Finite Fields and Their Applications 77 (2022) 101935

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Primitive idempotents in central simple algebras over $\mathbb{F}_q(t)$ with an application to coding theory ☆

J. Gómez-Torrecillas [a,*], P. Kutas [b], F.J. Lobillo [c], G. Navarro [d]

[a] *IMAG and Department of Algebra, University of Granada, E18071, Granada, Spain*
[b] *School of Computer Science, University of Birmingham, B15 2TT, Birmingham, United Kingdom*
[c] *CITIC and Department of Algebra, University of Granada, E18071, Granada, Spain*
[d] *CITIC and Department of Computer Science and A. I., University of Granada, E18071, Granada, Spain*

ARTICLE INFO

Article history:
Received 11 May 2019
Accepted 20 September 2021
Available online xxxx
Communicated by James W.P. Hirschfeld

MSC:
94B10
16H05
16H10
16K50

Keywords:
Global function field
Central simple algebra
Hasse invariants
Primitive idempotent
Skew constacyclic convolutional code

ABSTRACT

We consider the algorithmic problem of computing a primitive idempotent of a central simple algebra over the field of rational functions over a finite field. The algebra is given by a set of structure constants. The problem is reduced to the computation of a division algebra Brauer equivalent to the central simple algebra. This division algebra is constructed as a cyclic algebra, once the Hasse invariants have been computed. We give an application to skew constacyclic convolutional codes.

☆ Research partially supported by grant PID2019-110525GB-I00 from Agencia Estatal de Investigación (AEI) and from Fondo Europeo de Desarrollo Regional (FEDER).
* Corresponding author.
E-mail address: gomezj@ugr.es (J. Gómez-Torrecillas).

https://doi.org/10.1016/j.ffa.2021.101935

1. Introduction

We consider the following algorithmic problem. Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathcal{A}$ be a central simple algebra over $\mathbb{F}_q(t)$ (the field of rational functions in the variable t) with $\mathbb{F}_q(t)$-basis $b_1, \ldots, b_{n^2}$. Then one has that

$$b_i b_j = \sum_{k=1}^{n^2} \gamma_{ijk} b_k$$

where $\gamma_{ijk} \in \mathbb{F}_q(t)$. The γ_{ijk} are called structure constants. We consider $\mathcal{A}$ to be given as a collection of structure constants. The task is to find a primitive idempotent in $\mathcal{A}$. This problem is closely related to the factorization problem of Ore polynomials with coefficients in $\mathbb{F}_q(t)$ [10]. In [13] the split case, namely where $\mathcal{A} \cong M_n(\mathbb{F}_q(t))$, is studied. Here we investigate the problem when $\mathcal{A} \cong M_k(D)$ where D is a division algebra over $\mathbb{F}_q(t)$.

In Section 3 we reduce the problem of computing a primitive idempotent in $\mathcal{A}$ to computing D, the division algebra Brauer equivalent to $\mathcal{A}$ (building on the algorithm from [13]). A central simple algebra over $\mathbb{F}_q(t)$ is determined (up to Brauer equivalence) by its Hasse invariants (see, e.g., [6, Corollary 6.5.4]). This means that by computing the Hasse invariants of $\mathcal{A}$ and constructing a division algebra with those invariants provides a method for calculating the underlying division algebra of $\mathcal{A}$.

In [1] the authors propose a randomized polynomial time algorithm for constructing an $\mathbb{F}_q(t)$-division algebra provided that the invariant at infinity is zero and the degree of the algebra is coprime to q. We propose an algorithm where the invariant at infinity is not necessarily zero when $\mathbb{F}_q$ contains the nth roots of unity. Here n is the degree of the division algebra. When the degree of $\mathcal{A}$ is coprime to q, these algorithms can also be used to compute the Hasse invariants of $\mathcal{A}$.

We also give an application of our results. Linear convolutional codes of length n can be modeled (see [5,16,18]) as vector subspaces of $\mathbb{F}_q(t)^n$, where the variable t represents the delay operator. Based on this model, an approach to cyclic convolutional codes was proposed in [7]. So, given an automorphism σ of $\mathbb{F}_q(t)$, a skew cyclic convolutional code is a left ideal of a cyclic algebra $(\mathbb{F}_q(t), \sigma, 1)$, endowed with the Hamming metric induced by the natural basis of $(\mathbb{F}_q(t), \sigma, 1)$. These codes became MDS for the Hamming distance, and efficient algebraic decoding algorithms were designed for them [8,9]. A natural question is what can be done when the skew cyclic structure is given by a cyclic algebra of the form $(\mathbb{F}_q(t), \sigma, \lambda)$, for a general $\lambda \in \mathbb{F}_q(t)^\sigma$. This leads to the notion of skew constacyclic code. We will show that, if we know an explicit algebra isomorphism $(\mathbb{F}_q(t), \sigma, \lambda) \cong M_k(D)$, where D is a division algebra over $\mathbb{F}_q(t)^\sigma$, then the construction of skew convolutional codes and the decoding algorithms from [7,8] can be extended to skew constacyclic convolutional codes.

The structure of the paper is as follows. In Section 2 we recall some basic facts about quaternion and symbol algebras, and we provide randomized polynomial time algorithms

for computing quaternion and symbol algebras with given invariants. In Section 3 we show how one can compute a division algebra D Brauer equivalent to a given central simple $\mathbb{F}_q(t)$-algebra, and an explicit isomorphism with the corresponding matrix ring over D, using either the algorithms from Section 2 or the algorithm from [1]. In Section 4 we construct constacyclic convolutional codes of designed Hamming distance and propose a polynomial time decoding algorithm.

2. Quaternion and symbol algebras with prescribed invariants

Let K be a field such that the multiplicative group K^* contains a cyclic group of order n, and let $\epsilon \in K$ be a primitive n–th root of unity ϵ. Choose $a, b \in K^*$. The *symbol algebra* (or power residue algebra) $(a, b; K, \epsilon)$ is the K–algebra with generators u, v subject to the relations

$$u^n = a,\ v^n = b,\ uv = \epsilon vu.$$

When $n = 2$ (and, hence, K must be of characteristic different from 2), symbol algebras are called *quaternion algebras*.

Symbol algebras are central simple K–algebras [4, Chapter 11, Theorem 1].

2.1. Quaternion algebras

In this subsection we propose a randomized polynomial-time algorithm which constructs a quaternion algebra over $\mathbb{F}_q(t)$ with q an odd prime power which ramifies at prescribed places.

