On skew constacyclic codes and their surprising connection to nonassociative algebra

S. Pumplün, University of Nottingham

University of Ottawa, September 2025

Content:

Linear Codes

Let K be a field, $n > 1$ an integer. A *linear code C of length n over K* is a free sub vector space of K^n.

If for all $(c_0, \ldots, c_{n-1}) \in C$, also $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$, then C is called a *cyclic code*.

Equivalently, a cyclic code is an ideal in the ring

$$K[t]/(t^n - 1).$$

Why?

Identify $c = (c_0, \ldots, c_{n-1}) \in C$ with the polynomial $\sum_{i=0}^{n-1} c_i t^i \in K[t]$ via the K-vector space isomorphism

$$\Phi : K^n \longrightarrow K[t]/K[t](t^n - 1) = \{c(t) \in K[t] \,|\, deg(c) < n\},$$

$$\Phi(c_0, c_1, \ldots, c_{n-1}) = c(t) = \sum_{i=0}^{n-1} c_i t^i.$$

"Cyclically shifting" a codeword $c = (c_0, \ldots, c_{n-1})$ is the same as multiplying $c(t)$ by t in $K[t]/K[t](t^n - 1)$.

Let $C(t)$ be the set of polynomials $c(t) = \sum_{i=0}^{n-1} c_i t^i$ associated to the codewords $(c_0, \ldots, c_{n-1}) \in C$ of a linear code C of length n over K.
There is a one-to-one correspondence between the cyclic codes of length n over K and the ideals of $K[t]/K[t](t^n - 1)$, because for cyclic codes, the set $C(t)$ is an ideal. More precisely:

Let $g(t)$ be a divisor of $f(t) = t^n - 1$. Then g generates a principal ideal in $K[t]/K[t](t^n - 1)$;

multiply $g(t)$ by all polynomials $h(t)$ of degree less than n to get every codeword in associatied code C; $g(t)$ is the *generator* for the cyclic code C

Example: (A cyclic Code of length 4 over $\mathbb{F}_2$)

Let $n = 4$, $K = \mathbb{F}_2$, $f(t) = t^4 - 1 = (t^2 + t + 1)^2 \in \mathbb{F}_2[t]$. Take the generator polynomial

$$g(t) = t^2 + t + 1.$$

$C(t) = \{h(t) \cdot g(t) \in \mathbb{F}_2[t]/(t^n - 1) \mid h(t) \in \mathbb{F}_2[t], \deg h < 4\}.$

This $g(t)$ produces all codewords of the cyclic code C, so that C consists of the following codewords:

$$
\begin{array}{lll}
h(t) = 0: & 0 \cdot g(t) = 0 & \Rightarrow (0,0,0,0) \in C \\
h(t) = 1: & 1 \cdot g(t) = t^2 + t + 1 & \Rightarrow (1,1,1,0) \in C \\
h(t) = t: & t \cdot g(t) = t^3 + t^2 + t & \Rightarrow (0,1,1,1) \in C \\
h(t) = t+1: & (t+1) \cdot g(t) = t^3 + 1 & \Rightarrow (1,0,0,1) \in C
\end{array}
$$

All other $h(t)$ of degree less than 4 produce the same codewords.

Each codeword is closed under the cyclic shift (move last coordinate to the first):

$$(1,1,1,0) \to (0,1,1,1), \quad (0,1,1,1) \to (1,0,1,1), \ldots$$

Generalizations of cyclic codes Let $a \in K^{\times}$. A linear code $C \subset K^n$ is *constacyclic*,

if for each $(c_0, c_1, \ldots, c_{n-1}) \in C$, also $(ac_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.
Equivalently, we view a constacyclic code as an ideal in

$$K[t]/(t^n - a).$$

Note: $t^n - a$ needs to be reducible in order to get non-trivial ideals in $K[t]/(t^n - a)$.

