AAECC
DOI 10.1007/s00200-017-0344-9

ORIGINAL PAPER

How to obtain lattices from (f, σ, δ)-codes via a generalization of Construction A

S. Pumplün[1]

Received: 13 July 2016 / Revised: 20 September 2017 / Accepted: 29 September 2017

Abstract We show how cyclic (f, σ, δ)-codes over finite rings canonically induce a $\mathbb{Z}$-lattice in $\mathbb{R}^N$ by using certain quotients of orders in nonassociative division algebras defined using the skew polynomial f. This construction generalizes the one using certain σ-constacyclic codes by Ducoat and Oggier, which used quotients of orders in non-commutative associative division algebras defined by f, and can be viewed as a generalization of the classical Construction A for lattices from linear codes. It has the potential to be applied to coset coding, in particular to wire-tap coding. Previous results by Ducoat and Oggier are obtained as special cases.

Keywords Space–time block code · Linear (f, σ, δ)-code · Nonassociative algebra · Coset coding · Wiretap coding · Construction A · Order · Skew polynomial ring

Mathematics Subject Classification Primary 17A35; Secondary 11T71 · 94B40 · 94B05

1 Introduction

In the classical Construction A, a lattice is obtained by lifting a linear code over some finite ring [18]. This idea was recently generalized to the non-commutative setting by considering natural orders in cyclic algebras over number fields: by taking the quotient of the natural order by a suitable ideal, a ring is obtained which is isomorphic to the

✉ S. Pumplün
susanne.pumpluen@nottingham.ac.uk

[1] School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, UK

Published online: 16 October 2017

quotient of a twisted polynomial ring by some polynomial [19,41]. This established a connection between twisted polynomials and certain σ-constacyclic codes.

We generalize Construction A using skew polynomial rings $S[t;\sigma,\delta]$ and construct lattices by lifting cyclic (f,σ,δ)-codes, i.e. much more general linear codes than considered in [19,41], to lattices in nonassociative algebras. The multiplicative structure of the algebra is not necessary to build a lattice, so we do not limit our considerations to associative algebras as has been done so far.

As recently several classes of cyclic (f,σ,δ)-codes were constructed with a better minimal distance for certain lengths than previously known codes (e.g., see [5–11,15,20,27,36,59]), (f,σ,δ)-codes become increasingly important. These codes employ skew polynomial rings $S[t;\sigma,\delta]$ where S is a unital ring, σ an injective endomorphism of S and δ a left σ-derivation of S, and are built by choosing a monic polynomial $f \in S[t;\sigma,\delta]$ of degree m, and some monic right divisor g of f [13]. Every cyclic (f,σ,δ)-code is associated with a principal left ideal of a unital nonassociative algebra S_f defined by f, which is generated by some monic right divisor g of f.

The nonassociative algebra $S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f$ is defined on the additive subgroup $\{h \in S[t;\sigma,\delta] \,|\, \deg(h) < m\}$ of $S[t;\sigma,\delta]$ by using right division by f to define the algebra multiplication $g \circ h = gh \bmod_r f$ [51]. This can be seen as a canonical generalization of associative quotient algebras $S[t;\sigma,\delta]/(f)$, where we factor out a two-sided ideal generated by f, which occurs when Rf is a two-sided ideal. If S is a division algebra, the associative quotient algebras $S[t;\sigma,\delta]/(f)$ as well as the right nuclei of the nonassociative algebras S_f were used when constructing central simple algebras for instance in [1,2,28], [29, Sections 1.5, 1.8, 1.9], [42]. Due to their large nuclei, the algebras S_f were also successfully employed to systematically build fast-decodable fully diverse space–time block codes in [37,48,54], see [49], which are used for reliable high rate transmission over wireless digital channels with multiple antennas transmitting and receiving the data. Skew-polynomial rings and their ideals have been already used in other applications and when generalizing other classical notions like Gröbner bases [3] to a non-commutative setting, e.g. see [14,16,31,32,34,35,44,45,58], where they appear as examples of solvable polynomial rings, operator theory [26], and other codes, in particular (cyclic) convolutional codes and MDS codes cf. [21,22,24,25,38–40].

We choose suitable monic irreducible skew polynomials $f \in K[t,\sigma,\delta]$ with K/F a finite field extension of number fields, or $f \in D[t,\sigma,\delta]$ with D a cyclic division algebra over a number field, and define natural orders Λ in S_f. We then use the quotient of Λ by certain two-sided ideals to canonically construct a lattice L in $\mathbb{R}^N$, i.e. a $\mathbb{Z}$-module L of rank N, from a cyclic (f,σ,δ)-code over a finite ring.

The non-commutative setup treated in [19,41] is obtained as the special case where K/F is a cyclic field extension of degree n and $f(t) = t^n - c \in \mathcal{O}_F[t;\sigma]$ is *(right-)invariant*, i.e. satisfy $fR \subset Rf$, which makes Rf a two-sided ideal, and S_f non-commutative, but still associative.

The advantage of using nonassociative algebras as we do is the fact that this does not limit our choices of skew polynomials f to those which create two-sided ideals Rf. This means that we have a much larger choice of lattices we can build. Lattices now can be obtained by lifting any cyclic (f,σ,δ)-code, moreover, we can also lift σ-

constacyclic codes to lattices (now sitting inside nonassociative algebras). Sometimes there exist easy conditions for nonassociative cyclic algebras to be division algebras which is an additional bonus.

Our Construction A can be used to encode space–time block codes, for coset coding, and in particular for wiretap coding.

The paper is organized as follows: After collecting the results we need in Section 1, for monic and irreducible $f \in K[t; \sigma, \delta]$ we define a natural order in S_f, and investigate the quotients of a natural order by some ideals in Sect. 3. These results are then generalized in Sect. 5 to monic irreducible $f \in D[t; \sigma, \delta]$, where $D = (K/F, \rho, c)$ is a cyclic division algebra. In Sects. 4 and 6, we describe a lattice encoding of certain cyclic (f, σ, δ)-codes over the finite rings $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, where $\mathfrak{p}$ is a maximal ideal in some suitable subring of $\mathcal{O}_K$, and how it can be applied to space–time block codes.

Throughout the paper we will put a special emphasis on the nonassociative cyclic algebras $(K/F, \sigma, c)$ employed in [55], and on the generalized nonassociative cyclic algebras (D, σ, d), since these are used for iterated space–time block codes [48,49].

2 Preliminaries

2.1 Nonassociative algebras

Let R be a unital commutative ring and let A be an R-module. We call A an *algebra* over R if there exists an R-bilinear map $A \times A \to A$, $(x, y) \mapsto x \cdot y$, denoted simply by juxtaposition xy, the *multiplication* of A. An algebra A is called *unital* if there is an element in A, denoted by 1, such that $1x = x1 = x$ for all $x \in A$. We will only consider unital algebras.

For an R-algebra A, the *left nucleus* of A is defined as $\mathrm{Nuc}_l(A) = \{x \in A \mid [x, A, A] = 0\}$ where $[x, y, z] = (xy)z - x(yz)$ for $x, y, z \in A$, the *middle nucleus* as $\mathrm{Nuc}_m(A) = \{x \in A \mid [A, x, A] = 0\}$ and the *right nucleus* as $\mathrm{Nuc}_r(A) = \{x \in A \mid [A, A, x] = 0\}$. Their intersection $\mathrm{Nuc}(A) = \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A. The *center* of A is $\mathrm{C}(A) = \{x \in A \mid x \in \mathrm{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$ [53].

Let R be a Noetherian integral domain with quotient field F and A a finite-dimensional unital F-algebra. Then an *R-lattice* in A is an R-submodule Γ of A which is finitely generated and contains an F-basis of A. An *R-order* in A is a multiplicatively closed R-lattice containing 1_A (the multiplication may be not associative). An R-order will be called *maximal* if $\Gamma' \subset \Gamma$ implies $\Gamma' = \Gamma$ for every R-order Γ' in A.

An algebra $A \neq 0$ over a field F is called a *division algebra*, if for any $a \in A$, $a \neq 0$, the right multiplication with a, $L_a(x) = ax$, and the right multiplication with a, $R_a(x) = xa$, are bijective. Any division algebra is simple, that means has only trivial two-sided ideals. A finite-dimensional algebra A is a division algebra over F if and only if A has no zero divisors.

2.2 Skew polynomial rings

Let S be a unital (not necessarily commutative) ring, σ an injective ring homomorphism of S and $\delta : S \to S$ a left σ-derivation, i.e. an additive map such that $\delta(ab) = \sigma(a)\delta(b)+\delta(a)b$ for all $a, b \in S$, implying $\delta(1) = 0$. Let $\mathrm{Const}(\delta) = \{a \in S \mid \delta(a) = 0\}$ and $\mathrm{Fix}(\sigma) = \{a \in S \mid \sigma(a) = a\}$.

The *skew polynomial ring* $R = S[t; \sigma, \delta]$(defined first by Ore [43]) is the set of skew polynomials $a_0+a_1t+\cdots+a_nt^n$ with $a_i \in S$, where addition is defined term-wise and multiplication by $ta = \sigma(a)t+\delta(a)$ for all $a \in S$ (for properties see [17,23,26]). The ring $S[t; \sigma] = S[t; \sigma, 0]$ is called a *twisted polynomial ring* and $S[t; \delta] = S[t; id, \delta]$ a *differential polynomial ring*.

For $f = a_0+a_1t+\cdots+a_nt^n$ with $a_n \neq 0$ define $\deg(f) = n$ and $\deg(0) = -\infty$. Then $\deg(fg) \leq \deg(f)+\deg(g)$ with equality if

- f has an invertible leading coefficient,
- g has an invertible leading coefficient,
- S is a domain.

An element $f \in R$ is *irreducible* in R if it is not a unit and it has no proper factors, i.e if there do not exist $g, h \in R$ with $\deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

2.3 How to obtain nonassociative algebras from skew polynomial rings

From now on, let $R = S[t; \sigma, \delta]$ and σ injective. We do not assume S to be a division ring. We can still perform a right division by a polynomial $f \in R$ which has invertible leading coefficient d_m: for all $g(t) \in R$ of degree $l > m$, there exist uniquely determined $r(t), q(t) \in R$ with $\deg(r) < \deg(f)$, such that $g(t) = q(t)f(t)+r(t)$. Let $\mathrm{mod}_r f$ denote the remainder of right division by such an f [51, Proposition 1].

