Selfdual skew cyclic codes

Xavier Caruso, Fabrice Drain

Selfdual skew cyclic codes

Xavier Caruso & Fabrice Drain

October 15, 2024

Abstract

Given a finite extension $\mathbf{K}/\mathbf{F}$ of degree r of a finite field $\mathbf{F}$, we enumerate all selfdual skew cyclic codes in the Ore quotient ring $\mathbf{E}_k := \mathbf{K}[X; \mathrm{Frob}]/(X^{rk} - 1)$ for any positive integer k coprime to the characteristic p (separable case). We also provide an enumeration algorithm when k is a power of p (purely inseparable case), at the cost of some redundancies. Our approach is based on an explicit bijection between skew cyclic codes, on the one hand, and certain families of $\mathbf{F}$-linear subspaces of some extensions of $\mathbf{K}$. Finally, we report on an implementation in SageMath.

Contents

1 Introduction

Among linear codes, cyclic codes enjoy a rich algebraic structure as they are defined as ideals of quotient polynomial rings. This structure endows them with good properties (encoding, decoding, duality, dimension, distance, length). In the paper of Boucher, Geiselmann and Ulmer from 2006 [BGU06], cyclic codes are generalized by considering left ideals in Ore polynomial rings rather than in polynomial rings, obtaining thus a much larger class of linear codes called skew cyclic codes. In the present article, following their work, we study the selfdual property of these codes.

Let $\mathbf{K}/\mathbf{F}$ be an extension of finite fields of degree r. Let $\theta : \mathbf{K} \to \mathbf{K}$ be the Frobenius $x \mapsto x^q$ where q denotes the cardinality of $\mathbf{F}$. We consider the Ore polynomial ring $\mathbf{K}[X;\theta]$, defined as the set of classical polynomials equipped with the standard addition and the twisted multiplication derived from the law $X\kappa = \theta(\kappa)X$ where κ is any element of K. Skew cyclic codes are by definition left ideals of a quotient of the form $\mathbf{E}_k := \mathbf{K}[X;\theta]/(X^{rk} - 1)$. We notice that cyclic codes correspond to the special case of skew cyclic codes where $r = 1$.

The ambient space $\mathbf{E}_k$ is equipped with a bilinear form coming from the coordinatewise bilinear form on the vector space $\mathbf{K}^{rk}$, namely

$$\left(\sum_{i=0}^{kr-1} a_i X^i, \sum_{i=0}^{kr-1} x_i X^i\right) \mapsto \sum_{0 \leqslant i < rk} a_i b_i.$$

It thus makes sense to consider duality of skew cyclic codes. The topic was studied by Boucher among others. In her paper [Bou16], an enumeration of selfdual skew cyclic codes for $r = 2$ and for a prime field $\mathbf{F}$, is given. In a subsequent article [BBB20], an enumeration of selfdual skew cyclic codes for any nonnegative integer r, for $k = 1$ and for a prime field $\mathbf{F}$, is provided. In their conclusion, the authors suggest to further count and enumerate all selfdual skew cyclic codes for any values of the order r and of the degree k and for any finite base field $\mathbf{F}$. In the present paper, we give a complete answer to this question when the characteristic p of $\mathbf{F}$ is odd and k is coprime to it (separable case). We also study the case when k is a p-th power (purely inseparable case) and obtain partial result in this case, our enumeration algorithm suffering from some redundancy.

As we will show in Subsection 2.1, r has to be even for selfdual skew cyclic codes to exist. We thus set $r = 2s$. We first consider the separable case, *i.e.* we assume that k is coprime with p. For the purpose of stating our main results, we write $\mathbf{F}[Y]/(Y^k - 1)$ as a product of field extensions of $\mathbf{F}$, namely $\mathbf{F}[Y]/(Y^k - 1) = \prod_{1 \leqslant l \leqslant n} \mathbf{F}_l$ where each $\mathbf{F}_l$ corresponds to an irreducible factor of $Y^k - 1$. We let y_l denote the image of Y in $\mathbf{F}_l$ and we set $\mathbf{K}_l := \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l$. We also consider the involution τ acting on the indices l induced by the involution $Y \mapsto \frac{1}{Y}$ on the irreducible factors of $Y^k - 1$.

Let I be the subset of indexes $l \in \{1, \ldots, n\}$ which are fixed by τ and let $I_{\texttt{eucl}}$ (resp. $I_{\texttt{herm}}$) be the subset of I consisting of indexes l such that $y_l = \pm 1$ (resp. $y_l \neq \pm 1$). Let also J be the set of the nontrivial orbits of τ, $\{l, \tau(l)\}$ over the remaining indexes $l \in \{1, \ldots, n\} \backslash I$. Finally, for each l, we denote by $\mathcal{V}(\mathbf{K}_l/\mathbf{F}_l)$ the set of $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$. When $l \in I_{\texttt{eucl}}$ (resp. $l \in I_{\texttt{herm}}$), we shall further equip $\mathbf{K}_l$ with a $\mathbf{F}_l$-bilinear Euclidean (resp. Hermitian) form; we let $\mathcal{S}_{\texttt{eucl}}(\mathbf{K}_l/\mathbf{F}_l)$ (resp. $\mathcal{S}_{\texttt{herm}}(\mathbf{K}_l/\mathbf{F}_l)$) denote the set of isotropic subspaces of $\mathbf{K}_l$ of dimension $s := r/2$. Our main theorem is as follows.

Theorem 1.1 There exists an explicit bijection between the set of selfdual skew cyclic codes in $\mathbf{E}_k$ and the cartesian product of sets $W_{\mathtt{pal}} \times W_{\mathtt{nonpal}}$, where:

$$\begin{aligned} W_{\mathtt{pal}} &= \prod_{l \in I_{\mathtt{eucl}}} \mathcal{S}_{\mathtt{eucl}}(\mathbf{K}_l/\mathbf{F}_l) \times \prod_{l \in I_{\mathtt{herm}}} \mathcal{S}_{\mathtt{herm}}(\mathbf{K}_l/\mathbf{F}_l) \\ W_{\mathtt{nonpal}} &= \prod_{\{l,\tau(l)\} \in J} \mathcal{V}(\mathbf{K}_l/\mathbf{F}_l) \end{aligned}$$

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

Theorem 1.2 We assume that the caracteristic of $\mathbf{F}$ is odd. Then

- if k is even, there are no selfdual skew cyclic codes in $\mathbf{E}_k$,
- if k is odd, there exist selfdual skew cyclic codes in $\mathbf{E}_k$ if and only if s is even or $q \equiv 1 \pmod 4$.

Moreover, when selfdual codes exist, their number is given by

$$\prod_{l \in I_{\mathtt{eucl}}} \prod_{i=0}^{s-1} \left(q_l^i + 1\right) \times \prod_{l \in I_{\mathtt{herm}}} \prod_{i=0}^{s-1} \left(q_l^{i+1/2} + 1\right) \times \prod_{\{l,\tau(l)\} \in J} \sum_{k=0}^{r} \frac{(q_l^r - 1) \ldots (q_l^{r-k+1} - 1)}{(q_l^k - 1) \ldots (q_l - 1)}$$

where q_l denotes the cardinal of $\mathbf{F}_l$.

We also study the question of finding explicitely selfdual skew cyclic codes in $\mathbf{E}_k$ in odd characteristic. First of all, we describe algorithms, with polynomial complexity in k and r, for generating randomly such a code, with uniform distribution. We then move to the question of complete enumeration. Since selfdual skew cyclic codes are quite numerous (their number grows exponentially with respect to r), it sounds not that interesting to design an algorithm that outputs the complete list of such codes in one shot. Instead, we describe a routine that outputs a new code each time it is called with the guarantee that all codes will show up–and show up only once–at the end of the day. The cost of each indivual call to our algorithm is again polynomial in k and r.

Our method looks robust in the sense that we are confident that it could be adapted to other situations, *e.g.* even characteristic or negacyclic (or more generally, constacyclic) codes instead of cyclic codes. However, addressing the inseparable case where k is not coprime to p using analogue methods seems more delicate (although probably doable). In this paper, we outline a different method for enumerating all purely inseparable selfdual skew cyclic codes, for which k is a power of the characteristic p, by multiplying properly twisted separable selfdual skew cyclic codes with each other as described and illustrated by hand of SageMath computations in Section 4. This enumeration method could easily be used in combination with the enumeration method of the separable case to solve the general inseparable enumeration problem. However, it is not optimal as it comes with redundancies.

Organization of the paper. In Section 2, we define selfdual skew cyclic codes. Then, under the separability hypothesis that k is coprime to p, we relate the skew algebra $\mathbf{E}_k$ to a product of matrix algebras, and we transport the bilinear structure of $\mathbf{E}_k$ onto matrices. In Section 3, we use this reinterpretation to count selfdual skew cyclic codes and to generate them efficiently. In Section 3.5, we report on an implementation of our algorithms and provide some numerical experiments. The source code of the SageMath implementation is available at this location:

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

In Section 4, we sketch an enumeration algorithm for purely inseparable selfdual skew cyclic codes, in the case where k is a power of p. Finally we provide computation results for the enumeration of purely inseparable skew cyclic codes.

Conventions and notations. Throughout this paper, we will use the following notation:

- $\mathrm{End}_R(V)$ denotes, for any ring R and R-module V, the endomorphism ring of R-linear endomorphisms of V.
- $\mathrm{Mat}_{R,r\times r}$ denotes, for any ring R, the matrix ring of $r \times r$ square matrices with entries in R.
- M^{tr} denotes the transpose of the matrix M.
- id denotes the identity morphism.
- $\mathrm{GL}_n(F)$ denotes the general linear group of the vector space F^n over the finite field F.
- L^σ denotes the subfield of L fixed by the automorphism σ.
- $V^\perp$ denotes the orthogonal of the vector subspace V.

If F be a finite field, equipped with an involutive automorphism σ, we recall that a *σ-sesquilinear form* $\mathcal{B}$ of a F-vector space V is an additive map $\mathcal{B} : V \times V \to F$ such that

$$\mathcal{B}(\lambda u, \mu v) = \lambda \cdot \sigma(\mu) \cdot \mathcal{B}(u, v) \qquad \forall u, v \in V, \quad \forall \lambda, \mu \in F$$

In this paper, we will consider four different types of sesquilinear forms:

- (Euclidean case) $\sigma = \mathrm{id}$ and $\mathcal{B}$ is symmetric, *i.e.* $\mathcal{B}(u, v) = \mathcal{B}(v, u)$ for all $u, v \in V$,
- (skew-Euclidean case) $\sigma = \mathrm{id}$ and $\mathcal{B}$ is antisymmetric, *i.e.* $\mathcal{B}(u, v) = -\mathcal{B}(v, u)$ for all $u, v \in V$,
- (Hermitian case) $\sigma \neq \mathrm{id}$ and $\mathcal{B}$ is symmetric,
- (skew-Hermitian case) $\sigma \neq \mathrm{id}$ and $\mathcal{B}$ is antisymmetric.

We recall that, when $\mathcal{B}$ is nondegenerate, the ring $\mathrm{End}_F(V)$ of F-linear endomorphisms of V is equipped with an involutive anti-automorphism $f \mapsto f^\star$ characterized by

$$\forall u, v \in V, \quad \mathcal{B}\big(u, f^\star(v)\big) = \mathcal{B}\big(f(u), v\big)$$

It is called the *adjunction* relative to $\mathcal{B}$. We recall that $(f + g)^\star = f^\star + g^\star$ and $(f \circ g)^\star = g^\star \circ f^\star$ for $f, g \in \mathrm{End}_F(V)$. Moreover, the adjoint of the scalar multiplication by an element $a \in F$ is the multiplication by $\sigma(a)$. The adjoint construction allows finally to endow $\mathrm{End}_F(V)$ itself with a sesquilinear pairing, defined by $\langle f, g\rangle = \mathrm{Trace}(f \circ g^\star)$.

2 From skew cyclic codes to finite geometry

2.1 Definition of skew cyclic codes

Let $\mathbf{F}$ be a finite field of cardinality q and characteristic p. Let $\mathbf{K}$ be a finite extension of $\mathbf{F}$ of degree r. Let $\theta : x \mapsto x^q$ be the Frobenius automorphism of $\mathbf{K}$. We build the quotient of the free $\mathbf{K}$-algebra $\mathbf{K}\langle X\rangle$ by the noncommutative relation: $\forall\kappa \in \mathbf{K}$, $X\kappa = \theta(\kappa)X$. We then localize it at the powers of X. This results in the Ore Laurent polynomial ring $\mathbf{K}[X^{\pm 1};\theta]$. As shown in [Jac96, Theorem 1.1.22], its center is $\mathbf{F}[X] \cap \mathbf{K}[X^{\pm r}] = \mathbf{F}[X^{\pm r}]$. For any $f \in \mathbf{F}[X^{\pm r}]$, we can thus form the quotient $\mathbf{K}[X^{\pm 1};\theta]/(f(X))$, which keeps a ring structure. We will call *skew quotient algebra* the algebra $\mathbf{K}[X^{\pm 1};\theta]/(f(X))$ over its center.

