Selfdual skew cyclic codes

Xavier Caruso, Fabrice Drain

Selfdual skew cyclic codes

Xavier Caruso & Fabrice Drain

June 13, 2023

Abstract

Given a finite extension $\mathbf{K}/\mathbf{F}$ of degree r of a finite field $\mathbf{F}$ in characteristic p, we enumerate all selfdual skew cyclic codes in the Ore quotient ring $\mathbf{E}_k := \mathbf{K}[X^{\pm 1}; \theta]/(X^{kr} - 1)$ for any positive integer k coprime to the characteristic p. We use a new approach based on vector space duality, which establishes an order reversing and orthogonality preserving bijection between skew codes and vector subspaces. Finally we implement this enumeration in SageMath.

Contents

1 Introduction **2**

2 Insight for future work on the inseparable case **3**

3 General definitions and notations **4**

3.1 Definitions in finite geometry 4

3.2 Notations 5

4 Skew cyclic codes **6**

5 On the semisimple algebra $\mathbf{E}_k$ **7**

5.1 Semi-simplicity of the algebra $\mathbf{E}_k$ 7

5.2 The evaluation isomorphism $\mathcal{J}_l$ 8

5.3 Adjunction on $\mathbf{E}_k$ 10

6 Vector space duality **16**

7 Enumeration of selfdual skew cyclic codes **18**

7.1 Counting selfdual skew cyclic codes 18

7.2 Enumerating selfdual skew cyclic codes 26

8 SageMath enumeration of selfdual skew codes **34**

8.1 SageMath computation of cyclic or negacyclic codes 35

8.2 SageMath iteration time for the enumeration of selfdual skew codes 36

A Enumeration of inseparable selfdual skew cyclic codes **42**

A.1 Counting selfdual skew separable twisted codes 42

A.2 Enumeration of inseparable selfdual skew cyclic codes 43

A.3 SageMath enumeration of inseparable selfdual skew cyclic codes 46

1 Introduction

Among linear codes, cyclic codes enjoy a rich algebraic structure as they are defined as ideals of quotient polynomial ring. It endows them with good properties (encoding, decoding, duality, dimension, distance, length). Coding theorists are searching for generalizations that preserve these good properties. In this paper, following the paper of D. Boucher, W. Geiselmann and F. Ulmer from 2006 [BGU06], we generalize cyclic codes by considering left ideals in Ore polynomial rings rather than in polynomial rings. We thus obtain a much larger class of linear codes called skew cyclic codes. In our study, we will focus on the selfdual property of these codes.

For a finite extension $\mathbf{K}/\mathbf{F}$ of finite field of degree r, we define the Ore Laurent polynomial ring $\mathbf{K}[X^{\pm 1};\theta]$ as the quotient of the free $\mathbf{K}$-algebra $\mathbf{K}\langle X\rangle$ by the noncommutative relation: $\forall k \in \mathbf{K},\ X.k = \theta(k).X$, where θ is the Frobenius automorphism of $\mathbf{K}/\mathbf{F}$. The center of this algebra being $\mathbf{F}[X^{\pm r}]$, in particular, the ideal generated by the polynomial $X^{rk}-1$ is two-sided. So we can define skew cyclic $(X^{rk}-1,\mathbf{K}/\mathbf{F})$-codes in Hamming metric as ideals of the quotient: $\mathbf{E}_k := \mathbf{K}[X^{\pm 1};\theta]/(X^{rk}-1)$. We notice that cyclic codes correspond to the special case of skew cyclic codes where $r = 1$.

The duality of skew cyclic codes has been studied by D. Boucher among others. In her paper [Bou16], an enumeration of selfdual cyclic skew codes for $r = 2$ and q prime is given. In her subsequent article [BBB20], an enumeration of selfdual cyclic skew codes for $k = 1$, $r = n$ and q prime is provided. In both articles the duality considered is induced by the coordinatewise bilinear form on the vector space $\mathbf{K}^{rk}$: $((x_i)_{0\leqslant i<rk},(y_i)_{0\leqslant i<rk}) \mapsto \sum_{0\leqslant i<rk} x_i y_i$. In their conclusions, the papers suggest to further enumerate all selfdual skew cyclic codes for any values of the order r, the degree k and the finite base field $\mathbf{F}$. In our paper, we give a complete answer to this question in the separable case, where k is coprime to the characteristic of $\mathbf{F}$.

For the purpose of stating our main results, we note $\prod_{1\leqslant l\leqslant n} \mathbf{F}_l$ the decomposition of $\mathbf{F}[Y]/(Y^k-1)$ as a product of field extensions of $\mathbf{F}$ in an algebraic closure. We note y_l, a primitive element of $\mathbf{F}_l$ such that: $\mathbf{F}(y_l) = \mathbf{F}_l$. We note $\mathbf{K}_l := \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l$. We also note τ, the involution on the index l induced by the aforementioned duality on $\mathbf{K}^{rk}$. We get the following main result.

Theorem 2 (Cf. theorem 43) There exists an explicit bijection between the set of selfdual skew cyclic codes of $\mathbf{E}_k$ and the cartesian product of sets $W_{\texttt{palindromic}} \times W_{\texttt{nonpalindromic}}$, where:

$W_{\texttt{palindromic}}$ is the cartesian product over all indexes l invariant by τ of the sets of maximal isotropic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$.

$W_{\texttt{nonpalindromic}}$ is the cartesian product over all remaining unordered pairs of indexes $(l, \tau(l))$ (verifying $l \neq \tau(l)$) of the sets of $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$.

As a byproduct, we get the following counting of selfdual skew cyclic codes of $\mathbf{E}_k$.

Theorem 3 (Cf. theorem 58) The number of selfdual skew cyclic codes of $\mathbf{E}_k$ is given by:
$$\begin{cases} \text{If } p = 2, & \prod_{\{l|l=\tau(l),y_l=\pm 1\}} \prod_{i=1}^{s} \left(q_l^i + 1\right) \prod_{\{l|l=\tau(l),y_l\neq\pm 1\}} \prod_{i=1}^{s} \left(q_l^{i+1/2} + 1\right) \prod_{\{\{l,\tau(l)\}|l\neq\tau(l)\}} \sum_{k=0}^{k=r} \frac{(q_l^r-1)\ldots\left(q_l^{r-k+1}-1\right)}{\left(q_l^k-1\right)\ldots(q_l-1)} \\ \text{If } p \neq 2, & \prod_{\{l|l=\tau(l),y_l=\pm 1\}} \prod_{i=0}^{s-1} \left(q_l^i + 1\right) \prod_{\{l|l=\tau(l),y_l\neq\pm 1\}} \prod_{i=0}^{s-1} \left(q_l^{i+1/2} + 1\right) \prod_{\{\{l,\tau(l)\}|l\neq\tau(l)\}} \sum_{k=0}^{k=r} \frac{(q_l^r-1)\ldots\left(q_l^{r-k+1}-1\right)}{\left(q_l^k-1\right)\ldots(q_l-1)} \end{cases}$$
where q_l denotes the cardinal of $\mathbf{F}_l$

Organization of the paper

In section 2, we give an insight for future work on the inseparable case.

In section 3, we give general definitions and notations used in this paper.

In section 4, we define selfdual skew codes.

In section 5, we introduce the evaluation isomorphism $\mathcal{J}_l$. For each x_l in $\mathbf{K}_l$ satisfying $Norm_{\mathbf{K}_l/\mathbf{F}_l}(x_l) = y_l$, The isomorphism $\mathcal{J}_l$ is the evaluation at $x_l\theta$ from the central simple $\mathbf{F}_l$-algebra $\mathbf{E}_k^{(l)} := \mathbf{K}_l[X^{\pm 1};\theta]/(X^r - y_l)$ to the simple matrix algebra: $End_{\mathbf{F}_l}(\mathbf{K}_l)$.

In section 6, the duality between the left ideals of the endomorphism ring and the kernels of their generators being order reversing and orthogonality preserving, we deduce from it that selfdual skew cyclic codes correspond to maximal isotropic subspaces.

In section 7, we provide enumeration algorithms for separable selfdual skew cyclic codes of the Ore quotient ring: $\mathbf{K}[X^{\pm 1};\theta]/(X^{rk} - 1)$.

In section 8, computation results are provided for skew cyclic $(X^{rk} - 1, \mathbf{K}/\mathbf{F})$-codes and skew negacyclic $(X^{rk} + 1, \mathbf{K}/\mathbf{F})$-codes for $|\mathbf{F}| \leqslant 9$, $k \leqslant 9$ and $r \in \{4, 6, 8\}$. The source code of the SageMath implementation is available at this location:

`https://plmlab.math.cnrs.fr/caruso/selfdual-skew-cyclic-codes`

In appendix A, we provided enumeration algorithms for inseparable selfdual skew cyclic codes of the Ore quotient ring: $\mathbf{K}[X^{\pm 1};\theta]/(X^{rkp^m} - 1)$.

2 Insight for future work on the inseparable case

We intend, in a future paper, to address the inseparable case using analogue methods. However, several crucial elements of the theory have to be adapted in the inseparable case:

Isotropic spaces have to be enumerated on free modules over power series rings with coefficients in a finite field, and not on finite vector spaces anymore.

The echelon matrix representation of vector spaces has to be replaced by the Iwasawa decomposition of free sub-modules over a power series ring.

Fortunately, we can easily enumerate all selfdual skew cyclic codes by multiplying properly twisted separable selfdual skew cyclic codes with each other as described and illustrated by hand of SageMath computations in the appendix A.

3 General definitions and notations

3.1 Definitions in finite geometry

Let F be a finite field and let σ be an involutive automorphism of F, we recall that a F-vector space V can be equipped with a *σ-sesquilinear form* $\mathcal{B}$ satisfying:

$$\mathcal{B}(xu, yv) = x\sigma(y)\mathcal{B}(u, v)\ \forall u, v \in V,\ \forall x, y \in F$$

We will consider the four following main types of finite geometries.
V equipped with $\mathcal{B}$ is said to be an *Euclidean* space if we have:

$$\sigma = Id \texttt{ and } \mathcal{B}(u, v) = \mathcal{B}(v, u)\ \forall u, v \in V$$

V equipped with $\mathcal{B}$ is said to be a *skew-Euclidean* space if we have:

$$\sigma = Id \texttt{ and } \mathcal{B}(u, v) = -\mathcal{B}(v, u)\ \forall u, v \in V$$

V equipped with $\mathcal{B}$ is said to be a *Hermitian* space if we have:

$$\sigma^2 = Id, \sigma \neq Id \texttt{ and } \mathcal{B}(u, v) = \rho(\mathcal{B}(v, u))\ \forall u, v \in V$$

V equipped with $\mathcal{B}$ is said to be a *skew-Hermitian* space if we have:

$$\sigma^2 = Id, \sigma \neq Id \texttt{ and } \mathcal{B}(u, v) = -\rho(\mathcal{B}(v, u))\ \forall u, v \in V$$

Moreover, the endomorphism ring of F-linear endomorphisms $End_F(V)$ is equipped with an involutive anti-automorphism $f \mapsto f^*$ characterised by:

$$\forall f \in End_F(V),\ \forall u, v \in V, \mathcal{B}(u, f^*(v)) = \mathcal{B}(f(u), v)$$

We call this involutive anti-automorphism the adjunction relative to the bilinear form $\mathcal{B}$.

We recall also that a totally isotropic subspace W of V is characterised by $W \subset W^\perp$ and that such a subspace of (maximal) dimension, half the dimension of the ambiant space, is characterised by $W = W^\perp$.

Finally a *hyperbolic pair* in V equipped with $\mathcal{B}$ is a pair of vectors $\{u, v\}$ of V satisfying $\mathcal{B}(u, u) = 0$, $\mathcal{B}(v, v) = 0$ and $\mathcal{B}(u, v) = 1$.

The 2-dimensional subspace $< u, v >$ of V spanned by a hyperbolic pair $\{u, v\}$ is called a *hyperbolic plane*.

3.2 Notations

In this paper, we will use the following notations:

- $\mathbb{F}_q$ will denote a finite field of cardinal q
- $\mathbf{F}_l$ will denote the finite field extension of $\mathbf{F}$ such that, $\prod_{1 \leqslant l \leqslant n} \mathbf{F}_l = \mathbf{F}[Y]/(Y^k - 1)$
- y_l will denote a primitive element of the finite field extension $\mathbf{F}_l/\mathbf{F}$, so that we have: $\mathbf{F}(y_l) := \mathbf{F}_l$
- q_l will denote the cardinal of $\mathbf{F}_l$.
- $\mathbf{K}_l$ will denote the finite etale $\mathbf{F}_l$-algebra $\mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l$.
- $\mathbf{E}_{k,l}$ will denote the central simple $\mathbf{F}_l$-algebra $\mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l[X; \theta]/(X^r - 1)$.
- $End_R(V)$ will denote, for any ring R and R-module V, the endomorphism ring of all R-linear endomorphisms of V.
- $Mat_{R,r\times r}$ will denote, for any ring R, the matrix ring of all $r \times r$ square matrices with entries in R.
- M^{tr} will denote the transpose of the matrix M.
- Id will denote the identity morphism.

- $\mathcal{J}_l$ will denote the evaluation isomorphism

$$\mathcal{J}_l : \begin{cases} \mathbf{K}_l[X^{\pm 1};\theta] & \xrightarrow{\sim} End_{\mathbf{F}_l}(\mathbf{K}_l) \\ X & \mapsto x_l\theta \end{cases} \tag{3.1}$$

  where $Norm_{\mathbf{K}_l/\mathbf{F}_l}(x_l) = y_l$

- f^* will denote the adjunction in $\mathbf{E}_k$ or $\mathbf{E}_k^{(l)}$.

- $f^\bullet$ will denote the adjunction in $\mathbf{E}_{k,l}$ or $End_{\mathbf{F}_l}(\mathbf{K}_l)$.

- $GL_n(F)$ will denote the general linear group of the vector space F^n over the finite field F.

- L^σ will denote the subfield of the field L fixed by the automorphism σ.

- $V^\perp$ will denote the orthogonal of a vector subspace V.

4 Skew cyclic codes

Let $\mathbf{F}$ be a finite field of cardinal q and characteristic p. Let $\mathbf{K}/\mathbf{F}$ be a finite extension of $\mathbf{F}$ of degree r. Let θ be the Frobenius automorphism of $\mathbf{K}/\mathbf{F}$: $\mathbf{x} \mapsto \mathbf{x^q}$. Let $\mathbf{K}[X^{\pm 1};\theta]$ be the corresponding Ore Laurent polynomial ring defined as the quotient of the free $\mathbf{K}$-algebra $\mathbf{K}\langle X\rangle$ by the noncommutative relation: $\forall k \in \mathbf{K}$, $X.k = \theta(k).X$, localized by the powers of X. As shown in Theorem 1.1.22 in [Jac96], the center of the Ore Laurent polynomial ring $\mathbf{K}[X^{\pm 1};\theta]$ is $\mathbf{F}[X] \bigcap \mathbf{K}[X^{\pm r}] = \mathbf{F}[X^{\pm r}]$.

Definition 4 A *skew quotient algebra* is a quotient algebra $\mathbf{K}[X^{\pm 1};\theta]/(f(X))$, where f is taken in the center $\mathbf{F}[X^{\pm r}]$.

Remark 5 As quotient ring of the left and right Euclidean domain of skew Laurent polynomials, $\mathbf{K}[X^{\pm 1};\theta]$, it is a left and right principal ideal ring.

We now turn to the definition of selfdual skew cyclic codes.

Definition 6 The *Hamming distance* on left ideals of any skew quotient algebra $\mathbf{K}[X^{\pm 1};\theta]/(P(X))$ is defined as the Hamming distance of the underlying $\mathbf{K}$-vector spaces.

Definition 7 The *skew codes* of a skew quotient algebra $\mathbf{K}[X^{\pm 1};\theta]/(P(X))$ are its left ideals seen as vector subspaces over $\mathbf{K}$ and equipped with the Hamming metric.

The *skew cyclic codes* are skew codes of a skew quotient algebra of the form $\mathbf{K}[X^{\pm 1};\theta]/(X^{kr}-1)$.

The *skew negacyclic codes* are skew codes of a skew quotient algebra of the form $\mathbf{K}[X^{\pm 1};\theta]/(X^{kr}+1)$.

The *skew constacyclic codes* are skew codes of a skew quotient algebra of the form $\mathbf{K}[X^{\pm 1};\theta]/(X^{kr}+\alpha)$ with $\alpha \in \mathbf{F}^*$.

