*Glasgow Mathematical Journal* (2023), **65**, pp. 480–500
doi:10.1017/S001708952300006X

Glasgow Mathematical Journal

RESEARCH ARTICLE

# Division algebras and MRD codes from skew polynomials

D. Thompson[1] and S. Pumplün[2]

[1]28 Coral Lane Newhall Swadlincote DE11 0XU, United Kingdom
[2]School of Mathematical Sciences, University of Nottingham University Park, Nottingham NG7 2RD, United Kingdom
E-mails: thompson.danjames@gmail.com, susanne.pumpluen@nottingham.ac.uk

**Received:** 22 June 2021; **Revised:** 3 February 2023; **Accepted:** 27 February 2023; **First published online:** 20 April 2023

**Keywords:** skew polynomial ring, skew polynomials, division algebras, MRD codes

**2020 Mathematics Subject Classification:** *Primary* - 16S36

**Abstract**
Let $D$ be a division algebra, finite-dimensional over its center, and $R = D[t; \sigma, \delta]$ a skew polynomial ring. Using skew polynomials $f \in R$, we construct division algebras and maximum rank distance codes consisting of matrices with entries in a noncommutative division algebra or field. These include Jha Johnson semifields, and the classes of classical and twisted Gabidulin codes constructed by Sheekey.

## 1. Introduction

Rank distance codes are important both in coding theory and cryptography. One of the best-known maximum rank distance (MRD) codes is probably the Gabidulin code [10] which was mentioned already by Delsarte [8]. In coding theory, MRD codes are well suited to correct errors [6, 31]. In cryptography, they are used to design public-key cryptosystems, see for instance [9, 12].

MRD codes over general (non-finite) fields, in particular number fields, were already studied in [2] and later touched on in [34]. Rank metric codes over both cyclic and more general Galois extensions were considered in [3, 31, 32]. Although rank metric codes have been also constructed over finite principal ideal rings [19] and discretely valued rings [21], to our knowledge they have not yet been studied over noncommutative rings. In this paper, we also consider MRD codes in $M_k(B)$, where $B$ is a noncommutative division algebra.

We construct these MRD codes using skew polynomials. Skew polynomials have been successfully used in constructions of both division algebras (mostly semifields) and linear codes [2, 4, 5, 13, 26–28], in particular building space-time block codes (STBCs) [29] and MRD codes [33, 34].

Our codes can be seen as generalizations of both the classical and twisted Gabidulin codes in [10], resp., [33]. We put Sheekey's construction [34] in a broader context which helps to understand it better and potentially allows other ways to generalize MRD coding using skew polynomials. The drawback is that rather early on we have to rigorously restrict the choice of the polynomials $f$ we can employ and that the construction remains rather theoretical.

Sheekey [34] only considers skew polynomials $f \in K[t; \sigma]$ with coefficients in cyclic Galois field extensions for his construction and limits himself to the case that the minimal central left multiple of $f$ has maximal degree. He misses out on codes (with matrix entries both in a noncommutative division algebra, and with entries in fields) and algebras that can be obtained by employing skew polynomials with coefficients in a noncommutative division algebra. He also misses out on constructions using $f \in D[t; \delta]$. We construct both new division algebras and MRD codes with entries in a noncommutative division algebra, and with entries in fields.

The first five Sections of the paper contain the preliminaries (Section 1) and theoretical background needed to obtain the main results (Sections 2–5). Let $D$ be a division algebra of degree $d$ over its center, and $f \in R = D[t; \sigma, \delta]$ a monic irreducible skew polynomial with a bound that lies in the center $C(R)$ of $R$.

While developing the theory, we point out how the choice of $D$ and the polynomial $f$ has to be restricted in order to construct both division algebras and MRD codes out of $f$, a scalar $\nu \in D$ and a suitable $\rho \in \text{Aut}(D)$.

Apart from Section 9, we fix the following general assumptions unless specified otherwise: $R = D[t; \sigma]$, where $\sigma$ is an automorphism of $D$ of finite order $n$ modulo inner automorphisms, i.e. $\sigma^n = i_u$ for some inner automorphism $i_u(z) = uzu^{-1}$, and $F = C \cap \text{Fix}(\sigma)$. Choose $\rho \in \text{Aut}(D)$, such that $F/F'$ with $F' = \text{Fix}(\rho) \cap F$ is finite-dimensional. Let $\nu \in D^\times$.

Let $f \in R$ be monic and irreducible of degree $m > 1$, and $h$ the minimal central left multiple of $f$, so that $R/Rh \cong M_k(B)$ for some division algebra $B$ (Theorem 3). Let $l < k$ be a positive integer. Define $S_{n,m,l}(\nu, \rho, f) = \{a + Rh \mid a \in P\} \subset R/Rh$ with the set $P = \{d_0 + d_1 t + \cdots + d_{lm-1} t^{lm-1} + \nu\rho(d_0)t^{lm} \mid d_i \in D\}$. Let $L_a : R/Rf \to R/Rf$ be the left multiplication map $L_a(b + Rf) = ab + Rf$. We have well-defined maps $S_{n,m,l}(\nu, \rho, f) \longrightarrow \text{End}_B(R/Rf) \longrightarrow M_k(B), a \mapsto L_a \mapsto M_a$, where $M_a$ is the matrix representing $L_a$ with respect to a right $B$-basis of $R/Rf$. The image $\mathcal{C}_{n,m,l} = \{M_a \mid a \in S_{n,m,l}(\nu, \rho, f)\}$ of $S_{n,m,l}(\nu, \rho, h)$ in $M_k(B)$ is an $F'$-linear rank metric code. If $\mathcal{C}_{n,m,l}$ has distance $d_{\mathcal{C}} = k - l + 1$, then $\mathcal{C}_{n,m,l}$ is called a *maximum rank distance code* in $M_k(B)$. We will usually deal with the case that $deg(h) = dmn$, so that $B$ is a field.

The most general results are contained in Section 6: If $P$ does not contain a polynomial of degree $lm$, whose irreducible factors are all similar to $f$, then $\mathcal{C}_{n,m,l}$ is an $F'$-linear MRD code in $M_k(B)$ with minimum distance $k - l + 1$ (Theorem 19).

Furthermore, let $D = (E/C, \gamma, a)$ be a cyclic division algebra such that $\sigma|_E \in \text{Aut}(E)$ and $\gamma \circ \sigma|_E = \sigma|_E \circ \gamma$, and $\sigma^n(z) = u^{-1}zu$ for some $u \in E$. Let $f(t) = \sum_{i=0}^m a_i t^i \in E[t; \sigma]$ be a monic irreducible polynomial of degree $m$, such that $\deg(h) = dmn$, and such that all monic $f_i$ similar to $f$ lie in $E[t; \sigma]$. Then, the algebra $S_{n,m,1}(\nu, \rho, f)$ is a division algebra, if one of the following holds: (i) $\nu \notin E$ and $\rho|_E \in \text{Aut}(E)$; (ii) $\nu \in E^\times$ and $\rho|_E \in \text{Aut}(E)$, such that $N_{E/F'}(a_0)N_{E/F'}(\nu) \neq 1$ (Theorem 16). MRD codes are canonically obtained from the matrices representing the left multiplication of these division algebras.

In Section 7, the nuclei of the algebras and codes are investigated. We give some examples of algebras obtained from our construction employing $f(t) = t^n - \theta \in K[t; \sigma]$ in Section 8.

We conclude with a brief look at the constructions using a differential polynomial $f \in D[t; \delta]$, where the center of $D$ is a field of characteristic $p$, in Section 9.

The fact that we are using $f \in D[t; \sigma]$, respectively $f \in D[t; \gamma]$, means we have a larger choice of skew polynomials to build codes that Sheekey does, who only considers $f$ with coefficients in a cyclic field extension.

This work is part of the second author's PhD thesis [35].

## 2. Preliminaries

### *2.1. Nonassociative algebras*

Let $F$ be a field. 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. A nonassociative 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. If $A$ is finite-dimensional as an $F$-vector space, then $A$ is a division algebra if and only if $A$ has no zero divisors. The *left nucleus* of $A$ is defined as $\text{Nuc}_l(A) = \{x \in A \mid [x, A, A] = 0\}$, the *middle nucleus* of $A$ is $\text{Nuc}_m(A) = \{x \in A \mid [A, x, A] = 0\}$, and the *right nucleus* of $A$ is $\text{Nuc}_r(A) = \{x \in A \mid [A, A, x] = 0\}$, where $[x, y, z] = (xy)z - x(yz)$ is the *associator*. $\text{Nuc}_l(A)$, $\text{Nuc}_m(A)$, and $\text{Nuc}_r(A)$ are associative subalgebras of $A$. Their intersection $\text{Nuc}(A) = \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of $A$. $\text{Nuc}(A)$ is an associative subalgebra of $A$, and $x(yz) = (xy)z$ whenever one of the elements $x, y, z$ is in $\text{Nuc}(A)$. The *center* of $A$ is $\text{C}(A) = \{x \in \text{Nuc}(A) \mid xy = yx \text{ for all } y \in A\}$.

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

Let $A$ be a finite-dimensional central simple associative algebra over $F$ of degree $d$ and let $\overline{F}$ denote the algebraic closure of $F$. Then, $A \otimes_F \overline{F} \cong M_d(\overline{F})$, so that we can fix an embedding $A \longrightarrow M_d(\overline{F})$ and view every $a \in A$ as a matrix in $M_d(\overline{F})$. The characteristic polynomial

$$m_a(X) = X^d - s_1(a)X^{d-1} + s_2(a)X^{d-2} - \cdots + (-1)^d s_d(a),$$

of $a \in A$ has coefficients in $F$ and is independent of the choice of the embedding. The coefficient $N_A(a) = s_d(a)$ is called the *reduced norm of a* [20]. Let $K/F$ be a cyclic Galois extension of degree $d$ with Galois group $\mathrm{Gal}(K/F) = \langle \gamma \rangle$ and norm $N_{K/F}$. Let $c \in F^\times$. An *associative cyclic algebra* $(K/F, \gamma, c)$ of degree $d$ over $F$ is a $d$-dimensional $K$-vector space

$$(K/F, \gamma, c) = K \oplus eK \oplus e^2K \oplus \cdots \oplus e^{d-1}K,$$

with multiplication given by the relations $e^d = c,\ le = e\sigma(l)$, for all $l \in K$. $(K/F, \gamma, c)$ is a division algebra for all $c \in F^\times$, such that $c^s \notin N_{K/F}(K^\times)$ for all $s$ which are prime divisors of $d$, $1 \le s \le d-1$.

### 2.2. MRD codes

Let $K$ be a field. A *code* is a set of matrices $\mathcal{C} \subset M_{n,m}(K)$. Let $L \subset K$ be a subfield, then $\mathcal{C}$ is *L-linear* if $\mathcal{C}$ is a vector space over $L$. A *rank metric code* is a code $\mathcal{C} \subset M_{n,m}(K)$ equipped with the rank distance function $d(X, Y) = \mathrm{rank}(X - Y)$. Define the *minimum distance* of a rank metric code $\mathcal{C}$ as

$$d_{\mathcal{C}} = \min\{d(X, Y) \mid X, Y \in \mathcal{C}, X \neq Y\}.$$

An $L$-linear rank metric code $\mathcal{C}$ satisfies the Singleton-like bound

$$\dim_L(\mathcal{C}) \le n(m - d_{\mathcal{C}} + 1)[K:L],$$

where $\dim_L(\mathcal{C})$ is the dimension of the $L$-vector space $\mathcal{C}$ [2, Proposition 6].

An $L$-linear rank metric code attaining the Singleton-like bound is called a *maximum rank distance code* or *MRD code* (for MRD codes over cyclic field extensions see [2]).

If now $B$ is a not necessarily commutative division algebra then more generally, we again define a *code* as a set of matrices $\mathcal{C} \subset M_{n,m}(B)$. Let $B' \subset B$ be a subalgebra, then $\mathcal{C}$ is *$B'$-linear* (or simply *linear*), if $\mathcal{C}$ is a right $B'$-module.

A *rank metric code* $\mathcal{C} \subset M_{n,m}(B)$ is a code together with the distance function

$$d(X, Y) = \mathrm{colrank}(X - Y),$$

for all $X, Y \in M_{n,m}(B)$, where colrank is the column rank of $A$ (the rank of the right $B$-module generated by the columns of $A$). A matrix in $M_{n,m}(B)$ has column rank at most $m$; any matrix which attains this bound is said to have attained *full column rank*. The *minimum distance* of a rank metric code $\mathcal{C} \subset M_{n,m}(B)$ is defined as

$$d_{\mathcal{C}} = \min\{d(X, Y) \mid X, Y \in \mathcal{C}, X \neq Y\}.$$

To our knowledge, such codes $\mathcal{C} \subset M_{n,m}(B)$ have not previously been considered in the literature.

### 2.3. Skew polynomial rings

In the following, let $D$ be a central simple division algebra of degree $d$ over its center $C$, $\sigma$ a ring endomorphism of $D$ and $\delta : D \to D$ a *left $\sigma$-derivation*, i.e. an additive map such that $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in D$. The *skew polynomial ring* $D[t; \sigma, \delta]$ is the set of skew polynomials $g(t) = a_0 + a_1t + \cdots + a_nt^n$ with $a_i \in D$, with term-wise addition and multiplication defined via $ta = \sigma(a)t + \delta(a)$ for all $a \in D$ [22]. Define $\mathrm{Fix}(\sigma) = \{a \in D \mid \sigma(a) = a\}$ and $\mathrm{Const}(\delta) = \{a \in D \mid \delta(a) = 0\}$. If $\delta = 0$, define $D[t; \sigma] = D[t; \sigma, 0]$. If $\sigma = id$, define $D[t; \delta] = D[t; id, \delta]$.