Now let $\sigma \in \mathrm{Aut}(K)$. A linear code $C \subset K^n$ is a *skew* (σ, a)*-constacyclic code*, if for each $(c_0, c_1, \ldots, c_{n-1}) \in C$, also

$$(a\sigma(c_{n-1}), \sigma(c_0), \sigma(c_1), \ldots, \sigma(c_{n-2})) \in C.$$

Equivalently, a skew (σ, a)-constacyclic code is an left principal ideal $K[t;\sigma]g$ in the nonassociative ring

$$K[t;\sigma]/(t^n - a)$$

with generator polynomial $g(t)$, where g right divides f.

II. Skew-polynomial rings

The *skew-polynomial ring* $R = K[t;\sigma]$ is the set of polynomials

$$f(t) = \sum_{i=0}^{n} a_i t^i$$

with the usual term-wise addition. Multiplication given by

$$ta = \sigma(a)t + \delta(a) \text{ for all } a \in K.$$

R is an associative noncommutative unital ring, and $K[t] = K[t; id]$.

For $f(t) = \sum_{i=0}^{n} a_i t^i \in R$ with $a_n \neq 0$, we define the *degree* of f as $\deg(f) = n$ and put $\deg(0) = -\infty$.

$f(t)$ is called *irreducible*, if there do not exist $g, h \in R$ with $0 < \deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

Let $f = f_1 \cdots f_r \in R$ be a decomposition of f into irreducible polynomials. Then the irreducible factors $f_1, \ldots, f_r$ are uniquely determined up to order and similarity.

Example: Let $K = \mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$ with $\alpha^3 + \alpha + 1 = 0$, $\sigma : K \to K$, $\sigma(x) = x^2$, the Frobenius automorphism. Take $f(t) = t^3 - 1 \in K[t;\sigma]$. In $K[t]$,

$$f(t) = (t-1)(t-\alpha)(t-\alpha^2).$$

In $K[t;\sigma]$,

$$f(t) = (t-1)(t-1)(t-1) = (t-1)(t-\alpha)(t-\alpha^2) = (t-\alpha^2)(t-\alpha^4)(t-1)$$

$=$ ... etc.

III. The Petit algebras $K[t;\sigma,\delta]/K[t;\sigma](t^n-a)$

Let $f \in R = S[t;\sigma,\delta]$ be monic of degree $n \geq 2$. For all $g \in R$ there exist unique $r, q \in R$ with $\deg(r) < \deg(f)$, such that

$$g = qf + r.$$

The skew polynomials of degree less that n canonically represent the elements of the left R-module R/Rf.

$$R/Rf = \{g \in R \,|\, \deg(g) < n\}.$$

1. case: Rf is a two-sided ideal in R

$\Rightarrow R/Rf$ is an associative quotient ring with multiplication $gh = gh \,\mathrm{mod}_r f$ (the "classical case").
2. case: Rf is not a two-sided ideal in R
$\Rightarrow R/Rf$ with multiplication $gh = gh \,\mathrm{mod}_r f$ is a nonassociative unital ring (Petit 1966). Here, $\mathrm{mod}_r f$ on the r.h.s. denotes the remainder r.

Theorem (P. 2017) There is a one-to-one correspondence between principal left ideals of $R/R(t^n - a)$ and skew (σ, a)-constacyclic codes of length n over K.

More precisely: Let g be a monic right divisor of $f(t) = t^n - a$. Then g generates a principal left ideal in the nonassociative algebra R/Rf.

The set of vectors corresponding to the elements

$$\{g, tg, \dots, t^{k-1}g\} \subset R/R(t^n - a)$$

forms a basis of the code C and the dimension of C is $k = n - \text{deg}(g)$. This means g is a generator of C.

The matrix generating C represents the right multiplication with g in the nonasssociative Petit algebra $R/R(t^n - a)$.