Definition 8 Choosing for any element of $\mathbf{E}_k$ the unique lift in $\mathbf{K}[X;\theta] \subset \mathbf{K}[X^{\pm 1};\theta]$ of degree strictly less than kr defines an *isomorphism of* $\mathbf{K}$*-vector spaces*.

$$\begin{array}{ccccc} \lambda: & \mathbf{E}_k & \rightarrow & \mathbf{K}^{rk} \\ & f & \mapsto & \lambda(f) \end{array} \tag{4.1}$$

We are interested in the skew code duality for the following coordinatewise bilinear form.

Definition 9 In the canonical base of $\mathbf{K}^{rk}$, we define the *coordinatewise bilinear form* on $\mathbf{K}^{rk}$ by: $((x_i)_{0\leqslant i<rk},(y_i)_{0\leqslant i<rk}) \mapsto \sum_{0\leqslant i<rk} x_i y_i$.

We note that this bilinear form is nondegenerate.

Definition 10 The *self-orthogonal* skew codes are the skew codes I such that: $\lambda(I) \subset \lambda(I)^{\perp}$.

The *selfdual* skew codes are the skew codes I such that: $\lambda(I) = \lambda(I)^{\perp}$.

As we have $\dim(\lambda(I)) + \dim(\lambda(I)^{\perp}) = r$, a necessary condition for selfdual skew codes to exist is that r is even.

Hypothesis 11 We restrict the study in this paper to even orders $2s := r$.

5 On the semisimple algebra $\mathbf{E}_k$

5.1 Semi-simplicity of the algebra $\mathbf{E}_k$

For any nonnegative integer k, $X^{rk}-1$ is in the center. We can thus quotient the Ore Laurent polynomial ring by the two-sided ideal $(X^{rk}-1)$ to build the skew cyclic quotient algebra $\mathbf{E_k} := \mathbf{K}[X^{\pm 1};\theta]/(X^{rk}-1)$.

Proposition 12 The algebra $\mathbf{E}_k$ is semisimple in the separable case where k is coprime to p.

Proof. The detail of the following proof can be found in Proposition 20.7 in [Wis91]. The quotient $\mathbf{E}_k$ is Artinian so its Jacobson radical must be nilpotent. As k is coprime to p, $\mathbf{E}_k$ is separable and its Jacobson radical must thus be trivial. It follows that $\mathbf{E}_k$ is a semisimple algebra over $\mathbf{F}$. As it is finite-dimensional, it is a cartesian product of simple algebras over $\mathbf{F}$ which reduces by the Wedderburn theorem to a product of matrix algebras over finite, hence commutative, fields extensions of $\mathbf{F}$. □

Remark 13 In the inseparable case where k is not coprime to the characteristic p, the Jacobson radical is equal to the nilradical generated by $(X^{rk}-1)$, so $\mathbf{E_k}$ is not semisimple anymore. It is still a product of matrix algebras though, but over an Artinian $\mathbf{F}$-algebra, and not over a field $\mathbf{F}$ anymore.

Hypothesis 14 We place ourselves in the *separable case* where k is coprime to p, except in the appendix A where we treat the *inseparable case*

5.2 The evaluation isomorphism $\mathcal{J}_l$

We will show that the family of evaluation isomorphisms $(\mathcal{J}_l)_l$ where $\mathcal{J}_l$ is defined by: $\begin{cases} \mathbf{E}_k & \to End_{\mathbf{F}_l}(\mathbf{K}_l) \\ X & \mapsto x_l\theta \end{cases}$ with $Norm_{\mathbf{K}_l/\mathbf{F}_l}(x_l) = y_l$, when applied to the chinese remainder decomposition of the central semi-simple F-algebra $\mathbf{E}_k$, realizes an explicit isomorphism between $\mathbf{E}_k$ and a product of matrix algebras.

Indeed, expressing $\mathbf{E}_k$ as an $\mathbf{F}[Y]/(Y^k-1)$-algebra and decomposing Y^k-1 in a product of irreducible polynomials $P_l(Y)$ over $\mathbf{F}$, we obtain from the chinese remainder theorem:

$$\begin{aligned} \mathbf{E}_k &\simeq \mathbf{K}[Y,X;\theta]/((Y^k-1),X^r-Y) \simeq (\mathbf{K}[Y,X;\theta]/(Y^k-1))/(X^r-Y) \\ \mathbf{E}_k &\simeq \left(\mathbf{K}[Y,X;\theta]/(\prod_{1\leqslant l\leqslant n} P_l(Y))\right)/(X^r-Y) \end{aligned} \tag{5.1}$$

Noting $\mathbf{F}_l := \mathbf{F}[Y]/(P_l(Y))$, $\mathbf{K}_l := \mathbf{K}\otimes_{\mathbf{F}}\mathbf{F}_l$ $\mathbf{E}_k^{(l)} := \mathbf{K}_l[X^{\pm 1};\theta]/(X^r-y_l)$, we get the following lemma:

Lemma 15 The map:

$$\begin{array}{ccc} \mathbf{E}_k & \xrightarrow{\sim} & \prod_{1\leqslant l\leqslant n} \mathbf{E}_k^{(l)} \\ P & \mapsto & P \mod (X^r - y_l) \end{array} \tag{5.2}$$

is an isomorphism of rings.

We will now study each $\mathbf{E}_k^{(l)}$. $\mathbf{K}_l$ is a finite etale extension of the finite field $\mathbf{F}_l$, i.e. a finite product of finite extensions of $\mathbf{F}_l$. As it has finite cardinality, its norm is surjective and there exists an element x_l in $\mathbf{K}_l$ satisfying: $Norm_{\mathbf{K}_l/\mathbf{F}_l}(x_l) = y_l$, so that the evaluation isomorphism at $x_l X$ from $\mathbf{E}_{\mathbf{k}}^{(\mathbf{l})} := \mathbf{K}_l[X^{\pm 1};\theta]/(X^r - Norm_{\mathbf{K}_l/\mathbf{F}_l}(x_l))$ to $\mathbf{E}_{k,l} := \mathbf{K}_l[X^{\pm 1};\theta]/(X^r - 1)$ is well defined:

$$\begin{array}{ccc} \mathbf{E}_{\mathbf{k}}^{(\mathbf{l})} & \overset{\overline{Eval_{x_l X}}}{\rightarrow} & \mathbf{E}_{k,l} \\ P(X) & \mapsto & P(x_l X) \end{array} \tag{5.3}$$

Now we have the obvious evaluation isomorphism $X \mapsto \theta$, from $\mathbf{E}_{k,l}$ to $End_{\mathbf{F}_l}(\mathbf{K}_l)$

$$\begin{array}{ccc} \mathbf{E}_{k,l} & \overset{Eval_\theta}{\rightarrow} & End_{\mathbf{F}_l}(\mathbf{K}_l) \\ P(X) & \mapsto & P(\theta) \end{array} \tag{5.4}$$

Composing both evaluation isomorphisms and using lemma 15, we get:

Proposition 16 (see theorem 1.3.12 in [Jac96]) The evaluation map:

$$\begin{array}{cccc} (\mathcal{J}_l)_l : & \mathbf{E}_k & \overset{(Eval_{x_l\theta})_{1\leqslant l\leqslant n}}{\longrightarrow} & \prod_{1\leqslant l\leqslant n} End_{\mathbf{F}_l}(\mathbf{K}_l) \\ & P(X) & \overset{\sim}{\longmapsto} & (P(x_l\theta))_{1\leqslant l\leqslant n} \end{array} \tag{5.5}$$

is an isomorphism of central simple algebra over $\mathbf{F}_l$.

Proof. The family $(b_i X^j)_{0\leqslant i<r, 0\leqslant j<r}$ for an $\mathbf{F}_l$ base $(b_i)_{0\leqslant i<r}$ of $\mathbf{K}_l$ is a free family of $\mathbf{E}_k^{(l)}$ seen as $\mathbf{F}_l$ vector space. It has cardinality r^2. Now the evaluation morphism $Eval_{x_l\theta}$ is obviously injective on $\mathbf{E}_k^{(l)}$. So its image has dimension at least r^2. But the global dimension of $End_{\mathbf{F}_l}(\mathbf{K}_l)$ over $\mathbf{F}_l$ is exactly r^2. So the evaluation morphism $Eval_{x_l\theta}$ is surjective as well. □

Moreover we get:

Corollary 17 There is an isomorphism $\mathbf{E}_k \simeq \prod_{1 \leqslant l \leqslant n} Mat_{\mathbf{F}_l, r \times r}$.

Remark 18 To realize the evaluation isomorphism $\mathcal{J}_l$, a fast computation of preimages of the norm is needed. One possible method consists in finding an irreducible factor of the skew polynomial $X^r - y_l$ in $K_l[X;\theta]$. It is described in [CL17].

Remark 19 The evaluation isomorphism $\mathcal{J}_l$ is unique up to conjugation by an element of norm 1, i.e. up to another choice of x_l as preimage for y_l.

5.3 Adjunction on $\mathbf{E}_k$

We will now equip $\mathbf{E}_k$ with a nondegenerate bilinear form for which orthogonal left-ideals are mapped via λ to orthogonal vector spaces. We begin by defining the corresponding adjunction on $\mathbf{E}_k$. We start from the following $\mathbf{F}$-linear automorphism on $\mathbf{K}[X^{\pm 1};\theta]$

$$\begin{array}{ccc} \mathbf{K}[X^{\pm 1};\theta] & \xrightarrow{*} & \mathbf{K}[X^{\pm 1};\theta] \\ \sum_i f_i X^i & \mapsto & \sum_i X^{-i} f_i \end{array} \tag{5.6}$$

By linearity one checks on monomials that it is an anti-automorphism:

$$(f_i X^i g_j X^j)^* = (f_i \theta^i(g_j) X^{i+j})^* = X^{-(i+j)} f_i \theta^i(g_j) = X^{-j} g_j X^{-i} f_i = (g_j X^j)^* (f_i X^i)^*$$

Definition 20 We define the *adjunction* on $\mathbf{E}_k$ as the automorphism of $\mathbf{E}_k$ induced by the composition of the adjunction on $\mathbf{K}[X^{\pm 1};\theta]$ with the projection on $\mathbf{E}_k$.

$$\begin{array}{ccc} \mathbf{E}_k & \xrightarrow{*} & \mathbf{E}_k \\ \overline{\sum_i f_i X^i} & \mapsto & \overline{\sum_i X^{-i} f_i} \end{array} \tag{5.7}$$

This definition is licit because the adjunction maps the two-sided ideal $(X^{rk} - 1)$ on itself. Indeed $(X^{rk} - 1)^*$ is equal to the two-sided ideal $(X^{rk *} - 1)$ i.e. $-X^{-rk}(X^{rk} - 1)$ i.e. $(X^{rk} - 1)$. We also notice that the adjunction of $\mathbf{E}_k$, as quotient map of an anti-automorphism, is an anti-automorphism. So it maps the left ideals of $\mathbf{E}_k$ to its right ideals.

We now define a nondegenerate bilinear form corresponding to this adjunction.

Definition 21 The *reduced trace bilinear form* on $\mathbf{E}_k$ is the bilinear map sending f and g in $\mathbf{E}_k$ to $Trace_{K/F}((fg^*)(1))$ in $\mathbf{F}$.

The licitness of this definition is readily seen. It does not depend on the choice of representatives in $\mathbf{K}[X^{\pm 1};\theta]$. It is readily seen that the adjunction $f \mapsto f^*$ satisfies the adjunction characterisation relative to the reduced trace bilinear form. Indeed for any f,g,h in $\mathbf{E}_k$, we have:

$$Trace_{K/F}((f(hg)^*)(1)) = Trace_{K/F}((fg^*h^*)(1)) = Trace_{K/F}(((h^*f)g^*)(1))$$

Proposition 22 For a left ideal I of $\mathbf{E}_k$, we have $\lambda(I^\perp) = \lambda(I)^\perp$.

Proof. Let I be a left ideal of $\mathbf{E}_k$. An element g of $\mathbf{E}_k$ is orthogonal to I if and only if we have: $Trace_{\mathbf{K/F}}((fg^*)(1)) = 0$ for all elements $f \in I$. By $\mathbf{K}$-linearity, this holds if and only if we have $Trace_{\mathbf{K/F}}((\kappa fg^*)(1)) = 0$ for all elements $\kappa \in \mathbf{K}$ and all elements $f \in I$. By nondegeneration of $Trace_{\mathbf{K/F}}$, the condition becomes $(fg^*)(1) = 0$ for all elements $f \in I$. This in turn is true if and only if: $(\sum_{0\leqslant i<kr} \lambda(f)_i X^i X^{kr-i} \lambda(g)_{(kr-(kr-i))})(1) = 0$ for all elements $f \in I$ since $g^* = \sum_{0\leqslant i<kr} X^i g_{kr-i}$. Finally we obtain the orthogonality condition for the coordinatewise bilinear form on $\mathbf{K}^{rk}$: $\sum_{0\leqslant i<kr} \lambda(f)_i \lambda(g)_i = 0$ for all elements $f \in I$. □

We work with the reduced trace bilinear form rather than the coordinatewise bilinear form, so that we can induce corresponding reduced trace bilinear forms on the $\mathbf{F}_l$-algebras $\mathbf{E}_k^{(l)}$. We now describe them.

Definition 23 We say that a polynomial is *palindromic* if the set of its roots in an algebraic closure does not contain zero and is stable under the inversion map $x \mapsto \frac{1}{x}$.

Definition 24 Fixing y_l, a primitive element in $\mathbf{F}_l \simeq \mathbf{F}[Y]/(P_l(Y))$, we define the *involution* τ on the index set $\{1,\ldots,n\}$ of the chinese remainder decomposition, $F[Y]/(Y^k-1) \xrightarrow{\sim} \prod_{1\leqslant l\leqslant n} F[Y]/(P_l(Y))$, by the relation $P_{\tau(l)}(\frac{1}{y_l}) = 0$.

As the polynomial $Y^k - 1$ is palindromic, the index $\tau(l)$ exists, and τ is obviously involutive. On the other hand, we can define an involutive $\mathbf{F}$-linear automorphism σ on the ring

$\mathbf{F}[Y]/(Y^k-1)$ by:

$$\begin{array}{ccccc} \sigma: & \mathbf{F}[Y]/(Y^k-1) & \xrightarrow{\sim} & \mathbf{F}[Y]/(Y^k-1) \\ & Y & \mapsto & \frac{1}{Y} \end{array} \tag{5.8}$$

Definition 25 We induce from σ an automorphism σ_l from $\mathbf{F}_l$ to $\mathbf{F}_{\tau(l)}$ by $\sigma_l : y_l \mapsto \frac{1}{y_{\tau(l)}}$. We define also $Id \otimes \sigma_l$ as the *involutive isomorphism* from $\mathbf{K}_l$ to $\mathbf{K}_{\tau(l)}$ that acts trivially on $\mathbf{K}$ and whose restriction to $\mathbf{F}_l$ is σ_l.

The licitness of this definition is readily seen from the chinese remainder decomposition 15.

Definition 26 We define the *adjoint* of $f = \sum_i f_i X^i$ in $\mathbf{E}_k^{(l)}$ by $f^* = \sum_i X^{-i}(Id \otimes \sigma_l)(f_i)$ in $\mathbf{E}_{\mathbf{k}}^{(\tau(\mathbf{l}))}$.

Taking the adjoint mod $P_l(Y)$ is well defined as $P_l(Y)$ is central:

$$(\mathbf{E}_k^{(l)} P_l(Y))^* = P_l(Y)^* \mathbf{E}_k^{(l)*} = \mathbf{E}_k^{(l)*} P_l(Y)^* = \mathbf{E}_k^{(\tau(l))} P_{\tau(l)}(Y)$$

The definition is thus licit.

