A NOTE ON LINEAR CODES AND NONASSOCIATIVE ALGEBRAS OBTAINED FROM SKEW POLYNOMIAL RINGS

S. PUMPLÜN

Abstract. Different approaches to construct linear codes using skew-polynomials can be unified by using the nonassociative algebras built from skew-polynomial rings by Petit.

Introduction

In recent years, several classes of linear codes were obtained from skew-polynomial rings (also called Ore rings). Using this approach, self-dual codes were found with better minimal distances than the previously best known minimal distances for certain lengths. While the classical *cyclic codes* of length m over a finite field $\mathbb{F}_q$ are obtained from ideals in the commutative ring $\mathbb{F}_q[t]/(t^m-1)$, and *constacyclic codes* from ideals in the commutative ring $\mathbb{F}_q[t]/(t^m-1)$, $d \in \mathbb{F}_q$, *ideal σ-codes* are associated with left ideals $\mathbb{F}_q[t;\sigma]g/(t^m-1)$ in the non-commutative ring $\mathbb{F}_q[t;\sigma]/(t^m-1)$ with $t^m-1 \in R$ a two-sided element in the twisted polynomial ring $\mathbb{F}_q[t;\sigma]$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ and treated in [4]. Because t^m-1 is required to be a two-sided element in order for $\mathbb{F}_q[t;\sigma]/(t^m-1)$ to be a ring, this enforces restrictions on the possible lengths of the codes obtained: t^m-1 is two-sided if and only if the order n of σ divides m [10, (15)].

If Rf denotes the left ideal generated by an element $f \in R$, R a ring, then R/Rf is a left R-module. In [3], linear codes associated with left R-submodules Rg/Rf of R/Rf are considered, where $R = \mathbb{F}_q[t;\sigma]$ and g is a right divisor of f. These codes are called *module σ-codes*. Another generalization is then discussed in [1] and [6], where codes obtained from submodules of the R-module R/Rf for some monic polynomial $f \in R$ are investigated, where now $R = \mathbb{F}_q[t,\sigma,\delta]$.

In this note, we show that all these approaches can be unified by looking at the codes mentioned above as associated to the left ideals of the nonassociative algebra S_f defined by Petit [10]. For a unital division ring D (which here will be a finite field), and a polynomial f in the skew-polynomial ring $R = D[t;\sigma,\delta]$, Petit defined a nonassociative ring on the set $R_m = \{h \in D[t;\sigma,\delta] \,|\, \deg(h) < m\}$, using right division $g \circ h = gh \bmod_r f$ to define the algebra multiplication. $S_f = (R_m, \circ)$ is a nonassociative algebra over $F_0 = \{a \in D \,|\, ah = ha \text{ for all } h \in S_f\}$ whose left ideals are generated by the polynomials g which are right divisors of f.

The scenarios treated with respect to the linear codes mentioned above all require f to be reducible, so the corresponding, not necessarily associative, algebra S_f is not allowed to be

Date: 17.7.2014.

Key words and phrases. Skew-polynomials, Ore rings, finite rings, nonassociative algebras, linear code, σ-constacyclic code, σ-constacyclic code, (σ,δ)-code.

a division algebra here. The cyclic submodules studied in [2], [1] are exactly the left ideals in the algebra S_f. The (σ,δ)-codes of [6] are the codes $\mathcal{C}$ associated to a left ideal of S_f generated by a right divisor g of f with $f\in K[t;\sigma,\delta]$. We show that if σ is an automorphism of $K=\mathbb{F}_q$ and $\mathcal{C}$ a linear code over $\mathbb{F}_q$ of length m, then $\mathcal{C}$ is a σ-constacyclic code with constant d iff the skew-polynomial representation $\mathcal{C}(t)$ with elements $a(t)$ obtained from $(a_0,\dots,a_{m-1})\in\mathcal{C}$ is a left ideal of S_f with $f=t^m-d\in R=\mathbb{F}_q[t;\sigma]$, generated by a monic right divisor g of f in R.