IV. Hamming weight preserving isomorphisms

The three main parameters for a linear code C are

- its length n;
- its dimension k (of the sub vector space C in K^n, in this talk $k = n - deg(g)$);
- its minimum Hamming distance d: the Hamming distance of c and c' in C is the number of components where c and c' differ.

The *Hamming weight* of $(c_0, c_1, \dots, c_{n-1}) \in C$ is the number of nonzero components c_i.

We are interested in the ring isomorphisms G between $R/R(t^n - a)$ and $R/R(t^n - b)$ that preserve the Hamming weight (called *isometries*):

$$K[t;\sigma]/K[t;\sigma](t^n - a) \xrightarrow{\text{isometry } G} K[t;\sigma]/K[t;\sigma](t^n - b)$$

$$K[t;\sigma]g(t) \xrightarrow{1\text{–}1} S[t;\sigma]G(g(t))$$

$$\text{codes generated by } g(t) \xrightarrow{1\text{–}1} \text{codes generated by } G(g(t))$$

• Chen, Fan, Lin, Liu (2012) classify constacyclic codes over $\mathbb{F}_q$ using isomorphisms

$G : \mathbb{F}_q[t]/(t^n - a) \to \mathbb{F}_q[t]/(t^m - b)$ that satisfy $G|_{\mathbb{F}_q} = id$ and $G(t) = \alpha t^k$ for some integer $k > 0$ and some $\alpha \in \mathbb{F}_q^\times$.

• Boulanouar, Batoul, Boucher (2021) compute codes that are equivalent to skew cyclic and negacyclic codes using associative algebra isomorphisms $G : \mathbb{F}_q[t;\sigma]/\mathbb{F}_q[t;\sigma](t^n - a) \to \mathbb{F}_q[t;\sigma]/\mathbb{F}_q[t;\sigma](t^n - b)$ that satisfy $G|_{\mathbb{F}_q} = id$ and $G(t) = \alpha t$.

• Ou-azzou, Horlemann (2025) classify certain polycyclic codes over $\mathbb{F}_q$ using $\mathbb{F}_q$-algebra isomorphisms $G : \mathbb{F}_q[t]/(f) \to \mathbb{F}_q[t]/(h)$ that satisfy $G|_{\mathbb{F}_q} = id$ and $G(t) = \alpha t$ for some $\alpha \in \mathbb{F}_q^\times$.

• Ou-azzou, Najmeddine, Aydin (2025) and Ou-azzou, Horlemann, Aydin (2025) investigate skew constacyclic codes and skew polycyclic codes over $\mathbb{F}_q$ using nonassociative algebra isomorphisms $G : \mathbb{F}_q[t;\sigma]/\mathbb{F}_q[t;\sigma]f \to \mathbb{F}_q[t;\sigma]/\mathbb{F}_q[t;\sigma]h$ that satisfy $G|_{\mathbb{F}_q} = id$ and $G(t) = \alpha t^k$, but did not succeed in the $k > 1$ case.

Inspired by their work and our understanding of the isomorphisms of Petit algebras (Brown, Steele, Nevins, P.), we propose the following equivalence notions.

Definition Two rings $R/R(t^n - a)$ and $R/R(t^n - b)$ are called *isometric* if there exists an isomorphism $G = G_{\tau,\alpha,k} : R/R(t^n - a) \to R/R(t^n - b)$ such that $G|_K = \tau \in$ Aut(K) and $G(t) = \alpha t^k$ for some integer $k \geq 1$, and some $\alpha \in K^\times$, and *equivalent* if $k = 1$.
Note that $G_{\tau,\alpha,k}$ is Hamming weight preserving.

$G_{\tau,\alpha,k}$ is called an *isometry* or a *monomial isomorphism of degree* k. $G_{\tau,\alpha,1}$ is called an *equivalence*.
When $k=1$ we use the notation $G_{\tau,\alpha}$. We have

$$G_{\tau,\alpha}(\sum_{i=0}^{n-1} d_i t^i) = \sum_{i=0}^{n-1} \tau(d_i) N_i^\sigma(\alpha) t^i,$$

where $N_i^\sigma(\alpha) = \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha)$.