Remark 2.1 As a quotient ring of the left and right Euclidean domain of skew Laurent polynomials, $\mathbf{K}[X^{\pm 1};\theta]$, any skew quotient algebra is a left and right principal ideal ring.

We now move to the definition of selfdual skew cyclic codes. For any nonnegative integer k, $X^{rk} - 1$ is in the center of $\mathbf{K}[X^{\pm 1};\theta]$. We can thus form the quotient ring $\mathbf{E}_k := \mathbf{K}[X^{\pm 1};\theta]/(X^{rk} - 1)$. 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 $\lambda : \mathbf{E}_k \to \mathbf{K}^{rk}$.

Using the classical Hamming distance d on the $\mathbf{K}$-vector space $\mathbf{K}^{rk}$, we define the *Hamming distance* D between two elements f and g of $\mathbf{E}_k$ by $D(f, g) = d(\lambda(f), \lambda(g))$.

Definition 2.2 Given $\alpha \in \mathbf{F}^*$, *skew α-constacyclic codes* are left ideals of $\mathbf{K}[X^{\pm 1};\theta]/(X^{rk} + \alpha)$ endowed with the metric D. *Skew cyclic codes* (resp. *skew negacyclic codes*) are skew α-constacyclic codes for $\alpha = 1$ (resp. $\alpha = -1$).

We are interested in the skew cyclic code duality for the coordinatewise bilinear form, defined on $\mathbf{K}^{rk}$ by

$$\big((x_i)_{0\leqslant i<rk}, (y_i)_{0\leqslant i<rk}\big) \mapsto \sum_{0\leqslant i<rk} x_i y_i$$

We note that this bilinear form is nondegenerate.

Definition 2.3 A skew cyclic code is said *self-orthogonal* (resp. *selfdual*) if $\lambda(I) \subset \lambda(I)^\perp$ (resp. if $\lambda(I) = \lambda(I)^\perp$).

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

2.2 The evaluation isomorphism $\mathcal{E}_l$

We now place ourselves in the separable case, where k is coprime to p. It is then known that $\mathbf{E}_k$ is a semisimple algebra (see [Wis91, Proposition 20.7]). As $\mathbf{E}_k$ is finite-dimensional over $\mathbf{F}$, classical results imply that it is a cartesian product of matrix algebras over finite field extensions of $\mathbf{F}$. Hereunder, we describe an explicit isomorphism realizing this decomposition.

We note $Y := X^r$ and decompose $Y^k - 1$ as a product of irreducible polynomials $P_l(Y)$ over $\mathbf{F}$. We set $\mathbf{F}_l := \mathbf{F}[Y]/P_l(Y)$, $\mathbf{K}_l := \mathbf{K}[Y]/P_l(Y)$ and let y_l denote the image of Y in $\mathbf{K}_l$. We extend θ to an automorphism of $\mathbf{K}_l$ by letting it act trivially on y_l. We have a first decomposition

$$\begin{aligned}\mathbf{E}_k &\simeq \mathbf{K}[Y,X;\theta]/(Y^k-1, X^r-Y)\\ &\simeq \left(\frac{\mathbf{K}[Y,X;\theta]}{\prod\limits_{1\leqslant l\leqslant n} P_l(Y)}\right)/(X^r-Y) = \prod_{1\leqslant l\leqslant n} \mathbf{K}_l[X^{\pm1};\theta]/(X^r-y_l).\end{aligned} \tag{2.1}$$

We set $\tilde{\mathbf{E}}_k^{(l)} = \mathbf{K}_l[X^{\pm1};\theta]/(X^r-y_l)$ and now study each $\tilde{\mathbf{E}}_k^{(l)}$ separately. We observe that $\mathbf{K}_l$ is a finite étale 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, the norm map $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}$ is surjective; hence, there exists an element x_l in $\mathbf{K}_l$ satisfying $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(x_l) = y_l$. The change of variables $X \mapsto x_l X$ defines an isomorphism

$$\mathrm{Eval}_{x_l X} : \tilde{\mathbf{E}}_k^{(l)} \xrightarrow{\sim} \mathbf{E}_k^{(l)} := \mathbf{K}_l[X^{\pm1};\theta]/(X^r-1).$$

On the other hand, we have an evaluation morphism $X \mapsto \theta$:

$$\begin{array}{rccc}\mathrm{Eval}_\theta : & \mathbf{E}_k^{(l)} & \longrightarrow & \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)\\ & P(X) & \mapsto & P(\theta)\end{array}$$

Composing both maps, we obtain a third morphism $\mathcal{E}_l : \tilde{\mathbf{E}}_k^{(l)} \to \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$. Applying it to each term $\tilde{\mathbf{E}}_k^{(l)}$ of the decomposition (2.1), we finally end up with a map relating $\mathbf{E}_k$ to a product of matrix algebras.

Proposition 2.4 The map

$$\left(\mathcal{E}_l\right)_{l\in\{1,\ldots,n\}} : \mathbf{E}_k \longrightarrow \prod_{1\leqslant l\leqslant n} \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

is an isomorphism of $\mathbf{F}$-algebra.

Proof. (See also [Jac96, Theorem 1.3.12].) By Artin's lemma, the family $(\theta^i)_{0\leqslant i<r}$ is linearly independent. This proves the injectivity of $\mathcal{E}_l$. As the dimension (over $\mathbf{F}_l$) of its domain and the codomain are both r^2, surjectivity follows. The final evaluation map resulting from the composition of the chinese remainder isomorphism with the product of isomorphisms $\mathrm{Eval}_{x_l\theta}$ is thus an isomorphism. □

Remark 2.5 To compute the evaluation isomorphism $\mathcal{E}_l$, a fast computation of preimages by the norm is needed. One possible method consists in finding an irreducible factor of the skew polynomial $X^r - y_l$ in $\mathbf{K}_l[X;\theta]$. An algorithm for this task is described in [CL17].

Remark 2.6 By the Skolem-Noether theorem, the isomorphism $\mathcal{E}_l$ is uniquely defined up to conjugacy by an element of norm 1, *i.e.* up to another choice of x_l as preimage of y_l by the norm map.

2.3 Adjunctions on $\mathbf{E}_k$ and related spaces

In this subsection, we construct an alternative $\mathbf{F}$-bilinear pairing on $\mathbf{E}_k$ and show that it induces the same orthogonals than the coordinatewise bilinear form considered previously. Our variant is interesting because it will in turn induce a pairing on the simpler spaces $\mathbf{E}_k^{(l)}$.

We begin by defining an adjunction on $\mathbf{E}_k$. We start from the following $\mathbf{F}$-linear automorphism on $\mathbf{K}[X^{\pm 1};\theta]$

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

It is an involution. One moreover checks that it is an anti-morphism, *i.e.* it satisfies $(fg)^* = g^* f^*$ for all $f, g \in \mathbf{K}[X^{\pm 1};\theta]$. Indeed, by linearity, it is enough to check the desired property when f and g are monomials, which is a direct computation. We observe that the adjoint $(X^{rk} - 1)^*$ is a multiple of $X^{rk} - 1$ itself. The adjunction thus preserves the two-sided ideal generated by $X^{rk} - 1$; therefore, it passes to the quotient to define an anti-automorphism of $\mathbf{E}_k$. In a slight abuse of notation, we continue to write f^* when $f \in \mathbf{E}_k$. Since the adjunction is an anti-automorphism, we underline that it maps left ideals of $\mathbf{E}_k$ to right ideals.

We now define a nondegenerate bilinear form corresponding to this adjunction. We recall to this end that the evaluation of a skew polynomial $f = \sum_{i=0}^{N} f_i X^i$ of $\mathbf{K}[X;\theta]$ at 1 is defined by $f(1) := \sum_{i=0}^{N} f_i$. This definition passes again to the quotient $\mathbf{E}_k$. For $f, g \in \mathbf{E}_k$, we then set

$$\langle f, g \rangle := \mathrm{Trace}_{\mathbf{K}/\mathbf{F}}((fg^*)(1)) \in \mathbf{F}.$$

It is readily seen that $f \mapsto f^*$ satisfies the adjunction formula, in the sense that

$$\langle f, gh \rangle = \mathrm{Trace}_{\mathbf{K}/\mathbf{F}}((f(gh)^*)(1)) = \mathrm{Trace}_{\mathbf{K}/\mathbf{F}}(((fh^*)g^*)(1)) = \langle fh^*, g \rangle$$

for any $f, g, h \in \mathbf{E}_k$. Denoting by $I^\perp$ the orthogonal of $I \subset \mathbf{K}$, we have the following compatibility property.

Proposition 2.7 For any 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 $\mathrm{Trace}_{\mathbf{K}/\mathbf{F}}((fg^*)(1)) = 0$ for all $f \in I$. This holds if and only if $\mathrm{Trace}_{\mathbf{K}/\mathbf{F}}((\kappa fg^*)(1)) = 0$ for all $\kappa \in \mathbf{K}$ and all $f \in I$. By nondegeneracy of $\mathrm{Trace}_{\mathbf{K}/\mathbf{F}}$, the condition is further equivalent to $(fg^*)(1) = 0$ for all $f \in I$. This boils down finally to the orthogonality condition on $\mathbf{K}^{rk}$, namely $\sum_{0 \leqslant i < kr} \lambda(f)_i \lambda(g)_i = 0$ for all $f \in I$. ◻

In what follows, we prefer working with the pairing $\langle -, - \rangle$ because it corresponds to sesquilinear trace forms on the $\mathbf{F}_l$-algebras $\mathbf{E}_k^{(l)}$. We now describe them.

Definition 2.8 We say that a polynomial is *palindromic* if the set of its roots in an algebraic closure of its base field does not contain zero and is stable under the inversion map $x \mapsto \frac{1}{x}$. Equivalently a polynomial $\sum_{i=0}^{n} p_i x^i$ is *palindromic* if it is collinear to its reciprocal polynomial $\sum_{i=0}^{n} p_{n-i} x^{n-i}$.

We recall that we have the decomposition $F[Y]/(Y^k-1) \simeq \prod_{1\leqslant l\leqslant n} F[Y]/P_l(Y) \simeq \prod_{1\leqslant l\leqslant n} \mathbf{F}_l$.

Definition 2.9 We define a map $\tau : \{1,\ldots,n\} \to \{1,\ldots,n\}$ by the relation $P_{\tau(l)}(\frac{1}{y_l}) = 0$.

As the polynomial $Y^k - 1$ is palindromic and separable, the index $\tau(l)$ exists, and τ is obviously involutive. Furthermore, we let σ be the endomorphism of F-algebras of $\mathbf{F}[Y]/(Y^k-1)$ defined by $Y \mapsto \frac{1}{Y}$. It is also involutive. Moreover it induces an isomorphism $\sigma_l : \mathbf{F}_l \to \mathbf{F}_{\tau(l)}$ and we have $\sigma_l(y_l) = y_{\tau(l)}$. The tensor product $\mathrm{id} \otimes \sigma_l$ defines an involutive isomorphism $\mathbf{K}_l \to \mathbf{K}_{\tau(l)}$ extending σ_l. For simplicity, we will keep the notation σ_l for $\mathrm{id} \otimes \sigma_l$.

The next proposition shows that the adjunction behaves nicely with respect to the decomposition $\mathbf{E}_k = \prod_{l=1}^n \tilde{\mathbf{E}}_k^{(l)}$ we have established in Equation (2.1).

Proposition 2.10 The adjunction $f \mapsto f^*$ induces "partial" adjunctions $\tilde{\mathbf{E}}_k^{(l)} \to \tilde{\mathbf{E}}_k^{(\tau(l))}$, which are explicitly given by the formula

$$\sum_{i=0}^{\deg P_l - 1} f_i X^i \mapsto \sum_{i=0}^{\deg P_l - 1} X^{-i} \sigma_l(f_i), \quad \forall f_i \in \mathbf{K}_l. \tag{2.2}$$

Moreover, the "global" adjunction can be recovered by taking the product of the partial ones.

Proof. Let Q_l be the idempotent element of $F[Y]/(Y^k-1) \subset \mathbf{E}_k$ corresponding to the factor $\mathbf{F}_l$, *i.e.* the element defined by the congruences $Q_l \equiv 1 \pmod{P_l}$ and $Q_l \equiv 0 \pmod{P_{l'}}$ whenever $l' \neq l$. As automorphisms respect congruences, we have $Q_l^* = \sigma(Q_l) = Q_{\tau(l)}$. Besides $\tilde{\mathbf{E}}_k^{(l)} = Q_l \mathbf{E}_k = \mathbf{E}_k Q_l$. We thus have $\tilde{\mathbf{E}}_k^{(l)*} = (Q_l \mathbf{E}_k)^* = \mathbf{E}_k Q_l^* = \mathbf{E}_k Q_{\tau(l)} = \tilde{\mathbf{E}}_k^{(\tau(l))}$. The explicit formula (2.2) is derived after noticing that $f_i^* = \sigma_l(f_i)$ for $f_i \in \mathbf{K}_l$. Finally, the last statement of the proposition is clear. $\square$

We now aim at describing how the adjunction is transformed by the evaluation isomorphisms $\mathcal{E}_l$. For this, the first step is to understand its effect on $\mathbf{E}_k^{(l)}$ (without the tilde) which, we recall, is defined as $\mathbf{E}_k^{(l)} = \mathbf{K}_l[X;\theta]/(X^r-1)$. The adjunction $f \mapsto f^*$ again passes to the quotient and determines a well-defined adjunction $\mathbf{E}_k^{(l)} \to \mathbf{E}_k^{(\tau(l))}$, that we continue to denote $f \mapsto f^*$. Unfortunately, the latter is not exactly what we need; we are now going to fix this issue by defining a twisting version of it. For this, we first define $z_l := x_l \cdot \sigma_{\tau(l)}(x_{\tau(l)}) \in \mathbf{K}_l$.

