ON SKEW POLYNOMIAL CODES AND LATTICES FROM QUOTIENTS OF CYCLIC DIVISION ALGEBRAS

JÉRÔME DUCOAT AND FRÉDÉRIQUE OGGIER
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore

(Communicated by Camilla Hollanti)

Abstract. We propose a variation of Construction A of lattices from linear codes defined using the quotient \( \Lambda/p\Lambda \) of some order \( \Lambda \) inside a cyclic division \( F \)-algebra, for \( p \) a prime ideal of a number field \( F \). To obtain codes over this quotient, we first give an isomorphism between \( \Lambda/p\Lambda \) and a ring of skew polynomials. We then discuss definitions and basic properties of skew polynomial codes, which are needed for Construction A, but also explore further properties of the dual of such codes. We conclude by providing an application to space-time coding, which is the original motivation to consider cyclic division \( F \)-algebras as a starting point for this variation of Construction A.

1. Introduction

Connections between Euclidean lattices and linear codes over finite alphabets have been classically studied, through a series of constructions referred to as Constructions A,B,C,D or E [9]. Given the finite field \( \mathbb{F}_2 \), the original (binary) Construction A [12] considers the map \( \rho : \mathbb{Z}^N \to \mathbb{F}_2^N \) of reduction modulo 2 componentwise, for \( N \) some positive integer. If \( C \) is a binary linear code of length \( N \), then \( \rho^{-1}(C) \) (or its normalized version \( \frac{1}{\sqrt{2}} \rho^{-1}(C) \)) is a lattice. A series of duality follows, such as a correspondence between the dual code \( C^\perp \) of \( C \) and the dual lattice \( L^* \) of \( L \), self-dual codes and unimodular lattices, or between the weight enumerator of the code \( C \) and the theta series of the lattice \( L \). Construction A has been generalized in many ways, including, for citing a few examples, to: (1) cyclotomic fields \( \mathbb{Q}(\zeta_p) \) [11], where \( \zeta_p \) is a primitive \( p \)th root of unity, and \( p \) is prime, in which case \( \rho \) becomes the componentwise reduction modulo the prime ideal \( (1 - \zeta_p) \) of a vector with coefficients in the ring of integers \( \mathbb{Z}[\zeta_p] \), (2) to quadratic and imaginary fields and totally definite quaternion algebras over \( \mathbb{Q} \) as a way to construct modular lattices in [2], (3) to the construction of unimodular lattices using quaternary quadratic residue codes [5].

Construction A is also of interest from a communication point of view, since it provides a concrete way of doing coset coding [12], an encoding technique which is very useful to encode lattices, since it provides a natural way of mapping elements from finite alphabets (codewords) to real or complex symbols (lattice points).

2010 Mathematics Subject Classification: Primary: 11S45; Secondary: 11T71, 94B40.

Keywords and phrases: Constacyclic codes, division algebras, skew polynomial rings, space-time codes.

This work was supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07.
This paper addresses a variation of Construction A in the context of division algebras, and cyclic division algebras over a cyclic number field extension $K/F$ in particular. Denote by $O_F$ and $O_K$ their respective rings of integers, and by $\sigma$ the generator of the Galois group of $K/F$. Instead of using as a starting point the quotient of a number field by an ideal (as in [11] for example), we consider a specific $O_F$-order $\Lambda$ in a cyclic division $F$-algebra, and the quotient $\Lambda/p\Lambda$ for $p$ a prime ideal of $O_F$. Our motivation for this construction is two-fold: on the one hand, our construction can be seen as generalization of Construction A over cyclic division algebras, and on the other hand, we obtain an explicit way to do coset coding in the context of space-time coding, where codes with a lattice structure are commonly obtained from cyclic division algebras [4].

As shown in Section 2, the quotient $\Lambda/p\Lambda$ turns out to be isomorphic to the ring of skew polynomials $(O_K/pO_K)[x;\sigma]/(x^n - u)$, where $u$ is determined by the choice of the cyclic division $F$-algebra. To mimic the steps involved in Construction A, we next consider the problem of designing codes over $(O_K/pO_K)[x;\sigma]/(x^n - u)$ in Section 3, where a variation of Construction A is given. Let $\mathbb{F}_q$ denote the finite field with $q$ elements, $q$ a prime power. Codes over the skew polynomial ring $\mathbb{F}_q[x;\sigma]/(f(x))$, for $(f(x))$ a two sided ideal of $\mathbb{F}_q[x;\sigma]$, were introduced in [7] and furthermore studied in the context of cyclic codes in [6]. A generalization to Galois rings was obtained in [8]. We propose some basic definitions and properties of codes over the skew polynomial ring $(O_K/pO_K)[x;\sigma]/(x^n - u)$, by taking inspiration from [8] and generalizing some of the known results for the ring $\mathbb{F}_q[x;\sigma]/(f(x))$. We note that our results could be easily generalized to the case $(O_K/pO_K)[x;\sigma]/(f(x))$, which is not done in this paper because of our focus on cyclic division algebras.

Once equipped with suitable definitions for skew polynomial codes over the ring $(O_K/pO_K)[x;\sigma]/(x^n - u)$, it is natural to wonder about the dual of such codes. This is studied in Section 4.

We conclude by going back to the motivation to consider this variation of Construction A over a cyclic division $F$-algebra, namely its application to space-time coding, or more precisely, to derive a way to perform coset encoding, as detailed in Section 5.

2. Quotients of Cyclic Division Algebras

Let $K/F$ be a number field extension of degree $n$ with cyclic Galois group $\langle \sigma \rangle$, and respective rings of integers $O_K$ and $O_F$. Consider the cyclic $F$-algebra $A$ defined by

$$K \oplus Ke \oplus \cdots Ke^{n-1}$$

where $e^n = u \in F$, and $ek = \sigma(k)e$ for $k \in K$. We assume that $u^i, i = 0, \ldots, n - 1$, are not norms in $K/F$ so that the algebra is division ([4, Corollary VII.1.12]), and furthermore that $u \in O_F$.

**Definition 2.1.** For $S$ a Noetherian integral domain with quotient field $F$, and $A$ a finite dimensional $F$-algebra, an $S$-order in $A$ is a subring $\Lambda$ of $A$, having the same identity as $A$, and such that $\Lambda$ is a finitely generated module over $S$ and generates $A$ as a linear space over $F$. An order $\Lambda$ is called maximal if it is not properly contained in any other $S$-order.

Then

$$\Lambda = O_K \oplus O_K e \oplus \cdots \oplus O_K e^{n-1}$$
is an $O_F$-order of $A$ (we repeat that we assume that $u \in O_F$), which is typically not maximal. It is often called the natural order in the context of space-time coding.

Let $p$ be a prime ideal of $O_F$ so that $pA$ is a two-sided ideal of $A$, and $O_F/pO_F$ is isomorphic to the finite field $\mathbb{F}_{p^f}$, where $p$ is the prime number lying below $p$ and $f$ is the inertial degree of $p$ above $p$. Since $\Lambda$ is an $O_F$-module, we have the following ring homomorphism:

$$O_F \to \Lambda \to \Lambda/p\Lambda$$

and the image of $p = pA \cap O_F$ obviously lies in $pA$. Hence, it yields a ring homomorphism $\mathbb{F}_{p^f} = O_F/p \to \Lambda/p\Lambda$, which means that $\Lambda/p\Lambda$ is an $\mathbb{F}_{p^f}$-algebra.

