Skew Reed Muller codes

Willi Geiselmann, Félix Ulmer

Skew Reed-Muller Codes

Willi Geiselmann* and Felix Ulmer†

February 24, 2018

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 and θ an automorphism of A. A ***θ-derivation*** is a map $\delta : A \to A$ 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 by $A^\theta \subset A$ 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 $\{a_n X^n + \ldots + a_1 X + a_0 \,|\, a_i \in A \text{ and } n \in \mathbb{N}\}$ we consider the usual addition of polynomials and define a multiplication by the basic rule $X\,a = \theta(a)\,X + \delta(a)$ 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 [9]). The classical commutative polynomial ring corresponds to A commutative, $\theta = \mathrm{id}$ and $\delta : a \mapsto 0$. By repeating this construction we obtain the ***iterated skew polynomial ring*** $R_\ell = (\cdots(A[X_1;\theta_1,\delta_1])\ldots)[X_\ell;\theta_\ell,\delta_\ell]$ in ℓ variables over A, which we simply note $R_\ell = A[X_1;\theta_1,\delta_1][X_2;\theta_2,\delta_2]\ldots[X_\ell;\theta_\ell,\delta_\ell]$. For a finite field $\mathbb{F}_q$ and an automorphism $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ the univariate skew polynomial ring $\mathbb{F}_q[X;\theta]$ is a left and right euclidean ring (see [9]).

Definition 1.1 *A **code** $\mathcal{C}$ of length $n \in \mathbb{N}$ over a finite commutative ring A is a nonempty subset of A^n. The elements of $\mathcal{C}$ are called codewords. The code $\mathcal{C}$ is a **linear code** if it is an A-submodule of A^n. If A is a finite field $\mathbb{F}_q$, then a linear code of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_q^n$. The **Hamming distance** between two vectors of $\mathbb{F}_q^n$ is defined as the number of coordinates at which the two vectors differ. The **minimal distance** d of a k-dimensional linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is defined to be the minimum Hamming distance between two distinct codewords of $\mathcal{C}$. In this case we say that $\mathcal{C}$ is a code with **parameters** $[n,k,d]_q$.*

*KIT, Institut für Theoretische Informatik (ITI), Am Fasanengarten 5, D-76131 Karlsruhe

†IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

The ***Reed-Solomon codes*** over $\mathbb{F}_q$ that we will now define are examples of ***algebraic codes***, whose construction and properties result from the algebraic structure of the code. Reed-Solomon codes are constructed using evaluation of polynomials in $\mathbb{F}_q[X]$. In order to construct a Reed-Solomon code $\mathcal{C} \subset \mathbb{F}_q^n$ with parameters $[n, k, n-k+1]_q$ (where $n \leq q$) we start with the k-dimensional space of polynomials $\sum_{i=0}^{k-1} b_i X^i \in \mathbb{F}_q[X]$ of degree $< k$ and n distinct elements $\alpha_1, \ldots, \alpha_n$ of $\mathbb{F}_q$. The encoding of the message $(b_0, b_1 \ldots, b_{k-1})$ of length k corresponding to the polynomial $f = \sum_{i=0}^{k-1} b_i$ is the vector $(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \in \mathcal{C} \subset \mathbb{F}_q^n$. The minimal distance of this code is known to be best possible and the algebraic structure of the code can be used to efficiently correct up to $< \frac{n-k+1}{2}$ transmission errors. Note that the length of a Reed-Solomon code is bounded by the size q of the alphabet $\mathbb{F}_q$.

There exist two generalizations of Reed-Solomon codes to skew polynomial rings:

1. In [3] 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. [8]). This allows for a direct generalization of Reed-Solomon codes using univariate skew polynomial rings.

2. Consider $q = p^m$ and $\theta : \mathbb{F}_q \to \mathbb{F}_q; y \mapsto y^p$ the Frobenius morphism. The map $\varphi : \mathbb{F}_q[X;\theta] \to \mathrm{End}(\mathbb{F}_q)$, $\sum_{i=0}^{m} a_i X^i \mapsto \sum_{i=0}^{m} a_i \theta^i$ 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 polynomial $\sum_{i=0}^{m} a_i X^{q^i}$ at b. This evaluation leads to "Gabidulin codes" [7].

In both generalizations of Reed-Solomon codes the length 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 future project will be to generalize the notion of rank distance for the codes presented in this paper.