First we cite an estimate on the number of irreducible polynomials in a given residue class. This is an analogue of Dirichlet's theorem on primes in arithmetic progressions. However, in the function field case, a much stronger result is true:

Proposition 1. *[20, Theorem 5.1.] Let $a, m \in \mathbb{F}_q[t]$ be such that $deg(m) > 0$ and the $gcd(a, m) = 1$. Let N be a positive integer and let*

$$S_N(a, m) = \#\{f \in \mathbb{F}_q[t] \text{ monic irreducible} \mid f \equiv a \ (mod\ m),\ deg(f) = N\}.$$

Let $M = deg(m)$ and let $\Phi(m)$ denote the number of polynomials in $\mathbb{F}_q[t]$ relative prime to m whose degree is smaller than M. Then we have the following inequality:

$$|S_N(a, m) - \frac{q^N}{\Phi(m)N}| \leq \frac{1}{N}(M + 1)q^{\frac{N}{2}}.$$

We also state two lemmas from [14].

Lemma 2. *[14, Lemma 6] Let $a_1, a_2, a_3 \in \mathbb{F}_q[t]$ be nonzero polynomials. Let f be a monic irreducible polynomial. Let $\mathbb{F}_q(t)_{(f)}$ denote the f-adic completion of $\mathbb{F}_q(t)$. Let $v_f(a_i)$ denote the multiplicity of f in the prime decomposition of a_i. Then the following hold:*

1. *If $v_f(a_1) \equiv v_f(a_2) \equiv v_f(a_3) \pmod 2$, then the equation $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ is solvable in $\mathbb{F}_q(t)_{(f)}$.*
2. *Assume that not all the $v_f(a_i)$ have the same parity. Also suppose that $v_f(a_i) \equiv v_f(a_j) \pmod 2$. Then the equation $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ is solvable in $\mathbb{F}_q(t)_{(f)}$ if and only if $-f^{-v_f(a_ia_j)}a_ia_j$ is a square modulo f.*

Lemma 3. *[14, Lemma 10] Let $a_1, a_2, a_3 \in \mathbb{F}_q[t]$ be nonzero polynomials. Then the following hold:*

1. *If the degrees of the a_i all have the same parity then the equation $a_1x_1^2+a_2x_2^2+a_3x_3^2 = 0$ admits a nontrivial solution in $\mathbb{F}_q((\frac{1}{t}))$.*
2. *Assume that not all of the degrees of the a_i have the same parity. Also assume that $deg(a_i) \equiv deg(a_j) \pmod 2$. Let c_i and c_j be the leading coefficients of a_i and a_j respectively. Then the equation $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ has a nontrivial solution in $\mathbb{F}_q((\frac{1}{t}))$ if and only if $-c_ic_j$ is a square in $\mathbb{F}_q$.*

Assume S is a set of places of $\mathbb{F}_q(t)$. We propose an algorithm for constructing a quaternion algebra over $\mathbb{F}_q(t)$ which is split at a place w if and only if $w \notin S$. Such an algebra does exist if and only if the cardinality of S is even (see [19, Theorem III.3.1]).

Theorem 4. *Assume that S is an even finite set of places of $\mathbb{F}_q(t)$. Then there exists a randomized polynomial time algorithm (polynomial in d and $\log\ q$) which constructs a quaternion algebra H such that $H \otimes \mathbb{F}_q(t)_v$ is split if and only if $v \notin S$ (here, $\mathbb{F}_q(t)_w$ denotes the completion of $\mathbb{F}_q(t)$ at w).*

Proof. Let $H(a, b)$ denote the quaternion algebra $(a, b; \mathbb{F}_q(t), -1)$ with parameters $a, b \in \mathbb{F}_q(t)$. We will look for a and b in the form

$$a = f_1 \cdots f_k u, b = \lambda f_1 \cdots f_k$$

where the f_i are the finite places in S (which are monic irreducible polynomials), u is an irreducible polynomial in $\mathbb{F}_q[t]$ and $0 \neq \lambda \in \mathbb{F}_q$. First note that $H(a, b)$ is split at a place f (either a finite place or at infinity) if the equation

$$ax^2 + by^2 - z^2 = 0$$

is solvable in the completion $\mathbb{F}_q(t)_{(f)}$ [2, Project 4, Exercise 3.5].

If $H(a, b)$ should be split at infinity, then we choose the degree parity u in a way that the degree of a is even and we choose the leading coefficient of u to be 1. We choose λ to

be 1 (actually we could choose λ to be any nonzero element in $\mathbb{F}_q$). By Lemma 3, $H(a,b)$ will be split at infinity.

If $H(a,b)$ should not be split at infinity, then there are two cases. If the degree of b is odd (we have not chosen a λ yet but since λ is a nonzero constant it will not influence the degree of b), then we choose u in a way that the degree parity of a is even and we choose the leading coefficient of u to be a non-square element in $\mathbb{F}_q$. If the degree of b is even, then we choose λ to be a non-square element in $\mathbb{F}_q$ and we choose u in a way that the degree of a is odd (we do not have any constraints on the leading coefficient of u, thus we choose it to be 1). By Lemma 3, $H(a,b)$ will be a division algebra at infinity.

Thus we have imposed degree parity and leading coefficient conditions on u and we have chosen a suitable λ.

Now we impose conditions on u to ensure that, for all i, we have that $H(a,b)_{(f_i)}$ is a division algebra. By Lemma 2, we have that this happens if and only if $-u\lambda$ is not a square mod f_i. Note that we have already chosen λ, thus only choosing u in a suitable way remains. For every i we pick residue classes α_i modulo f_i in the following fashion. If $-\lambda$ is a square modulo f_i, then we pick α_i to be a non-square element modulo f_i. Thus if $u \equiv \alpha_i \ (mod\ f_i)$ then $-u\lambda$ is a non-square element mod f_i. If $-\lambda$ is not a square modulo f_i, then we pick $\alpha_i = 1$. By the Chinese Remainder Theorem, there exists a unique residue class B modulo $f_1 \cdots f_k$ which satisfies the condition $B \equiv \alpha_i \ (mod\ f_i)$. Thus, if

$$u \equiv B \ (mod\ f_1 \cdots f_k),$$

then $H(a,b)_{(f_i)}$ will be a division algebra for all f_i.

Now we summarize the steps of the algorithm. Let $F = f_1 \cdots f_k$ and let $d = deg\ F$

1. Choose a λ, a degree parity ϵ (which is zero if the degree of u should be even, otherwise it is 1) and a leading coefficient μ in the way described above.
2. Compute the residue class B modulo $f_1 \cdots f_k$ by Chinese remaindering.
3. Pick a random monic polynomial g of degree $3d + \epsilon$. Check if the polynomial $u' = f_1 \cdots f_k g + \frac{B}{\mu}$ is irreducible. If u' is irreducible, then let $u = \mu u$. Output $a = f_1 \cdots f_k u$ and $b = \lambda f_1 \cdots f_k$. If u' is not irreducible, then pick a new g.

The output quaternion algebra $H(a,b)$ does not split at any place $w \in S$. Also, it splits at every place except maybe at u by Lemma 2 and 3. Thus, since the number of places where it does not split is even by [19, Theorem III.3.1], it must split at u as well.

Finally, we need to show that the algorithm runs in polynomial time. The first three steps are deterministic and run in polynomial time.