Proposition 27 The following diagram commutes:

$$\begin{array}{ccc} \mathbf{E}_k & \xrightarrow{\ *\ } & \mathbf{E}_k \\ \downarrow \wr & & \downarrow \wr \\ \prod_{1 \leqslant l \leqslant n} \mathbf{E}_k^{(l)} & \xrightarrow{\ *\ } & \prod_{1 \leqslant l \leqslant n} \mathbf{E}_{\mathbf{k}}^{(\tau(\mathbf{l}))} \end{array} \qquad \begin{array}{ccc} f & \xmapsto{\ *\ } & f^* \\ \downarrow \wr & & \downarrow \wr \\ (f(P_l(X^r)))_l & \xmapsto{\ *\ } & (f^*(P_{\tau(l)}(X^r)))_l \end{array} \tag{5.9}$$

Proof. We check the commutativity of the diagram on an arbitrary element $\sum_i f_i X^i$ of the $\mathbf{F}_l$-

algebra $\mathbf{E}_k^{(l)}$:

$$\begin{array}{ccc}
\sum_{0\leqslant i<r}\sum_{0\leqslant j_i<\deg P_l} f_i X^{i+rj_i} & \longmapsto^{*} & \sum_{0\leqslant i<r}\sum_{0\leqslant j_i<\deg P_l} X^{r(k-j_i)-i} f_i \\
\downarrow \wr & & \downarrow \wr \\
(\sum_{0\leqslant i<r}\sum_{0\leqslant j_i<\deg P_l} f_i \otimes_{\mathbf{F}} 1 X^{i+rj_i}(P_l(X^r)))_l & & (\sum_{0\leqslant i<r}\sum_{0\leqslant j_i<\deg P_l} X^{r(k-j_i)-i} f_i \otimes_{\mathbf{F}} 1(P_{\tau(l)}(X^r)))_l \\
\| & & \| \\
(\sum_{0\leqslant i<r}\sum_{0\leqslant j_i<\deg P_l} f_i \otimes_{\mathbf{F}} {y_l}^{j_i} X^i(P_l(X^r)))_l & \longmapsto^{*} & (\sum_{0\leqslant i<r}\sum_{0\leqslant j_i<\deg P_l} X^{-i}(Id\otimes\sigma_l)(f_i\otimes_{\mathbf{F}} {y_l}^{j_i})(P_{\tau(l)}(X^r)))_l \\
 & & \| \\
 & & (\sum_{0\leqslant i<r}\sum_{0\leqslant j_i<\deg P_l} X^{-i} f_i \otimes_{\mathbf{F}} {y_{\tau(l)}}^{-j_i}(P_{\tau(l)}(X^r)))_l
\end{array} \tag{5.10}$$

□

Having defined the adjunction on $\mathbf{E}_k^{(l)}$, we now determine its transformation under the evaluation isomorphism $\mathcal{J}_l$. We define the automorphism $\mathcal{Z}_l$ by:

$$\begin{array}{ccccc}
\mathcal{Z}_l: & \mathbf{E}_{k,l} & \xrightarrow{\sim} & \mathbf{E}_{k,l} \\
 & X & \mapsto & x_l.(Id\otimes\sigma_{\tau(l)})(x_{\tau(l)}).X
\end{array} \tag{5.11}$$

In order to make the diagram 5.13 commutative, we have to twist the adjunction $*$ on the target side into an adjunction $x\mapsto x^\bullet := \mathcal{Z}_l(x^*)$ using the additional automorphism $\mathcal{Z}_l$, so that we have:

$$Trace(\mathcal{J}_l(\mathbf{E}_k^{(l)} f)\mathcal{J}_{\tau(l)}((\mathbf{E}_{\mathbf{k}}^{(\tau(\mathbf{l}))} g)^*)(1)) = 0 \iff Trace(\mathbf{E}_{k,l}\mathcal{J}_l(f)(\mathbf{E}_{k,\tau(l)}\mathcal{J}_{\tau(l)}(g))^\bullet(1)) = 0$$

where $\mathbf{E}_{k,l}$ denotes the central semi-simple algebra: $\mathbf{K}_l[X^{\pm 1};\theta]/(X^r-1)$

Lemma 28 The automorphism of $\mathbf{E}_{k,l}$, $\mathcal{Z}_l: X\mapsto x_l.(Id\otimes\sigma_{\tau(l)})(x_{\tau(l)}).X$, is the conjugation with respect to an explicit element ζ_l of $\mathbf{K}_l$

Proof. The norm of $x_l(Id\otimes\sigma_{\tau(l)})(x_{\tau(l)})$ is equal to

$$Norm_{\mathbf{K}_l/\mathbf{F}_l}(x_l)(Id\otimes\sigma_{\tau(l)})(Norm_{\mathbf{K}_{\tau(l)}/\mathbf{F}_{\tau(l)}}(x_{\tau(l)})) = y_l(Id\otimes\sigma_{\tau(l)})(y_{\tau(l)}) = 1$$

Hence the automorphism of $\mathbf{K}[X^{\pm 1};\theta]$: $X\mapsto x_l.(Id\otimes\sigma_{\tau(l)})(x_{\tau(l)}).X$ is well defined in

$\mathbf{E}_{k,l}$. The Hilbert 90 theorem guarantees the existence of an element ζ_l of $\mathbf{K}_l$ such that: $\theta(\zeta_l) = x_l(Id \otimes \sigma_{\tau(l)})(x_{\tau(l)})\zeta_l$. We have $x_l.(Id \otimes \sigma_{\tau(l)})(x_{\tau(l)}).X = \zeta_l^{-1} X \zeta_l$. □

Lemma 29 The element ζ_l can be chosen invariant by $(Id \otimes \sigma_l)$ in the palindromic case ($\tau(l) = l$).

Proof. As $(Id \otimes \sigma_l)(\zeta_l)$ satisfies $\theta((Id \otimes \sigma_l)(\zeta_l)) = x_l(Id \otimes \sigma_l)(x_l)(Id \otimes \sigma_l)(\zeta_l)$, we can take, $\zeta_l + (Id \otimes \sigma_l)(\zeta_l)$. In the special case where $\zeta_l + (Id \otimes \sigma_l)(\zeta_l)$ is equal to zero, obviously $Id \otimes \sigma_l$ is not trivial and we are in the Hermitian case where $y_l \neq \pm 1$. As $\frac{\zeta_l}{y_l}$ satisfies also $\theta(\frac{\zeta_l}{y_l}) = x_l(Id \otimes \sigma_{\tau(l)})(x_{\tau(l)})\frac{\zeta_l}{y_l}$, we can thus take $\frac{\zeta_l}{y_l} + (Id \otimes \sigma_l)(\frac{\zeta_l}{y_l}) = \zeta_l(\frac{1}{y_l} - y_l)$, which is nonzero in this case. □

Remark 30 The element ζ_l can be efficiently computed using the cohomological formula in the proof of the Hilbert 90 theorem. It is the inverse of any nonzero element in the image of the endomorphism: $\sum_{0 \leqslant i < r} \prod_{0 \leqslant j < i} \theta^j(x_l(Id \otimes \sigma_{\tau(l)})(x_{\tau(l)}))\theta^i$, as one can readily check.

Definition 31 We define the *involutive anti-isomorphism* $\bullet$ from each $\mathbf{E}_{k,l}$ into $\mathbf{E}_{k,\tau(l)}$ by composing $*$ with $\mathcal{Z}_l$.

$$\begin{array}{lccc} \mathcal{Z}_l \circ * : & \mathbf{E}_{k,l} & \stackrel{\bullet}{\to} & \mathbf{E}_{k,\tau(l)} \\ & f = \sum_i f_i X^i & \mapsto & f^\bullet = \zeta_{\tau(l)}^{-1} \sum_i X^{-i}(Id \otimes \sigma_l)(f_i)\zeta_{\tau(l)} \end{array} \tag{5.12}$$

Proposition 32 The following diagram commutes:

$$\begin{array}{ccc} \prod\limits_{1 \leqslant l \leqslant n} \mathbf{E}_k^{(l)} \simeq \mathbf{E}_k & \stackrel{*}{\longrightarrow} & \prod\limits_{1 \leqslant l \leqslant n} \mathbf{E}_{\mathbf{k}}^{(\tau(\mathbf{l}))} \simeq \mathbf{E}_k \\ \Big\downarrow {\scriptstyle (X \mapsto x_l.X)_l} & & \Big\downarrow {\scriptstyle (X \mapsto x_l.X)_l} \\ \prod\limits_{1 \leqslant l \leqslant n} \mathbf{E}_{k,l} & \stackrel{\bullet}{\longrightarrow} & \prod\limits_{1 \leqslant l \leqslant n} \mathbf{E}_{k,\tau(l)} \end{array} \tag{5.13}$$

Proof. By additivity, it suffices to check the commutativity on monomials κX^i. On one hand, we have: $(\kappa X^i)^* = X^{-i}(Id \otimes \sigma_{\tau(l)})(\kappa)$. The evaluation isomorphism $\mathcal{J}_l$ maps the right hand side to

$$X^{-i}(Id \otimes \sigma_{\tau(l)})(\kappa)(\prod_{0 \leqslant t < i} \theta^t(x_l))^{-1} \tag{5.14}$$

On the other hand, it maps the left hand side to $\kappa \prod_{0 \leqslant t<i} \theta^t(x_l) X^i$, whose adjoint is:

$$(x_l(Id \otimes \sigma_{\tau(l)})(x_{\tau(l)})X)^{-i}(Id \otimes \sigma_{\tau(l)})(\kappa \prod_{0 \leqslant t<i} \theta^t(x_{\tau(l)})) \tag{5.15}$$

Both terms 5.15 and 5.14 coincide. □

Definition 33 We define the *involutive isomorphism* $\bullet$ from $End_{\mathbf{F}_l}(\mathbf{K}_l)$ into $End_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)})$ by:

$$\begin{array}{ccccc} \bullet : & End_{\mathbf{F}_l}(\mathbf{K}_l) & \stackrel{\bullet}{\rightarrow} & End_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)}) \\ & f = \sum_{0 \leqslant i<r} f_i \theta^i & \mapsto & f^\bullet = \zeta_l^{-1} \sum_{0 \leqslant i<r} \theta^{-i}((Id \otimes \sigma_{\tau(l)})(f_i))\theta^{-i}\zeta_l \end{array} \tag{5.16}$$

Definition 34 We define the corresponding *trace form* over the product of the $\mathbf{F}_l$-linear vector space $\mathbf{K}_l$ with the $\mathbf{F}_{\tau(l)}$-linear vector space $\mathbf{K}_{\tau(l)}$, by:

$$(\kappa, \rho)_{\mathbf{F}_l} := Trace_{\mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l / \mathbf{F}_l}(\zeta_l . \kappa . (Id \otimes \sigma_{\tau(l)})(\rho))$$

Remark 35 We notice that this trace form is bilinear in the nonpalindromic and in the Euclidean (for $y_l = \pm 1$) palindromic case and sesquilinear in the Hermitian (for $y_l \neq \pm 1$) palindromic case.

Proposition 36 The involutive isomorphism $\bullet$ is the adjunction relative to the trace bilinear form defined in 34.

Proof. We have to check the adjunction characterisation. For any element $f := \sum_{0 \leqslant i \leqslant r-1} f_i \theta^i \in End_{\mathbf{F}_l}(\mathbf{K}_l)$, we must have $(\kappa, f(\rho))_{\mathbf{F}_l} = (f^\bullet(\kappa), \rho)_{\mathbf{F}_l}$. By r-periodicity of $(\theta^i)_{0 \leqslant i \leqslant r-1}$ and re-indexation $k \mapsto k - i$, we get:

$$\begin{array}{lcl} (\kappa, f(\rho))_{\mathbf{F}_l} & = & \sum_{0 \leqslant k \leqslant r-1} \theta^k(\zeta_l \kappa (Id \otimes \sigma_{\tau(l)})(\sum_{0 \leqslant i \leqslant r-1} f_i \theta^i(\rho))) \\ (\kappa, f(\rho))_{\mathbf{F}_l} & = & \sum_{0 \leqslant k \leqslant r-1} \theta^k(\sum_{0 \leqslant i \leqslant r-1} \zeta_l \theta^{-i}((Id \otimes \sigma_{\tau(l)})(f_i)) \frac{\theta^{-i}(\zeta_l)}{\zeta_l} \theta^{-i}(\kappa)\rho) \\ (\kappa, f(\rho))_{\mathbf{F}_l} & = & Trace_{\mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l / \mathbf{F}_l}(\zeta_l . f^\bullet(\kappa)\rho) \end{array} \tag{5.17}$$

□

Composing both isomorphisms: $X \mapsto x_l X$ and $X \mapsto \theta$, we obtain the following commutative diagram:

$$\begin{array}{ccccc} \mathbf{E}_k^{(l)} & \xrightarrow{\overline{Eval_{x_l}}_X} & \mathbf{E}_{\mathbf{y_1}} := \mathbf{K}_l[X^{\pm 1};\theta]/(X^r-1) & \xrightarrow{Eval_\theta} & \mathbf{K}_l[\theta] \simeq End_{\mathbf{F}_l}(\mathbf{K}_l) \\ \downarrow{\scriptstyle f\mapsto f^*} & & \downarrow{\scriptstyle f\mapsto f^\bullet} & & \downarrow{\scriptstyle f\mapsto f^\bullet} \\ \mathbf{E}_{\mathbf{k}}^{(\tau(\mathbf{l}))} & \xrightarrow{\overline{Eval_{x_l}}_X} & \mathbf{E}_{k,\tau(l)} := \mathbf{K}_{\tau(l)}[X;\theta]/(X^r-1) & \xrightarrow{Eval_\theta} & \mathbf{K}_{\tau(l)}[\theta] \simeq End_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)}) \end{array} \tag{5.18}$$

Finally, we state and prove the following product criterion, that will be used first in the proof of the orthogonality preservation of vector space duality and secondly for checking the validity of our symbolic computation of selfdual skew codes in SageMath.

Proposition 37 Let E be either the algebra $\mathbf{E}_k \times \mathbf{E}_k$, $\mathbf{E}_k^{(l)} \times \mathbf{E}_{\mathbf{k}}^{(\tau(\mathbf{l}))}$, $\mathbf{E}_{k,l} \times \mathbf{E}_{k,\tau(l)}$ or $End_{\mathbf{F}_l}(\mathbf{K}_l) \times End_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)})$. Let $[\_,\_]$ be the corresponding trace bilinear form, and $f \mapsto f^\star$ the corresponding adjunction. The skew codes generated by f and g in E are orthogonal if and only if we have $fg^\star = 0$ in E.

Proof. By nondegeneration of $[\_,\_]$, $fg^\star = 0$ is equivalent to: $[E, fg^\star] = 0$ By adjunction relation, the condition becomes: $[gE, f] = 0$ Since the adjunction is an isomorphism, we have: $[gEE^\star, f] = 0$ And since $[\_,\_]$ is a trace form: $[gE, fE] = 0$ □

Corollary 38 With the same notations as in Proposition 37, a skew code of E generated by an element $f \in E$, is selfdual if and only if we have $ff^\star = 0$ and $\deg(f) = s$

Remark 39 The product criterion $f^\star g = 0$ is equivalent to $g^\star f = 0$ by adjunction. It is also equivalent to $gf^\star = 0$ and $fg^\star = 0$. Indeed if we have $g^\star f = 0$, $fg^\star f$ is also equal to zero in E and by left and right divisibility, taking lifts of f and g, we obtain: $\tilde{f}\tilde{g}^\star\tilde{f} = (X^{rk}-1)\tilde{f}\tilde{h}\tilde{f}$, for some $\tilde{h}$. So by right Euclidean division by $\tilde{f}$, we get $\tilde{f}\tilde{g}^\star = (X^{rk}-1)\tilde{f}\tilde{h}$, which implies $fg^\star = 0$ in E.

6 Vector space duality

In the preceding section we reduced the problem of finding selfdual skew cyclic codes in $\mathbf{E}_k$ to that of finding selfdual skew cyclic codes in $End_{\mathbf{F}_l}(\mathbf{K}_l)$ for each index l. We will now further reduce the problem to the enumeration of maximal isotropic spaces of $\mathbf{K}_l$ for each index l. To this

end we apply the classical duality between $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ and left ideals of $End_{\mathbf{F}_l}(\mathbf{K}_l)$ [Ber] (Cf. definition of τ 24):

- In the palindromic case where $\tau(l) = l$
- In the nonpalindromic case where $\tau(l) \neq l$

Definition 40 Given a field L and any L-vector spaces W, the *vector space duality* associates to every L-vector subspace V of W, the left ideal I_V of $End_L(W)$ constituted by the endomorphisms vanishing on V. It associates dually to every left ideal I of $End_L(W)$, the L-vector subspace intersection of the kernels of the morphisms in I. This correspondence can be expressed as:

$$\begin{cases} V_I = & \bigcap_{f \in I} \ker(f) \\ I_V = & \{f \in End_{\mathbf{F}_l}(\mathbf{K}_l) | V \subset \ker(f)\} \end{cases} \tag{6.1}$$

This duality map is obviously order reversing. Moreover it is a bijective and involutive correspondence between the set of left ideals of $End_L(W)$ and the set of L-vector subspaces of W.

Lemma 41 For a Hermitian bilinear form, the orthogonal vector space of the image of $f \in End_L(V)$ is equal to the kernel of its adjoint.

