

ON INDECOMPOSABLE IDEALS OVER SOME ALGEBRAS

ALESSANDRO ARDIZZONI AND FABIO STUMBO

ABSTRACT. In this paper we investigate a family of algebras endowed with a suitable non-degenerate bilinear form that can be used to define two different notions of dual for a given right ideal. We apply our results to the classification of the right ideals and their duals in the cyclic group algebra, in the Taft algebra and in another example of Hopf algebra arising as bosonization.

[2010]Primary 16T05; Secondary 15A63, 94B15, 94B05

CONTENTS

Introduction	1
1. Bilinear forms	3
2. Indecomposable ideals in $\mathbb{k}\langle\omega, N\rangle$	6
3. Ideals and their orthogonals for Hopf algebras	9
4. Examples and applications	12
4.1. Cyclic group algebra	12
4.2. Taft algebra	14
4.3. Another example	18
References	23

INTRODUCTION

Fix a base field \mathbb{k} . Recall that a linear code of length $n \geq 2$ is a vector subspace of \mathbb{k}^n . A linear code C is called cyclic whenever $(c_0, c_1, \dots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$. By considering the cyclic group algebra $\mathbb{k}\langle x \rangle := \mathbb{k}[X]/(X^n - 1)$, where we set $x := X + (X^n - 1)$, then the assignments

$$(0.1) \quad \mathbb{k}\langle x \rangle \ni c_0 + c_1x + \dots + c_{n-1}x^{n-1} \longleftrightarrow (c_0, c_1, \dots, c_{n-1}) \in \mathbb{k}^n$$

yield a bijective correspondence between ideals in $\mathbb{k}\langle x \rangle$ and cyclic codes of length n . Moreover, if g is the generator polynomial for a cyclic code, then the dual code corresponds, via the map (0.1), to the orthogonal of the ideal (g) with respect to the usual scalar product defined by $\langle x^i, x^j \rangle = \delta_{i,j}$.

Key words and phrases. Cyclic codes, monomial bilinear forms, indecomposable ideals, orthogonals, Hopf algebras.

This note was written while the first author was member of the “National Group for Algebraic and Geometric Structures, and their Applications” (GNSAGA-INdAM). We would like to thank Michela Ceria for meaningful discussions on the topics treated in the present paper. We are also in debt with Lea Terracini for her contribution in the computations of the indecomposable ideals of the Taft algebra and their orthogonals. **Finally we are grateful to the referee for useful comments.**
~~Corresponding Author: Alessandro Ardizzoni.~~

Since $\mathbb{k}\langle x \rangle$ is the group algebra over the cyclic group of order n , i.e. $\langle x \rangle := \{1, x, \dots, x^{n-1}\}$, it is in particular a Hopf algebra. This constitutes a link between the study of the ideals in Hopf algebras and Coding Theory. It is then natural to look at a right ideal in a Hopf algebra as a sort of ‘‘Hopf code’’. Following this idea, a characterization of all projective indecomposable ideals in the Taft algebra was given in [CGL].

The particular description of dual codes in the Hopf algebra $\mathbb{k}\langle x \rangle$ places the notion of orthogonal with respect to a suitable non-degenerate bilinear form as the proper counterpart of the concept of dual code.

We will show that both the cyclic group algebra and the Taft algebra come out to be endowed with a non-degenerate bilinear form that we will call monomial and that can be used to compute explicitly the indecomposable right ideals and their orthogonals.

More generally in this paper we investigate a family of algebras endowed with a monomial non-degenerate bilinear form: this form can be used to define two different notions of dual for a given right ideal. As an application, we recover the classification of the right ideals and their duals in the cyclic group and Taft algebras and provide the same classification for another example of Hopf algebra arising as a bosonization in [CDMM].

The paper is organized as follows.

In Section 1 we introduce and characterize the concept of monomial bilinear form on a finite-dimensional vector space V . This type of form is the main tool in our paper. In Lemma 8, we study the behaviour of orthogonals of subspaces of V spanned by a subset of the basis, with respect to a monomial bilinear form.

In Section 2 we introduce the \mathbb{k} -algebra $\mathbb{k}(\omega, N)$ presented by generators and relations. It can also be introduced as a quotient of an Ore extension with zero derivation. In Theorem 12 we provide an irredundant set of representatives of indecomposable right ideals in $\mathbb{k}(\omega, N)$. We also give an explicit description of all indecomposable right ideals therein. This is of interest from the Coding Theory point of view because isomorphic ideals needs not to give rise to equivalent codes. Then we attach to $\mathbb{k}(\omega, N)$ a particular bilinear form which we prove to be monomial in Lemma 13. In Theorem 14, we describe explicitly the orthogonals, with respect to this form, of the representatives of indecomposable right ideals mentioned above.