For $f(t) = a_0 + a_1t + \cdots + a_nt^n \in R = D[t; \sigma, \delta]$ with $a_n \neq 0$, we define the *degree* of $f$ as $\deg(f) = n$ and $\deg(0) = -\infty$. A skew polynomial $f \in R$ is *irreducible* if it is not a unit and it has no proper factors,

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

i.e if there do not exist $g, h \in R$ with $1 \leq \deg(g), \deg(h) < \deg(f)$ such that $f = gh$ [18, p. 2 ff.]. We call $f \in R$ *right-invariant* if $Rf$ is a left and a right ideal in $R$, and a *two-sided maximal element*, if $f$ is right-invariant and $Rf$ is a nonzero maximal ideal in $R$ (equivalently, if $f \neq 0$ and $R/Rf$ is a simple ring) [18, p. 13]. Two nonzero skew polynomials $f_1, f_2 \in R$ are *similar*, written $f_1 \sim f_2$, if $R/Rf_1 \cong R/Rf_2$ [18, p. 11].

A skew polynomial $f \in R$ is *bounded* if there exists a nonzero polynomial $f^* \in R$ such that $Rf^*$ is the largest two-sided ideal of $R$ contained in $Rf$. The polynomial $f^*$ is uniquely determined by $f$ up to scalar multiplication by elements of $D^\times$ and is called a *bound* of $f$.

If $f \in R$ has degree $m$, then for all $g \in R$ of degree $l \geq m$, there exist uniquely determined $r, q \in R$ with $\deg(r) < \deg(f)$, such that $g = qf + r$. Let $\mathrm{mod}_r f$ denote the remainder of right division by $f$. The skew polynomials $R_m = \{g \in R \mid \deg(g) < m\}$ of degree less that $m$ canonically represent the elements of the left $R$-modules $R/Rf$. Furthermore, $R_m$ together with the multiplication $g \circ h = gh \,\mathrm{mod}_r f$ is a unital nonassociative algebra $S_f = (R_m, \circ)$ over $F_0 = \{a \in D \mid ah = ha \text{ for all } h \in S_f\} = \mathrm{Comm}(S_f) \cap D$, called a *Petit algebra*. When the context is clear, we simply use juxtaposition for multiplication in $S_f$. Note that $C(D) \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta) \subset F_0$. For all $a \in D^\times$, we have $S_f = S_{af}$; thus, without loss of generality we can assume $f$ is monic when working with Petit algebras $S_f$. If $f$ has degree 1 then $S_f \cong D$.

**Lemma 1.** *Let R be a ring with no zero divisors. For all $g \in C(R)$, every right divisor of g in R also divides g on the left.*

*Proof.* Suppose $\gamma$ is a right divisor of $g$. Then, $g = \delta\gamma$ for some $\delta \in R$. As $g$ lies in the center of $R$, we have $\delta g = g\delta = \delta\gamma\delta$. This rearranges to $0 = \delta g - \delta\gamma\delta = \delta(g - \gamma\delta)$. As $R$ contains no zero divisors and $\delta \neq 0$, it follows that $g = \gamma\delta$. □

### *2.4. The minimal central left multiple of $f \in D[t; \sigma]$*

From now on let, $\sigma$ be an automorphism of $D$ of finite order $n$ modulo inner automorphisms, i.e. $\sigma^n = i_u$ for some inner automorphism $i_u(z) = uzu^{-1}$. Then, the order of $\sigma|_C$ is $n$. W.l.o.g., we choose $u \in \mathrm{Fix}(\sigma)$. Let $R = D[t; \sigma]$ and define $F = C \cap \mathrm{Fix}(\sigma)$. $R$ has center

$$C(R) = F[u^{-1}t^n] = \left\{ \sum_{i=0}^{k} a_i (u^{-1}t^n)^i \mid a_i \in F \right\} \cong F[x]$$

with $x = u^{-1}t^n$ [18, Theorem 1.1.22]. All polynomials $f \in R$ are bounded.

For any $f \in R = D[t; \sigma]$ with a bound in $C(R)$, we define the *minimal central left multiple mclm(f) of f in R* to be the unique polynomial of minimal degree $h \in C(R) = F[u^{-1}t^n]$ such that $h = gf$ for some $g \in R$, and such that $h(t) = \hat{h}(u^{-1}t^n)$ for some monic $\hat{h}(x) \in F[x]$. Define $E_{\hat{h}} = F[x]/(\hat{h}(x))$. If $f$ has nonzero constant term, then $f^* \in C(R)$ [11, Lemma 2.11]). From now on, we assume that $f$ has nonzero constant term and denote by $h \in C(R)$, $h(t) = \hat{h}(u^{-1}t^n)$, the minimal central left multiple of $f$. Then, $h$ equals the bound of $f$ up to a scalar multiple from $D$. If $f$ is irreducible in $R$, then $\hat{h}(x)$ is irreducible in $F[x]$. If $\hat{h} \in F[x]$ is irreducible, then $f = f_1 \cdots f_r$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all $i, j$ ([23], cf. [36]).

**Lemma 2.** *Let $f \in R$.*

- (i) *If $f \in R$ is irreducible, then every $g \in R$ similar to $f$ has $h$ as its minimal central left multiple.*
- (ii) *Suppose that $\hat{h} \in F[x]$ is irreducible. Then, $f = f_1 \cdots f_r$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all $i, j$.*

This follows easily from [7, p. 9, Corollary 2] and [18, Theorem 1.2.9].

The quotient algebra $R/Rh$ has center $C(R/Rh) \cong F[x]/(\hat{h}(x))$, cf. [11, Lemma 4.2]. Define $E_{\hat{h}} = F[x]/(\hat{h}(x))$. Suppose that $\hat{h}(x) \neq x$ and that $\hat{h}$ is irreducible in $F[x]$. Then, $h$ generates a maximal two-sided ideal $Rh$ in $R$ [18, p. 16] and $R/Rh$ is simple over its center $E_{\hat{h}}$.

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

**Theorem 3** [23]. *Let $f \in R = D[t;\sigma]$ be monic and irreducible of degree $m > 1$ with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$. Then,, $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree $s = dn/k$, where $k$ is the number of irreducible factors of $h$ in $R$, and*

$$R/Rh \cong M_k(\mathrm{Nuc}_r(S_f)).$$

*In particular, this means $\deg(\hat{h}) = \frac{dm}{s}$, $\deg(h) = km = \frac{dnm}{s}$, and*

$$[\mathrm{Nuc}_r(S_f) : F] = s^2 \cdot \frac{dm}{s} = dms.$$

*Moreover, $s$ divides $\gcd(dm, dn)$. If $f$ is not right-invariant, then $k > 1$ and $s \neq dn$.*

We know that $[S_f : F] = [S_f : C][C : F] = d^2m \cdot n$. Since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of $S_f$, comparing dimensions we obtain that

$$d^2mn = [S_f : F] = [S_f : \mathrm{Nuc}_r(S_f)] \cdot [\mathrm{Nuc}_r(S_f) : F] = k \cdot dms,$$

that is $[S_f : \mathrm{Nuc}_r(S_f)] = k$.

If $f$ is not right-invariant which is equivalent to $S_f$ being not associative, which in turn is equivalent to $k > 1$, then $s \neq dn$ looking at the degree of $h$. Note that $\deg(h) = dnm$ is the largest possible degree of $h$.

All of the above applies in particular to the special case that $D$ is a finite field extension $K$ of $C$ of degree $n$, and $\sigma \in \mathrm{Aut}(K)$ has order $n$. Then, $R = K[t;\sigma]$ has center $C(R) = F[t^n] = \{\sum_{i=0}^{k} a_i(t^n)^i \mid a_i \in F\} = F[x]$ where $F = \mathrm{Fix}(\sigma)$ [18, Theorem 1.1.22].

## 3. Constructing sets of matrices employing irreducible $f \in D[t;\sigma]$

Let $R = D[t;\sigma]$ be as in Section 2.3 and $f \in R$ be an irreducible monic polynomial of degree $m > 1$ with nonzero constant term and minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$. Let

$$E_f = \{z(t) + Rf \mid z(t) = \hat{z}(u^{-1}t^n) \in F[u^{-1}t^n]\} \subset R/Rf.$$

Together with the multiplication $(x + Rf) \circ (y + Rf) = (xy) + Rf$ for all $x, y \in F[u^{-1}t^n]$, $E_f$ becomes an $F$-algebra.

**Lemma 4.** *(i) For each $z(t) = \hat{z}(u^{-1}t^n) \in F[u^{-1}t^n]$ with $\hat{z} \in F[x]$, we have $z \in Rf$ if and only if $z \in Rh$. (ii) $(E_f, \circ)$ is a field isomorphic to $E_{\hat{h}}$.*

*Proof.* (i) As $h = gf$ for some $g \in R$, each $z \in Rh$ also lies in $Rf$.

Conversely, let $z(t) = \hat{z}(u^{-1}t^n) \in F[u^{-1}t^n]$ with $\hat{z} \in F[x]$ be such that $z \in Rf$. By the Euclidean division algorithm in $F[x]$, there exist unique $\hat{q}(x), \hat{r}(x) \in F[x]$ such that $\hat{z} = \hat{q}\hat{h} + \hat{r}$, where $\deg(\hat{r}) < \deg(\hat{h}) = s$ or $\hat{r} = 0$. If $\hat{r} \neq 0$, then $\hat{r} = \hat{z} - \hat{q}\hat{h}$, i.e. we found $q(t) = \hat{q}(u^{-1}t^n), r(t) = \hat{r}(u^{-1}t^n) \in F[u^{-1}t^n]$, such that $r(t) = z(t) - q(t)h(t) \in Rf$. Let $\hat{r'}(x) = r_0^{-1}\hat{r}(x) \in F[x]$, where $r_0 \in F^\times$ is the leading coefficient of $\hat{r}(x)$, then $r'(t) = \hat{r'}(u^{-1}t^n)$ is monic by definition.

As $r'(t) = \hat{r'}(u^{-1}t^n) \in Rf$, too, there exists $a(t) \in R$ such that $r'(t) = a(t)f(t)$. Thus, $r'(t) \in F[u^{-1}t^n]$ is a monic polynomial of degree less than $s$ which is right divisible by $f$. This contradicts the definition of $h$ as the minimal central left multiple of $f$. Thus, we conclude that $r = 0$ and $z = qh \in Rh$, as required. (ii) $E_f$ is a commutative associative ring with identity $1 + Rf$. Define the map $G : E_f \to E_{\hat{h}}$, $G(z + Rf) = z + Rh$ for all $z \in F[u^{-1}t^n]$. $G$ is well-defined and surjective. For all $x, y \in F[u^{-1}t^n]$, we have $G(x + Rf) + G(y + Rf) = (x + Rh) + (y + Rh) = (x + y) + Rh = G(x + y + Rf)$, $G(1 + Rf) = 1 +$

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

$Rh$, and $G(x+Rf)G(y+Rf)=(x+Rh)(y+Rh)=xy+Rh=G(xy+Rf)$, yielding that $G$ is an isomorphism. To check injectivity, we note that $G(x+Rf)=0+Rh$ if and only if $x\in Rh$. By Lemma 4 (i), this implies $x\in Rf$ and so $x+Rf=0+Rf$. □

Let $B=\mathrm{Nuc}_r(S_f)$ and $k$ be the number of irreducible factors of $h(t)$ in $R$.

**Lemma 5.** *The left $R$-module $R/Rf$ is a right $B$-module of rank $k$ via the scalar multiplication $R/Rf\times B\longrightarrow R/Rf$, $(a+Rf)(z+Rf)=az+Rf$ for all $z\in F[u^{-1}t^n]$ and $a\in R$. We can identify $R/Rf$ with $B^k$ via a canonical basis.*

*Proof.* Since the Petit algebra $S_f=R/Rf$ with its multiplication $ab=ab\,\mathrm{mod}_r f$ is a nonassociative unital algebra with right nucleus $B$, $R/Rf$ is a right $B$-module via the given scalar multiplication. As $R/Rf$ is a vector space of dimension $d^2mn$ over $F$, $R/Rf$ is free of rank $k$ over $B$. □

Let $\nu\in D^\times$ and $\rho\in\mathrm{Aut}(D)$, and define $F'=\mathrm{Fix}(\rho)\cap F$. We assume in the following that $F/F'$ is finite-dimensional. Let $s$ be the degree of $B$ over $E_{\hat h}$. We assume $f$ is not right-invariant, i.e. $k>1$.

Let $l<k=dn/s$ be a positive integer. Define the set $S_{n,m,l}(\nu,\rho,f)=\{a+Rh\mid a\in P\}\subset R/Rh$, where

$$P=\{d_0+d_1t+\cdots+d_{lm-1}t^{lm-1}+\nu\rho(d_0)t^{lm}\mid d_i\in D\}\subset D[t;\sigma].$$

$S_{n,m,l}(\nu,\rho,f)$ is a vector space over $F'$ of dimension $d^2nml[F:F']$. $R/Rf$ is a right $B$-module of rank $k$, as shown above. Let $L_a:R/Rf\to R/Rf$ be the left multiplication map $L_a(b+Rf)=ab+Rf$. Then, $L_a$ is $B$-linear, as we have $a(x\alpha)=(ax)\alpha$ for all $\alpha\in B$, $a,x\in R/Rf$, and therefore, $L_a(x\alpha)=L_a(x)\alpha$ for all $\alpha\in B$. Thus, $L_a\in\mathrm{End}_B(R/Rf)$ and

$$R/Rh\cong M_k(B)\cong\mathrm{End}_B(B^k)=\mathrm{End}_B(R/Rf)$$

by Theorem 3. Hence, we have well-defined maps

$$L:S_{n,m,l}(\nu,\rho,f)\to\mathrm{End}_B(R/Rf),\,a\mapsto L_a,$$

$$\lambda:S_{n,m,l}(\nu,\rho,f)\to M_k(B),\,a\mapsto L_a\mapsto M_a,$$

where $M_a$ is the matrix representing $L_a$ with respect to a $B$-basis of $R/Rf$. We denote the image of $S_{n,m,l}(\nu,\rho,h)$ in $M_k(B)$ by

$$\mathcal{C}_{n,m,l}=\{M_a\mid a\in S_{n,m,l}(\nu,\rho,f)\}.$$

The code $\mathcal{C}=\mathcal{C}_{n,m,l}$ is $F'$-linear by construction, and a generalized rank metric code. If $\mathcal{C}$ has minimum distance $d_{\mathcal{C}}$, the Singleton-like bound canonically generalizes to the bound

$$\dim_{F'}(\mathcal{C})\leq k(k-d_{\mathcal{C}}+1)[B:F'],$$

with $[B:F']=s[F:F']$. If $d_{\mathcal{C}}=k-l+1$, then $\dim_{F'}(S_{n,m,l}(\nu,\rho,f))=d^2nml/dms[B:F']=d^2mnl[F:F']=lk[B:F']=lkdms[F:F']$. Thus, if $d_{\mathcal{C}}=k-l+1$, then $\mathcal{C}$ attains this bound and $\mathcal{C}$ is a *maximum rank distance code* in $M_k(B)$.

We will usually deal with the case that $\deg(h)=dmn$, so that $B=E_{\hat h}$ is a field, $s=1$, and $\mathcal{C}_{n,m,l}\subset M_{dn}(E_f)$. Note that if $l=1$ and $d_{\mathcal{C}}=k$, this generalized Singleton-like bound is achieved trivially: we obtain examples of MRD codes in $M_k(B)$. This arises when we look at division algebras $S_{n,m,1}(\nu,\rho,f)$ and the matrices representing their left multiplication, cf. Remark 17 and Corollary 18.

## 4. The rank of the matrix that corresponds to the element $a+Rh$

Let $R=D[t;\sigma]$ be as in Section 3, and $f\in R$ be an irreducible monic polynomial of degree $m>1$ with minimal central left multiple $h$. Let $B=\mathrm{Nuc}_r(S_f)$. We have $\deg(\hat h)=km$ and $R/Rh\cong M_k(B)$ as $E_{\hat h}$-algebras by Theorem 3. Let $\Psi:R/Rh\to M_k(B)$, $\Psi(a+Rh)=M_a$, be this isomorphism. For $M_a\in M_k(B)$,

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

consider the right $B$-linear map $L_{M_a} : M_k(B) \to M_k(B)$, $L_{M_a} : X \mapsto M_aX$. Then, we obtain the following generalization of [34], Proposition 7 (which was only proved for $f$ with coefficients in a finite field, i.e. for the special case that $\deg(h) = nm$ is maximal):

**Theorem 6.** *Let* $\deg(h) = km$. *Then* $M_a \in M_k(B)$ *and*

$$\dim_B(\mathrm{im}(L_{M_a})) = k^2 - \frac{k}{m}\deg(\mathrm{gcrd}(a,h)), \quad \mathrm{colrank}(M_a) = k - \frac{1}{m}\deg(\mathrm{gcrd}(a,h))$$

*for all* $a + Rh \in R/Rh$. *In particular, if* $\deg(h) = dmn$, *then* $M_a \in M_n(E_{\hat{h}})$, *and*

$$\mathrm{rank}(M_a) = dn - \frac{1}{m}\deg(\mathrm{gcrd}(a(t), h(t))).$$

*Proof.* For each $M_a \in M_k(B)$, define $\mathrm{Ann}_r(M_a) = \{N \in M_k(B) \mid M_aN = 0\}$. Then, $\mathrm{Ann}_r(M_a)$ is the kernel of the endomorphism $L_{M_a} : M_k(B) \to M_k(B)$. By the Rank-Nullity Theorem for free right $B$-modules of finite rank [16, ch. IV, Cor. 2.14], it follows that

$$k^2 = \dim_B(\mathrm{im}(L_{M_a})) + \dim_B(\mathrm{Ann}_r(M_a)).$$

We conclude that $\dim_B(im(L_{M_a})) = k^2 - \dim_B(\mathrm{Ann}_r(M_a))$. Now for each $b + Rh$, $M_aM_b = 0$ if and only if $\Psi(a + Rh)\Psi(b + Rh) = 0$. As $\Psi$ is multiplicative, this is true if and only if $\Psi((a + Rh)(b + Rh)) = 0$. This means $(a + Rh)(b + Rh) = 0$. Hence, it is clear that $\mathrm{Ann}_r(M_a) \cong \mathrm{Ann}_r(a)$, where

$$\mathrm{Ann}_r(a) = \{b + Rh \in R/Rh \mid (a + Rh)(b + Rh) = 0 + Rh\},$$

so $\dim(\mathrm{Ann}_r(M_a)) = \dim(\mathrm{Ann}_r(a))$. Let $\gamma = gcrd(a,h)$ so $h = \delta\gamma$ for some $\delta \in R$. As $h \in C(R)$ and $R$ is a domain, we also have $h = \gamma\delta$ by Lemma 1. Let $b \in R$ be the unique element such that $a = b\gamma$. Then, $gcrd(b,\delta) = 1$, else $\gamma$ is not the greatest common right divisor of $a$ and $h$.Let $v \in R$. By the left Euclidean division algorithm, there exist unique $u, w \in R$ such that $v = \delta u + w$ where $deg(w) < \deg(\delta)$ and $\mathrm{gcld}(w,\delta) = 1$. It follows that $av = a\delta u + aw = b\gamma\delta u + b\gamma w = bhu + b\gamma w$, and therefore, $av + Rh = b\gamma w + Rh$. Suppose $b\gamma w \equiv 0 \mathrm{mod}_r h$. As $gcrd(b,\delta) = 1$, there exist $c, d \in R$ such that $cb + d\delta = 1$, so $cb\gamma + d\delta\gamma = \gamma$. As $\delta\gamma = h$, this implies $cb\gamma \equiv \gamma : \mathrm{mod}_r h$. Hence, $\gamma w \equiv cb\gamma w \equiv 0 : \mathrm{mod}_r h$. However, $\deg(w) < deg(\delta)$ so $\deg(\gamma w) < \deg(\gamma\delta) = \deg(h)$; due to this, $\gamma w \equiv 0 : \mathrm{mod}_r h$ implies that $\gamma w = 0$. As $\gamma \neq 0$ and $R$ is a domain, we conclude that $w = 0$.Hence, $(a + Rh)(v + Rh) = 0 + Rh$ if and only if $v = \delta u$ where $\deg(u) < \deg(\gamma)$. As $\delta$ is uniquely defined by $a$ and $h$, every element of $\mathrm{Ann}_r(a)$ is determined by $u \in R$ such that $\deg(u) < \deg(\gamma)$. Thus,

$$\begin{aligned}\mathrm{Ann}_r(a) &= \{v + Rh \in R/Rh \mid (a + Rh)(v + Rh) = 0 + Rh\}\\ &= \{\delta u \mid u \in R, \deg(u) < deg(\gamma)\} \cong R_{deg(\gamma)} = \{g \in R \mid \deg(g) < deg(\gamma)\}.\end{aligned}$$

As $\{1, t, \ldots, t^{deg(\gamma)-1}\}$ is a $D$-basis for the free left $D$-module $R_\gamma$, it follows that $\dim_D(\mathrm{Ann}_r(a)) = \deg(\gamma)$, so $\dim_F(\mathrm{Ann}_r(a)) = \deg(\gamma)d^2n$. Since $\dim_{E_{\hat{h}}}(B) = s^2 = d^2n^2/k^2$ and $[E_{\hat{h}} : F] = km/n$, we obtain $\dim_F(B) = d^2mn/k$. Hence, we get

$$\dim_B(\mathrm{Ann}_r(a)) = \frac{\deg(\gamma)d^2nk}{d^2mn} = \frac{\deg(\gamma)k}{m},$$

and so

$$\dim_B(\mathrm{im}(L_A)) = k^2 - \dim_B(\mathrm{Ann}_r(M_a)) = k^2 - \frac{k}{m}\deg(\gamma).$$

Let $\underline{c_i}$, respectively $\underline{r_i}$, denote the columns, and rows of $M_a$ and $\underline{x_i}$ denote the columns of $X$. Computing the matrix using dot product notation, we have

$$M_aX = \begin{pmatrix} \underline{r_1}\cdot\underline{x_1} & \cdots & \underline{r_1}\cdot\underline{x_k} \\ \vdots & \ddots & \vdots \\ \underline{r_k}\cdot\underline{x_1} & \cdots & \underline{r_k}\cdot\underline{x_k} \end{pmatrix}$$

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

The $i^{th}$ column of $M_aX$ is equal to

$$\begin{pmatrix} \underline{r_1} \cdot \underline{x_i} \\ \vdots \\ \underline{r_k} \cdot \underline{x_i} \end{pmatrix} = \underline{c_1}\lambda_1 + \cdots + \underline{c_k}\lambda_k$$

for some $\lambda_j \in B$. Hence, the dimension of the right $B$-module generated by the $i^{th}$ column of $M_aX$ is exactly the column rank of $M_a$. As there are $k$ columns of $M_aX$, it follows that $\dim_B(\mathrm{im}(L_{M_a})) = k\,\mathrm{colrank}(M_a)$. □

All of the above applies in particular to the special case that $K/F$ is a field extension and $\sigma \in \mathrm{Aut}_F(K)$ of finite order $n$, $R = K[t;\sigma]$ and $C(R) = F[t^n] \cong F[x]$. Let $f \in R$ be a monic irreducible polynomial of degree $m > 1$, $B = \mathrm{Nuc}_r(S_f)$, and $h(t) = \hat{h}(t^n)$ its minimal central left multiple, $\deg(\hat{h}) = km$. Then, $\Psi : R/Rh \to M_k(B)$, $\Psi(a + Rh) = M_a$ is an $E_f$-algebra isomorphism. For each $M_a \in M_k(B)$, we have the endomorphism $L_{M_a} : M_k(B) \to M_k(B)$ by $L_{M_a} : X \mapsto M_aX$. Analogously to Theorem 6, we can prove:

**Theorem 7** (for fnite fields and thus $\deg(h) = nm$ maximal, cf. [34], Proposition 7). *Suppose that* $\deg(h) = km$, *then for all* $a + Rh \in R/Rh$ *we have*

$$\dim_B(\mathrm{im}(L_{M_a})) = k^2 - \frac{k}{m}\deg(\mathrm{gcrd}(a,h)), \quad \mathrm{colrank}(M_a) = k - \frac{1}{m}\deg(\mathrm{gcrd}(a,h)).$$

*In particular, if* $\deg(h) = mn$ *then* $M_a \in M_n(E_{\hat{h}})$ *and* $\mathrm{rank}(M_a) = n - \frac{1}{m}\deg(\mathrm{gcrd}(a,h))$.

This generalizes [34, Remark 6].

## 5. Using the norm of $D(t;\sigma)$ to investigate $f$

### *5.1. The algebra $(D(x), \widetilde{\sigma}, ux)$*

Let $C/F$ be a finite cyclic field extension of degree $n$ with $\mathrm{Gal}(C/F) = \langle\sigma\rangle$. Let $D$ be a finite-dimensional division algebra of degree $d$ with center $C$ and suppose that $\sigma$ extends to a $C$-algebra automorphism of $D$ that we call $\sigma$, too. Let $R = D[t;\sigma]$ as in Section 3. Then, there exists $u \in D^\times$ such that $\sigma^n = i_u$ and $\sigma(u) = u$. These two relations determine $u$ up to multiplication with elements from $F^\times$ [25, Lemma 19.7].

The quotient algebra $(D,\sigma,a) = D[t;\sigma]/(t^n - a)D[t;\sigma]$, where $f(t) = t^n - a \in D[t;\sigma]$ with $d \in F^\times$, is called a *generalized cyclic algebra*. The special case where $D = C$ yields the cyclic algebra $(C/F,\gamma,a)$ [18, p. 19].

Let $D(t;\sigma) = \{f/g \mid f \in D[t;\sigma], g \in C(D[t;\sigma])\}$ be the ring of central quotients of $D[t;\sigma]$. Let $\widetilde{\sigma}$ denote the extension of $\sigma$ to $D(x)$ that fixes $x$ [14, Lemma 2.1]. Then, $C(D(t;\sigma)) = \mathrm{Quot}(C(D[t;\sigma])) = F(x)$, $x = u^{-1}t^n$, is the center of $D(t;\sigma)$, where $\mathrm{Quot}(U)$ denotes the quotient field of an integral domain $U$. More precisely, $D(t;\sigma) \cong (D(x),\widetilde{\sigma},ux)$ is a generalized cyclic algebra of degree $dn$ over its center $F(x)$ and a division algebra [14, Theorems 2.2, 2.3].

Let $N$ be the reduced norm of $(D(x),\widetilde{\sigma},ux)$.

**Lemma 8.** *Let* $f \in R$. *If* $N(f)$ *is irreducible in* $F[x]$, *then* $f$ *is irreducible in* $R$.

*Proof.* If $f = gp$ for $g,p \in R$ then $N(f) = N(g)N(p)$ is reducible in $F[x]$, since both $N(g)$ and $N(p)$ lie in $F[x]$, which immediately yields the assertion. □

From now on, we assume that

$$D = (E/C,\gamma,a) \text{ is a cyclic division algebra over } C \text{ of degree } d,$$

$$\sigma|_E \in \mathrm{Aut}(E) \text{ such that } \gamma \circ \sigma = \sigma \circ \gamma \text{ and } u \in E.$$

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

Then, $\sigma|_E$ has order $n$. Write $m = kn + r$ for some $0 \leq r < n$. Let $f = \sum_{i=0}^{m} a_i t^i \in R$ be a polynomial such that $a_0 \neq 0$ and $h \in R$ be the minimal central left multiple of $f$ in $R$.

**Theorem 9** [36]. *For $f \in E[t;\sigma] \subset D[t;\sigma]$, we have*

$$N(f(t)) = N_{E/F}(a_0) + \cdots + (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m x^{dm}.$$

**Theorem 10.** *Suppose that* $\deg(h) = dmn$.

*(i)* [36, *Theorem* 14 (i)] *If $\hat{h}$ is irreducible in $F[x]$, then $f$ is irreducible in $R$.*
*(ii)* [36, *Theorem* 14 (ii)] *If $f$ is irreducible, then $N(f)$ is irreducible in $F[x]$.*
*(iii)* *If $f \in E[t;\sigma]$, then $N(f) = (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m \hat{h}$ and*

$$N_{E/F}(a_0) = (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m h_0,$$

*if $h_0$ denotes the constant term of $\hat{h}$.*

*Proof.* (iii) By Theorem 9, we have $\deg(N(f)) = dmn$ in $R$. $N(f)$ is a two-sided multiple of $f$ in $R$; therefore, the bound $f^*$ of $f$ divides $N(f)$ in $R$. Since $(f,t)_r = 1$, $f^* \in C(R)$ and therefore $f^*$ equals $h$ up to some factor in $F^\times$. Thus, $h(t) = \hat{h}(u^{-1}t^n)$ must divide $N(f)$ in $R$. Write $N(f) = g(t)h(t)$ for some $g \in R$. Comparing degrees in $R$, we obtain $\deg N(f) = \deg(g(t)) + dmn = dmn$, which implies $\deg(g) = 0$, i.e. $g(t) = a \in A^\times$. This implies that $N(f) = ah(t) = a\hat{h}(u^{-1}t^n)$. Comparing highest coefficients of $N(f)$ and $a\hat{h}$ yields that $a = (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m$ by Theorem 9, so that comparing constant terms we get that $N_{E/F}(a_0) = (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m h_0$, if $h_0$ is the constant term of $\hat{h}(x)$. □

**Theorem 11.** *Let $f \in E[t;\sigma] \subset R$ be monic and irreducible of degree $m$. Let* $\deg(\hat{h}) = dm$ *and suppose that all the monic polynomials similar to $f$ lie in $E[t;\sigma]$. If $g$ is a monic divisor of $h$ in $R$ of degree $lm$, then*

$$N_{E/F}(g_0) = N_{E/F}(a_0)^l.$$

*Proof.* We know that $h(t) = \hat{h}(u^{-1}t^n)$, with $\hat{h}(x)$ irreducible in $F[x]$, since $f$ is irreducible. Thus, $h$ is a t.s.m. element in Jacobson's terminology [18] and the irreducible factors $f_1(t), \ldots, f_k(t)$ of any decomposition of $h(t)$ are all similar and are all similar to $f$, as $f$ must be one of them by the definition of $h$. Now, $g(t)$ is a monic divisor of $h$. Thus, we can decompose $g(t)$ into a product of irreducible factors and up to similarity the irreducible factors of $g$ will be the same as suitably chosen irreducible factors of $h$ by [18, Theorem 1.2.9.]. Hence, w.l.o.g. $g = f_1 f_2 \cdots f_l$, where the $f_i$ are irreducible in $R$ and $f_i$ is similar to $f$ for all $i = 1, 2, \ldots, l$ [18, Theorem 1.2.19]. Thus by Lemma 2, the minimal central left multiple of each $f_i$ is equal to $h$. Since $f$ is monic, we may assume w.l.o.g. that all $f_i$ are monic. By Theorem 10 and since all $f_i \in E[t;\sigma]$ by our assumption, this implies that $N_{E/F}(f_i(0)) = (-1)^{dm(n-1)} N_{E/C}(u)^m h_0 = N_{E/F}(a_0)$. As the constant term of $g$ is equal to $\prod_{i=1}^{l} f_i(0)$, we see that

$$\begin{aligned} N_{E/F}(g_0) &= \prod_{i=1}^{l} N_{E/F}(f_i(0)) = [(-1)^{dm(n-1)} N_{E/C}(u)^m h_0]^l \\ &= (-1)^{ldm(n-1)} N_{E/C}(u)^{lm} h_0^l = N_{E/F}(a_0)^l. \end{aligned}$$

□

We are not able to say if the assumptions on the $f_i$'s in the above result are empty or trivial.

### 5.2. The algebra $(K(x)/F(x), \widetilde{\sigma}, x)$

Let $K/F$ be a cyclic field extension of degree $n$ with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$, $R = K[t;\sigma]$ and $x = t^n$. We now look at the cyclic algebra $(K(x)/F(x), \widetilde{\sigma}, x)$ (this case corresponds to $D = C$ in the previous Section).

Let $N$ be the reduced norm of $(K(x)/F(x), \widetilde{\sigma}, x)$ over $F(x)$ (cf. also [18, Proposition 1.4.6]). We have $\widetilde{\sigma}|_K = \sigma$, and $N$ is a nondegenerate form of degree $n$. Let $f = \sum_{i=0}^{m} a_i t^i \in R$ be a polynomial of degree $m$ such that $a_0 \neq 0$ and $h \in R$ be the minimal central left multiple of $f$ in $R$. Then $N(f(t)) = N_{K/F}(a_0) + \cdots + (-1)^{m(n-1)} N_{K/F}(a_m) x^m$ [36, Theorem 3].

**Theorem 12.** *Suppose that* $\deg(h) = mn$.

*(i)* [36, *Theorem* 6 (i)] *If* $\hat{h}$ *is irreducible in* $F[x]$, *then* $f$ *is irreducible in* $R$.
*(ii)* [36, *Theorem* 6 (ii)] *If* $f$ *is irreducible, then* $N(f)$ *is irreducible in* $F[x]$.
*(iii)* $N_{K/F}(a_0) = (-1)^{m(n-1)} h_0$, *if* $h_0$ *denotes the constant term of* $\hat{h}$.

Theorem 12 (iii) is proved analogously as Theorem 10 (iii).

**Theorem 13** (cf. [34, Theorem 5] for finite fields, the proof is the same). *Suppose that* $f$ *is not right-invariant. If* $\deg(h) = mn$ *and* $g$ *is a monic divisor of* $h(t)$ *in* $R$ *of degree* $ml$, *then*

$$N_{K/F}(g_0) = N_{K/F}(a_0)^l.$$

## 6. Division algebras and MRD codes employing $f \in R$

### *6.1. The case that* $f \in D[t;\sigma]$

Let $f \in R = D[t;\sigma]$ be a monic polynomial of degree $m$. Let $\rho \in \mathrm{Aut}(D)$, $\nu \in D$ and $F' = \mathrm{Fix}(\rho) \cap F$ where $F = C \cap \mathrm{Fix}(\sigma)$. Let $b(t), c(t) \in R_m = \{g \in R \mid \deg(g) < m\}$ and $b_0$ be the constant term of $b(t)$. Then, the multiplication defined via

$$b(t) \circ c(t) = (b(t) + \nu\rho(b_0)t^m)c(t) \ \mathrm{mod}_r f,$$

makes $R_m$ into a non-unital nonassociative ring $(R_m, \circ)$. When the context is clear, we will drop the $\circ$ notation and simply use juxtaposition. $(R_m, \circ)$ is an algebra over $F'$.

**Example 14.** *If* $f(t) = t - c \in D[t;\sigma]$ *for some* $c \in D$, $\nu \neq 0$, *then* $(R_m, \circ)$ *has the multiplication*

$$\begin{aligned} a \circ b &= (a + \nu\rho(a)t)b) \ \ \mathrm{mod}_r f \\ &= ab + \nu\rho(a)\sigma(b)t \ \ \mathrm{mod}_r f \\ &= ab + \nu\rho(a)\sigma(b)c, \end{aligned}$$

*for all* $a, b \in D$. *This generalizes the algebras studied in* [30]. *If* $R = K[t;\sigma]$ *for some finite field extension* $K/F$; *this is the multiplication of Albert's twisted semifields* [1]. *If* $F/F'$ *is finite and* $(R_m, \circ)$ *is not a division algebra,* $a \circ b = 0$ *for some nonzero* $a, b \in D$, *if and only if* $ab = -\nu\rho(a)\sigma(b)c$. *Taking norms of both sides and canceling* $N_{D/F'}(ab)$ *on both sides, we obtain that* $N_{D/F'}(-\nu c) = (-1)^{d^2 n[F:F']} N_{D/F'}(\nu c) = 1$. *Thus, if* $F/F'$ *is finite and* $N_{D/F'}(\nu c) \neq (-1)^{d^2 n[F:F']}$ *then* $(R_m, \circ)$ *is a division algebra.*

From now on for the rest of the paper, we again assume that $f$ is an irreducible monic polynomial of degree $m > 1$, $(f, t)_r = 1$, and that $h$ is the minimal central left multiple of $f$. Let $F/F'$ be finite-dimensional, and

$$P = \{d_0 + d_1 t + \cdots + d_{lm-1} t^{lm-1} + \nu\rho(d_0)t^{lm} \mid d_i \in D\} \subset D[t;\sigma].$$

**Theorem 15.** *Let* $l = 1$. *Then:*

*(i)* *Let* $b(t) \in R_m$ *with constant coefficient* $b_0$. *If* $b(t) + \nu\rho(b_0)t^m \in P$ *is reducible in* $R$, *then* $b(t)$ *is not a left zero divisor in* $(R_m, \circ)$.

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

*(ii) If $\nu = 0$, then $(R_m, \circ)$ is a division algebra over $F'$, which for $m \geq 2$ is a Petit algebra.*
*(iii) If $P$ does not contain any polynomial similar to $f$, then $(R_m, \circ)$ is a division algebra over $F'$.*

Note that $f$ may be right-invariant.

*Proof.* Suppose that there are $b(t) = b_0 + b_1 t + \cdots + b_{m-1}t^{m-1}$, $c(t) \in R_m$, such that

$$b(t) \circ c(t) = (b(t) + \nu\rho(b_0)t^m)c(t) \mathrm{mod}_r f = 0.$$

Then, there exists $g \in R_m$ such that $(b(t) + \nu\rho(b_0)t^m)c(t) = g(t)f(t)$. Since $f$ is irreducible and of degree $m$, while $deg(c) < m$, $f$ must be similar to an irreducible factor of $b(t) + \nu\rho(b_0)t^m$, because of the uniqueness of an irreducible decomposition in $R$ up to similarity. But $b(t) + \nu\rho(b_0)t^m$ has degree at most $m$, so $f$ is similar to $b(t) + \nu\rho(b_0)t^m$. Thus, $b(t) + \nu\rho(b_0)t^m$ must have degree $m$ and be irreducible as well. Hence if $b(t) + \nu\rho(b_0)t^m$ is not similar to $f$ then $b(t) + \nu\rho(b_0)t^m$ is not a left zero divisor in $(R_m, \circ)$. This happens for instance, if $\nu = 0$ or if $b(t) + \nu\rho(b_0)t^m$ is reducible. Moreover, $(R_m, \circ)$ is a division algebra if $P$ does not contain any polynomial similar to $f$. □

We are again not able to say if the assumptions on the $f_i$'s in the following result are empty or trivial.

**Theorem 16.** *Let $D = (E/C, \gamma, a)$ be a cyclic division algebra over $C$ of degree $d$ such that $\sigma|_E \in \mathrm{Aut}(E)$ and $\gamma \circ \sigma|_E = \sigma|_E \circ \gamma$. Suppose that $\sigma^n(z) = u^{-1}zu$ with $u \in E$.*

*Let $f(t) = \sum_{i=0}^m a_i t^i \in E[t;\sigma] \subset D[t;\sigma]$ be monic and irreducible, and let $\deg(h) = dmn$. Suppose that all monic $f_i$ similar to $f$ lie in $E[t;\sigma]$. Then, $(R_m, \circ)$ is a division algebra over $F'$, if one of the following holds: (i) $\nu \notin E$ and $\rho|_E \in \mathrm{Aut}(E)$. (ii) $\nu \in E^\times$ and $\rho|_E \in \mathrm{Aut}(E)$, such that*

$$N_{E/F'}(a_0)N_{E/F'}(\nu) \neq 1.$$

Note that our global assumption that $\sigma^n(z) = u^{-1}zu$ for all $z \in D$, so that $\sigma^n(e) = u^{-1}eu = e$ for all $e \in E$, forces $(\sigma|_E)^n = id$.

*Proof.* By Theorem 15, $(R_m, \circ)$ is a division algebra, if the set $P$ with $l = 1$ does not contain any polynomial similar to $f$. All polynomials similar to $f$ are irreducible factors of $h(t)$, so $(R_m, \circ)$ is a division algebra, if $P$ does not contain any irreducible factor of $h(t)$. Suppose that $P$ contains an irreducible factor $g$ of $h$ with constant term $g_0$. Then, $g$ has degree $m$ as it is similar to $f$. Let $g_m t^m$ be its highest coefficient, so that $g_m^{-1}g$ is a monic divisor of $h$.

By Theorem 10 and since $g \in E[t;\sigma]$ by assumption, this implies

$$N_{E/F}(g_0 g_m^{-1}) = (-1)^{m(n-1)}h_0 = N_{E/F}(a_0),$$

and in particular, that $g_0$ and $g_m$ are both nonzero. Since $g \in P$, we also have $g_m = \nu\rho(g_0)$. Suppose $\nu \notin E$ and $\rho(E) \subset E$. Since the coefficients of the $f_i$ all lie in $E$, we have $g_m \neq \nu\rho(g_0)$ which yields a contradiction. Hence, there is no divisor $g$ of $h$ in $P$ and $S$ is a division algebra. Suppose that $\nu \in E^\times$ and $\rho(E) \subset E$. Substituting $g_m = \nu\rho(g_0)$ into the above equation yields

$$N_{E/F}(g_0) = N_{E/F}(a_0)N_{E/F}(\nu\rho(g_0)).$$

Applying $N_{F/F'}$ to both sides implies that

$$N_{E/F'}(g_0) = N_{F/F'}(N_{E/F}(a_0))N_{E/F'}(\nu\rho(g_0)).$$

Now $N_{E/F'}(\rho(g_0)) = N_{E/F'}(g_0)$, so we can cancel the nonzero term $N_{E/F'}(g_0)$ to obtain $1 = N_{E/F'}(a_0)$ $N_{E/F'}(\nu)$. □

**Remark 17.** *Let $S = S_{n,m,1}(\nu, \rho, f) = \{a + Rh \mid a \in P\}$. We can use $\mathcal{C}(S) \subset M_k(B)$ to define a multiplication on $B^m$. As $\dim_F(D) = d^2 n$ and $\dim_F(B) = d^2 mn/k$, there exists an $F$-vector space isomorphism between $D^m$ and $B^k$. Similarly, there exists an isomorphism $G : V_f \to B^k$, $G(a + Rf) = \underline{a}$. Define $* : B^k \times B^k \to B^k$ by*

$$\underline{a} * \underline{b} = M_a \cdot \underline{b}$$

*for all* $\underline{a}, \underline{b} \in B^k$, *where* $M_a \in \mathcal{C}(S)$ *is the representation of the map* $L_{a(t)+\nu\rho(a_0)t^m} \in \mathrm{End}_B(R/Rf)$ *induced by* $G$. *(Each* $a \in R_m$ *corresponds to a map* $L_{a(t)+\nu\rho(a_0)t^m}$. *As* $\mathrm{End}_B(R/Rf) \cong M_k(B)$ *and* $\dim(R_m) = \dim(\mathcal{C}(S))$, *there is a canonical bijection between* $L_{a(t)+\nu\rho(a_0)t^m}$ *and* $M_a$.*) As* $M_a$ *represents* $L_a \in \mathrm{End}_B(R/Rf)$, $(B^k, *)$ *is isomorphic to* $R/Rf$ *equipped with the multiplication* $(a + Rf)(b + Rf) = L_{a(t)+\nu\rho(a_0)t^m}(b + Rf)$. *Thus,* $(R_m, \circ)$ *and* $(B^k, *)$ *are isomorphic algebras and* $S_{n,m,1}(\nu, \rho, f)$ *is the same algebra as* $(R_m, \circ)$.

If $l = 1$, we write $S(\nu, \rho, f) = S_{n,m,1}(\nu, \rho, f)$ for $(R_m, \circ)$. $S(\nu, \rho, f)$ is a division algebra if and only if every matrix in $\mathcal{C}_{n,m,1}$ has full column rank. It then canonically defines an $F'$-linear *MRD* code in $M_k(B)$, $B = \mathrm{Nuc}_r(S_f)$. Therefore, we obtain from all of the above results:

**Corollary 18.** *Let* $D = (E/C, \gamma, a)$ *be a cyclic division algebra over* $C$ *of degree* $d$ *such that* $\sigma|_E \in \mathrm{Aut}(E)$ *and* $\gamma \circ \sigma = \sigma \circ \gamma$. *Suppose that* $\sigma^n(z) = u^{-1}zu$ *with* $u \in E$.

*Let* $f = \sum_{i=0}^m a_i t^i \in R$ *be monic and irreducible of degree* $m$. *Then,* $B$ *is a division algebra over* $E_{\hat{h}}$ *and* $S(\nu, \rho, f)$ *defines an* $F'$*-linear MRD code in* $M_k(B)$ *with minimum distance* $k$, *if one of the following holds:*

- *(i)* $\nu = 0$. *Then,* $S(\nu, \rho, f)$ *is a (unital) Petit algebra.*
- *(ii)* $P$ *does not contain any polynomial similar to* $f$.
- *(iii) Suppose* $\rho|_E \in \mathrm{Aut}(E)$, $f = \sum_{i=0}^m a_i t^i \in E[t; \sigma] \subset R$, $\deg(h) = dmn$, *all the monic polynomials similar to* $f$ *lie in* $E[t; \sigma]$, *and one of the following holds:*
  - *(a)* $\nu \notin E$,
  - *(b)* $N_{E/F'}(\nu)N_{E/F'}(a_0) \neq 1$. *Then, we get an* $F'$*-linear MRD code in* $M_{dn}(E_{\hat{h}})$ *with minimum distance* $dn$.

The case $\nu = 0$ produces the MRD codes which are associated with the unital Petit algebras. They can be viewed as generalized Gabidulin codes.

More generally, we can also construct MRD codes for $l > 1$. Let $f \in R$ not be right-invariant, and let $l < k$ be a positive integer.

**Theorem 19.** *Suppose that* $P$ *does not contain any polynomial of degree* $lm$, *whose irreducible factors are all similar to* $f$. *Then, the set* $S_{n,m,l}(\nu, \rho, f)$ *defines an* $F'$*-linear MRD code in* $M_k(B)$ *with minimum distance* $k - l + 1$. *In particular, if* $\deg(h) = dmn$, *then this code is an* $F'$*-linear MRD code in* $M_{dn}(E_{\hat{h}})$ *with minimum distance* $dn - l + 1$.

We are not able to say if the assumption on $P$ can be satisfied in this general setup. It is satisfied in the case considered in [34, Theorem 7].

*Proof.* We have to show that the minimum column rank of the matrix corresponding to a nonzero element in $S_{n,m,l}(\nu, \rho, f)$ is $k - l + 1$. By Theorem 6, this is equivalent to finding an element $g \in A$ such that the greatest common right divisor of $g$ and $h$ has degree at most $(l - 1)m$. Suppose towards a contradiction that there exists $g \in A$ such that $\deg(\mathrm{gcrd}(g, h)) = lm$; since $\deg(g) \leq lm$, it follows that $g$ must be a divisor of $h$. As any divisor of $h$ is a product of irreducible polynomials similar to $f$, $g$ must be a product of polynomials similar to $f$. This contradicts our assumption, so any matrix has rank at least $k - l + 1$. □

**Theorem 20** (for $f \in K[t; \sigma]$, $K$ a finite field, this is [34, Theorem 7]). *Let* $f = \sum_{i=0}^m a_i t^i \in E[t; \sigma] \subset R = D[t; \sigma]$ *be monic irreducible, and let* $\deg(h) = dmn$. *Suppose that all monic* $f_i$ *similar to* $f$ *lie in* $E[t; \sigma]$. *Then,* $S_{n,m,l}(\nu, \rho, f)$ *defines an* $F'$*-linear MRD code in* $M_{dn}(E_{\hat{h}})$ *with minimum distance* $dn - l + 1$, *if one of the following holds:*

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

*(i)* $\nu = 0$
*(ii)* $\nu \notin E$ *and* $\rho|_E \in \mathrm{Aut}(E)$.
*(iii)* $\nu \in E$, $\rho|_E \in \mathrm{Aut}(E)$ *and* $N_{E/F'}(\nu)N_{E/F'}(a_0)^l \neq 1$.

The proof is straightforward.

### 6.2. The case $R = K[t;\sigma]$

Let $f = \sum_{i=0}^{m} a_i t^i \in R = K[t;\sigma]$ be an irreducible monic polynomial of degree $m$ with minimal central left multiple $h$. Suppose throughout this section that $F/F'$ is a finite field extension, $\nu \in K$, and $\rho \in \mathrm{Aut}(K)$. Let $1 < l < k$ and $S_{n,m,l}(\nu,\rho,f) = \{a + Rh \mid a \in P\} \subset R/Rh$, where $P = \{d_0 + d_1 t + \cdots + d_{lm-1}t^{lm-1} + \nu\rho(d_0)t^{lm} \mid d_i \in K\}$. Then, we obtain the following results:

**Theorem 21.** *Let* $l = 1$.

*(i) Let* $b(t) \in R_m$ *with constant coefficient* $b_0$. *If* $b(t) + \nu\rho(b_0)t^m \in P$ *is reducible in R, then* $b(t)$ *is not a left zero divisor in* $S(\nu,\rho,f)$.
*(ii) If* $\nu = 0$, *then* $S(\nu,\rho,f)$ *is a division algebra over* $F'$, *a unital Petit algebra.*
*(iii) If P does not contain any polynomial similar to f, then* $S(\nu,\rho,f)$ *is a division algebra over* $F'$.

The proof is analogous to the one of Theorem 15. Note that $f$ may be right-invariant here. Using Theorems 10 and 13, we obtain (for finite fields, cf. [34], the proof is analogous):

**Theorem 22.** *Suppose that* $\deg(h) = mn$. *Then,* $S(\nu,\rho,f)$ *is a division algebra over* $F'$ *if*

$$N_{K/F'}(a_0)N_{K/F'}(\nu) \neq 1.$$

**Corollary 23.** $B = \mathrm{Nuc}_r(S_f)$ *is a division algebra and the left multiplication of the algebra* $S(\nu,\rho,f)$ *defines an* $F'$*-linear MRD code in* $M_k(B)$ *with minimum distance k, if one of the following holds:*

*(i)* $\nu = 0$.
*(ii) P does not contain any polynomial similar to f.*
*(iii)* $\deg(h) = mn$ *and* $\nu \in K$ *such that* $N_{K/F'}(\nu) \neq 1/N_{K/F'}(a_0)$. *In this case, the algebra* $S(\nu,\rho,f)$ *defines an* $F'$*-linear MRD code in* $M_n(E_{\hat{h}})$ *with minimum distance n.*

Note that the condition on $f$ in (iii) is satisfied for all $f$ if $gcd(m,n) = 1$ or if $n$ is prime.
We now look at the case that $1 < l < k$ and also assume that $f$ is not right-invariant.

**Theorem 24** (for finite fields, cf. [34, Theorem 7]). *If* $\deg(h) = mn$, *then the set* $S_{n,m,l}(\nu,\rho,f)$ *defines an* $F'$*-linear MRD code in* $M_n(E_{\hat{h}})$ *with minimum distance* $n - l + 1$ *for any* $\nu \in K$ *such that*

$$N_{K/F'}(\nu) \neq 1/N_{K/F'}(a_0)^l.$$

Note that $k = n$ here since $\deg(h) = mn$.

**Corollary 25.** *The set* $S_{n,m,l}(\nu,\rho,h)$ *defines an* $F'$*-linear MRD code in* $M_n(E_{\hat{h}})$ *with minimum distance* $n - l + 1$, *if one of the following holds:*

*(i)* $\deg(h) = mn$ *and* $\nu = 0$,
*(ii) n is prime or* $gcd(m,n) = 1$, *and* $1 \neq N_{K/F'}(\nu)N_{K/F'}(a_0)^l$
*(iii)* $\deg(h) = mn$ *and* $N_{K/F'}(\nu) \notin (F'^{\times})^l$.

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

The codes $S_{n,m,l}(0, \rho, h)$ generalize the Gabidulin codes constructed in [10] that go back to [8].

Note that $N_{K/F'}(\nu) \notin (F'^{\times})^l$ implies $N_{K/F'}(\nu) \neq N_{K/F'}(a_0)^l$ for any $f$. Thus, (ii) implies (iii) above.

**Theorem 26.** *Suppose that $P$ does not contain any polynomial of degree $lm$, whose irreducible factors are all similar to $f$. Then the set $S_{n,m,l}(\nu, \rho, f)$ defines an $F'$-linear MRD code in $M_k(B)$ with minimum distance $k - l + 1$. In particular, if $\deg(h) = mn$ then $S_{n,m,l}(\nu, \rho, f)$ defines an $F'$-linear MRD code in $M_n(E_{\hat{h}})$ with minimum distance $n - l + 1$.*

*Proof.* We have to show that the minimum column rank of the matrix corresponding to a nonzero element in $S_{n,m,l}(\nu, \rho, f)$ is $k - l + 1$. By Theorem 7, this is equivalent to finding an element $g \in P$ such that the greatest common right divisor of $g$ and $h$ has degree at most $(l-1)m$. Suppose towards a contradiction that $\deg(gcrd(g, h)) = lm$; since $\deg(g) \leq lm$, it follows that $g$ must be a divisor of $h$.

As any divisor of $h$ is a product of irreducible polynomials similar to $f$, $g$ must be a product of polynomials similar to $f$. This contradicts our assumption, so any matrix has rank at least $k - l + 1$. □

## 7. Nuclei

Let $\mathcal{M} = \mathcal{M}(A) = \{L_a \mid a \in A\} \subseteq \mathrm{End}_F(A)$ be the spread set of an $F$-algebra $A$, where $L_a$ is the left multiplication map in $A$. We define the *left* and *right idealizers* of $\mathcal{M}$ as

$$I_l(\mathcal{M}) = \{\Phi \in \mathrm{End}_F(A) \mid \Phi\mathcal{M} \subseteq \mathcal{M}\}, \text{ respectively, } I_r(\mathcal{M}) = \{\Phi \in \mathrm{End}_F(A) \mid \mathcal{M}\Phi \subseteq \mathcal{M}\}.$$

The *centralizer* of $\mathcal{M}$ is defined as $\mathrm{Cent}(\mathcal{M}) = \{\Phi \in \mathrm{End}_F(A) \mid \Phi M = M\Phi \quad \forall M \in \mathcal{M}\}$. We call $Z(\mathcal{M}) = I_l(\mathcal{M}) \cap \mathrm{Cent}(\mathcal{M})$ the *center* of $\mathcal{M}$.

**Theorem 27** (cf. [34, Proposition 5] for finite fields). *Let $A$ be a unital division algebra and $\mathcal{M}$ be the spread set of $A$. Let $\mathcal{M}^*$ be the spread set associated with the opposite algebra $A^{op}$. Then*

$$\mathrm{Nuc}_l(A) \cong I_l(\mathcal{M}), \quad \mathrm{Nuc}_m(A) \cong I_r(\mathcal{M}), \quad \mathrm{Nuc}_r(A) \cong \mathrm{Cent}(\mathcal{M}^*), \quad C(A) \cong Z(\mathcal{M}).$$

The proof from [34] holds verbatim in our general setting.

The above results can now be applied to determine the nuclei and center of the non-unital algebras $S = S_{n,m,l}(\nu, \rho, f)$.

In the following, let $R = D[t; \sigma]$. We use the assumptions on $D$, respectively $K$, and $\sigma$ from Section 6.

Let $f \in R$ be an irreducible monic polynomial of degree $m$, and let $h$ be the minimal central left multiple of $f$. We assume throughout that $f$ is not right-invariant, so that $k > 1$.

**Remark 28.** *The algebras $S_{n,m,l}(0, \rho, f)$ are unital Petit algebras and hence have left nucleus* $\mathrm{Nuc}_m(S) = D$*, and their right nucleus $\{g \in R_m \mid fg \in Rf\}$ is the eigenspace of $f$. If $S_{n,m,l}(0, \rho, f)$ is not associative, then $\{d \in D \mid dg = gd$ for all $g \in S\}$ is their center* [26].

**Theorem 29.** *Let $R = D[t; \sigma]$ and $\deg(h) = dmn$. Suppose $l \leq dn/2$, $n > 1$ and $lm > 2$. Let $S = S_{n,m,l}(\nu, \rho, f)$ and $\mathcal{M}$ be the image of $S$ in $\mathrm{End}_{E_f}(R/Rf)$, that means the corresponding rank metric code lies in $M_n(E_{\hat{h}})$. If $\nu \neq 0$, we have*

*(i)* $I_l(\mathcal{M}) \cong \{g_0 \in D \mid g_0\nu = \nu\rho(g_0)\} \subset D$ *(in particular, $I_l(\mathcal{M}) \cong \mathrm{Fix}(\rho)$ if $\nu \in C$),*
*(ii)* $I_r(\mathcal{M}) \cong \mathrm{Fix}(\rho^{-1} \circ \sigma^{lm}) \subset D$*,*
*(iii)* $\mathrm{Cent}(\mathcal{M}) \cong E_{\hat{h}}$, $Z(\mathcal{M}) \cong F'$.

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

*If* $\nu = 0$*, we have*

*(iv)* $I_l(\mathcal{M}) \cong D$*,* $I_r(\mathcal{M}) \cong D$*,*
*(v)* $\text{Cent}(\mathcal{M}) \cong E_{\hat{h}}$*,* $Z(\mathcal{M}) \cong F$*.*

Much of the proof works identically to the proof of [34, Theorem 9]. We sketch the proof to highlight the main differences in this more general case. The $lm = 2$ case has to be considered separately, and we have only been able to solve that for $F = \mathbb{R}$.

*Proof.* Let $\mathcal{M} = \{L_a \in \text{End}_{E_f}(R/Rf) \mid a \in P\}$ be the image of $S$ in $\text{End}_{E_f}(R/Rf) \subset \text{End}_F(R/Rf)$. In the following, we identify each element in $\mathcal{M}$ with the element $g \in S$ that induces it. Analogously to the proof of [34, Theorem 9], $\{g \in I_l(\mathcal{M}) \mid \deg(g) \leq lm\} = \{g_0 \in D \mid g_0\nu = \nu\rho(g_0)\}$. If $\nu = 0$, then $1 \in \mathcal{M}$ so $I_l(\mathcal{M}) \subset \mathcal{M}$ so all $g \in I_l(\mathcal{M})$ have degree at most $lm$. Consider $\nu \neq 0$. To check there are no elements $g \in I_l(\mathcal{M})$ of degree higher than $lm$, we follow the approach of [34, Theorem 9] and consider $gt \bmod \hat{h}(u^{-1}t^n)$. Recalling $\deg(h) = dm$, we have $h(t) = (u^{-1}t^n)^{dm} + \cdots = u^{-dm}(t^n + h'_{dm-1}t^{(dm-1)n} + \cdots + h'_0)$ so

$$gt \bmod h(t) = \left(\sum_{i=0}^{dmn-1} g_{i-1}t^i\right) - g_{dmn-1}u^{dm}\left(\sum_{j=0}^{dm-1} h'_j t^{nj}\right).$$

As $g \in I_l(\mathcal{M})$, this implies $gt \bmod h \in \mathcal{M}$, so for all $i \in \{lm+1, \ldots, dmn-1\}$, we have

$$g_{i-1} = \begin{cases} 0 & \text{for } i \not\equiv 0 \bmod n \\ g_{dmn-1}u^{dm}h'_{i/n} & \text{for } i \equiv 0 \bmod n \end{cases} \tag{1}$$

where $h'_{i/n} = 0$ if $i/n$ is not an integer. We will show that $g_{dmn-1} = 0$ and thus $\deg(g) \leq lm - 1$. As $lm > 2$, this follows verbatim from [34, Theorem 9].

The same holds for $I_r(\mathcal{M})$ following Sheekey's proof with the appropriate amendments made for $D[t;\sigma]$. The results for $\text{Cent}(\mathcal{M})$ and $Z(\mathcal{M})$ hold verbatim from [34, Theorem 9]. □

**Corollary 30.** *Let* $R = D[t;\sigma]$ *and* $\deg(h) = dmn$*. Suppose* $n > 1$*,* $m > 2$ *and* $S = S_{n,m,1}(\nu, \rho, f)$ *with* $\nu \neq 0$ *be a division algebra. Then,*

*(i)* $\text{Nuc}_l(S) \cong \{g_0 \in D \mid g_0\nu = \nu\rho(g_0)\} \subset D$*, so in particular* $\text{Nuc}_l(S) = \text{Fix}(\rho) \subset D$*, if* $\nu \in C$*.*
*(ii)* $\text{Nuc}_m(S) \cong \text{Fix}(\rho^{-1} \circ \sigma^m) \subset D$*.*
*(iii)* $C(S) = \text{Fix}(\rho) \cap F = F'$*.*
*(iv)* $\dim_{F'}\text{Nuc}_r(S) = \dim_{F'}(E_{\hat{h}}) = \deg(\hat{h})[F:F'] = [F:F']dm$*.*

**Theorem 31.** *Let* $R = K[t;\sigma]$ *and* $\deg(h) = mn$*. Suppose* $l \leq n/2$*,* $n > 1$ *and* $lm > 2$*. Let* $S = S_{n,m,l}(\nu, \rho, f)$ *with* $\nu \neq 0$ *and* $\mathcal{M}$ *be the image of* $S$ *in* $\text{End}_{E_f}(R/Rf)$*, so that the corresponding rank metric code lies in* $M_n(E_{\hat{h}})$*. Then,*

*(i)* $I_l(\mathcal{M}) \cong \text{Fix}(\rho) \subset K$*,* $I_r(\mathcal{M}) \cong \text{Fix}(\rho^{-1} \circ \sigma^{lm}) \subset K$*,*
*(ii)* $\text{Cent}(\mathcal{M}) \cong E_{\hat{h}}$*,* $Z(\mathcal{M}) \cong F'$*. If* $\nu = 0$*, we have*
*(iii)* $I_l(\mathcal{M}) \cong K$*,* $I_r(\mathcal{M}) \cong K$*,*
*(iv)* $\text{Cent}(\mathcal{M}) \cong E_{\hat{h}}$*,* $Z(\mathcal{M}) \cong F$*.*

Again, the proof is analogous to the one of [34], Theorem 9 (it does not use the fact that for finite fields the right nucleus of $S_f$ is $E_{\hat{h}}$, it only uses that $R/Rh$ has center $E_{\hat{h}}$).

**Corollary 32.** *Let* $R = K[t;\sigma]$ *and* $\deg(h) = mn$*. Suppose that* $n > 1$*,* $m > 2$ *and that* $S = (S(\nu, \rho, f), \circ)$ *is a division algebra with* $\nu \neq 0$*. Then,*

*(i)* $\text{Nuc}_l(S) = \text{Fix}(\rho) \subset K$*,*
*(ii)* $\text{Nuc}_m(S) = \text{Fix}(\rho^{-1} \circ \sigma^m) \subset K$*,*

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

*(iii)* $C(S) = \mathrm{Fix}(\rho) \cap F = F'$.
*(iv)* $\dim_{F'} \mathrm{Nuc}_r(S) = \dim_{F'}(E_{\hat{h}}) = \deg(\hat{h})[F : F'] = [F : F']m$.

Theorems 29, 31 and Corollaries 30, 32 generalize [34, Theorem 9, Corollary 1] which were proved for semifields.

## 8. Examples of division algebras and an MRD code when $f(t) = t^n - \theta \in K[t; \sigma]$

### 8.1. $K = F(\theta)$

Let $K = F(\theta)$ be an extension of prime degree $n$. Let $f(t) = t^n - \theta \in K[t; \sigma]$. We now compute the rank metric code associated with the $F'$-algebra $S_{n,n,1}(\nu, \rho, f)$. Note that $f(t) = t^3 - \theta \in K[t; \sigma]$ is irreducible if and only if $\theta \neq \sigma^2(z)\sigma(z)z$ for all $z \in K$. If $F$ contains a primitive $n$th root of unity, then $f(t)$ is irreducible if and only if $\theta \neq \sigma^{n-1}(z) \cdots \sigma(z)z$ for all $z \in K$.

We assume that $f$ is irreducible. Define $h(t) = (t^n - \theta)(t^n - \sigma(\theta)) \cdots (t^n - \sigma^{n-1}(\theta)) = (t^n)^n + \cdots + (-1)^n N_{K/F}(\theta)$, then $h(t) = \mathrm{mclm}(f)$: as $t^n - \sigma^i(\theta) \in K[t^n]$, the factors of $h(t)$ all commute and $h(t) \in K[t^n]$. Since $\sigma(h(t)) = (t^n - \sigma(\theta)) \cdots (t^n - \sigma^{n-1}(\theta))(t^n - \theta) = h(t)$, we know that $h(t) \in \mathrm{Fix}(\sigma)[t] = F[t]$ so $h(t) \in F[t] \cap K[t^n] = F[t^n] = C(R)$. Hence $h(t) = \hat{h}(t^n)$ with $\hat{h}(x) = x^n + (-1)^n N_{K/F}(\theta) \in F[x]$. Thus $f$ divides $h$ both from the left and the right by Lemma 1.

As $n$ is prime, the minimal central left multiple of $f$ must have degree $n$ in $F[x]$ by Theorem 3; thus, $h(t) = \mathrm{mclm}(f)$, and hence, $\hat{h}(x) = x^n + (-1)^n N_{K/F}(\theta)$ also is an irreducible polynomial in $F[x]$. As a field, $E_f = \{z + Rf \mid z \in F[t^n]\}$ is generated by $\{1 + Rf, t^n + Rf, t^{2n} + Rf, \ldots, t^{n(n-1)} + Rf\} = \{1 + Rf, \theta + Rf, \theta^2 + Rf, \ldots, \theta^{n-1} + Rf\}$ over $F$. As $K$ is generated by $\{1, \theta, \ldots, \theta^{n-1}\}$, there is a canonical isomorphism $E_f \longrightarrow K, x + Rf \mapsto x$.

It is clear that $\{1 + Rf, t + Rf, \ldots, t^{n-1} + Rf\}$ is an $E_f$-basis for $R/Rf$. Let $a = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + \nu\rho(a_0)t^n \in S(\nu, \rho, h)$. In order to determine $M_a$, we consider how $L_{a_it^i}$ acts on the basis elements of $R/Rf$. As left multiplication is distributive, i.e. $L_{a+b}(x) = L_a(x) + L_b(x)$, it follows that $L_a = \sum_{i=0}^n L_{a_it^i}$, where $a_n = \nu\rho(a_0)$. For each $i$, we have:

$$\begin{aligned}
L_{a_it^i}(1 + Rf) &= a_it^i + Rf = (t^i + Rf)(\sigma^{n-i}(a_i) + Rf)\\
L_{a_it^i}(t + Rf) &= a_it^{i+1} + Rf = (t^{i+1} + Rf)(\sigma^{n-i-1}(a_i) + Rf)\\
&\vdots \qquad\qquad \vdots\\
L_{a_it^i}(t^{n-i} + Rf) &= a_it^n + Rf = a_i\theta + Rf = (1 + Rf)(a_i\theta + Rf)\\
L_{a_it^i}(t^{n-i+1} + Rf) &= a_it^{n+1} + Rf = a_ix\theta + Rf = (t + Rf)(\sigma(a_i)\theta + Rf)\\
&\vdots \qquad\qquad \vdots\\
L_{a_it^i}(t^{n-1} + Rf) &= a_it^{i-1}\theta + Rf = (t^{i-1} + Rf)(\sigma^{n-i+1}(a_i)\theta + Rf).
\end{aligned}$$

Thus, the matrix representing $L_{a_it^i}$ is given by

$$M_{a_it^i} = \begin{pmatrix}
0 & 0 & \cdots & 0 & \sigma^{n-i}(a_i) & 0 & \cdots & 0\\
0 & 0 & \cdots & 0 & 0 & \sigma^{n-(i+1)}(a_i) & \cdots & 0\\
\vdots & & \ddots & & & & \ddots & \vdots\\
0 & & & \ddots & & & & \sigma(a_m)\\
a_i\theta & & & & & \ddots & & 0\\
0 & \sigma^{n-1}(a_i)\theta & & & & & & \\
\vdots & & \ddots & & & & \ddots & \vdots\\
0 & 0 & \cdots & \sigma^{n-(i-1)}(a_i)\theta & 0 & 0 & \cdots & 0
\end{pmatrix}.$$

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

As $M_a = \sum_{i=0}^{n} M_{a_i t^i}$, we obtain $M_a = (m_{i,j})_{i,j}$ where

$$m_{i,j} = \begin{cases} \sigma^{n+1-i}(a_0) + \sigma^{n+1-i}(\nu\rho(a_0))\theta & \text{for } i=j, \\ \sigma^{n+1-i}(a_{i-j}) & \text{for } i>j, \\ \sigma^{n+1-i}(a_{n+i-j})\theta & \text{for } i<j. \end{cases}$$

This yields $\mathcal{C}_{n,n,1} = \{M_a \mid a_k \in K \text{ for } k=0,1,\ldots,n-1\} \subset M_n(K)$ as the matrix spread set of the $n^2[F:F']$-dimensional $F'$-algebra $S_{n,n,1}(\nu,\rho,f)$. The algebra associated with this spread set is a division algebra if $N_{K/F'}(\theta)N_{K/F'}(\nu) \neq 1$ (Theorem 22). In that case, the spread set will be an MRD code. In particular, for $\nu = 0$ this condition is satisfied for any irreducible $f(t) = t^n - \theta$. This is the well known result that for irreducible $f$, the Petit algebra $S_f$ is a division algebra and so are all its isotopes. For $n > 2$ and $\nu \neq 0$, Corollary 32 yields

$$\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = \mathrm{Fix}(\rho) \subset K, \quad C(S) = F', \quad \dim_{F'} \mathrm{Nuc}_r(S) = [F:F']m.$$

### *8.2. Real division algebras of dimension 4*

Over a finite field $F$, all division algebras of dimension 4 over $F$ which have $F$ as their center and a nucleus of dimension 2 over $F$ can be constructed as algebras $S_{n,m,1}(\nu,\rho,f)$ for suitable parameters [34]. Let us now look at some real division algebras we obtain with our construction. If $\nu = 0$, then any choice of an irreducible $f \in \mathbb{C}[t;\bar{\ }]$ will yield an algebra isotopic to a real Petit division algebra. If $\nu \neq 0$, any choice of irreducible $f \in \mathbb{C}[t;\bar{\ }]$ where $N_{\mathbb{C}/\mathbb{R}}(a_0) \neq 1/N_{\mathbb{C}/\mathbb{R}}(\nu)$ also yields a division algebra (Theorem 22).

Let $b \in \mathbb{R}$ and $f(t) = t^2 - bi \in \mathbb{C}[t;\bar{\ }]$. Then, $h(t) = \hat{h}(t^2)$, $\hat{h}(x) = x^2 + b^2 \in \mathbb{R}[x]$, is the minimal central left multiple of $f$, as $h(t) = t^4 + b^2 = (t^2+bi)(t^2-bi)$. For all $b > 0$, $f(t) = t^2 - bi$ is irreducible in $\mathbb{C}[t;\bar{\ }]$.

For every irreducible $f(t) = t^2 - bi$, and $\nu \in \mathbb{C}$ such that $N_{\mathbb{C}/\mathbb{R}}(\nu) \neq \frac{1}{b^2}$, we obtain a four-dimensional real division algebra $S_{2,2,1}(\nu,\rho,f)$ and an MRD code given by its matrix spread set

$$\mathcal{C}_{2,2,1} = \left\{ \begin{pmatrix} z_0 + \nu\rho(z_0)bi & z_1 bi \\ \overline{z_1} & \overline{z_0 + \nu\rho(z_0)bi} \end{pmatrix} \mid z_0, z_1 \in \mathbb{C} \right\},$$

where $\rho$ is either the identity or the complex conjugation.

As mentioned in Theorem 7, [34, Theorem 9] uses results to deal with the case when $lm = 2$ that are valid over finite fields, but can be extended to $R = \mathbb{C}[t;\bar{\ }]$, for instance for $f(t) = t^2 - i$:

**Theorem 33.** *Let $f(t) = t^2 - i \in \mathbb{C}[t;\bar{\ }]$. Suppose $S = S_{2,2,1}(\nu,\rho,f)$ is a division algebra for some $\nu \neq 0$ and $\rho \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. Then,*

*(i)* $\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = \mathrm{Fix}(\rho)$,
*(ii)* $C(S) = \mathbb{R}$,
*(iii)* $\dim_{\mathbb{R}}(\mathrm{Nuc}_r(S)) = \dim_{\mathbb{R}}(\mathbb{R}[t^2]) = 2$.

*Proof.* We have $h(t) = t^4 + 1 \in \mathbb{R}[t^2]$. Suppose $g + Rh \in I_l(\mathcal{M})$ for some $g(t) = g_0 + g_1 t + g_2 t^2 + g_3 t^3 \in R$. Then, $ga \in S(\nu,\rho,h)$ for all $a \in S$. Direct and laborious computation yields $g_2 = 0$, $g_3 = -g_1\overline{\nu}$, and $\nu\rho(g_0 a_0 + g_1\overline{\nu a_1}) = g_0\nu\rho(a_0) + g_1\overline{a_1}$. This is satisfied for all $a_0, a_1 \in \mathbb{C}$ if and only if $\nu\rho(g_0) = g_0\nu$ and $g_1 = \nu\rho(g_1\overline{\nu})$.

If $\rho = id$, it follows that either $g_1 = 0$ or $N_{\mathbb{C}/\mathbb{R}}(\nu) = 1$; as $S$ is a division algebra, Theorem 13 (or [34, Theorem 4]) forces $g_1 = 0$ and so $g = g_0$ for some $g_0 \in \mathbb{C}$. Thus $I_l(\mathcal{M}) = \mathbb{C}$.If $\rho = \bar{\ }$, then $g_1 = \nu^2 g_1$ so either $g_1 = 0$ or $\nu = \pm 1$. As $N_{\mathbb{C}/\mathbb{R}}(\nu) \neq 1$ [34, Theorem 4], this forces $g_1 = 0$ so $g = g_0$ for some $g_0 \in \mathbb{R}$. In this case, $I_l(\mathcal{M}) = \mathbb{R}$.

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

The computations for $I_r(\mathcal{M})$ follow analogously and $\mathrm{Cent}(\mathcal{M})$ and $Z(\mathcal{M})$ follow from the proof of [34, Theorem 4]. We obtain the final result on the nuclei using Theorem 27 to relate the idealizers and centralizer of $\mathcal{M}$ to the nuclei of the algebra $S$. □

**Example 34.** *If $f(t) = t^2 - i$, we obtain division algebras $S$ for all $\nu \in \mathbb{C}$ such that $N_{\mathbb{C}/\mathbb{R}}(\nu) \neq 1$. If $\nu \neq 0$ and $S$ is a division algebra, then $C(S) = \mathbb{R}$ and $\dim_{\mathbb{R}} \mathrm{Nuc}_r(S) = 2$. Since therefore $\mathrm{Nuc}_r(S)$ is a two-dimensional division algebra over $\mathbb{R}$, $\mathrm{Nuc}_r(S)$ is an Albert isotope of $\mathbb{C}$ and can be found in the classification in [15, Theorem 1]: it must be $\mathbb{C}$, $\mathbb{C}^{(^-,^-)}$, $\mathbb{C}^{(1+L(v)^-,^-)}$, $\mathbb{C}^{(^-,1+L(v)^-)}$, or $\mathbb{C}^{(1+L(v)^-,1+L(w)^-)}$, with $u, v \in \mathbb{C}$ suitably chosen.*

*If additionally $\rho = id$, then $\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = \mathbb{C}$, and if $\rho = ^-$ then $\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = \mathbb{R}$. Note that the four-dimensional algebras in the first class are all isotopes of nonassociative quaternion algebras.*

## 9. Constructing algebras and codes using irreducible $f \in R = D[t; \delta]$

We now consider the same construction using differential polynomial rings. Let $C$ a field of characteristic $p$ and $D$ be a finite-dimensional division algebra with center $C$. Let $R = D[t; \delta]$, where $\delta$ is a derivation of $D$, such that $\delta|_C$ is algebraic with minimum polynomial $g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \cdots + c_e t \in F[t]$ of degree $p^e$, with $F = C \cap \mathrm{Const}(\delta)$. (This includes the special case where $d = 1$, that is $R = K[t; \delta]$, and $\delta$ is an algebraic derivation with minimum polynomial $g$.) Then, $g(\delta) = id_{d_0}$ is an inner derivation of $D$. W.l.o.g. we choose $d_0 \in F$, so that $\delta(d_0) = 0$ [18, Lemma 1.5.3]. Then, $C(D[t; \delta]) = F[x] = \{\sum_{i=0}^k a_i(g(t) - d_0)^i \mid a_i \in F\}$ with $x = g(t) - d_0$. The two-sided $f \in R$ are of the form $f(t) = uc(t)$ with $u \in D$ and $c(t) \in C(R)$ [18, Theorem 1.1.32]. All polynomials $f \in R$ are bounded.

For every $f \in R$, the *minimal central left multiple of $f$ in $R$* is the unique polynomial of minimal degree $h \in C(R) = F[x]$ such that $h = gf$ for some $g \in R$, and such that $h(t) = \hat{h}(g(t) - d_0)$ for some monic $\hat{h}(x) \in F[x]$. The bound $f^*$ of $f$ is the unique minimal central left multiple of $f$ up to some scalar.

From now on, let $f \in R = D[t; \delta]$ be a monic irreducible polynomial of degree $m > 1$ and let $h(t) = \hat{h}(g(t) - d_0)$ be its minimal central left multiple. Then, $\hat{h}(x)$ is irreducible in $F[x]$ and $h$ generates a maximal two-sided ideal $Rh$ in $R$ [18, p. 16]. We have

$$C(R/Rh) \cong F[x]/F[x]\hat{h}(x)$$

[17, Proposition 4], and $\deg(h) = p^e deg(\hat{h})$. Define $E_{\hat{h}} = F[x]/F[x]\hat{h}(x)$ and let $k$ be the number of irreducible factors of $h$ in $R$.

**Theorem 35** [23]. $\mathrm{Nuc}_r(S_f)$*is a central division algebra over $E_{\hat{h}}$ of degree $s = dp^e/k$, and*

$$R/Rh \cong M_k(\mathrm{Nuc}_r(S_f)).$$

*In particular, this means that* $\deg(\hat{h}) = \frac{dm}{s}$, $\deg(h) = km = \frac{dp^e m}{s}$, *and*

$$[\mathrm{Nuc}_r(S_f) : F] = s^2 \cdot \frac{dm}{s} = dms.$$

*Moreover, $s$ divides* $\gcd(dm, dp^e)$. *If $f$ is not right-invariant, then $k > 1$ and $s \neq dp^e$.*

The proof is analogous to the one of Theorem 3. In particular, $[S_f : F] = [S_f : C]p^e = d^2 m \cdot p^e$. Comparing dimensions, we obtain again that $[S_f : \mathrm{Nuc}_r(S_f)] = k$, and if $f$ is not right-invariant, $k > 1$.

For each $z(t) = \hat{z}(g(t) - d_0) \in F[g(t) - d_0]$ with $\hat{z} \in F[x]$, we have $z \in Rf$ if and only if $z \in Rh$. Let

$$E_f = \{z(t) + Rf \mid z(t) = \hat{z}((g(t) - d_0)) \in F[(g(t) - d_0)]\} \subset R/Rf.$$

Together with the multiplication $(x + Rf) \circ (y + Rf) = (xy) + Rf$ for all $x, y \in F[(g(t) - d_0)]$, $E_f$ is a field extension of $F$ of degree $\deg(\hat{h})$ isomorphic to $E_{\hat{h}}$. Let $B = \mathrm{Nuc}_r(S_f)$, then $B$ has degree $s$ over $E_{\hat{h}}$, and

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

$R/Rf$ is a free right $B$-module of dimension $k$ via $R/Rf \times B \longrightarrow R/Rf$, $(a+Rf)(z+Rf) = az+Rf$. We assume $f$ is not right-invariant which yields $k>1$.