Reed-Muller codes are based on the evaluation of multivariate polynomials. A polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_\ell]$ of total degree $s < q-1$ contains $k = \binom{\ell+s}{s}$ coefficients $(b_0, \ldots, b_{k-1})$. In order to construct a Reed-Muller code $\mathcal{C} \subset \mathbb{F}_q^n$ we choose $n \leq q^\ell$ points $a_i = (\alpha_{i,1}, \ldots, \alpha_{i,\ell}) \in \mathbb{F}_q^\ell$. The encoding of the message $(b_0, b_1 \ldots, b_{k-1})$ of length k corresponding to the polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_\ell]$ is the vector $(f(a_1), f(a_2), \ldots, f(a_n)) \in \mathcal{C} \subset \mathbb{F}_q^n$. Reed-Muller codes, unlike Reed-Solomon codes, are not optimal with respect to the minimal distance. However, the maximal length of the code is $n = q^\ell$, so that the alphabet size q can be exponentially smaller than the length of the code.

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 about the automorphism ring and the derivations of

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

Classical examples are quantum Weyl algebras where the ground ring A is central ([6], Section 2.3.3), iterated skew polynomial rings of derivation type ([12]) and iterated skew polynomial rings whose variables commute ([5]). None of those examples turned out to be sufficiently general. In this paper, our examples will be built using inner automorphisms and inner derivations.

Example 2.1 *Consider a ring A and an invertible element ν in A. Then $\theta_\nu^A : A \to A; a \mapsto \nu^{-1}a\nu$ 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 $\theta \in \mathrm{Aut}(A)$ and an element $\beta \in A$. The map $\delta_\beta^{A,\theta} : A \to A; a \mapsto \beta a - a^\theta \beta$ 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 rings that differ by inner derivations or inner automorphisms will often lead to equivalent codes. A more general family of skew polynomial rings would probably lead to better codes.

Example 2.3 *Consider $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, $\theta_1 : \mathbb{F}_4 \to \mathbb{F}_4; y \to y^2$ 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 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 $X_1\alpha = \alpha^2 X_1 + 1$ together with*

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

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*

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

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 $f \in \mathbb{F}_q[X_1, \ldots, X_\ell]$ at the point $(\alpha_1, \ldots, \alpha_\ell)$ can be seen as the remainder of successive divisions of f by $X_1 - \alpha_1, \ldots, X_\ell - \alpha_\ell$, i.e.:

$$f = q_1(X_1 - \alpha_1) + \ldots + q_\ell(X_\ell - \alpha_\ell) + f(\alpha_1, \ldots, \alpha_\ell).$$

The result is independent of the order of the division, which corresponds to the fact that $\{X_1 - \alpha_1, \ldots, X_\ell - \alpha_\ell\}$ is a ***Gröbner basis*** for the ideal generated by this set. We refer to [2] for the definition of a Gröbner basis and a ***reduced Gröbner basis***.

There exist several generalizations of the notion of Gröbner basis to various types of iterated skew polynomial rings in the literature [10, 11].

We refer to [10] 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 $\mathcal{M} = \{X^\alpha = X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_m^{\alpha_m} \mid \alpha_i \in \mathbb{N}\}$ (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 $X^\gamma = \max\{X^\alpha | c_\alpha \neq 0\}$ is the ***leading monomial*** of $f$and c_α is the ***leading coefficient*** of f, denoted respectively by $\mathrm{lm}(f)$ and $\mathrm{lc}(f)$. Then the least common multiple of X^α and X^β is defined as $\mathrm{lcm}(X^\alpha, X^\beta) = X^\gamma$ where $\gamma_i = \max(\alpha_i, \beta_i)$. We will be interested in left ideals I of skew polynomial rings $R_\ell = A[X_1; \theta_1, \delta_1][X_2; \theta_2, \delta_2]\ldots[X_\ell; \theta_\ell, \delta_\ell]$.