When Aut(K) is abelian, σ has finite order m, $m \geq n-1$ and $t^n - a$ is not two-sided, then all Hamming weight preserving isomorphisms between $R/R(t^n-a)$ and $R/R(t^n-b)$ will be monomial of degree one (Brown-P. 2018, P. 2025).

Let $\mathbf{C}_a$ be the class of all skew (σ, a)-constacyclic codes and $\mathbf{C}_b$ the class of all skew (σ, b)-constacyclic codes.

Definition $\mathbf{C}_a$ and $\mathbf{C}_b$ are called *isometric*, if there exists an isometry $G_{\tau,\alpha,k} : R/R(t^n - a) \to R/R(t^n - b)$, and *Chen-isometric*, if $\tau = id$;
$\mathbf{C}_a$ and $\mathbf{C}_b$ are called *equivalent*, if there exists an equivalence $G_{\tau,\alpha} : R/R(t^n - a) \to R/R(t^n - b)$, and *Chen-equivalent*, if $\tau = id$.

From now on let K/F be a cyclic Galois extension of degree m, $\mathrm{Gal}(K/F) = \langle \sigma \rangle$.

Theorem (P. 2025) (i) The classes $\mathbf{C}_a$ and $\mathbf{C}_b$ are equivalent if and only if there exists $\tau \in \mathrm{Aut}(K)$ that commutes with σ and $\alpha \in K^\times$, such that

$$\tau(a) = N_n^\sigma(\alpha) b$$

(resp., Chen-equivalent iff this is true with $\tau = id$).
(ii) Let $m \geq n-1$ and assume that $t^n - a$ does not generate a two-sided ideal in $K[t;\sigma]$. Then $\mathbf{C}_a$ and $\mathbf{C}_b$ are isometric if and only if they are equivalent.

V. Equivalent and isometric skew constacyclic codes (Nevins-P. 2025)

Theorem (i) The Hamming weight preserving homomorphisms between two proper nonassociative algebras $K[t;\sigma]/K[t;\sigma](t^n - a)$ and $K[t;\sigma]/K[t;\sigma](t^n - b)$ all have the form $G_{\tau,\alpha}$ for some $\tau \in \mathrm{Aut}(K)$ commuting with σ, and some $\alpha \in K^{\times}$.
(ii) Non monomial homomorphisms between proper nonassociative algebras $K[t;\sigma]/K[t;\sigma](t^n - a)$ and

$K[t;\sigma]/K[t;\sigma](t^n - b)$ do not occur, subject to a technical hypothesis.
(iii) Let $m \nmid n$. If $G : K[t;\sigma]/K[t;\sigma](t^n - a) \to K[t;\sigma]/K[t;\sigma](t^n - b)$ is a nonzero homomorphism whose restriction to K is given by some $\tau \in \mathrm{Aut}(K)$ commuting with σ, then $G = G_{\tau,\alpha}$.

Remark - Homomorphisms have not been investigated so far, only isomorphisms.
- (ii), (iii) will help us parametrize the division algebras $K[t;\sigma]/K[t;\sigma](t^m - a)$, too (Nevins-P., work in progress, 2025), we only did the case $n = m$ (Nevins-P. J. Algebra, 2025).

Theorem Suppose that all $\tau \in \mathrm{Aut}(K)$ commute with σ. Suppose $m \nmid n$, or that one of a or b is not in F.

The classes $\mathbf{C}_a$ and $\mathbf{C}_b$ of skew constacyclic codes of length n are isometric iff they are equivalent.

Proposition The class of skew (σ, a)-constacyclic codes and the class of skew constacyclic (i.e., $(\sigma, 1)$-constacyclic) codes of length n are equivalent iff $a \in N_n^\sigma(K^\times)$. For skew constacyclic codes, isometry and equivalence coincide when n does not divide m.