We analyze the last step similarly as in the proof of [14, Theorem 30]. We have the following inequality due to Proposition 1:

$$\left| S_N(B,F) - \frac{q^N}{\Phi(F)N} \right| \leq \frac{1}{N}(d+1)q^{\frac{N}{2}}.$$

We set $N = 4d + \epsilon$, which implies that

$$\frac{S_N(B,F)}{q^{N-d}} \geq \frac{q^N}{q^{N-d}\Phi(F)N} - \frac{(d+1)q^{\frac{N}{2}}}{Nq^{N-d}} \geq \frac{1}{N} - \frac{d+1}{Nq^{\frac{N}{2}-d}} \geq \frac{1}{N} - \frac{d+1}{Nq^d} \geq \frac{1}{3N}.$$

This means that the probability that after $3N$ rounds we do not find an irreducible polynomial in the residue class is smaller than $\frac{1}{2}$. Hence this step runs in polynomial time. □

2.2. Symbol algebras

Our next goal is to generalize the algorithm from Theorem 4 to symbol algebras.

We first recall some basic facts on symbol algebras which will be useful for the construction of our algorithms. Let K be a field such that K^* contains a cyclic subgroup of order n, and take $\epsilon \in K^*$ a primitive n–th root of unity. Symbol algebras support the following splitting condition.

Proposition 5. *[4, Chapter 11, Corollary 4]. The symbol algebra $(a, b; K, \epsilon)$ is split if and only if b is a norm in the extension $K(a^{\frac{1}{n}})|K$.*

Proposition 5 implies that if a is an n–th power in K, then $(a, b; K, \epsilon)$ splits. We also have the following formula.

Proposition 6. *[4, Chapter 11, Lemma 3]*

$$(a, b; K, \epsilon) \otimes (a', b; K, \epsilon) \sim (aa', b; K, \epsilon),$$

where $\sim$ denotes Brauer equivalence.

In this section we assume that $\mathbb{F}_q$ contains the *nth* roots of unity, i.e., $q \equiv 1 \ (mod\ n)$. Let $\epsilon \in \mathbb{F}_q$ be a primitive n–th root of unity.

Proposition 7. *Let f be a monic irreducible polynomial in $\mathbb{F}_q[t]$, where $q \equiv 1 \ (mod\ n)$. Let ϵ be a primitive nth root of unity in $\mathbb{F}_q$. Denote by $\mathbb{F}_q(t)_{(f)}$ the completion of $\mathbb{F}_q(t)$ at the place corresponding to f. Let a, a' be units in the local ring of $\mathbb{F}_q(t)_{(f)}$, and $b \in \mathbb{F}_q(t)_{(f)}$. Suppose that $a \equiv a' \ (mod\ f)$. Then the symbol $\mathbb{F}_q(t)_{(f)}$–algebras $(a, b; \mathbb{F}_q(t)_{(f)}, \epsilon)$ and $(a', b; \mathbb{F}_q(t)_{(f)}, \epsilon)$ are Brauer equivalent.*

Proof. If c is a unit and $c \equiv 1 \ (mod\ f)$, then c is an nth power by Hensel's lemma, thus the algebra $(c, b; \mathbb{F}_q(t)_{(f)}, \epsilon)$ splits. Now one has to observe that $a'a^{-1} \equiv 1 \ (mod\ f)$, and that the opposite algebra of $(a, b; \mathbb{F}_q(t)_{(f)}, \epsilon)$ is Brauer equivalent to $(a^{-1}, b; \mathbb{F}_q(t)_{(f)}, \epsilon)$. □

We would like to cite a lemma from [1, Theorem 5] which provides a formula for calculating Hasse-invariants of cyclic algebras over local fields. The notation (F, σ, a)

stands for the cyclic F^σ–algebra built from an automorphism σ of F of finite order and $a \in F^\sigma$.

Proposition 8. *Let K be a local field (with valuation v_K) and let W be an unramified cyclic extension of K of degree n. Let σ be the unique automorphism of W that reduces to the Frobenius automorphism on residue fields. Then the Hasse invariant of the cyclic algebra (W, σ, b) is $\frac{v_K(b)}{n}$.*

Remark 9. If σ reduces to the kth power of the Frobenius automorphism, where k is coprime to n, then the Hasse invariant of (W, σ, b) is $\frac{k' v_K(b)}{n}$ where $kk' \equiv 1 \ (mod\ n)$ [17, Chapter 32].

We are now ready to describe the procedure for the construction of a symbol algebra with prescribed Hasse invariants.

Theorem 10. *Assume that we are given a set of monic irreducible polynomials $f_1, \ldots, f_k$ (in $\mathbb{F}_q[t]$) and a sequence of rational numbers (in reduced form) $\frac{r_1}{s_1}, \ldots, \frac{r_k}{s_k}, \frac{r_0}{s_0}$. Suppose that the sum of these rational numbers is an integer. Assume that the least common multiple of the s_i is n. Then there exists a randomized polynomial time algorithm which constructs a division $\mathbb{F}_q(t)$-algebra D, whose local Hasse invariant at f_i is equal $\frac{r_i}{s_i}$, for $i = 1, \ldots, k$, its local Hasse-invariant at infinity is equal to $\frac{r_0}{s_0}$, and the local Hasse-invariant at every other place is 0.*

Proof. First assume that the degree of $f_1 \cdots f_k$ is coprime to n. Let ϵ be a primitive nth root of unity in $\mathbb{F}_q$. Denote the symbol basis of the symbol algebra by u, v, i.e.,

$$u^n = a,\ v^n = b,\ uv = \epsilon vu.$$

We look for a and b in the form

$$a = s,\ b = f_1 \cdots f_k \lambda,$$

where s is a monic irreducible polynomial in $\mathbb{F}_q[t]$ and $\lambda \in \mathbb{F}_q^*$. The algorithm as in Theorem 4 boils down to choosing s and λ in an appropriate way. First, we impose congruence conditions on s in a way that the resulting algebra has Hasse-invariants $\frac{r_i}{s_i}$ at the places f_i for $i = 1, \ldots, k$. Define the residue class r_i' modulo n such that $\frac{r_i}{s_i} = \frac{r_i'}{n}$. We look at the algebra $D \otimes \mathbb{F}_q(t)_{(f_i)}$. Let $K_i = \mathbb{F}_q[t]/(f_i)$ which is a finite field with $q^{deg\ f_i}$ elements. Note that $C_i = K_i^*/K_i^{*n}$ is a cyclic group of order n. By Proposition 7, it is enough to find a $\omega_i \in K_i$ such that the symbol algebra $(\omega_i, b; \mathbb{F}_q(t)_{(f_i)}, \epsilon)$ has Hasse invariant $\frac{r_i}{s_i}$ as a central simple $\mathbb{F}_q(t)_{(f_i)}$-algebra. Choose $\delta_i \in K_i$ to be a generator of C_i. Then, by Proposition 8 (and the remark after it), $(\delta_i, b, \mathbb{F}_q(t)_{(f_i)}, \epsilon)$ has Hasse invariant $\frac{o_i}{n}$ where $(o_i, n) = 1$. Since $(o_i, n) = 1$, there exists a residue class o_i' modulo n such that $o_i o_i' \equiv r_i' \ (mod\ n)$. Choose $\omega_i = \delta_i^{o_i'}$. Proposition 6 implies that $(\omega_i, b; \mathbb{F}_q(t)_{(f_i)\epsilon})$

has Hasse invariant $\frac{r_i}{s_i}$. Thus choose s to be congruent to ω_i modulo f_i (this imposes k congruence conditions on s which can be made into one using Chinese remaindering as in Theorem 4).