In Section 3 we turn our attention to Hopf algebras. A peculiar result in Hopf theory is the Structure Theorem for Hopf Modules. Given a finite-dimensional Hopf algebra H , the structure theorem yields a right H -linear isomorphism $\phi : H \rightarrow H^*$. Surprisingly, ϕ comes out to generalize the map (0.1) giving the correspondence mentioned above for cyclic codes; thus ϕ looks like a natural tool to generalize cyclic codes to Hopf algebras. In general ϕ yields a bijective correspondence between right ideals in H and right H -submodules of H^* (which play the role of generalized cyclic codes). We attach to ϕ a specific non-degenerate bilinear form and use it to define two different notions of dual for a given right ideal: both comes out to be right ideals as well. We investigate this form in the case when H or its antipode S satisfy some properties, such as H being cosemisimple in Lemma 19.

In Section 4 we collect and investigate the main examples and applications of our results.

First we recover the cyclic group algebra as a trivial case of $\mathbb{k}(\omega, N)$ taking $\omega = \text{Id}$ and $N = 1$ in Subsection 4.1.

Then, in Subsection 4.2, we apply our machinery to the Taft algebra. This is achieved regarding the Taft algebra as an algebra of the form $\mathbb{k}(\omega, N)$ in Lemma 24 and showing in Lemma 26 that the non-degenerate bilinear form attached to ϕ is one of the canonical monomial forms we investigated on $\mathbb{k}(\omega, N)$. As a consequence we recover all indecomposable right ideals for the Taft algebra in Theorem 28 and the corresponding orthogonals in Theorem 29.

Finally in Subsection 4.3, we consider a 24-dimensional Hopf algebra arising as a bosonization described in [CDMM]. Following the lines of the previous examples, we show in Lemma 30 that also this algebra is of the form $\mathbb{k}(\omega, N)$ and in Lemma 32 that the non-degenerate bilinear form attached to ϕ is one of the canonical monomial forms we investigated on $\mathbb{k}(\omega, N)$. Also in this case we obtain a complete description of indecomposable right ideals in Theorem 34 and their orthogonals in 35. This classification is new at the best of our knowledge.

1. BILINEAR FORMS

In this section we deal with general results concerning vector spaces.

Let V be a finite-dimensional vector space and let $\langle -, - \rangle : V \times V \rightarrow \mathbb{k}$ be a bilinear form on V . The form is non-degenerate if and only if the linear map $\phi : V \rightarrow V^*$, defined by setting $\phi(v) = \langle v, - \rangle$ for every $v \in V$, is an isomorphism.

If $\langle -, - \rangle$ is non-degenerate there is a unique linear map $\gamma : V \rightarrow V$ such that

$$(1.1) \quad \langle x, y \rangle = \langle y, \gamma(x) \rangle, \text{ for all } x, y \in V,$$

The map γ is necessarily injective whence invertible as V is finite-dimensional. We call it the *Nakayama isomorphism* (if V is an algebra and the form is associative, i.e. $\langle xy, z \rangle = \langle x, yz \rangle$ for all $x, y, z \in V$, then γ becomes an algebra automorphism known as the Nakayama automorphism).

Given a linear subspace W of V , we define the left and right orthogonals of W as the vector subspaces

$$\begin{aligned} W^{\perp L} &:= \{x \in V \mid \langle x, y \rangle = 0, \forall y \in W\}, \\ W^{\perp R} &:= \{x \in V \mid \langle y, x \rangle = 0, \forall y \in W\}. \end{aligned}$$

We will simply write W^\perp when $W^{\perp L} = W^{\perp R}$. In particular this happens if, for every $x, y \in V$, one has $\langle x, y \rangle = 0 \Leftrightarrow \langle y, x \rangle = 0$.