From [14], we have the following $\mathbb{F}_{p^f}$-algebra isomorphism:

$$\Lambda/p\Lambda \cong (O_K/pO_K) \oplus (O_K/pO_K)e \oplus \cdots \oplus (O_K/pO_K)e^{n-1},$$

where $e(k + pO_K) = (\sigma(k) + pO_K)e$ for all $k \in O_K$ and $e^n = u + p$.

Indeed, since $p$ is a prime ideal of $O_F$ and $\sigma_F = \text{id}_F$, we have $\sigma(pO_K) \subset pO_K$, which means that $\sigma$ can be factorized as a ring homomorphism by the natural projection $\pi: O_K \to O_K/pO_K :$ more explicitly, there exists a ring homomorphism $\sigma: O_K/pO_K \to O_K/pO_K$ such that $\sigma = \sigma \circ \pi$. By a slight abuse of notation, we keep the notation $\sigma$ for the map $\sigma$.

Since $O_K$ is a Dedekind domain, $pO_K = p_1^{e_1}p_2^{e_2}\cdots p_g^{e_g}$ with $p_i$ a prime ideal of $O_K$ and $e_i \geq 0$ for $i = 1, \ldots, g$.

In the particular case where $p$ is inert in $K/F$, $pO_K$ is a prime ideal of $O_K$. Then the finite ring $O_K/pO_K$ is an integral domain, so it is isomorphic to the finite field $\mathbb{F}_{p^{ef}}$. The induced ring homomorphism $\sigma: \mathbb{F}_{p^{ef}} = O_K/pO_K \to O_K/pO_K = \mathbb{F}_{p^f}$ is thus a generator of the cyclic Galois group of $\mathbb{F}_{p^f}/\mathbb{F}_{p^f}$.

**Definition 2.2.** Given a ring $S$ with a group $G = \langle \sigma \rangle$ acting on it, the skew polynomial ring $S[x;\sigma]$ is the set of all polynomials $s_0 + s_1x + \ldots + s_mx^m$, $s_i \in S$, $m \geq 0$ with multiplication twisted by the relation $xs = \sigma(s)x$ for all $s \in S$.

We will consider the skew polynomial ring $(O_K/pO_K)[x;\sigma]$. Note that since $u \in F$, $x^n - u$ belongs to the center of $(O_K/pO_K)[x;\sigma]$ and the ideal $(x^n - u)$ is two-sided.

**Lemma 2.3.** There is an $\mathbb{F}_{p^f}$-algebra isomorphism between $\Lambda/p\Lambda$ and the quotient $(O_K/pO_K)[x;\sigma]/(x^n - u)$.

**Proof.** We define the map

$$\varphi: (O_K/pO_K)[x;\sigma] \to \Lambda/p\Lambda$$

$$f(x) \mapsto f(e)$$

Using the isomorphism given above and in [14], it is easily seen that $\varphi$ is a surjective $\mathbb{F}_{p^f}$-algebra homomorphism. Moreover, the kernel of $\varphi$ is the two-sided ideal of $(O_K/pO_K)[x;\sigma]$ generated by $x^n - u$. Indeed, it is easily seen that $x^n - u$ lies in $\ker(\varphi)$. Conversely, let $f(x) \in \ker(\varphi)$. We write

$$f(x) = \sum_{i=0}^{m} s_i x^i, \quad s_i \in O_K/pO_K, \quad i = 0, \ldots, m.$$ 

Then $f(e) = 0$ in $\Lambda/p\Lambda$. The ring $(O_K/pO_K)[x;\sigma]$ is not always right or left Euclidean, as it would be if $O_K/pO_K$ were a finite field. However, since $x^n - u$ is a monic polynomial (or more precisely since its leading coefficient is a unit in
\( \mathcal{O}_K/p\mathcal{O}_K \), we can still perform the long division algorithm: indeed, if \( m \geq n \), we may perform a right division of \( f(x) \) by \( x^n - u \) as follows. Note that the polynomial
\[
 f(x) - s_m x^{m-n}(x^n - u) = \sum_{i=0}^{m-1} s_i x^i + s_m u x^{m-n}
\]
has degree smaller than that of \( f \). This procedure of subtracting left multiple of \( x^n - u \) can be repeated until we obtain a polynomial of degree smaller than \( n \), thus, there exist some polynomials \( g(x) \) and \( h(x) \) such that
\[
 f(x) = g(x)(x^n - u) + h(x)
\]
where \( h(x) \) has degree \( \leq n - 1 \). Hence, \( f(e) = 0 \) is equivalent to \( h(e) = 0 \). Yet, \( 0 = h(e) = r_0 + r_1 e + \cdots + r_{n-1} e^{n-1} \) in \( \Lambda/p\Lambda \cong (\mathcal{O}_K/p\mathcal{O}_K) \oplus (\mathcal{O}_K/p\mathcal{O}_K)e \oplus \cdots \oplus (\mathcal{O}_K/p\mathcal{O}_K)e^{n-1} \). Therefore, \( r_0 = r_1 = \cdots = r_{n-1} = 0 \) and \( h(x) = 0 \). We conclude that \( f(x) \) is a (left) multiple of \( x^n - u \). Consequently, \( \ker(\varphi) = (x^n - u) \) and we get the desired isomorphism.

This lemma generalizes the isomorphism of [10, Lemma 1] for \( p \) inert.

Denote by \( \psi \) the inverse isomorphism of the one given in Lemma 2.3:
\[
 \psi : \Lambda/p\Lambda \cong (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]/(x^n - u).
\]

Let \( I \) be a left ideal of \( \Lambda \). Assume that \( I \cap \mathcal{O}_K \supset p \). Then \( I/p\Lambda \) is an ideal of \( \Lambda/p\Lambda \).

In the sequel, we will study the left ideal \( \psi(I/p\Lambda) \) of \( (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]/(x^n - u) \).

**Remark 1.** The quotient \( \Lambda/p\Lambda \) can be looked at from different view points (see [14] for a different approach that aims at a classification result). In this paper, we will pursue the skew polynomial ring view point, as discussed in the coming section.

## 3. Skew-polynomial codes and a variation of Construction A

Classical cyclic codes over the finite field \( \mathbb{F}_q \) are ideals of the polynomial ring \( \mathbb{F}_q[x]/(x^n - 1) \). Since this is a principal ideal domain, every ideal has a generator polynomial, which in turn defines a cyclic code, and codewords are then multiples of this generator polynomial. In [7], the definition of codes over polynomial rings was extended to that of codes over the skew-polynomial rings \( \mathbb{F}_q[x; \sigma] \). We are interested here in codes over the skew-polynomial rings \( (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]/(x^n - u) \).

### 3.1. Division in skew-polynomial rings

A first major difference between \( \mathbb{F}_q[x; \sigma] \) and \( (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma] \) is, as noted in the proof of Lemma 2.3, that the skew polynomial ring \( (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma] \) is not in general right or left Euclidean anymore. However, this can be sorted out, using the same technique as that explained in [8], which was also used for the proof of Lemma 2.3.