A Gröbner basis can be computed in a Poincaré-Birkhoff-Witt extension (PBW) (see also [10], Definition 1.2):

Definition 3.1 *(see [11], Definition 3.2.1) Let A and B be two associative rings with $A \subset B$. The ring B is called a (finite) Poincaré-Birkhoff-Witt PBW extension* **(PBW extension)** *of A if there exist $X_1, X_2, \ldots, X_\ell$ in B such that*

1. *the monomials $X_1^{i_1}X_2^{i_1}\cdots X_\ell^{i_\ell}$ form a basis for B as a free left A-module, where $i_1, \ldots, i_\ell$ are in $\mathbb{N}$;*
2. *$X_ia - aX_i = [X_i, a] \in A$ for each $i \in \{1, \ldots, n\}$ and any $a \in A$;*
3. *$X_iX_j - X_jX_i = [X_i, X_j] \in A + AX_1 + \cdots + AX_\ell$ for all i, j in $\{1, \ldots, n\}$.*

We write $B = A\langle X_1, \ldots, X_\ell\rangle$.

In [10, 11] 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 $R_\ell = (\cdots A[X_1;\theta_1,\delta_1])\ldots)[X_\ell;\theta_\ell,\delta_\ell]$ be an iterative skew polynomial ring in $n \in \mathbb{N}$. We call the ring **left-lex-solvable**, for the lexicographical order $1 \prec X_1 \prec \ldots \prec X_\ell$, if*

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

Suppose now that R_ℓ is a left-lex-solvable iterated skew polynomial ring in the (non commuting) variables $X_1 \ldots, X_m$. We say that $X^\alpha \in \mathcal{M}$ is divisible by X^β if $X^\alpha = \mathrm{lm}(X^\omega X^\beta)$ 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*** given in ([10], Definition 2.5). If $X^\gamma = \mathrm{lm}(\mathrm{lcm}(X^\alpha X^\beta))$, $t_f = X^{\gamma-\alpha}$ and $t_g = X^{\gamma-\beta}$, then

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

If the iterative skew polynomial ring R_ℓ is left-lex-solvable, then, according to ([10], Section 2.2) the classical Buchberger algorithm, applied to the above S-polynomials using a lexicographic order $X_1 \prec \ldots \prec X_\ell$, produces a left Gröbner basis of any left ideal $I \subset_\ell$. For a given Gröbner basis $G = \{g_1,\ldots,g_s\}$ of a left ideal $I \subset R_\ell$, the ***right reduction*** of f by G is the unique polynomial $\overline{f}^G \in R_\ell$ in the decomposition $f = \left(\sum_{j=1}^s q_j \cdot g_i\right) + \overline{f}^G$ with the property that no leading monomial of any $g_i \in G$ divides any monomial of $\overline{f}^G$.

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

1. *$I = (g_1,\ldots,g_s) \neq \{1\}$ (we exclude the "always zero" evaluation which is of no interest for Reed-Muller type codes).*
2. *the right reduction $\overline{f}^{\mathcal{B}_I}$ of any $f \in B$ by $\mathcal{B}_I$ belongs to F.*

Proposition 3.4 *Let F be a field, R_ℓ a left-lex-solvable skew polynomial ring over F generated by $X_1,\ldots,X_\ell$ and $\prec$ an admissible monomial ordering. If the ordering $\prec$ is a well ordering, then any reduced evaluation basis $\mathcal{B}_I$ is of the form*

$$\{X_1 - \alpha_1, X_2 - \alpha_2, \ldots, X_\ell - \alpha_\ell\}$$

where $\alpha_i \in F$.

Proof. For an evaluation basis $\mathcal{B}_I$ 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 $X_i - \alpha_i = (\sum_{g_i \in \mathcal{B}_I} h_i g_i) \in I$. We suppose that $X_1 \prec \cdots \prec X_\ell$ 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 $X_1 - \alpha_1, \ldots X_i - \alpha_i$ belongs to $\mathcal{B}_I$. A reduced evaluation basis $\mathcal{B}_I$ cannot contain any other monomial divisible by $X_1, \ldots, X_i$, and X_{i+1} is a minimal leading monomial among the other polynomials of $\mathcal{B}_I$. Suppose that $X_j \in \{X_1, \ldots, X_i\}$ divides the monomial X_{i+1}, then $X_{i+1} = MX_j$ for some monomial M which must contain a variable in $\{X_{i+1}, \ldots, X_\ell\}$. Reordering the variables in MX_j using (2) in Definition 3.2, we obtain a leading term containing X_j and therefore a contradiction. As a result, $X_{i+1} - \alpha_{i+1}$ belongs to $\mathcal{B}_I$.

