rightarrow \mathbb{F}_4^2$ with $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$, map to a $[224, 20, 32]_4$ code.

References

- [1] Abramov, S.A., Le H.Q., and Li Z., *Univariate Ore polynomial rings in computer algebra*, Journal of Mathematical Sciences, Vol. 131, No. 5 (2005)
- [2] D. Boucher and F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Designs, Codes and Cryptography, 70, 405–431 (2014)
- [3] Hashemi, A. and Alvandi, *Applying Buchberger’s criteria for computing Gröbner bases over finite-chain rings*, Journal of Algebra and Its Applications, 12 (2013)
- [4] L. Chaussade, *Codes correcteurs avec les polynômes tordus*, Thèse Université de Rennes 1, novembre 2010.
- [5] F. Dumas, *An introduction to noncommutative polynomial invariants*, CIMPA course “Homological methods and representations of non-commutative algebras”, Argentina, 2006
- [6] E.M. Gabidulin (1985), Theory of codes with maximum rank distance, *Probl. Peredach. Inform.*, **21**, 3–16 (in Russian; pp. 1–12 in the English translation).
- [7] T.Y. Lam and A. Leroy, Vandermonde and Wronskian Matrices over Division Rings, *Journal of Algebra*, **119** pp. 308-336 (1988)
- [8] O. Ore, Theory of Non-Commutative Polynomials, *The Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp 480-508 (1933)
- [9] X. Zhao and Y. Zhang, *A signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings*, Open Mathematics. Volume 13, Issue 1, ISSN (Online) 2391-5455, DOI: 10.1515/math-2015-0028, May 2015
- [10] Yang Zhang, *Algorithms for Noncommutative Differential Operators*, PhD University of Western Ontario, 2004.
- [11] Voskoglou, M. Gr, *Derivations and Iterated Skew Polynomial Rings*, International journal of applied mathematics and informatics, Issue 2, Volume 5, 2011

WILLI GEISELMANN, KIT, INSTITUT FÜR THEORETISCHE INFORMATIK (ITI), AM FASANENGARTEN 5, D-76131 KARLSRUHE

E-mail address: willi.geiselmann@kit.edu

FELIX ULMER, UNIV RENNES, CNRS, IRMAR - UMR 6625, F-35000 RENNES, FRANCE

E-mail address: felix.ulmer@univ-rennes1.fr