Let \( f(x) = \sum_{i=0}^{m} s_i x^i \) and \( g(x) = \sum_{i=0}^{l} t_i x^i \) be two polynomials of respective degree \( m \) and \( l \), with coefficients in \( \mathcal{O}_K/p\mathcal{O}_K \). Suppose that \( t_l \) is invertible and \( m > l \), then a right (respectively left) division of \( f(x) \) by \( g(x) \) is obtained as follows: consider the polynomial
\[
 f(x) - \frac{s_m}{\sigma^{m-l}(t_l)} x^{m-l} g(x)
\]
respectively
\[
 f(x) - g(x) \sigma^{-l} \left( \sum_{i=0}^{m-1} \frac{s_i}{t_i} \right) x^{m-l}.
\]
Since \( \sigma \) is an automorphism, \( 1 = \sigma(t_i t_i^{-1}) = \sigma(t_i) \sigma(t_i^{-1}) \), which implies that \( \sigma(t_i) \) is invertible. Hence, \( \sigma(t_i) \) is invertible for all \( 1 \leq j \leq m \). Moreover, we have

\[
\begin{align*}
f(x) - \frac{s_m}{\sigma^{m-l}(t_i)}x^{m-l}g(x) &= f(x) - s_m x \sigma^{m-l-1}(t_i^{-1}) x^{m-l}g(x) = \\
&= f(x) - s_m x^{m-l} \sigma^{m-l-(m-l)}(t_i^{-1}) g(x) \\
&= f(x) - s_m x^{m-l} t_i^{-1}(t_1 x') + \sum_{i=0}^{l-1} t_i x^i \\
&= f(x) - s_m x^m - \sum_{i=0}^{l-1} s_m \sigma^{m-l}(t_i^{-1} t_i) x^{i+m-l}.
\end{align*}
\]

Similarly, we have

\[
\begin{align*}
f(x) - g(x) \sigma^{-l} \left( \frac{s_m}{t_i} \right) x^{m-l} &= f(x) - \sum_{i=0}^{l} t_i x^i \sigma^{-l} \left( \frac{s_m}{t_i} \right) x^{m-l} \\
&= f(x) - \sum_{i=1}^{l} t_i x^{i-1} \sigma^{-l} \left( \frac{s_m}{t_i} \right) x^{m-l+1} - t_0 \sigma^{-l} \left( \frac{s_m}{t_i} \right) x^{m-l} \\
&= \cdots \\
&= f(x) - \sum_{i=0}^{l} t_i \sigma^{-i} \left( \frac{s_m}{t_i} \right) x^{m-l+i} \\
&= f(x) - s_m x^m - \sum_{i=0}^{l-1} t_i \sigma^{-i} \left( \frac{s_m}{t_i} \right) x^{m-l+i}.
\end{align*}
\]

Hence, both polynomials \( f(x) - \frac{s_m}{\sigma^{m-l}(t_i)} x^{m-l} g(x) \) and \( f(x) - g(x) \sigma^{-l} \left( \frac{s_m}{t_i} \right) x^{m-l} \) have degree \( < m \). Therefore this procedure can be iterated, to find polynomials \( q(x), r(x) \) such that

\[
f(x) = q(x) g(x) + r(x), \quad \text{resp.} \quad f(x) = g(x) q(x) + r(x), \quad \deg(r(x)) < \deg(g(x)).
\]

If \( r(x) = 0 \), we say that \( g(x) \) is a right, resp. left, divisor of \( f(x) \).

We next discuss the unicity of the remainder of this division. Suppose

\[
f(x) = q_1(x) g(x) + r_1(x) = q_2(x) g(x) + r_2(x)
\]

then \( (q_1(x) - q_2(x)) g(x) = r_2(x) - r_1(x) \). Suppose that \( q_1(x) - q_2(x) \) is not zero, then the degree of \( (q_1(x) - q_2(x)) g(x) \) is greater than \( \deg(g(x)) \), while the degree of \( r_2(x) - r_1(x) \) is less than \( \deg(g(x)) \), therefore \( q_1(x) = q_2(x) \) and \( r_1(x) = r_2(x) \).

The proof for left division is done similarly.

3.2. Principal ideals and codes. Thanks to the unicity of the remainder, the skew polynomials of degree less than \( n \) are canonical representatives of the elements of \( (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[x; \sigma]/(x^n - u) \).

**Lemma 3.1.** Any right divisor \( g(x) \) of \( x^n - u \) generates a left principal ideal \( (g(x))/(x^n - u) \) of \( (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[x; \sigma]/(x^n - u) \). The set of left multiples of \( g(x) \) by skew polynomials of degree less than \( k = n - \deg(g(x)) \) are canonical representatives of the elements of \( (g(x))/(x^n - u) \).
Proof. For any right divisor \( g(x) \) of \( x^n - u \), the ideal \( (x^n - u) \) is contained in \( (g(x)) \). By the correspondence theorem for rings, \( (g(x))/(x^n - u) \) is a left ideal of \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u) \). Since skew polynomials of degree less than \( n \) are canonical representatives, the elements of the ideal \( (g(x))/(x^n - u) \) are left multiples of \( g(x) \) by skew polynomials of degree less than \( k = n - \deg g(x) \).

**Corollary 1.** For \( g(x) \) a right divisor of \( x^n - u \), the ideal \( (g(x))/(x^n - u) \) is an \( \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \)-module, isomorphic to a submodule of \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n \). It forms a code of length \( n \) and of dimension \( k = n - \deg g(x) \) over \( \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \), consisting of codewords \( a = (a_0, a_1, \ldots, a_{n-1}) \) that are coefficient tuples of the left multiples \( a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \) of \( g(x) \). This code is called a \( \sigma \)-constacyclic code.

**Proof.** Let \( g(x) \) be a right divisor of \( x^n - u \) in \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] \). The left ideal \( (g(x)) \) in \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] \) is then an \( \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \)-module and by taking the quotient by the monic skew-polynomial \( x^n - u \), \( (g(x))/(x^n - u) \) is a submodule of the free \( \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \)-module \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u) \) of rank \( n \). By Lemma 1, the images of the skew polynomials \( g(x), xg(x), \ldots, x^{k-1}g(x) \) in the quotient \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u) \) form a basis of \( g(x)/(x^n - u) \) as an \( \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \)-module. We then use the \( \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \)-module isomorphism

\[
(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u) \rightarrow (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n
\]

\[
\sum_{i=0}^{n-1} a_i x^i + (x^n - u)(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] \mapsto (a_0, \ldots, a_{n-1})
\]

to conclude.

Note that for a \( \sigma \)-constacyclic code \( \mathcal{C} \), corresponding to a left principal ideal \( \mathcal{I} \) of \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u) \), if \( (a_0, \ldots, a_{n-1}) \in \mathcal{C} \), then \( a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \in \mathcal{I} \), and \( xa(x) \in \mathcal{I} \). Since

\[
xa(x) = x(a_0 + a_1x + \ldots + a_{n-1}x^{n-1}) = \sigma(a_0)x + \sigma(a_1)x^2 + \ldots + \sigma(a_{n-1})u
\]

we have that

\[
(u\sigma(a_{n-1}), \sigma(a_0), \ldots, \sigma(a_{n-1})) \in \mathcal{C},
\]

which explains the choice of the terminology “constacyclic”.

Let us comment on the proposed definition of \( \sigma \)-constacyclic code.

1. We could also use the terminology central \( \sigma \)-code proposed in [7] since \( x^n - u \) lies in the center of \( (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] \).
2. A cyclic code would correspond to the case \( u = 1 \).
3. This definition could be made more general by considering another suitable polynomial than \( x^n - u \), which would yield a complete generalization of the definition of \( \sigma \)-code proposed in [7]. This is not done here, simply because the polynomial is given by the cyclic algebra structure, but this could be an interesting research direction of its own.
4. Finally, we may (and do) restrict our study of \( \sigma \)-constacyclic codes to right divisors \( g(x) \) of \( x^n - u \) that are monic: indeed, if \( g(x) \) has leading coefficient \( a \), it is necessarily invertible (since \( g(x) \) is a divisor of \( x^n - u \) and the constacyclic codes derived from \( g(x) \) and \( a^{-1}g(x) \) are equal.

The next result describes a parity check polynomial.
Proposition 1. Set $h(x) = \sum_{i=0}^{k-1} h_i x^i + x^k$. If $h(x)g(x) = x^n - u$, then
$$g(x)h(x) = x^n - u.$$ Furthermore, let $C$ be the code generated by $g(x)$. Let $a \in (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)^n$ and let $a(x)$ be its corresponding polynomial. Then $a$ is a codeword of $C$ if and only if $a(x)h(x) = 0$ in $(\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[x; \sigma]/(x^n - u)$.

Proof. Since $x^n - u$ is central,
$$h(x)g(x)h(x) = (x^n - u)h(x) = h(x)(x^n - u) = h(x)h(x)g(x)$$
and
$$h(x)[g(x)h(x) - h(x)g(x)] = 0.$$ The first claim follows from the fact that $h(x)$ is monic and thus not a zero divisor.

If $a \in C$ then $a(x) = b(x)g(x)$ and using the first claim
$$a(x)h(x) = b(x)g(x)h(x) = 0 \mod x^n - u.$$ Conversely, if $a(x)h(x) = 0$, then for some $b(x)$, $a(x)h(x) = b(x)(x^n - u) = b(x)g(x)h(x)$. Since $h(x)$ is monic and thus not a zero divisor, $a(x) = b(x)g(x)$ as needed. \qed

3.3. A Construction A. Using the isomorphism $\psi$ defined in Section 2, for every left ideal $\mathcal{I}$ of $\Lambda$, we consider the $\sigma$-code $C = \psi(\mathcal{I}/\mathcal{p}\Lambda)$ over $\mathbb{F}_q$.

A lattice of dimension $N$ is here a discrete additive subgroup of $\mathbb{R}^N$ of rank $N$ as a $\mathbb{Z}$-module.

We set the map :
$$\rho : \Lambda \rightarrow \psi(\mathcal{I}/\mathfrak{p}\Lambda) = (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[x; \sigma]/(x^n - u),$$
compositum of the canonical projection $\Lambda \rightarrow \Lambda/\mathfrak{p}\Lambda$ with $\psi$. Then
$$L = \rho^{-1}(\mathcal{O}) = \mathcal{I}$$
is a lattice in $\mathbb{R}^N$, that is a $\mathbb{Z}$-module of rank $N = n^2[F : \mathbb{Q}]$ since $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank $n[F : \mathbb{Q}]$. The embedding into $\mathbb{R}^N$ is obtained by considering $A \otimes_{\mathbb{Q}} \mathbb{R}$ for $A$ the cyclic division $F$-algebra under consideration.

From this point of view, the above construction may be interpreted as a variation of Construction A [9], which consists of obtaining a lattice from a linear code over a finite field (ring), as shortly described in the introduction. This is also a generalization of the lattice construction of [13], defined over number fields.

3.4. Examples. Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$. Let $\Omega$ be the quaternion division algebra defined by
$$\Omega = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e,$$with $e^2 = -1$. Since $N_{K/F}(a + ib) = a^2 + b^2$, $a, b \in \mathbb{Z}$, $-1$ cannot be a norm and $\Omega$ is indeed a quaternion division algebra. We set $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$.

We provide different examples based on primes with different ramification.

Example 1. Set $p = 3$, which remains inert in $\mathbb{Q}(i)$. Hence, $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$ and $\Lambda/3\Lambda \simeq \mathbb{F}_9 \oplus \mathbb{F}_9 e$. Take $\mathcal{I} = (1 + i + e)\Lambda$. Then $\mathcal{I}$ contains 3 since the reduced norm of $1 + i + e$ is $N(1 + i + e) = (1 + i + e)(1 - i - e) = 3$. Let $\alpha$ denote a primitive root of $\mathbb{F}_9$ over $\mathbb{F}_3$, satisfying $\alpha^2 + 1 = 0$ and note that $\sigma$ becomes the generator of the Galois group of $\mathbb{F}_9/\mathbb{F}_3$, $\sigma(\alpha) = \alpha^3$. We have
$$\psi((1 + i + e) \mod 3) = 1 + \alpha + x,$$
which is a right divisor of $x^2 + 1$ in $F_9[x; \sigma]$:

$$(x - 1 + \alpha)(x + 1 + \alpha) = x^2 + \sigma(1 + \alpha) x + (\alpha - 1) x + (\alpha + 1)(\alpha - 1) = x^2 + 1.$$  

Therefore, the left ideal $(x + 1 + \alpha)F_9[x; \sigma]/(x^2 + 1)$ consisting of the left multiples of $x + 1 + \alpha$ modulo $x^2 + 1$ is a $\sigma$-constacyclic code of length $n = 2$ and dimension $k = n - \deg g(x) = 1$. Left multiples of $x + 1 + \alpha$ modulo $x^2 + 1$ are explicitly given by $(b_0 + b_1 x)(x + \alpha + 1) = [b_0(\alpha + 1) - b_1] + [b_0 + b_1(1 - \alpha)] x$ and codewords are of the form

$$(a_0, a_1) = ((\alpha + 1)a_1, a_1), \; a_1 \in F_9.$$  

Taking the pre-image by $\psi$, it corresponds to the left-ideal $I/3\Lambda$, with $I = (1 + i + e)\Lambda$.

**Example 2.** Set $p = 5$, which splits in $Q(i)$, namely $(5) = (1 + 2i)(1 - 2i)$. Then $Z[i]/5Z[i] \cong Z[i]/(1 + 2i) \times Z[i]/(1 - 2i) \cong F_5 \times F_5$ and $\Lambda/5\Lambda \cong (F_5 \times F_5) \oplus (F_5 \times F_5) e$. The first isomorphism comes from the Chinese Remainder Theorem, since $(1 - 2i)$ and $(1 + 2i)$ are coprime. An element of $Z[i]$ is mapped to $F_5 \times F_5$ via the composition of the natural projection and the above isomorphism by $\pi : a + ib \mapsto (a + 2b \mod 5, a + 3b \mod 5)$. Since $\pi((a + ib)(c + di)) = \pi(ac - bd + i(ad + bc)) = (ac - bd + 2(ad + bc) \mod 5, ac - bd + 3(ad + bc) \mod 5)$ while $\pi((a + ib)(c + di)) = (a + 2b \mod 5, a + 3b \mod 5, c + 3d \mod 5) = (ac + 2ad + 2bc - b \mod 5, ac + 3ad + 3bc - b \mod 5)$, and $\pi(a + ib + c + i d) = a + c + 2(b + d) = a + 2b + c + 2d = (a + ib) + \pi(c + id)$, $\pi$ is indeed a ring homomorphism. Note that $\sigma$ becomes the isomorphism of the form $(a, b), a \in F_5$. Take $I = (1 + 2e)\Lambda$, which contains 5 since the reduced norm of 1 + 2c is $N(1 + 2c) = (1 + 2e)(1 - 2e) = 5$. Then

$$\psi((1 + 2e)\mod 5) = (1, 1) + (2, 2)x,$$

which is a divisor of $x^2 + 1$, since

$$((1, 1) + (2, 2)x)((1, 1) - (2, 2)x) = (1, 1) - (2, 2)x + (2, 2)x + (1, 1)x^2.$$

Then the left ideal $((1, 1) + (2, 2)x)(F_5 \times F_5)[x; \sigma]/(x^2 + 1)$ forms a $\sigma$-constacyclic code of length $n = 2$ and $k = 1$. Codewords are of the form $[(b_0, b_1) + (c_0, c_1)x][(1, 1) + (2, 2)x]$ or equivalently, $[(b_0, b_1) + (c_0, c_1)x][(3, 3) + (1, 1)x] = [(3b_0, 3b_1) - (c_0, c_1)] + [(b_0, b_1) + (3c_0, 3c_1)]x$, that is

$$(3a, a), \; a = (a_0, a_1) \in F_5 \times F_5.$$  

Again, taking the pre-image by $\psi$, it corresponds to the left-ideal $I/5\Lambda$, with $I = (1 + 2e)\Lambda$.