1. Preliminaries

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

An algebra $A\neq 0$ is called a *division algebra* if for any $a\in A$, $a\neq 0$, the left multiplication with a, $L_a(x)=ax$, and the right multiplication with a, $R_a(x)=xa$, are bijective. A is a division algebra if and only if A has no zero divisors ([12], pp. 15, 16).

For an F-algebra A, associativity in A is measured by the *associator* $[x,y,z]=(xy)z-x(yz)$. The *left nucleus* of A is defined as $\mathrm{Nuc}_l(A)=\{x\in A\,|\,[x,A,A]=0\}$, the *middle nucleus* of A is defined as $\mathrm{Nuc}_m(A)=\{x\in A\,|\,[A,x,A]=0\}$ and the *right nucleus* of A is defined as $\mathrm{Nuc}_r(A)=\{x\in A\,|\,[A,A,x]=0\}$. Their intersection $\mathrm{Nuc}(A)=\{x\in A\,|\,[x,A,A]=[A,x,A]=[A,A,x]=0\}$ is the *nucleus* of A. $\mathrm{Nuc}(A)$ is an associative subalgebra of A containing $F1$ and $x(yz)=(xy)z$ whenever one of the elements x,y,z is in $\mathrm{Nuc}(A)$. The *center* of A is $\mathrm{C}(A)=\{x\in A\,|\,x\in\mathrm{Nuc}(A)$ and $xy=yx$ for all $y\in A\}$.

1.2. **Skew-polynomial rings.** In the following, we use the terminology used by Jacobson [7] and Petit [10]. Let D be a unital associative division ring, σ a ring endomorphism of D and δ a *left σ-derivation* of D, i.e. an additive map such that

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

for all $a,b\in D$, implying $\delta(1)=0$. The *skew-polynomial ring* $D[t;\sigma,\delta]$ is the set of polynomials

$$a_0+a_1t+\dots+a_nt^n$$

with $a_i\in D$, where addition is defined term-wise and multiplication by

$$ta=\sigma(a)t+\delta(a)\quad (a\in D).$$

That means,

$$at^nbt^m=\sum_{j=0}^{n}a(S_{n,j}b)t^{m+j}$$

$(a,b\in D)$, where the map $S_{n,j}$ is defined recursively via

$$S_{n,j}=\delta(S_{n-1,j})+\sigma(S_{n-1,j-1}),$$

with $S_{0,0} = id_D$, $S_{1,0} = \delta$, $S_{1,1} = \sigma$ and so $S_{n,j}$ is the sum of all polynomials in σ and δ of degree j in σ and degree $n-j$ in δ [7, p. 2]. If $\delta = 0$, then $S_{n,j} = \sigma^n$. $D[t;\sigma] = D[t;\sigma,0]$ is called a *twisted polynomial ring* and $D[t;\delta] = D[t;id,\delta]$ a *differential polynomial ring.* For the special case that $\sigma = id$ and $\delta = 0$, we obtain the usual ring of left polynomials $D[t] = D[t;id,0]$, often also denoted $D_L[t]$ in the literature, with its multiplication given by

$$(\sum_{i=1}^{s} a_i t^i)(\sum_{i=1}^{t} b_i t^i) = \sum_{i,j} a_i b_j t^{i+j}.$$

If D has finite dimension over its center and σ is a ring automorphism of D, then $R = D[t;\sigma,\delta]$ is either a twisted polynomial or a differential polynomial ring by a linear change of variables [7, Thm. 1.2.21]. Note also that if σ and δ are F-linear maps then $D[t;\sigma,\delta] \cong D[t]$ by a linear change of variables.