Therefore $\mathcal{B}_I$ contains $X_1 - \alpha_1, \ldots, X_\ell - \alpha_\ell$. Since the basis 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 $(X_1 - \alpha_1, X_2 - \alpha_2, \ldots, X_\ell - \alpha_\ell)$. ∎

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*

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

over a finite field $\mathbb{F}_q$, and $\prec$ an admissible monomial ordering on R and a list $\mathcal{B}_{I_1}, \ldots, \mathcal{B}_{I_n}$ of Gröbner bases which are evaluation bases for R_ℓ over $\mathbb{F}_q$. If an $\mathbb{F}_q$-subspace W of polynomials of R_ℓ is of dimension k, then a ***skew Reed-Muller encoding*** *of length n of $f \in W$ is given by*

$$\left(\overline{f}^{\mathcal{B}_{I_1}}, \ldots, \overline{f}^{\mathcal{B}_{I_n}}\right) \in \mathbb{F}_q^n.$$

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

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

$$\mathcal{C} = \left\{ \left(\overline{f}^{\mathcal{B}_{I_1}}, \ldots, \overline{f}^{\mathcal{B}_{I_n}}\right) \mid f \in W \right\}$$

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

$$\lambda f = (\sum_{g_i \in \mathcal{B}_{I_s}} \lambda h_i g_i) + \lambda \cdot \overline{f}^{\mathcal{B}_{I_s}} \quad (1)$$

$$\tilde{f} + f = (\sum_{g_i \in \mathcal{B}_{I_s}} (\tilde{h}_i + h_i) g_i) + \overline{\tilde{f}}^{\mathcal{B}_{I_s}} + \overline{f}^{\mathcal{B}_{I_s}}. \quad (2)$$

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

$$R_\ell \to \mathbb{F}_q; f \mapsto \overline{f}^{\mathcal{B}_{I_s}},$$

the fact that we obtain a linear code over $\mathbb{F}_q$ relies only on the fact that the map $R_\ell \to \mathbb{F}_q; f \mapsto \overline{f}^{\mathcal{B}_{I_s}}$ 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

A finite commutative ring with identity $1 \neq 0$ is called a ***finite chain ring*** if its ideals are linearly ordered by inclusion. 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 [4]. In a finite chain ring A the unique maximal ideal is generated by an element ω of nilpotency index m (i.e. m is the smallest integer such that $\omega^m = 0$) any element a can be written in the form $\mu_a \omega^{m_a}$ where $0 \leq m_a \leq m-1$ and μ_a is a invertible element of A, unique modulo ω^{m-m_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 $m = 2$. 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 $\theta_3 : A \to A$ 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 $\theta_2 : A \to A$ 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 ([4], Definition 3.4). Suppose now that R is a left-lex-solvable iterated polynomial ring in the (non commuting) variables $X_1 \ldots, X_m$ over a finite commutative chain ring A. Recall that $\mathrm{lcm}(X^\alpha, X^\beta) = X^\gamma$ where $\gamma_i = \max(\alpha_i, \beta_i)$ and that $X^\alpha \in \mathcal{M}$ is divisible by X^β if $X^\alpha = \mathrm{lm}(X^\omega X^\beta)$ 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 ([4], Definition 3.2) to the non-commutative situation we define that the polynomial g ***reduces*** the monomial $\mu_f \omega^{m_f} X^\alpha$ if

1. $\mathrm{lm}(g) = X^\beta$ with $\beta < \alpha$;
2. if $\mathrm{lc}(X^{\alpha-\beta} g) = \mu_g \omega^{m_g}$ with $m_g < m_f$.

The corresponding reduction step is the result of

$$\mu_f \omega^{m_f} X^\alpha - \mu_f \mu_g^{-1} \omega^{m_f - m_g} X^{\alpha-\beta} g.$$

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

Let f and g be two non zero polynomials whose leading monomials are X^α and X^β. If $X^\gamma = \mathrm{lm}(\mathrm{lcm}(X^\alpha, X^\beta))$, $a_f = \mathrm{lc}(X^{\gamma-\alpha} f) = \mu_f \omega^{m_f}$, $b_g = \mathrm{lc}(X^{\gamma-\beta} g) = \mu_g \omega^{m_g}$ and $m_{f,g} = \max\{m_f, m_g\}$. We follow the definition of an S-polynomial of ([4], Definition 3.4):

$$\mathrm{SPoly}(f, g) = \mu_f^{-1} \omega^{m_{f,g} - m_f} X^{\gamma-\alpha} f - {\mu_g}^{-1} \omega^{m_{f,g} - m_g} X^{\gamma-\beta} g.$$