Now we impose degree conditions on s and choose λ in a way that the resulting symbol algebra has Hasse-invariants $\frac{r_0}{s_0}$ at infinity. Again let $\frac{r_0}{s_0} = \frac{r'}{n}$

If we want the algebra to split at infinity (i.e., $r = 0$), then choose the degree of s to be divisible by n. Indeed, then s is an nth power by Hensel's lemma in $\mathbb{F}_q((\frac{1}{t}))$, hence by Proposition 5 the algebra splits. Assume that $r \neq 0$. Let $F = f_1 \cdots f_k$ and let $deg\ F \equiv l\ (mod\ n)$. Then choose the degree of s to be congruent to $n-l$ modulo n. Then $(uv)^n = \epsilon^{\frac{n(n-1)}{2}} sF\lambda = c$. Note that c is a polynomial whose degree is divisible by n and its leading coefficient is λ. Let $\mu = \epsilon^{\frac{n(n-1)}{2}}\lambda$. We will now choose an appropriate $\mu \in \mathbb{F}_q$. Then we put $\lambda = (\epsilon^{\frac{n(n-1)}{2}})^{-1}\mu$. Let $w = uv$. Observe that $uw = \epsilon wu$. Now we have the desired unramified extension that splits $D \otimes \mathbb{F}_q((\frac{1}{t}))$, namely the nth root of μFs. Now we proceed in the same manner as at the finite primes. First choose μ_0 to be a generator of $\mathbb{F}_q^*/\mathbb{F}_q^{*^n}$. Then Proposition 7 shows that by choosing $\mu = \mu_0$ we get a Hasse invariant $\frac{o}{n}$ at infinity where $(o, n) = 1$. Let o' be such that $oo' \equiv r'\ (mod\ n)$. By choosing $\mu = \mu_0^{o'}$ we get the desired Hasse-invariant.

Now we consider the case where $deg\ F$ is not coprime to n. Suppose $deg\ F \equiv l\ (mod\ n)$. Choose an irreducible polynomial g (different from the f_i) such that $deg\ g \equiv n + 1 - l\ (mod\ n)$. Such a polynomial can be found just by picking a large enough degree and choosing a polynomial at random. Then we look for a and b in the following form:

$$a = s,\ b = f_1 \cdots f_k g\lambda.$$

By implying the same conditions modulo f_i apply on s as in the first part of the proof we guarantee that the local Hasse-invariants at the f_i are $\frac{r_i}{s_i}$. We add the extra condition that $s \equiv 1\ (mod\ g)$. Proposition 5 implies that D splits at g. Finally, by choosing λ and the degree of s in a suitable way we can achieve that the Hasse-invariant at infinity is $\frac{r}{s}$ as in the first part of the proof (as now the degree of $f_1 \cdots f_k g$ is congruent to 1 modulo n).

Note that, by Proposition 5, D splits at every finite place different from the f_i, as a polynomial over a finite field always has a zero if the number of its variables is greater than its degree (by Chevalley's theorem), and the existence of roots over a local field is reduced to finite fields by Hensel's Lemma.

We must consider the Hasse invariant at s. The Hasse-invariant at s must be zero as the sum of all Hasse-invariants adds up to an integer.

Finally, D is indeed a division algebra as it has index n (it has period n and in the case of global fields, the period equals the index) and is of dimension n^2 over $\mathbb{F}_q(t)$. □

3. Construction of an explicit isomorphism from a simple algebra to its matrix form

Let $\mathcal{A}$ be a central simple algebra over $\mathbb{F}_q(t)$ of finite dimension n^2. Let $b_1, \ldots, b_{n^2}$ be an $\mathbb{F}_q(t)$-basis of $\mathcal{A}$. Then, for $i, j = 1, \ldots n^2$,

$$b_i b_j = \sum_{k=1}^{n^2} \gamma_{ijk} b_k,$$

for $\gamma_{ijk} \in \mathbb{F}_q(t)$. We consider $\mathcal{A}$ to be given as a collection of *structure constants*

$$\{\gamma_{ijk} : 1 \leq i, j, k \leq n^2\}.$$

Consider the following problem:

Problem 11. Compute an explicit isomorphism of $\mathbb{F}_q(t)$–algebras $\mathcal{A} \cong M_k(D)$, for a suitable division $\mathbb{F}_q(t)$–algebra D.

If the algebra $\mathcal{A}$ is known to be split, then a randomized polynomial time algorithm is proposed in [13] which finds an explicit isomorphism $\mathcal{A} \cong M_n(\mathbb{F}_q(t))$. We will first use such a solution to Problem 11 when $D = \mathbb{F}_q(t)$, in conjunction with [15], to get a randomized polynomial time algorithm which solves the general case, whenever D is known.

Proposition 12. *Assume that a division $\mathbb{F}_q(t)$–algebra D is given by structure constants and it is known that $\mathcal{A} \cong M_k(D)$. There exists a randomized polynomial time algorithm which computes an explicit isomorphism $\mathcal{A} \cong M_k(D)$.*

Proof. First, observe that, from the $\mathbb{F}_q(t)$–basis of D and the structure constants of D, one easily gets m and a basis of $M_k(D)$ with the corresponding structure constants. Now, we know that $\mathcal{A} \otimes M_k(D)^{op} \cong M_{n^2}(\mathbb{F}_q(t))$. Using the randomized polynomial time algorithm from [13] one can compute an explicit isomorphism θ between $\mathcal{A} \otimes M_k(D)^{op}$ and $M_{n^2}(\mathbb{F}_q(t))$. Finally, [15, Section 4] describes a randomized polynomial time method for computing an explicit isomorphism ϕ between $\mathcal{A}$ and $M_k(D)$ using θ. □

We have reduced Problem 11 to the following one.

Problem 13. Let $\mathcal{A}$ be a central simple $\mathbb{F}_q(t)$-algebra of dimension n^2 over $\mathbb{F}_q(t)$ given by structure constants. Compute the structure constants of a division $F_q(t)$–algebra D such that $\mathcal{A} \cong M_k(D)$.

The algorithm we propose to deal with Problem 13 rests upon the idea of computing first the local Hasse invariants of $\mathcal{A}$ and, with them at hand, construct a division algebra

with the same local Hasse invariants. To this end, we need an algorithm for computing local indices of a central simple algebra over $\mathbb{F}_q(t)$, which is already provided by [12].