Suppose $f(t) = \sum_{i=0}^{m} d_it^i \in R = S[t; \sigma, \delta]$ has an invertible leading coefficient d_m. Let $R_m = \{g \in R \mid \deg(g) < m\}$. Then R_m together with the multiplication $g \circ h = gh \bmod_r f$ becomes a unital nonassociative ring $S_f = (R_m, \circ)$ also denoted by R/Rf [51].

This construction was introduced by Petit [46,47] for unital division rings S. S_f is a unital nonassociative algebra over $S_0 = \{a \in S \mid ah = ha \text{ for all } h \in S_f\}$ which is a commutative subring of S. We call S_f a *Petit algebra*. The algebra S_f is associative if and only if Rf is a two-sided ideal in R ([51, Theorem 4 (ii)], or [46, (1)] if S is a division ring). For all invertible $a \in S$ we have $S_f \cong S_{af}$, so that without loss of generality it suffices to only consider monic polynomials in the construction.

If S_f is not associative then $S \subset \mathrm{Nuc}_l(S_f)$ and $S \subset \mathrm{Nuc}_m(S_f)$, $\mathrm{Nuc}_r(S_f) = \{g \in R_m \mid fg \in Rf\}$ and S_0 is the center of S_f [51]. It is easy to see that $C(S) \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta) \subset S_0$.

If S is a division algebra and S_f is a finite-dimensional vector space over S_0, then S_f is a division algebra if and only if $f(t)$ is irreducible in R [46, (9)].

For $f(t) = \sum_{i=0}^{m} d_it^i \in S[t; \sigma]$, t is left-invertible in S_f if and only if d_0 is invertible by a simple degree argument. Thus if f is irreducible (hence $d_0 \neq 0$) and S a division ring then t is always left-invertible in S_f and $S_0 = \mathrm{Fix}(\sigma) \cap C(S)$ is the center of S_f [51, Theorem 8 (ii)].

The S-basis $1, t, t^2, \ldots, t^{n-1}$ is the *canonical basis* for the left S-module S_f. Since $S \subset \mathrm{Nuc}_m(S_f)$ and $S \subset \mathrm{Nuc}_l(S_f)$, the right multiplication with $0 \neq a \in S_f$ in S_f, $R_h : S_f \longrightarrow S_f,\ p \mapsto pa$, is an S-module endomorphism, and after expressing R_a in matrix form with respect to the canonical basis of S_f, the map

$$\gamma : S_f \to \mathrm{End}_K(S_f), a \mapsto R_a$$

induces an injective S-linear map

$$\gamma : S_f \to \mathrm{Mat}_m(S), a \mapsto R_a \mapsto M(a).$$

This fact is exploited when designing space–time block codes which employ one of the following two special cases of algebras:

Definition 1 (i) Let S/S_0 be an extension of commutative unital rings and $G = \langle \sigma \rangle$ a finite cyclic group of order m acting on S such that $S_0 = \mathrm{Fix}(\sigma)$. For any $c \in S$,

$$S_f = S[t; \sigma]/S[t; \sigma](t^m - c)$$

is called a *nonassociative cyclic algebra* $(S/S_0, \sigma, c)$ *of degree* m.

(ii) Let D be a finite-dimensional central division algebra over $F = \mathrm{C}(D)$ of degree n, $\sigma \in \mathrm{Aut}(D)$ such that $\sigma|_F$ has finite order m and $f(t) = t^m - d \in D[t; \sigma]$. Let $F_0 = F \cap \mathrm{Fix}(\sigma)$. The F_0-algebra $S_f = D[t; \sigma]/D[t; \sigma]f(t)$ is called a *(generalized) nonassociative cyclic algebra of degree* m. We denote this algebra by (D, σ, d) and call $1, e, \ldots, e^n, t, et \ldots, e^{n-1}t, \ldots e^n t^{m-1}$ its *canonical basis* as a left K-vector space.

Remark 1 If $c \in S \backslash S_0$, then $(S/S_0, \sigma, c)$ has nucleus S and center S_0. These algebras first appeared over finite fields in [52], over general fields they were studied in [56], and over number fields, in [55]. If $c \in S_0^{\times}$, $S[t; \sigma]/S[t; \sigma](t^m - c)$ is a classical associative cyclic algebra, cf. [19,41]. If $c = 0$, $S[t; \sigma]/S[t; \sigma](t^m)$ is a commutative associative algebra, the direct product of m copies of S. If S/S_0 is a cyclic Galois field extension of degree m with Galois group $\langle \sigma \rangle$ and $c \in S \backslash S_0$, then $\mathrm{Nuc}((S/S_0, \sigma, c)) = K$. If m is prime then $(S/S_0, \sigma, c)$ is a division algebra. For non-prime m, a division algebra for all choices of c such that $1, c, \ldots, c^{m-1}$ are linearly independent [56].

Example 2 Let F and L be fields, $F_0 = F \cap L$, and let K be a cyclic field extension of both F and L such that $\mathrm{Gal}(K/F) = \langle \rho \rangle$ and $[K : F] = n$, $\mathrm{Gal}(K/L) = \langle \sigma \rangle$ and $[K : L] = m$, such that ρ and σ commute. Let $D = (K/F, \rho, c)$ be an associative cyclic division algebra over F of degree n with canonical basis $1, e, \ldots, e^{n-1}$ (where $e^n = c$, $el = \rho(l)e$ for every l in K), and $c \in F_0$. For $x = x_0 + x_1 e + x_2 e^2 + \cdots + x_{n-1} e^{n-1} \in D$, extend σ to an automorphism $\sigma \in \mathrm{Aut}_L(D)$ of order m via

$$\sigma(x) = \sigma(x_0) + \sigma(x_1)e + \sigma(x_2)e^2 + \cdots + \sigma(x_{n-1})e^{n-1}.$$

For all $d \in D^\times$, $S_f = D[t;\sigma]/D[t;\sigma](t^m - d)$ is the generalized nonassociative cyclic algebra (D, σ, d) of dimension m^2n^2 over F_0. For all $d \in F^\times$, we have

$$S_f = D[t;\sigma]/D[t;\sigma](t^m - d) = (L/F_0, \rho, c) \otimes_{F_0} (F/F_0, \sigma, d) = (D, \sigma, d)$$

(D, σ, d) is associative if and only if $d \in F_0$. For $f \in F_0[t]$, (D, σ, d) is a *generalized cyclic algebra* of degree n [29, Section 1.4].

2.4 Space–time block coding

An $(s \times t)$ *space–time block code* (STBC) is a set $\mathcal{C}$ of complex $s \times t$ matrices. $\mathcal{C}$ is called *linear* if $X, X' \in \mathcal{C}$ implies $X \pm X' \in \mathcal{C}$. A linear code is called *fully diverse*, if $\det X \neq 0$ for all $0 \neq X \in \mathcal{C}$.

Let K/F be a Galois field extension of degree n and K an imaginary number field. Nonassociative cyclic division algebras $A = (K/F, \sigma, c)$ of degree n can be used to build linear $n \times n$ STBCs with entries in K, since the right multiplication in A induces the injective K-linear map $\gamma : A \hookrightarrow \mathrm{End}_K(A) \hookrightarrow \mathrm{Mat}_(K)$, $a \mapsto R_a \mapsto M(a)$ (cf. Sect. 2.3). The set of matrices $\gamma(A)$ is a linear STBC that is fully diverse since A is a division algebra.

Let $A = (D, \sigma, d)$ be a generalized nonassociative cyclic division algebra, with $D = (K/F, \sigma, c)$ an associative cyclic algebra of degree n. Again, A can be used to build a fully diverse linear $mn \times mn$ STBC with entries in K: we know $\gamma : A \hookrightarrow \mathrm{End}_D(A)$, $a \mapsto R_a$ is an injective D-linear map, and $K \subset D$. Using the canonical K-basis of A, we obtain an $mn \times mn$-matrix $M(a)$ representing R_a for every $a \in A$. Thus we have $\gamma : A \hookrightarrow \mathrm{End}_D(A) \hookrightarrow \mathrm{Mat}_{mn}(K)$, $a \mapsto R_a \mapsto M(a)$ and $\gamma(A)$ is a fully diverse linear STBC.

When $d \in L^\times$ or $d \in F^\times$, $\gamma(A)$ is used for the codes in [49,50,54]. For $m = 2$, $\gamma(A)$ is used in the iterated codes constructed in [37]. In particular, for $d \in F^\times$ the algebra in Example 2 is employed for the space–time block codes in [54], see also [48].

2.5 Cyclic (f, σ, δ)-codes

Let $f \in S[t;\sigma,\delta]$ be monic of degree m and σ injective. We associate to an element $a(t) = \sum_{i=0}^{m-1} a_i t^i$ in S_f the vector $(a_0, \ldots, a_{m-1})$. A *linear code of length m over S* is a submodule of the S-module S^m. Conversely, for any linear code $\mathcal{C}$ of length m we denote by $\mathcal{C}(t)$ the set of skew polynomials $a(t) = \sum_{i=0}^{m-1} a_i t^i \in S_f$ associated to the codewords $(a_0, \ldots, a_{m-1}) \in \mathcal{C}$.

A *cyclic* (f, σ, δ)*-code* $\mathcal{C} \subset S^m$ is a set consisting of the vectors $(a_0, \ldots, a_{m-1})$ obtained from elements $h = \sum_{i=0}^{m-1} a_i t^i$ in a left principal ideal $S_f g$ where $S_f = S[t;\sigma,\delta]g/S[t;\sigma,\delta]f$, and g is a monic right divisor of f. A code $\mathcal{C}$ over S is called σ*-constacyclic* if there is a non-zero $c \in S$ such that

$$(a_0, \ldots, a_{m-1}) \in \mathcal{C} \Rightarrow (\sigma(a_{m-1})c, \sigma(a_0), \ldots, \sigma(a_{m-2})) \in \mathcal{C}.$$

Lemma 3 *(cf. [51, Proposition 7]) Let $f \in R = S[t; \sigma, \delta]$ be monic of degree m.*

(a) Let σ be injective. Then:
- *Every right divisor g of f of degree $< m$ with an invertible leading coefficient generates a principal left ideal in S_f.*
- *All left ideals in S_f which contain a non-zero polynomial g of minimal degree with invertible leading coefficient are principal left ideals, and g is a right divisor of f in R.*
- *([13, Theorem 1]) Each principal left ideal generated by a monic right divisor of f is an S-module which is isomorphic to a submodule of S^m and forms a code of length m and dimension $m - \deg(g)$.*

(b) Let S be a division ring. Then all left ideals in S_f are generated by some monic right divisor g of f in R.