Lemma 1. [Ja, Section 6.1] *Assume $\langle -, - \rangle$ is non-degenerate and let U and W be subspaces of V . Then*

- if $U \subseteq W$ then $W^{\perp L} \subseteq U^{\perp L}$ and $W^{\perp R} \subseteq U^{\perp R}$;
- $(U + W)^{\perp L} = U^{\perp L} \cap W^{\perp L}$ and $(U + W)^{\perp R} = U^{\perp R} \cap W^{\perp R}$;
- $(U \cap W)^{\perp L} = U^{\perp L} + W^{\perp L}$ and $(U \cap W)^{\perp R} = U^{\perp R} + W^{\perp R}$;
- $\dim_{\mathbb{k}} W^{\perp L} = \dim_{\mathbb{k}} V - \dim_{\mathbb{k}} W = \dim_{\mathbb{k}} W^{\perp R}$;
- $W^{\perp R \perp L} = W = W^{\perp L \perp R}$.

Lemma 2. *Let $\gamma : V \rightarrow V$ be a \mathbb{k} -linear isomorphism such that (1.1) holds true. Then $W^{\perp R} = \gamma(W^{\perp L})$ for every subspace W of V .*

Proof. Let $x \in V$. Then $\gamma(x) \in W^{\perp R}$ if and only if $\langle y, \gamma(x) \rangle = 0$, for every $y \in W$. By (1.1) this is equivalent to $\langle x, y \rangle = 0$, for every $y \in W$ i.e. $x \in W^{\perp L}$. Thus $\gamma(x) \in W^{\perp R}$ if and only if $x \in W^{\perp L}$. Since γ is invertible we conclude. \square

As usual let us denote by \mathcal{S}_n the group of permutations of the set $\{1, \dots, n\}$ for every $n \geq 1$.

Definition 3. Given a \mathbb{k} -vector space V with basis $\mathcal{B} = \{v_1, \dots, v_n\}$, a *right monomial transformation of V with respect to \mathcal{B}* (see e.g. [Wo, page 12]) is a \mathbb{k} -linear map $T := T(\sigma, k_i) : V \rightarrow V$ such that $T(v_i) = k_i v_{\sigma(i)}$ where $\sigma \in \mathcal{S}_n$ and $k_i \in \mathbb{k} \setminus \{0\}$ for every $i \in \{1, \dots, n\}$.

Lemma 4. *The following are equivalent for a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V .*

- (1) *There is $\sigma \in \mathcal{S}_n$ and non-zero elements $d_i \in \mathbb{k}$ such that, for every $i, j \in \{1, \dots, n\}$, one has $\langle v_i, v_j \rangle = d_i \delta_{\sigma(i), j}$.*
- (2) *There is $\sigma \in \mathcal{S}_n$ and non-zero elements $d_i \in \mathbb{k}$ such that $\phi(v_i) = d_i v_{\sigma(i)}^*$, where v_j^* is the dual basis element defined by $v_j^*(v_i) = \delta_{i, j}$.*
- (3) *The matrix of $\langle -, - \rangle$ relative to \mathcal{B} is of form $D \cdot P$ where D is a non-singular diagonal matrix and P is a permutation matrix.*
- (4) *The \mathbb{k} -linear map $T : \mathbb{k}^n \rightarrow \mathbb{k}^n : e_i \mapsto \sum_{j=1}^n \langle v_i, v_j \rangle e_j$ (i.e. the linear map attached to the matrix of $\langle -, - \rangle$ relative to \mathcal{B}) is a right monomial transformation of \mathbb{k}^n with respect to the canonical basis $\{e_1, \dots, e_n\}$.*

Proof. (1) \Leftrightarrow (2). This equivalence follows from the equalities $\phi(v_i)(v_j) = \langle v_i, v_j \rangle$ and $(d_i v_{\sigma(i)}^*)(v_j) = d_i \delta_{\sigma(i), j}$.

(1) \Leftrightarrow (3). Take $D = \text{diag}(d_1, \dots, d_n)$ and let P be the matrix whose (i, j) -entry is given by $\delta_{\sigma(i), j}$. Then the (i, j) -entry of $D \cdot P$ is exactly $d_i \delta_{\sigma(i), j}$.

(1) \Leftrightarrow (4). By definition T is a right monomial transformation if and only if there is a permutation σ of $\{1, \dots, n\}$ and non-zero elements $d_i \in \mathbb{k}$ such that $T(e_i) = d_i e_{\sigma(i)}$. \square

Definition 5. We say that the bilinear form $\langle -, - \rangle$ is *monomial* (with respect to \mathcal{B}) if one of the equivalent conditions of Lemma 4 holds. Note that a monomial bilinear form is necessarily non-degenerate since $\phi(v_i) = d_i v_{\sigma(i)}^*$ for every $i \in \{1, \dots, n\}$.