Lemma 14. *[12, Proposition 6.5.3]. There exists a randomized polynomial time algorithm for computing the local index at a given irreducible $f \in \mathbb{F}_q(t)$ of a central simple $\mathbb{F}_q(t)$-algebra $\mathcal{A}$ defined by structure constants.*

Proof. The proof of [12, Proposition 6.3.5] boils down, in this case, to the following procedure. Compute a maximal $\mathbb{F}_q[t]$-order Γ in $\mathcal{A}$ using the algorithm from [12, Theorem 6.4.2]. Let f be a monic irreducible polynomial. Then $\Gamma/f\Gamma$ is a finite algebra C over the field $\mathbb{F}_q[t]/(f)$. Then one computes the radical of C using the algorithm from [3] and then one computes the factor $C/Rad(C)$. Then the dimension of this radical-free part over its center is the local index at f. □

Proposition 15. *There exists a randomized polynomial time algorithm which computes the Hasse-invariants of a central simple $\mathbb{F}_q(t)$-algebra $\mathcal{A}$ given by structure constants, assuming that $gcd(q, n) = 1$ where n is the degree of $\mathcal{A}$ over $\mathbb{F}_q(t)$.*

Proof. Compute a maximal $\mathbb{F}_q[t]$-order Γ in $\mathcal{A}$ using the algorithm from [13]. The Hasse-invariant is zero for every monic irreducible polynomial which does not divide the discriminant of Γ. Thus by factoring the discriminant we have a list of monic irreducible polynomials for which the Hasse-invariant needs to be computed.

First we propose an algorithm that decides whether the Hasse-invariant of $\mathcal{A}$ at the place f equals k/n or not, for each $k = 0, \ldots, n-1$. We choose a finite place g (i.e., a monic irreducible polynomial) which is different from f. Using the algorithm from [1] we construct a division algebra D with Hasse invariants $\frac{n-k}{n}$ at f and $\frac{k}{n}$ at g (this splits at infinity since the sum of the Hasse-invariants is an integer). Using Lemma 14, we compute the local index of the central simple algebra $\mathcal{A} \otimes D$ at f. Since the local Hasse invariants of the tensor product of two central simple algebras add up, the Hasse invariant of $\mathcal{A}$ at f is $\frac{k}{n}$ if and only if the local index at f of $\mathcal{A} \otimes D$ is equal to 1.

Finally we do this computation for every k and every monic irreducible f dividing the discriminant of Γ and we are done. □

Theorem 16. *Let $\mathcal{A}$ be a central simple $\mathbb{F}_q(t)$-algebra of dimension n^2 given by structure constants. Assume that $\mathcal{A}$ is split at infinity and that $(n, q) = 1$. There exists a randomized polynomial time algorithm for computing a central division $\mathbb{F}_q(t)$–algebra D and an explicit isomorphism $\mathcal{A} \cong M_k(D)$.*

Proof. By Proposition 8, we can compute the set S of Hasse invariants of $\mathcal{A}$. For the second step, construct a division algebra D (D should be given by an $\mathbb{F}_q(t)$-basis and structure constants), whose non-zero Hasse-invariants are exactly the elements of the set S. This can be done by the algorithm from [1]. We need to show that the denominator of each nonzero Hasse-invariant is relative prime to q. The least common multiple of the s_i

is equal to the index of $\mathcal{A}$. Since the index of $\mathcal{A}$ is a divisor of n and $(q, n) = 1$, each of the s_i is coprime to q. This implies that the algorithm from [1] can be applied. Note that this algorithm returns D in a cyclic algebra form, not in a structure constant from. However, from a cyclic algebra representation there exists a polynomial time algorithm which computes structure constants. Finally, apply the algorithm from Proposition 12. □

The following consequence of Theorem 16 will be used later.

Corollary 17. *Let $\mathcal{A}$ be a central simple $\mathbb{F}_q(t)$-algebra of dimension n^2 over $\mathbb{F}_q(t)$ given by structure constants. Assume that $\mathcal{A}$ is split at infinity and that $(n, q) = 1$. There exists a randomized polynomial time algorithm for computing a primitive idempotent of $\mathcal{A}$.*

Actually the conditions for Corollary 17 can be relaxed. Assume that $\mathcal{A}$ is not split at infinity but it is split at a place corresponding to the monic irreducible polynomial $f(t) = t + c$ where $c \in \mathbb{F}_q$. Let $s = \frac{1}{f}$. Then one has that $\mathbb{F}_q(t) = \mathbb{F}_q(s)$ only now the infinite place of $\mathbb{F}_q(s)$ corresponds to the finite place f of $\mathbb{F}_q(t)$. This shows the following:

Theorem 18. *Let $\mathcal{A}$ be a central simple $\mathbb{F}_q(t)$-algebra of dimension n^2 given by structure constants. Assume that $(n, q) = 1$ and that $\mathcal{A}$ is either split at infinity or at a finite place f where f corresponds to a linear polynomial. Then there exists a randomized polynomial time algorithm which finds a primitive idempotent in $\mathcal{A}$, henceforth, an explicit isomorphism $\mathcal{A} \cong M_k(D)$ for a division $\mathbb{F}_q(t)$–algebra D Brauer equivalent to $\mathcal{A}$.*

Proof. By computing the nonzero Hasse-invariants of $\mathcal{A}$ we obtain a linear polynomial $f(t) = t + c$ at which $\mathcal{A}$ splits. Then let $s = \frac{1}{t+c}$ and rewrite the structure constants of $\mathcal{A}$ in terms of s (every structure constant is a rational function in s). Now this new algebra is split at infinity, thus we can find a primitive idempotent $\mathcal{A}$ using Corollary 17. Finally substitute $s = \frac{1}{t+c}$ and obtain the primitive idempotent as an $\mathbb{F}_q(t)$-linear combination of the basis elements. Finally, a straightforward argument shows how to get an explicit isomorphism $\mathcal{A} \cong M_k(D)$ from a primitive idempotent of $\mathcal{A}$. □

Theorem 18 implies that assuming that the degree of the algebra and q are relatively prime we only encounter a problem if $\mathcal{A}$ is split at every linear place. This is much less restrictive than the original conditions of Corollary 17 or Theorem 16. In conclusion, Theorem 18 solves Problem 11 completely if $\mathbb{F}_q$ contains the nth roots of unity and for "almost all" central simple $\mathbb{F}_q(t)$-algebras when $\mathbb{F}_q$ does not contain a primitive nth root of unity.

4. Constructing constacyclic convolutional codes

In this section we consider skew-constacyclic convolutional codes which are related to skew-cyclic convolutional codes in a similar fashion as linear constacyclic block codes are

related to cyclic codes. Our main goal is to construct skew-constacyclic convolutional codes of designed Hamming distance and propose a decoding algorithm.

