Advances in Mathematics of Communications
Volume 7, No. 4, 2013, 463–474
doi:10.3934/amc.2013.7.463

(σ, δ)-CODES

M'Hammed Boulagouaz
University of King Khalid, Abha, Saudi Arabia
and
Faculty of Sciences and Technics of Fés, Morocco

André Leroy
Université d'Artois, Lille Nord de France
Rue Jean Souvraz
Lens, 62300 France

(Communicated by Steven Dougherty)

Abstract. In this paper we introduce the notion of cyclic $(f(t), \sigma, \delta)$-codes for $f(t) \in A[t; \sigma, \delta]$. These codes generalize the θ-codes as introduced by D. Boucher, F. Ulmer, W. Geiselmann [2]. We construct generic and control matrices for these codes. As a particular case the (σ, δ)-W-code associated to a Wedderburn polynomial are defined and we show that their control matrices are given by generalized Vandermonde matrices. All the Wedderburn polynomials of $\mathbb{F}_q[t; \theta]$ are described and their control matrices are presented. A key role will be played by the pseudo-linear transformations.

1. Introduction and preliminaries

The use of rings in coding theory started when it appeared that working over rings allowed certain codes to be looked upon as linear codes. The use of *noncommuative* rings emerged recently in coding theory due to the pertinence of Frobenius rings for generalizing Mac Williams theorems (cf. [17], for details) and also because of the use of Ore polynomial rings as source of generalizations of cyclic codes (cf. e.g. [2, 3, 16]). With some few exceptions (e.g. [13, 4]) the Ore polynomial rings used so far in coding theory are mainly of automorphisms type with a (finite) field as base ring. This paper shows how one can use general Ore extensions to not only define codes, but as well give their generic and control matrices. Factorizations techniques in Ore polynomial rings play an important role in these questions and the interested reader can consult [6, 9, 10] for more information on this matter. Since they are intimately related to modules over Ore extensions and to factorizations, pseudo-linear transformations will play an important role in this paper. The reader may consult [7, 11, 12] for more details on pseudo-linear transformations.

Definitions 1. Let A be a ring with 1 and σ a ring endomorphism of A.

(a) An additive map $\delta \in End(A, +)$ is a σ-derivation if, for any $a, b \in A$, we have:

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b.$$

2010 *Mathematics Subject Classification:* Primary: 94B05, 94B15; Secondary: 16S36.
Key words and phrases: Cyclic codes, Ore extensions, pseudo-linear transformations.
The work of the first author was supported by the Deanship of Scientific Research at King Khalid University (project KKU-S179-33).

(b) Let δ be a σ-derivation of a ring A. The elements of the skew polynomial ring $R = A[t;\sigma,\delta]$ are sums $\sum a_i t^i$. They are added as ordinary polynomials and the multiplication is based on the commutation law

$$ta = \sigma(a)t + \delta(a),\ for\ a \in A.$$

(c) The degree of a nonzero polynomial $f = a_0 + a_1 t + a_2 t^2 + \dots a_n t^n \in R = A[t;\sigma,\delta]$ is defined to be $\deg(f) = max\{i|a_i \neq 0\}$ and we put, as usual, $\deg(0) = -\infty$.

Examples 1. (1) If $\sigma = id.$ and $\delta = 0$ we have $A[t;\sigma,\delta] = A[t]$, the usual polynomial ring in a commuting variable. If only $\sigma = id.$ but $\delta \neq 0$ we denote $A[t;id.,\delta]$ as $A[t;\delta]$ and speak of a polynomial ring of derivation type. On the other hand, if $\delta = 0$ but $\sigma \neq id.$, we write $A[t;\sigma,\delta]$ as $A[t;\sigma]$ and refer to this Ore extension as a polynomial ring of endomorphism type.

(2) Let σ stand for the usual conjugation of the complex number $\mathbb{C}$ and consider $\mathbb{C}[t;\sigma,0]$. Notice that, since $\sigma^2 = id.$, we can check that t^2 is a central polynomial.

(3) Let k be field, $R = k[x][t;id.;d/dx]$. This is the weyl algebra. The commutation law is $tx - xt = 1$. If char$k = 0$ the Weyl algebra is a simple ring. In contrast if char$k = p > 0$ then t^p and x^p are central elements.

(4) For $a \in A$, we define the inner σ-derivation induced by a (denoted $d_{a,\sigma}$) in the following way: for $r \in A$, $d_{a,\sigma}(r) := ar - \sigma(r)a$. Let us remark that $A[t;\sigma,d_{a,\sigma}] = A[t-a,\sigma]$. Similarly, for an inner automorphism I_a induced by an invertible element $a \in A$ and defined by $I_a(x) = axa^{-1}$ for $x \in A$, we have $A[t;I_a] = A[a^{-1}t]$. Let us mention that an easy computation shows that if there exists a central element $c \in Z(A)$, where $Z(A)$ denotes the center of A, such that $c - \sigma(c)$ is an invertible element of $Z(A)$, then the derivation δ is inner induced by $(c-\sigma(c))^{-1}\delta(c)$. In particular, if A is a field then either $\sigma = id$ or δ is inner. More particularly, all Ore extensions built on a finite field $\mathbb{F}_q$ are of the form $\mathbb{F}_q[t;\theta]$ where θ is an automorphism of $\mathbb{F}_q$.

(5) It is well-known that finiteness conditions force (σ)-derivations to be inner (Cf. e.g. [1]). We now give an easy example of a (finite) ring having a non-inner σ-derivation. Let K be any ring and σ a non inner automorphism of K. Consider the ring $A \subset M_2(K)$ defined by:

$$A := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a,b \in K,\ \sigma(a) = a \right\}.$$

We extend σ to A by letting it act on each coefficient of the matrices and define the additive map δ by setting:

$$\delta\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = \begin{pmatrix} 0 & \sigma(b) \\ 0 & 0 \end{pmatrix} \quad \text{for} \quad a,b \in K \quad \text{with } \sigma(a) = a.$$

One can check that this map is indeed a non inner sigma-derivation. For instance one can put $K = \mathbb{F}_q$ and let σ be the Frobenius map. Hence, in this case, A is a finite ring with a non-inner σ-derivation.