Lemma 2.11 There exists a family of nonzero elements $\zeta_l \in \mathbf{K}_l$ such that $\theta(\zeta_l) = z_l \zeta_l$ and $\sigma_l(\zeta_l) = \zeta_{\tau(l)}$ for all l.

Proof. Since $\sigma_l \circ \sigma_{\tau(l)} = \mathrm{id}$, we have $\sigma_l(x_l \cdot \sigma_{\tau(l)}(x_{\tau(l)})) = x_{\tau(l)} \sigma_l(x_l)$, which ensures that z_l is invariant under σ_l. Furthermore, we observe that $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(z_l) = y_l \cdot \sigma_{\tau(l)}(y_{\tau(l)}) = 1$. Hence, the Hilbert 90 Theorem guarantees the existence of an element ζ_l of $\mathbf{K}_l^*$ such that $\theta(\zeta_l) = z_l \zeta_l$ and hence $z_l X = \zeta_l^{-1} X \zeta_l$. Moreover, as automorphisms of finite fields commute, $\sigma_l(\zeta_l)$ satisfies $\theta(\sigma_l(\zeta_l)) = z_l \sigma_l(\zeta_l)$. Set $\zeta_l' := \zeta_l + \sigma_{\tau(l)}(\zeta_{\tau(l)})$, so that we have $\sigma_l(\zeta_l') = \zeta_{\tau(l)}'$. If $\zeta_l' \neq 0$, it satisfies $z_l X = \zeta_l'^{-1} X \zeta_l'$ as well. On the contrary, if $\zeta_l' = 0$, we have $\sigma_{\tau(l)}(\zeta_{\tau(l)}) = -\zeta_l$. In this case, σ_l is nontrivial and so $y_{\tau(l)} \neq \pm 1$. As $\frac{\zeta_l}{y_l}$ satisfies also $\theta\big(\frac{\zeta_l}{y_l}\big) = z_l \frac{\zeta_l}{y_l}$, the element $\zeta_l'' := \frac{\zeta_l}{y_l} + \sigma_{\tau(l)}\big(\frac{\zeta_{\tau(l)}}{y_{\tau(l)}}\big) = \zeta_l\big(\frac{1}{y_l} - y_l\big)$ is nonzero and satisfies $z_l X = \zeta_l''^{-1} X \zeta_l''$. Since we moreover have $\sigma_l(\zeta_l'') = \zeta_{\tau(l)}''$, the lemma is proved. $\square$

Remark 2.12 The element ζ_l can be efficiently computed using the following formula from the proof of the Hilbert 90 Theorem: it can be chosen as the multiplicative inverse of any nonzero element in the image of the endomorphism $\sum_{0\leqslant i<r}\prod_{0\leqslant j<i}\theta^j(z_l)\theta^i$.

Definition 2.13 For $f \in \mathbf{E}_k^{(l)}$, we set $f^\bullet := (\zeta_l f \zeta_l^{-1})^* = \zeta_{\tau(l)}^{-1} f^* \zeta_{\tau(l)} \in \mathbf{E}_k^{(\tau(l))}$.

Lemma 2.14 For all $f \in \tilde{\mathbf{E}}_k^{(l)}$, we have $f^*(x_{\tau(l)}X) = f(x_l X)^\bullet$.

Proof. By additivity, it is enough to check the formula when f is the monomial κX^i. We thus have $f^* = X^{-i}\sigma_l(\kappa)$ and so

$$\begin{aligned} f^*(x_{\tau(l)}X) &= X^{-i}\sigma_l(\kappa)\left(\prod_{t=0}^{i-1}\theta^t(x_{\tau(l)})\right)^{-1} \\ f(x_l X)^\bullet &= \left(\kappa\prod_{t=0}^{i-1}\theta^t(x_l)X^i\right)^\bullet = (z_{\tau(l)}X)^{-i}\sigma_l\left(\kappa\prod_{t=0}^{i-1}\theta^t(x_l)\right). \end{aligned}$$

We conclude by noticing that $\prod_{t=0}^{i-1}\theta^t(z_{\tau(l)}) = \prod_{t=0}^{i-1}\theta^t(x_{\tau(l)})\sigma_l\left(\prod_{t=0}^{i-1}\theta^t(x_l)\right)$. ☐

Following the isomorphism $\mathbf{E}_k^{(l)} \simeq \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ and its counterpart for $\tau(l)$, we find that the adjunction $f \mapsto f^\bullet$ induces another anti-isomorphism $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l) \xrightarrow{\bullet} \mathrm{End}_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)})$. We are now going to prove that the latter is the adjunction map associated to some explicit bilinear map. Precisely, we introduce the twisted bilinear trace form

$$\begin{array}{rcl} \mathbf{K}_l \times \mathbf{K}_{\tau(l)} & \longrightarrow & \mathbf{F}_l \\ (\kappa,\rho) & \mapsto & (\kappa,\rho)_{\mathbf{F}_l} := \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l\cdot\kappa\cdot\sigma_{\tau(l)}(\rho)) \end{array} \tag{2.3}$$

In the palindromic case, we have $\mathbf{K}_{\tau(l)} = \mathbf{K}_l$ and we observe that the above pairing is Euclidean when $y_l = \pm 1$ and Hermitian otherwise. In all cases, the bilinear form $(-,-)_{\mathbf{F}_l}$ is nondegenerate and hence identifies $\mathbf{K}_l$ with the dual of $\mathbf{K}_{\tau(l)}$.

Proposition 2.15 The involutive isomorphism $\bullet$ is the adjunction relative to $(-,-)_{\mathbf{F}_l}$, *i.e.*

$$(f(\kappa),\rho)_{\mathbf{F}_l} = (\kappa, f^\bullet(\rho))_{\mathbf{F}_l}, \qquad \forall f\in\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l), \quad \forall\kappa\in\mathbf{K}_l, \quad \forall\rho\in\mathbf{K}_{\tau(l)}.$$

Proof. We write $f = \sum_{0\leqslant i\leqslant r-1} f_i\theta^i$ with $f_i \in \mathbf{K}_l$ and compute

$$\begin{aligned} (f(\kappa),\rho)_{\mathbf{F}_l} &= \sum_{k=0}^{r-1}\theta^k\left(\zeta_l\cdot\sigma_{\tau(l)}(\rho)\cdot\sum_{i=0}^{r-1}f_i\theta^i(\kappa)\right) \\ &= \sum_{i=0}^{r-1}\sum_{k=0}^{r-1}\theta^{k+i}\left(\zeta_l\cdot\theta^{-i}(f_i)\cdot\frac{\theta^{-i}(\zeta_l)}{\zeta_l}\cdot\theta^{-i}(\sigma_{\tau(l)}(\rho))\cdot\kappa\right) \\ &= \sum_{k=0}^{r-1}\theta^k\left(\sum_{i=0}^{r-1}\zeta_l\cdot\theta^{-i}(f_i)\cdot\theta^{-i}(\zeta_l\sigma_{\tau(l)}(\rho))\cdot\zeta_l^{-1}\cdot\kappa\right) \\ &= \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l\cdot\sigma_{\tau(l)}(f^\bullet(\rho))\cdot\kappa) = (\kappa,f^\bullet(\rho))_{\mathbf{F}_l} \end{aligned}$$

which is exactly what we want. ☐

Finally, composing the morphisms $X \mapsto x_l X$ and $X \mapsto \theta$, we obtain the following commutative diagram:

$$\begin{tikzcd}
\tilde{\mathbf{E}}_k^{(l)} \arrow[r, "X\mapsto x_l X"] \arrow[d, "f\mapsto f^*"] & \mathbf{E}_k^{(l)} \arrow[r, "X\mapsto\theta"] \arrow[d, "f\mapsto f^\bullet"] & \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l) \arrow[d, "\text{adjunction for } (-,-)_{\mathbf{F}_l}"] \\
\tilde{\mathbf{E}}_k^{(\tau(l))} \arrow[r, "X\mapsto x_{\tau(l)} X"] & \mathbf{E}_k^{(\tau(l))} \arrow[r, "X\mapsto\theta"] & \mathrm{End}_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)})
\end{tikzcd} \tag{2.4}$$

where we note that the composite of the horizontal maps is $\mathcal{E}_l$ on the top, and $\mathcal{E}_{\tau(l)}$ on the bottom.

2.4 Vector space duality

In the previous subsections, we reduced the problem of finding selfdual skew cyclic codes in $\mathbf{E}_k$ to that of finding selfdual skew cyclic codes in the product of the $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$. We will now further reduce this problem to that of finding maximal isotropic $\mathbf{F}_l$-vector spaces of $\mathbf{K}_l$ in the palindromic case and of $\mathbf{K}_l \times \mathbf{K}_{\tau(l)}$ in the nonpalindromic case.

To this end, we apply the classical duality between $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ and left ideals of $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ [Ber]. Let us recall it briefly. Given a field F and a finite dimensional F-vector space W, the *vector space duality* associates to every F-vector subspace V of W, the left ideal I_V of $\mathrm{End}_F(W)$ formed by the endomorphisms vanishing on V. Dually, it associates to every left ideal I of $\mathrm{End}_F(W)$, the intersection of the kernels of the morphisms in I. With formulas, it can be expressed as

$$\begin{aligned} I \mapsto V_I &= \bigcap_{f\in I} \ker(f), \\ V \mapsto I_V &= \big\{\, f \in \mathrm{End}_F(W) \,|\, V \subset \ker(f) \,\big\}. \end{aligned}$$

This duality defined an order-reversing one-to-one correspondence between the set of left ideals of $\mathrm{End}_F(W)$ and the set of F-vector subspaces of W. Moreover, for all $V \subset W$, we have $\dim_F I_V = (\dim_F W - \dim_F V) \cdot \dim_F W$.

We now assume in addition that we are given an involution $\sigma : F \to F$ and that W is endowed with a nondegenerate σ-sesquilinear form. We recall that this datum equips $\mathrm{End}_F(W)$ with a sesquilinear form as well. In particular, taking orthogonals over W and $\mathrm{End}_F(W)$ makes sense.

Proposition 2.16 For all subspace V of W, we have $I_V^\perp = I_{V^\perp}$.

Proof. Given $f \in I_V$ and $g \in I_{V^\perp}$, we have $f \circ g^\star = 0$ since f vanishes on V and $\mathrm{im}\, g^\star = (\ker g)^\perp \subset V$. Therefore f and g are orthogonal in $\mathrm{End}_F(W)$. It follows that $I_V^\perp \subset I_{V^\perp}$. The equality follows by comparing dimensions. ☐

We are now ready to apply what precedes to codes and prove the main theorem of this section.

Theorem 2.17 There exists an explicit bijection between the set of selfdual skew cyclic codes of $\mathbf{E}_k$ and the cartesian product of sets $W_{\mathtt{pal}} \times W_{\mathtt{nonpal}}$, where:

- $W_{\mathtt{pal}}$ is the cartesian product, over the set I of indexes invariant under τ, of the sets of isotropic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ of dimension $r/2$,

- $W_{\texttt{nonpal}}$ is the cartesian product, over the set J of all remaining nontrivial orbits of τ, of the sets of $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$.

Proof. By what we have done in previous subsections, selfdual codes in $\mathbf{E}_k$ are in bijection with left ideals of the cartesian product

$$\prod_{l=1}^{n} \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

that are equal to their orthogonal. Besides, the orthogonal of an ideal can be taken component by component, with the care that the orthogonal of the l-th component lies in the $\tau(l)$-th component. Therefore, when $\tau(l) = l$, the l-th component must be selfdual itself whereas, when $\tau(l) \neq l$, the component at position l can be anything but it determines the component at position $\tau(l)$. Using now the vector space duality, we can further replace ideals of $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ by $\mathbf{F}_l$-subspaces of $\mathbf{K}_l$. This operation preserves the orthogonality condition as the vector space duality commutes with orthogonals.