Proposition 42 For any L-vector space V, and any nondegenerate bilinear form, along with its corresponding adjunction $\star$, and defined on $V \times V^\star$, we have: $I_V^\perp = I_{V^\perp}$

Proof. For $g \in End_L(V^\star)$, $\mathcal{C}_g^\perp$ is a left-submodule of $End_L(V)$. We thus have $\mathcal{C}_f = \mathcal{C}_g^\perp$ for some $f \in End_L(V)$. By the product criterion 37, this corresponds to the condition: $fg^\star = 0$. But $\{f \in End_L(V) | f \circ g^\star = 0\} = \{f \in End_L(V) | f(g^\star(L)) = 0\}$ is the left ideal vanishing on $Im(g^\star)$, i.e. on $\ker(g)^\perp$ by lemma 41. We conclude: $\mathcal{C}_g^\perp = \mathcal{C}_f = I_{\ker(g)^\perp}$. □

We can now prove the main Proposition 2.

Theorem 43 There exists an explicit bijection between the set of selfdual skew cyclic codes of $\mathbf{E}_k$ and the cartesian product of sets $W_{\texttt{palindromic}} \times W_{\texttt{nonpalindromic}}$, where:

- $W_{\texttt{palindromic}}$ is the cartesian product over all indexes l invariant by τ of the sets of maximal isotropic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$.
- $W_{\texttt{nonpalindromic}}$ is the cartesian product over all remaining unordered pairs of indexes $(l, \tau(l))$ (verifying $l \neq \tau(l)$) of the sets of $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$.

Proof. As we assumed $\dim \mathbf{K} =: r$ to be even, selfdual skew cyclic codes correspond to isotropic spaces of maximal dimension $s := r/2$. We apply the duality to the $\mathbf{F}_l$-vector spaces $\mathbf{K}_l$ with the corresponding adjunction: $\mathbf{E}_{k,l} \overset{*}{\to} \mathbf{E}_{k,\tau(l)}$ and nondegenerate bilinear form on $\mathbf{K}_l \times \mathbf{K}_{\tau(l)}$. The duality being bijective, order reversing and preserving the orthogonality relation between skew codes in $\mathbf{E}_{k,l}$ and $\mathbf{F}_l$-vector subspaces, the diagrams 5.18 and 5.9 being commutative and thus preserving the product criterion 38 for selfdual codes, selfdual skew cyclic codes of $\mathbf{E}_k$ correspond to the product of the sets constituted by the cartesian product of the sets of maximal isotropic palindromic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$, and by the cartesian product of the sets of maximal isotropic nonpalindromic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l \times \mathbf{K}_{\tau(l)}$. As in the nonpalindromic case, isotropic vector subspace of $\mathbf{K}_l \times \mathbf{K}_{\tau(l)}$ equal to their orthogonal are of the form $W \oplus W^\perp$ for some $\mathbf{F}_l$-vector subspace W of $\mathbf{K}_l$, they correspond exactly to the $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$. □

7 Enumeration of selfdual skew cyclic codes

In the preceding sections we showed that enumerating selfdual skew cyclic codes boils down to enumerating maximal isotropic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ in the palindromic case, and to enumerating $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ in the nonpalindromic case. We will now describe algorithms that fulfill this requirement.

7.1 Counting selfdual skew cyclic codes

In order to count selfdual skew cyclic codes, we introduce the q-binomial coefficients defined by:

$$\binom{n}{k}_q = \frac{(1-q^n)(1-q^{n-1})\dots(1-q^{n-k+1})}{(1-q)(1-q^2)\dots(1-q^k)}$$

where n and k are nonnegative integers. If $k > n$, this evaluates to 0. For $r = 0$, the value is 1 since both the numerator and denominator are empty products.

All of the factors in numerator and denominator are divisible by $1 - q$, and the quotient is the q-number (q-analog of an integer k):

$$[k]_q = \sum_{0 \leqslant i < k} q^i = 1 + q + q^2 + \dots + q^{k-1} = \begin{cases} \frac{1-q^k}{1-q} \text{ for } q \neq 1 \\ k \text{ for } q = 1 \end{cases} \tag{7.1}$$

Dividing out these factors gives the equivalent formula:

$$\binom{m}{r}_q = \frac{[m]_q[m-1]_q \dots [m-r+1]_q}{[1]_q[2]_q \dots [r]_q} \quad (r \leqslant m)$$

In terms of the q-factorial $[n]_q! = [1]_q[2]_q \dots [n]_q$, the formula can be stated as

$$\binom{m}{r}_q = \frac{[m]_q!}{[r]_q![m-r]_q!} \quad (r \leqslant m)$$

We will use following lemmas on q-binomials.

Lemma 44 The q-binomial coefficient $\binom{n}{k}_q$ counts the number of $\mathbb{F}_q$-vector subspaces of rank k in the ambiant $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$.

Proof. The q-binomial coefficient is equal to the number of free families of rank k on the numerator. As the denumerator is equal to the number of bases for a given $\mathbb{F}_q$-vector subspace of dimension k, the quotient is the q-binomial number expected. □

Lemma 45 There is an analog of the binomial theorem for q-binomial coefficients, known as the q-binomial theorem:

$$\prod_{k=0}^{n-1}(1+q^k t) = \sum_{k=0}^{n} q^{k(k-1)/2}\binom{n}{k}_q t^k$$

Proof. See the article of Pólya [PA71]. □

We also need the following classical theorem due to Witt.

Proposition 46 (Witt decomposition) Let F be a finite field, V a $2s$ dimensional F-vector space. Let $\mathcal{B}$ be a nondegenerate σ-sesquilinear form on V, resp. bilinear form on V. Then there exist H_i hyperbolic planes (Cf. the definition in 3), and an invariant, d, of V called the Witt index and equal to s or $s-1$, such that one has the orthogonal decomposition:

$$V \simeq \perp_{1 \leqslant i \leqslant d} H_i \perp W$$

where $\dim(W) = s - 2d$ and W does not contain any nonzero isotropic vector. The dimension of any maximal isotropic space is given by the Witt index d.

Proof. See the proof in Theorem 3.11 [Art11]. □

Remark 47 From the Witt decomposition theorem, we see that maximal isotropic spaces of dimension s exist in $\mathbf{K}_l$ if and only if the Witt index of $\mathbf{K}_l$ is s.

7.1.1 Counting selfdual skew codes in the nonpalindromic case

Proposition 48 Noting $q_l := |\mathbf{F}_l| = q^{\deg P_l}$, the number of maximal isotropic spaces in the nonpalindromic case is:

$$\sum_{k=0}^{k=r} \begin{pmatrix} r \\ k \end{pmatrix}_{q_l} = \sum_{k=0}^{k=r} \frac{(q_l^r - 1)\dots(q_l^{r-k+1} - 1)}{(q_l^k - 1)\dots(q_l - 1)}$$

Proof. Enumerating maximal selfdual ideals over $\mathbf{E}_{k,l} \times \mathbf{E}_{k,\tau(l)}$ boils down to enumerating all $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ by 43. The number of selfdual codes in such pairs $\mathbf{E}_{k,l} \times \mathbf{E}_{k,\tau(l)}$ is thus equal to the sum over all possible dimensions k from 0 to r of the numbers of vector subspaces of dimension k, which, by lemma 44, are given by the q-binomial coefficients. □

7.1.2 Explicit existence criterion for selfdual skew codes in the palindromic case

As stated by the Witt decomposition theorem 46, computing the Witt index of $\mathbf{K}_l$ provides an explicit existence condition for selfdual skew codes. For this computation, we need to introduce the notion of discriminant of a finite etale algebra over its base field.

Definition 49 We recall that the *discriminant* $\delta_{\mathbf{K}_l/\mathbf{F}_l}$ *of the finite etale* $\mathbf{F}_l$*-algebra* $\mathbf{K}_l$ is given by $\det\left(Trace_{\mathbf{K}_l/\mathbf{F}_l}(e_i e_j)\right)_{i,j}$ modulo squares in $\mathbf{F}_l^*$, where (e_i) is a base of the $\mathbf{F}_l$-vector space $\mathbf{K}_l$.

We also define the *discriminant* δ_{ζ_l} *of the finite etale* $\mathbf{F}_l$*-algebra* $\mathbf{K}_l$ *for the trace bilinear form that we defined on* $\mathbf{K}_l$ as $\det\left(Trace_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l e_i e_j)\right)_{i,j}$ modulo squares in $\mathbf{F}_l^*$.

This definition does not depend on the choice of the base (e_i). Indeed, given any base change matrix M, we get:

$$\left(Trace_{\mathbf{K}\otimes_{\mathbf{F}}\mathbf{F}(y_l)/\mathbf{F}(y_l)}(\zeta_l M(e_i)M(e_j))\right)_{i,j} = \left(\sum_{l,m} {M^{\mathsf{tr}}}_{i,l}\, Trace_{\mathbf{K}\otimes_{\mathbf{F}}\mathbf{F}(y_l)/\mathbf{F}(y_l)}(\zeta_l e_l e_m) \sum_{m,j} M_{m,j}\right)_{i,j}$$

And on the other hand we have $\det(M)\det(M^{\mathsf{tr}}) = 1$ in $\mathbf{F}(y_l)^*/\left(\mathbf{F}(y_l)^*\right)^2$.

We have the following classical existence criterion on (maximal) isotropic subspace of dimension s:

Proposition 50 We assume $\sigma_l(y_l) = y_l$ and $p \neq 2$. Then there exists an isotropic subspace of dimension s in $\mathbf{K}_l$ if and only if $(-1)^s \delta_{\zeta_l}$ is a square in $(\mathbf{F}_l)^*$.

Proof. For sake of completeness, we recall the proof. By Witt decomposition theorem 46 applied to our quadratic form, the maximal isotropic spaces of dimension s exist if and only if the Witt

index is s. If this is the case, then obviously δ_{ζ_l} is congruent to $(-1)^s$, as one can check by computing the discriminant of the matrix representing the bilinear form in a base constituted by hyperbolic pairs (Cf. 3):

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

If this is not the case, then δ_{ζ_l} cannot be congruent to $(-1)^s$. Indeed restricted to the last nonhyperbolic hyperplane of the Witt decomposition, the matrix representing the symmetric bilinear form in a suitable base has the form: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ if $\delta_{\zeta_l} \cong (-1)^s$. But it is readily seen that this defines a subspace having nontrivial isotropic vectors, which contradicts the assumption on the Witt index. □

We can make this criterion explicit by effectively computing -1 and δ_{ζ_l} in $\mathbf{F}_l^*/(\mathbf{F}_l^*)^2$.

Lemma 51 -1 is a square in $\mathbf{F}_l^*$ if and only if $p \equiv 1(4)$ or $[\mathbf{F}_l : \mathbb{F}_p]$ is even.

Proof. If $p \equiv 1(4)$ or $[\mathbf{F}_l : \mathbb{F}_p]$ is even, $\mathbf{F}_l^*$ has an element of order 4, so there is an element different from 1 and -1 such that $x^4 = 1$, i.e, $(x^2-1)(x^2+1) = 0$, hence $x^2 + 1 = 0$. One checks the reciprocal assertion. □

Lemma 52 The discriminant δ_{ζ_l} is equal to $Norm_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)\delta_{\mathbf{K}_l/\mathbf{F}_l}$.

Proof. Noting $\mathrm{Mat}(\zeta_l)$ the matrix representing the multiplication by ζ_l in the base (e_i) and $\mathrm{Mat}(\zeta_l)^{\mathsf{tr}}$ its transpose, we get:

$$\det\left(\sum_l \mathrm{Mat}(\zeta_l)^{\mathsf{tr}}{}_{i,l}\, Trace_{\mathbf{K}_l/\mathbf{F}_l}(e_l e_j)\right)_{i,j} = det(\mathrm{Mat}(\zeta_l)^{\mathsf{tr}})\delta_{\mathbf{K}_l/\mathbf{F}_l} = Norm_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)\delta_{\mathbf{K}_l/\mathbf{F}_l}$$

□

Lemma 53 The discriminant $\delta_{\mathbf{K}_l/\mathbf{F}_l}$ is a square in $\mathbf{F}_l^*$ if and only if the Galois group of $\mathbf{F}_l/\mathbf{F}$ is a subgroup of the alternating group, i.e. if and only if the degree of the extension $[\mathbf{F}_l : \mathbb{F}_p]$ is odd.

Proof. The proof can be found in Corollary 4.2 from [Mil20]. □

In addition $Norm_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)$ can also be computed.

Lemma 54 The norm $Norm_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)$ is a square in $\mathbf{F}_l^*$ if and only if $y_l = 1$.

Proof. We have:

$$Norm_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)^{\frac{q-1}{2}} = (\zeta_l^{\sum_{0\leqslant i<2s} q_l^i})^{\frac{q-1}{2}}$$

Moreover, as $2s$ is even we have:

$$(\zeta_l^{\sum_{0\leqslant i<2s} q_l^i})^{\frac{q-1}{2}} = (\zeta_l^{q-1})^{\frac{\sum_{0\leqslant i<2s} q_l^i}{2}} = (x_l(Id\otimes\sigma_l)(x_l))^{\frac{\sum_{0\leqslant i<2s} q_l^i}{2}}$$

Using the chinese remainder isomorphism between $\mathbf{K}_l/\mathbf{F}_l$ and a product of $\mathbf{F}_l$-field extensions:

$$\begin{array}{ccc} \mathbf{K}_l & \xrightarrow{\sim} & \prod_i \mathbf{L}_{l,i} \\ x_l & \mapsto & (x_{l,i})_i \end{array} \tag{7.2}$$

The Frobenius automorphism generates the cyclic Galois group of each $\mathbf{L}_{l,i}$. Thus for a palindromic index i (satisfying $\tau(i) = i$), $Id\otimes\sigma_l$ induces the following involutive mapping: $Id\otimes\sigma_{l,i} : x_{l,i} \mapsto x_{l,i}^{q_l^{n_i}}$ for some positive integers n_i. For nonpalindromic indexes i (satisfying $\tau(i) \neq i$), $Id\otimes\sigma_l$ induces the following involutive mapping: $Id\otimes\sigma_{l,i} : x_{l,i} \mapsto x_{l,\tau(i)}$ for some element $x_{l,\tau(i)} \in \mathbf{L}_{l,\tau(i)}$. As these nonpalindromic terms can be grouped by products of identical pairs in $\mathbf{L}_{l,i} \times \mathbf{L}_{l,\tau(i)}$, we get

$$(x_l(Id\otimes\sigma_l)(x_l))^{\frac{\sum_{0\leqslant i<2s} q_l^i}{2}} \mapsto ((x_{l,i}^{\frac{\sum_{0\leqslant i<2s} q_l^i + \sum_{0\leqslant i<2s} q_l^{n_i} q_l^i}{2}})_{\texttt{palindromic } i}, (x_{l,\tau(i)}^{2\frac{\sum_{0\leqslant i<2s} q_l^i}{2}}, x_{l,i}^{2\frac{\sum_{0\leqslant i<2s} q_l^i}{2}})_{\texttt{nonpalindromic } \{i,\tau(i)\}})$$

On the other hand, for palindromic indexes, by $2s$-periodicity of θ, we have $x_{l,i}^{\sum_{0\leqslant i<2s} q_l^i} = x_{l,i}^{\sum_{n_i\leqslant i<2s+n_i} q_l^i}$. So we get $x_{l,i}^{\frac{\sum_{0\leqslant i<2s} q_l^i + \sum_{0\leqslant i<2s} q_l^{n_i} q_l^i}{2}} = x_{l,i}^{\sum_{0\leqslant i<2s} q_l^i}$. Since the chinese remainder isomorphism maps y_l i.e. $Norm_{\mathbf{K_l}/\mathbf{F}_l}(x_l)$ to $(x_{l,i}^{\sum_{0\leqslant i<2s} q_l^i})_i$, we get in the end $Norm_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)^{\frac{q-1}{2}} = y_l$.

We deduce from this equality and Euler's criterion that the norm $Norm_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)$ is a square in $\mathbf{F}_l^*$, if and only if $y_l = 1$. □

Corollary 55 When k is even, there are no selfdual skew cyclic codes in $\mathbf{E}_k$.