For $f = a_0 + a_1 t + \cdots + a_n t^n$ with $a_n \neq 0$ define $\deg(f) = n$ and $\deg(0) = -\infty$. Then $\deg(fg) = \deg(f) + \deg(g)$. An element $f \in R$ is *irreducible* in R if it is no unit and it has no proper factors, i.e if there do not exist $g, h \in R$ with $\deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

$R = D[t;\sigma,\delta]$ is a left principal ideal domain and there is a right-division algorithm in R [7, p. 3]: for all $g, f \in R$, $g \neq 0$, there exist unique $r, q \in R$, and $\deg(r) < \deg(f)$, such that

$$g = qf + r.$$

If σ is a ring automorphism then $R = D[t;\sigma,\delta]$ is a left and right principal ideal domain (a PID) [7, p. 6] and there is also a left-division algorithm in R [7, p. 3 and Prop. 1.1.14]. (We point out that our terminology is the one used by Petit in [10] and in the coding literature we cite; it is different from Jacobson's, who calls what we call left a right-division algorithm and vice versa.)

If σ is a ring automorphism, two non-zero elements $f, g \in R$ are called *similar* ($f \sim g$) if and only if there exist $h, q, u \in R$ such that

$$1 = hf + qg \text{ and } u'f = gu$$

for some $u' \in R$ if and only if $R/Rf = R/Rg$ [7, p. 11]. If σ is a ring automorphism, $R = D[t;\sigma,\delta]$ is a PID, hence any element $f \in R$, $f \neq 0$ which is not a unit in R, can be written as $f = p_1 \cdots p_s$ with irreducible $p_i \in R$. If $f = p_1 \cdots p_s = p'_1 \cdots p'_t$, where the p_i and the p'_i are irreducible, then $s = t$ and there exists a permutation $\pi \in S_s$ such that $p_i \sim p'_{\pi(i)}$ for all i. This is the Fundamental Theorem of Arithmetic in a PID [7, Theorem 1.2.9]. Obviously, $f \sim g$ implies that $\deg(f) = \deg(g)$.

2. How to obtain nonassociative division algebras from skew-polynomial rings

Let D be a unital associative division algebra and $f \in D[t;\sigma,\delta]$ of degree m.

Definition 1. (cf. [10, (7)]) Let $\mathrm{mod}_r f$ denote the remainder of right division by f. Then

$$R_m = \{g \in D[t;\sigma,\delta] \,|\, \deg(g) < m\}$$

together with the multiplication

$$g \circ h = gh \,\mathrm{mod}_r f$$

becomes a unital nonassociative algebra $S_f = (R_m, \circ)$ over $F_0 = \{a \in D \,|\, ah = ha \text{ for all } h \in S_f\}$. This algebra is also denoted by R/Rf [10, 11] if we want to make clear which ring R is involved in the construction.

Note that F_0 is a subfield of D [10, (7)].

Remark 1. Suppose that $\delta = 0$.
(i) If $\deg(g)\deg(h) < m$ then the multiplication of f and g in S_f is the same as the multiplication in R [10, (10)]. Moreover, for $f(t) = t^m - \sum_{i=0}^{m-1} d_i t^i \in R = D[t;\sigma]$, we have

$$t^m = \sum_{i=0}^{m-1} d_i t^i$$

in S_f, so that for $i + j > m$,

$$t^i t^j = t^{i+j-m} \sum_{i=0}^{m-1} d_i t^i.$$

For $f(t) = t^m - d_0 \in R$, multiplication in S_f is thus defined via

$$(at^i)(bt^j) = \begin{cases} a\sigma^j(b)t^{i+j} & \text{if } i + j < m, \\ a\sigma^j(b)t^{(i+j)-m}d_0 & \text{if } i + j \geq m, \end{cases}$$

for all $a, b \in D$ and then linearly extended.
(ii) Given a cyclic Galois field extension K/F of degree m with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$, the cyclic algebra $(K/F, \sigma, d)$ is the algebra S_f with $R = K[t;\sigma^{-1}]$ and $f(t) = t^m - d$ (cf. [10, p. 13-13]), and is nonassociative iff $d \notin F$.