Proof (a) Let $g(t)$ be such a right divisor of $f(t)$, then the ideal Rf is contained in Rg and it is easy to check that $Rg/Rf = \{h \in R_m \mid h = sg \text{ for some } s \in R_m\}$ is a left ideal in S_f.

The proof of the second assertion is similar to the one of [12, Lemma 1]: Suppose that I is a left ideal in S_f which contains a non-zero polynomial g of minimal degree with invertible leading coefficient. For any $p \in I \subset R_m$, a right division by g yields unique $r, q \in R$ with $\deg(r) < \deg(g)$ such that $p = qg + r$ and hence $r = p - qg \in I$. Since we chose $g \in I$ to have minimal degree, we conclude that $r = 0$, implying $p = qg$ and so $I = Rg$ is a principal left ideal, and g is a right divisor of f in R.

(b) Let I be a left ideal of S_f. If $I = \{0\}$ then $I = (0)$. So suppose $I \neq (0)$ and choose a monic non-zero polynomial g in $I \subset R_m$ of minimal degree. As in the proof of (i), for any $p \in I$, a right division by g yields unique $r, q \in R$ with $\deg(r) < \deg(g)$ such that $p = qg + r$ and hence $r = p - qg \in I$. Since $g \in I$ has minimal degree, $r = 0$, and so $I = Rg$. □

Let $f, g, h, h' \in S[t; \sigma, \delta]$ be monic polynomials such that $f = gh = h'g$. Let $\mathcal{C}$ be the cyclic (f, σ, δ)-code corresponding to g and $c(t) = \sum_{i=0}^{m-1} c_i t^i \in S[t; \sigma, \delta]$. Then $(c_0, \ldots, c_{m-1}) \in \mathcal{C}$ is equivalent to $c(t)h(t) = 0$ in S_f [13, Theorem 2], i.e. h is a parity check polynomial for $\mathcal{C}$.

The codes $\mathcal{C}$ of length m we consider consist of all elements $(a_0, \ldots, a_{m-1})$ obtained from polynomials $a(t) = \sum_{i=0}^{m-1} a_i t^i$ in a left principal ideal $S_f g$ of S_f, with g a monic right divisor of f; σ-constacyclic codes are obtained when $f(t) = t^m - c \in S[t; \sigma]$.

For a field K, every skew polynomial ring $K[t; \sigma, \delta]$ can be made into either a twisted or a differential polynomial ring by a linear change of variables [29, 1.1.21]. When constructing linear codes, however, we will consider general skew polynomial rings. They might produce better distance bounds than cyclic (f, σ, δ)-codes constructed only with an automorphism, where $\delta = 0$, see [8] for examples of this phenomenon.

3 Natural orders in S_f and their quotients by a prime ideal, I

In the following, we use the notation from [19, Section 2]. Let K/F be a Galois extension of number fields of degree n with $\mathcal{O}_F$ and $\mathcal{O}_K$ the rings of integers of F, respectively K.

3.1 The setup

Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_F$, p the prime lying below $\mathfrak{p}$ and $\mathcal{O}_F/\mathfrak{p} = \mathbb{F}_{p^j}$, where j is the inertial degree of $\mathfrak{p}$ above p. Let $\pi : \mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ be the canonical projection. Let $\sigma \in G = \mathrm{Gal}(K/F)$. We have $\sigma(\mathfrak{p}\mathcal{O}_K) \subset \mathfrak{p}\mathcal{O}_K$ since $\sigma|_F = id$. Thus σ induces a ring homomorphism

$$\overline{\sigma} : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K, \quad a + \mathfrak{p}\mathcal{O}_K \mapsto \sigma(a) + \mathfrak{p}\mathcal{O}_K$$

with $\pi \circ \sigma|_{\mathcal{O}_K} = \overline{\sigma} \circ \pi$ and $\mathrm{Fix}(\overline{\sigma}) = \mathbb{F}_{p^j}$. Suppose that δ is an F-linear left σ-derivation on K such that $\delta(\mathcal{O}_K) \subset \mathcal{O}_K$. Then δ induces a left $\overline{\sigma}$-derivation $\overline{\delta} : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. Since $\mathcal{O}_K$ is a Dedekind domain we have

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_g^{e_g}$$

for suitable prime (maximal) ideals $\mathfrak{p}_i$ of $\mathcal{O}_K$, $e_i \geq 0$. The ideals $\mathfrak{p}_t^{e_t}$ are pair-wise comaximal. By the Chinese Remainder Theorem, we have thus the following direct sum of rings:

$$\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathcal{O}_K/\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1}\mathcal{O}_K \times \cdots \times \mathcal{O}_K/\mathfrak{p}_g^{e_g}\mathcal{O}_K.$$

G acts trivially on each of these $\mathfrak{p}_t$, therefore there is an induced action of G on each $\mathcal{O}_K/\mathfrak{p}_t^{e_t}\mathcal{O}_K$ and the above is an isomorphism of G-modules (cf. [41, (9)]). That means on each ring $\mathcal{O}_K/\mathfrak{p}_t^{e_t}\mathcal{O}_K$ there is a canonical induced automorphism $\overline{\sigma}$ and a canonical left $\overline{\sigma}$-derivation $\overline{\delta}$ induced by δ.

In particular, if $\mathfrak{p}$ is inert in K/F, $\mathfrak{p}\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$ and thus $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathbb{F}_{p^{nj}}$ a finite field, and $\overline{\sigma} \in \mathrm{Gal}(\mathbb{F}_{p^{nj}}/\mathbb{F}_{p^j})$ (cf. [19, Section 2] if $\delta = 0$ and K/F is cyclic).

3.2 Natural orders

Suppose $f(t) = \sum_{i=0}^{m} d_i t^i \in \mathcal{O}_K[t;\sigma,\delta]$ is monic and irreducible in $K[t;\sigma,\delta]$. Consider the nonassociative division algebra

$$S_f = K[t;\sigma,\delta]/K[t;\sigma,\delta]f$$

over F. Then the nonassociative $\mathcal{O}_F$-algebra

$$\Lambda = \mathcal{O}_K[t;\sigma,\delta]/\mathcal{O}_K[t;\sigma,\delta]f$$

is an $\mathcal{O}_F$-order in S_f called the *natural order* and $\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K t \oplus \cdots \oplus \mathcal{O}_K t^{m-1}$ as left $\mathcal{O}_K$-module. Since f is irreducible in $K[t; \sigma, \delta]$, Λ does not have any zero divisors. The center of Λ contains $\mathcal{O}_F$. Hence for every maximal ideal $\mathfrak{p}$ in $\mathcal{O}_F$, $\mathfrak{p}\Lambda$ is a two-sided ideal of Λ.

Λ is usually not maximal, but it is uniquely determined whenever Rf is not a two-sided ideal, since in that case K is the left and middle nucleus of S_f and uniquely determines $\mathcal{O}_K$ and in turn Λ. (For examples of classes of maximal orders in nonassociative cyclic algebras of degree two, cf. [30,33], the results there can be generalized to nonassociative algebras of any degree n.)

Remark 4 S_f is associative if and only if Rf is a two-sided ideal [51, Theorem 4 (ii)]. Therefore our definition generalizes the non-commutative natural orders in [19] which were only defined for two-sided ideals Rf and $\delta = 0$.

For any $g(t) = \sum_{i=0}^{m-1} a_i t^i \in \mathcal{O}_K[t; \sigma, \delta]$ define $\overline{g}(t) = \sum_{i=0}^{m-1} \overline{a_i} t^i \in (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}, \overline{\delta}]$ with $\overline{a_i} = a_i + \mathfrak{p}\mathcal{O}_K$. Let $\overline{f}(t) = \sum_{i=0}^{m} \overline{d_i} t^i \in (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}, \overline{\delta}]$ with $\overline{d_i} = d_i + \mathfrak{p}\mathcal{O}_K$.

Lemma 5 *(i) The surjective homomorphism of nonassociative rings*

$$\Psi : \Lambda \longrightarrow S_{\overline{f}}, \quad g \mapsto \overline{g}$$

has kernel $\mathfrak{p}\Lambda$.

(ii) Ψ induces an $\mathbb{F}_{p^j}$-algebra isomorphism given by

$$\Psi : \Lambda/\mathfrak{p}\Lambda \longrightarrow S_{\overline{f}}, \quad g + \mathfrak{p}\Lambda \mapsto \overline{g}.$$

Proof (i) Λ is nonassociative $\mathcal{O}_F$-algebra and Ψ is a well-defined surjective homomorphism with kernel $\mathfrak{p}\Lambda$: For all $g = \sum_{i=0}^{m-1} b_i t^i \in \mathfrak{p}\Lambda$ it follows that $\overline{g} = \sum_{i=0}^{m-1} \overline{b_i} t^i = 0$ in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}, \overline{\delta}]$, so that $\mathfrak{p}\Lambda \subset ker(\Psi)$.
Suppose conversely there is a nonzero $g \in \Lambda$ such that $\Psi(g) = \overline{g} = 0$, then $g = hf + r$ in $\mathcal{O}_K[t; \sigma, \delta]$ with a nonzero $r \in \mathcal{O}_K[t; \sigma, \delta]$, and so $\overline{g} = \overline{h}\,\overline{f} + \overline{r}$ with $\overline{r} = 0$ in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}, \overline{\delta}]$. We have $\mathfrak{p}\Lambda = \{al \mid a \in \mathfrak{p}, l \in \Lambda\} = \{\sum_{i=0}^{m-1} a_i t^i \mid a_i \in \mathfrak{p}\mathcal{O}_K\}$. This implies that $r \in \mathfrak{p}\mathcal{O}_K[t; \sigma, \delta] = \mathfrak{p}\Lambda$.
(ii) follows from (i). □

Example 6 Let $\mathrm{Gal}(K/F) = < \sigma >$ and $f(t) = t^n - d \in \mathcal{O}_K[t; \sigma]$ irreducible in $K[t; \sigma]$. $A = (K/F, \sigma, d)$ is a nonassociative cyclic division algebra of degree n over F and $S_{\overline{f}} = \left((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/\mathbb{F}_{p^j}, \overline{\sigma}, \overline{d}\right)$ with $\overline{f}(t) = t^n - \overline{d} \in (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}]$. If $d \in \mathcal{O}_F$ is non-zero, A is associative and Λ depends on the choice of the maximal subfield K in A. Then $S_{\overline{f}}$ is an associative (generalized) cyclic algebra as in [19,41] and $\overline{f}(t)$ is reducible whenever $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is a field.