Remark 6. Let V be a vector space with basis $\mathcal{B} = \{v_1, \dots, v_n\}$. The following are equivalent for $\tau \in \mathcal{S}_n$ and non-zero elements $c_i \in \mathbb{k}$.

- (1) For every $i, j \in \{1, \dots, n\}$, one has $\langle v_i, v_j \rangle = c_i \langle v_j, v_{\tau(i)} \rangle$.
- (2) One has that (1.1) holds true where $\gamma := T(\tau, c_i) : V \rightarrow V$ is the linear map defined by $v_i \mapsto c_i v_{\tau(i)}$. Note that γ is necessarily invertible.

Remark 7. Let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis of V and let W be a subspace of V . Assume there is a right monomial transformation $\gamma = T(\tau, c_i)$ such that (1.1) holds true. By [Wo, Proposition 6.1], we have that γ is an isometry of V with respect to the basis \mathcal{B} . By Lemma 2 we also have $W^{\perp R} = \gamma(W^{\perp L})$. Then $W^{\perp R}$ and $W^{\perp L}$ are equivalent codes in the sense of [Wo, page 565].

In the following result we describe the connection between the left and right orthogonals in case of vector subspaces spanned by suitable basis elements.

Lemma 8. *Let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis of V and let $W_B := \text{Span}_{\mathbb{k}} \{v_i \mid i \in B\}$ for some $B \subseteq \{1, \dots, n\}$.*

1) *Assume there is a right monomial transformation $\gamma = T(\tau, c_i)$ such that (1.1) holds true. Then $W_B^{\perp R} = W_{\tau(B)}^{\perp L}$ where $\tau(B) := \{v_{\tau(i)} \mid i \in B\}$.*

2) *If $\langle -, - \rangle$ is monomial with respect to \mathcal{B} , then **there is $\sigma \in \mathcal{S}_n$ such that the hypothesis of 1) holds for $\tau := \sigma^2$.***

Proof. 1) From the assumption one gets $\langle v_i, v \rangle = c_i \langle v, v_{\tau(i)} \rangle$ for every $v \in V$. Since $c_i \neq 0$ we deduce that $\langle v_i, v \rangle = 0$ if and only if $\langle v, v_{\tau(i)} \rangle = 0$. Now $v \in W_B^{\perp R}$ if and only if $\langle v_i, v \rangle = 0$ for every $i \in B$ if and only if, by the foregoing, $\langle v, v_{\tau(i)} \rangle = 0$ for every $i \in B$ if and only if $v \in W_{\tau(B)}^{\perp L}$.

2) By Lemma 4, there exists a permutation σ of $\{1, \dots, n\}$ and $\langle v_i, v_j \rangle = d_i \delta_{\sigma(i), j}$ for some non-zero $d_i \in \mathbb{k}$. Then we can take $c_i := \frac{d_i}{d_{\sigma(i)}}$ and compute

$$\langle v_j, c_i v_{\sigma^2(i)} \rangle = c_i d_j \delta_{\sigma(j), \sigma^2(i)} = c_i d_j \delta_{\sigma(i), j} = c_i d_{\sigma(i)} \delta_{\sigma(i), j} = d_i \delta_{\sigma(i), j} = \langle v_i, v_j \rangle.$$

□

Remark 9. In the case of the Taft algebra A we will provide a particular $\langle -, - \rangle$ which satisfies the conditions in Lemma 8 but not $\langle x, y \rangle = 0 \Leftrightarrow \langle y, x \rangle = 0$ for every $x, y \in A$, cf. [Ja, Theorem 6.2].

The proof of the following result is straightforward. We keep it for the reader's sake.

Proposition 10. *Let A be an algebra. Let V be a vector space endowed with a non-degenerate bilinear form $\langle -, - \rangle$ and let γ be the isomorphism given in (1.1). Let W be a subspace of V .*

1) *If V has a left A -module structure, then V has (necessarily unique) right A -module structures \triangleleft and \blacktriangleleft defined for every $x, y \in V, c \in A$, respectively, by*

$$\langle x \triangleleft c, y \rangle = \langle x, cy \rangle \quad \text{and} \quad \langle x, y \blacktriangleleft c \rangle = \langle cx, y \rangle.$$

Moreover $\{c \in A \mid \gamma(cx) = c\gamma(x), \forall x \in V\} = \{c \in A \mid y \triangleleft c = y \blacktriangleleft c, \forall y \in V\}$. In particular γ is left A -linear if and only if $\triangleleft = \blacktriangleleft$.