Proof. If k is even, $\mathbf{E}_k$ factors as follows:

$$\mathbf{E}_k \simeq \prod_{l, P_l(\pm 1)!=0} (\mathbf{K}[Y]/(P_l(Y))[X;\theta])/(X^r - Y) \times \mathbf{K}[X^{\pm 1};\theta]/(X^r+1) \times \mathbf{K}[X^{\pm 1};\theta]/(X^r-1)$$

So there are no selfdual skew codes in $\mathbf{K}[X^{\pm 1};\theta]/(X^r+1) \times \mathbf{K}[X^{\pm 1};\theta]/(X^r-1)$. Indeed, noting l_{-1} the index corresponding to the root -1 of $Y^k - 1$, we have: $\delta_{l_{-1}} = Norm_{\mathbf{K}_{l_{-1}}/\mathbf{F}_{l_{-1}}}(\zeta_{l_{-1}})\delta_{\mathbf{K}_{l_{-1}}/\mathbf{F}_{l_{-1}}}$ where $\zeta_{l_{-1}}$ satisfies: $\theta(\zeta_{l_{-1}}) = x_{l_{-1}}(Id \otimes \sigma_l)(x_{l_{-1}})\zeta_{l_{-1}}$, $x_{l_{-1}}$ satisifies $Norm_{\mathbf{K}_{l_{-1}}/\mathbf{F}_{l_{-1}}}(x_{l_{-1}}) = -1$. As shown in the lemma 54: $Norm_{\mathbf{K}_{l_{-1}}/\mathbf{F}_{l_{-1}}}(\zeta_{l_{-1}})$ is not a square in $\mathbf{F}^*_{l_{-1}}$. So $\delta_{\mathbf{K}_{l_{-1}}/\mathbf{F}_{l_{-1}}}$ and $\delta_{l_{-1}}$ cannot be squares in $\mathbf{F}^*_{l_{-1}}$ simultaneously and we can conclude by proposition 50. □

The following tables summarize the results we can deduce from Proposition 50 and Lemmas 51, 52, 53, 54

In the Euclidean case, i.e. for $y_l = \pm 1$:

	$[\mathbf{F} : \mathbb{F}_p]$ even	$[\mathbf{F} : \mathbb{F}_p]$ odd
s even	False	True
s odd	False	$p \equiv 3(4)$

In the Hermitian case, i.e. for $y_l \neq \pm 1$:

	$[\mathbf{F} : \mathbb{F}_p]$ even	$[\mathbf{F} : \mathbb{F}_p]$ odd
s even	True	False
s odd	True	$p \equiv 1(4)$

In the Hermitian case:

	$[\mathbf{F}_l : \mathbb{F}_p]$ always even
s even or odd	True

7.1.3 Counting selfdual skew codes in the palindromic case

When maximal isotropic spaces exist in an ambiant $\mathbb{F}_q$-vector space, their number is given by Segre's formulas [Seg59] [Ple65] [Ann09].

Proposition 56 Number $\mathcal{I}so_d$ of maximal isotropic spaces of dimension d:

In the Euclidean case, i.e. for $y_l = \pm 1$:

$$\begin{cases} \text{In even characteristic: } \mathcal{I}so_d = \prod_{i=1}^{d} \left(q^i + 1\right) \\ \text{In odd characteristic: } \mathcal{I}so_d = \prod_{i=0}^{d-1} \left(q^i + 1\right) \end{cases} \tag{7.3}$$

In the Hermitian case, i.e. for $y_l \neq \pm 1$:

$$\begin{cases} \text{In even characteristic: } \mathcal{I}so_d = \prod_{i=1}^{d} \left(q^{i+1/2}+1\right) \\ \text{In odd characteristic: } \mathcal{I}so_d = \prod_{i=0}^{d-1} \left(q^{i+1/2}+1\right) \end{cases} \tag{7.4}$$

For sake of completeness, we recall the proof in odd characteristic. We need the following lemma.

Lemma 57 Number $\mathcal{I}soVect_d$ of isotropic vectors in an ambiant $\mathbb{F}_q$-vector space in odd characteristic:

In the Euclidean case: $\mathcal{I}soVect_d = (q^d-1)(q^{d-1}+1)$

In the Hermitian case: $\mathcal{I}soVect_d = (q^d-1)(q^{d-1+1/2}+1)$

Proof. In odd characteristic, given an isotropic base $((u_i)_{0\leqslant i<d}, (v_i)_{0\leqslant i<d})$ corresponding to the Witt decomposition 46 of the ambiant space of dimension $2d$, in d hyperplanes $H_i :=< u_i, v_i >$ such that $\mathbf{F}_l^{2s} \simeq \oplus_{0\leqslant i<d} H_i$, an isotropic vector $((a_i)_{0\leqslant i<d}, (b_i)_{0\leqslant i<d})$ verifies:

In the Euclidean case: $\sum a_i b_j = 0$.

In the Hermitian case: $\sum \sigma_l(a_i) b_i + \sum a_i \sigma_l(b_i) = 0$. This corresponds to independant equations $\sum a_i \sigma_l(b_i) = \alpha$, for any anti-invariant α, i.e. satisfying $\sigma_l(\alpha) = -\alpha$.

Hence we have the following counting.

In the Euclidean case, given a nonzero vector y, x lies in a hyperplane of the vector space $\mathbf{F}_l^d$. We thus have $(q_l^d-1)q_l^{d-1}$ solutions for y nonzero and (q_l^d-1) additional non trivial solutions for y equal to zero. Finally we get $\mathcal{I}soVect_d = (q_l^d-1)(q_l^{d-1}+1)$ nonzero isotropic vectors in the ambiant space.

In the Hermitian case, a hyperplane over $\mathbf{F}_l$, has cardinal q_l^{d-1}, and the number of anti-invariant scalars in $\mathbf{F}_l$ is $q_l^{1/2}$ (q_l is indeed a square because P_l is palindromic and thus its roots can be counted pairwise in the Hermitian case). Hence given a nonzero vector y, we have $(q_l^d-1)q_l^{d-1+1/2}$ solutions for y nonzero and (q_l^d-1) additional non trivial solutions for y equal to zero as in the Euclidean case. Finally we get $\mathcal{I}soVect_d = (q_l^d-1)(q_l^{d-1+1/2}+1)$ nonzero isotropic vectors. □

Proof. (Segre's formulas) We start with an empty family u of isotropic vectors of the ambiant space. At each step d from 0 to $s-1$ we pick an arbitrary isotropic vector among $\mathcal{I}soVect_{s-d}$ possibilities (as defined in 57) in the orthogonal complement of the isotropic space spanned by the family u and append it to the family. It is readily seen that the family u is free and totally

isotropic. Once we have obtained a maximal isotropic family, Witt's decomposition theorem ensures that its rank, the Witt index, is an invariant equal to s. The number of maximal isotropic bases is thus equal to the product $\mathcal{P} : \prod_{1\leqslant d\leqslant s} \mathcal{I}soVect_d$ (as defined in 57). The general linear group of $GL_s(\mathbb{F}_q)$ acting freely and transitively on these maximal isotropic bases, the maximal iostropic spaces correspond exactly to its orbits. Dividing $\mathcal{P}$ by the cardinal of $GL_s(\mathbb{F}_q)$, $\prod_{i=1}^{s}(q_l^i-1)$ we thus obtain Segre's formula stated above. □

Corollary 58 We apply Proposition 56 to our situation. The global number $\mathcal{N}$ of selfdual skew cyclic codes in $\mathbf{E}_k$ is equal to the product of the numbers of maximal isotropic spaces V_l of dimension $s = r/2$ in palindromic $\mathbf{K}_l$, $\mathcal{N}_{V_l}$, times the product of the numbers of arbitrary subspaces W_l over pairs of nonpalindromic spaces, $\mathcal{N}_{W_l}$.

$$\mathcal{N} = |\{\prod_{\{l|l=\tau(l)\}} \mathcal{N}_{V_l} \times \prod_{\{\{l,\tau(l)\}|l\neq\tau(l)\}} \mathcal{N}_{W_l} | W_l \text{ arbitrary}, V_l \text{ maximal isotropic}\}|$$

In a condensed form, we obtain the following number of selfdual skew cyclic codes in $\mathbf{E}_k$:

$$\prod_{\{l|l=\tau(l),y_l=\pm1\}} \prod_{i=0}^{s-1}\left(q_l^i+1\right) \prod_{\{l|l=\tau(l),y_l\neq\pm1\}} \prod_{i=0}^{s-1}\left(q_l^{i+1/2}+1\right) \prod_{\{\{l,\tau(l)\}|l\neq\tau(l)\}} \sum_{k=0}^{k=r} \frac{(q_l^r-1)\dots(q_l^{r-k+1}-1)}{(q_l^k-1)\dots(q_l-1)}$$

Example 59 For $\mathbf{K}=\mathbb{F}_{3^{2s}}$, $\theta : x \mapsto x^3$ and $\mathbf{K}^\theta = \mathbb{F}_3$, the number of selfdual skew cyclic codes grows as $\mathcal{O}(q^{s(s-1)/2})$ as s grows larger, whereas the number of skew cyclic codes (number of s dimensional $\mathbb{F}_3$-vector subspaces of $\mathbb{F}_{3^{2s}}$) grows as $\mathcal{O}(q^{s^2})$ as s grows larger.

For $\mathbf{K}=\mathbb{F}_{3^6}$, $\theta : x \mapsto x^3$ and $\mathbf{K}^\theta = \mathbb{F}_3$, the number of selfdual skew cyclic codes in $\mathbf{E}_1 = \mathbf{K}[X;\theta]/(X^6-1)$ is: 80 among 33880 skew codes, whereas for $\mathbf{K}=\mathbb{F}_{3^{18}}$, $\theta : x \mapsto x^3$ and $\mathbf{K}^\theta = \mathbb{F}_3$, the number of selfdual skew cyclic codes in $\mathbf{E}_1 = \mathbf{K}[X;\theta]/(X^{18}-1)$ is: 469740602936729600 among 791614563787525746761491781638123230424 skew codes.

Remark 60 We recover also the number of selfdual cyclic codes from the case $r=1$ in Segre's formula. We observe that, as we are in the separable case, $(X-1)$ is always a palindromic factor of (X^k-1) of multiplicity 1. Thus there exist no selfdual cyclic codes at all in the separable case in $\mathbb{F}_p[X]/(X^k-1)$. With regard to this fact, skew cyclic codes enjoy much more dual symmetries than cyclic codes. Nethertheless, the ratio of the number of skew cyclic codes over selfdual skew cyclic codes increases as fast as $\mathcal{O}(q^{\frac{s^2+s}{2}})$ as s grows larger. The best ratio is obtained for $s=1$, and $q=3$, in odd characteristic. In this case, half of the skew cyclic codes are selfdual skew cyclic codes.

7.2 Enumerating selfdual skew cyclic codes

As we have to enumerate very large numbers of selfdual skew cyclic codes, we shall first ensure that our enumeration algorithms return uniformly distributed codes among all possible selfdual skew cyclic codes. Secondly we shall provide an iterative algorithm, that returns a new code at each iteration, with a low and constant complexity at each iteration. We use the keyword *next* to denote the operation which returns the next result on an iterator and *yield*, the operation that returns a generator object, to be iterated.

7.2.1 Enumeration in the nonpalindromic case

Let $W_0 \times W_0^{\perp}$ be the ambiant Hermitian vector space. We want to enumerate all totally isotropic vector subspaces of $W_0 \times W_0^{\perp}$ of maximal dimension $2s$.

Algorithm 61 Enumeration of selfdual skew codes in the nonpalindromic case

Input: Iterator I on all reduced echelon matrix A of size $(s, 2s)$, Nonpalindromic polynomial P_l generating the two-sided ideal in the skew cyclic algebra $\mathbf{E}_{k,l}$, the skew cyclic algebra $\mathbf{E}_k$

Output: h is the next selfdual skew codes

1: $A \leftarrow$ next I
2: $V \leftarrow \ker(A)$
3: $(e_i)_i \leftarrow$ base of V
4: $f \leftarrow \text{leftlcm}((e_i)_i)$ in $K_l[X;\theta]/(P_l)$
5: $g \leftarrow P_l.\text{right\_quo\_rem}(f)$
6: $g_{star} \leftarrow g^{\bullet}$
7: $\tilde{f} \leftarrow$ lift of f in $\mathbf{E}_k$
8: $\tilde{g_{star}} \leftarrow$ lift of g_{star} in $\mathbf{E}_k$
9: $h \leftarrow \text{leftlcm}(f, g_{star})$ in $\mathbf{E}_k$
10: yield h

Proof. For any element f in $\mathbf{E}_{k,l}$, the elements h in $\mathbf{E}_{k,l}$ satisfying $f.h = 0$ constitute a right ideal generated by an element $g^{\bullet}$. It is clear from proposition 42 that selfdual skew codes are the codes (I_f, I_g) for any f in $\mathbf{E}_{k,l}$. So the enumeration reduces to that of $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$. We proceed to the latter enumeration using the bijection between $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$, and reduced echelon matrices of dimension s over $2s$ with entries in $\mathbf{F}_l$. □

7.2.2 Enumeration in the palindromic case in odd characteristic

Let W_0 be the ambiant Hermitian vector space whose Witt decomposition 46 is given by: $W_0 \simeq \oplus_{1 \leqslant i \leqslant s} H_i$, where H_i are hyperbolic planes (Cf. the definition in 3). We want to enumerate all totally isotropic vector subspaces of W_0 of maximal dimension s.

Algorithm 62 Direct sum decomposition of hyperbolic planes in the Hermitian case

Input: W_0: The ambiant Hermitian vector space

Output: U,V build a uniformly random direct sum decomposition of hyperbolic planes

1: $U, V, W \leftarrow [], [], W_0$
2: **while** $W \neq 0$ **do**
3: Pick two random vectors u and v in W
4: **if** $< u, v > \neq 0$ and (u, v) is free **then**
5: Solve the equation $(\mathcal{E}) < u + \lambda v, u + \lambda v >= 0$ for λ (Hermitian quadratic equation)
6: $u \leftarrow u + \lambda v$
7: $u \leftarrow u - \lambda v$
8: Solve $< u, \nu v >= 1$ for ν (linear)
9: $v \leftarrow \nu v$, now (u, v) is a hyperbolic pair
10: $U \leftarrow U + [u]$, $V \leftarrow V + [v]$
11: $W \leftarrow < U, V >^{\perp} \subset W_0$
12: **end if**
13: **end while**

Proposition 63 The algorithm terminates with probability 1 and if it terminates, it is correct

We need the following lemmas to determine the probability for the quadratic equation at line 5 of the algorithm 62 to be solvable and to solve it when it is possible.

Lemma 64 Picking then two random vectors u and v that are not collinear in W of dimension $2d$ and such that $< u, v > \neq 0$ is an event of probability $\frac{({q_l}^{2d}-1)(q_l^{2d}-q_l^{2d-1})}{{q_l}^{4d}}$. Moreover this probability is always greater than $\frac{3}{8}$

Proof. This is the number of pairs of vectors with a first nonzero vector and another vector not contained in the hyperplane defined by the equation $< u, v >= 0$, divided by the number of pairs of vectors in $\mathbf{F}_l^{2d}$. Moreover, the probability increases with q_l and d, and its value at $q_l = 2$ and $d = 1$ is $\frac{3}{8}$. □

Lemma 65 (Cf. 5) The equation $(\mathcal{E}) < u+\lambda v, u+\lambda v >= 0$ has a solution in λ for any vector u and v in the ambiant Hermitian vector space. Denoting $Norm^{-1}_{\mathbf{F}_l/\mathbf{F}_l^{\sigma_l}}(x)$ a preimage by the norm map of the element x, a solution is given by the formula:

$$\lambda = \frac{Norm^{-1}_{\mathbf{F}_l/\mathbf{F}_l^{\sigma_l}}\left(\frac{N(<u,v>)}{<v,v>}(\frac{N(<u,v>)}{<v,v>} - < u,u >)\right) - \frac{N(<u,v>)}{<v,v>}}{< v,u >}$$

Proof. $(\mathcal{E})$ can be rewritten as $< u,u > + Trace_{\mathbf{F}_l/\mathbf{F}_l^{\sigma_l}}(\lambda < v,u >) + Norm_{\mathbf{F}_l/\mathbf{F}_l^{\sigma_l}}(\lambda) < v,v >= 0$
Noting $\mu := \lambda < v,u >$, $N(x) := Norm_{\mathbf{F}_l/\mathbf{F}_l^{\sigma_l}}(x)$, $Tr(x) := Trace_{\mathbf{F}_l/\mathbf{F}_l^{\sigma_l}}(x)$ and $\alpha := \mu + \frac{N(<u,v>)}{<v,v>}$, it follows:
$N(\mu) = (\alpha - \frac{N(<u,v>)}{<v,v>})(\sigma_l(\alpha) - \frac{N(<u,v>)}{<v,v>})$
$N(\mu) = N(\alpha) - \frac{N(<u,v>)}{<v,v>}Tr(\alpha) + (\frac{N(<u,v>)}{<v,v>})^2$
$Tr(\mu) = Tr(\alpha) - 2\frac{N(<u,v>)}{<v,v>}$
Injecting the trace and norm of μ in $(\mathcal{E})$, we obtain:
$(\mathcal{E}) \iff < u,u > + Tr(\alpha) - 2\frac{N(<u,v>)}{<v,v>} + (N(\alpha) - \frac{N(<u,v>)}{<v,v>}Tr(\alpha) + (\frac{N(<u,v>)}{<v,v>})^2)\frac{<v,v>}{N(<u,v>)} = 0$
$(\mathcal{E}) \iff N(\alpha) = \frac{N(<u,v>)}{<v,v>}(\frac{N(<u,v>)}{<v,v>} - < u,u >)$
One can solve this last equation for α per surjectivity of the norm. □

Proof. (of Proposition 63) We initialize W to $W_0 := \mathbf{K}_l$. We pick two random vectors u and v that are not collinear in W of dimension $2d$ and such that $< u,v >\neq 0$.