(6) Let p be a prime number, $n \in \mathbb{N}$ and $q = p^n$. Consider $R = \mathbb{F}_q$ the finite field with q elements and θ the Frobenius automorphism defined by $\theta(a) = a^p$ for $a \in \mathbb{F}_q$. Skew polynomial ring $\mathbb{F}_q[t;\theta]$ have been used recently in the context of noncommutative codes. The main advantage of $R = \mathbb{F}_q[t;\theta]$ versus the classical $\mathbb{F}_q[x]$ is that a given polynomial $p(t) \in R$ admits generally

many different factorizations. For instance let us consider $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, where $\alpha^2+\alpha+1=0$, and some factorizations of $t^4+1 \in \mathbb{F}_4[t;\theta]$:

$$\begin{aligned} t^4+1 &= (t^2+1)(t^2+1) \\ &= (t^2+\alpha t+\alpha)(t^2+\alpha t+\alpha^2) \\ &= (t^2+\alpha^2 t+\alpha^2)(t^2+\alpha^2 t+\alpha) \\ &= (t^2+\alpha t+\alpha^2)(t^2+\alpha t+\alpha) = ... \end{aligned}$$

In fact, it has been shown recently that factorizations in $\mathbb{F}_q[t;\theta]$ can be worked out from factorizations in $\mathbb{F}_q[x]$ (cf. [12]).

2. Polynomial and pseudo-linear maps

Let A, σ and δ be a ring, an endomorphism and a σ-derivation of A, respectively. Let us put $R = A[t;\sigma,\delta]$.

For any $f(t) \in R$ and $a \in A$ there exists a unique $q(t) \in A[t,\sigma,\delta]$ and a unique $s \in A$ such that:

$$f(t) = q(t)(t-a)+s.$$

Definitions 2. (a) With these notations, the (right) polynomial map associated to $f(t) \in R$ is

$$f : A \longrightarrow A \quad \text{given by} \quad f(a) := s$$

(b) For $i \geq 0$, the right polynomial map determined by t^i will be denoted by N_i. With these notations one has that $(\sum_{i=0}^n b_i t^i)(a) = \sum_{i=0}^n b_i N_i(a)$ for any polynomial $f(t) = \sum_{i=0}^n b_i t^i \in R$. When $\delta = 0$ one has $N_i(a) = \sigma^{i-1}(a)\sigma^{i-2}(a)\ldots\sigma(a)a$, this justifies the notation N_i.

(c) Let ${}_AV$ be a left A-module. An additive map $T : V \longrightarrow V$ such that, for $\alpha \in A$ and $v \in V$,

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v.$$

is called a (σ,δ) pseudo-linear transformation (or a (σ,δ)-PLT, for short).

Examples 2.

1. If $\sigma = id.$ and $\delta = 0$ we get back the standard way of evaluating a polynomial. It should be noted though, that, since R is not commutative, we have to specify that this is a right polynomial map. For instance, although for $c \in A$ $f(t) = ct = tc \in R = A[t]$, the polynomial map we consider here is the map $f : A \longrightarrow A$ defined by $f(a) = ca$, for any $a \in A$.
2. Let A, σ and δ be a ring, an endomorphism of A and a σ-derivation of A respectively. If $a \in A$, the map

$$T_a : A \longrightarrow A \quad x \mapsto T_a(x) = \sigma(x)a + \delta(x)$$

is a (σ,δ)-PLT defined on the left A-module: ${}_AA$.
   - $\diamond$ if $\sigma = id$ and $\delta = 0$, we get $T_a(x) = xa$.
   - $\diamond$ if $a = 0$, we get $T_0 = \delta$
   - $\diamond$ if $a = 1$ and $\delta = 0$, we get that $T_1 = \sigma$.
   - $\diamond$ if $a = 1$, we get that $T_1 = \sigma + \delta$.
3. Let V be a free left A-module with basis $\beta = \{e_1, \ldots, e_n\}$ and let $T : V \to V$ be a (σ,δ)-PLT. This gives rise to a (σ,δ)-PLT on the left A-module A^n as follows: first define $C = (c_{ij}) \in M_n(A)$ by $T(e_i) = \sum_i^n c_{ij}e_j$. Then we extend component-wise σ and δ to the ring A^n. Finally we then define a (σ,δ)-PLT on A^n (considered as a left A-module) by $T_C(\underline{v}) = \sigma(\underline{v})C + \delta(\underline{v})$, for $\underline{v} \in A^n$. Indeed, it is easy to check that we have $T_C(\alpha\underline{v}) = \sigma(\alpha)T_C(\underline{v}) + \delta(\alpha)\underline{v}$.

(4) Let us remark that powers of a (σ, δ)-pseudo-linear transformation defined on a left A-module V are usually not pseudo-linear. For instance it is easy to check that, for $\alpha \in A$ and $v \in V$, we have

$$T^n(\alpha v) = \sum_{i=0}^{n} f_i^n(\alpha) T^i(v),$$

where f_i^n stands for the sum of all words in σ and δ having $n-i$ letters δ and i letters σ.

In order to increase the sources of Codes, ring structures (and two sided ideals) have been replaced by modules (and one-sided ideals). In the case of modules over Ore extensions the next proposition shows that pseudo-linear maps are unavoidable. In fact, they are also very useful since they are intimately related to factorizations. For instance they offer a generalization of the classical fact that in a commutative setting the evaluation map is a ring homomorphism (cf. Lemma 1).