2) *If V has a right A -module structure, then V has (necessarily unique) left A -module structures \triangleright and \blacktriangleright defined for every $x, y \in V, c \in A$, respectively, by*

$$\langle c \triangleright x, y \rangle = \langle x, yc \rangle \quad \text{and} \quad \langle x, c \blacktriangleright y \rangle = \langle xc, y \rangle.$$

Moreover $\{c \in A \mid \gamma(xc) = \gamma(x)c, \forall x \in V\} = \{c \in A \mid c \triangleright y = c \blacktriangleright y, \forall y \in V\}$. In particular γ is right A -linear if and only if $\triangleright = \blacktriangleright$.

For $c \in A$, we have

$$\begin{aligned} (V \triangleleft c)^{\perp R} &= (V \blacktriangleleft c)^{\perp L} = \text{Ann}_{\bullet V}(c) := \{v \in V \mid cv = 0\}, \\ (c \triangleright V)^{\perp R} &= (c \blacktriangleright V)^{\perp L} = \text{Ann}_{V \bullet}(c) := \{v \in V \mid vc = 0\}. \end{aligned}$$

Let $a, b \in A$ be such that $ab = 1$. Then

$$\begin{aligned} (bW)^{\perp L} &= W^{\perp L} \triangleleft a & \text{and} & & (W \triangleleft a)^{\perp R} &= bW^{\perp R} \\ (W \blacktriangleleft a)^{\perp L} &= bW^{\perp L} & \text{and} & & (bW)^{\perp R} &= W^{\perp R} \blacktriangleleft a \\ (Wa)^{\perp L} &= b \triangleright W^{\perp L} & \text{and} & & (b \triangleright W)^{\perp R} &= W^{\perp R} a \\ (b \blacktriangleright W)^{\perp L} &= W^{\perp L} a & \text{and} & & (Wa)^{\perp R} &= b \blacktriangleright W^{\perp R} \end{aligned}$$

Proof. We just prove the assertions involving \triangleleft , the other ones being similar. Since $\phi : V \rightarrow V^*$ is an isomorphism and V^* is a right A -module we can endow V with a unique right A -module structure such that ϕ is right A -linear. The right A -linearity of ϕ is equivalent to $\langle x \triangleleft c, y \rangle = \langle x, cy \rangle$, for every $x, y \in V, c \in A$.

We compute

$$\begin{aligned}\langle x, y \blacktriangleleft c \rangle &= \langle cx, y \rangle = \langle y, \gamma(cx) \rangle; \\ \langle x, y \triangleleft c \rangle &= \langle y \triangleleft c, \gamma(x) \rangle = \langle y, c\gamma(x) \rangle.\end{aligned}$$

Then $\gamma(cx) = c\gamma(x)$ for every $x \in V$ if and only if $y \blacktriangleleft c = y \triangleleft c$ for every $y \in V$.

From $\langle x \triangleleft c, y \rangle = \langle x, cy \rangle$ it is clear that $(V \triangleleft c)^{\perp R} = \text{Ann}_{\bullet V}(c)$.

Then

$$\langle x \triangleleft a, by \rangle = \langle x, aby \rangle = \langle x, y \rangle$$

so that $x \in W^{\perp L}$ if and only if $x \triangleleft a \in (bW)^{\perp L}$. Thus $(bW)^{\perp L} = W^{\perp L} \triangleleft a$. Similarly $(W \triangleleft a)^{\perp R} = bW^{\perp R}$. \square

2. INDECOMPOSABLE IDEALS IN $\mathbb{k}(\omega, N)$

Let us consider the main example of algebra we will deal with. Let $N \geq 2$ be an integer, let S be a finite set of cardinality at least N and let ω be a permutation on S .

Consider the \mathbb{k} -algebra $A = \mathbb{k}(\omega, N)$ generated by $\{e_s, x \mid s \in S\}$ with relations, for every $s, t \in S$,

$$(2.1) \quad e_s e_t = \delta_{s,t} e_t, \quad 1_A = \sum_{s \in S} e_s, \quad x^N = 0, \quad e_s x = x e_{\omega(s)}.$$

It is clear that A has basis

$$\mathcal{B} := \{x^n e_s \mid 0 \leq n \leq N-1, s \in S\} = \{e_t x^n \mid 0 \leq n \leq N-1, t \in S\},$$

where the last equality follows by the relation $e_s x = x e_{\omega(s)}$, for all $s \in S$.