If $d \in \mathcal{O}_K \backslash \mathcal{O}_F$, A is not associative and the natural order

$$\Lambda = \mathcal{O}_K[t; \sigma]/\mathcal{O}_K[t; \sigma]f = \mathcal{O}_K \oplus \mathcal{O}_K t \oplus \cdots \oplus \mathcal{O}_K t^{n-1}$$

of A is uniquely determined. If n is prime then f is irreducible and A a division algebra for every $d \in \mathcal{O}_K \backslash \mathcal{O}_F$. If n is not prime and $1, d, \ldots, d^{n-1}$ are linearly independent then f is irreducible and A a division algebra (Remark 1). Furthermore,

$$\Lambda/\mathfrak{p}\Lambda \cong ((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/\mathbb{F}_{p^j}, \overline{\sigma}, \overline{d}) = S_{\overline{f}}.$$

Remark 7 Suppose that K/F is cyclic of degree n and inertial with respect to $\mathfrak{p}$, then $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathbb{F}_{p^{jn}}$ and $\mathrm{Gal}(\mathbb{F}_{p^{jn}}/\mathbb{F}_{p^j}) = \langle\overline{\sigma}\rangle$. Let $f(t) = \sum_{i=0}^{n} d_i t^i \in \mathcal{O}_K[t; \sigma, \delta]$ be such that $\overline{f}(t) = t^n - \overline{d_0}$.

(i) In [19], only polynomials $f(t) = t^n - d_0$ with $d_0 \in \mathcal{O}_F$ are considered which makes the ideal $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}]\overline{f}$ two-sided and the resulting $\mathbb{F}_{p^j}$-algebra associative. In this case, $\overline{f}(t) = t^n - \overline{d_0}$ is always reducible in $\mathbb{F}_{p^{jn}}[t; \overline{\sigma}]$.

(ii) By Lemma 3, if $\overline{f}$ is irreducible, then $S_{\overline{f}}$ has no non-trivial left ideals. For instance, if n is prime and $d_0 \notin \mathcal{O}_F$ then for all $\overline{d_0} \neq 0$,

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathbb{F}_{p^{jn}}/\mathbb{F}_{p^j}, \overline{\sigma}, \overline{d_0})$$

is always a division algebra, i.e. $f(t) = t^n - \overline{d_0}$ is irreducible, and so there are no non-trivial left ideals by Lemma 3 (b).

4 Lattice encoding of cyclic (f, σ, δ)-codes over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, I

We keep the assumptions and notation from Sect. 3. Let $\mathcal{I} = \Lambda g(t)$ be a principal left ideal of Λ generated by a monic polynomial $g(t)$ such that $\mathfrak{p} \subset \mathcal{I} \cap \mathcal{O}_F$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is a principal left ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a principal left ideal of $((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/\mathbb{F}_{p^j}, \overline{\sigma}, \overline{c})$ generated by the monic polynomial $\Psi(g + \mathfrak{p}\Lambda) = \overline{g}$. That means, $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to an $(\overline{f}, \overline{\sigma}, \overline{\delta})$-code $\mathcal{C}$ over $\mathbb{F}_q$. In particular, if we choose $f(t)$ such that $\overline{f}(t) = t^m - \overline{c}$ with $\overline{c}$ non-zero, then $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to a $\overline{\sigma}$-constacyclic code over $\mathbb{F}_q$.

If $\overline{f}$ is irreducible and $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ a field, then $S_{\overline{f}}$ has no nontrivial principal left ideals which contain a non-zero polynomial of minimal degree with invertible leading coefficient and so $\mathcal{C}$ has length n and dimension n, or is zero, whereas when $\overline{f}$ is reducible and $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ a field, an $(\overline{f}, \overline{\sigma}, \overline{\delta})$-code $\mathcal{C}$ corresponds to a right divisor $\overline{g}$ of $\overline{f}$ and has dimension $n - \deg(\overline{g})$. So we will look for irreducible f where $\overline{f}$ is reducible.

4.1 Construction A

Let

$$\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda)$$

be the canonical projection $\Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda$ composed with Ψ. We know that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n[F : \mathbb{Q}]$. Then

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$$

is a $\mathbb{Z}$-module of dimension $N = nm[F : \mathbb{Q}]$. The embedding of this lattice into $\mathbb{R}^N$ is canonically determined by considering $A \otimes_{\mathbb{Q}} \mathbb{R}$. Now all works exactly as as explained in [19, Section 3.3]. The construction of L can be seen as a non-commutative variation of the classical Construction A in [18].

This way we can construct a lattice L in $\mathbb{R}^N$ from the linear code $\mathcal{C}$ over the finite ring $S = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. The non-commutative variation of Construction A in [19] is the special case that $f(t) = t^n - c \in \mathcal{O}_F[t] \subset K[t; \sigma]$, where S_f is associative.

Example 8 Let $K[t; \sigma] = \mathbb{Q}(i)[t; \sigma]$ with σ the complex conjugation, so that $F = \mathbb{Q}$, $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$. Let $f(t) = t^2 - t + (i - 3) \in \mathbb{Z}[i][t, \sigma]$, then $f(t)$ is irreducible in $\mathbb{Q}(i)[t; \sigma]$, since $\sigma(z)z - z \neq i - 3$ for all $z \in \mathbb{Q}(i)$ [46, (17)]. Let $p = 3$. Then $\mathbb{Z}[i]/3\mathbb{Z}[i] = \mathbb{F}_9$ and using the natural order $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]t$ in S_f, we obtain the nonassociative algebra $\Lambda/3\Lambda \cong S_{\overline{f}}$ over $\mathbb{F}_3$ with $\overline{f}(t) = t^2 - (\alpha + \alpha^3 - 1)t + \alpha - 3 \in \mathbb{F}_9[t; \overline{\sigma}]$ where $\overline{\sigma}(\alpha) = \alpha^3$, if α is a primitive root of $\mathbb{F}_9$ over $\mathbb{F}_3$, that is $\alpha^2 + 1 = 0$. Since

$$\overline{f}(t) = (t - 2 + \alpha)(t + 1 + \alpha),$$

$\overline{f}$ is reducible in $\mathbb{F}_9[t; \overline{\sigma}]$. The left ideal generated by $(t + 1 + \alpha)$ in $S_{\overline{f}}$ yields a cyclic $(f, \sigma, 0)$-code of length 2 and dimension one. Taking the pre-image of it under Ψ it corresponds to a principal left ideal $\mathcal{I}/3\Lambda$ in $\Lambda/3\Lambda$.

4.2 Examples involving nonassociative quaternion algebras

Let $K = \mathbb{Q}(i)$, $F = \mathbb{Q}$, so that $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$. The examples given in [19] are special cases of our construction using cyclic algebras. We now consider some algebras which are not associative.

Let $f(t) = t^2 - bt - c \in \mathbb{Z}[i][t, \sigma]$ be irreducible in $\mathbb{Q}(i)[t; \sigma]$. This is equivalent to $\sigma(z)z - bz - c \neq 0$ for all $z \in \mathbb{Q}(i)$ [46, (17)]. In particular, if $b, c \in \mathbb{Z}$ then $f(t)$ is irreducible if $b^2 + 4c < 0$ (alternatively, if f is an irreducible polynomial in $\mathbb{R}$) by [4, Corollary 2.6]. Suppose that $\overline{f}(t) = t^2 - \overline{c} \in (\mathbb{Z}[i]/\mathfrak{p}\mathbb{Z}[i])[t; \overline{\sigma}]$ for some maximal ideal $\mathfrak{p}$ in $\mathcal{O}_F$.

For the natural order $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]t$, we obtain the (perhaps nonassociative) quaternion algebra

$$\Lambda/\mathfrak{p}\Lambda \cong ((\mathbb{Z}[i]/\mathfrak{p}\mathbb{Z}[i])/\mathbb{F}_{p^j}, \overline{\sigma}, \overline{c}) = S_{\overline{f}}.$$

In particular, $\Lambda/\mathfrak{p}\Lambda = (\mathbb{Z}[i]/\mathfrak{p}\mathbb{Z}[i]) \oplus (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)t$ as $(\mathbb{Z}[i]/\mathfrak{p}\mathbb{Z}[i])$-module.

For any choice of $c \in \mathbb{Z}$ such that $c \notin \mathfrak{p}\mathbb{Z}[i]$, $\overline{f}(t) = t^2 - \overline{c} \in \mathcal{O}_K[t, \sigma]$ is reducible.

For $b = 0$ and any choice of $c \in \mathbb{Z}[i]\backslash\mathbb{Z}$, $f(t) = t^2 - c \in \mathbb{Z}[i][t, \sigma]$ is irreducible in $\mathbb{Q}(i)[t; \sigma]$ and therefore

$$A = S_f = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, c)$$

a nonassociative quaternion division algebra (for instance, $ct = (t^2)t \neq t(t^2) = \sigma(c)t$ in A.) We can also write A as the Cayley–Dickson doubling $\mathrm{Cay}(\mathbb{Q}(i), c)$, defined in the obvious way.

Example 9 Let $f(t) = t^2 - c \in \mathbb{Z}[i][t; \sigma]$, $c \in \mathbb{Z}[i]\backslash\mathbb{Z}$. Choose any p which remains inert in $\mathbb{Q}(i)$, then $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathbb{F}_{p^{2j}}$, where j is the inertial degree of $\mathfrak{p}$ above p, and

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathbb{F}_{p^{2j}}/\mathbb{F}_{p^j}, \overline{\sigma}, \overline{c}).$$

If $\overline{c} \neq 0$ this is a division algebra because $f(t) = t^2 - \overline{c}$ is irreducible. Given any principal left ideal $\mathcal{I}$ of Λ containing p, $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is thus either trivial or all of $S_{\overline{f}} = \mathbb{F}_{p^{2j}}[t; \overline{\sigma}]/\mathbb{F}_{p^{2j}}[t; \overline{\sigma}]\overline{f}$.