Proposition 1. *Let A be a ring $\sigma \in End(A)$ and δ a σ-derivation of A. For an additive group $(V, +)$ the following conditions are equivalent:*

(i) *V is a left $R = A[t; \sigma, \delta]$-module;*
(ii) *V is a left A-module and there exists a (σ, δ) pseudo-linear transformation $T : V \longrightarrow V$;*
(iii) *There exists a ring homomorphism $\Lambda : R \longrightarrow End(V, +)$.*

Proof. (i)$\Longrightarrow$ (ii) The pseudo-linear map is given by the left multiplication by t.
(ii)$\Longrightarrow$ (iii) The ring homomorphism $\Lambda : R \longrightarrow End(V, +)$ is defined by $\Lambda(f(t)) = f(T)$, where, for $f(t) = \sum_{i=0}^{n} a_i t^i \in R$, $f(T)$ stands for $\sum_{i=0}^{n} a_i T^i \in End(V, +)$.
(iii)$\Longrightarrow$(i) This is classical. □

As a special case of the example (3) above let us mention the important pseudo-linear transformation associated to a given monic polynomial f of degree n (or rather to its companion matrix C_f). The left A-module V is, in this case, R/Rf. This is given in the following definition.

Definition 1. Let $f(t) = \sum_{i=0}^{n} a_i t^i \in A[t; \sigma, \delta]$ be a monic polynomial of degree n and let

$$C_f = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{n-1} \end{pmatrix}$$

be its companion matrix. Then the map

$T_f : A^n \longrightarrow A^n$ defined by $T_f(x_1, ..., x_n) := (\sigma(x_1), ..., \sigma(x_n))C_f + (\delta(x_1), ..., \delta(x_n))$

is a pseudo-linear transformation called the pseudo-linear transformation associated to f.

Example 1. For $a \in A$ the map:

$$T_a : A \longrightarrow A$$
$$x \longrightarrow T_a(x) = \sigma(x)a + \delta(x)$$

is the pseudo-linear transformation associated to $f(t) = t - a$.

Proposition 2. *Let a be an element in A and $p(t) \in A[t; \sigma, \delta]$. Then:*

(1) $N_0(a) = 1$ *and for* $i \geq 0$, $N_{i+1}(a) = \sigma(N_i(a))a + \delta(N_i(a))$.
(2) $p(T_a)(1) = p(a)$.

Proof. (1) Since $N_i(a)$ is the remainder upon right division of t^i by $t-a$, we have $t^{i+1} = tt^i = t(q_i(t)(t-a)+N_i(a)) = tq_i(t)(t-a)+\sigma(N_i(a))t+\delta(N_i(a)) = (tq_i(t)+\sigma(N_i(a)))(t-a)+\sigma(N_i(a))a+\delta(N_i(a))$. This gives the required equality.
(2) It is enough to show that, for $i \geq 0$, $N_i(a) = T_a^i(1)$. This is clear for $i = 0$. Using the point (a) above and an induction we get $N_{i+1}(a) = \sigma(N_i(a))a+\delta(N_i(a)) = T_a(N_i(a)) = T_a(T_a^i(1)) = T_a^{i+1}(1)$. □

Lemma 1. *Let* $T : V \longrightarrow V$ *be a* (σ,δ) *pseudo-linear transformation defined on a left* A*-module* V. *Then for any polynomial* $p(t), q(t) \in R = A[t;\sigma,\delta]$ *we have* $(p(t)q(t))(T) = p(T)q(T) \in End(V,+)$.

Proof. Let us recall that if $p(t) = \sum_i a_i t^i \in R$ then $p(T)$ is the additive endomorphism defined by $p(T)(v) = \sum_i a_i T^i(v)$, for $v \in V$. Since for $v \in V$ the left R-module structure of V is induced by $t.v := T(v)$, the equality given in the lemma is in fact a simple translation of the fact that $(p(t)q(t)).v = p(t).(q(t).v)$ for $v \in V$, $p(t), q(t) \in R$. □

The formula $p(T_a)(1) = p(a)$ in Proposition 2 can be interpreted as saying that $p(t) \in R(t-a)$ if and only if $p(T_a)(1) = 0$. This can be generalized as follows: for a monic polynomial $f(t) \in R = A[t;\sigma,\delta]$ we denote, as earlier, T_f the pseudo-linear map defined on A^n by the companion matrix of f. We then have $p(t) \in Rf(t)$ if and only if $p(T_f)(1,0,\ldots,0) = (0,\ldots,0)$ (cf. Theorem 1.10 in [12]). Making use of the above lemma 1 we then easily get that, for $p(t), q(t) \in R$ with $\deg(q) < \deg(f)$, $p(t)q(t) \in Rf$ if and only if $p(T_f)q(T_f)(1,0,\ldots,0) = (0,\ldots,0) = p(T_f)(\underline{q})$. We refer the reader to [12] for details. For easy reference, let us sum up this in the following lemma.

Lemma 2. *Let* $f(t), p(t), q(t)$ *be polynomials in* $R = A[t;\sigma,\delta]$ *such that* $f(t)$ *is monic and* $\deg(q) < \deg(f) = n$ *then* $p(t)q(t) \in Rf(t)$ *if and only if* $p(T_f)(\underline{q}) = (0,\ldots,0)$, *where, for* $q(t) = \sum_{i=0}^{n-1} q_i t^i$, *we denote* $\underline{q}$ *the* n*-tuple* $(q_0, q_1, \ldots, q_{n-1})$.

For a monic polynomial $f(t) \in R = A[t;\sigma,\delta]$ of degree n let us mention the following proposition which shows how to translate results from the R/Rf to A^n.

Proposition 3. *Let* $f(t) \in R = A[t;\sigma,\delta]$ *be a monic polynomial of degree* $n > 0$. *The map* $\varphi : R/Rf(t) \longrightarrow A^n$ *given by* $\varphi(p+Rf) = p(T_f)(1,0,\ldots,0)$ *is a bijection.*

Proof. Since T_f represents the left multiplication by t on $R/Rf(t)$ and since this corresponds to the pseudo-linear transformation T_f, the above bijection is clear. □

The above bijection endows A^n with a left $R = A[t;\sigma,\delta]$-module structure.