Let $R = \mathbb{k}[x \mid x^N = 0]$ be the subalgebra of A generated by x .

Set also $H := \mathbb{k}[e_s \mid s \in S]$.

Following the lines of [CGL], for $s \in S, t = 0, \dots, N-1$ we set $N_{s,t} := e_s x^t R$.

Remark 11. The algebra A given above can be constructed as follows. Let $H = \mathbb{k}^S = \text{Map}(S, \mathbb{k})$ be the algebra of functions on the set S . Define $e_s : S \rightarrow \mathbb{k}$ by setting $e_s(t) := \delta_{s,t}$. Then $\{e_s \mid s \in S\}$ is a basis of H and for every $s, t \in S$, one has

$$e_s e_t = \delta_{s,t} e_t, \quad 1_A = \sum_{s \in S} e_s.$$

Define the map $\varphi : H \rightarrow H$ by setting $\varphi(e_s) := e_{\omega^{-1}(s)}$. It is easy to check that φ is an algebra map. Consider the Ore extension $H[X, \varphi]$ with zero derivation i.e. $H[X]$ as an abelian group with multiplication induced by $X e_s = \varphi(e_s) X$. Then $A = \mathbb{k}(\omega, N)$ is the quotient of $H[X, \varphi]$ modulo the two-sided ideal $\langle X^N \rangle$ generated by X^N , with notation $x := X + \langle X^N \rangle$ and by identifying e_s with its class modulo $\langle X^N \rangle$.

Denote by $\mathcal{L}(M_R)$ the set of right R -submodules of a given right R -module M_R . Let $\mathcal{L}_{\text{in}}(M_R)$ denote the set of right R -submodules which are indecomposable. The first assertion of the following result was already proved for Taft algebras in [CGL, Section 2], see also [CVZ, Theorem 2.5].

Theorem 12. *Consider the algebra $A = \mathbb{k}(\omega, N)$ and let R be the subalgebra of A generated by x . Then the $N_{s,t}$'s form an irredundant set of representatives of $\mathcal{L}_{\text{in}}(A_A)$ and*

$$\mathcal{L}_{\text{in}}(A_A) = \{(1 + rx)N_{s,t} \mid r \in R, s \in S, 0 \leq t \leq N - 1\}.$$

Proof. We have already observed that A has basis

$$\mathcal{B} := \{x^n e_s \mid 0 \leq n \leq N - 1, s \in S\} = \{e_t x^n \mid 0 \leq n \leq N - 1, t \in S\}.$$

Let us show that A is a serial ring. Since $1_A = \sum_{s \in S} e_s$ and the e_s 's are orthogonal idempotents, we have that $A = \bigoplus_{s \in S} e_s A$. Thus each direct summand $e_s A$ of A is projective too. By (2.1), we deduce $e_s A = e_s R$ and hence $\mathcal{L}(e_s A_A) = \mathcal{L}(e_s R_R)$. The map

$$g_s : R \rightarrow e_s R : r \mapsto e_s r$$

is an isomorphism of right R -modules so that it induces a bijection

$$\mathcal{L}(R_R) \rightarrow \mathcal{L}(e_s R_R) : I \mapsto g_s(I) = e_s I.$$

Since $\mathcal{L}(R_R) = \{x^t R \mid 0 \leq t \leq N\}$ we get

$$\mathcal{L}(e_s A_A) = \mathcal{L}(e_s R_R) = \{e_s x^t R \mid 0 \leq t \leq N\} = \{N_{s,t} \mid 0 \leq t \leq N - 1\} \cup \{0\}.$$

Since $N_{s,t} \subseteq N_{s,w}$ for $t \geq w$, we deduce that $\mathcal{L}(e_s A_A)$ is totally ordered. Thus $e_s A$ is uniserial for every $s \in S$ and hence A is a right serial ring. Similarly one proves it is a left serial ring. Thus it is a serial ring as claimed.

Note that, since uniserial implies indecomposable, we get that

$$\mathcal{L}_{\text{in}}(e_s A_A) = \mathcal{L}(e_s A_A) \setminus \{0\} = \{N_{s,t} \mid 0 \leq t \leq N - 1\}.$$

Let $M \in \mathcal{L}_{\text{in}}(A_A)$. Apply [Fa, Theorem 3.29] to $P = A_A$. Then there is a decomposition $A_A = P_1 \oplus \cdots \oplus P_l$ into uniserial projective modules such that $M = (M \cap P_1) \oplus \cdots \oplus (M \cap P_l)$. Since M is indecomposable, we get $M = M \cap P_w$ for some w . Hence $M \subseteq P_w$. Since each P_i is uniserial, it is in particular indecomposable.