We present cyclic algebras as factor rings of skew polynomial rings, with the aim of making use of the computational tools (e.g. extended Euclidean Algorithm) available for these non-commutative polynomials. We will need also to consider the more general situation of K–linear codes, where K be a finite extension of $\mathbb{F}_q(t)$, even thought our primary interest is the case $K = \mathbb{F}_q(t)$. We start by recalling the definition of skew polynomial rings over K.

Definition 19. Let σ be an automorphism of K of order n. Then $R = K[x;\sigma]$ consists of the usual polynomials over K with the standard addition and multiplication induced by the relation $xa = \sigma(a)x$, where $a \in K$.

Let us denote the fixed field of σ by K^σ. Suppose $\lambda \in K^\sigma$. Then it is easy to see that the Ore polynomial $x^n - \lambda$ is in the center of R, and $\mathcal{A} = K[x,\sigma]/(x^n - \lambda)$ is a cyclic algebra over K^σ which is isomorphic, as a K–vector space, to K^n by the following map:

$$\mathfrak{v} : \sum_{i=0}^{n-1} a_i x^i \mapsto (a_0, \ldots, a_{n-1}) \in K^n.$$

Thus we can define the Hamming weight of an element in $\mathcal{A}$.

Definition 20. The Hamming weight $w(f)$ of an element $f = \sum_{i=0}^{n-1} a_i x^i \in \mathcal{A}$ is the number of nonzero a_i. The Hamming distance between $f, g \in \mathcal{A}$ is defined by $d(f,g) = w(f-g)$.

Next we define skew-constacyclic codes.

Definition 21. Let $\mathcal{A} = K[x,\sigma]/(x^n - \lambda)$. A skew-constacyclic K–linear convolutional code is a left ideal of $\mathcal{A}$ endowed with the Hamming distance.

Skew-cyclic convolutional codes from [7] are obtained by setting $K = \mathbb{F}_q(t), \lambda = 1$. The rest of the section will be divided into two subsections. In the first subsection we consider the case where λ is a norm in the extension $K|K^\sigma$. We are mainly interested in the case when $K = \mathbb{F}_q(t)$. However, we will prove results for general K as well, as we need them in the other subsection.

The second subsection is devoted to the case where $K = \mathbb{F}_q(t)$ and λ is not a norm in the extension $\mathbb{F}_q(t)|\mathbb{F}_q(t)^\sigma$. Here we start from a primitive idempotent of $\mathcal{A}$. Next we construct a set of orthogonal idempotents which are permuted by σ^m (the starting idempotent is denoted by e), where m is the index of $\mathcal{A}$. We consider the left ideal generated $e, \sigma^m(e), \ldots, \sigma^{m(k-2)}(e)$ and show that this code has Hamming minimum distance at least k and propose a decoding algorithm.

4.1. The norm case

In this subsection we consider the case where λ is a norm in the extension $K|K^\sigma$.

Definition 22. Let K be a finite extension of $\mathbb{F}_q(t)$ and let σ be an automorphism of finite order n of K. Then the jth norm map N_j is defined in the following way:

$$N_0(x) = 1,\ N_j(x) = x\sigma(x)\cdots\sigma^{j-1}(x)$$

It is well known that the cyclic algebras $\mathcal{A} = K[x,\sigma]/(x^n - \lambda)$ and $\mathcal{B} = K[y,\sigma]/(y^n - 1)$ are isomorphic. The key observation of this subsection is that there is a map from $\mathcal{A} = K[x,\sigma]/(x^n - \lambda)$ to $\mathcal{B} = K[y,\sigma]/(y^n - 1)$ which is not only an isomorphism of rings, but is also an isometry with respect to the Hamming distance.

Proposition 23. *Let θ be the map $\mathcal{A} \to \mathcal{B}$ defined by*

$$\theta : \sum_{i=0}^{n-1} a_i x^i \mapsto \sum_{i=0}^{n-1} a_i N_i(a) y^i,$$

where $N_{K|K^\sigma}(a) = \lambda$. Then θ is an algebra isomorphism which is an isometry with respect to the Hamming distance.

Proof. It is easy to check that θ is a homomorphism of K^σ–algebras. It is also an isometry since $N_i(a) \neq 0$, because the norm of a is λ (which is nonzero). The inverse of θ is the map

$$\theta^{-1} : \sum_{i=0}^{n-1} a_i y^i \mapsto \sum_{i=0}^{n-1} a_i N_i(a^{-1}) x^i. \quad \square$$

First we consider the case when $K = \mathbb{F}_q(t)$. The map θ^{-1} provides an easy way to construct codes of designed distance δ from skew codes. First we construct a skew Reed-Solomon code of designed distance δ in $\mathcal{B} = \mathbb{F}_q(t)[y,\sigma]/(y^n - 1)$ (using the method from [8]). Let this code be C. By Proposition 23, $\theta^{-1}(C)$ is a skew-constacyclic code in $\mathcal{A} = \mathbb{F}_q(t)[x,\sigma]/(x^n - \lambda)$. The only thing we need is to be able to solve the norm equation $N_{\mathbb{F}_q(t)|\mathbb{F}_q(t)^\sigma}(a) = \lambda$. This can be done using the algorithm from [13] since $\mathbb{F}_q(t)^\sigma$ is isomorphic to $\mathbb{F}_q(t)$ (by Lüroth's theorem) and such an isomorphism can be computed by the method of [11]. The decoding procedure from [8] can also be adjusted. You receive an element m in $\mathcal{A}$. Then apply θ to m and decode it in $\mathcal{B}$ as $c \in \mathcal{B}$. Finally $\theta^{-1}(c)$ is the decoding of m. Naturally, these codes will also be MDS. We summarize these observations in a theorem:

Theorem 24. *Let $\mathcal{A} = \mathbb{F}_q(t)[x,\sigma]/(x^n - \lambda)$, where λ is a norm in the extension $\mathbb{F}_q(t)|\mathbb{F}_q(t)^\sigma$. Then there exists a randomized polynomial time algorithm which computes*

skew-constacyclic MDS codes of designed distance δ and there also exists a polynomial time decoding algorithm for these codes.

These results imply that the norm case is closely related to the skew-cyclic case. The following proposition is a slight generalization of [8, Theorem 4] which will be needed when dealing with a λ which is not a norm. For $f_1, \ldots, f_t \in K[x;\sigma]$, the notation $[f_1, \ldots, f_t]_\ell$ stands for the least common left multiple of $f_1, \ldots, f_t$.

Proposition 25. *Let K be a finite extension of $\mathbb{F}_q(t)$ and let $\mathcal{A} = K[x;\sigma]/(x^n - 1)$. Let α generate a normal basis of the extension $K|K^\sigma$ and let $\beta = \alpha^{-1}\sigma(\alpha)$. Let m be a divisor of n. Then the code generated by*

$$[x - \beta, x - \sigma^m(\beta), \ldots, x - \sigma^{m(k-2)}(\beta)]_l$$

has Hamming distance at least k.