Let us remark that if $(a_0, a_1, \ldots, a_{n-1}) \in A^n$ then $\varphi(\sum_{i=0}^{n-1} a_i t^i + Rf) = (a_0, \ldots, a_{n-1})$. Notice also that the practical effect of this proposition is a way of computing the remainder of the euclidean right division by $f(t)$.

3. Generic and control matrices of (σ,δ)-codes

Let A be a ring, σ, δ be an endomorphism and a σ-derivation of A respectively.

Definitions 3. Let $f(t)$ be a monic polynomial in $R = A[t;\sigma,\delta]$. A cyclic (f,σ,δ)-code is the image $\varphi(Rg/Rf)$ of the cyclic module Rg/Rf where $g(t) \in A[t;\sigma,\delta]$ is

a monic polynomial such that $f(t) \in Rg(t)$ and φ is the map described in Proposition 3. A cyclic (f, σ, δ)-code $C \subseteq A^n$ is then the subset of A^n consisting of the coordinates of the elements of Rg/Rf in the basis $\{1, t, \ldots, t^{n-1}\}$ for some right monic factor $g(t)$ of $f(t)$.

In the next theorem we answer a few natural questions related to these notions.

Theorem 1. *Let $g(t) := g_0 + g_1 t + \cdots + g_r t^r \in R$ be a monic polynomial ($g_r = 1$). With the above notations we have*

(a) *The code corresponding to Rg/Rf is a free left A-module of dimension $n - r$ where $\deg(f) = n$ and $\deg(g) = r$.*
(b) *If $v := (a_0, a_1, \ldots, a_{n-1}) \in C$ then $T_f(v) \in C$.*
(c) *The rows of the matrix generating the code C are given by*

$$(T_f)^k(g_0, g_1, \ldots, g_r, 0, \ldots, 0), \quad \text{for } 0 \leq k \leq n - r - 1.$$

Proof. (a) We have $f = hg$ for some monic polynomial $h \in R$. Hence as left R-modules we have also $Rg/Rf \cong R/Rh$. Since h is monic R/Rh is a free A-module of rank $\deg(h) = n - r$.
(b) $v = (a_0, \ldots, a_{n-1}) \in C$ if and only if $q(t) := \sum_{i=0}^{n} a_i t^i + Rf \in Rg/Rf$. Since $tq(t) \in Rg/Rf$ and left multiplication by t on R/Rf corresponds to the action of T_f on A^n, we do get that $T_f((a_0, \ldots, a_{n-1})) \in C$, as required.
(c) Clearly for any $k \geq 0$ we have that $T_f^k(g_0, \ldots, g_r, 0, \ldots, 0) \in C$. On the other hand it is clear that $g + Rf, tg + Rf, \ldots, t^{n-r-1}g + Rf$ are left linearly independent over A and hence constitutes a basis of Rg/Rf. In terms of code words this gives that the vectors $T_f^k((g_0, \ldots, g_r, 0, \ldots, 0))$ for $0 \leq k \leq n - r - 1$ form a left A-basis of the code C. □

Examples 3. In the five first examples hereunder $A = \mathbb{F}_{p^n}$ stands for a finite field.

(1) If $\sigma = Id.$, $\delta = 0$, $f = t^n - 1$ and $f = gh$
  (b) gives the cyclicity condition for the code.
  (c) we get the standard generating matrix of a cyclic code.
(2) If $\sigma = Id.$, $\delta = 0$, $f = t^n - \lambda$ and $f = gh$
  (b) gives the constacyclicity condition for the code.
  (c) we get the standard generating matrix of a constacyclic code.
(3) $f = t^n - 1 \in R = \mathbb{F}_q[t; \theta]$ ($\theta =$ "$Frobenius$") and $f = gh \in R$
  (b) gives the θ-cyclicity condition for the code.
  (c) we get the standard generating matrix of a θ-cyclic code (cf. [2]).
(4) If $\sigma = \theta$, $\delta = 0$, $f = t^n - \lambda$ and $f = gh$.
  (b) gives the θ-constacyclicity condition for the code.
  (c) we get the standard generating matrix of a θ-constacyclic code (cf. [3]).
(5) If $A = \mathbb{F}_q$ is a finite field and $\theta \in Aut(\mathbb{F}_q)$ we get the skew codes defined in several papers. Notice that, as mentioned in example 1(4) all the Ore extensions over a finite field are of this form.
(6) Of course, over a finite ring we can also consider Ore extensions of derivation type. For instance, let R be the Ore extension $R := \mathbb{F}_p[x]/(x^p - 1)[t; \frac{d}{dx}]$, where $\frac{d}{dx}$ denotes the usual derivation. $f(t) = t^p - 1$ is in fact a central polynomial in R. Although this polynomial is the standard one for building cyclic codes we will see many differences in the case of cyclic $(id., \delta)$-codes. First let us give the form of the (right) roots of $t^p - 1$ in $A := \mathbb{F}_p[x]/(x^p - 1)$. We must find the elements $q(x) \in A$ such that $N_p(q(x)) = 1$. It is easy to compute

that $N_p(q(x)) = q(x)^p + \frac{d^{p-1}}{dx}(q(x))$ (or cf [12]). Hence since $x^p = 1$, we have $N_p(q(x)) = q(x) + \frac{d^{p-1}}{dx}(q(x))$. Set $q(x) = \sum_{i=0}^{p-1} a_i x^i$. One can check that $N_p(q(x)) = 1$ if and only if $\sum_{i=0}^{p-2} a_i = 1$. In order to be concrete, let us fix $p = 5$. In this case x and $x+x^4$ are roots of t^5-1 and one can easily compute that the polynomial $g(t) := t^2 - 2xt + x^2 - 1$ is in fact the least left common multiple of $t - x$ and $t - (x + x^4)$ in R. A simple reasoning involving the division algorithm then shows that $g(t)$ is a right (and hence left, since $f(t)$ is central) factor of $t^5 - 1$. The generating matrix of the cyclic ($id.$, $\frac{d}{dx}$)-code corresponding to the left module Rg/Rf is given by:

$$G := \begin{pmatrix} x^2-1 & -2x & 1 & 0 & 0 \\ 2x & x^2+2 & -2x & 1 & 0 \\ 2 & 4x & x^2 & -2x & 1 \end{pmatrix}.$$

Property (b) in the above theorem 1 characterizes the codes that can be obtained using a factor of a monic polynomial f.