We finally conclude by noticing that a subspace of $\mathbf{K}_l$ which is equal to its orthogonal is nothing else than an isotropic subspace of half dimension, that is of dimension $r/2$. $\square$

3 Counting and generating selfdual skew cyclic codes

We keep the notation introduced before. In particular, we recall that $\mathbf{K}/\mathbf{F}$ is an extension of finite fields of degree r and that $\mathbf{E}_k = \mathbf{K}[X;\theta]/(X^{kr}-1)$ (where $\theta : x \mapsto x^q$ with $q = \mathrm{Card}\ \mathbf{F}$). Besides, we set $Y = X^r$ and assume that k is coprime with r. Under this hypothesis, the polynomial $Y^k - 1$ is separable and we write down its decomposition as a product of irreductible factors $Y^k - 1 = P_1(Y)\cdots P_n(Y)$. We recall also that we have introduced an involution $\tau : \{1,\ldots,n\} \to \{1,\ldots,n\}$ defined by the condition that the roots of P_l and the inverses of the roots of $P_{\tau(l)}$. In Subsection 2.2, we proved that we have an isomorphism of the form

$$\mathbf{E}_k \simeq \prod_{l=1}^{s} \mathbf{K}_l[X;\theta]/(X^r - y_l) \simeq \prod_{l=1}^{s} \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

where $\mathbf{F}_l = \mathbf{F}[Y]/P_l(Y)$, $\mathbf{K}_l = \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l = \mathbf{K}[Y]/P_l(Y)$ and y_l is the image of Y in $\mathbf{K}_l$. In Subsection 2.3, we showed that this decomposition preserves orthogonality in some precise sense. This allowed us to conclude (see Theorem 2.17) that enumerating selfdual skew cyclic codes sitting in $\mathbf{E}_k$ boils down to enumerating maximal isotropic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ when $\tau(l) = l$ (palindromic case), and to enumerating $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ otherwise.

In this section, we rely on this theoretical result, first, to count skew cyclic codes and, second, to construct them explicitely. More precisely, we shall address two different problems: that of random generation and that of complete enumeration.

Throughout this section, we assume that the caracteristic of $\mathbf{F}$ *is odd.*

3.1 Existence criterion

By Theorem 2.17, there exist selfdual codes in $\mathbf{E}_k$ if and only if for each l such that $\tau(l) = l$, the space $\mathbf{K}_l$ admits a totally isotropic subspace of dimension $s := r/2$. We then aim at providing simpler conditions for this property to hold. For this, we shall use Witt's decomposition theorem as a fundamental tool. Let us recall it briefly. Let F be a field of odd characteristic, and let $\sigma : F \to F$ be a ring homomorphism which is an involution (possibly the identity). Let also V be a finite dimension vector space over F, endowed with a σ-sesquilinear form $\mathcal{B} : V \times V \to F$. We recall that a *hyperbolic pair* is a pair of vectors (u, v) of V satisfying $\mathcal{B}(u, u) = 0$, $\mathcal{B}(v, v) = 0$ and $\mathcal{B}(u, v) = 1$, and that the 2-dimensional subspace of V spanned by a hyperbolic pair (u, v) is called a *hyperbolic plane*.

Theorem 3.1 Keeping the previous notation, there exists an invariant d (called the Witt index of V) and hyperbolic planes $H_1, \ldots, H_d$ such that one has the orthogonal decomposition

$$V \simeq \left(\bigoplus_{1 \leqslant i \leqslant d} H_i \right) \oplus W$$

where W is a subspace that does not contain any nonzero isotropic vector.

Moreover, the dimension of any maximal isotropic space is equal to d.

Proof. See for instance [Art11, Theorem 3.11]. □

When F is a finite field, more can be said. For simplicity, we assume that $\dim V = 2s$. If $\sigma \neq \mathrm{id}$, the Witt index of V is always s. On the contrary, when $\sigma = \mathrm{id}$, it can be either s or $s-1$ but we can decide between those two values by looking at the discriminant δ_V of V (defined as the determinant of the matrix of $\mathcal{B}$ is some basis); precisely, the Witt index is s if and only if $(-1)^s \delta_V$ is a square in $F^\times$. (See [Sch85, Theorem 3.3] for more details.)

In our case, Theorem 2.17 tells us that we are looking for isotropic vectors of dimension s in $\mathbf{K}_l$; we recall from Equation (2.3) that the latter is endowed with the sesquilinear form

$$(\kappa, \rho)_{\mathbf{F}_l} = \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l \cdot \kappa \cdot \sigma_{\tau(l)}(\rho))$$

where $\sigma_{\tau(l)} : \mathbf{K}_{\tau(l)} \to \mathbf{K}_l$ is the map induced by $\sigma_{\tau(l)}(Y) = \frac{1}{Y}$ and ζ_l is an element of $\mathbf{K}_l$ defined in Lemma 2.11. We then need to compute the discriminant δ_{ζ_l} of this sesquilinear form.

Lemma 3.2 We assume that $\sigma_l = \mathrm{id}$ and we let $\delta_{\mathbf{K}_l/\mathbf{F}_l}$ be the discriminant of the extension $\mathbf{K}_l/\mathbf{F}_l$ (which is, by definition, the discriminant of the bilinear form $(\kappa, \rho) \mapsto \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\kappa\rho)$). Then

1. the discriminant δ_{ζ_l} is equal to $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l) \cdot \delta_{\mathbf{K}_l/\mathbf{F}_l}$,
2. the discriminant $\delta_{\mathbf{K}_l/\mathbf{F}_l}$ is a square in $\mathbf{F}_l$ if and only if the degree of the extension $[\mathbf{F}_l : \mathbf{F}]$ is even,
3. if $y_l = 1$ (resp. $y_l = -1$), $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)$ is a square (resp. is not a square) in $\mathbf{F}_l$.

Proof. 1. We fix a basis of $\mathbf{K}_l$ over $\mathbf{F}_l$ and write $\mathrm{Mat}(\zeta_l)$ for the matrix representing the multiplication by ζ_l in this basis. Then $\delta_{\zeta_l} = \det\left(\mathrm{Mat}(\zeta_l)^{\mathrm{tr}}\right) \cdot \delta_{\mathbf{K}_l/\mathbf{F}_l} = \mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l) \cdot \delta_{\mathbf{K}_l/\mathbf{F}_l}$.

2. From $\mathbf{K}_l = \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l$, we deduce that $\delta_{\mathbf{K}_l/\mathbf{F}_l} = \delta_{\mathbf{K}/\mathbf{F}} \in \mathbf{F}$. Moreover, we know that $\delta_{\mathbf{K}/\mathbf{F}}$ is a square in $\mathbf{F}$ if and only if the Galois group of $\mathbf{K}/\mathbf{F}$ is a subgroup of the alternating group (see [Mil20, Corollary 4.2]), which never occurs in our situation given that $\mathrm{Gal}(\mathbf{K}/\mathbf{F})$ is a cyclic group of even cardinality. We conclude that $\delta_{\mathbf{K}/\mathbf{F}}$ is a square in $\mathbf{F}_l$ if and only if the extension $\mathbf{F}_l/\mathbf{F}$ has even degree.
3. We assume that $y_l = \pm 1$ and compute

$$\begin{aligned}\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)^{\frac{q-1}{2}} &= \left(\zeta_l^{\sum_{0\leqslant i<2s} q^i}\right)^{\frac{q-1}{2}} \\ &= \left(\zeta_l^{q-1}\right)^{\frac{\sum_{0\leqslant i<2s} q^i}{2}} = \left(x_l\sigma_l(x_l)\right)^{\frac{\sum_{0\leqslant i<2s} q^i}{2}}\end{aligned}$$

As $y_l = \pm 1$, the automorphism σ_l is the identity and so $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)^{\frac{q-1}{2}} = y_l$. We conclude by applying Euler's criterion. ☐

Corollary 3.3 We assume that the caracteristic of $\mathbf{F}$ is odd.

1. If k is even, there are no selfdual skew cyclic codes in $\mathbf{E}_k$.
2. If k is odd, there exist selfdual skew cyclic codes in $\mathbf{E}_k$ if and only if $(-1)^s$ is a square in $\mathbf{F}$, if and only if s is even or $q \equiv 1 \pmod 4$.

Proof. We first notice that, whenever $y_l \neq \pm 1$, there is no obstruction to the existence of an isotropic subspace of half dimension. On the contrary, when $y_l = 1$ (resp. $y_l = -1$), it follows from Lemma 3.2 that an isotropic subspace of $\mathbf{K}$ of dimension s exists if and only if $(-1)^s$ is a square (resp. is not a square) in $\mathbf{F}$.

When k is even, the decomposition of $\mathbf{E}_k$ exhibits both factors $\mathbf{K}[X;\theta]/(X^r+1)$ and $\mathbf{K}[X;\theta]/(X^r-1)$. Since $(-1)^s$ cannot be simultaneously a square and a nonsquare, we conclude that selfdual skew cyclic codes cannot exist in this case. On the contrary, when k is odd, the factor $\mathbf{K}[X;\theta]/(X^r+1)$ does not show up and we are left to the condition corresponding to $y_l = 1$.

Finally, the fact that if $(-1)^s$ is a square in $\mathbf{F}$ if and only if s is even or $q \equiv 1 \pmod 4$ is a direct application of Euler's criterion. ☐

3.2 Counting selfdual skew cyclic codes

We now aim at counting the number of selfdual codes sitting in $\mathbf{E}_k$, when they exist. In what follows, we then assume that the existence criterion of Corollary 3.3 is fulfilled. It follows from Theorem 2.17 that out task reduces to finding the cardinality of $W_{\texttt{pal}}$ and $W_{\texttt{nonpal}}$.

3.2.1 The nonpalindromic case

We start by the nonpalindromic case, which is by far the easiest. For this counting, we will use q-analogues of integers. We recall briefly that the q-analogue of $n \in \mathbf{N}$ is, by definition, $[n]_q := 1 + q + q^2 + \cdots + q^{n-1}$. The q-factorial of n is defined by $[n]_q! = [1]_q[2]_q \ldots [n]_q$ and we set

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{[n]_q!}{[k]_q!\,[n-k]_q!} = \frac{(1-q^n)(1-q^{n-1})\ldots(1-q^{n-k+1})}{(1-q)(1-q^2)\ldots(1-q^k)}$$

where n and k are nonnegative integers with $k \leqslant n$. It is a classical fact that the q-binomial coefficients count the number of $\mathbb{F}_q$-vector subspaces of dimension k in the ambient $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$.

Therefore, with the notation of Theorem 2.17, we have

$$\mathrm{Card}(W_{\texttt{nonpal}}) = \prod_{\{l,\tau(l)\}\in J} \left(\sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix}_{q_l} \right). \tag{3.1}$$

3.2.2 The palindromic case

If V is a finite dimensional vector space equipped with a sesquilinear form, we denote by $\mathrm{Iso}(V)$ the number of isotropic subspaces of V of half dimension. It turns out that the behaviour of $\mathrm{Iso}(V)$ have been studied for a long time (see for instance [Seg59, Ple65, BBB20]) and that explicit formulas are known. Those are called Segre's formulas and are recalled in the following theorem.

Theorem 3.4 Let F be a finite field of odd caracteristic and cardinality q_F and let $\sigma : F \to F$ be an involutive ring automorphism. Let V be a F-vector space of dimension $2s$ equipped with a nondegenerate σ-sesquilinear form, whose Witt index is s. Then:

1. if $\sigma = \mathrm{id}$ (Euclidean case), then $\mathrm{Iso}(V) = \prod_{i=0}^{s-1} \left(q_F^i + 1\right)$,
2. if $\sigma \neq \mathrm{id}$ (Hermitian case), then $\mathrm{Iso}(V) = \prod_{i=0}^{s-1} \left(q_F^{i+1/2} + 1\right)$.

Proof. We recall briefly the idea of the proof as it will be useful afterwards. Let $\mathrm{iso}(W)$ be the number of isotropic vectors in a Euclidean or Hermitian vector space W over F. We claim that, if W has dimension $2d$ and Witt index d, then

1. if $\sigma = \mathrm{id}$ (Euclidean case), then $\mathrm{iso}(W) = (q_F^d - 1)(q_F^{d-1} + 1)$,
2. if $\sigma \neq \mathrm{id}$ (Hermitian case), then $\mathrm{iso}(W) = (q_F^d - 1)(q_F^{d-1/2} + 1)$

Indeed, let us fix an isotropic basis $((u_i)_{0\leqslant i<s}, (v_i)_{0\leqslant i<s})$ corresponding to the Witt's decomposition of W (see Theorem 3.1) and let $((a_i)_{0\leqslant i<s}, (b_i)_{0\leqslant i<s})$ be the coordinates in this basis of a vector. In the Euclidean case, the fact that this vector is isotropic reduces to the equation $\sum_{0\leqslant i<s} a_i b_i = 0$. Now, fixing a nonzero vector $(a_i)_{0\leqslant i<s}$ of $\mathbf{F}_l^s$, this occurs if and only if $(b_i)_{0\leqslant i<s}$ lies in some hyperplane. We thus have $(q_F^s - 1)q_F^{s-1}$ solutions corresponding to nonzero $(a_i)_{0\leqslant i<s}$, to which one should add $(q_F^s - 1)$ more solutions when all a_i vanish. Finally, we get $\mathrm{iso}(W) = (q_F^d - 1)(q_F^{d-1} + 1)$ as claimed.