Theorem 2. *(cf. [10]) Let $f \in R = D[t;\sigma,\delta]$.*
(i) If S_f is not associative then

$$\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = D \text{ and } \mathrm{Nuc}_r(S_f) = \{g \in R \,|\, fg \in Rf\}.$$

(ii) Let $f \in R$ be irreducible and S_f a finite-dimensional F_0-vector space or a finite-dimensional right $\mathrm{Nuc}_r(S_f)$-module. Then S_f is a division algebra.
(iii) S_f is associative if and only if f is a two-sided element if and only if Rf is a two-sided ideal

If f is irreducible then S_f is an associative algebra if and only if $f \in C(R)$.
(iv) Let $f = t^m - \sum_{i=0}^{m-1} d_i t^i \in R = D[t;\sigma]$. Then $f(t)$ is a two-sided element of S_f if and only if $\sigma^m(z)d_i = d_i\sigma^i(z)$ for all $z \in D$, $0 \leq i < m$ and $\sigma(d_i) = d_i$ for all i, $0 \leq i < m$.

3. Linear codes associated to left ideals of S_f

Let K be a finite field, σ an automorphism of K and $F = \mathrm{Fix}(\sigma)$, $[K : F] = n$. By a linear base change we can always assume $\delta = 0$. However, [1] and [6] show that this limits the choices of available codes.

Unless specified otherwise, let $R = K[t;\sigma,\delta]$ and $f \in R$ be a monic polynomial of degree m. Analogously as for instance in [3], [4], [1], [2], we associate to an element $a(t) = \sum_{i=0}^{m-1} a_i t^i$

in S_f the vector $(a_0, \dots, a_{m-1})$. Our codes $\mathcal{C}$ of length m consist of all $(a_0, \dots, a_{m-1})$ obtained this way from the elements $a(t) = \sum_{i=0}^{m-1} a_i t^i$ in a left ideal I of S_f. Conversely, for a linear code $\mathcal{C}$ of length n we denote by $\mathcal{C}(t)$ the set of skew-polynomials $a(t) = \sum_{i=0}^{m-1} a_i t^i \in S_f$ associated to the codewords $(a_0, \dots, a_n) \in \mathcal{C}$.

Proposition 3. *Let D be a unital associative division ring and $R = D[t; \sigma, \delta]$.*
(i) All left ideals in S_f are generated by some monic right divisor g of f in R.
(ii) If S_f is irreducible, then S_f has no non-trivial left ideals.

Proof. (i) The proof is analogous to the one of [5, Lemma 1], only that now we are working in the nonassociative ring S_f: Let I be a left ideal of S_f. If $I = \{0\}$ then $I = (0)$. So suppose $I \neq (0)$ and choose a monic non-zero polynomial g in $I \subset R_m$ of minimal degree. For $p \in I \subset R_m$, a right division by g yields unique $r, q \in R$ with $\deg(r) < \deg(g)$ such that

$$p = qg + r$$

and hence $r = p - qg \in I$. Since we chose $g \in I$ to have minimal degree, we conclude that $r = 0$, implying $p = qg$ and so $I = Rg$.
(ii) follows from (i). □

We conclude that the cyclic submodules studied in [2], [1] are exactly the left ideals in the algebra S_f. The (σ, δ)-codes of [6] are the codes $\mathcal{C}$ associated to a left ideal of S_f generated by a non-trivial right divisor g of f with $f \in K[t; \sigma, \delta]$. Note that when we look at the nonassociative case, where f is not two-sided anymore, it can happen that f is irreducible in $K[t; \sigma, \delta]$, hence does not have any non-trivial right divisors g.