**Example 3.** Set $p = 2$, which is ramified in $Q(i)$: $(2) = (1 + i)^2$. Then $Z[i]/2Z[i] \cong F_2 + vF_2 = \{0, 1, v, v + 1\}$ with $v^2 = 0$, and $\Lambda/2\Lambda \cong (F_2 + vF_2) \oplus (F_2 + vF_2)e$. In this case, the natural projection $\pi$ from $Z[i]$ to $F_2 + vF_2$ is given by $\pi : a + ib \mapsto (a + b \mod 2)$. We check that $\pi$ is a ring homomorphism:

$$\pi((a + ib)(c + di)) = \pi(ac - bd + i(ad + bc)) = (ac + bd + ad + bc \mod 2) + \pi(ad + bc \mod 2)$$

while $\pi(a + ib)\pi(c + di) = ((a + b \mod 2) + v(b \mod 2))(c + d \mod 2) + v(d \mod 2) = (a + b)(c + d) \mod 2 + (a + b)b + v(b \mod 2)(c + d) \mod 2 + v(b \mod 2)(c + d) \mod 2 + v(c + d) \mod 2.$

Moreover, since $p = 2$ totally ramifies in $Z[i]$, $\sigma$ becomes the identity map. Take $I = (1 + e)\Lambda$, which contains 2 since the reduced norm of $(1 + e)$ is $N(1 + e) = (1 + e)(1 - e) = 2$. Then

$$\psi((1 + e)\mod 2) = 1 + x,$$
which is a divisor of $x^2 + 1 = (x + 1)(x + 1)$. As in the previous cases, the left ideal $(1 + x)([F_2 + vF_2][x; \sigma]/x^2 + 1)$ forms a $\sigma$-constacyclic code of length $n = 2$ and $k = 1$. Codewords are of the form $(b_0 + b_1 x)(1 + x)$, that is we get the repetition code

$$(a_0, a_1) = (a_0, a_0), \quad a_0 \in F_2 + vF_2.$$ 

As above, taking the pre-image by $\psi$, it corresponds to the left-ideal $I/2\Lambda$, with $I = (1 + e)\Lambda$.

4. DUAL CODES AND LATTICES

Having defined constacyclic codes over $(O_K/pO_K)[x; \sigma]/(x^n - u)$, it is natural to wonder about the dual of such codes.

4.1. Dual codes. Consider the following Euclidean scalar product in $(O_K/pO_K)^n$:

$$\langle y, z \rangle = \sum_{i=1}^{n} y_i z_i.$$

**Definition 4.1.** For an $(n, k)$ code $C$, its Euclidean dual code $C^\perp$ is given by

$$C^\perp = \{y, \langle c, y \rangle = 0 \text{ for all } c \in C\}.$$ 

An $(n, k)$ code $C$ is said to be Euclidean self-dual if $C$ is equal to its Euclidean dual.

It is probably helpful to recall how the generator polynomial of a cyclic code over a finite field is computed. Take $h(x)$ its parity check polynomial, with degree $d$ and constant term $h_0$, and compute $h_0^{-1} x^d h(x^{-1})$. The procedure in the case of interest here is somewhat similar, except for one difficulty: we need to give a meaning to $h(x^{-1})$ in the non-commutative case, which is classically done through localization (as also done in [8]) and the notion of right Ore set.

**Definition 4.2** ([1, Def. II.2.3]). An Ore set $S$ is a multiplicative subset of a ring $R$ that satisfies the right Ore condition, namely $S$ satisfies the following three conditions:

1. $S$ is closed under multiplication, and $1 \in S$.
2. For any $s \in S$, $s$ is not a left or right zero divisor.
3. Right Ore condition: for all $r \in R$ and $s \in S$, there exist $r_1 \in R$ and $s_1 \in S$ such that $sr_1 = rs_1$.

It is known [1, Thm II.2.4] that given a ring $R$, if $S \subset R$ is a right Ore set, then there is a ring $RS^{-1}$ of right fractions and an injective ring homomorphism $R \to RS^{-1}$ such that (a) the image of every element $r \in R$ is invertible in $RS^{-1}$, and (b) every element of $RS^{-1}$ can be written as a product $rs^{-1}$.

**Proposition 2.** Consider the ring $(O_K/pO_K)[x; \sigma]$ as above, and take $S$ to be $S = \{x^i, i \geq 0\}$. Then $S$ is a right Ore set, and the right localization $(O_K/pO_K)[x; \sigma]S^{-1}$ exists. Furthermore, the subring $A = \{\sum_{i=0}^{d} x^{-i} a_i\}$ of $(O_K/pO_K)[x; \sigma]S^{-1}$, with multiplication $ax^{-1} = x^{-1} \sigma(a)$ is isomorphic to the ring $(O_K/pO_K)[x^{-1}, \sigma^{-1}]$.

**Proof.** We need to check the definition of an Ore set.

Let us check the right Ore condition: for all $r \in R = (O_K/pO_K)[x; \sigma]$ and $s \in S$, there exist $r_1 \in R$ and $s_1 \in S$ such that $sr_1 = rs_1$. Take $s = x^i \in S$ for some $i$, and $r = r(x) = \sum_{i=0}^{d} r_i x^i \in (O_K/pO_K)[x; \sigma]$. We need to show that
there exists $r_1 = r_1(x)$ such that $x^i r_1(x) = r(x) x^j$ for some $x^j$. Pick $j \geq i$ and $r_1(x) = \sum_{l=0}^d \sigma^{-i}(r_1) x^{j+l-i}$. Then
\[
x^i \sum_{l=0}^d \sigma^{-i}(r_1) x^{j+l-i} = \sum_{l=0}^d r_1 x^{j+l} = r_1(x) x^j
\]
as needed to show the existence of the localization $(\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]S^{-1}$.

Next, consider the map
\[
\theta : (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma] \to A, \quad \sum_{i=0}^d a_i x^i \mapsto \sum_{i=0}^d x^{-i} a_i.
\]
We have, assuming without loss of generality that $t \geq d$ and $a_{d+1} = \ldots = a_t = 0$, that
\[
\theta(\sum_{i=0}^d a_i x^i + \sum_{i=0}^t b_i x^i) = \theta(\sum_{i=0}^t (a_i + b_i) x^i) = \theta(\sum_{i=0}^d a_i x^i) + \theta(\sum_{i=0}^t b_i x^i)
\]
and
\[
\theta(\sum_{i=0}^d a_i x^i \sum_{i=0}^t b_i x^i) = \theta \left( \sum_{k=0}^{d+t} \left( \sum_{i+j=k} a_i \sigma^i(b_j) \right) x^k \right)
\]
\[
= \sum_{k=0}^{d+t} x^{-k} \left( \sum_{i+j=k} a_i \sigma^i(b_j) \right)
\]
\[
= \sum_{k=0}^{d+t} \sum_{i+j=k} x^{-j} x^{-i} \sigma^i(b_j) a_i
\]
\[
= \sum_{k=0}^{d+t} \sum_{i+j=k} x^{-i} b_j x^{-i} a_i
\]
\[
= \theta(\sum_{i=0}^t b_i x^i) \theta(\sum_{i=0}^d a_i x^i).
\]
It follows that $\theta$ is an anti-isomorphism of rings.