Definition 2. A monic polynomial $f(t) \in R = A[t;\sigma,\delta]$ is invariant if $Rf(t) = f(t)R$.

Let $C(t) = Rg(t)/Rf(t)$ be a module code, where $f(t), g(t) \in R$ are monic polynomials such that $Rf(t) \subseteq Rg(t)$. Remark that if either $f(t)$ or $g(t)$ is invariant then we can write $f(t) = h'(t)g(t) = g(t)h(t)$, for some monic polynomials $h(t), h'(t) \in R$. When there exist monic polynomials $h(t), h'(t) \in R$ such that $f(t) = h'(t)g(t) = g(t)h(t)$ the cyclic module $Rg(t)/Rf(t)$ can be described via annihilators and the code C via control matrices. We start with the following easy lemma. The proof is left to the reader.

Lemma 3. *Let $f, g, h, h' \in R$ be monic polynomials such that $f = gh = h'g$. Then*

(a) $gR = ann_R(h' + fR)$ *and* $gR/fR = \{p + fR \,|\, p \in ann_R(h' + fR)\}$.
(b) $Rg = ann_R(h + Rf)$ *and* $Rg/Rf = \{p + Rf \,|\, p \in ann_R(h + Rf)\}$.

Theorem 2. *Let $f, g, h, h' \in R$ be monic polynomials such that $f = gh = h'g$ and let C denote the code corresponding to the cyclic module Rg/Rf. Then the following statements are equivalent:*

(i) $(c_0, \ldots, c_{n-1}) \in C$,
(ii) $(\sum_{i=0}^{n-1} c_i t^i)h(t) \in Rf$,
(iii) $\sum_{i=0}^{n-1} c_i T_f^i(\underline{h}) = \underline{0}$,
(iv) $\sum_{j=0}^{n-1}(\sum_{i=j}^{n-1} c_i f_j^i(\underline{h}))N_j(C_f) = \underline{0}$.

Proof. (i) $\Leftrightarrow$ (ii) This is just the definition of $ann_R(h + Rf)$.
(ii) $\Leftrightarrow$ (iii) This comes from Lemma 2.
(iii) $\Leftrightarrow$ (iv) It was mentioned in 2 (4) that, for $\alpha \in A$ and $v \in V$, we have $T^n(\alpha v) = \sum_{i=0}^{n} f_i^n(\alpha)T^i(v)$. Similarly we have, for any $i \geq 0$ $T_f^i(v) = \sum f_j^i(v)N_j(C_f)$. This formula was proved in [11]. □

In view of the above it seems natural to set the following definition.

Definition 3. For a left (resp. right) linear code $C \subseteq A^n$, we say that a matrix H is a control matrix if $C = lann(H)$ (resp. $C = rann(H)$).

From the above theorem 2(iii) we immediately get the following corollary.

Corollary 1. *For a code C determined by the left R-module Rg/Rf such that there exist monic polynomials $h, h' \in R$ with $f = gh = h'g$ the matrix H whose i^{th} row is $T_f^{i-1}(\underline{h})$, for $1 \leq i \leq \deg(f)$ is a control matrix.*

We show hereunder that the above Theorem 2 and Corollary 1 give back the control matrix of classical cyclic and skew cyclic codes.

Examples 4. (1) Let $f(t) = t^n - 1 \in R = F[t]$, where F is a (finite) field. and let $g(t), h(t) \in R$ be such that $t^n - 1 = g(t)h(t) = h(t)g(t)$. We write $h(t) = \sum_{i=0}^{k} h_i t^i$. For $\underline{v} = (v_0, \ldots, v_{n-1}) \in k^n$, the action of T_f^i is given by $T_f^i(\underline{v}) = (v_0, \ldots, v_{n-1})C^i$, where C is the companion matrix associated to the polynomial $t^n - 1$. Theorem 2 shows that a control matrix associated to the code C corresponding to Rg/Rf is the following:

$$\begin{pmatrix} h_0 & h_1 & \ldots & h_k & 0 & 0 & \ldots & 0 \\ 0 & h_0 & \ldots & h_{k-1} & h_k & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ldots & 0 \\ 0 & 0 & \ldots & h_0 & h_1 & \ldots & \ldots & h_k \\ h_k & 0 & \ldots & 0 & h_0 & \ldots & \ldots & h_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ h_2 & h_3 & \ldots & \ldots & \ldots & \ldots & \ldots & h_1 \\ h_1 & h_2 & \ldots & \ldots & \ldots & \ldots & \ldots & h_0 \end{pmatrix}.$$

Of course, the dimension of Rg/Rf is equal to k and hence the rank of the control matrix must be $n - k$. In other words, any set of $n - k$ independent columns of the above matrix will have C as its (left) kernel. Since the last $n - k$ columns are in echelon form, they are independent and hence these last columns give as well a control matrix, say H. Since F is commutative we can see the code as a right linear code and use the standard transposition to get the control matrix of this "right" linear code. A control matrix for C considered as a right linear code is thus just the transpose of H. This is the standard control matrix.