The class of skew (σ, a)-constacyclic codes and the class of skew negacyclic (i.e., $(\sigma, -1)$-constacyclic) codes of length n are equivalent iff $-a \in N_n^\sigma(K^\times)$. For skew σ-negacyclic codes of length n, isometry and equivalence coincide when n does not divide m.

Theorem Let $K = \mathbb{F}_{p^r}$ and $\sigma(x) = x^{p^s}$ with $s|r$ so that $m = r/s$ and $F = \mathbb{F}_{p^s}$ is the fixed field of σ. Define

$$[n]_s = \frac{p^{sn} - 1}{p^s - 1} = p^{s(n-1)} + p^{s(n-2)} + \cdots + p^s + 1.$$

The number of different Chen-isometry classes of skew (σ, a)-constacyclic codes of length n arising from nonassociative algebras is N where

$$N = \begin{cases} \gcd([n]_s, p^r - 1) & \text{if } m \nmid n; \text{ and} \\ \left(1 - \frac{1}{[m]_s}\right) \gcd([n]_s, p^r - 1) & \text{if } m|n. \end{cases}$$

There are additionally $\gcd([n]_s, p^r - 1)/[m]_s$ different Chen-equivalence classes (and thus at most this many Chen-isometry classes) of families of skew (σ, a)-constacyclic codes with associative ambient algebras, for which $m \mid n$ and $a \in F^\times$.

Example Let gcd$([n]_s, p^r - 1) = p^r - 1$ then $N_n^\sigma(\mathbb{F}_q^\times) = \{1\}$ and so no $\mathbf{C}_a$ and $\mathbf{C}_b$ for two distinct $a, b \in \mathbb{F}_q^\times$ will be Chen-equivalent. Thus, there are many distinct classes of skew constacyclic codes up to Chen-equivalence.

There are r choices for $\tau \in$ Gal$(\mathbb{F}_{p^r}/\mathbb{F}_p)$ and so $\{a^{p^v} \mid 0 \leq v < r\} \subset \mathbb{F}_{q^r}$ is an equivalence class with r elements $\Rightarrow$ the corresponding (σ, a^{p^v})-constacyclic codes are Chen-equivalent $\Rightarrow$ there are fewer equivalence classes than Chen equivalence classes.

Example Let l be prime, $K = \mathbb{F}_{p^{l^2}}$, $F = \mathbb{F}_{p^l}$. We obtain a total of only

$$\frac{p^{l^2} - p^l}{l^2} + \frac{p^l - p}{l} + p - 1$$

equivalence classes of skew constacyclic codes of length n, compared with a total of

$$p^{l^2} - 1 = (p^{l^2} - p^l) + (p^l - p) + (p - 1)$$

equivalence classes with respect to Chen equivalence.

VI. Outlook: skew polycyclic codes

Let $f(t) = t^n - \sum_{i=0}^{n-1} a_i t^i \in S[t;\sigma]$ be a reducible monic polynomial of degree n.

A linear code $C \subset S^n$ is a *(right) skew* (f,σ)*-polycyclic code* if for each codeword $(c_0, c_1, \dots, c_{n-1})$ of C, also

$(0, \sigma(c_0), \sigma(c_1), \dots, \sigma(c_{n-2})) + \sigma(c_{n-1})(a_0, a_1, \dots, a_{n-1}) \in C$.

A skew (f,σ)-polycyclic code $C \subset K^n$ is a subset of K^n consisting of the vectors $(c_0, \dots, c_{n-1})$ obtained from all the elements $h = \sum_{i=0}^{n-1} c_i t^i$ in a left principal ideal $g\,R/Rf$ of R/Rf, where g is monic.

For $\sigma = id$, we obtain *polycyclic codes* where $f(t) \in K[t]$.