Note that $\text{End}_A(e_s A) \cong e_s A e_s \stackrel{(2.1)}{=} e_s R e_s$. Since $R = \mathbb{k}[x \mid x^N = 0]$ is a local ring, we have that $e_s R$ is a local right R -module so that, by [Fa, Theorem 1.11], we get that $e_s R e_s$ is a local ring.

By Krull-Schmidt-Remak-Azumaya Theorem (cf. [Fa, Theorem 2.12]), the two decompositions $\bigoplus_{s \in S} e_s A = A_A = P_1 \oplus \cdots \oplus P_l$ are necessarily isomorphic so that $P_w \cong e_s A$ for some $s \in S$. Let $f_w : e_s A \rightarrow P_w$ this isomorphism of right A -modules.

We have $f_w(e_s) = f_w(e_s e_s) = f_w(e_s) e_s \in A e_s = R e_s$ so that we can write $f_w(e_s) = u e_s$ for some $u \in R$. We can assume that u has the form $u = (1 + rx)x^t$ for some w so that $f_w(e_s) = (1 + rx)x^t e_s$. Thus

$$\begin{aligned} P_w &= f_w(e_s A) = f_w(e_s) A = (1 + rx)x^t e_s A = (1 + rx)x^t e_s R \\ &= (1 + rx)e_{\omega-t(s)} x^t R = (1 + rx)N_{\omega-t(s),t}. \end{aligned}$$

Via f_w we have that $P_w \cong e_s A = e_s R = N_{s,0}$. Thus

$$\begin{aligned} N &= \dim_{\mathbb{k}}(N_{s,0}) = \dim_{\mathbb{k}}(P_w) \\ &= \dim_{\mathbb{k}}((1 + rx)N_{\omega-t(s),t}) = \dim_{\mathbb{k}}(N_{\omega-t(s),t}) = N - t \end{aligned}$$

so that $t = 0$ and hence $P_w = (1 + rx)N_{s,0}$ and $f_w(e_s) = (1 + rx)e_s$. Hence $f_w(a) = (1 + rx)a$ for every $a \in e_s A$.

The isomorphism f_w induces a bijection

$$\mathcal{L}_{\text{in}}(e_s A_A) \rightarrow \mathcal{L}_{\text{in}}((P_w)_A) : I \mapsto f_w(I) = (1 + rx)I.$$

Since M is indecomposable and $M \subseteq P_w$ then $M \in \mathcal{L}_{\text{in}}((P_w)_A)$ so that it comes out to be isomorphic to an element of $\mathcal{L}_{\text{in}}(e_s A_A) = \{N_{s,t} \mid s \in S, 0 \leq t \leq N-1\}$. This proves that the $N_{s,t}$'s form an irredundant set of representatives of $\mathcal{L}_{\text{in}}(A_A)$. Moreover $M = (1+rx)N_{s,t}$ for some $s \in S, 0 \leq t \leq N-1$.

We have so proved that $\mathcal{L}_{\text{in}}(A_A) \subseteq \{(1+rx)N_{s,t} \mid r \in R, s \in S, 0 \leq t \leq N-1\}$.

For the other inclusion, since $(1+rx)N_{s,t} \cong N_{s,t}$ and $N_{s,t} \in \mathcal{L}_{\text{in}}(e_s A_A)$, we get that $(1+rx)N_{s,t}$ is indecomposable. \square

In the rest of this section we fix a permutation μ on S , a permutation ν on $\{0, 1, \dots, N-1\}$ and define a bilinear form $\langle -, - \rangle : A \times A \rightarrow \mathbb{k}$ by setting, for $s, t \in S, 0 \leq m, n \leq N-1$,

$$(2.2) \quad \langle e_s x^m, e_t x^n \rangle := d_{(s,m)} \delta_{\mu(s),t} \delta_{\nu(m),n}$$

where $d_{(s,m)} \in \mathbb{k} \setminus \{0\}$ for all s, m .