Proof. The same proof as the proof of Theorem 4 in [8] applies. □

Moreover, such a code can also be decoded by the same algorithm as described in [8].

4.2. The case where λ is not a norm

In this section, we deal with the case where λ is not a norm. We assume we know an explicit algebra isomorphism between $\mathcal{A} = \mathbb{F}_q(t)[x,\sigma]/(x^n - \lambda)$ and $M_{n/m}(D)$ where D is a division algebra of index m over $\mathbb{F}_q(t)^\sigma$. Such an isomorphism can be computed by means of the algorithms from Section 3.

The following theorem provides an orthogonal system of primitive idempotents adapted to our purposes. First note that σ, when applied coefficientwise to an Ore polynomial, is an automorphism of $\mathcal{A}$. By an abuse of notation we will denote this automorphism also by σ.

Theorem 26. *Let $\mathcal{A} = \mathbb{F}_q(t)[x,\sigma]/(x^n - \lambda)$ and assume that λ is not an rth power for every r dividing n, and that $(q,n) = 1$. Let m be the index of $\mathcal{A}$. Suppose we have an isomorphism between $\mathcal{A}$ and $M_{n/m}(D)$ where D is the division algebra Brauer equivalent to $\mathcal{A}$. Then there exists a randomized polynomial time algorithm which finds a primitive idempotent e_0 such that $e_0, \sigma^m(e_0), \ldots, \sigma^{n-m}(e_0)$ is an orthogonal system of primitive idempotents in $\mathcal{A}$.*

Proof. We already have an isomorphism between $\mathcal{A}$ and $M_{n/m}(D)$ so, by an abuse of notation, we refer to x as a matrix from $M_{n/m}(D)$. Let $s \in M_{n/m}(D)$ be the matrix with λ in the bottom left corner, 1s over the diagonal and zero everywhere else (this is the usual companion matrix of the polynomial $y^{n/m} - \lambda$). Let $K = \mathbb{F}_q(t)^\sigma$. The minimal polynomial of both s and x^m over K is $y^{n/m} - \lambda \in K[y]$. The polynomial $y^{n/m} - \lambda$ is

irreducible over K because λ is not an rth power by assumption for every r dividing n. This implies that $K(s)$ and $K(x^m)$ are subfields of $\mathcal{A}$ which are isomorphic, thus, by the Noether-Skolem theorem, they are conjugate. This means that there exists an element $z \in K(x)$ which is a conjugate of s and $z^{n/m} = \lambda$. Since $(n, q) = 1$ there exists a field automorphism of $K(x)$ which maps z to x^m. By the Noether-Skolem theorem this field automorphism is also realized by a conjugation. Finally we get that s and x^m are conjugates. An element h can be computed by solving a system of linear equations for which $h^{-1}x^m h = s$.

Let f be the primitive idempotent in $M_{n/m}(D)$ having 1 in the top left corner and zero everywhere else. Then $f, s^{-1}fs, \ldots, s^{1-n/m}fs^{n/m-1}$ is a complete orthogonal system of primitive idempotents. Since $h^{-1}x^m h = s$ we have that

$$f, h^{-1}x^{-m}hfh^{-1}x^m h, \ldots, (h^{-1}x^{-m}h)^{1-n/m}f(h^{-1}x^m h)^{n/m-1}$$

is a complete system of primitive orthogonal idempotents. It is now easy to see that choosing $e_0 = hfh^{-1}$ suffices. □

So, we will assume we are given a primitive idempotent $e \in \mathcal{A}$ such that

$$e_0, \sigma^m(e_0), \ldots, \sigma^{n-m}(e_0)$$

is an orthogonal system of primitive idempotents in $\mathcal{A}$. Let $e = 1 - e_0$. Now we are ready to define our code.

Definition 27. A skew Reed-Solomon constacyclic convolutional code of designed distance $k \leq \frac{n}{m}$ is defined as the code generated, as a left ideal, by

$$[e, \sigma^m(e), \ldots, \sigma^{m(k-2)}(e)]_l.$$

Now are goal is to justify the previous definition and show that the code has indeed Hamming distance at least k.

Theorem 28. *The code C generated by $[e, \sigma^m(e), \ldots, \sigma^{m(k-2)}(e)]_l$ has Hamming distance at least k and it also admits a decoding algorithm which runs in polynomial time.*

The first key idea of the proof is the construction of an isometric embedding of $\mathcal{A} = \mathbb{F}_q(t)[x, \sigma]/(x^n - \lambda)$ into $\mathcal{A}' = M[x, \phi]/(x^n - \lambda)$ where M is the splitting field of the polynomial $s^n - \lambda \in \mathbb{F}_q(t)[s]$ and ϕ is an automorphism of M which restricted to L is σ.

Proposition 29. *Let σ be an automorphism of $\mathbb{F}_q(t)$ of order n. Let $\lambda \in \mathbb{F}_q(t)^\sigma$ and let M be the splitting field of the polynomial $s^n - \lambda \in \mathbb{F}_q(t)[s]$. Then there exists an automorphism ϕ of M with the following properties:*

1. *ϕ restricted to $\mathbb{F}_q(t)$ is σ and ϕ has order n,*
2. *λ is a norm in the extension $M|M^\phi$.*

Proof. We distinguish two cases. First assume that $\mathbb{F}_q$ contains the nth roots of unity. Then $M = \mathbb{F}_q(t)(\lambda^{\frac{1}{n}})$. The field M admits an $\mathbb{F}_q(t)$-basis $1, \lambda^{\frac{1}{n}}, \ldots, \lambda^{\frac{l}{n}}$ where $l = \frac{n}{d}$ (if d is the largest positive integer for which λ is a dth power where d divides n). Then consider the following map:

$$\phi : \mu_0 + \mu_1\lambda^{\frac{1}{n}} + \cdots + \mu_k\lambda^{\frac{l}{n}} \mapsto \sigma(\mu_0) + \sigma(\mu_1)\lambda^{\frac{1}{n}} + \cdots + \sigma(\mu_k)\lambda^{\frac{l}{n}}.$$

The map ϕ is an automorphism of M since λ is fixed by σ. Also ϕ has order n since its nth power is the identity and restricted $\mathbb{F}_q(t)$ it is σ which has order n (as an automorphism of $\mathbb{F}_q(t)$). Finally, since $\lambda^{\frac{1}{n}}$ is fixed by ϕ, we have that λ is the norm of $\lambda^{\frac{1}{n}}$ in the extension $M|M^\phi$.

Now assume that $\mathbb{F}_q$ does not contain the nth roots of unity. Then $M = \mathbb{F}_r(t)(\lambda^{\frac{1}{n}})$ where $\mathbb{F}_r$ is an extension of $\mathbb{F}_q$ by a primitive nth root of unity. In this case we first extend σ to $\mathbb{F}_r(t)$ in a natural way (the image of t is exactly the same as in $\mathbb{F}_q(t)$). This fixes $\mathbb{F}_r$. Then we extend in the exact same fashion as in the previous case. □

Proposition 29 gives us an isometric embedding of $\mathcal{A} = \mathbb{F}_q(t)[x,\sigma]/(x^n - \lambda)$ into $\mathcal{A}' = M[x,\phi]/(x^n - \lambda)$. Actually $\mathcal{A}'$ naturally contains $\mathcal{A}$. The important observation is that $\mathcal{A}'$ is now a full matrix algebra over the field M^ϕ.