If $\overline{c} = 0$, i.e. when $c \in \mathfrak{p}\mathcal{O}_K$ then $\overline{f}(t) = t^2$ and $S_{\overline{f}}$ is a commutative associative algebra. There are no $\overline{\sigma}$-constacyclic codes since here $\overline{c} = 0$. Thus this algebra cannot be used for lattice encoding of $\overline{\sigma}$-constacyclic codes.

E.g., take $p = 3$. If $c = i$ then $\Lambda/3\Lambda \cong (\mathbb{F}_9/\mathbb{F}_3, \overline{\sigma}, \overline{i})$ is a nonassociative quaternion division algebra over $\mathbb{F}_3$ where $\overline{\sigma}(\alpha) = \alpha^3$, if α is a primitive root of $\mathbb{F}_9$ over $\mathbb{F}_3$, that is $\alpha^2 + 1 = 0$. $\mathcal{I} = (1+i)\Lambda$ satisfies $3 \in \mathcal{I} \cap \mathcal{O}_F$ (since $1 - 2i \in \mathbb{Z}[i]$, so $(1+i)(1-2i) = 3 \in \mathcal{I}$). Hence $\mathcal{I}/3\Lambda$ is a left principal ideal of $\Lambda/3\Lambda \cong (\mathbb{F}_9/\mathbb{F}_3, \overline{\sigma}, \overline{i})$, generated by $\Psi((1 + i) + 3\Lambda)$, implying $\mathcal{I}/3\Lambda \cong (\mathbb{F}_9/\mathbb{F}_3, \overline{\sigma}, \overline{i})$. Since here $\overline{f}$ is irreducible, the only available (and trivial) $\overline{\sigma}$-constacyclic code here is the one corresponding to the algebra $(\mathbb{F}_9/\mathbb{F}_3, \overline{\sigma}, \overline{i})$.

If $c = 3i$, then $\overline{f}(t) = t^2$ and $\Lambda/3\Lambda \cong (\mathbb{F}_9/\mathbb{F}_3, \overline{\sigma}, 0)$ is a commutative associative algebra over $\mathbb{F}_3$. There are no $\overline{\sigma}$-constacyclic codes since $\overline{c} = 0$, hence this example cannot be used for lattice encoding of $\overline{\sigma}$-constacyclic codes.

Example 10 Let $f(t) = t^2 - c \in \mathbb{Z}[i][t; \sigma]$, $c \in \mathbb{Z}[i]\backslash\mathbb{Z}$.

(i) Choose any p which splits in $\mathbb{Q}(i)$, e.g. $p = 5$. Then $(5) = (1 + 2i)(1 - 2i)$ means that $\mathbb{Z}[i]/5\mathbb{Z}[i] \cong \mathbb{Z}[i]/(1 - 2i) \times \mathbb{Z}[i]/(1 + 2i) \cong \mathbb{F}_5 \times \mathbb{F}_5$ and

$$\Lambda/5\Lambda = (\mathbb{F}_5 \times \mathbb{F}_5) \oplus (\mathbb{F}_5 \times \mathbb{F}_5)e$$

is a nonassociative quaternion algebra over $\mathbb{F}_5$ with

$$\Lambda/5\Lambda \cong ((\mathbb{F}_5 \times \mathbb{F}_5)/\mathbb{F}_5, \overline{\sigma}, \overline{c}) = S_{\overline{f}} \text{ with } \overline{f}(t) = t^2 - \overline{c} \in (\mathbb{F}_5 \times \mathbb{F}_5)[t; \overline{\sigma}].$$

Here, $\overline{\sigma}(a, b) = (b, a)$ fixes the elements (a, a), $a \in \mathbb{F}_5$. The algebra $\Lambda/5\Lambda$ is a split nonassociative quaternion algebra [57], however for all $\overline{c} \neq 0$, $\overline{f}$ is irreducible in $(\mathbb{F}_5 \times \mathbb{F}_5)[t; \overline{\sigma}]$, since $\overline{c} \notin \mathbb{F}_5$. In this case, there are no non-trivial divisors of $\overline{f}$ and hence no non-trivial codes to lift. If $\overline{c} = 0$ then $\overline{f}(t) = t^2$ and $\Lambda/5\Lambda$ a commutative associative algebra. There are no $\overline{\sigma}$-constacyclic codes since $\overline{c} = 0$.

(ii) Choose $p = 2$ which ramifies in $\mathbb{Q}(i)$. Then $\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{F}_2 + \mathbb{F}_2 v = \{0, 1, v, v+1\}$ with $v^2 = 0$. I.e., $\mathbb{F}_2 + \mathbb{F}_2 v$ is the finite chain ring of characteristic 2, nilpotency index 2 and residue field $\mathbb{F}_2$. Here $\overline{\sigma} = id$,

$$\Lambda/2\Lambda = (\mathbb{F}_2 + \mathbb{F}_2 v) \oplus (\mathbb{F}_2 + \mathbb{F}_2 v)e$$

and we have the following $\mathbb{F}_2$-algebra isomorphism:

$$\Lambda/2\Lambda \cong ((\mathbb{F}_2 + \mathbb{F}_2 v)/\mathbb{F}_2, id, \overline{c}) = S_{\overline{f}}$$

with $\overline{f}(t) = t^2 - \overline{c} \in (\mathbb{F}_2 + \mathbb{F}_2 v)[t]$, $c \in \mathbb{Z}[i]\backslash\mathbb{Z}$. For both $\overline{c} = v$ and $\overline{c} = v + 1$, it is easy to show that $\overline{f}$ is irreducible, and if $\overline{c} = 0$ again $\overline{f} = t^2$. We conclude that $p = 2$ does not yield an algebra which can be employed for lattice encoding.

4.3 Nonassociative cyclic algebras of non-prime degree

For a nonassocative cyclic algebra $A = (K/F, \sigma, c)$ of prime degree n, A is a division algebra if and only if $c \in K\backslash F$. Examples 9 and 10 demonstrate that this poses a problem when trying to find irreducible $f(t) = t^n - c$ such that $\overline{f}(t) = t^n - \overline{c}$ is reducible and $0 \neq \overline{c}$, since $\overline{f}(t)$ is either irreducible, or $\overline{c} = 0$. This is not the case when n is not prime:

Example 11 Let $f(t) = t^4 - c$. Let ω_{15} be a primitive 15th root of unity, $K = \mathbb{Q}(i, \omega_{15} + \omega_{15}^{-1})$, and $F = \mathbb{Q}(i)$. Choose $c \in \mathcal{O}_K\backslash\mathcal{O}_F$ such that $1, c, c^2, c^3$ are F-linearly independent. Then $D = (\mathbb{Q}(i, \omega_{15} + \omega_{15}^{-1})/\mathbb{Q}(i), \sigma, c)$ is a nonassociative cyclic division algebra of degree 4 and

$$\Lambda = \mathbb{Z}[i, \omega_{15} + \omega_{15}^{-1}] \oplus \mathbb{Z}[i, \omega_{15} + \omega_{15}^{-1}]t \oplus \mathbb{Z}[i, \omega_{15} + \omega_{15}^{-1}]t^2 \oplus \mathbb{Z}[i, \omega_{15} + \omega_{15}^{-1}]t^3$$

is the natural order in D.

Let $\mathfrak{p} = (1 + i)$. Then $\mathfrak{p}$ is unramified in $\mathbb{Q}(i, \omega_{15} + \omega_{15}^{-1})$, $\mathbb{Z}[i]/(1 + i) \cong \mathbb{F}_2$, and

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathbb{F}_{16}/\mathbb{F}_2, \overline{\sigma}, \overline{c})$$

is a nonassociative cyclic algebra of degree 4 over $\mathbb{F}_2$ which for $\overline{c} \neq 0$ is never a division algebra, since $1, c, c^2, c^3$ are always linearly dependent over $\mathbb{F}_2$. Hence $f(t) = t^4 - \overline{c}$ is reducible. If $\overline{c} = 1$ then given any principal left ideal $\mathcal{I}$ of Λ containing $(1 + i)$ that is generated by a monic polynomial, $\Psi(\mathcal{I}/(1 + i)\Lambda)$ corresponds to a $\overline{\sigma}$-constacyclic code over $\mathbb{F}_{16}$.

5 Natural orders in S_f and their quotients by a prime ideal, II

5.1 The setup

Let K/F be a cyclic Galois extension of number fields of degree n and let $D = (K/F, \rho, c)$ be a cyclic division algebra over F such that $c \in \mathcal{O}_F^{\times}$. Let $\mathcal{D} = (\mathcal{O}_K/\mathcal{O}_F, \rho, c)$ be the generalized associative cyclic algebra over $\mathcal{O}_F$ of degree n such that $\mathcal{D} \otimes_{\mathcal{O}_F} F = (K/F, \rho, c) = D$. Then $\mathcal{D} = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1}$ is a natural $\mathcal{O}_F$-order of D, cf. 3.2 or [19].

Let $\sigma \in \mathrm{Aut}(D)$ and δ be a σ-derivation on D, satisfying the following criteria:

- $F_0 = F \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ is a number field.
- $\sigma(\mathcal{D}) \subset \mathcal{D}$ and $\delta(\mathcal{D}) \subset \mathcal{D}$.
- $S_0 = \mathcal{O}_F \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ is the ring of integers of F_0 where here σ and δ denote the restrictions of σ and δ to $\mathcal{D}$.

Suppose $f(t) = \sum_{i=0}^{m} d_i t^i \in \mathcal{D}[t; \sigma, \delta]$ is monic and irreducible in $D[t; \sigma, \delta]$. Consider the division algebra

$$S_f = D[t; \sigma, \delta]/D[t; \sigma, \delta]f$$

over F_0. Then the S_0-algebra

$$\Lambda = \mathcal{D}[t; \sigma, \delta]/\mathcal{D}[t; \sigma, \delta]f$$

is an S_0-order in S_f which we call the *natural order* (this is again usually not maximal). Λ is not uniquely determined even when Rf is not a two-sided ideal. It depends on the choice of the maximal subfield in D which we will assume to be K.