Based on the above proposition, it is now possible to extend the computation of the generator polynomial from the commutative to the non-commutative case. Recall that we may assume the generator polynomial $g(x)$ to be monic, without loss of generality.

**Proposition 3.** Consider a code with generator $g(x)$ and parity check polynomial $h(x) = \sum_{k=0}^{k-1} h_i x^i + x^k$, that is $g(x), h(x)$ satisfy $h(x) g(x) = x^n - u$. Suppose that $u^2 = 1$. The Euclidean dual $g^\perp(x)/(x^n-u)$ of the $\sigma$-constacyclic code $(g(x))/(x^n-u)$ is a $\sigma$-constacyclic code whose generator polynomial is given by
\[
g^\perp(x) = 1 + \sum_{i=1}^k \sigma^i(h_{k-i}) x^i,
\]
or equivalently by the monic polynomial $-ug^\perp(x)$.
Proof. To show that \( g^\perp(x)/(x^n-u) \) is a \( \sigma \)-constacyclic code, we need to show that \( g^\perp(x) \) is a right divisor of \( x^n-u \). We know that \( g(x) \) is, namely there exists a polynomial \( h(x) \) such that

\[
g(x)h(x) = h(x)g(x) = x^n - u.
\]

Then, using the anti-isomorphism

\[
\theta : (O_K/pO_K)[x; \sigma] \rightarrow A,
\]

\[
\sum_{i=0}^{d} a_i x^i \mapsto \sum_{i=0}^{d} x^{-i} a_i
\]

of the previous proposition:

\[
x^k \theta(h(x)) \theta(g(x)) x^{n-k} = x^k \theta(g(x)h(x)) x^{n-k} = x^k \theta(x^n - u) x^{n-k} = x^k(x^n - u) x^{n-k} = 1 - ux^n = -u(x^n - \frac{1}{u}) = -u(x^n - u),
\]

since \( u^2 = 1 \). Therefore \( x^k \theta(h(x)) \) is a left divisor of \( x^n - u \), and

\[
x^k \theta(h(x)) = x^k \theta(\sum_{i=0}^{k-1} h_i x^i + x^k) = x^k(\sum_{i=0}^{k-1} x^{-i} h_i + x^{-k}) = \sum_{i=0}^{k-1} \sigma^i(h_i) x^{k-i} + 1.
\]

By the first part of Proposition 1, \( x^k \theta(h(x)) \) is also a right divisor of \( x^n - u \). Now that we have shown that \( g^\perp(x) \) is indeed a \( \sigma \)-constacyclic code, we are left to show that it is the dual of \( C \).

Let \( a(x) = \sum_{i=0}^{n-1} a_i x^i \) be the polynomial corresponding to the codeword \( a = (a_0, a_1, \ldots, a_{n-1}) \). Then we denote, for any \( 0 \leq l \leq n-k-1 \), by \( d_l(x) \) the polynomial \( x^l g(x) \), which corresponds to the codeword:

\[
d_l = (0_1 \, x^l \, h_0, \sigma^{l+1} h_{k-1}, \ldots, \sigma^{l+k} h_0, 0_1 \times (n-k-l+1)) \quad l = 0, \ldots, n-k-1.
\]

Hence, \( a \) is orthogonal to the \( n-k \) vectors \( d_l \) \((0 \leq l \leq n-k-1)\): indeed, note that

\[
d_l a^T = \sum_{i=l}^{l+k-1} a_i \sigma^i(h_{l+k-i})
\]

which turns out to be the coefficient of \( x^{k+l} \) in \( a(x) h(x) \), \( l = 0, \ldots, n-k-1 \). Since \( \deg h(x) = k \), \( \deg(a(x) h(x)) < n + k \), say \( a(x) h(x) = p(x) = \sum_{i=0}^{n+k-1} p_i x^i \), which means that modulo \( x^n - u \),

\[
a(x) h(x) = \sum_{i=0}^{n-1} p_i x^i + \sum_{i=n}^{n+k-1} p_i x^i = \sum_{i=0}^{n-1} p_i x^i + \sum_{j=n}^{k-1} p_{j+n} x^j (-u).
\]

Moreover, since \( a \in \mathcal{C} \), by Proposition 1, we have \( a(x) h(x) = 0 \) modulo \( x^n - u \), implying that the coefficients of \( x^{k+l} \), \( l = 0, \ldots, n-k-1 \), are equal to zero. This proves the orthogonality of \( d_l \) with respect to \( a \).

Therefore, the \( O_K/pO_K \)-module generated by the codewords \( d_l \) \((0 \leq l \leq n-k-1)\) is contained in \( \mathcal{C}^\perp \).

We now show that the module \( O_K/pO_K[d_0, \ldots, d_{n-k-1}] \) has rank \( n-k \). Indeed, let \( \lambda_0, \ldots, \lambda_{n-k-1} \in O_K/pO_K \) such that \( \sum_{l=0}^{n-k-1} \lambda_l d_l = 0 \). The first coordinate of
The parity check polynomial is \( h = \lambda \), so \( \lambda = 0 \). Then \( \sum_{l=1}^{n-k-1} \lambda_l d_l = 0 \) and by the same argument, we prove successively that \( \lambda_1 = 0 \), \( \ldots \), \( \lambda_{n-k-1} = 0 \). This proves that the \( n-k \) vectors \( d_0, \ldots, d_{n-k-1} \) are linearly independent over \( \mathcal{O}_K / \mathcal{pO}_K \).

We remark that in our context of cyclic division \( F \)-algebras, \( u \) is restricted to \( F \), therefore the polynomial \( x^n - u \in (\mathcal{O}_K / \mathcal{pO}_K)[x; \sigma] \) actually has a constant term \( u \) which belongs to \( \mathcal{O}_F / \mathcal{pO}_F \). Therefore the condition \( u^2 - 1 \) means that \( u \) is of order 2 in a finite field, that is \( u = \pm 1 \). This is however not the case more generally.

**Example 4.** Let us continue Example 1. We have \( u^2 = 1 \) in a finite field, that is \( u \in \mathbb{F}_2 \), or equivalently \((3, 3) + (1, x) = (1, 1) + (1, 1)x^2 \) with parity check polynomial \( h(x) = x + x - 1 \). From Proposition 3, we have that \( g^2(x) = 1 + x + x^2 \) is indeed a quaternion division algebra. We set \( \Lambda = \mathbb{Z} \), so \( \lambda = 0 \) and by the same argument, we prove successively that \( \lambda_1 = 0 \), \( \ldots \), \( \lambda_{n-k-1} = 0 \). This proves that the \( n-k \) vectors \( d_0, \ldots, d_{n-k-1} \) are linearly independent over \( \mathcal{O}_K / \mathcal{pO}_K \).

Finally we provide another example of self-dual code.

**Example 5.** For Example 2, we have \((1, 2) + (2, 2)x((1, 1) - (2, 2)x) = (1, 1) + (1, 1)x^2 \) or equivalently \((3, 3) + (1, 1)x = (1, 1) + (1, 1)x^2 \) with parity check polynomial \( h(x) = (2, 2) + (1, 1)x \). From Proposition 3, we have that \( g^2(x) = 1 + x + x^2 \) is indeed a quaternion division algebra. We set \( \Lambda = \mathbb{Z} \), so \( \lambda = 0 \) and by the same argument, we prove successively that \( \lambda_1 = 0 \), \( \ldots \), \( \lambda_{n-k-1} = 0 \). This proves that the \( n-k \) vectors \( d_0, \ldots, d_{n-k-1} \) are linearly independent over \( \mathcal{O}_K / \mathcal{pO}_K \).