(2) In the same way as (1) we can consider the θ-cyclic codes and obtain their control matrices retrieving formulas proved elsewhere (e.g. [2]). In fact we more generally consider the following situation Let A be a ring and σ an automorphism of A (classically A is a finite field and σ is the Frobenius automorphism). Assume $t^n - 1 = gh = h'g$, where $g, h, h' \in R$ are monic polynomials. Let us write $h(t) = \sum_{i=0}^{k} h_i t^i$, with $h_k = 1$. The pseudo-linear transformation defined by $f(t) = t^n - 1$ is the map $T_f : A^n \longrightarrow A^n$ defined by $T_f(\underline{v}) = \sigma(\underline{v})C$, where C is the companion matrix associated to $t^n - 1$ and $\underline{v} \in A^n$. It is easy to check that the following matrix H is a control matrix for the code C determined by the module Rg/Rf:

$$H = \begin{pmatrix} h_0 & h_1 & \ldots & h_k & 0 & 0 & \ldots & 0 \\ 0 & \sigma(h_0) & \ldots & \sigma(h_{k-1}) & \sigma(h_k) & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ldots & 0 \\ 0 & 0 & \ldots & \sigma^{n-k-1}(h_0) & \sigma^{n-k-1}(h_1) & \ldots & \ldots & \sigma^{n-k-1}(h_k) \\ \sigma^{n-K}(h_k) & 0 & \ldots & 0 & \sigma^{n-k}(h_0) & \ldots & \ldots & \sigma^{n-k}(h_{k-1}) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ \sigma^{n-2}(h_2) & \sigma^{n-2}(h_3) & \ldots & \ldots & \ldots & \ldots & \ldots & \sigma^{n-2}(h_1) \\ \sigma^{n-1}(h_1) & \sigma^{n-1}(h_2) & \ldots & \ldots & \ldots & \ldots & \ldots & \sigma^{n-1}(h_0) \end{pmatrix}.$$

So the last $n-k$ columns are in echelon form and hence linearly independent. The dimension of the code being equal to k, in good cases (e.g. if the ring is

a field), this means that they define a control matrix as well. The transpose of these last columns is exactly the control matrix obtained by other authors in the case when A is a commutative field.

(3) Let us now give an example of a cyclic code using a derivation. Let A be a ring and δ be a (usual) derivation on A. For $a \in A$ we consider the polynomial $f(t) := (t^2 - a)^2 \in A[t;\delta]$ and put $g = h = t^2 - a$. We easily compute $f(t) = t^4 - 2at^2 - 2\delta(a)t - \delta^2(a) + a^2$. The generic matrix G and control matrix H are equal:

$$H = \begin{pmatrix} -a & 0 & 1 & 0 \\ -\delta(a) & -a & 0 & 1 \\ -a^2 & 0 & a & 0 \\ a\delta(a) - \delta(a)a & -a^2 & \delta(a) & a \end{pmatrix}.$$

One can check that $\underline{g}H = (-a, 0, 1, 0)H = (0, 0, 0, 0)$. Set H_1, H_2, H_3, H_4 to represent the different columns of H, then $H_1 + H_3(-a) + H_4\delta(a) = 0 \in A^4$ and $H_2 + aH_4 = 0 \in A^4$. Let H' be the 4×2 matrix $H' = (H_3, H_4)$. We easily get that $lann(H') = lann(H) = C$. This shows that H' is a control matrix of the code C.

(4) We now compute a control matrix of the cyclic code given in the above example 3 (4). We have $R := \mathbb{F}_5[x]/(x^5 - 1)[t; \frac{d}{dx}]$, and $f(t) = t^5 - 1$. This last polynomial is central and can be factorized as $f(t) = g(t)h(t) = h(t)g(t)$ where $g(t) := t^2 - 2xt + x^2 - 1$ and $h(t) = t^3 + 2xt^2 + (3x^2 + 2)t + (4x^3 + 3x)$. The code we are considering corresponds to the module $Rg(t)/(t^5 - 1)$. The control matrix is given by the matrix $H \in M_5(\mathbb{F}_5)$ whose rows are given by $T_f^i(\underline{h})$, $0 \le i \le 4$. The first row is thus $\underline{h}$ the second row is $\underline{h}C_f + \frac{d}{dx}(\underline{h})$. Here C_f is the companion matrix of $t^5 - 1$ and acts as cyclic permutation. Hence we get

$$H = \begin{pmatrix} 4x^3 + 3x & 3x^2 + 2 & 2x & 1 & 0 \\ 2x^2 + 3 & 4x^3 + 4 & 3x^2 + 4 & 2x & 1 \\ 4x + 1 & 4x^2 + 2 & 4x^3 & 3x^2 + 1 & 2x \\ 2x + 4 & 2x + 1 & x^2 + 2 & 4x^3 + 6x & 3x^2 + 3 \\ 3x^2 & 2x + 1 & 4x + 1 & 3x^2 + 3 & 4x^3 + 2x \end{pmatrix}.$$

4. (σ,δ)-W-CODES

We will consider cyclic $(f(t), \sigma, \delta)$-codes corresponding to left cyclic modules of the form $Rg(t)/Rf(t)$ where $f(t), g(t) \in R = A[t;\sigma,\delta]$ are monic polynomials but $g(t)$ is a Wedderburn polynomial as explained in the following definitions.

Definitions 4. (a) A monic polynomial $g(t) \in R = A[t;\sigma,\delta]$ of degree r is a Wedderburn polynomial if there exist elements $a_1, \ldots, a_r \in A$ such that $Rg(t) = \bigcap_{i=0}^{r} R(t - a_i)$. We will refer to these polynomials as W- polynomials.

(b) The $n \times r$ generalized Vandermonde matrix defined by $a_1, \ldots, a_r$ is given by:

$$V_n(a_1, \ldots, a_r) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_r \\ \ldots & \ldots & \ldots & \ldots \\ N_{n-1}(a_1) & N_{n-1}(a_2) & \ldots & N_{n-1}(a_r) \end{pmatrix}.$$

Recall that, for $0 \le i \le n - 1$, $N_i(a)$ is the evaluation of t^i at $a \in A$ (cf. Definitions 2).

(c) A (σ,δ)-W-code $C \subseteq A^n$ is the set of n-tuples in A^n corresponding to a cyclic left R-module of the form $Rg(t)/Rf(t)$ such that $g(t)$ is a W-polynomial.