Either u and v are both isotropic and they can be renormalized into a hyperbolic pair (Cf. 3). Indeed by surjectivity of the norm, there exist an element $\alpha \in \mathbf{F}_l$ such that $< u,v >= \alpha\sigma_l(\alpha)$, so that $(\frac{u}{\alpha}, \frac{v}{\alpha})$ is a hyperbolic pair.

Or one of them is not isotropic, say v (wlog), so that $< v,v >\neq 0$. In this latter case we solve the equation $(\mathcal{E})$ for λ and replace u by $u+\lambda v$ and v by $u-\lambda v$, building as previously a hyperbolic pair.

We then append the hyperbolic plane $< u,v >$ to the growing direct sum of hyperbolic planes $< U,V >$ and take its orthogonal W' in W_0. Using Witt decomposition 46, we get $W' \simeq \oplus_{1\leqslant i\leqslant d-1} H_i$, so we can reset W to W' and repeat the process until W is equal to zero. Witt decomposition theorem 46, guarantees that this process ends properly and that we end up with a direct sum of hyperbolic planes. Finally at each step the hyperbolic plane picked is uniformly distributed among all available hyperbolic planes, the set of available hyperbolic planes has a constant cardinal and it is itself uniformly distributed relatively to the last picked

hyperbolic plane (by Witt decomposition 46), so the final direct sum of hyperbolic planes obtained is uniformly distributed as well. □

Mean complexity 66 The mean complexity $\mathcal{C}$ in s of the algorithm is less than a constant times the complexity of taking the orthogonal at each step, as the random event at each step is uniformly distributed and has a nonzero minimal probability (greater than $\frac{3}{8}$). Thus $\mathcal{C} = \mathcal{O}(\sum_{1 \leqslant i \leqslant s} s^3) = \mathcal{O}(s^4)$

Algorithm 67 Direct sum decomposition of hyperbolic planes in the Euclidean case

Input: W_0: The ambiant Euclidean vector space

Output: U,V build a uniformly random direct sum decomposition of hyperbolic planes

1: $U, V, W \leftarrow [], [], W_0$
2: **while** $W \neq 0$ **do**
3: Pick two random vectors u and v
4: **if** $< u, v > \neq 0$ and (u, v) is free **then**
5: Solve $< u + \lambda v, u + \lambda v >= 0$ for λ (Euclidean quadratic equation)
6: **if** The discriminant is a square in $\mathbf{F}_l^*$ **then**
7: $u \leftarrow u + \lambda v$
8: $u \leftarrow u - \lambda v$
9: Solve $< u, \nu v >= 1$ for ν (linear)
10: $v \leftarrow \nu v$, now (u, v) is a hyperbolic pair
11: $U \leftarrow U + [u]$, $V \leftarrow V + [v]$
12: $W \leftarrow < u, v >^{\perp}$
13: **end if**
14: **end if**
15: **end while**

Proposition 68 The algorithm terminates with probability 1 and if it terminates, it is correct

We need the following lemmas to determine the probability for the quadratic equation at line 5 of the algorithm 67 to be solvable and to solve it when it is possible.

Lemma 69 If -1 is a square in $\mathbf{F}_l^*$, The probability $\mathcal{P}_{q_l,s}$ for the discriminant of the equation to be square at each step $i \in \{1, \ldots, s\}$ is equal to $\mathcal{P}_{q_l,i} = \frac{(q_l^{i-1}+1)(q_l^{2i-1}+q_l^i-q_l^{i-1}-q_l)(q_l+1)}{2(q_l^i+1)(q_l^{2i-1}-1)}$. Moreover this probabililty decreases with i and q_l and we have $\lim_{s\to\infty, q_l\to\infty} \mathcal{P}_{q_l,s} = \frac{1}{2}$

Proof. The equation is solvable exactly when the plane spanned by u and v is a hyperbolic plane. For any step $i \in \{1, \ldots, s\}$ the application mapping the pairs of noncollinear isotropic vectors in $W \simeq \mathbf{F}_l^{2i}$ to their span is surjective on the set of hyperbolic planes. The cardinal of its preimage for any hyperbolic plane is the number of pairs of noncollinear vectors in the hyperbolic plane. Hence it is:

$$\frac{(q_l^i-1)(q_l^{i-1}+1)((q_l^i-1)(q_l^{i-1}+1)-(q_l-1))}{2(q_l-1)^2}$$

The number of arbitrary planes is on the other side: $\frac{(q_l^{2s}-1)(q_l^{2s}-q_l)}{(q_l^2-1)(q_l^2-q_l)}$. Finally we get the probability:

$$\mathcal{P}_{q_l,i} = \frac{(q_l^i-1)(q_l^{i-1}+1)((q_l^i-1)(q_l^{i-1}+1)-(q_l-1))(q_l^2-1)(q_l^2-q_l)}{2(q_l^{2s}-1)(q_l^{2s}-q_l)(q_l-1)^2}$$

$$\mathcal{P}_{q_l,i} = \frac{(q_l^{i-1}+1)(q_l^{2s-1}+q_l^i-q_l^{i-1}-q_l)(q_l+1)}{2(q_l^i+1)(q_l^{2s-1}-1)}$$

We observe

$$\frac{(q_l^{i-1}+1)(q_l^{2s-1}+q_l^i-q_l^{i-1}-q_l)(q_l+1)}{2(q_l^i+1)(q_l^{2s-1}-1)} \underset{i\to\infty}{\sim} \frac{q_l^{i-1}q_l^{2s-1}(q_l+1)}{2q^iq_l^{2s-1}} \underset{i\to\infty}{\sim} \frac{q_l+1}{2q} \underset{q_l\to\infty}{\sim} \frac{1}{2}$$

□

Remark 70 For $i=1$, we check: $\frac{(q_l^{i-1}+1)(q_l^{2s-1}+q_l^i-q_l^{i-1}-q_l)(q_l+1)}{2(q_l^i+1)(q_l^{2s-1}-1)} = 1$

Lemma 71 Solving $< u+\lambda v, u+\lambda v >= 0$ for λ is equivalent to solving $< u,u > +2\lambda < u,v > +\lambda^2 < v,v >= 0$ for λ. Noting Δ the discriminant: $\Delta := < u,v >^2 - < u,u >< v,v >$. If Δ is a square in $\mathbf{F}_l^*$, we find two solutions, $\lambda = \frac{-<u,v>\pm\sqrt{\Delta}}{<v,v>}$, else there are no solutions.

Proof. (of Proposition 68) As in the Hermitian case, we start by taking two non-collinear random elements u and v in $\mathbf{K}_l$. If u is isotropic, the equation: $< u+\lambda v, u+\lambda v >= 0$ is linear in λ and has always a solution λ_0. We can thus make the base change $u \leftarrow u, v \leftarrow u - \lambda_0 v$. If u isn't isotropic we have to solve the quadratic equation: $< u+\lambda v, u+\lambda v >= 0$ for λ using lemma 71. If there are solutions, we make the base change $u \leftarrow u+\lambda v, v \leftarrow u - \lambda v$. If there are no solutions, we pick two random vectors again. Asymptotically in s and q_l, this operation thus increase the mean complexity of a factor 2, as the lemma 69 shows. As in the Hermitian case, Witt decomposition theorem 46 produces a direct sum of hyperbolic plane, provided the existence criterion on the discriminant is fulfilled. Finally as the discriminant of the bilinear form

restricted to the remaining direct sum of hyperbolic planes does not depend on the hyperbolic plane chosen, the algorithm's returned value remains uniformly distributed. □

Mean complexity 72 The mean complexity $\mathcal{C}$ in s of the algorithm is a less than a constant times the complexity of taking the orthogonal at each step, as the random event at each step is uniformly distributed and has a nonzero minimal probability (greater than $\frac{3}{16}$). Thus $\mathcal{C} = \mathcal{O}(\sum_{1 \leqslant i \leqslant s} s^3) = \mathcal{O}(s^4)$

The random direct sum of hyperbolic planes obtained, can now be used to enumerate all maximal isotropic spaces.

Algorithm 73 Enumeration of maximal isotropic spaces in the Euclidean case

Input: Iterator I on all reduced echelon matrix A of growing size (i, s), U, V, bases of supplementary maximal isotropic building pairwise hyperbolic pairs

Output: W is the next maximal isotropic space

1: $A \leftarrow$ next I

2: $B \leftarrow$ next solution of the orthogonality system given by A among $q_l^{i(i-1)/2}$ solutions.

3: $(0, C) \leftarrow$ single reduced echelon matrix, whose image is the totally isotropic orthogonal to (A, B) in the vector space spanned by the $(v_i)_{0 \leqslant i \leqslant s}$

4: $W \leftarrow Im((A, B)) \bigoplus Im((0, C))$

5: yield W

Proposition 74 The algorithm is correct

Proof. We enumerate all maximal isotropic spaces in an analogue fashion as for the enumeration of subspaces of dimension s in an ambiant space of dimension $2s$ using the formula: $\binom{2s}{s}_{q_l} = \sum_{i=0}^{s} q_l^{i^2} \binom{s}{i}_{q_l}^2$.

The algorithm for subspaces enumeration in general is the following. Given a base of the ambiant vector space, we use the bijection between its vector subspaces and the reduced echelon matrices in this base, whose image correspond to the vector subspaces, to reduce the problem to the enumeration of all $(s, 2s)$-sized reduced echelon matrices.

We enumerate these $\binom{2s}{s}_{q_l}$ different reduced echelon matrices M of size $(s, 2s)$ by decomposing the matrix M in s types of reduced echelon matrices of the form $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ for block matrices A of the size (i, s) for each index i between 0 and s. There are thus for each index i, $\binom{s}{i}_{q_l}$ possibilities

for choosing A, $\binom{s}{s-i}_{q_l} = \binom{s}{i}_{q_l}$ possibilities for choosing C and $q_l^{i^2}$ possibilities for choosing the matrix B as its entries can be choosen arbitrarily once the pivots of C have been deleted.

Summing over all indices, and for each index, multiplying all independent possibilities for A, B and C, we obtain the expected formula $\binom{2s}{s}_{q_l} = \sum_{i=0}^{s} q_l^{i^2} \binom{s}{i}_{q_l}^2$.

$$\binom{2s}{s}_{q_l} = |M_{\text{echelon}}| = \left| \left[\begin{array}{c|c} A_{\text{echelon}}(i,s) & B_{\text{pivot deletion}}(i,s) \\ \hline 0 & C_{\text{echelon}}(s-i,s) \end{array} \right] \middle| 0 \leqslant i \leqslant s \right| = \sum_{i=0}^{s} q_l^{i^2} \binom{s}{i}_{q_l}^2$$

Now we adapt this strategy to the case of isotropic spaces. Starting with a base $(u_i)_{0 \leqslant i \leqslant s}$ and $(v_i)_{0 \leqslant i \leqslant s}$ of supplementary maximal isotropic spaces such that (Witt decomposition 46) the bilinear form is represented in this base by the matrix: $\begin{pmatrix} 0 & Id \\ Id & 0 \end{pmatrix}$, as it is obtained by the algorithm previously described, we express the global $(s, 2s)$ sized matrix as a generator matrix M for a maximal isotropic space expressed in this base. For each reduced echelon matrix A in the upper left corner of M generating a subspace of $< U >$ of dimension i, we get as in the previous enumeration corresponding matrices B and C. But now the additional orthogonality relations on the rows expressed in the base of the $(u_i)_{0 \leqslant i \leqslant s}$ and $(v_i)_{0 \leqslant i \leqslant s}$ leads to $i(i+1)/2$ (number of unordered pairs of orthogonal rows of (A, B)) independent additional equations for B. Noting $A = (a_{i,j})_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant s}$ $B = (b_{i,j})_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant s}$, this set of equations is explicitly the following:

$$\begin{array}{ccccc} \Sigma_{1 \leqslant j \leqslant s}\, a_{1,j} b_{1,j} + b_{1,j} a_{1,j} = 0 & & \cdots & & \cdots \quad \Sigma_{1 \leqslant j \leqslant js}\, a_{1,j} b_{d,j} + b_{1,j} a_{d,j} = 0 \\ & \ddots & & & \vdots \\ & & \Sigma_{1 \leqslant j \leqslant s}\, a_{k,j} b_{k,j} + b_{k,j} a_{k,j} = 0 & \cdots & \Sigma_{1 \leqslant j \leqslant js}\, a_{k,j} b_{d,j} + b_{k,j} a_{d,j} = 0 \\ & & & \ddots & \vdots \\ & & & & \Sigma_{1 \leqslant j \leqslant js}\, a_{d,j} b_{d,j} + b_{d,j} a_{d,j} = 0 \end{array} \tag{7.5}$$

or matricially:

$$AB^{\mathsf{tr}} + BA^{\mathsf{tr}} = 0$$

Let us note α, β and γ the endomorphisms induced by the matrices A, B, and C in the base $((u_i)_{0 \leqslant i \leqslant s}, (v_i)_{0 \leqslant i \leqslant s})$. From the system of equations we get: $\alpha \circ \beta^\bullet + \beta \circ \alpha^\bullet = 0$ and we have also $\alpha \circ \gamma^\bullet = 0$, which implies $\ker(\alpha) \supset Im(\gamma^\bullet)$. By checking both dimensions equal to $s-i$, we deduce $\ker(\alpha) = Im(\gamma^\bullet)$. Moreover, as we made the pivot with C in B, we have: $Im(\beta^\bullet) \cap Im(\gamma^\bullet) = 0$.

We get $Im(\beta^\bullet) \cap \ker(\alpha) = 0$. This means that α restricted to $Im(\beta^\bullet)$ is injective. Noting $\mu = \alpha \circ \beta^\bullet$, the system of equations reduces to assert that μ is antisymmetric. We thus have to solve: $\beta^\bullet = \alpha|^{-1}_{Im(\beta^\bullet)}\mu$ for any antisymmetric endomorphism μ represented by an antisymmetric matrix M of dimension $d \times d$ in the chosen base. This gives $q_l^{i(i-1)/2}$ solutions for B.

On the other hand, for $(0, C)$, there is no choice but to take the reduced echelon matrix corresponding to the right kernel of A: the single totally isotropic space spanned by the $(v_i)_{0 \leqslant i \leqslant s}$ and orthogonal to (A, B). □

Mean complexity 75 The mean complexity $\mathcal{C}$ in s of one iteration of the algorithm is a less than a constant times the complexity of taking the orthogonal at each step. Thus $\mathcal{C} = \mathcal{O}(\sum_{1 \leqslant i \leqslant s} s^3) = \mathcal{O}(s^4)$

Remark 76 As a byproduct of Proposition 74, we obtain a bijective proof of the q-binomial formula stated in 45 for the evaluation at 1:

$$\prod_{i=0}^{s-1}(1 + xq_l^i)|_{x=1} = \sum_{i=0}^{s} x^i q_l^{\binom{i}{2}} \binom{s}{i}_{q_l} |_{x=1}$$

$$\prod_{i=0}^{s-1}(1 + q_l^i) = \sum_{i=0}^{s} q_l^{\binom{i}{2}} \binom{s}{i}_{q_l}$$

Algorithm 77 Enumeration of maximal isotropic spaces in the Hermitian case

Input: Iterator I on all reduced echelon matrix A of growing size (i, s), U, V, bases of supplementary maximal isotropic building pairwise hyperbolic pairs

Output: W is the next maximal isotropic space

1: $A \leftarrow$ next I

2: $B \leftarrow$ next solution of the orthogonality system given by A among $q_l^{i^2/2}$ solutions.