**Example 6.** Let \( K = \mathbb{Q}(\sqrt{2}) \) and \( F = \mathbb{Q} \). Then \( \mathcal{O}_F = \mathbb{Z} \) and \( \mathcal{O}_K = \mathbb{Z}[\sqrt{2}] \). Let \( \Omega \) be the quaternion division algebra defined by

\[
\Omega = \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2})e,
\]

with \( e^2 = -5 \). Since \( N_{K/F}(a + \sqrt{2}b) = a^2 + 2b^2 \), \( a, b \in \mathbb{Z} \), \(-5 \) cannot be a norm and \( \Omega \) is indeed a quaternion division algebra. We set \( \Lambda = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{2}] \). \( \Lambda \) is a quaternion division algebra. We set \( \Lambda = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{2}] \). \( \Lambda / \Lambda e \simeq \mathbb{F}_9 \). Take \( \mathcal{I} = (\sqrt{2} + e) \mathcal{L} \). Then \( \mathcal{I} \) contains 3 since the reduced norm \( N(\sqrt{2} + e) = (\sqrt{2} + e)(\sqrt{2} - e) = -2 - \sqrt{2}e - \sqrt{2} - e^2 = 3 - \sqrt{2}e = 3 \). Let \( \alpha \) denote a primitive root of \( \mathbb{F}_9 \) over \( \mathbb{F}_3 \), satisfying \( \alpha^2 + 1 = 0 \) and as before, \( \sigma(\alpha) = \alpha^3 \). We have

\[
\psi((\sqrt{2} + e) \bmod 3) = \alpha + x,
\]

which is a right divisor of \( x^2 + 5 = x^2 + 2 \) in \( \mathbb{F}_9[x; \sigma] \):

\[
(x + \alpha)(x + \alpha) = x^2 + \sigma(\alpha)x + (\alpha)x + \alpha^2 = x^2 + 2.
\]

Therefore, the left ideal \( (x + \alpha)\mathbb{F}_9[x; \sigma]/(x^2 + 2) \) is a \( \sigma \)-constacyclic code of length \( n = 2 \) and dimension 1. Left multiples of \( x + \alpha \) modulo \( x^2 + 2 \) are explicitly given by \( (b_0 + b_1x)(x + \alpha) = [b_0(\alpha) + b_1] + [b_0 + b_1(-\alpha)]x \) and codewords are of the form

\[
(a_0, a_1) = (aa_1, a_1), \quad a_1 \in \mathbb{F}_9.
\]
This code is self-dual, since \( u = 2 \) satisfies \( u^2 = 1 \) and \( g^+(x) = 1 + \sigma(\alpha)x = 1 - \alpha x = -\alpha(\alpha + x) \). Taking the pre-image by \( \psi \), it corresponds to the left-ideal \( \mathcal{I}/3\Lambda \), with \( \mathcal{I} = (\sqrt{2} + e)\Lambda \).

4.2. LATTICES FROM DUAL CODES. Recall the proposed variation of Construction A. Given the map
\[
\rho : \Lambda \to \psi(\Lambda/p\Lambda) = (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]/(x^n - u),
\]
compositum of the canonical projection \( \Lambda \to \Lambda/p\Lambda \) with \( \psi \), we obtained a lattice \( L \) given by
\[
L = \rho^{-1}(\mathcal{C}) = \mathcal{I}.
\]
Now let \( \mathcal{C}^\perp \) be the dual of \( \mathcal{C} \). Then
\[
L' = \rho^{-1}(\mathcal{C}^\perp)
\]
is also a lattice.

**Example 7.** Let us continue Examples 1 and 4. To the code \( \mathcal{C} \) given by the left multiples of \((x + 1 + \alpha) \mod x^2 + 1\) corresponds the lattice \( \rho^{-1}(\mathcal{C}) = (1 + i + e)\Lambda \).

The dual lattice \( \mathcal{C}^\perp \) is generated by the left multiples of \( 1 - (\alpha + 1)x \mod x^2 + 1 \) to which corresponds the lattice \( \rho^{-1}(\mathcal{C}^\perp) = (1 - (i + 1)e)\Lambda \).

We make an obvious observation.

**Lemma 4.3.** If \( \mathcal{C} \subset \mathcal{C}^\perp \), we have the inclusion \( L \subset L' \).

**Proof.** Let \( x \in L \). Then \( \rho(x) \in \mathcal{C} \), so \( \rho(x) \in \mathcal{C}^\perp \) and \( x \in L' \).

5. APPLICATION TO SPACE-TIME CODES

We conclude by discussing our motivation to look at the question of defining a variation of Construction A over a cyclic division \( F \)-algebra, which comes from space-time coding. We start with a brief introduction to define space-time coding which is independent of the the above paper, but may be helpful to recall the context of space-time code design in general, before we discuss coset coding for space-time coding.

5.1. SPACE-TIME CODING. Cyclic division algebras are by now classically used to design space-time codes [15, 4]. Unlike in classical coding theory where codewords are typically vectors with coefficients over finite fields (or finite rings), in the context of space-time coding, codewords are matrices with coefficients coming from number fields, and matrix codewords are obtained as follows. We recall the assumption that \( u \in \mathcal{O}_F \). To any element \( a = a_0 + a_1 e + \cdots + a_{n-1} e^{n-1} \) of \( \Lambda \), we can associate a matrix in \( \text{Mat}_n(\mathcal{O}_K) \) (since \( u \in \mathcal{O}_F \)) by:

\[
M(a) = \begin{bmatrix}
a_0 & u\sigma(a_{n-1}) & u\sigma^2(a_{n-2}) & \cdots & u\sigma^{n-1}(a_1) \\
\sigma(a_0) & u\sigma^2(a_{n-1}) & \cdots & u\sigma^{n-1}(a_2) \\
\vdots & \vdots & \ddots & \vdots \\
\sigma(a_{n-2}) & \sigma^2(a_{n-3}) & \cdots & u\sigma^{n-1}(a_{n-1}) \\
a_{n-2} & \sigma(a_{n-3}) & \cdots & \sigma^{n-1}(a_0)
\end{bmatrix}.
\]

The map
\[
\Lambda \to \text{Mat}_n(\mathcal{O}_K)
\]
\[
a \mapsto M(a)
\]
is an $\mathcal{O}_K$-algebra injective homomorphism. A space-time code (or codebook) is

given by $\{M(a), a \in \Lambda\}$. The first design criterion to obtain good space-time codes

is the so-called full diversity property [4], which requests that $\det(M(a) - M(a')) \neq 0$, $a \neq a'$. The condition that the $F$-algebra is division is critical to fulfill the full
diversity design criterion.

We illustrate this by continuing Example 1.

**Example 8.** For $q = a + be$ in the natural order $\mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ of the quaternion

algebra $\Omega$, $a, b \in \mathbb{Z}[i]$

$$M(q) = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$$

where $\bar{\cdot}$ is the non-trivial Galois automorphism of $\mathbb{Q}(i)/\mathbb{Q}$. Let $t = (a + be)(1 + i + e)$

be an element of $\mathcal{I} = \Lambda(1 + i + e)$ (with $a, b \in \mathbb{Z}[i]$). Then

$$t = a(1 + i) - b + (a + b(1 - i))e.$$ Hence,

$$M(t) = \begin{bmatrix} a(1 + i) - b & -(\pi + \bar{b}(1 + i)) \\ a + b(1 - i) & \pi(1 - i) - \bar{b} \end{bmatrix},$$

and we obtain the space-time code

$$\left\{ \begin{bmatrix} a(1 + i) - b & -(\pi + \bar{b}(1 + i)) \\ a + b(1 - i) & \pi(1 - i) - \bar{b} \end{bmatrix}, a, b \in \mathbb{Z}[i] \right\}.$$ Note that $\mathcal{I} = \rho^{-1}(C)$ is a real lattice with rank 4, embedded into $\mathbb{R}^4$ using $\Omega \otimes_{\mathbb{Q}} \mathbb{R}$.

5.2. Coset Coding. Let now $v = (v_1, \ldots, v_n)$ be an information vector containing

the data to be transmitted, which should be mapped to a lattice point in $L$, where $L$ is used as a lattice code. Mapping a vector with coefficients in a finite ring to a lattice point is not an easy task, and can be facilitated by the use of Construction A. This is best illustrated in the case of the binary Construction A, even though the principle holds more generally. It is known for example that the 8-dimensional lattice $E_8$ can be obtained by taking the quotient of $\mathbb{Z}^8$ by $2\mathbb{Z}^8$, and by choosing the Reed-Muller code of length 8 and dimension 4 [9]. The role of an encoder is to map an 8-dimensional binary vector $(v_1, \ldots, v_8)$ to a point in $E_8$. The encoder uses 4 binary symbols to choose one point (among a constellation of 16 points) in $2\mathbb{Z}^8$ and the other 4 binary symbols are mapped to a codeword using the generator matrix of the Reed-Muller code. It is not easy otherwise to find an algorithmic way to map 8-dimensional binary vectors into a finite constellation of points of $E_8$.

The same procedure can be repeated for the proposed Construction A from cyclic
division algebras.

The lattice $L = \rho^{-1}(C) = \mathcal{I}\Lambda$ may by construction be written as a union of cosets of $p\Lambda$, where each coset representative may be chosen to be a codeword in the code $C$. Namely, if $g(x)$ is a right divisor of $x^n - u$ and if a $\sigma$-constacyclic code $C = (g(x))/(x^n - u) \subset (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]/(x^n - u)$ has dimension $k = n - \deg(g)$, since

$$\Lambda/p\Lambda \cong (\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]/(x^n - u)$$

there is an isomorphism

$$\mathcal{I}/p\Lambda \cong C.$$ This allows us to associate in a unique way a coset of $p\Lambda$ to a codeword. The mapping from $v$ to a point in $L$ may be done by attributing some information
coefficients $v_1, \ldots, v_k$ to be encoded using the code $C$, and the rest of the information coefficients to be mapped to a point in the lattice $p\Lambda$. This simplifies the encoding in the cases where $p\Lambda$ is a lattice “easier” to label than $L$, which happens in the original Construction A where this lattice turns out to be a scaled version of $\mathbb{Z}^n$, but also in many cases where $p$ gives rise to a lattice isomorphic to $\mathbb{Z}^n$ (or another lattice whose points are easy to label).

5.3. Wiretap coset coding. Irrespectively of the lattice obtained from $p\Lambda$, coset encoding is necessary in the context of wiretap codes. Wiretap codes are used in the context of wiretap channels, which model communication in the presence of an eavesdropper (or wiretapper). In a wiretap context, a code should not only provide reliability between a transmitter and a receiver, but also ensure confidentiality, should an eavesdropper try to intercept the message. To protect from wiretapping, controlled randomness is used at the transmitter. This is typically done using coset coding, which can be implemented via Construction A. Construction A allows us to see a lattice as a union of cosets, as discussed above. Information symbols which are meant to be confidential are used to choose one coset, which becomes the intended message to be sent. Randomness is then used to pick one element at random within the coset. If we rephrase this in our context, information symbols are mapped to a codeword in $C$, while random symbols are picked uniformly at random in the lattice $p\Lambda$ to create confusion at the eavesdropper. Wiretap space-time codes have been studied in [3], where coset encoding of space-time codes is assumed. However, no concrete way to do so was proposed. The construction of the lattice $L = \rho^{-1}(C) = I$ as presented in this work thus enables coset encoding for wiretap space-time codes.

6. Future work

In this paper, we presented a construction of lattices from constacyclic codes over skew-polynomials, which can be interpreted as a variation of the well known Construction A of lattices from linear codes. The starting point was the quotient $\Lambda/p\Lambda$ of a given order $\Lambda$ from a cyclic division $F$-algebra, which is motivated by applications of such algebras to space-time coding. Natural future research directions include:

- To continue the study of constacyclic codes over $(\mathcal{O}_K/p\mathcal{O}_K)[x; \sigma]/(x^n - u)$, in particular by replacing the polynomial $x^n - u$ with a more general polynomial $f(x)$. This may include looking at the characterization of self-dual codes. One could alternatively consider duality with respect to a Hermitian inner product.
- Linking the properties of the constacyclic code $C$ to that of the lattice $L = \rho^{-1}(C)$: there are standard duality results for the classical Construction A, relating the dual lattice of $L^*$ with $L'$, or the weight enumerator of the code with the theta series of the lattice, which have not yet been considered. This leads to further properties of lattices that could be explored, such as extremality and modularity.
- Design of wiretap space-time codes: this consists of choosing the cyclic division $F$-algebra $A$, the corresponding two-sided ideal $I$ and constacyclic code $C$, to optimize the confusion at the eavesdropper.

References

[1] M. Artin, Noncommutative Rings, 1999.
[2] C. Bachoc, Applications of coding theory to the construction of modular lattices, *J. Combin. Theory Ser. A.*, **78** (1997), 92–119.

[3] J.-C. Belfiore and F. Oggier, An error probability approach to MIMO wiretap channels, *IEEE Trans. Commun.*, **61** (2013), 3396–3403.

[4] G. Berhuy and F. Oggier, *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication*, AMS, 2013.

[5] A. Bonnecaze, P. Solé and A. R. Calderbank, Quadratic residue codes and unimodular lattices, *IEEE Trans. Inf. Theory*, **41** (1995), 366–377.

[6] D. Boucher, W. Geiselmann and F. Ulmer, Skew cyclic codes, *Appl. Algebra Engin. Commun. Comput.*, **18** (2007), 379–389.

[7] D. Boucher and F. Ulmer, Coding with skew polynomial rings, *J. Symb. Comput.*, **44** (2009), 1644–1656.

[8] D. Boucher, F. Ulmer and P. Solé, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, **2** (2008), 273–292.

[9] J. H. Conway and N. J. A Sloane, *Sphere Packings, Lattices and Groups*, Springer.

[10] J. Ducoat and F. Oggier, Lattice encoding of cyclic codes from skew-polynomial rings, in *Coding Theory and Applications*, Springer, 2015, 161–167.

[11] W. Ebeling, *Lattices and Codes, A Course Partially Based on Lectures by Friedrich Hirzebruch*, Springer, 2013.

[12] G. D. Forney, Coset Codes Part I: Introduction and geometrical classification, *IEEE Trans. Inf. Theory*, **34** (1988), 1123–1151.

[13] F. Oggier and J.-C. Belfiore, Enabling multiplication in lattice codes via construction A, in *IEEE Int. Workshop Inf. Theory*, 2013, 1–5.

[14] F. Oggier and B. A. Sethuraman, Quotients of orders in cyclic algebras and space-time codes, *Adv. Math. Commun.*, **7** (2013), 441–461.

[15] B. A. Sethuraman, B. S. Rajan and V. Shashidhar, Full-diversity, high-rate space-time block codes from division algebras, *IEEE Trans. Inf. Theory*, **49** (2003), 2596–2616.

Received December 2014; revised August 2015.

*E-mail address: jerome.ducoat@gmail.com*

*E-mail address: frederique@ntu.edu.sg*