For $\rho \in \mathrm{Aut}(D)$ define $F' = \mathrm{Fix}(\rho) \cap F$. We assume that $F/F'$ is finite-dimensional. Let $\nu \in D$ and $1 \leq l < k = dp^e/s$. Define the set $S_{p^e,m,l}(\nu,\rho,f) = \{a+Rh \mid a \in P\} \subset R/Rh$, where

$$P = \{a_0 + a_1 t + \cdots + a_{lm-1}t^{lm-1} + \nu\rho(a_0)t^{lm} \mid a_i \in D\} \subset D[t;\delta].$$

$S_{p^e,m,l}(\nu,\rho,f)$ is a vector space over $F'$ of dimension $d^2p^em[F:F']$. We identify each element of $S_{p^e,m,l}(\nu,\rho,f)$ with a map in $\mathrm{End}_B(R/Rf)$ as follows: For each $a \in S_{p^e,m,l}(\nu,\rho,f)$, let $L_a : R/Rf \to R/Rf$ be the left multiplication map $L_a(b+Rf) = ab+Rf$. Let $M_a$ be the matrix in $M_k(B)$ representing $L_a$ with respect to a $B$-basis of $R/Rf$ and denote the image of $S = S_{p^e,m,l}(\nu,\rho,f)$ in $M_k(B)$ by

$$\mathcal{C}_{p^e,m,l} = \{M_a \mid a \in S_{p^e,m,l}(\nu,\rho,f)\}.$$

For $l=1$, this construction again yields algebras over $F'$: define a multiplication on the $F'$-vector space $R_m = \{g \in R \mid deg(g) < m\}$ via

$$a(t) \circ b(t) = (a(t) + \nu\rho(a_0)t^m)b(t) \bmod_r(f).$$

For $m>1$, $(R_m,\circ)$ is isomorphic to $S(\nu,\rho,f) = S_{p^e,m,1}(\nu,\rho,f)$. Therefore, we also denote $(R_m,\circ)$ by $S(\nu,\rho,f) = S_{p^e,m,1}(\nu,\rho,f)$.

**Example 36.** *Let $R = D[t;\delta]$ and $f(t) = t+c$ for some $c \in D$. For $\nu \in D^\times$ and $\rho \in \mathrm{Aut}(D)$, $S_{p^e,1,1}(\nu,\rho,f) = (D,\circ)$ has the multiplication*

$$\begin{aligned} x \circ y &= (x + \nu\rho(x)t)y) : \mathrm{mod}_r f = xy + \nu\rho(x)yt + \nu\rho(x)\delta(y) : \mathrm{mod}_r f \\ &= xy + \nu\rho(x)(\delta(y) - yc) \end{aligned}$$

*for all $x,y \in D$.*

**Theorem 37.** *Let $f \in D[t;\delta]$ be irreducible and $\deg(h) = km$. For all $a+Rh \in R/Rh$,*

$$\dim_B(\mathrm{im}(L_{M_a})) = k^2 - \frac{k}{m}\deg(\mathrm{gcrd}(a, \hat{h}(g(t)-d_0))),$$

$$\mathrm{colrank}(M_a) = k - \frac{1}{m}\deg(\mathrm{gcrd}(a, \hat{h}(g(t)-d_0))).$$

*In particular, if $\deg(h) = dmp^e$ then $M_a \in M_{p^e}(E_{\hat{h}})$ and*

$$\mathrm{rank}(M_a) = dp^e - \frac{1}{m}\deg(\mathrm{gcrd}(a, \hat{h}(g(t)-d_0))).$$

Thus, $S_{p^e,m,1}(\nu,\rho,f)$ is a division algebra if and only if there are no divisors of $h$ in $S_{p^e,m,1}(\nu,\rho,f)$. More generally for $l>1$, the above result means:

**Theorem 38.** *Suppose that $P$ does not contain any polynomial of degree $lm$, whose irreducible factors are all similar to $f$. Then, the set $S_{p^e,m,l}(\nu,\rho,f)$ defines an $F'$-linear MRD code in $M_k(B)$ with minimum distance $k-l+1$. In particular, if $\deg(h) = dmp^e$, then this code is an $F'$-linear MRD code in $M_{dp^e}(E_{\hat{h}})$ with minimum distance $dp^e - l + 1$.*

**Corollary 39.** *Suppose that $l=1$.*

*(i) If $a(t) + \nu\rho(a_0)t^m \in P$ is reducible, then $a(t)$ is not a left zero divisor of $(R_m,\circ)$.*
*(ii) If $\nu = 0$ then $(R_m,\circ)$ is a division algebra over $F'$, which for $m \geq 2$ is a Petit algebra.*
*(iii) If $P$ does not contain any polynomial similar to $f$, then $(R_m,\circ)$ is a division algebra over $F'$.*

The proofs are all identical to their analogues where $f \in D[t;\sigma]$.

https://doi.org/10.1017/S001708952300006X Published online by Cambridge University Press

**Remark 40.** *One can also use the reduced norm $N$ of the central simple algebra $D(t;\delta)$ in this setting: given a central simple algebra $D$ with a maximal subfield $E$ and $R = D[t;\delta]$, take the ring of central quotients $D(t;\delta) = \{f/g \mid f \in R, g \in C(R)\}$ of $R$. It has center $C(D(t;\delta)) = \mathrm{Quot}(C(R)) = F(x)$, where $x = g(t) = d_0$. Let $\tilde{\delta}$ be the extension of $\delta$ to $D(x)$ such that $\tilde{\delta} = id_{t|D(x)}$. Then, $D(t;\delta)$ is a central simple $F(x)$-algebra, more precisely $D(t;\delta) \cong (D(x), \tilde{\delta}, d_0 + x)$, i.e. $D(t;\delta)$ is a generalized differential algebra.*

*Let $N$ be the reduced norm of $D(t;\delta)$. For all $f \in R$, $N(f) \in F[x]$ and $f$ divides $N(f)$. Let $\omega : D \to M_d(E)$ be the left regular representation of $D$. For any $f \in R$ of degree $m$, $N(f) = \pm \det(\omega(a_m))^{p^e} x^{dm} + \dots$. In particular, $N(f)$ has degree $dm$ [36]. As the bound of $f$ has degree $dm$ in $F[x]$, it follows that $N(f)$ is equal to the bound of $f$. Thus if $\deg(\hat{h}) = dm$, we conclude that $\hat{h}(x) = \pm N(f)$.*

*There is more work to be done, for example, to determine the constant term of $N(f(t))$. This may lead to criteria on how to obtain division algebras using our construction. Additionally, the nuclei of both the algebras and the codes need to be calculated. For instance, consider the special case where $d = 1$, i.e. $R = K[t;\delta]$ for some field extension $K/F$. If $f(t) = a_0 + a_1 t + \cdots + a_m t^m \in R = K[t;\delta]$ has degree $m$, then $N(f(t)) = (-1)^{m(p^e-1)} a_m^{p^e} x^m + \dots$* [36, Thm 18(ii)] *Thus,*

$$N(f(t)) = a_m^{p^e} x^m + \dots$$

*To find the constant term of $N(f)$ is difficult. It is possible to compute special cases though, for example, for $f(t) = g(t) + a \in K[t;\delta]$, $N(f(t)) = (x + a)^{p^e}$* [36].

**Acknowledgement.** We would like to thank J. Sheekey for several helpful discussions on the subject, and the referee, whose comments greatly improved our paper.

## References

[1] A. A. Albert, *Modern higher algebra* (Dover Publications Inc., Mineola, NY, 2018).

[2] D. Augot, P. Loidreau and G. Robert, Generalized Gabidulin codes over fields of any characteristic, *Design Code Cryptogr.* **86**(8) (2018), 1807–1848. DOI 10.1007/s10623-017-0425-6.

[3] D. Augot, A. Couvreur, J. Lavauzelle and A. Neri, *SIAM J. Appl. Algebra Geom*. **5**(2) (2021), 165–199. DOI 10.1137/20M1348583.

[4] D. Boucher and F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, *Design Code Cryptogr.* **70**(3) (2014), 405–431. DOI 10.1007/s10623-012-9704-4.

[5] M. Boulagouaz and A. Leroy, $(s, d)$-codes, *Adv. Math. Commun. (AMC)* **7**(4) (2013), 463–474. DOI 10.3934/amc.2013.7.463.

[6] M. Blaum and R. J. McEliece, Coding protection for magnetic tapes: A generalization of the Patel-Hong code, *IEEE Trans. Inform. Theory* **31**(5) (1985), 690–693. DOI 10.1109/TIT.1985.1057098.

[7] J. Carcanague, Idéaux bilatères d'un anneau de polynômes non commutatifs sur un corps, *J. Algebra* **18**(1) (1971), 1–18. DOI 10.1016/0021-8693(71)90125-6.

[8] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Comb. Theory, Ser. A* **25**(3) (1978), 226–241. DOI 10.1016/0097-3165(78)90015-8.

[9] C. Faure and P. Loidreau, A new public-key cryptosystem based on the problem of reconstructing p-polynomials, *Coding and Cryptography* (Springer, 2006), 304–315, Available at: https://perso.univ-rennes1.fr/pierre.loidreau/articles/wcc

[10] E. M. Gabidulin, Theory of codes with maximum rank distance, *Probl. Inf. Transm.* **21** (1985), 1–12.

[11] J. Gòmez-Torrecillas, F. J. Lobillo and G. Navarro, Computing the bound of an Ore polynomial. Applications to factorization, *J. Symb. Comput*. **92** (2019), 269–297. DOI 10.1016/j.jsc.2018.04.018.

[12] E. M. Gabidulin, A. V. Paramonov and O. V. Tretjakov, Ideals over a noncommutative ring and their application in cryptology, in *Advances in cryptology - EUROCRYPT 91 (D. W. Davies, Editor)*, vol. 547 (LNCS, Springer, 1991), 482–489.

[13] N. Fogarty and H. Gluesing-Luerssen, A circulant approach to skew-constacyclic codes, *Finite Fields Appl*. **35** (2015), 92–114. DOI 10.1016/j.ffa.2015.03.008.

[14] T. Hanke, A direct approach to noncrossed product division algebras, *Dissertation, Universität Potsdam, Naturwissenschaftliche Fakultät*. DOI 10.48550/arXiv.1109.1580.

[15] M. Hübner and H. P. Petersson, Two-dimensional real division algebras revisited, *Available at:* https://www.fernuni-hagen.de/MATHEMATIK/ALGGEO/Petersson/Separata/Two-dimensonal%2BWidmung.pdf.

[16] T. W. Hungerford, Algebra, *Graduate texts in mathematics*, vol. 73 (Springer Verlag, New York, 1980).

[17] S. Ikehata, Purely inseparable ring extensions and Azumaya algebras, *Math. J. Okayama Univ*. **41** (1999), 63–69, Available at: https://www.math.okayama-u.ac.jp/mjou/mjou41/

[18] N. Jacobson, *Finite-dimensional division algebras over fields*. (Springer Verlag, Berlin-Heidelberg-New York, 1996).

[19] H. T. Kamche and C. Mouaha, *IEEE Transactions of Information Theory* **65**(12) (2019), 7718–7735. DOI 10.1109/TIT.2019.2933520.

[20] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, The book of involutions, vol. 44 (*AMS Society. Colloquium Publications,* 1998).

[21] Y. E. Maazouz, M. A. Hahn, A. Neri and M. Stanojkovski, (2021), DOI 10.48550/arXiv.2104.03216.

[22] O. Ore, Theory of noncommutative polynomials, *Ann. Math.* **34**(3) (1933), 480–508. DOI 10.2307/1968173.

[23] A. Owen, On the right nucleus of Petit algebras (University of Nottingham, 2022). DOI 10.48550/arXiv.2206.09436.

[24] S. Pai and B. S. Rajan, A Singleton bound for generalized ferrer's diagram rank metric codes, Online at arxiv: 1506.05558 [cs.IT]. DOI 10.48550/arXiv.1506.05558.

[25] R. S. Pierce, *Associative algebras*. (Springer-Verlag, New York, 1982).

[26] 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.

[27] S. Pumplün, *Finite nonassociative algebras obtained from skew polynomials and possible applications to* $(f, \sigma, \delta)$*-codes*, *Adv. Math. Commun. (AMC)* **11**(3) (2017), 615–634. DOI 10.3934/amc.2017046.

[28] S. Pumplün, *How to obtain lattices from* $(f, \sigma, \delta)$-codes via a generalization of Construction A, *Appl. Algebra Eng. Commun. Comput*. **29**(4) (2018), 313–333. DOI 10.1007/s00200-017-0344-9.

[29] S. Pumplün, Quotients of orders in algebras obtained from skew polynomials with applications to coding theory, *Commun. Algebra* **46**(11) (2018), 5053–5072. DOI 10.1080/00927872.2018.1461882.

[30] S. Pumplün, Albert's twisted field construction using algebras with a multiplicative norm, *J. Food Protect*. **57**(3) (1994), 246–248. DOI 10.48550/arXiv.1504.00188.

[31] R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, *IEEE Trans. Inform. Theory* **37**(2) (1991), 328–336. DOI 10.1109/18.75248.

[32] R. M. Roth, Tensor codes for the rank metric, *IEEE Trans. Inform. Theory* **72**(6) (1996), 2146–2157. DOI 10.1109/ISIT.1995.535754.

[33] J. Sheekey, A new family of linear maximum rank distance codes, *Adv. Math. Commun. (AMC)* **10**(3) (2016), 475–488. DOI 10.3934/amc.2016019.

[34] J. Sheekey, *New semifields and new MRD codes from skew polynomial rings*, *J. LMS* **101**(1) (September 2019), 432–456. DOI 10.1112/jlms.12281.

[35] D. Thompson, New classes of nonassociative division algebras and MRD codes, PhD Thesis (University of Nottingham, 2021). Available at: http://eprints.nottingham.ac.uk/64396/~

[36] D. Thompson and S. Pumplün, The norm of a skew polynomial, *J. Algebra Represent. Theory* **25**(4) (2022), 869–887. DOI 10.1007/s10468-021-10051-z.