3: $(0, C) \leftarrow$ single reduced echelon matrix, whose image is the totally isotropic orthogonal of (A, B) in the vector space spanned by the $(v_i)_{0 \leqslant i \leqslant s}$

4: $W \leftarrow Im((A, B)) \bigoplus Im((0, C))$

5: yield W

Proposition 78 The algorithm is correct

Proof. We use the same algorithm as in the Euclidean case but the orthogonality equations are

now put in the Hermitian setting. This set of equations is explicitly the following:

$$\begin{array}{ccccc}
\sum_{1\leqslant j\leqslant s} a_{1,j}\sigma_l(b_{1,j}) + b_{1,j}\sigma_l(a_{1,j}) = 0 & \cdots & \cdots & \sum_{1\leqslant j\leqslant js} a_{1,j}\sigma_l(b_{d,j}) + b_{1,j}\sigma_l(a_{d,j}) = 0 \\
\ddots & & & \vdots \\
 & \sum_{1\leqslant j\leqslant s} a_{k,j}\sigma_l(b_{k,j}) + b_{k,j}\sigma_l(a_{k,j}) = 0 & \cdots & \sum_{1\leqslant j\leqslant js} a_{k,j}\sigma_l(b_{d,j}) + b_{k,j}\sigma_l(a_{d,j}) = 0 \\
 & & \ddots & \vdots \\
 & & & \sum_{1\leqslant j\leqslant js} a_{d,j}\sigma_l(b_{d,j}) + b_{d,j}\sigma_l(a_{d,j}) = 0
\end{array} \tag{7.6}$$

or matricially:

$$A\sigma_l(B^{\mathsf{tr}}) + B\sigma_l(A^{\mathsf{tr}}) = 0$$

We follow the proof of 74, we now have that $M = \alpha \circ \beta^{\bullet}$ is Hermitian antisymmetric. And we have thus for fixed entries in the upper triangular part of B, $\sqrt{q_l}^i$ additional solutions on the diagonal of B. This gives $q_l^{i(i-1)/2+i/2} = q_l^{\frac{i^2}{2}}$ possibilities for B. □

Mean complexity 79 The mean complexity $\mathcal{C}$ in s of one iteration of the algorithm is a less than a constant times the complexity of taking the orthogonal at each step. $\mathcal{C} = \mathcal{O}(\sum_{1\leqslant i\leqslant s} s^3) = \mathcal{O}(s^4)$

Remark 80 As a byproduct of Proposition 74, we obtain a bijective proof of the q-binomial formula stated in 45 for the evaluation at $x = \sqrt{q_l}$:

$$\prod_{i=0}^{s-1}(1 + xq_l^i)|_{x=\sqrt{q_l}} = \sum_{i=0}^{s} x^i q_l^{\binom{i}{2}} \binom{s}{i}_{q_l} |_{x=\sqrt{q_l}}$$

$$\prod_{i=0}^{s-1}(1 + q_l^{i+\frac{1}{2}}) = \sum_{i=0}^{s} q_l^{\frac{i^2}{2}} \binom{s}{i}_{q_l}$$

8 SageMath enumeration of selfdual skew codes

We implemented the algorithms of section 7 in SageMath. Our package is available at

`https://plmlab.math.cnrs.fr/caruso/selfdual-skew-cyclic-codes`

It consists in a main class instantiated with the extension $\mathbf{K}/\mathbf{F}$ of order r and a palindromic polynomial of the center $P(X^r)$ in $\mathbf{F}(X^{\pm r})$ of $\mathbf{K}[X^{\pm 1};\theta]$ as parameters. It provides an iterator on all selfdual codes for the Ore algebra $\mathbf{K}[X^{\pm 1};\theta]/P(X^r)$. Hereunder, a simple use case of the library to compute the first iteration of $\mathbf{E}_1$ for $p = 3$ and $s = 3$:

```
sage:load("selforthogonal_codes.sage")
sage:p, s, P = 3, 3, [1, -1]
sage:A = SelfDualCodes(GF(p)["y"](P), GF(p)["z"].irreducible_element(2 * s))
sage:iter = A.enumerate_selfdual_codes(True)
sage:next(iter)
```

$x^3 + (z^5 + z^4 + 2z^3 + z^2 + z + 1)x^2 + (z^4 + z^3 + 2z^2 + z + 1)x + 2z^4 + z^3 + 2z^2 + 2z + 1$

8.1 SageMath computation of cyclic or negacyclic codes

Hereunder, we provide computations for the palindromic Euclidean, Hermitian, skew-Euclidean and skew-Hermitian cases and nonpalindromic case. (see the four types of geometries 3) Skew-Euclidean and skew-Hermitian cases are described in appendix A.

Case 81 Palindromic Euclidean:
$q = 3$,$s = 3$ and $P(Y) = Y - 1$

```
sage:A = SelfDualCodes(PolynomialRing(GF(3), y)([1, 2]), 3)
sage:iter = A.enumerate_selfdual_codes(True)
```

H90 preimage of $x\bar{x}$ with $norm(x) = y$: zeta = 1
Enumerating the 80 selfdual codes...
selfdual code in E: $x^3 + (2z_6^3 + z_6 + 1)x^2 + (z_6^5 + z_6^3 + 2)x + 2z_6^4 + z_6^3 + 2z_6^2 + 2z_6 + 1$
Total time (ms): 35.42

```
sage:next(iter)
```

selfdual code in E: $x^3 + (2z_6^5 + z_6^4 + 2z_6^3 + z_6^2 + 2)x^2 + (2z_6^5 + z_6^4 + 2z_6^3 + 2z_6 + 1)x + z_6^5 + 2z_6^4 + z_6^2 + 2z_6$
Total time (ms): 31.98

Case 82 Palindromic Hermitian case:
$q = 3$,$s = 3$ and $P(Y) = Y^2 + 1$

```
sage:A = SelfDualCodes(PolynomialRing(GF(3), y)([1, 0, 1]), 3)
sage:iter = A.enumerate_selfdual_codes(True); next(iter)
```

H90 preimage of $x\bar{x}$ with $norm(x) = y$: $zeta = z_6^4 + z_6^3 + 2z_6^2 + 2z_6 + 1$
Enumerating the 1640 selfdual codes...
selfdual code in E: $x^6 + (z_6^4 + 2z_6 + 2)x^5 + (2z_6^5 + 2z_6^4 + z_6 + 1)x^4 + (2z_6^5 + z_6^4 + z_6^3 + z_6^2)x^3 + (z_6^5 + z_6^4 + 2z_6^2)x^2 + (2z_6^4 + z_6^3 + z_6^2 + z_6)x + z_6^5 + 2z_6^4 + 2z_6^3 + z_6^2 + 1$
Total time (ms): 36.35

```
sage:next(iter)
```

selfdual code in E: $x^6 + (2z_6^4 + 2z_6^3 + 2z_6)x^5 + (2z_6^5 + 2z_6^4 + 2z_6^3 + 2z_6^2 + z_6 + 2)x^4 + (2z_6^5 + 2z_6^2 + z_6)x^3 + (z_6^5 + 2z_6^4 + z_6^2 + 1)x^2 + (z_6^3 + 2z_6^2)x + z_6^4 + 2z_6^3 + z_6^2 + z_6 + 2$

Total time (ms): 37.64

Case 83 Palindromic Skew-Euclidean case:
$q = 3, s = 3, \iota = -\theta^s(iota) \in GF(3^6)$ and $P(Y) = Y - 1$

```
sage:A = SelfDualCodes(PolynomialRing(GF(3), y)([1, 2]), 3, iota, True)
sage:iter = A.enumerate_selfdual_codes(True); next(iter)
```

H90 preimage of $x\bar{x}$ with $norm(x) = y$: $zeta = 2z_6^5 + z_6^4 + z_6^3 + 2z_6^2 + 2$

Enumerating the 1120 selfdual codes...

selfdual code in E: $x^3 + (z_6^5 + z_6^4 + z_6 + 2)x^2 + (z_6^4 + z_6^3 + 2z_6^2 + z_6 + 1)x + 2z_6^4 + 2z_6^3 + 1$

Total time (ms): 41.50

```
sage:next(iter)
```

selfdual code in E: $x^3 + (z_6^5 + z_6^4 + 2z_6^3 + z_6^2 + 2z_6 + 1)x^2 + (z_6^5 + z_6^3 + z_6 + 2)x + 2z_6^5 + 2z_6^3 + z_6 + 2$

Total time (ms): 42.02

Case 84 Palindromic Skew-Hermitian case:
$q = 3, s = 3, \iota = -\theta^s(iota) \in GF(3^6)$ and $P(Y) = Y^2 + 1$

```
sage:A = SelfDualCodes(PolynomialRing(GF(3), y)([1, 0, 1]), 3, iota, True)
sage:iter = A.enumerate_selfdual_codes(True); next(iter)
```

H90 preimage of $x\bar{x}$ with $norm(x) = y$: $zeta = (2z_6^5 + 2z_6^3 + 1)y + 2z_6^4 + z_6^3 + 2z_6^2 + 2z_6 + 1$

Enumerating the 14948416 selfdual codes...

selfdual code in E: $x^6 + (z_6^5 + z_6)x^5 + (z_6^3 + z_6^2 + 2z_6)x^4 + (z_6^5 + z_6^3 + z_6^2 + 1)x^3 + (z_6^5 + 2z_6^4 + z_6^3 + z_6^2 + 2)x^2 + (z_6^4 + z_6^2 + 2z_6 + 2)x + z_6^5 + z_6^4$

Total time (ms): 44.15

```
sage:next(iter)
```

selfdual code in E: $x^6 + (2z_6^5 + 2z_6^4 + z_6 + 1)x^5 + (2z_6^5 + z_6^2)x^4 + (2z_6^4 + 2z_6^2)x^3 + (z_6^5 + z_6^3 + 2z_6^2 + z_6 + 2)x^2 + (z_6^5 + z_6^3 + 2z_6^2 + z_6)x + 1$

Total time (ms): 45.33

8.2 SageMath iteration time for the enumeration of selfdual skew codes

We provide computation results for skew cyclic $(X^{rk} - 1, \mathbf{K}/\mathbf{F})$-codes and skew negacyclic $(X^{rk} + 1, \mathbf{K}/\mathbf{F})$-codes for $|\mathbf{F}| \leqslant 9$, $k \leqslant 9$ and $r \in \{4, 6, 8\}$ on a computer with following characteristics:

- processeur x64: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz 2.59 GHz
- mémoire RAM: 16,0 Go

Case 85 $s = 2$:

$P(Y)$	$p = 3$	$p = 5$	$p = 7$	$p = 3^2$
$Y - 1$	no codes.	no codes.	no codes.	no codes.
$Y^3 - 1$	inseparable	no codes.	no codes.	inseparable
$Y^5 - 1$	no codes.	inseparable	no codes.	no codes.
$Y^7 - 1$	no codes.	no codes.	inseparable	no codes.
$Y^9 - 1$	inseparable	no codes.	no codes.	inseparable
$Y + 1$	9 ms 8 codes.	9 ms 12 codes.	16 ms 16 codes.	21 ms 20 codes.
$Y^2 + 1$	16 ms 112 codes.	6 ms 1120 codes.	15 ms 2752 codes.	15 ms 9104 codes.
$Y^3 + 1$	inseparable	26 ms 9072 codes.	22 ms 58432 codes.	inseparable
$Y^4 + 1$	18 ms 9104 codes.	21 ms 440080 codes.	35 ms 7573504 codes.	48 ms 82882816 codes.
$Y^5 + 1$	62 ms 58400 codes.	inseparable	111 ms 94120000 codes.	128 ms 1065800000 codes.
$Y^6 + 1$	inseparable	47 ms 492889600 codes.	59 ms 16862891008 codes.	inseparable
$Y^7 + 1$	80 ms 4409216 codes.	300 ms 2953126512 codes.	inseparable	250 ms 5671878518080 codes.
$Y^8 + 1$	463 ms 155747211899539264 codes.	87 ms 44667536 codes.	113 ms 153321876880 codes.	108 ms 37546305270016 codes.
$Y^9 + 1$	inseparable	218 ms 2232563643072 codes.	125 ms 815875477905664 codes.	inseparable

(8.1)

Case 86 $s = 3$:

$P(Y)$	$p = 3$	$p = 5$
$Y - 1$	21 ms 80 codes.	no codes.
$Y^3 - 1$	inseparable	no codes.
$Y^5 - 1$	101 ms 34485200000 codes.	inseparable
$Y^7 - 1$	195 ms 632674347361280 codes.	no codes.
$Y^9 - 1$	inseparable	no codes.
$Y + 1$	no codes.	21 ms 312 codes.
$Y^2 + 1$	152 ms 27328 codes.	12 ms 3583232 codes.
$Y^3 + 1$	inseparable	57 ms 737335872 codes.
$Y^4 + 1$	38 ms 540023488 codes.	47 ms 4298676317632 codes.
$Y^5 + 1$	no codes.	inseparable
$Y^6 + 1$	inseparable	101 ms 15403154538981146624 codes.
$Y^7 + 1$	no codes.	398 ms 2343178995193968789312 codes.
$Y^8 + 1$	209 ms 155747211899539264 codes.	270 ms 14621913851167452151565632 codes.
$Y^9 + 1$	inseparable	450 ms 55375318194661179051543198 72 codes.

(8.2)

$P(Y)$	$p = 7$	$p = 3^2$
$Y - 1$	207 ms 800 codes.	no codes.
$Y^3 - 1$	42 ms 49557536000 codes.	inseparable
$Y^5 - 1$	129 ms 1329328526500000000 codes.	no codes.
$Y^7 - 1$	inseparable	no codes.
$Y^9 - 1$	342 ms 3285136932442382207872260115712000 codes.	inseparable
$Y + 1$	no codes.	56 ms 1640 codes.
$Y^2 + 1$	36 ms 46255616 codes.	32 ms 540023488 codes.
$Y^3 + 1$	no codes.	inseparable
$Y^4 + 1$	74 ms 2139582011539456 codes.	141 ms 291625367591686144 codes.
$Y^5 + 1$	no codes.	317 ms 304739936129000000000 codes.
$Y^6 + 1$	139 ms 80064991841686623715328 codes.	inseparable
$Y^7 + 1$	inseparable	601 ms 957587390996230804352539827 20 codes.
$Y^8 + 1$	270 ms 14621913851167452151565632 codes.	280 ms 29961005860191265067993153904 64 codes.
$Y^9 + 1$	no codes.	inseparable

(8.3)

Case 87 $s = 4$:

$P(Y)$	$p = 3$	$p = 5$
$Y - 1$	no codes.	no codes.
$Y^3 - 1$	inseparable	no codes.
$Y^5 - 1$	no codes.	inseparable
$Y^7 - 1$	no codes.	no codes.
$Y^9 - 1$	inseparable	no codes.
$Y + 1$	59 ms 2240 codes.	49 ms 39312 codes.
$Y^2 + 1$	78 ms 59793664 codes.	29 ms 281268665344 codes.
$Y^3 + 1$	inseparable	128 ms 7258242894319872 codes.
$Y^4 + 1$	88 ms 2584219514040576 codes.	108 ms 26237287231770008445184 codes.
$Y^5 + 1$	220 ms 4618366957232000000 codes.	inseparable
$Y^6 + 1$	inseparable	200 ms 737972676192712267014451226450329 6 codes.
$Y^7 + 1$	286 ms 185303919822256877419151360 codes.	387 ms 1407816664669230874145646249088174533 12 codes.
$Y^8 + 1$	406 ms 3562996965217630611881373225216 codes.	551 ms 5447087381612336324621234851501496923875043 84 codes.
$Y^9 + 1$	inseparable	691 ms 2599276379436443575720930358836160190638568430387 2 codes.

(8.4)

Case 88 $s = 4$ (remaining cases):

$P(Y)$	$p = 7$
$Y - 1$	no codes.
$Y^3 - 1$	no codes.
$Y^5 - 1$	no codes.
$Y^7 - 1$	inseparable
$Y^9 - 1$	no codes.
$Y + 1$	58 ms 275200 codes.
$Y^2 + 1$	89 ms 38093535023104 codes.
$Y^3 + 1$	90 ms 14058141548980940800 codes.
$Y^4 + 1$	174 ms 145111741055645 1065813794816 codes.
$Y^5 + 1$	336 ms 3101439596560774735006000000000000 codes.
$Y^6 + 1$	388 ms 44720054178174175715919090093196510756864 codes.
$Y^7 + 1$	inseparable
$Y^8 + 1$	586 ms 13781677699890256475581830987425220847119291720086978 56 codes.
$Y^9 + 1$	784 ms 52051173341161148133210198956987605412904394606708739768320 0 codes.