According to [4] we also need the notion of an ***A-polynomial***. Consider f with $\mathrm{lc}(f) = \mu_a \omega^{m_a}$ with $m_a > 0$ (i.e. a non invertible zero divisor):

$$\mathrm{APoly}(f) = \omega^{m - m_a} f$$

A basis of an ideal is a Gröbner basis if all S-polynomials between the elements of the basis and all A-polynomials of the elements of the basis 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 $(X_1 - \alpha_1, \ldots, X_\ell - \alpha_\ell)$.

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 evaluation of all* $|A|^3$ *polynomials of total degree* 1*, we obtain a linear code of length* 88 *over* A *which maps, using the mapping* $A \to \mathbb{F}_4^2$ *given by* $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$*, to a* $[176, 6, 88]_4$ *code.*

2. *Considering the evaluation of all* $|A|^6$ *polynomials of total degree* 2*, we obtain a linear code of length* 88 *over* A *which maps to a* $[176, 12, 16]_4$ *code.*

3. *Considering the evaluation of all* $|A|^9$ *polynomials of total degree* 3*, we obtain a linear code of length* 88 *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 evaluation of all* $|A|^3$ *polynomials of total degree* 1*, we obtain a linear code of length* 96 *over* A *which maps, under the above mapping, to a* $[192, 6, 96]_4$ *code.*

2. *Considering the evaluation of all* $|A|^6$ *polynomials of total degree* 2*, we obtain a linear code of length* 96 *over* A *which maps to a* $[192, 12, 16]_4$ *code.*

3. *Considering the evaluation of all* $|A|^9$ *polynomials of total degree* 3*, we obtain a linear code of length* 96 *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 evaluation of all* $|A|^3$ *polynomials of total degree* 1*, we obtain a linear code of length* 112 *over* A *which, under the mapping* $A \to \mathbb{F}_4^2$ *with* $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$*, map to a* $[224, 6, 96]_4$ *code.*

2. *Considering the evaluation of all* $|A|^6$ *polynomials of total degree* 2*, we obtain a linear code of length* 112 *over* A *which under the mapping* $A \to \mathbb{F}_4^2$ *with* $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$*, map to a* $[224, 12, 64]_4$ *code.*

3. *Considering the evaluation of all* $|A|^9$ *polynomials of total degree* 3*, we obtain a linear code of length* 112 *over* A *which under the mapping* $A \to \mathbb{F}_4^2$ *with* $(\alpha_1 + \alpha_2 z) \mapsto (\alpha_2, \alpha_1 + \alpha_2)$*, map to a* $[224, 20, 32]_4$ *code.*

References

[1] S.A. Abramov, H.Q. Le, and Z. Li, *Univariate Ore polynomial rings in computer algebra*, Journal of Mathematical Sciences, Vol. 131, No. 5 (2005)

[2] W.W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, 3, American Mathematical Society (1996)

[3] D. Boucher and F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Designs, Codes and Cryptography, 70, 405–431 (2014)

[4] A. Hashemi and P. Alvandi, *Applying Buchberger's criteria for computing Gröbner bases over finite-chain rings*, Journal of Algebra and Its Applications, 12 (2013)

[5] L. Chaussade, *Codes correcteurs avec les polynômes tordus*, Thèse Université de Rennes 1, novembre 2010.

[6] F. Dumas, *An introduction to noncommutative polynomial invariants*, CIMPA course "Homological methods and representations of noncommutative algebras", Argentina, 2006

[7] 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).

[8] T.Y. Lam and A. Leroy, Vandermonde and Wronskian Matrices over Division Rings, *Journal of Algebra,* **119** pp. 308-336 (1988)

[9] O. Ore, Theory of Non-Commutative Polynomials, *The Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp. 480-508 (1933)

[10] 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

[11] Yang Zhang, *Algorithms for Noncommutative Differential Operators*, PhD University of Western Ontario, 2004.

[12] M. Gr. Voskoglou, *Derivations and Iterated Skew Polynomial Rings*, International journal of applied mathematics and informatics, Issue 2, Volume 5, 2011