Since f is irreducible in $D[t; \sigma, \delta]$, Λ does not have zero divisors. If $1, e, \ldots, e^{n-1}$ is the canonical basis of D then

$$\begin{aligned}\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1} \oplus \mathcal{O}_K t \oplus \mathcal{O}_K et \\ \oplus \cdots \oplus \mathcal{O}_K e^{n-1} t \oplus \cdots \oplus \mathcal{O}_K e^{n-1} t^{m-1}\end{aligned}$$

as left $\mathcal{O}_K$-module.

Let $\mathfrak{p}$ be a prime ideal in S_0 such that $\mathfrak{p}\mathcal{O}_F$ is maximal. Since S_0 lies in the centers of both $\mathcal{D}$ and Λ, $\mathfrak{p}\mathcal{D}$ is a two-sided ideal of $\mathcal{D}$ and $\mathfrak{p}\Lambda$ is a two-sided ideal of Λ. Let $\pi : \mathcal{D} \longrightarrow \mathcal{D}/\mathfrak{p}\mathcal{D}$ be the canonical projection. We have $\sigma(\mathfrak{p}\mathcal{D}) \subset \mathfrak{p}\mathcal{D}$ since $\mathfrak{p} \subset \mathrm{Fix}(\sigma)$ and $\sigma(\mathcal{D}) \subset \mathcal{D}$ by assumption. Thus σ induces a ring homomorphism

$$\overline{\sigma} : \mathcal{D}/\mathfrak{p}\mathcal{D} \longrightarrow \mathcal{D}/\mathfrak{p}\mathcal{D}$$

with $\mathrm{Fix}(\overline{\sigma}) = \mathrm{Fix}(\sigma)/\mathfrak{p}\mathrm{Fix}(\sigma)$ and $\pi \circ \sigma = \overline{\sigma} \circ \pi$. We also have $\delta(\mathfrak{p}\mathcal{D}) \subset \mathfrak{p}\mathcal{D}$ by assumption, so that δ induces a left $\overline{\sigma}$-derivation $\overline{\delta} : \mathcal{D}/\mathfrak{p}\mathcal{D} \longrightarrow \mathcal{D}/\mathfrak{p}\mathcal{D}$ with field of constants $\mathrm{Const}(\overline{\delta}) = \mathrm{Const}(\delta)/\mathfrak{p}$. Let

$$\overline{S_0} = \mathrm{Fix}(\overline{\sigma}) \cap \mathrm{Const}(\overline{\delta}) \cap \overline{F}$$

with $\overline{F} = \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F = \mathbb{F}_{p^j}$, where j is the inertial degree of $\mathfrak{p}$ above p. For any $g(t) = \sum_{i=0}^{m-1} a_i t^i \in \mathcal{D}[t; \sigma, \delta]$ define $\overline{g}(t) = \sum_{i=0}^{m-1} \overline{a_i} t^i \in (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]$ with $\overline{a_i} = a_i + \mathfrak{p}\mathcal{D}$. Let $\overline{f}(t) = \sum_{i=0}^{m} \overline{d_i} t^i \in (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]$ with $\overline{d_i} = d_i + \mathfrak{p}\mathcal{D}$, then

$$S_{\overline{f}} = (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]\overline{f}.$$

Since $\overline{S_0} = S_0/\mathfrak{p} \cong \mathrm{Fix}(\overline{\sigma}) \cap \mathrm{Const}(\overline{\delta}) \cap \overline{F}$, $S_{\overline{f}}$ is an algebra over a subfield of $\mathbb{F}_{p^j}$.

Lemma 12 *(i) The surjective homomorphism of additive groups*

$$\Psi : \Lambda \longrightarrow (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]\overline{f}, \quad g \mapsto \overline{g}$$

has kernel $\mathfrak{p}\Lambda$.

(ii) Ψ induces an $\overline{S_0}$-algebra isomorphism

$$\Psi : \Lambda/\mathfrak{p}\Lambda \cong (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]\overline{f}, \quad g + \mathfrak{p}\Lambda \mapsto \overline{g}$$

Proof (i) For all $g = \sum_{i=0}^{m-1} b_i t^i \in \mathfrak{p}\Lambda$ we have $\overline{g} = \sum_{i=0}^{m-1} \overline{b_i} t^i = 0$ in $(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]$, so that $\mathfrak{p}\Lambda \subset ker(\Psi)$.

Suppose conversely there is a nonzero $g \in \Lambda$ such that $\Psi(g) = \overline{g} = 0$, then $g = hf + r$ in $\mathcal{D}[t; \sigma, \delta]$ with a nonzero $r \in \mathcal{D}[t; \sigma, \delta]$, and so $\overline{g} = \overline{h}\,\overline{f} + \overline{r}$ with $\overline{r} = 0$ in $(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]$. We have $\mathfrak{p}\Lambda = \{al \,|\, a \in \mathfrak{p}, l \in \Lambda\} = \{\sum_{i=0}^{m-1} a_i t^i \,|\, a_i \in \mathfrak{p}\mathcal{D}\}$. This implies that $r \in \mathfrak{p}\mathcal{D}[t; \sigma, \delta] = \mathfrak{p}\Lambda$.

(ii) follows from (i). □

5.2 A special case

Let $S_f = (D, \sigma, d)$ be the F_0-algebra constructed in Example 2 where now F, L and K be number fields. Suppose that $c \in \mathcal{O}_{F_0}$ and that $d \in \mathcal{O}_L^\times$ or $d \in \mathcal{O}_F^\times$. Then $\mathcal{D} = (\mathcal{O}_K/\mathcal{O}_F, \rho, c)$ is an associative cyclic algebra over $\mathcal{O}_F$ of degree n such that $\mathcal{D} \otimes_{\mathcal{O}_F} F = (K/F, \rho, c) = D$ is a division algebra over F. For $x = x_0 + x_1 e + x_2 e^2 + \cdots + x_{n-1} e^{n-1} \in D$, define

$$\sigma(x) = \sigma(x_0) + \sigma(x_1)e + \sigma(x_2)e^2 + \cdots + \sigma(x_{n-1})e^{n-1}.$$

Since $c \in \mathcal{O}_{F_0}$, $\sigma \in \mathrm{Aut}_L(D)$ has order m and restricts to $\sigma \in \mathrm{Aut}_{\mathcal{O}_L}(\mathcal{D})$.

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{F_0}$ such that $\mathfrak{p}\mathcal{O}_F$ is maximal. Then

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}]\overline{f} \cong (\overline{D}, \overline{\sigma}, \overline{d})$$

is an algebra over $\overline{F_0} = \mathcal{O}_{F_0}/\mathfrak{p}$, with $\overline{D} = \mathcal{D}/\mathfrak{p}\mathcal{D}$ a generalized associative cyclic algebra over $\mathbb{F}_{p^j} = \mathrm{Fix}(\overline{\rho})$.

Example 13 Let ω denote the primitive third root of unity, ω_7 a primitive 7th root of unity and $\theta = \omega_7 + \omega_7^{-1} = 2\cos(\frac{2\pi}{7})$. Put $F = \mathbb{Q}(\theta)$. Let $K = F(\omega) = \mathbb{Q}(\omega, \theta)$ and consider the quaternion division algebra $D = (K/F, \sigma, -1)$. Note that $\sigma(\omega) = \omega^2$.

Let $L = \mathbb{Q}(\omega)$, so that K/L is a cubic cyclic field extension whose Galois group is generated by the automorphism $\tau : \omega_7+\omega_7^{-1} \mapsto \omega_7^2+\omega_7^{-2}$. Note that $\omega \in \mathcal{O}_L = \mathbb{Z}[\omega]$.

The multiplication of the division algebra $A = (D, \tau, \omega)$ is behind the fully diverse codes employed in [54] (cf. [48]). Here,

$$\Lambda = \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}] \oplus \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]e \oplus \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]e^2 \oplus \dots$$

is a natural order in A.

Let $p = 2$, then $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_F = \mathbb{Z}[\omega_3]$ which remains prime in $\mathcal{O}_K = \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]$ and $\mathbb{Z}[i]/\mathfrak{p} \cong \mathbb{F}_4$. $\mathfrak{p}$ is inert in $K = \mathbb{Q}(\omega_3, \omega_7 + \omega_7^{-1})$. Now

$$\mathcal{D}/\mathfrak{p}\mathcal{D} = (\mathbb{F}_{64}/\mathbb{F}_8, \overline{\sigma}, -1) \cong \mathrm{Mat}_2(\mathbb{F}_8)$$

is a split quaternion algebra over $\mathbb{F}_8$. Thus

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathrm{Mat}_2(\mathbb{F}_8), \overline{\tau}, \overline{\omega})$$

where $\overline{\omega} \in \mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$.

6 Lattice encoding of cyclic (f, σ, δ)-codes over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, II

We continue to assume the setup from Sect. 5.1.

6.1 A second generalization of Construction A

Let $\mathcal{I}$ be a principal left ideal of Λ generated by a monic polynomial $g(t)$, such that $\mathfrak{p} \subset \mathcal{I} \cap S_0$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is a non-zero principal left ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a principal left ideal of $S_{\overline{f}}$ generated by the monic polynomial $\Psi(g + \mathfrak{p}\Lambda) = \overline{g}$. That means $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to an $(\overline{f}, \overline{\sigma}, \overline{\delta})$-code $\mathcal{C}$ over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

In particular, if we choose $\delta = 0$ and $f(t)$ such that $\overline{f}(t) = t^m - \overline{c} \in \mathcal{D}/\mathfrak{p}\mathcal{D}$ with $\overline{c}$ non-zero, then $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a $\overline{\sigma}$-constacyclic code over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

If $\overline{f}$ is irreducible and $\mathcal{D}/\mathfrak{p}\mathcal{D}$ is a division algebra, then the algebra $S_{\overline{f}}$ is simple. Then any non-zero code $\mathcal{C}$ must have length m and dimension m (and correspond to the whole algebra), whereas whenever $\overline{f}$ is reducible, $\mathcal{C}$ respectively $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to a right divisor $\overline{g}$ of $\overline{f}$ and has dimension $m - \deg(\overline{g})$. Let

$$\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda)$$

be the canonical projection $\Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda$ composed with Ψ. We know that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n[F : \mathbb{Q}]$. Therefore

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$$

is a $\mathbb{Z}$-module of dimension $N = n^2m[F : \mathbb{Q}]$. The embedding of this lattice into $\mathbb{R}^N$ is canonically determined by considering $S_f \otimes_{\mathbb{Q}} \mathbb{R}$. Again all works exactly as

explained in [19, Section 3.3] (since associativity is not relevant for the argument). The construction of L can again be seen as a second (nonassociative) variation of the non-commutative Construction A in [18].