The Hermitian case is similar, expect that the equation to solve is now $\sum_{0\leqslant i<s} \sigma_l(a_i) b_i + \sum a_i \sigma_l(b_i) = 0$, which reduces to $\sum_{0\leqslant i<s} a_i \sigma_l(b_i) = \alpha$ where α satisfies $\sigma_l(\alpha) = -\alpha$. We conclude repeating the argument of the Euclidean case and using that there are exacly $q_F^{1/2}$ values for α.

We are now ready to prove Segre's formula. We start by taking $W_0 = V$ and by picking an isotropic vector w_0 in W. This corresponds to iso_s possibilities. Once this is achieved, we set $W_1 := (Fw_0)^\perp / Fw_0$. This is a space of dimension $2(s-1)$, whose Witt index is $s-1$. Therefore, we can apply again our claim and find that there are exactly iso_{s-1} isotropic vectors in W_1. We choose one of them, that we denote by w_1. Now we repeat the argument until we reach w_{s-1}. This corresponds to $\mathrm{iso}(W_0) \cdot \mathrm{iso}(W_1) \cdots \mathrm{iso}(W_{s-1})$

choices. However, each of them corresponds $q_F \cdot q_F^2 \cdots q_F^{s-1} = q_F^{s(s-1)/2}$ choices of families of vecteurs of V since w_i has q^i preimages in V. We conclude that the number of bases of a maximal isotropic subspace of V is equal to $q_F^{s(s-1)/2} \cdot \mathrm{iso}(W_0) \cdot \mathrm{iso}(W_1) \cdots \mathrm{iso}(W_{s-1})$. We finally obtain $\mathrm{Iso}(V)$ by dividing by the cardinality of $\mathrm{GL}_s(F)$. $\square$

Remark 3.5 In the Euclidean case, one can alternatively prove Segre's formula by remarking that the orthogonal group of V acts transitively on the set of maximal isotropic subspaces and that the stabilizer of a given maximal isotropic subspace U can be presented as a semi-direct product of $\mathrm{GL}(U)$ and the group of antisymmetric linear applications from U to its dual $\mathrm{Hom}_F(U, F)$. From this description we find that the number of maximal isotropic subspaces is

$$\frac{\mathrm{Card}\big(O_{2s}(F)\big)}{q_F^{s(s-1)/2} \cdot \mathrm{Card}\big(\mathrm{GL}_s(F)\big)}$$

a formula from which one can eventually derive Segre's theorem. A similar approach also works in the Hermitian case.

Keeping the notation of Theorem 2.17, it follows from Theorem 3.4 that

$$\mathrm{Card}(W_{\mathtt{pal}}) = \prod_{\substack{l \in I \\ y_l = \pm 1}} \prod_{i=0}^{s-1} \left(q_l^i + 1\right) \times \prod_{\substack{l \in I \\ y_l \neq \pm 1}} \prod_{i=0}^{s-1} \left(q_l^{i+1/2} + 1\right). \tag{3.2}$$

We notice moreover that there is always exactly one index l for which $y_l = 1$, and there is at most one index l such that $y_l = -1$ (such an index actually exists if and only if k is even). In both cases, the corresponding field $\mathbf{F}_l$ is $\mathbf{F}$, and so $q_l = q$.

Now combining Equations (3.1) and (3.2), we get the number of selfdual skew cyclic codes sitting in $\mathbf{E}_k$, which proves Theorem 1.2.

Example 3.6 For $\mathbf{K} = \mathbb{F}_{q^{2s}}$ and $\theta : x \mapsto x^q$, the number of selfdual skew cyclic codes is equivalent to $q^{\frac{s(s-1)}{2}}$ as s grows to infinity, whereas the number of skew cyclic codes (number of s dimensional $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^{2s}}$) is equivalent to q^{s^2} as s grows to infinity.

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

Remark 3.7 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. Nevertheless, 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.

3.3 Random generation of selfdual skew cyclic codes

Since the number of selfdual skew cyclic codes grows exponentially fast with respect to the dimension r, an algorithm outputting in one shot the complete list of these codes would be necessarily very unefficient (the better we can expect is exponential complexity) and hence, probably not quite useful. Instead, in what follows, we address a different question, which is that of random generation: we aim at finding a fast algorithm that outputs a unique code in this huge list with the guarantee that the returned code is *uniformly distributed* among all of them. Such an algorithm could be very useful to generate *typical* selfdual skew cyclic codes and to check their properties.

3.3.1 From skew cyclic codes to finite geometry: explicit methods

Before designing our algorithms, we need to explain how we represent the objects on the computer. We recall that a skew cyclic code is, by definition, a left ideal of $\mathbf{E}_k = \mathbf{K}[X;\theta]/(X^{kr}-1)$. Hence it necessarily has the form $\mathbf{E}_k f$ for some $f \in \mathbf{K}[X;\theta]$. We can further normalize this generator by requiring that it is monic and has minimal degree; normalizing a generator amounts to replacing f by $\operatorname{rgcd}(f, X^{kr}-1)$ (where rgcd denotes the right gcd). The same discussion applies similarly to all quotients of a Ore polynomial ring by a two-sided ideal and so, in particular, to $\mathbf{K}[X;\theta]/P_l(Y)$ and the algebras $\tilde{\mathbf{E}}_k^{(l)} = \mathbf{K}_l[X;\theta]/(X^r - y_l)$.

We recall further that we have the following sequence of isomorphisms:

$$\mathbf{E}_k \simeq \prod_{l=1}^{n} \mathbf{K}[X;\theta]/P_l(Y) \simeq \prod_{l=1}^{n} \tilde{\mathbf{E}}_k^{(l)} \simeq \prod_{l=1}^{n} \operatorname{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

and that the left ideals of $\operatorname{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ are in one-to-one correspondence with the $\mathbf{F}_l$-linear subspaces of $\mathbf{K}_l$ (see Subsection 2.4). We aim at making explicit all these identifications.

Going back and forth between $\mathbf{E}_k$ and $\prod_{l=1}^{n} \tilde{\mathbf{E}}_k$ is not difficult. Indeed, if a code sitting in $\mathbf{E}_k$ is generated by f, its image in $\mathbf{E}_k$ will be generated by f as well. Conversely, if one starts with a family of codes $\big(\tilde{\mathbf{E}}_k^{(l)} f_l\big)_{1\leqslant l\leqslant n}$, its preimage in $\mathbf{E}_k$ is the code generated by a Ore polynomial f satisfying the set of congruences

$$f \equiv f_l \pmod{P_l(Y)} \qquad (1 \leqslant l \leqslant n). \tag{3.3}$$

We need to be careful however that f_l has *a priori* coefficients in $\mathbf{K}_l$; in order to view it as a Ore polynomial in $\mathbf{K}[X;\theta]$, we have to replace each occurrence of y_l by $Y = X^r$. The system of congruences (3.3) can then be solved using the Chinese Remainder Theorem; we underline that noncommutativity is not an issue here because all the moduli $P_l(Y)$ lie in the center. We also stress that the solution f to (3.3) is in general not normalized, even if the f_l are; if one wants to normalize it, one needs to compute an additional rgcd.

We now explain how to navigate between $\tilde{\mathbf{E}}_k^{(l)}$ and $\operatorname{End}_{\mathbf{F}_l}(\mathbf{K}_l)$. We first recall that the isomorphism between those two rings is given by $X \mapsto x_i\theta$. Hence the ideal of $\operatorname{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ that corresponds to the ideal $\tilde{\mathbf{E}}_k^{(l)} f$ of $\tilde{\mathbf{E}}_k^{(l)}$ is the ideal consisting on linear maps vanishing on the kernel of $f(x_i\theta)$. The associated $\mathbf{F}_l$-linear of $\mathbf{K}_l$ is then just $\ker f(x_l\theta)$. The correspondence in the other direction is also given by an explicit formula: if V is a $\mathbf{F}_l$-subvector space of $\mathbf{K}_l$ and $(v_1, \ldots, v_d)$ is a basis of V, a generator of the ideal of $\tilde{\mathbf{E}}_k^{(l)}$ corresponding to V is

$$\operatorname{llcm}\left(X - \frac{x_l\theta(v_1)}{v_1}, \ldots, X - \frac{x_l\theta(v_d)}{v_d}\right)$$

where llcm denotes the left lcm.

To conclude, we record the following proposition which elucidates how duality acts on our representations.

Proposition 3.8 We set $E = E' = \mathbf{E}_k$ and $P = Y^k - 1$ (resp. $E = \mathbf{E}_k^{(l)}$, $E' = \mathbf{E}_k^{(\tau(l))}$ and $P = P_l$).

(a) Given $f, g \in K[X;\theta]$, the ideal Ef and $E'g$ are orthogonal if and only if $fg^* = 0$ in E.

(b) Given $f \in K[X,\theta]$ dividing P, the orthogonal of Ef is the ideal $E'g^*$ where g is defined by $fg = P$.

Proof. (a) By nondegeneracy of sesquilinear form $\langle -, - \rangle$, the condition $fg^* = 0$ is equivalent to $gf^* = 0$ and then to $\langle E, gf^* \rangle = 0$. By adjunction relation, the condition becomes $\langle Ef, g \rangle = 0$. Since the adjunction is an isomorphism, the condition is further equivalent to $\langle (E')^* Ef, g \rangle = 0$ and finally to $\langle Ef, E'g \rangle = 0$.
(b) By what precedes, the ideals Ef and $E'g^*$ are orthogonal. We conclude by noticing that $\dim Ef + \dim E'g^* = (\deg P - \deg f) + (\deg P - \deg g) = \deg P$. $\square$

Remark 3.9 As a corollary, Proposition 3.8 provides a simple criterion to check that the code $\mathbf{E}_k f$ is selfdual: assuming that f is normalized, it is the case if and only if $ff^* = 0$ in $\mathbf{E}_k$ and $\deg f = s$.

Algorithm 1: Explicit bijection with $W_{\texttt{nonpal}} \times W_{\texttt{pal}}$

Input: a family $\big((V_l)_{l\in I}, (V_l)_{\{l,\tau(l)\}\in J}\big) \in W_{\texttt{nonpal}} \times W_{\texttt{pal}}$
Output: the normalized generator of the corresponding selfdual skew cyclic code

for $l \in I$ **:**
  pick a basis $(v_1, \ldots, v_s)$ of V_l
  $f_l \leftarrow \operatorname{llcm}\big(X - x_l\theta(v_i)/v_i,\ 1 \leqslant i \leqslant s\big)$
  do the subtitution $y_l \to X^r$ in f_l /* now $f_l \in \mathbf{K}[X;\theta]$ */
  $f_l \leftarrow \operatorname{rgcd}(f_l, P_l(Y))$
for $\{l, \tau(l)\} \in J$ **:**
  pick a basis $(v_1, \ldots, v_d)$ of V_l
  $f_l \leftarrow \operatorname{llcm}\big(X - x_l\theta(v_i)/v_i,\ 1 \leqslant i \leqslant d\big)$
  do the subtitution $y_l \to X^r$ in f_l /* now $f_l \in \mathbf{K}[X;\theta]$ */
  $f_l \leftarrow \operatorname{rgcd}(f_l, P_l(Y))$
  define $f_{\tau(l)}$ by the equality $f_l f_{\tau(l)}^* = P_l(Y)$
  $f_{\tau(l)} \leftarrow \operatorname{rgcd}(f_{\tau(l)}, P_{\tau(l)}(Y))$
compute f such that $f \equiv f_l \pmod{P_l(Y)}$ for $1 \leqslant l \leqslant n$
return $\operatorname{rgcd}(f, X^{rk} - 1)$

The discussion of this subsection is summarized by Algorithm 1 which computes the normalized generator of the code sitting in $\mathbf{E}_k$ that corresponds to some element of $W_{\texttt{nonpal}} \times W_{\texttt{pal}}$ *via* the bijection of Theorem 2.17. The next subsections are devoted to explain how to produce a random element in (each component of) $W_{\texttt{nonpal}} \times W_{\texttt{pal}}$.

3.3.2 The nonpalindromic case

We first consider the indices l such that $\tau(l) \neq l$. At those places, we simply need to generate a uniformly distributed random $\mathbf{F}_l$-subspace of $\mathbf{K}_l$. We proceed as follows. We first construct the dimension: we sample an integer $d \in \{0, \dots, r\}$ with distribution given by:

$$\text{Prob}[d = i] \quad \text{proportionnal to} \quad \begin{bmatrix} r \\ i \end{bmatrix}_{q_l}.$$

Once this is achieved, we sample d random elements in $\mathbf{K}_l$ with uniform distribution. If they are linearly independant over $\mathbf{F}_l$, we output the vector space they generate. Otherwise, we throw them and start again with d new elements. The probability of failure is

$$\left(1 - \frac{1}{q_l^r}\right)\left(1 - \frac{1}{q_l^{r-1}}\right) \cdots \left(1 - \frac{1}{q_l^{r-d+1}}\right) \geqslant 1 - \left(\frac{1}{q_l^r} + \cdots + \frac{1}{q_l^{r-d+1}}\right) \geqslant 1 - \frac{1}{q_l - 1},$$

proving that, in average, we will need to repeat our process only $O(1)$ times.