Wedderburn polynomials have been studied in details in [9] and [10]. The generic matrix corresponding to a (σ,δ)-W-code is the standard one described in 1. But an easy control matrix can be obtained as described in the next proposition.

Let us first state a general lemma.

Lemma 4. *Let $f(t), g(t), h(t) \in R = A[t;\sigma,\delta]$ be monic polynomials such that $f(t) = h(t)g(t)$. Then $Rg(t)/Rf(t) = \{p(t)g(t) + Rf(t) \mid \deg p(t) < \deg h(t)\}$.*

Proof. This is obvious: if $m(t)g(t) + Rf(t) \in Rg(t)/Rf(t)$, dividing by the monic polynomial $h(t)$, we can write $m(t) = q(t)h(t) + p(t)$ with $\deg p(t) < \deg h(t)$ and we have $m(t)g(t) + Rf(t) = p(t)g(t) + Rf(t)$. □

Proposition 4. *Let $f(t), g(t) \in R = A[t;\sigma,\delta]$ be monic polynomials of degree n and r respectively. Suppose that $g(t)$ is a Wedderburn polynomial with $f(t) \in Rg(t)$ and let C be the (σ,δ)-W-code of length n corresponding to the left cyclic R-module $Rg(t)/Rf(t)$. Let $a_1, \ldots, a_r \in A$ be such that $Rg(t) = \bigcap_{i=0}^{r} R(t-a_i)$. Then $(c_0, c_1, \ldots, c_{n-1}) \in C$ if and only if $(c_0, c_1, \ldots, c_{n-1})V_n(a_1, \ldots, a_r) = (0, \ldots, 0)$.*

Proof. Let us remark that a polynomial $h(t) = \sum_{i=0}^{n-1} h_i t^i \in Rg(t)$ if and only if $h(a_i) = 0$ for all $1 \le i \le r$. Since $(h(a_0), \ldots, h(a_r)) = (h_0, \ldots, h_{n-1})V_n(a_1, \ldots, a_r)$, we have $h(t) \in Rg(t)$ if and only if $(h_0, \ldots, h_{n-1})V_n(a_1, \ldots, a_r) = (0, \ldots, 0)$. This yields the thesis. □

Example 2. Let us consider (6) in Examples 3. We have $A := \mathbb{F}_5[x]/(x^p - 1)$ and $R = A[t; \frac{d}{dx}]$. The polynomial $g(t)$ and $f(t)$ in this example are respectively $g(t) = t^2 - 2xt + x^2 - 1$ and $f(t) = t^5 - 1$. Since $g(t)$ is the least left common multiple of $t - x$ and $t - (x + x^4)$ we get immediately that the control H matrix is the transpose of the following matrix

$$H^t = V_5(x, x + x^4)^t = \begin{pmatrix} 1 & x & x^2+1 & x^3+3x & x^4+x^2+3 \\ 1 & x+x^4 & 3+x^2 & x+x^3+3x^4 & x^4 \end{pmatrix}.$$

One may easily check that $GH = 0$, where G is the matrix which generates the code given in this example (cf. 3.

The proposition above amounts to saying that a control matrix is given by the Vandermonde matrix $V_n(a_1, \ldots, a_r)$. The Vandermonde matrix determined by Wedderburn polynomial $g(t)$ can thus be used as a control matrix for the (σ,δ)-W-code C.

Remarks 1.

(1) The Vandermonde matrices are strongly related to Wronskian matrices and to noncommutative symmetric functions. In a (σ,δ)-setting information can be found in [5]. In particular, in this reference an axiomatic method is developed in order to compute the least left common multiple of polynomials of the form $t - a_1, \ldots, t - a_n$.

(2) In general the existence of a least left common multiple of linear polynomials of the form $t - a_1, \ldots, t - a_r$ is not guaranteed (for a general ring A). The exact necessary and sufficient conditions for the existence of a LLCM of such polynomials is given in Theorem 7.2 in [5].

(3) If A is a division ring the existence of LLCM of $t - a_1, \ldots, t - a_r$ is clear but its degree can be less then r even if the elements $a_1, \ldots, a_r$ are all distinct. For several necessary and sufficient conditions for this degree to be equal to

r we refer the reader to [9] and [10]. In the case of a finite field $\mathbb{F}_q$ such a condition can be found in [14], pp 117-119.

The next theorem gives a characterization of the W-polynomials in $R=\mathbb{F}_q[t;\theta]$.

Theorem 3. *Let p be a prime number and $n\in\mathbb{N}$. Let also R be the Ore extension $R=\mathbb{F}_q[t;\theta]$, where $q=p^n$ and θ is the Frobenius map. We extend θ to R by defining $\theta(t)=t$. Then:*

(a) *The polynomial $G(t)=t^{(p-1)n+1}-t$ (resp. $G_0(t)=t^{(p-1)n}-1$) is the least left common multiple of all the linear polynomials $t-a$, $a\in\mathbb{F}_q$ (resp. $0\neq a\in\mathbb{F}_q$).*

(b) *Let $G(t)$ and $G_0(t)$ be as in the statement (a) above. For any $h(t)\in\mathbb{F}_q[t;\theta]$, we have $G(t)h(t)=\theta(h(t))G(t)$. The polynomial $G_0(t)=t^{(p-1)n}-1$ belongs to the center of R.*

(c) *Let $G(t)$ and $G_0(t)$ be as in the statement (a) above. If $g(t),h(t)\in\mathbb{F}_q[t;\theta]$ are monic polynomials such that $h(t)g(t)=G(t)$, then $\theta(g(t))h(t)=G(t)$. Similarly if $h(t)g(t)=G_0(t)$ then $g(t)h(t)=G_0(t)$.*

(d) *The W-polynomials are exactly the right (and left) factors of the polynomial $G(t)$ mentioned in statement (a).*