In this way we can construct a lattice L in $\mathbb{R}^N$ from the linear $(\overline{f}, \overline{\sigma}, \overline{\delta})$-code $\mathcal{C}$ over a finite ring.

Note that even if $R = D[t; \sigma, \delta]$ is isomorphic to $D[t; \sigma]$ or $D[t; \delta]$, like when σ or δ are inner, we conjecture that the codes/lattices we obtain from using different ways to write R can be substantially different in performance, similarly as the examples obtained in [8], where some of the codes obtained by working with the general skew polynomial ring $\mathbb{F}_q[t; \sigma, \delta]$ have a better distance bound than the ones obtained with $\delta = 0$.

6.2 Space–time block codes

We now apply the above considerations to space–time block coding (cf. 2.4).

Example 14 Let $A = (K/F, \sigma, c)$, $c \in \mathcal{O}_K$ non-zero, be a nonassociative cyclic division algebra over F of degree m with $c \in \mathcal{O}_K$. Take the natural order $\Lambda = \mathcal{O}_K[t; \sigma]/\mathcal{O}_K[t; \sigma]f$, and let $a = a_0 + a_1 t + \cdots + a_{m-1}t^{m-1}$, $b = b_0 + b_1 t + \cdots + b_{m-1}t^{m-1} \in \Lambda$. If we identify a with the vector $(a_0, a_1, \ldots, a_{m-1})$, we can express $R_a \in \mathrm{End}_{\mathcal{O}_K}(\Lambda)$ as an $m \times m$-matrix $M(a)$ with entries in $\mathcal{O}_K$:

$$M(a) = \begin{bmatrix} a_0 & c\sigma(a_{m-1}) & c\sigma^2(a_{m-2}) & \cdots & c\sigma^{m-1}(a_1) \\ a_1 & \sigma(a_0) & c\sigma^2(a_{m-1}) & \cdots & c\sigma^{m-1}(a_2) \\ a_2 & \sigma(a_1) & \sigma^2(a_0) & \cdots & c\sigma^{m-1}(a_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & \sigma(a_{m-2}) & \sigma^2(a_{m-3}) & \cdots & \sigma^{m-1}(a_0) \end{bmatrix}^T . \tag{1}$$

If we identify b with $(b_0, b_1, \ldots, b_{m-1})$, the right multiplication with a in Λ is given by the matrix multiplication $b \cdot a = bM(a)$. The family of matrices $\{M(a) \mid 0 \neq a \in A\}$ is a fully diverse linear space–time block code $\mathcal{C}$.

Let $\mathfrak{p} \subset \mathcal{O}_F$ be a maximal ideal. Then $\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda) = ((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/\mathbb{F}_{p^f}, \overline{\sigma}, \overline{c})$. Hence $L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$ is a fully diverse space–time block code over $\mathcal{O}_K$ which is a $\mathbb{Z}$-lattice whose embedding into $\mathbb{R}^m$ is canonically determined by $A \otimes_{\mathbb{Q}} \mathbb{R}$.

Nonassociative cyclic division algebras as above can be employed to obtain fully diverse multiple-input double-output codes [55]. The algebras $A = (D, \sigma^{-1}, d)$ we consider next are used for the systematic space–time block code constructions of the fast-decodable iterated codes in [37,49,50,54].

Example 15 Let $A = (D, \sigma, d)$ be a division algebra of degree n and $d \in \mathcal{O}_L$ or $d \in \mathcal{O}_F$.

For $x = x_0 + x_1 t + x_2 t^2 + \cdots + x_{m-1}t^{m-1}$, $y = y_0 + y_1 t + y_2 t^2 + \cdots + y_{m-1}t^{m-1} \in \Lambda$, $x_i, y_i \in \mathcal{D}$, represent x as $(x_0, x_1, \ldots, x_{m-1})$ and y as $(y_0, y_1, \ldots, y_{m-1})$. Then $R_x \in \mathrm{End}_{\mathcal{D}}(\Lambda)$ is given by the $m \times m$-matrix

$$M(x) = \begin{bmatrix} x_0 & d\sigma(x_{m-1}) & d\sigma^2(x_{m-2}) & \cdots & d\sigma^{m-1}(x_1) \\ x_1 & \sigma(x_0) & d\sigma^2(x_{m-1}) & \cdots & d\sigma^{m-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & \cdots & d\sigma^{m-1}(x_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{m-1} & \sigma(x_{m-2}) & \sigma^2(x_{m-3}) & \cdots & \sigma^{m-1}(x_0) \end{bmatrix}^T$$

with entries in $\mathcal{D}$. We can write the multiplication in Λ as $y \cdot x = yM(x)$. Now substitute the right regular representation $\gamma(d)$ in $\mathcal{D}$ for d in $M(x)$ and the right regular representation $\gamma(x_i)$ in $\mathcal{D}$ for each entry x_i in $M(x)$. This way we obtain a block matrix

$$\gamma(M(x)) := \begin{bmatrix} \gamma(x_0) & \gamma(d)\sigma(\gamma(x_{m-1})) & \cdots & \gamma(d)\sigma^{m-1}(\gamma(x_1)) \\ \gamma(x_1) & \sigma(\gamma(x_0)) & \cdots & \gamma(d)\sigma^{m-1}(\gamma(x_2)) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma(x_{m-1}) & \sigma(\gamma(x_{m-2})) & \cdots & \sigma^{m-1}(\gamma(x_0)) \end{bmatrix}^T$$

where $\sigma(\gamma(x_i))$ means we apply σ to each entry of the $n\times$-matrix $\gamma(x_i)$. Products are the usual matrix products. This is an $mn \times mn$ matrix with entries in $\mathcal{O}_K$. It represents right multiplication in Λ. Writing elements in $\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1} t^{m-1}$ as row vectors of length mn with entries in $\mathcal{O}_K$, we obtain $y \cdot x = y\,\gamma(M(x))$.

The family of matrices $\{\gamma(M(x))\}$ is a fully diverse linear space–time block code $\mathcal{C}$. In particular, if $d \in \mathcal{O}_F$, then $\det(\gamma(M(x))) \in \mathcal{O}_F$ ([37], [49, Remark 5]) and if $d \in \mathcal{O}_L$, then

$$\gamma(M(x)) = \begin{bmatrix} \gamma(x_0) & d\sigma(\gamma(x_{n-1})) & d\sigma^2(\gamma(x_{n-2})) & \cdots & d\sigma^{m-1}(\gamma(x_1)) \\ \gamma(x_1) & \sigma(\gamma(x_0)) & d\sigma^2(\gamma(x_{n-1})) & \cdots & d\sigma^{m-1}(\gamma(x_2)) \\ \gamma(x_2) & \sigma(\gamma(x_1)) & \sigma^2(\gamma(x_0)) & \cdots & d\sigma^{m-1}(\gamma(x_3)) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma(x_{n-1}) & \sigma(\gamma(x_{n-2})) & \sigma^2(\gamma(x_{n-3})) & \cdots & \sigma^{m-1}(\gamma(x_0)) \end{bmatrix}^T$$

and $\det(\gamma(M(x))) \in L \cap \mathcal{O}_K = \mathcal{O}_L$ ([54], [49, Lemma 19]).

Let $\mathfrak{p} \subset \mathcal{O}_{F_0}$ be a prime ideal such that $\mathfrak{p}\mathcal{O}_F$ is maximal. Then

$$\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda) = (\overline{D}, \overline{\sigma}, \overline{d}).$$

Here, $L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$ induces a fully diverse STBC over $\mathcal{O}_K$ which is a $\mathbb{Z}$-lattice whose embedding into $\mathbb{R}^N$, $N = mn^2$, is canonically determined by $A \otimes_{\mathbb{Q}} \mathbb{R}$.

Remark 16 The explanations in [19, Section 5.2, 5.3] hold analogously for our generalization of Construction A in Sect. 4.1 and the examples here, and show the potential of the construction for coset coding used in space–time block coding, in particular for wiretap space–time block coding, but also for linear codes over finite rings. Moreover, the matrix generating a cyclic (f, σ, δ)-code $\mathcal{C} \subset S^m$ represents the right multiplication R_g in S_f and is a control matrix of $\mathcal{C}$ [51].

7 Conclusion

We presented a method how to construct a lattice from a suitable (f, σ, δ)-code defined over a finite ring which can be seen as a generalization of the classical Construction A. This can be summarized as follows: Let D be a cyclic division algebra over F which is already defined over $\mathcal{O}_F$, or a Galois field extension and f defined over its ring of integers. Take the additional assumptions on σ and δ as given in the corresponding previous sections.

- Choose some monic skew polynomial $f \in \mathcal{D}[t; \sigma, \delta]$ (resp., $f \in \mathcal{O}_K[t; \sigma, \delta]$ in the field case) which is irreducible in $D[t; \sigma, \delta]$.
- Take a natural order Λ of S_f.
- Choose a prime ideal $\mathfrak{p}$ in S_0. This yields the finite ring $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ you consider the code $\mathcal{C}$ to be defined over. $\overline{f}$ must be reducible in $(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]$.
- Choose a principal left ideal $\mathcal{I}$ of Λ generated by a monic polynomial, such that $\mathfrak{p} \subset \mathcal{I} \cap S_0$.
- $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to an $(\overline{f}, \overline{\sigma}, \overline{\delta})$-code $\mathcal{C}$ over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, and $L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$ is a $\mathbb{Z}$-lattice whose embedding into $\mathbb{R}^N$ is canonically determined by $S_f \otimes_{\mathbb{Q}} \mathbb{R}$.

If we want to apply this construction to space time block coding instead, we substitute the last step with:

- Take the matrix representing right multiplication in Λ and let $\mathcal{C}$ be the associated space–time block code. Then $\rho^{-1}(\mathcal{C}) = \mathcal{I}$ is a fully diverse space–time block code which is a $\mathbb{Z}$-lattice.