Remark 4. Let $m \geq 2$. Since for $a(t) \in S_f$ also $ta(t) \in S_f$, we obtain for instance for $f(t) = t^m - d \in K[t; \sigma]$ that

$$ta(t) = \sigma(a_0)t + \sigma(a_1)t^2 + \cdots + \sigma(a_{m-1})t^m = \sigma(a_{m-1})d + \sigma(a_0)t + \sigma(a_1)t^2 + \cdots + \sigma(a_{m-2})t^{m-1}$$

in S_f, so that

$$(a_0, \dots, a_{m-1}) \in \mathcal{C} \Rightarrow (\sigma(a_{m-1})d, \sigma(a_0), \dots, \sigma(a_{m-2})) \in \mathcal{C}$$

is a σ-constacyclic code (even if S_f is division). With the same argument, every left ideal Rg in S_f with $g \in R$ a right divisor of $f = t^m - d$ yields a σ-constacyclic code $\mathcal{C}$ for $d \neq 1$ and a σ-cyclic code for $d = 1$.

In [5, Theorem 1] it is shown that the code words of a σ-cyclic code are coefficient tuples of elements $a(t) = \sum_{i=0}^{m-1} a_i t^i \in \mathbb{F}_q[t; \sigma]/(t^m - 1)$, which are left multiples of some element $g \in \mathbb{F}_q[t; \sigma]/(t^m - 1)$ which is a right divisor of f, under the assumption that the order n of σ divides m. The assumption that n divides m guarantees that Rf is a two-sided ideal, i.e. that S_f is associative, but is not required:

Theorem 5. *Let σ be an automorphism of $K = \mathbb{F}_q$ and $\mathcal{C}$ a linear code over $\mathbb{F}_q$ of length m. Then $\mathcal{C}$ is a σ-constacyclic code (with constant d) iff the skew-polynomial representation $\mathcal{C}(t)$ with elements $a(t)$ obtained from $(a_0, \dots, a_{m-1}) \in \mathcal{C}$ is a left ideal of S_f with $f = t^m - d \in R = \mathbb{F}_q[t; \sigma]$, generated by a monic right divisor g of f in R.*

Proof. $\Leftarrow$: This is Remark 8.

$\Rightarrow$: The argument is analogous to the proof of [5, Theorem 1]: If we have a σ-constacyclic code $\mathcal{C}$, then its elements define polynomials $a(t) \in \mathbb{F}_q[t;\sigma] = K[t;\sigma]$. These form a left ideal $\mathcal{C}(t)$ of S_f with $f = t^m - d \in \mathbb{F}_q[t;\sigma]$: The code is linear and so the skew-polynomial representation $\mathcal{C}(t)$ is an additive group. For $(a_0, \dots, a_{m-1}) \in \mathcal{C}$,

$$ta(t) = \sigma(a_0)t + \sigma(a_1)t^2 + \cdots + \sigma(a_{m-1})t^m$$

and since $f = t^m - d$ we get in $S_f = R/Rf$ that

$$ta(t) = \sigma(a_{m-1})d + \sigma(a_0)t + \sigma(a_1)t^2 + \cdots + \sigma(a_{m-2})t^{m-1}.$$

Since $\mathcal{C}$ is σ-constacyclic with constant d, $ta(t) \in \mathcal{C}(t)$. Clearly, by iterating this argument, also $t^s a(t) \in \mathcal{C}(t)$ for all $s \le m-1$. By iteration and linearity of $\mathcal{C}$, thus $h(t)a(t) \in \mathcal{C}(t)$ for all $h(t) \in R_m$, so $\mathcal{C}(t)$ is closed under multiplication and a left ideal of S_f. $\square$

Corollary 6. *Let σ be an automorphism of $K = \mathbb{F}_q$ and $\mathcal{C}$ a linear code over $\mathbb{F}_q$ of length m. Then $\mathcal{C}$ is a σ-cyclic code iff the skew-polynomial representation $\mathcal{C}(t)$ with elements $a(t)$ obtained from $(a_0, \dots, a_{m-1}) \in \mathcal{C}$ is a left ideal of S_f generated by a monic right divisor g of $f = t^m - 1 \in R = \mathbb{F}_q[t;\sigma]$.*

Remark 7. Let $f(t) \in R = K[t;\sigma]$ and $F = \mathrm{Fix}(\sigma)$. Let $f = t^m - d$. Then f is a two-sided element (thus S_f associative and f reducible) iff m divides the order n of σ and $d \in F$. For $d = 1$ in particular, f is two-sided iff m divides the order n of σ.