Up to a multiplicative constant, the mean complexity of the algorithm is then equal to the complexity of checking linearly independence of d vectors in a space of dimension r, which is within $O(r^3)$ by Gaussian elimination.

3.3.3 The Hermitian case

We now move to the Hermitian case, *i.e.* we assume that $\tau(l) = l$ and $y_l \neq \pm 1$. We thus want to design an algorithm outputting a uniformly distributed random isotropic $\mathbf{F}_l$-subspace of $\mathbf{K}_l$ (endowed with the Hermitian pairing $(-,-)_{\mathbf{K}_l}$ defined in (2.3), assuming that the existence criterion of Corollary 3.3 is fulfilled.

Actually, we will work in the following more general situation: we consider a finite field F of cardinality q_F equipped with a nontrivial involutive automorphism $\sigma : F \to F$. We also consider an Hermitian space V of dimension r and denote by $\langle -, - \rangle$ the bilinear form on it. We assume that V has Witt index s (*i.e.* that V is isomorphic to the orthogonal direct sum of s hyperbolic planes) and aim at sampling a random isotropic subspace of V of dimension s.

For $u, v \in V$, we consider the following equation in λ:

$$(\mathcal{E}_{u,v}) : \quad \langle u + \lambda v, u + \lambda v \rangle = 0.$$

We briefly recall its resolution. If $\langle v, v \rangle = 0$, the equation reduces to $\text{Trace}_{F/F^\sigma}(\lambda \cdot \langle v, u \rangle) = -\langle u, u \rangle$ which, per surjectivity of the trace, can be solved as soon as $\langle v, u \rangle \neq 0$.

On the contrary, when $\langle v, v \rangle \neq 0$, we consider the *discriminant* of $(\mathcal{E}_{u,v})$ defined by $\Delta := \langle u, v \rangle \cdot \langle v, u \rangle - \langle u, u \rangle \cdot \langle v, v \rangle$. One readily checks that Δ is invariant under σ and that the equation $(\mathcal{E}_{u,v})$ can be rewritten $\text{Norm}_{F/F^\sigma}(\langle u, v \rangle + \lambda \cdot \langle v, v \rangle) = \Delta$. The solutions of $(\mathcal{E}_{u,v})$ are then the elements of the form

$$\lambda = \frac{\delta - \langle u, v \rangle}{\langle v, v \rangle}$$

where δ is a preimage of Δ by the norm map. Since the latter is surjective (because we are working over finite fields), a solution always exists.

We are now ready to present Algorithm 2: it computes a basis $(u_1, \ldots, u_s, v_1, \ldots, v_s)$ of V such that each pair (u_i, v_i) is hyperbolic and, writing $H_i \subset V$ for the hyperbolic plane they generate, we have the orthogonal decomposition $V = \bigoplus_{i=1}^{s} H_i$.

Algorithm 2: Decomposition as a direct sum of hyperbolic planes (Hermitian case)

Input: V: the ambient Hermitian vector space
Output: $\mathbf{u}, \mathbf{v}$: a basis of hyperbolic pairs

1: $\mathbf{u}, \mathbf{v}, W \leftarrow [\,], [\,], 0$
2: **while** $W \neq V$ **:**
3:     pick two random vectors u and v in $W^{\perp}$
4:     **if** (u, v) are linearly independent and $\langle v, v\rangle \neq 0$ **:**
5:         $\lambda \leftarrow$ a random solution of the equation $(\mathcal{E}_{u,v})$
6:         $u \leftarrow u + \lambda v$ `/* now` $\langle u, u\rangle = 0$ `*/`
7:         $\lambda \leftarrow$ a solution of the equation $(\mathcal{E}_{v,u})$
8:         $v \leftarrow v + \lambda u$ `/* now` $\langle v, v\rangle = 0$ `*/`
9:         $v \leftarrow v / \langle v, u\rangle$ `/* now` (u, v) `is a hyperbolic pair */`
10:         $\mathbf{u} \leftarrow \mathbf{u} + [u]$, $\mathbf{v} \leftarrow \mathbf{v} + [v]$
11:         $W \leftarrow W + Fu + Fv$
12: **return** $\mathbf{u}, \mathbf{v}$

Proposition 3.10 Algorithm 2 is correct. Moreover, it terminates almost surely and its average complexity is $O(r^3)$ operations in F^{σ}.

Proof. We first prove correctness. It follows from the construction that, after the first successful iteration of the loop, (u, v) is a hyperbolic pair in V. Indeed, we notice that the subspace H_1 generated by u and v does not change throughout the loop, and so it is still a plane at the end. Moreover, each update successively ensures that $\langle u, u\rangle = 0$, then $\langle v, v\rangle = 0$ and finally $\langle u, v\rangle = 1$. We observe that $\langle v, u\rangle$ cannot vanish on line 9 because otherwise the Hermitian form would be degenerated. After this, we update W so that we continue to work in the orthogonal complement of H_1 which have dimension $2(s-1)$ and Witt index $s-1$ thanks to Witt's cancellation theorem. The induction then goes.

To prove termination, it is enough to justify that the probability of picking u and v satisfying the requirements of line 3 is bounded from below by a positive absolute constant. When W has dimension $2d$, the number of vectors $u, v \in W$ is q_F^{4d}. On the other hand, a pair (u, v) is rejected when v is isotropic or when u and v are collinear. The number of suitable pairs are then

$$\left(q_F^{2d} - (q_F^{d} - 1)(q_F^{d-1} + 1)\right) \cdot \left(q_F^{2d} - q_F\right)$$

(see the proof of Theorem 3.4 for the counting of isotropic vectors). One checks that the latter is at least $\frac{10}{27} q_F^{4d}$ as soon as $q_F \geqslant 3$, meaning that the probability of success of the test in line 3 is at least $\frac{10}{27}$.

Finally, regarding complexity, we claim that each successful iteration of the loop costs at most $O(r^2)$ operations in F^{σ}. To achieve this, we first observe that solving the equation $(\mathcal{E}_{u,v})$ amounts to find a uniformly distrbuted preimage of the discriminant by the norm map; this can be done using the algorithms of [CL17] for a constant cost. Similarly solving $(\mathcal{E}_{v,u})$ reduces to a linear system, which can be attacked by simple linear algebra over F^σ for a constant cost again. Regarding the computation of W, we may process as follows: we maintain a matrix M in reduced row echelon form representing the subspace of $V^\star = \mathrm{Hom}_F(V, F)$ generated by the forms $\langle -, w\rangle$ with $w \in W$. At each update of W on line 11, we need to add two new lines to M and re-echelon it; this has a cost of $O(r^2)$ operations in F using standard Gaussian elimination. Moreover, knowing M, sampling u and v on line 3 amounts to finding two random solutions of the linear system $MX = 0$. Since M is already row-echeloned, this can be done for a cost of $O(r^2)$ operations in F as well. □

Finally, the link between Algorithm 2 and the question we are interested in is established in the next proposition.

Proposition 3.11 If $\mathbf{u}, \mathbf{v}$ is the output of Algorithm 2, then the space generated by $\mathbf{u}$ is a uniformly distributed random isotropic subspace of V of dimension s.

Proof. The fact that the span of $\mathbf{u}$ is an isotropic subspace of dimension s is clear. To prove that it is uniformly distributed, we notice that, after line 3, the plane $Fu + Fv$ is uniformly distributed among all planes in $W^\perp$. Since this plane stays unchained until the end of the loop, it remains uniformly distributed.

We now fix a hyperbolic plane $H \subset W^\perp$, together with a nonisotropic vector $v \in H$. We claim that, when u varies in H, the vector u one obtains after the replacement of line 6 is uniformly distributed in the set $\mathcal{I}_H$ of isotropic vectors in H. In order to prove this, for $u \in H$, we define $L(u) \subset H$ as the affine line passing through u and directed by v. We also set $S(u) := L(u) \cap \mathcal{I}_H$. Clearly, for any fixed u noncollinear to v, the $L(\alpha u)$ form a partition of $H\backslash Fv$ when α varies in $F^\times$. Since v is itself nonisotropic, we conclude that

$$\mathcal{I}_H = \bigsqcup_{\alpha \in F^\times} S(\alpha u). \tag{3.4}$$

Moreover, the multiplication by α defines a bijection $S(u) \to S(\alpha u)$; hence, all the $S(\alpha u)$ have the same cardinality. Coming back now to the algorithm, we notice that the effect of lines 5 and 6 is to replace u by a uniformly distributed random vector in $S(u)$. The decomposition (3.4), combined with the fact that all $S(\alpha u)$ have the same cardinality, then implies that the vector u obtained after line 6 gets uniformly distributed in $\mathcal{I}_H$ when u varies on any given line of H that does not contain v. Since this holds for any line, our claim is proved.

The proposition follows by combining all what precedes. □

3.3.4 The Euclidean case

We move to the Euclidean case, *i.e.* we consider the same setting as before expect that we now assume that σ is the identity. The equation $(\mathcal{E}_{u,v})$ continues to make sense but its resolution is a bit different. Precisely, expanding the scalar product, we find that it is equivalent to

$$\langle u, u\rangle + 2\lambda \cdot \langle u, v\rangle + \lambda^2 \cdot \langle v, v\rangle = 0.$$

If $\langle v, v\rangle = 0$, it is a linear equation that we can solve as soon as $\langle u, v\rangle \neq 0$. On the contrary, if $\langle v, v\rangle \neq 0$, it is a quadratic equation whose (reduced) discriminant is $\Delta := \langle u, v\rangle^2 - \langle u, u\rangle \cdot \langle v, v\rangle$ (this is in fact the same as before!). The equation $(\mathcal{E}_{u,v})$ has no solution when Δ is not a square and it has one or two solutions otherwise: if $\delta^2 = \Delta$, they are given by $\lambda = \frac{\delta - \langle u,v\rangle}{\langle v,v\rangle}$.

Lemma 3.12 When u and v varies among pairs of noncollinear vectors in V, the probability that the equation $(\mathcal{E}_{u,v})$ has a solution is at least $\frac{1}{2}$.

Proof. The equation is solvable exactly when u and v span an hyperbolic plane since, thanks to Witt's theorem, a plane is hyperbolic as soon as it contains an isotropic vector. We then need to estimate the probability that a given plane is hyperbolic. The total number of planes is given by

$$B = \frac{(q_F^{2s} - 1)(q_F^{2s} - q_F)}{(q_F^2 - 1)(q_F^2 - q_F)}.$$

Counting the number of hyperbolic planes is more delicate. In order to do it, we consider the map

$$\begin{array}{rccc} \mathcal{S}: & \left\{ \begin{array}{c} \text{pair of noncollinear} \\ \text{isotropic vectors} \end{array} \right\} & \longrightarrow & \{\text{hyperbolic planes}\} \\ & (x, y) & \mapsto & Fx + Fy. \end{array}$$

By the argument of the proof of Theorem 3.4, the fibers of $\mathcal{S}$ have all cardinality $2(q_F - 1)\big(2(q_F - 1) - (q_F - 1)\big) = 2 \cdot (q_F - 1)^2$. Similarly, the domain of $\mathcal{S}$ has cardinality $(q_F^s - 1)(q_F^{s-1} + 1)\big((q_F^s - 1)(q_F^{s-1} + 1) - (q_F - 1)\big)$. Hence, the number of hyperbolic planes is

$$A = \frac{(q_F^s - 1)(q_F^{s-1} + 1)\big((q_F^s - 1)(q_F^{s-1} + 1) - (q_F - 1)\big)}{2 \cdot (q_F - 1)^2}.$$

The probability we are looking for is the quotient A/B, and calculus now proves that it is always greater than $\frac{q_F - 1}{2q_F} > \frac{1}{2}$. $\square$

From here, we can write down Algorithm 3 (which is a direct translation of Algorithm 2).

Proposition 3.13 Algorithm 3 is correct. It terminates almost surely and its average complexity is $O(r^3)$ operations in F. Moreover, if $\mathbf{u}, \mathbf{v}$ is the output of Algorithm 2, then the space generated by $\mathbf{u}$ is a uniformly distributed random isotropic subspace of V of dimension s.

Proof. After Lemma 3.12, this is a repetition of the proofs of Proposition 3.10 and 3.11. $\square$

3.4 Enumeration of selfdual skew cyclic codes

We finally address the question of enumeration. As we already said earlier, an algorithm that outputs in one shot the complete list of selfdual codes in $\mathbf{E}_k$ would only have a limited interest because the number of such codes grows exponentially with respect to r.