If desired, this method can be extended to work for any Noetherian integral domain and central simple algebra over its quotient field. It can be applied for coset coding and wiretap coding analogously as described in [19, Sections 5.2, 5.3].

It would be interesting to investigate which properties of $\mathcal{C}$ carry over to the lattice STBC L and find examples of well performing coset codes.

References

1. Amitsur, A.S.: Differential polynomials and division algebras. Ann. Math. **59**(2), 245–278 (1954)
2. Amitsur, A.S.: Non-commutative cyclic fields. Duke Math. J. **21**, 87–105 (1954)
3. Apel, J.: Gröbnerbasen in Nichtkommutativen Algebren und ihre Anwendung. Dissertation, Leipzig (1988)
4. Bergen, J., Giesbrecht, M., Shivakumar, P.N., Zhang, Y.: Factorizations for difference operators. Adv. Differ. Equ. **2015**, 57 (2015)
5. Bhaintwal, M.: Skew quasi-cyclic codes over Galois rings. Des. Codes Cryptogr. **62**(1), 85–101 (2012)
6. Batoul, A., Guenda, K., Gulliver, T.A.: On self-dual cyclic codes over finite chain rings. Des. Codes Cryptogr. **70**(3), 347–358 (2014)
7. Boucher, D., Solè, P., Ulmer, F.: Skew-constacyclic codes over Galois rings. Adv. Math. Commun. **2**(3), 273–292 (2008)

8. Boucher, D., Ulmer, F.: Linear codes using skew polynomials with automorphisms and derivations. Des. Codes Cryptogr. **70**(3), 405–431 (2014)
9. Boucher, D., Ulmer, F.: Self-dual skew codes and factorization of skew polynomials. J. Symb. Comput. **60**, 47–61 (2014)
10. Boucher, D., Ulmer, F.: Coding with skew polynomial rings. J. Symb. Comput. **44**(12), 1644–1656 (2009)
11. Boucher, D., Ulmer, F.: Codes as Modules Over Skew Polynomial Rings. Cryptography and Coding, Lecture Notes in Computer Science, vol. 5921, pp. 38–55. Springer, Berlin (2009)
12. Boucher, D., Geiselmann, W., Ulmer, F.: Skew-cyclic codes. AAECC **18**, 370–389 (2007)
13. Boulagouaz, M., Leroy, A.: (σ, δ)-codes. Adv. Math. Commun. **7**(4), 463–474 (2013)
14. Bueso, J., Gomez-Torrecillas, J., Verschoren, A.: Methods in Non-commutative Algebra. Kluwer Academic Press, Dordrecht (2003)
15. Cao, Y.: On constacyclic codes over finite chain rings. Finite Fields Appl. **24**, 124–135 (2013)
16. Ceria, M., Mora, T.: Buchberger–Zacharias theory of multivariate Ore extensions. J. Pure Appl. Algebra **221**(12), 2974–3026 (2017)
17. Cohn, P.M.: Skew Fields. Theory of General Division Rings. Encyclopedia of Mathematics and its Applications, **57**. Cambridge University Press, Cambridge (1995)
18. Conway, J.H., Sloane, N.J.: Sphere Packings, Lattices and Groups. Springer, Berlin (1999)
19. Ducoat, J., Oggier, F.: On skew polynomial codes and lattices from quotients of cyclic division algebras. Adv. Math. Commun. **10**(1), 79–94 (2016)
20. Fogarty, N., Gluesing-Luerssen, H.: A circulant approach to skew-constacyclic codes. Finite Fields Appl. **35**, 92–114 (2015)
21. Gómez-Torrecillas, J., Lobillo, F.J., Navarro, G.: A new perspective of cyclicity in convolutional codes. IEEE Trans. Inf. Theory **62**(5), 2702–2706 (2016)
22. Gómez-Torrecillas, J., Lobillo, F.J., Navarro, G.: Convolutional codes with a matrix-algebra word-ambient. Adv. Math. Commun. **10**(1), 29–43 (2016)
23. Gómez-Torrecillas, J., Lobillo, F.J., Navarro, G.: An isomorphism test for modules over a non-commutative PID. Applications to similarity of Ore polynomials. J. Symb. Comput. **75**, 149–170 (2016)
24. Gómez-Torrecillas, J.G., Lobillo, F.J., Navarro, G.: Separable automorphisms on matrix algebras over finite field extensions: applications to ideal codes. In: Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation, ISSAC'15, pp. 189–195, ACM, New York (2015)
25. Gómez-Torrecillas, J., Lobillo, F.J., Navarro, G.: Information-bit error rate and false positives in an MDS code. Adv. Math. Commun. **9**(2), 149–168 (2015)
26. Gómez-Torrecillas, J.: Basic module theory over non-commutative rings with computational aspects of operator algebras. With an appendix by V. Levandovskyy. Lecture Notes in Computer Science 8372, Algebraic and algorithmic aspects of differential and integral operators, pp. 23–82. Springer, Heidelberg (2014)
27. Gao, J.: Kong, Qiong 1-generator quasi-cyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{s-1}\mathbb{F}_{p^m}$. J. Franklin Inst. **350**(10), 3260–3276 (2013)
28. Hoechsmann, Klaus: Simple algebras and derivations. Trans. Am. Math. Soc. **108**, 1–12 (1963)
29. Jacobson, N.: Finite-dimensional division algebras over fields. Springer, Berlin (1996)
30. Kauta, J. S.: Maximal orders and valuation rings in nonassociative quaternion algebras. In: Proceedings of the 39th Symposium on Ring Theory and Representation Theory, pp. 65-74, Symposium Ring Theory Represent. Theory Organ. Commun., Yamaguchi (2007)
31. Kandri-Rody, A., Weispfenning, W.: Non-commutative Gröbner bases in algebras of solvable type. J. Symb. Comput. **9**, 1–26 (1990)
32. Kredel, H.: Solvable Polynomial Rings. Shaker, Herzogenrath (1993)
33. Lee, H.J., Waterhouse, W.C.: Maximal orders in nonassociative quaternion algebras. J. Algebra **146**(2), 441–453 (1992)
34. Levandovskyy, V.: Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation. Dissertation, Kaiserslautern (2005). http://kluedo.ub.uni-kl.de/volltexte/2005/1883/
35. Levandovskyy, V.: PBW bases, non-degeneracy conditions and applications. In: Buchweitz, R.-O., Lenzing, H. (Eds.), Representation of Algebras and Related Topics. Proceedings of the ICRA X Conference, **45**, pp. 229–246 (2005)

36. Liu, X., Liu, H.: LCD codes over finite chain rings. Finite Fields Appl. **34**, 1–19 (2015)
37. Markin, N., Oggier, F.: Iterated space-time code constructions from cyclic algebras. IEEE Trans. Inf. Theory **59**(9), 5966–5979 (2013)
38. Nebe, G., Schaefer, A.: A nilpotent non abelian group code. Algebra Discrete Math. **18**, 268–273 (2014)
39. Nebe, G., Willems, W.: On self-dual MRD codes. Adv. Math. Commun. **10**, 633–642 (2016)
40. Nebe, G., Liebhold, D., Vazquez Castro, A.: Network coding with flags. To appear in Designs, Codes and Cryptography
41. Oggier, F., Sethuraman, B.A.: Quotients of orders in cyclic algebras and space–time codes. Adv. Math. Commun. **7**(4), 441–461 (2013)
42. Ore, O.: Formale Theorie der linearen Differentialgleichungen. (Zweiter Teil). (German). J. Reine Angew. Math. **168**, 233–252 (1932)
43. Ore, O.: Theory of noncommutative polynomials. Ann. Math. **2**, 480–508 (1933)
44. Pesch, M.: Gröbner Bases in Skew Polynomial Rings. Shaker, Herzogenrath (1998)
45. Pesch, M.: Two-sided Gröbner bases in iterated Ore extensions. Prog. Comput. Sci. Appl. Logic **15**, 225–243 (1991). Birkhäuser
46. Petit, J.-C.: Sur certains quasi-corps généralisant un type d'anneau-quotient, Séminaire Dubriel. Algèbre et théorie des nombres 20 (1966–67), 1-18
47. Petit, J.-C. : Sur les quasi-corps distributifes à base momogène, C. R. Acad. Sc. Paris 266 Série A, 402–404 (1968)
48. Pumplün, S., Steele, A.: Fast-decodable MIDO codes from nonassociative algebras. Int. J. Inf. Coding Theory (IJICOT) **3**(1), 15–38 (2015)
49. Pumplün, S., Steele, A.: The nonassociative algebras used to build fast-decodable space–time block codes. Adv. Math. Commun. **9**(4), 449–469 (2015)
50. Pumplün, S.: How to obtain division algebras used for fast decodable space-time block codes. Adv. Math. Commun. **8**(3), 323–342 (2014)
51. Pumplün, S.: Finite nonassociative algebras obtained from skew polynomials and possible applications to (f, σ, δ)-codes. Adv. Math. Commun. **11**(3), 615–634 (2017). doi:10.3934/amc.2017046
52. Sandler, R.: Autotopism groups of some finite non-associative algebras. Am. J. Math. **84**, 239–264 (1962)
53. Schafer, R.D.: An Introduction to Nonassociative Algebras. Dover Publications Inc., New York (1995)
54. Srinath, K.P., Rajan, B.S.: Fast-decodable MIDO codes with large coding gain. IEEE Trans. Inf. Theory **2**(60), 992–1007 (2014)
55. Steele, A., Pumplün, S., Oggier, F.: MIDO space–time codes from associative and non-associative cyclic algebras. In: IEEE Information Theory Workshop (ITW) 2012, pp. 192–196 (2012)
56. Steele, A.: Nonassociative cyclic algebras. Isr. J. Math. **200**(1), 361–387 (2014)
57. Waterhouse, W.C.: Nonassociative quaternion algebras. Algebras Gr. Geom. **4**, 365–378 (1987)
58. Weispfenning, V.: Finite Gröbner bases in non-noetherian skew polynomial rings. In: Proceedings ISSAC'92, pp. 320–332. ACM (1992)
59. Wu, M.: Free cyclic codes as invariant submodules over finite chain rings. Int. Math. Forum **8**(37–40), 1835–1838 (2013)