Let C be the code generated by $[e, \sigma^m(e), \ldots, \sigma^{m(k-2)}(e)]_l$. Now the element e is contained in $\mathcal{A}'$ as well. Consider the left ideal L of $\mathcal{A}'$ generated by e.

Lemma 30. *The left ideal L is contained in a maximal left ideal generated by $x - \beta$ and such a β can be computed in polynomial time.*

Proof. First we show that if we already have a maximal left ideal I containing L, then we can compute β. A maximal left ideal has dimension $n(n-1)$ over M^ϕ. The M-subspace generated by 1 and x has dimension $2n$ over M^ϕ. Thus these two subspaces have a nontrivial intersection (a nonzero intersecting element is of the form $a_1x + a_2$, where $a_1, a_2 \in M$ and $a_1 \neq 0$ since otherwise it would be invertible). Now we proceed by proposing an algorithm for finding a maximal left ideal containing e. Since we have an element (the element $\lambda^{\frac{1}{n}}$) in M whose norm is λ in the extension $M|M^\phi$ we can compute an explicit isomorphism between $\mathcal{A}'$ and $M_n(M^\phi)$ (if one has an element $\mu \in M$ whose norm is λ, then $y - \mu$ is a rank 1 element in $\mathcal{A}'$). The element e is diagonalizable with eigenvalues 0 and 1. We compute an eigenbasis and thus a diagonalization. Let geg^{-1} be the diagonal matrix with 0s and 1s in the diagonal. Let w be a matrix where all the zeros in the diagonal of geg^{-1} are switched to 1s except at one place. Then w generates a maximal left ideal which contains geg^{-1}. This implies that the maximal left ideal $g^{-1}wg$ contains e. □

Now we are ready to prove Theorem 28.

Proof of Theorem 28. Let us consider the code C generated by $[e, \sigma^m(e), \ldots, \sigma^{m(k-2)}(e)]_l$. Let $\mathcal{A}' = M[x,\phi]/(x^n - \lambda)$ as defined in Proposition 29 and compute β as described in Lemma 30. Let α be an element in M which generates a normal basis of the extension $M|M^\phi$. Let $a = \frac{\beta\alpha}{\phi(\alpha)}$ and let $\gamma = \phi(\alpha)\alpha^{-1}$. Now consider the embedding θ of $\mathcal{A}'$ into $B = M[y,\phi]/(y^n - 1)$ defined by:

$$\theta : \sum_{i=0}^{n-1} a_i x^i \mapsto \sum_{i=0}^{n-1} a_i N_i(a) y^i.$$

The maximal left ideal of $\mathcal{A}'$ generated $x - \beta$ maps to the maximal left ideal $y - \frac{\beta}{a} = y - \gamma$. Thus the left ideal C embeds isometrically into the left ideal of $\mathcal{B}$ generated by

$$[y - \gamma, y - \phi^m(\gamma), \ldots, \phi^{m(k-2)}]_\ell.$$

Proposition 25 shows that the Hamming distance of C is at least k (as it is contained in a code which has Hamming distance at least k). Decoding also works now in a natural way. We decode the code in $\mathcal{B}$ (this is now a skew-cyclic RS-code). Then we compute its preimage via the map θ (the method for computing the inverse of θ is described in the previous subsection). □

Theorem 28 shows that these constacyclic codes are subcodes of skew-cyclic RS codes over extensions of $\mathbb{F}_q(t)$. The bound we prove on their Hamming distance is tight in the sense that if $\mathcal{A}$ is a division algebra then the Hamming distance of any constacyclic code is 1.

References

[1] G. Böckle, D. Gvirtz, Division algebras and maximal orders for given invariants, LMS J. Comput. Math. 19 (2016) 178–195.
[2] A.M. Cohen, H. Cuypers, H. Sterk (Eds.), Some Tapas of Computer Algebra, vol. 4, Springer Science and Business Media, 2013.
[3] A.M. Cohen, G. Ivanyos, D.B. Wales, Finding the radical of an algebra of linear transformations, J. Pure Appl. Algebra 117–118 (1997) 177–193.
[4] P.K. Draxl, Skew Fields, Cambridge University Press, 1983.
[5] G.D. Forney, Convolutional codes I: algebraic structure, IEEE Trans. Inf. Theory 16 (1970) 720–738.
[6] P. Gille, T. Szamuely, Central Simple Algebras and Galois Cohomology, Cambridge University Press, 2006.
[7] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, A new perspective of cyclicity in convolutional codes, IEEE Trans. Inf. Theory 62 (2016) 2702–2706.
[8] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, A Sugiyama-like decoding algorithm for convolutional codes, IEEE Trans. Inf. Theory 63 (2017) 6216–6226.
[9] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, Peterson-Gorenstein-Zierler algorithm for skew RS codes, Linear Multilinear Algebra 66 (2018) 469–487.
[10] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, Computing the bound of an Ore polynomial. Applications to factorization, J. Symb. Comput. 92 (2019) 269–297.

[11] J. Gutierrez, R. Rubio, D. Sevilla, Unirational Fields of Transcendence Degree One and Functional Decomposition, Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation, ACM, 2001.
[12] G. Ivanyos, Algorithms for algebras over global field, Ph. D. thesis, Hungarian Academy of Sciences, 1996.
[13] G. Ivanyos, P. Kutas, L. Rónyai, Computing explicit isomorphisms with full matrix algebras over $\mathbb{F}_q(x)$, Found. Comput. Math. 18 (2018) 381–397.
[14] G. Ivanyos, P. Kutas, L. Rónyai, Explicit equivalence of quadratic forms over $\mathbb{F}_q(t)$, Finite Fields Appl. 55 (2019) 33–63.
[15] G. Ivanyos, L. Rónyai, J. Schicho, Splitting full matrix algebras over algebraic number fields, J. Algebra 354 (2012) 211–223.
[16] R. Johannesson, K. Zigangirov, Fundamentals of Convolutional Coding, IEEE Series on Digital & Mobile Communication, IEEE Press, New York, 1999.
[17] I. Reiner, Maximal Orders, Academic Press, London, 1975.
[18] J. Rosenthal, R. Smarandache, Maximum distance separable convolutional codes, Appl. Algebra Eng. Commun. Comput. 10 (1999) 15–32.
[19] M-F. Vignéras, Arithmétique des Algèbres de Quaternions, LNM, vol. 800, Springer, 1980.
[20] D. Wan, Generators and irreducible polynomials over finite fields, Math. Comput. 66 (1997) 1195–1212.