When f is not two-sided anymore, it can happen that f is irreducible in $K[t;\sigma]$, hence does not have any non-trivial right divisors g. Any right divisor g of degree k of, for instance, $f = t^m - d$ can be used to construct a σ-constacyclic $[m, m-k]$-code (with constant d). We note:

(i) $f(t) = t^3 - d$ is reducible in R if and only if

$$\sigma(z)^2\sigma(z)z = d \text{ or } \sigma(z)^2\sigma(z)z = d$$

for some $z \in K$ [10, (18)] . (Thus $t^3 - 1$ is always reducible in $K[t;\sigma]$.)

(ii) Suppose m is prime and F contains a primitive mth root of unity. Then $f(t) = t^m - d$ is reducible in R if and only if

$$d = \sigma^{m-1}(z) \cdots \sigma(z)z \text{ or } \sigma^{m-1}(d) = \sigma^{m-1}(z) \cdots \sigma(z)z$$

for some $z \in K$ [10, (19)]. (Thus $t^m - 1$ is always reducible in $K[t;\sigma]$, if F contains a primitive mth root of unity.)

(iii) Let K/F have degree m, $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ and $R = K[t;\sigma]$, $f = t^m - d$ with $d \notin F$.

(a) If the elements $1, d, \dots, d^m$ are linearly dependent over F, then f is reducible.

(b) If m is prime then f is irreducible [13] and thus there are no σ-constacyclic codes with constant d apart from the $[m, m]$-code associated with S_f itself.

We note that when working over finite fields, the division algebras S_f are finite semifields which are closely related to the semifields constructed by Johnson and Jha [8] obtained by employing semi-linear transformations. Results for these semifields and their spreads might be useful for future linear code constructions.

References

[1] D. Boucher, F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Des. Codes Cryptogr. 70 (2014), no. 3, 405431.

[2] D. Boucher, F. Ulmer, *Self-dual skew codes and factorization of skew polynomials*, J. Symbolic Comput. 60 (2014), 4761.

[3] D. Boucher, F. Ulmer, *Codes as modules over skew polynomial rings. Cryptography and coding*, 3855, Lecture Notes in Comput. Sci., 5921, Springer, Berlin, 2009.

[4] D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. 44 (2009), no. 12, 1644-1656.

[5] D. Boucher, W. Geiselmann, F. Ulmer, *Skew-cyclic codes*, AAECC (18) (2007), 370-389.

[6] M. Boulagouaz, A. Leroy, (σ, δ)*-codes,* Adv. Math. Commun. 7 (4) (2013), 463474.

[7] N. Jacobson, "Finite-dimensional division algebras over fields," Springer Verlag, Berlin-Heidelberg-New York, 1996.

[8] V. Jha, N. L. Johnson, emphAn analogue of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem, Algebras, Group, Geom. 6 (1) (1989), 1- 35.

[9] M. Lavrauw, J. Sheekey, *Semifields from skew-polynomial rings*, Adv. Geom. 13 (4) (2013), 583-604.

[10] J.-C. Petit, *Sur certains quasi-corps généralisant un type d'anneau-quotient*, Séminaire Dubriel. Algèbre et théorie des nombres 20 (1966 - 67), 1-18.

[11] J.-C. Petit, *Sur les quasi-corps distributifes à base momogène*, C. R. Acad. Sc. Paris 266 (1968), Série A, 402-404.

[12] R.D. Schafer, "An Introduction to Nonassociative Algebras," Dover Publ., Inc., New York, 1995.

[13] A. Steele, " Nonassociative cyclic algebras," to appear in Israel J. Math., available at `http://molle.fernuni-hagen.de/~loos/jordan/archive/nonassoc_cyclic/index.html`.

E-mail address: `susanne.pumpluen@nottingham.ac.uk`

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom