Lattice Encoding of Cyclic Codes from Skew-polynomial Rings

Jérôme Ducoat and Frédérique Oggier

Abstract We propose a construction of lattices from cyclic codes from skew-polynomial rings. This construction may be seen as a variation of Construction A of lattices from linear codes, obtained from quotients of orders in cyclic division algebras. An application is coset encoding of wiretap space-time codes.

Key words: Lattices, Cyclic Division Algebras, Skew-polynomials, Cyclic codes

1 Introduction

Constructions of lattices from linear codes over finite fields (or rings) have been classically studied, starting from the so-called Construction A [6, 4] of lattices from binary linear codes. Let $\rho : \mathbb{Z}^N \mapsto \mathbb{F}_2^N$ be the map of reduction modulo 2 componentwise. Let $C \subset \mathbb{F}_2^N$ be an (N,k) linear binary code. Then $\rho^{-1}(C)$ is a lattice. One possible way of generalizing this construction is by considering cyclotomic fields [5]. Let $\mathbb{Q}(\zeta_p)$ be a cyclotomic field, with ring of integers $\mathbb{Z}[\zeta_p]$, where ζ_p is a primitive pth root of unity, p a prime. Let $\rho : \mathbb{Z}[\zeta_p]^N \mapsto \mathbb{F}_p^N$ be this time the reduction componentwise modulo the prime ideal $\mathfrak{p} = (1-\zeta_p)$. Then $\rho^{-1}(C)$ is a lattice, when C is an (N,k) linear code over $\mathbb{F}_p$. In particular, $p = 2$ yields the binary Construction A. A similar construction from number fields with a totally ramified prime has been proposed in [7].

Let K/F be a cyclic extension of number fields, with respective maximal orders $\mathscr{O}_K$ and $\mathscr{O}_F$. We are proposing a variation of the above Constructions A, where

Jérôme Ducoat
Nanyang Technological University, Division of Mathematical Sciences, 21 Nanyang Link, 637371, Singapore, e-mail: jducoat@ntu.edu.sg

Frédérique Oggier
Nanyang Technological University, Division of Mathematical Sciences, 21 Nanyang Link, 637371, Singapore, e-mail: frederique@ntu.edu.sg

lattices are obtained from quotients of the natural order Λ of a cyclic division algebra, as explained in Section 2, instead of quotients of the maximal order of number fields. The resulting quotient $\Lambda/\mathfrak{p}\Lambda$ of the natural order of a cyclic division algebra by a two-sided ideal $\mathfrak{p}\Lambda$, where $\mathfrak{p}$ is a prime ideal of $\mathscr{O}_F$ inert in K/F, turns out to be isomorphic to a ring of skew-polynomials. Denote this isomorphism by ψ. Let C be a cyclic code constructed over the ring of skew-polynomials (see Section 3) and let ρ denote the compositum of the canonical projection $\Lambda \to \Lambda/\mathfrak{p}\Lambda$ with ψ. Then $\rho^{-1}(C)$ is a lattice. Application of this construction to space-time coding, more specifically to coset encoding, is discussed in Section 4.

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 $\mathscr{O}_K$ and $\mathscr{O}_F$. Consider the cyclic algebra

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

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. Let Λ be its natural order

$$\Lambda = \mathscr{O}_K \oplus \mathscr{O}_K e \oplus \cdots \oplus \mathscr{O}_K e^{n-1}.$$

Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_F$ so that $\mathfrak{p}\Lambda$ is a two-sided ideal of Λ. Assume that $\mathfrak{p}$ is inert in K/F, so that $\mathfrak{p}\mathscr{O}_K$ is a prime ideal of $\mathscr{O}_K$. Then $\Lambda/\mathfrak{p}\Lambda$ is an $\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K$-algebra and from [9], we have the following isomorphism :

$$\Lambda/\mathfrak{p}\Lambda \simeq (\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K) \oplus (\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K)e \oplus \cdots \oplus (\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K)e^{n-1}.$$

Note that since $\mathfrak{p}\mathscr{O}_K$ is a prime ideal of $\mathscr{O}_K$, the finite ring $\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K$ is an integral domain, so is a finite field that we denote by $\mathbb{F}_q$. Here, $q = p^{nf}$, where p is the prime number lying below $\mathfrak{p}$ and f is the inertial degree of $\mathfrak{p}$ above p.

The algebra $\Lambda/\mathfrak{p}\Lambda$ can alternatively be described in terms of skew-polynomial with coefficients in $\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K = \mathbb{F}_q$.

Definition 1. Given a ring R with a group $\langle\sigma\rangle$ acting on it, the skew-polynomial ring $S[x;\sigma]$ is the set of polynomials $s_0 + s_1x + \ldots + x_nx^n$, $s_i \in S$ for $i = 0, \ldots, n$, with $xs = \sigma(x)s$ for all $s \in S$.

Lemma 1. *There is an $\mathbb{F}_q$-algebra isomorphism between $\Lambda/\mathfrak{p}\Lambda$ and the quotient of $\mathbb{F}_q[x;\sigma]$ by the two-sided ideal generated by $x^n - u$.*

Proof. We define the map

$$\begin{aligned} \varphi : \mathbb{F}_q[x;\sigma] &\to \Lambda/\mathfrak{p}\Lambda \\ f(x) &\mapsto f(e). \end{aligned}$$

Using the isomorphism given above and in [9], it is easily seen that φ is a surjective $\mathbb{F}_q$-algebra homomorphism. Moreover, the kernel of φ is the two-sided ideal of $\mathbb{F}_q[x;\sigma]$ 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

$$f(x)=\sum_{i=0}^{m}s_ix^i$$

for some $s_i\in\mathbb{F}_q$, $i=0,...,m$. Then $f(e)=0$ in $\Lambda/\mathfrak{p}\Lambda$. Since the ring $\mathbb{F}_q[x;\sigma]$ is left Euclidean [10] , 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, $0=h(e)=r_0+r_1e+\cdots+r_{n-1}e^{n-1}$ in $\Lambda/\mathfrak{p}\Lambda\simeq(\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K)\oplus(\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K)e\oplus\cdots\oplus(\mathscr{O}_K/\mathfrak{p}\mathscr{O}_K)e^{n-1}$. 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. □

Denote by ψ the inverse isomorphism of the one given in Lemma 1:

$$\psi:\Lambda/\mathfrak{p}\Lambda\cong\mathbb{F}_q[x;\sigma]/(x^n-u).$$

Note that since $u\in F$, x^n-u belongs to the center of $\mathbb{F}_q[x;\sigma]$ and the ideal (x^n-u) is two-sided.

Let $\mathscr{I}$ be a left ideal of Λ. Assume that $\mathscr{I}\cap\mathscr{O}_F\supset\mathfrak{p}$. Then $\mathscr{I}/\mathfrak{p}\Lambda$ is an ideal of $\Lambda/\mathfrak{p}\Lambda$. In the sequel, we will study the left ideal $\psi(\mathscr{I}/\mathfrak{p}\Lambda)$ of $\mathbb{F}_q[x;\sigma]/(x^n-u)$.

3 Polynomial Codes and a Variation of Construction A

Definition 2. [3] Let $f\in\mathbb{F}_q[x;\sigma]$ be a polynomial of degree n. If (f) is a two-sided ideal of $\mathbb{F}_q[x;\sigma]$, then a σ-*code* consists of codewords $a=(a_0,a_1,\ldots,a_{n-1})$ that are coefficient tuples of elements $a(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ of a left ideal of $\mathbb{F}_q[x;\sigma]/(f)$. The elements $a(x)$ are left multiples of a right divisor g of f. If f lies in the center of $\mathbb{F}_q[x;\sigma]$, then the σ-code corresponding to the left ideal $(g)/(f)$ is called *a central* σ-*code*.

Using the isomorphism ψ defined in Section 2, for every left ideal $\mathscr{I}$ of Λ, we consider the σ-code $C=\psi(\mathscr{I}/\mathfrak{p}\Lambda)$ over $\mathbb{F}_q$.

We set the map :

$$\rho:\Lambda\to\psi(\Lambda/\mathfrak{p}\Lambda)=\mathbb{F}_q[x;\sigma]/(x^n-u),$$

compositum of the canonical projection $\Lambda \to \Lambda/\mathfrak{p}\Lambda$ with ψ. We then set

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

Then L is a lattice, that is a $\mathbb{Z}$-module of rank $n^2[F:\mathbb{Q}]$ since $\mathscr{O}_K$ is a $\mathbb{Z}$-module of rank $n[F:\mathbb{Q}]$.

From this point of view, the above construction may be interpreted as a variation of Construction A [4], 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 [8], defined over number fields.

Example 1. Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathscr{O}_F = \mathbb{Z}$ and $\mathscr{O}_K = \mathbb{Z}[i]$. Set $p = 3$, which remains inert in $\mathbb{Q}(i)$. Hence, $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$. Let $\mathfrak{Q}$ be the quaternion division algebra defined by

$$\mathfrak{Q} = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e,$$

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 $\mathfrak{Q}$ is indeed a quaternion division algebra. We set $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ and $\mathscr{I} = (1+i+e)\Lambda$. Then $\mathscr{I}$ contains 3 since the norm of $1+i+e$ is 3. Let α denote a primitive root of $\mathbb{F}_9$ over $\mathbb{F}_3$, satisfying $\alpha^2+1=0$. We have

$$\psi((1+i+e)\text{mod}3) = 1+\alpha+x,$$

which is a right divisor of x^2+1 in $\mathbb{F}_9[x;\sigma]$:

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

Therefore, the left ideal $(x+1+\alpha)\mathbb{F}_9[x;\sigma]/(x^2+1)$ consisting of the left multiples of $x+1+\alpha$ modulo x^2+1 is a central σ-code. Taking the pre-image by ψ, it corresponds to the left-ideal $\mathscr{I}/3\Lambda$, with $\mathscr{I} = \Lambda(1+i+e)$.

4 Application to Space-time Codes

Cyclic division algebras are by now classically used to design space-time codes [11, 2]. Matrix codewords are obtained as follows. From now on, to make the notation easier, we assume that $u \in \mathscr{O}_F$. To any element $a = a_0 + a_1 e + \cdots + a_{n-1}e^{n-1}$ of Λ, we can associate a matrix in $\text{Mat}_n(\mathscr{O}_K)$ (since $u \in \mathscr{O}_F$) by :

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

The map

$$\begin{aligned} \Lambda &\to \mathrm{Mat}_n(\mathscr{O}_K) \\ a &\mapsto M(a) \end{aligned}$$

is an $\mathscr{O}_K$-algebra injective homomorphism.

We apply this to our previous example.

Example 2. For $q = a+be$ in the natural order $\mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ of the quaternion algebra $\mathfrak{Q}$, $a, b \in \mathbb{Z}[i]$

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

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

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

Hence,

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

Note that $\mathscr{I} = \rho^{-1}(C)$ is a real lattice with rank 4 embedded in $\mathbb{R}^8$: by vectorizing the matrices $M(t)$ and separating real and imaginary parts, a generator matrix of this lattice is given by

$$\begin{bmatrix} 1 & 1 & 1 & 0 & -1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 & 0 & 1 & -1 & -1 \\ -1 & 0 & 1 & -1 & -1 & -1 & -1 & 0 \\ 0 & -1 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Let now $v = (v_1, \ldots, v_n)$ be the information vector to be mapped to a lattice point in L, where L is used as a lattice code. The lattice $L = \rho^{-1}(C) = \mathscr{I}\Lambda$ may by construction be written as a union of cosets of $\mathfrak{p}\Lambda$, where each coset representative may be chosen to be a codeword in the code C. Namely, if g is a right divisor of $x^n - u$ and if a central σ-code $C = (g)/(x^n-u) \subset \mathbb{F}_q[x;\sigma]/(x^n-u)$ has dimension $k = n - \deg(g)$, since

$$\Lambda/\mathfrak{p}\Lambda \cong \mathbb{F}_q[x;\sigma]/(x^n-u)$$

there is an isomorphism

$$\mathscr{I}/\mathfrak{p}\Lambda \cong C.$$

This allows us to associate in a unique way a coset of $\mathfrak{p}\Lambda$ 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 $\mathfrak{p}\Lambda$. Coset encoding is necessary in the context of wiretap codes [1]: information symbols are mapped to a codeword in C, while random symbols are picked uniformly at random in the lattice $\mathfrak{p}\Lambda$ to confuse the eavesdropper. The construction of the lattice $L = \rho^{-1}(C) = \mathscr{I}$ thus enables coset encoding for wiretap space-time codes.

5 Future Work

In this paper, we presented a construction of lattices from cyclic codes from skew-polynomials, which can be seen as a variation of the well known Construction A of lattices from linear codes. Natural future research directions include:

- Linking the properties of the cyclic code C to that of the lattice $L = \rho^{-1}(C)$: there are standard duality results for the classical Construction A, relating the dual of the code with the dual of the lattice, as well as the weight enumerator of the code with the theta series of the lattice.
- Design of wiretap space-time codes: this consists of choosing the cyclic division algebras, the corresponding two-sided ideal and cyclic code, to optimize the confusion at the eavesdropper.

Acknowledgements The research of J. Ducoat and F. Oggier is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07.

References

1. Belfiore, J.C., Oggier, F.: An error probability approach to MIMO wiretap channels. IEEE Transactions on Communications **61**(8) (2013)
2. Berhuy, G., Oggier, F.: An Introduction to Central Simple Algebras and Their Applications to Wireless Communication. AMS
3. Boucher, D., Ulmer, F.: Coding with skew polynomial rings. Journal of Symbolic Computation **44**, 1644–1656 (2009)
4. Conway, J., Sloane, N.: Sphere Packings, Lattices and Groups. Springer
5. Ebeling, W.: Lattices and Codes, A Course Partially Based on Lectures by Friedrich Hirzebruch. Advanced Lectures in Mathematics. Springer
6. Forney, G.D.: Coset codes − part i: Introduction and geometrical classification. IEEE Trans. on Inform. Theory **34**(5) (1988)
7. Kositwattanarerk, W., Ong, S., Oggier, F.: Wiretap encoding of lattices from number fields using codes over $\mathbb{F}_p$. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT). Istanbul (2013)
8. Oggier, F., Belfiore, J.C.: Enabling multiplication in lattice codes via construction a. In: Proceedings of the IEEE International Workshop on Information Theory. Sevilla (2013)
9. Oggier, F., Sethuraman, B.A.: Quotients of orders in cyclic algebras and space-time codes. Advances in Mathematics of Communication **7**, 441–461 (2013)
10. Ore, O.: Theory of non-commutative polynomials. Annals of Mathematics **34**, 1644–1656 (1933)
11. Sethuraman, B.A., Rajan, B.S., Shashidhar, V.: Full-diversity, high-rate space-time block codes from division algebras. IEEE Trans. on Inform. Theory **49**(10) (2003)