Proof. (a) The fact that the polynomial $G(t)$ is a least left common multiple of the polynomials $t-a$, such that $a\in\mathbb{F}_q$ was proved in Theorem 2.3 in [12].
(b) Since $\theta^n=id.$, it is easy to check that $G(t)a=\theta(a)G(t)$ and $G_0(t)a=aG_0(t)$, for any $a\in A$. This yields the results.
(c) Multiplying the equality $h(t)g(t)=G(t)$ by $g(t)$ on the right we get $h(t)g(t)^2=G(t)g(t)=\theta(g(t))G(t)=\theta(g(t))h(t)g(t)$. Since R is an integral domain we obtain $G(t)=h(t)g(t)=\theta(g(t))h(t)$. The statement related to $G_0(t)$ is obtained similarly.
(d) Let $g(t)$ be a Wedderburn polynomial, say $Rg(t)=\bigcap_{i=0}^{r}R(t-a_i)$. Since $G(a_i)=0$, for any $i=0,\dots r$, we immediately get that $G(t)\in Rg(t)$. This shows that $g(t)$ is a right factor of $G(t)$. By its definition, $G(t)$ is a Wedderburn polynomial. It is a standard fact that factors of Wedderburn polynomials are themselves Wedderburn (cf. [9]). □

Example 3. Consider the field $\mathbb{F}_16$ presented as $\mathbb{F}_2(a,b)$ where $a^2+a+1=0$ and $b^2+ab+1=0$. In $R=\mathbb{F}_16[t;\theta$, where $thta$ is the Frobenius map, we easily check that the left common multiple of $t-a$ and $t-b$ is $g(t):=t^2+at+a$. We also verify that $(t^2+at+a+1)g(t)=t^4+1$. The control matrix corresponding to the code $Rg/R(t^4-1)$ is given by $V_4(a,b)$. Explicitly we have

$$V_4(a,b)^t=\begin{pmatrix}1 & a & N_2(a) & N_3(a)\\ 1 & b & N_2(b) & N_3(b)\end{pmatrix}^t=\begin{pmatrix}1 & a & 1 & a\\ 1 & b & ab+a & ab+1\end{pmatrix}^t.$$

Theorem 3 also shows that even without knowing the roots of the Wedderburn polynomial $g(t)$, we immediately get a control matrix. This is the content of the following corollary.

Corollary 2. *Let $g(t)\in R=\mathbb{F}_q[t;\theta]$ be a W-polynomial of degree r. As in the previous theorem let us denote $G_0(t)=t^{(p-1)n}-1$ and $G(t)=t^{(p-1)n+1}-t$. Let $g(t),h(t)\in R$ be monic polynomials such that $G(t)=h(t)g(t)$ and consider the cyclic $(G(t),\theta,0)$-code C defined by the R-module $Rg(t)/RG(t)$.*

(a) *There exists $1\leq l\leq n$ such that $\theta^l(g(t))=g(t)$ and we then have $G(t)=h(t)g(t)=g(t)\theta^{l-1}(h(t))$.*

(b) *The control matrix of the code C is given by the matrix whose rows are $T_G^i(\theta^{l-1}(\underline{h}))$ for $0\leq i\leq(p-1)n$.*

(c) *Suppose the polynomial* $g(t)$ *is such that* $g(0) \neq 0$. *Then there exists* $h'(t) \in R$ *such that* $G_0(t) = h'(t)g(t) = h(t)g'(t)$. *The control matrix of the code corresponding to the cyclic module* $Rg(t)/RG_0(t)$ *is given by the matrix whose rows are* $T^i_{G_0}(\underline{h'})$ *for* $0 \leq i \leq (p-1)n-1$.

Proof. The proofs are left to the reader. □

Acknowledgments

This paper was partially prepared while the first author visited the University of Artois. He would like to thank the members of this institution for their kind hospitality.

References

[1] S. A. Amitsur, Derivations in simple rings, *Proc. London Math. Soc.*, **3** (1957), 87–112.
[2] D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, *Appl. Algebra Engin. Commun. Comp.*, **18** (2007), 379–389.
[3] D. Boucher, P. Solé and F. Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, **2** (2008), 273–292.
[4] D. Boucher and F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, *Des. Codes Cryptogr.*, to appear.
[5] J. Delenclos and A. Leroy, Noncommutative symmetric functions and W-polynomials, *J. Algebra Appl.*, **6** (2007), 815–837.
[6] M. Giesbrecht, Factoring in skew polynomial rings over finite fields, *J. Symb. Comp.*, **26** (1998), 463–468.
[7] N. Jacobson, On pseudo linear transformations, *Ann. Math.*, **38** (1937), 484–507.
[8] S. K. Jain and S. R. Nagpaul, *Topics in Applied Abstract Algebra*, AMS, 2005.
[9] T. Y. Lam and A. Leroy, Wedderburn polynomials over division rings, I, *J. Pure Appl. Algebra*, **186** (2004), 43–76.
[10] T. Y. Lam, A. Leroy and A. Ozturk, Wedderburn polynomial over division rings, II, *Contemp. Math.*, **456** (2008), 73–98.
[11] A. Leroy, Pseudo-linear transformation and evaluation in Ore extension, *Bull. Belg. Math. Soc.*, **2** (1995), 321–345.
[12] A. Leroy, Noncommutative polynomial maps, *J. Algebra Appl.*, **11** (2012).
[13] S. R. López-Permouth and S. Szabo, Convolutional codes with additional algebraic structures, *J. Pure Appl. Algebra*, (2012).
[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1978.
[15] P. Solé, Codes over rings, in *Proceeding of the CIMPA Summer School*, Ankara, Turkey, 2008.
[16] P. Solé and O. Yemen, Binary quasi-cyclic codes of index 2 and skew polynomial rings, *Finite Fields Appl.*, **18** (2012), 685–699.
[17] J. Wood, Code equivalence characterizes finite Frobenius rings, *Proc. Amer. Math. Soc.*, **136** (2008), 699–706.

Received for publication October 2012.

E-mail address: boulag@rocketmail.com
E-mail address: andre.leroy@univ-artois.fr