(8.5)

Case 89 $s = 4$ (remaining cases):

$P(Y)$	$p = 3^2$
$Y - 1$	no codes.
$Y^3 - 1$	inseparable
$Y^5 - 1$	no codes.
$Y^7 - 1$	no codes.
$Y^9 - 1$	inseparable
$Y + 1$	177 ms 1197200 codes.
$Y^2 + 1$	69 ms 2584219514040576 codes.
$Y^3 + 1$	inseparable
$Y^4 + 1$	412 ms 667819049674811077800177441l776 codes.
$Y^5 + 1$	723 ms 5089176886279936209860153000000000000 codes.
$Y^6 + 1$	inseparable
$Y^7 + 1$	1367 ms 764881183604399196721916115374038762837039539333l200 codes.
$Y^8 + 1$	2159 ms 126949473741500456442962145661815998477024161360796538582466l6 codes.
$Y^9 + 1$	inseparable

(8.6)

A Enumeration of inseparable selfdual skew cyclic codes

Factorizations over inseparable $\mathbf{E_k}$ have been studied in [BU14]. But we will use another approach using twisted skew separable codes $\mathbf{E}_{\mathbf{k},\mathbf{l}}^{(\xi\mathbf{X^t})}$. These are defined as skew separable codes of $\mathbf{E}_{\mathbf{k},\mathbf{l}}$ corresponding to the usual adjunction on $\mathbf{E}_{\mathbf{k},\mathbf{l}}$ composed with the conjugation by ξX^t. We aim at obtaining all inseparable codes as products of twisted skew separable codes.

A.1 Counting selfdual skew separable twisted codes

We can count all possible selfdual skew codes from one single skew code by using the transitive right action of the orthogonal group in the Euclidean case, the unitary group in the Hermitian case, the symplectic group in the skew-Euclidean case or the skew-unitary group in the skew-Hermitian case, on those codes. The action is well defined as the following computation shows in the Euclidean or Hermitian case:
$\forall o \in \{\text{orthogonal group}\}\ \forall f \in \{\text{maximal orthogonal codes}\}\ fo(fo)^* = foo^*f^* = ff^* = 0.$

In the skew-Euclidean or skew-Hermitian case:
$\forall o \in \{\text{symplectic group}\}\ \forall f \in \{\text{maximal orthogonal codes}\}\ fs(fs)^* = fss^*f^* = -ff^* = 0$.

Choosing a base, these classical groups corresponding to the coordinatewise bilinear form are conjugated to those related to our trace bilinear form. So in order to get the number of maximal orthogonal codes, we can take the cardinal of the quotient of the classical group by its stabilizer.

In the Euclidean case, choosing a base $< U, V >$ constituted pairwise by hyperbolic pairs $< u, v >$ as described in the algorithm 67, this cardinal is that of the general linear subgroup acting on the maximal isotropic spaces times the number of matrices in the upper right block: i.e. $q_l^{s^2}$ divided by the number of equations for the rows to be isotropic: $q_l^{s(s+1)/2}$. So in the end we find the orthogonal Segre's formula again for the number of maximal isotropic subspaces: $\prod_{0 \leqslant i < s}(1 + q^i)$

In the skew-Euclidean case, the cardinal of the stabilizer, is $q_l^{s^2}$ divided by the number of equations for the rows to be isotropic, which is now less than in the Euclidean case: $q_l^{s(s-1)/2}$. So in the end we find the symplectic Segre's formula again for the number of maximal isotropic subspaces: $\prod_{0 < i \leqslant s}(1 + q^i)$, using the symplectic action [Han05].

```
sage: G=GO(14,GF(9),1)
....: H=GL(7,GF(9))
....: segre=prod(1+9^i for i in range(7))
....: G.cardinality()/H.cardinality()/9**(21)==segre
True
sage: G=Sp(14,GF(9),1)
....: H=GL(7,GF(9))
....: segre=prod(1+9^i for i in range(1,8))
....: G.cardinality()/H.cardinality()/9**(28)==segre
True
```

A.2 Enumeration of inseparable selfdual skew cyclic codes

Definition 90 We fix parameters $t \in \{0, s\}$ and $\xi \in \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l$ with $\sigma_l(\xi) = \xi$, and $\theta^t(\xi) = -\xi$ if $t = s$. We define $\mathbf{E}_{\mathbf{k,l}}^{(\xi \mathbf{X^t})}$, the quadratic space $\mathbf{E}_{k,l}$ along with its ξX^t-twisted bilinear form $(\kappa, \rho) = Trace_{\mathbf{K}_l/\mathbf{F}_l}(\zeta.\xi\kappa\theta^t(\sigma_l(\rho)))$ corresponding to the *twisted adjunction*: $f^{\bullet_{\xi X^t}} = X^t\xi^{-1}\zeta^{-1}\sum_i X^{-i}\sigma_l(f_i)\zeta\xi X^{-t}$.

The ξX^t-twisted bilinear form is Euclidean if $y_l = \pm 1$ and $t = 0$

It is Hermitian if $y_l \neq \pm 1$ and $t = 0$

It is skew-Euclidean if $y_l = \pm 1$ and $t = s$

It is skew-Hermitian if $y_l \neq \pm 1$ and $t = s$

Lemma 91 The two expressions $(\kappa, f(\rho))_{\mathbf{F}_l}^{(\xi X^t)}$ and $(f^{\bullet_{\xi X^t}}(\kappa), \rho)_{\mathbf{F}_l}^{(\xi X^t)}$ coincide.

Lemma 92 The set of ξ-twisted selfdual skew codes is in bijection with the set of non-twisted selfdual skew codes and their intersection is empty for any twisting verifying $\theta^s(\xi) = -\xi$.

Proof. We have trivially for any monic skew polynomial f of degree s generating a selfdual code C_f of $\mathbf{E}_{k,l}$:

$$f\xi f^{\bullet_\xi}\xi^{-1} = \frac{ff^\bullet}{X^s(X^r-1)}X^s(X^r-1) = f(0)X^s(X^r-1)$$

We assume ξ to be σ_l-invariant. So, by Hilbert-90, we can solve the equation $\gamma\sigma_l(\gamma) = \xi$ for γ in ${\mathbf{K}_l}^{\theta^s}$. Noting then $g = \sigma_l(\gamma)f\gamma^{-1}$, we get a bijection $f \mapsto g$ between nontwisted and ξ-twisted selfdual skew codes:

$$gg^{\bullet_\xi} = \sigma_l(\gamma)f\xi f^{\bullet_\xi}\gamma = \sigma_l(\gamma)ff^\bullet\frac{1}{\sigma_l(\gamma)} = f(0)X^s(X^r-1)$$

. Moreover if we assume $\theta^s(\xi) = -\xi$ and $ff^\bullet = ff^{\bullet_\xi} = f\xi^{-1}f^\bullet\xi = 0$ in $\mathbf{E}_{k,l}$ then by evaluating lifts at 0, we get: $f(0) = \frac{\theta^s(\xi)}{\xi} = -1$. But this is not possible because $X^s(X^r-1) \neq ff^\bullet$. Indeed ${ff^\bullet}_{r+s} = {ff^\bullet}_s = -1$ whereas ${X^s(X^r-1)}_{r+s} = 1 \neq -1 = {X^s(X^r-1)}_s$. □

Algorithm 93 Enumeration of inseparable selfdual skew cyclic codes

Input: $(X^k-1)^n$: The cyclic polynomial to factorize as ff^*, $\mathcal{C}_\kappa$: The family of all κ-twisted code indexed by κ

Output: f: The next selfdual skew code

1: $i \leftarrow n$
2: $\kappa \leftarrow 1$
3: $f \leftarrow 1$
4: **while** $i > 0$ **do**
5: Find the next solution f_i from the family $\mathcal{C}_\kappa$
6: $f \leftarrow f_i f$
7: $\kappa \leftarrow \kappa f_i(0)X^{s(i\%2)}$
8: $i \leftarrow i-1$
9: **end while**
10: yield f

Proposition 94 The enumeration algorithm 93 is exhaustive

Proof. (sketch of a proof) If we are in the Hermitian case or if the existence criterion is fullfilled in the Euclidean case, there exists at least one inseparable case of the form: $\prod_l f_i$ with $f_i {f_i}^{\bullet_{\kappa_i X^{s(i\%2)}}} = 0$ The theorem 1.3 in [Gie98] due to Ore (1933) guarantees that the degree of each f_i in any other factorization in irreducible factors is equal to s. We thus search all solutions $\prod_{1\leqslant i\leqslant n} f_i$ with $\deg(f_i) = s$ satisfying $\prod_{1\leqslant i\leqslant n} f_i (\prod_{1\leqslant i\leqslant n} f_i)^* \propto X^{sn}(X^r-1)^n$. Per induction, it suffices to show that f_n is twisted selfdual. If f_n divides X^r-1, $f_n^\bullet$ too, and so by left and right Euclidean division, we get: $f_n \kappa f_n^\bullet = \propto X^s(X^r-1)$ for a scalar $\kappa \in \mathbf{K}_l$. If f_n does not divide X^r-1, as it is irreducible, it is coprime to X^r-1. Thus having fixed such a skew polynomial f_n invertible in $\mathbf{E}_k$, we can make an explicit bijection between the solutions of $\mathcal{S}_{n-1} = \{\prod_{1\leqslant i\leqslant n-1} f_i | \prod_{1\leqslant i\leqslant n-1} f_i (\prod_{1\leqslant i\leqslant n-1} f_i)^* \in (X^{sm}(X^r-1)^m)\, m\, maximal\}$ and $\mathcal{S}_n|_{f_n} = \{\prod_{1\leqslant i\leqslant n} f_i | \prod_{1\leqslant i\leqslant n} f_i (\prod_{1\leqslant i\leqslant n} f_i)^* \in (X^{sm}(X^r-1)^m)\, m\, maximal\}$, by conjugating $\mathcal{S}_{n-1}$ with f_n. To be explicit, this conjugation formula leads to the twisted nondegenerate sesquilinear form: $(\kappa,\rho) = Trace_{\mathbf{K}_l/\mathbf{F}_l}(\zeta.\kappa(f_n {f_n}^*)(\theta)(\sigma_l(\rho)))$; the nondegeneration coming from the fact that f_n is coprime to X^r-1 and thus $f_n\hat{}*$ and $f_n f_n\hat{}*$ too. As the order m corresponding to $\mathcal{S}_{n-1}$ is less than $n-1$, the order of $\mathcal{S}_n|_{f_n}$ too. We deduce from this fact that there are no selfdual codes $\prod_{1\leqslant i\leqslant n} f_i$ for f_n coprime to X^r-1. □

Proposition 95 The algorithm is correct

Proof. In order to enumerate all inseparable selfdual skew cyclic codes, at the price of some redundancy, we can assume without loss of generality (see 94) that the general solution is a product of twisted selfdual skew codes $f_1 \ldots f_n$, taking the f_i left monic, and we start by solving the equation $f_n f_n^\bullet = 0(X^r-1)$. This has been done in the preceding section. Now we obtain a scalar $\kappa_n = \frac{f_n f_n^\bullet}{X^s(X^r-1)}$ which is equal to $f_n(0)$. We then define another twisted adjunction to solve $f_{n-1}\kappa_n X^s f_{n-1}^\bullet = 0(X^r-1)$. Let $\bullet_{\kappa_n}$ be defined by: $f_i^{\bullet_{\kappa_n}} = \sigma_l(\kappa_n) f_i^\bullet {\kappa_n}^{-1}$. The equation becomes $f_{n-1}X^s f_{n-1}^{\bullet_{\kappa_n}}\kappa_n = 0(X^r-1)$. Solving it, we now obtain a scalar $\kappa_{n-1}\kappa_n = \frac{f_{n-1}X^s f_{n-1}^{\bullet_{\kappa_n}}}{X^r(X^r-1)}$. At the next step, the monomials X^s cancel and we are back in the Hermitian case. And so on so forth, getting alternatively a skew Hermitian (resp. skew Euclidean) and a Hermitian (resp. Euclidean) bilinear form. We have to check that the κ_i satisfy the required symmetry for the selfdual skew codes to exist: A monic polynomial f satisfying the product criterion: $f f^{\bullet_{\kappa X^t}} = 0$ in $\mathbf{E}_{\mathbf{k}}^{(\mathbf{l},\kappa\mathbf{X^t})}$ has a constant term $f_0 = f(0)$ satisfying:

$$(X^s + \ldots + f_0)\kappa X^t (X^r f_0 + \ldots + X^s) = \theta^s(\kappa)\theta^{s+t}(f_0) X^s X^t X^r + f_0 \kappa X^t X^s \propto X^{r+s+t} - X^{s+t}$$

Thus we have:

$$\begin{cases} \theta^s(f_0) = -f_0 \text{ for } \theta^s(\kappa) = \kappa \text{ , } t = 0 & (1) \\ \theta^s(\kappa) = -\kappa \text{ for } t = s \text{ symplectic case} & (2) \\ -f_0\kappa = \theta^s(\kappa f_0) \text{ for } t = 0 & (3) \end{cases} \tag{A.1}$$

If we start with $\kappa = 1$, we get the symplectic case from (1) and (2) with κ satisfying $\theta^s(\kappa) = -\kappa$, at the next step then an orthogonal case, then again alternatively a symplectic case with κ satisfying $\theta^s(\kappa) = -\kappa$ from (3) etc ... □

Remark 96 Noting $f_i^{(j)} = X^j f_i X^{-j}$, we have r redundant factorizations of the form $\prod_i f_i^{(j)} = \prod_i f_i$ modulo $(X^r - 1)^n$ except for θ^j invariant f_i's.

A.3 SageMath enumeration of inseparable selfdual skew cyclic codes

For $F = GF(3)$ and $K = GF(3^6)$, $k = 1$ and $m = 1$, the upper bound on the number of generated inseparable selfdual skew codes is numerically equal to: $80 * 1120 * 80$, where 80 is the number of orthogonal isotropic spaces and 1120 the number of symplectic isotropic spaces. A sage enumeration based on this algorithm provides a number n of maximal isotropic codes equal to $n = 2360960$. We have not much redundancies since $80 * 1120 * 80 \approx 3 * 2360960$.

Remark 97 In addition to those codes, there are Euclidean cases where the global code $\prod_i f_i$ contains at least one sequence $f_i f_{i+1}$ with $f_{i+1} = f_i^*$. In these cases (whose count is given by the catalan numbers) we can cancel this product in our algorithm taking the resulting constant term into account. Their number for $F = GF(3)$ and $K = GF(3^6)$, $k = 1$ and $m = 1$ is 14224.

Remark 98 In our example, the θ^s invariance (for $s = 3$) does not occur since it would imply the existence of selfdual skew cyclic codes in $K^{\theta^s}[X;\theta]/(X^s - 1)$ and $K^{\theta^s}[X;\theta]/(X^s + 1)$. But as s is odd this can not happen. The θ^2 invariance does obviously not occur either on the f_i's.

References

[Ann09] Guenther Annika. A mass formula for selfdual permutation codes. *Finite Fields and their Applications*, 15:517–533, 2009.

[Art11] M. Artin. *Algebra*. Pearson Education, 2011.

[BBB20] Aicha Batoul, Delphine Boucher, and Ranya Boulanouar. A construction of selfdual skew cyclic and negacyclic codes of length n over $\mathbb{F}_{p^n}$. In *WAIFI 2020: Arithmetic of Finite Fields*, volume 12542 of *Lecture Notes in Computer Science*, RENNES, France, July 2020.

[Ber] Grégory Berhuy. More one vector space duality.

[BGU06] Delphine Boucher, Willi Geiselmann, and Félix Ulmer. Skew-cyclic codes, 2006.

[Bou16] Delphine Boucher. Construction and number of selfdual skew codes over F_{p^2}. *Advances in Mathematics of Communications*, Volume 10(Issue 4):765 – 795, November 2016.

[BU14] Delphine Boucher and Felix Ulmer. Self-dual skew codes and factorization of skew polynomials. *Journal of Symbolic Computation*, 60:47–61, 01 2014.

[CL17] Xavier Caruso and Jérémy Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *Journal of Symbolic Computation*, 79:411–443, 2017.

[Gie98] M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *Journal of Symbolic Computation*, 26(4):463–486, 1998.

[Han05] Genevieve Hanlon. Counting points in sp(2n, fq) maximal parabolic subgroup. 04 2005.

[Jac96] Nathan Jacobson. Finite dimensional division algebras over fields. 1996.

[Mil20] J.S. Milne. *Fields and Galois theory*. 2020.

[PA71] G. Pólya and G.L. Alexanderson. Gaussian binomial coefficients. *Elemente der Mathematik*, 26:102–109, 1971.

[Ple65] V. Pless. The number of isotropic subspaces in a finite geometry. *Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat.*, 39:418–421, 1965.

[Seg59] Beniamino Segre. Le geometrie di galois. *Annali di Matematica Pura ed Applicata*, 48:1–96, 1959.

[Wis91] R. Wisbauer. *Foundations of Module and Ring Theory: A Handbook for Study and Research (1st ed.)*. 1991.