Instead, we will work with iterators, that are, roughly speaking, procedures that produce a new item each time they are called, without precomputing the entire list at the beginning. Concretely, we

Algorithm 3: Direct sum decomposition of hyperbolic planes in the Euclidean case

Input: V: the ambient Euclidean vector space

Output: $\mathbf{u}, \mathbf{v}$: a basis of hyperbolic pairs

- $\mathbf{u}, \mathbf{v}, W \leftarrow [\,], [\,], 0$
- **while** $W \neq V$ **:**
  - pick two random vectors u and v in $W^\perp$
  - **if** (u, v) are linearly independent and $\langle v, v\rangle \neq 0$ **:**
    - $\Delta \leftarrow \langle u, v\rangle^2 - \langle u, u\rangle \cdot \langle v, v\rangle$
    - **if** Δ is a square in F **:**
      - $\lambda \leftarrow$ a random solution of the equation $(\mathcal{E}_{u,v})$
      - $u \leftarrow u + \lambda v$ `/* now` $\langle u, u\rangle = 0$ `*/`
      - $\lambda \leftarrow$ a solution of the equation $(\mathcal{E}_{v,u})$
      - $v \leftarrow v + \lambda u$ `/* now` $\langle v, v\rangle = 0$ `*/`
      - $v \leftarrow v/\langle v, u\rangle$ `/* now` (u, v) `is a hyperbolic pair */`
      - $\mathbf{u} \leftarrow \mathbf{u} + [u]$, $\mathbf{v} \leftarrow \mathbf{v} + [v]$
      - $W \leftarrow W + Fu + Fv$
- **return** $\mathbf{u}, \mathbf{v}$

model iterators by importing the keywords **yield** and **next** from the Python syntax. When a procedure containing the keyword **yield** is called, it is not executed but instead returns an object called *iterator*, which can be understood as a pointer to the current state of execution of the procedure. Now, each time the iterator is called through the keyword **next**, the execution of the procedure continues until a statement **yield** is encoutered; at that point, the execution is stopped and the iterator outputs the attribute of the **yield** instruction.

In all what follows, we assume[1] that we have at our disposal, for all integers $m \leqslant n$ and any finite field F, an iterator producing the list of all matrices in reduced row echelon form with m rows and n columns. We note that such matrices are in one-to-one correspondence with m-dimensional F-linear subspaces of F^n (the subspace being the span of the rows of the matrix). In a similar fashion, we also assume that, for any given linear system, we have at our disposal an iterator running over its solutions.

We now explain how to build iterators over each component of the product $W_{\texttt{nonpal}} \times W_{\texttt{pal}}$.

3.4.1 The nonpalindromic case

In this case, we have to construct an iterator running over all $\mathbf{F}_l$-linear subspaces of $\mathbf{K}_l$. In order to reduce this task to a matrix enumeration, we first pick a basis of $\mathbf{K}_l$ over $\mathbf{F}_l$ (this can be done easily; for example, a basis of $\mathbf{K}$ over $\mathbf{F}$ does the job). Once this is achieved, we take an iterator that runs over all matrices over $\mathbf{F}_l$ in reduced row echelon form with r columns, which directly solves our problem.

3.4.2 The Euclidean case

As in Subsection 3.3.4, we work with a general r-dimensional Euclidean space V over a finite field F of cardinality q_F and assume that V has Witt index s. By the results of Subsection 3.3.4, we can

[1] Such an iterator is available in many softwares, including SageMath. It is moreover easy to construct: we iterate over the subset of $I \subset \{1, \ldots, n\}$ of cardinality m and, for each such I, we run over all the matrices in reduced row echelon form with pivots at positions in I.

further assume that we are given an hyperbolic basis of V, that is a basis $(u_1, \ldots, u_s, v_1, \ldots, v_s)$ such that $\langle u_i, v_i \rangle = 1$ and all other scalar products between elements in the basis vanish.

In order to take advantage of this basis, we will enumerate the s-dimensional subvector spaces of V in a slightly different manner. Those spaces are parametrized by the matrices M in reduced row echelon form of size $s \times (2s)$, but we shall further split M and write it as a block matrix as follows:

$$M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}.$$

Here A, B and C all have s columns and the horizontal separation is positionned is such a way that the last line of A is not identically zero. The matrices A and C are then reduced row echelon matrices of size $d \times s$ and $(s-d) \times s$ respectively (for some d). Besides, the columns of B in front of the pivots of C all vanish. Conversely, if we choose A, B and C satisfying the above conditions, the resulting block matrix M will be in reduced row echelon form. In other words, there is a bijection between the matrices M, on the one hand, and the triples (A, B, C), on the other hand; in the sequel, we will constantly rely on it to enumerate the M.

Remark 3.14 At the level of cardinalities, the above bijection leads to the (classical) formula

$$\begin{bmatrix} 2s \\ s \end{bmatrix}_{q_F} = \sum_{d=0}^{s} q_F^{d^2} \cdot \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}^2.$$

The (A, B, C)-presentation is quite interesting for our purpose because the isotropy condition translates to the equations:

$$AB^{\mathrm{tr}} + BA^{\mathrm{tr}} = 0 \tag{3.5}$$

$$AC^{\mathrm{tr}} = 0 \tag{3.6}$$

Equation (3.6) means that the row-span of A should be orthogonal to the row-span of C for the standard scalar product on F^s. Since those two spaces have completary dimension, we conclude that $\mathrm{RowSpan}(C)$ must be the orthogonal of $\mathrm{RowSpan}(A)$. Given that, in addition, C must also be in reduced row echelon form, we conclude that C is uniquely determined by A: it is the reduced row echelon basis of $\mathrm{RowSpan}(A)^\perp$.

Once C is known, one also knows its pivots and the shape of B is determined. Equation (3.5) then appears as a linear equation on the entries of B, which can be easily solved using Gaussian elimination.

All of this leads to Algorithm 4.

Regarding complexity, it is clear that, in the worst case, an iteration of Algorithm 4 requires at most $O(r^6)$ operations in F since it only involves Gaussian elimination in dimension at most $O(r^2)$. However, in most cases, an iteration only consists in going from one solution B to the next one; once a basis of the space of solutions has been computed, this costs only $O(r^2)$ operations in F.

Remark 3.15 Denoting by d the number of rows of A, one can prove that the linear system (3.5)

Algorithm 4: Iterator over maximal isotropic spaces (Euclidean case)

$\mathcal{A} \leftarrow$ iterator over reduced row echelon matrices over F with s columns
while $A \leftarrow$ **next**$(\mathcal{A})$ **:**
  $C \leftarrow$ reduced row echelon basis of $\mathrm{RowSpan}(A)^{\perp}$
  $\mathcal{B} \leftarrow$ iterator over solutions of (3.5) with vanishing columns in front of pivots of C
  while $B \leftarrow$ **next**$(\mathcal{B})$ **:**
    yield $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$

consists of $\frac{d(d+1)}{2}$ linearly independent equations. Therefore, the set of admissible B is a F-vector space of dimension $\frac{d(d-1)}{2} = \binom{d}{2}$; hence it has cardinality $q_F^{\binom{d}{2}}$. From this, we derive that the number of isotropic subspaces of V of dimension s is equal to

$$\sum_{d=0}^{s} q_F^{\binom{d}{2}} \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}.$$

Comparing with Segre's formula (see Theorem 3.4), we find the identity

$$\prod_{d=0}^{s-1} (1 + q_F^d) = \sum_{d=0}^{s} q_F^{\binom{d}{2}} \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}$$

which is actually a special case of the well-known polynomial identity [PA71]:

$$\prod_{k=0}^{n-1} (1 + q^k t) = \sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_{q} t^k. \tag{3.7}$$

As a byproduct, our approach then provides a *bijective proof* of this identity when $t = 1$ and q is a power of a prime number.

3.4.3 The Hermitian case

We now equip F with a nontrivial involution $\sigma : F \to F$ and assume that the pairing $\langle -, - \rangle$ on V is σ-sesquilinear. In this new situation, all the discussion of Subsection 3.4.2 applies, except that the Equations (3.5) and (3.6) have to be replaced by the following ones:

$$A\sigma(B^{\mathrm{tr}}) + B\sigma(A^{\mathrm{tr}}) = 0 \tag{3.8}$$

$$A\sigma(C^{\mathrm{tr}}) = 0 \tag{3.9}$$

As in the Euclidean case, it turns out that Equation (3.9) fully determines C; precisely C is the reduced row echelon basis of $\mathrm{RowSpan}(\sigma(A))^{\perp}$. Similarly, Equation (3.8) provides a linear system on the entries on B but we need to careful that it is F^{σ}-linearity and not F-linearity as before. Anyway, the system can equally be solved using Gaussian elimination.

Taking these remarks into account, we end up with Algorithm 5

Remark 3.16 Similarly to the Euclidean case, our approach gives a bijective proof of the numerical

Algorithm 5: Iterator over maximal isotropic spaces (Hermitian case)

$\mathcal{A} \leftarrow$ iterator over reduced row echelon matrices over F with s columns
while $A \leftarrow \mathbf{next}(\mathcal{A})$ **:**
  $C \leftarrow$ reduced row echelon basis of $\mathrm{RowSpan}(\sigma(A))^{\perp}$
  $\mathcal{B} \leftarrow$ iterator over solutions of (3.8) with vanishing columns in front of pivots of C
  while $B \leftarrow \mathbf{next}(\mathcal{B})$ **:**
    yield $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$

identity

$$\prod_{d=0}^{s-1}(1 + q_F^{d+1/2}) = \sum_{d=0}^{s} q_F^{d^2/2} \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}$$

which is Equation (3.7) evaluated at $q = q_F$ and $t = \sqrt{q}$.

3.5 An implementation in SageMath

We implemented the algorithms of this section 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 constructor parameters. It provides an iterator on all selfdual codes for the Ore algebra $\mathbf{K}[X^{\pm 1}; \theta]/P(X^r)$. Hereunder, we present a bunch of examples covering all the encoutered situations : palindromic Euclidean and palindromic Hermitian.

We start by loading our package and defining the relevant base rings.

```
sage: load("selforthogonal_codes.sage")
None
sage: q = s = 3; F = GF(q); Fy.<y> = F[]
sage: Q = F['z'].irreducible_element(2*s, "adleman-lenstra")
sage: Q
z^6 + z^5 + z^4 + z^3 + z^2 + z + 1
```

Case 3.17 Palindromic Euclidean: $q = 3$, $s = 3$ and $P(Y) = Y - 1$

```
sage: A = SelfDualCodes(y - 1, Q)
sage: iter = A.enumerate_selfdual_codes()
sage: next(iter)
x^3 + (z^5 + 2*z^4 + z^3 + 2*z^2)*x^2 + (2*z^4 + 2*z^3 + 1)*x + z^4 + z
    ^3 + 2*z^2 + 2*z + 1
sage: next(iter)
x^3 + (2*z^4 + 2*z^2 + z + 2)*x^2 + (z^5 + z^4 + z^3 + 2*z^2 + z + 2)*x
    + z^3 + z^2 + z + 2
```

$P(Y)$	$q=3$	$q=5$	$q=7$	$q=3^2$
$Y-1$	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	9 ms	16 ms	21 ms
Y^2+1	16 ms	6 ms	15 ms	15 ms
Y^3+1	inseparable	26 ms	22 ms	inseparable
Y^4+1	18 ms	21 ms	35 ms	48 ms
Y^5+1	62 ms	inseparable	111 ms	128 ms
Y^6+1	inseparable	47 ms	59 ms	inseparable
Y^7+1	80 ms	300 ms	inseparable	250 ms
Y^8+1	463 ms	87 ms	113 ms .	108 ms
Y^9+1	inseparable	218 ms	125 ms	inseparable

Figure 1: Timings for $s=2$

Case 3.18 Palindromic Hermitian case: $q=3$, $s=3$ and $P(Y)=Y^2+1$

```
sage: A = SelfDualCodes(y^2 + 1, Q)
sage: iter = A.enumerate_selfdual_codes()
sage: next(iter)
x^6 + (2*z^5 + z^4 + z^2 + 2)*x^5 + (z^5 + z^3 + 2*z^2 + 2*z + 2)*x^4 +
    (z^5 + z^3)*x^3 + (z^5 + z^2 + 1)*x^2 + (z^5 + 2*z^4 + z^3 + z^2 + 2*
    z + 1)*x + z^5 + z^3 + 2*z^2 + z + 2
```

Benchmarks for a larger set of inputs are reported on Figures 1, 2 and 3; there were run on computer with Intel(R) Core(TM) i7-9750H CPU 2.60GHz processor x64 and 16 GB of RAM.

4 Enumeration of purely inseparable selfdual skew cyclic codes

We now address the case where k is not coprime to the characteristic p. We aim at finding an enumeration algorithm of selfdual skew cyclic codes in this case too. If k decomposes as $k'p^m$ with k'

$P(Y)$	$q = 3$	$q = 5$	$q = 7$	$q = 3^2$
$Y - 1$	21 ms	no codes.	207 ms	no codes.
$Y^3 - 1$	inseparable	no codes.	42 ms	inseparable
$Y^5 - 1$	101 ms	inseparable	129 ms	no codes.
$Y^7 - 1$	195 ms	no codes.	inseparable	no codes.
$Y^9 - 1$	inseparable	no codes.	342 ms	inseparable
$Y + 1$	no codes.	21 ms	no codes.	56 ms
$Y^2 + 1$	152 ms	12 ms	36 ms	32 ms
$Y^3 + 1$	inseparable	57 ms	no codes.	inseparable
$Y^4 + 1$	38 ms	47 ms	74 ms	141 ms
$Y^5 + 1$	no codes.	inseparable	no codes.	317 ms
$Y^6 + 1$	inseparable	101 ms	139 ms	inseparable
$Y^7 + 1$	no codes.	398 ms	inseparable	601 ms .
$Y^8 + 1$	209 ms	270 ms	270 ms	280 ms
$Y^9 + 1$	inseparable	450 ms	no codes.	inseparable

Figure 2: Timings for $s = 3$

$P(Y)$	$q = 3$	$q = 5$	$q = 7$	$q = 3^2$
$Y - 1$	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
$Y + 1$	59 ms	49 ms	58 ms	177 ms
$Y^2 + 1$	78 ms	29 ms	89 ms	69 ms
$Y^3 + 1$	inseparable	128 ms	90 ms	inseparable
$Y^4 + 1$	88 ms	108 ms	174 ms	412 ms
$Y^5 + 1$	220 ms	inseparable	336 ms	723 ms
$Y^6 + 1$	inseparable	200 ms	388 ms	inseparable
$Y^7 + 1$	286 ms	387 ms	inseparable	1367 ms
$Y^8 + 1$	406 ms .	551 ms	586 ms	2159 ms
$Y^9 + 1$	inseparable	691 ms	784 ms	inseparable

Figure 3: Timings for $s = 4$

coprime with p, it follows easily from the chinese remainder isomorphism

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

that we can recover an enumeration algorithm for any k by combining the separable case and the case where $k = p^m$ (purely inseparable case).

4.1 Enumeration of purely inseparable selfdual skew cyclic codes

In order to solve the purely inseparable case, we follow a factorization approach, inspired by but slightly different from that of article [BU14]. We introduce twisted skew separable codes $\mathbf{E}_{k,l}^{(\xi X^t)}$, that are slight generalizations of previously considered skew separable codes. They are defined as skew separable codes of $\mathbf{E}_k^{(l)}$ corresponding to the usual adjunction on $\mathbf{E}_k^{(l)}$ composed with the conjugation by ξX^t for $\xi \in \mathbf{K}_l$ and $t \in \{0, s\}$. We will then obtain all inseparable selfdual codes as products of twisted skew separable selfdual codes.

Definition 4.1 We fix parameters $t \in \{0, s\}$, $\xi \in \mathbf{K}_l$. We denote by $\mathbf{E}_{k,l}^{(\xi X^t)}$, the space $\mathbf{E}_k^{(l)}$ equipped with the ξX^t-twisted bilinear form $(\kappa, \rho) = \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta.\xi\kappa\theta^t(\sigma_l(\rho)))$.

The corresponding *adjunction* is $f^{\bullet_{X^t\xi^{-1}}} = X^t\xi^{-1}\zeta^{-1}\sum_i X^{-i}\sigma_l(f_i)\zeta\xi X^{-t}$; we have

$$(\kappa, f(\rho))_{\mathbf{F}_l}^{(\xi X^t)} = (f^{\bullet_{X^t\xi^{-1}}}(\kappa), \rho)_{\mathbf{F}_l}^{(\xi X^t)}.$$

In the sequel, we will take $\sigma_l(\xi) = \xi$, and if $t = s$ $\theta^t(\xi) = -\xi$, so that the ξX^t-twisted bilinear form enjoys following symmetries:

- it 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 $t = s$.

Remark 4.2 Reusing the method of Remark 3.5, we can compute the number of twisted codes when $k = 1$. For example, in the skew-Euclidean case, it is given by

$$\frac{\mathrm{Card}\big(\mathrm{Sp}_{2s}(\mathbf{F}_l)\big)}{q_l^{s(s+1)/2}\cdot \mathrm{Card}\big(\mathrm{GL}_s(\mathbf{F}_l)\big)} = \prod_{d=1}^{s}(1+q_l^d)$$

where Sp_{2s} stands for the symplectic group. We refer to [Han05] for more details.

Lemma 4.3 The set of ξ-twisted selfdual skew cyclic codes is in bijection with the set of nontwisted selfdual skew cyclic codes and their intersection is empty if $\theta^s(\xi) \neq \xi$.

Proof. We have for any monic skew polynomial f of degree s generating a selfdual code C_f of $\mathbf{E}_k^{(l)}$:

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

where $f(0)$ denotes the constant term in f. As we assume ξ to be σ_l-invariant, 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 cyclic codes:

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

Moreover, if we assume $\theta^s(\xi) \neq \xi$ 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 $f(0) = f(0)\frac{\theta^s(\xi)}{\xi}$, and so $f(0) = 0$ and thus $f = 0$, which contradicts the hypothesis. $\square$

Algorithm 6 is an iterator that enumerates selfdual skew cyclic codes sitting in $\mathbf{E}_k$. It is exhaustive, in the sense that it lists every selfdual code at least once, but it is slightly redundant.

Algorithm 6: Enumeration of purely inseparable selfdual skew cyclic codes

```
1: 𝒞 ← array of length p^m of maps of iterators on all twisted codes indexed by all possible
   twists ξX^{s(deg(f)/s %2)} where ξ can be choosen among all representatives of ℙ^r_{F_l} in K_l if deg(f)/s
   is even and otherwise among all representatives of ℙ^r_{F_l} in K_l that are antisymmetric
   relatively to θ^s.
2: procedure RunThroughRemainingCodes(f)
3:     i ← deg(f)/s
4:     if i = p^m :
5:         yield f
6:     else
7:         while f_i ← next(𝒞[i][f(0)X^{s(i%2)}]) :
8:             RunThroughRemainingCodes(f_i f)
9: RunThroughRemainingCodes(1)
```

Theorem 4.4 Algorithm 6 is correct and exhaustive

Proof. In order to enumerate all inseparable selfdual skew cyclic codes, at the cost of some redundancy, we can assume without loss of generality (See the last part of the proof, hereunder) that the general solution is a product of twisted selfdual skew cyclic codes $f_1 \dots f_n$, where the f_i are left monic. We start by solving the equation $f_n f_n^\bullet \equiv 0 \mod (X^r-1)$. 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 $f_n(0)$. 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 $f_{n-1}X^s f_{n-1}^{\bullet_{\kappa_n}} = 0\,(X^r-1)$. Solving it, we now obtain a scalar $\kappa_{n-1} = \frac{f_{n-1}X^s f_{n-1}^{\bullet_{\kappa_n}}}{X^{r+s}(X^r-1)}$. At the next step, the monomials X^s cancel, and we are back in the Hermitian case: $f_{n-2}f_{n-2}^{\bullet_{\kappa_{n-1}\kappa_n}} = 0\,(X^r-1)$. 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 cyclic codes to exist. A monic polynomial f satisfying the product criterion: $ff^{\bullet_{\kappa X^t}} = 0$ in $\mathbf{E}_{k,l}^{(\kappa X^t)}$

has a constant term $f(0)$ satisfying:

$$(X^s + \cdots + f(0))\kappa X^t (X^r f(0) + \cdots + X^s) = \theta^s(\kappa)\theta^{s+t}(f(0))X^s X^t X^r + f(0)\kappa X^t X^s \\ \propto X^{r+s+t} - X^{s+t}.$$

Thus we have:

$$\theta^s(f(0)) = -f(0) \quad \text{for } \theta^s(\kappa) = \kappa\,,\ t = 0 \tag{4.1}$$

$$\theta^s(\kappa) = -\kappa \quad \text{for } t = s \text{ (symplectic case)} \tag{4.2}$$

$$-f(0)\kappa = \theta^s(\kappa f(0)) \quad \text{for } t = 0 \tag{4.3}$$

If we start with $\kappa = 1$, we get the symplectic case from (4.1) and (4.2) with κ satisfying $\theta^s(\kappa) = -\kappa$, at the next step. We have then an orthogonal case, then again alternatively a symplectic case with κ satisfying $\theta^s(\kappa) = -\kappa$ from (4.3), *etc.*

We now prove that the algorithm is exhaustive. We observe that the projection

$$\begin{array}{ccc} \mathbf{E}_k^{(l)} = \mathbf{K}_l[X^{\pm 1};\theta]/(X^r-1)^{p^m} & \longrightarrow & \mathbf{K}_l[X^{\pm 1};\theta]/(X^r-1) = \mathbf{E}_1^{(l)} \\ f & \mapsto & \bar{f} \end{array}$$

preserves the selforthogonality property. Noting $f_{p^m} := \tilde{\bar{f}}$ the unique lift of $\bar{f}$ on the basis $(X^i)_{0\leqslant i<r}$, we have a factorization $f_{p^m} = r_{p^m} g_{p^m}$ for a skew polynomial r_{p^m} of degree striclty less than s and a selfdual skew cyclic code g_{p^m} in E_1. Indeed any selforthogonal subspace of $\mathbf{E}_1^{(l)}$ of dimension strictly less than r, corresponding to a monic skew polynomial f can be extended, by Witt's decomposition, to a maximal isotropic space corresponding to a selfdual monic skew polynomial g of degree s. Now this vector space inclusion corresponds by duality to a factorization $\bar{f} = rg$ for a skew polynomial r of degree striclty less than s. Expressing $(X^r - 1)$ as a product of the selfdual codes g_{p^m}, $\frac{g^*_{p^m} g_{p^m}}{g_{p^m}(0)X^s}$ we get that any selforthogonal skew cyclic code $f \in \mathbf{E}_k^{(l)}$ can be written in the form

$$f = h(X^r-1) + f_{p^m} = \left(h\frac{g^*_{p^m}}{g_{p^m}(0)X^s} + r_{p^m}\right) g_{p^m}$$

where $\deg h = (p^m-2)s$ and $\frac{1}{X^s g_{p^m}(0)} g^*_{p^m} \in \mathbf{K}_l[X;\theta]$ is of degree s. Let us note $f' = g\frac{1}{X^s g_{p^m}(0)} g^*_{p^m} + r_{p^m}$. We have $\deg f' = (p^m-1)s$ and $f' g_{p^m}(f' g_{p^m})^* = f' g(0) X^s f'^* (X^r-1) \equiv 0 \mod (X^r-1)^{p^m}$ and hence $f' f'^{\bullet_{X^s g_{p^m}(0)}} \equiv 0 \mod (X^r-1)^{p^m-1}$. With the same reasoning, replacing f by f' and the adjunction $*$ by $\bullet_{X^s g_{p^m}(0)}$, we get yet another twisted separable selfdual skew cyclic code f_{p^m-1} and another skew polynomial f'' such that $f'' f''^{\bullet_{g_{p^m-1}(0) g_{p^m}(0)}} \equiv 0 \mod (X^r-1)^{p^m-2}$. In turn replacing f' by f'' and the adjunction $\bullet_{X^s g_{p^m}(0)}$ by $\bullet_{g_{p^m-1}(0) g_{p^m}(0)}$, we get yet another twisted separable selfdual skew cyclic code g_{p^m-2} and another skew polynomial f'' such that $f'' f''^{\bullet_{X^s g_{p^m-2}(0) g_{p^m-1}(0) g_{p^m}(0)}} \equiv 0 \mod (X^r-1)^{p^m-3}$. Per induction we thus a factorization $g_0 g_1 \cdots g_{p^m-1} g_{p^m}$ of f into twisted separable selfdual skew cyclic codes as claimed. ◻

Remark 4.5 We notice the reason for the redundancy in the enumeration algorithm from the above proof of the exhaustivity. Indeed the many different factorizations $f_i = r_i g_i$ for selforthogonal f_i at each step lead to as many redundant enumerations of the same inseparable selfdual skew cyclic code f.

4.2 SageMath enumeration of inseparable selfdual skew cyclic codes

For $F = GF(3)$, $K = GF(3^6)$ and $k = 3$, the upper bound on the number of generated inseparable selfdual skew cyclic codes is numerically equal to $80 \times 1120 \times 80$, where 80 is the number of orthogonal isotropic spaces and 1120 the number of symplectic isotropic spaces (see Remark 4.2). A SageMath enumeration based on this algorithm provides a number n of maximal isotropic codes equal to $n = 2360960$. We have not many redundancies since $80 \times 1120 \times 80 \approx 3 \times 2360960$. For the purpose of this heavy computation we implemented the PARI/GP optimization for finite field extensions in a dedicated branch of our code, which is only valid for prime base fields. The computation takes place in less than 10 minutes on the aforementioned computer.

References

[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.

[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.

[Sch85] W. Scharlau. *Quadratic and Hermitian Forms*. Grundlehren der mathematischen Wissenschaften. World Publishing Corporation, 1985.

[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.