Lemma 13. *The form $\langle -, - \rangle$ is monomial with respect to the basis*

$$\mathcal{B} = \{e_s x^m \mid s \in S, 0 \leq m \leq N-1\}.$$

Moreover the Nakayama isomorphism γ is given by

$$\gamma(e_s x^m) = \frac{d_{(s,m)}}{d_{(\mu(s),\nu(m))}} e_{\mu^2(s)} x^{\nu^2(m)} \quad \forall s, m.$$

Proof. Set $v_{(s,m)} := e_s x^m$. Then $\langle v_{(s,m)}, v_{(t,n)} \rangle = d_{(s,m)} \delta_{\sigma((s,m)),(t,n)}$ where σ is the permutation defined by $\sigma := \mu \times \nu : (s, m) \mapsto (\mu(s), \nu(m))$.

Thus, by definition, the form $\langle -, - \rangle$ is monomial with respect to \mathcal{B} . By Lemma 8, there is a right monomial transformation $\gamma = T(\tau, c_{(s,m)})$ (which is necessarily the Nakayama isomorphism) such that (1.1) holds true for $\tau := \sigma^2 = \mu^2 \times \nu^2$ and

$$c_{(s,m)} = \frac{d_{(s,m)}}{d_{\sigma((s,m))}} = \frac{d_{(s,m)}}{d_{(\mu(s),\nu(m))}}.$$

Thus $\gamma(v_{(s,m)}) = c_{(s,m)} v_{\tau((s,m))}$ and hence $\gamma(e_s x^m) = \frac{d_{(s,m)}}{d_{(\mu(s),\nu(m))}} e_{\mu^2(s)} x^{\nu^2(m)}$. \square

Apply Proposition 10 to $V = A$ and $\langle -, - \rangle$ as above. Then A has a unique right A -module structure \triangleleft defined by $\langle x \triangleleft c, y \rangle = \langle x, cy \rangle$, for every $x, y, c \in A$ and a unique right A -modules structure \blacktriangleleft defined by $\langle x, y \blacktriangleleft c \rangle = \langle cx, y \rangle$.

Moreover, if $a \in A$ is a unit, for every subspace W of A one has

$$(aW)^{\perp L} = W^{\perp L} \triangleleft a^{-1} \quad \text{and} \quad (aW)^{\perp R} = W^{\perp R} \blacktriangleleft a^{-1}.$$

In view of Theorem 12, we know that

$$\mathcal{L}_{\text{in}}(A_A) = \{(1+rx)N_{s,t} \mid r \in R, s \in S, 0 \leq t \leq N-1\}$$

so that we can compute the orthogonals of all indecomposable right ideals as

$$(2.3) \quad ((1+rx)N_{s,t})^{\perp L} = N_{s,t}^{\perp L} \triangleleft (1+rx)^{-1}$$

$$(2.4) \quad ((1+rx)N_{s,t})^{\perp R} = N_{s,t}^{\perp R} \blacktriangleleft (1+rx)^{-1}.$$

It remains to compute $N_{s,m}^{\perp L}$ and $N_{s,m}^{\perp R}$.

Theorem 14. *Let $s \in S$ and m be an integer such that $0 \leq m \leq N-1$. We have*

$$N_{s,0}^{\perp R} = N_{\mu^2(s),0}^{\perp L} = \bigoplus_{t \neq \mu(s)} N_{t,0}.$$

Assume $\nu(m) := N - 1 - m$ for all m . Then

$$N_{s,m}^{\perp R} = N_{\mu^2(s),m}^{\perp L} \quad \text{and} \quad N_{s,m}^{\perp R} = N_{s,0}^{\perp R} \oplus N_{\mu(s),N-m}.$$

Proof. Note that $N_{s,0} := e_s R$ has basis $B = \{e_s x^m \mid 0 \leq m \leq N-1\}$ which is a subset of the basis $\mathcal{B} = \{e_s x^m \mid s \in S, 0 \leq m \leq N-1\}$. In view of Lemma 13, this basis satisfies the conditions of Lemma 8 for $\tau = \mu^2 \times \nu^2$, so that

$$\tau(B) = \left\{ e_{\mu^2(s)} x^{\nu^2(m)} \mid 0 \leq m \leq N-1 \right\} = \left\{ e_{\mu^2(s)} x^n \mid 0 \leq n \leq N-1 \right\}$$

and hence $N_{s,0}^{\perp R} = W_B^{\perp R} = W_{\tau(B)}^{\perp L} = N_{\mu^2(s),0}^{\perp L}$.

By definition, we have

$$\langle e_s x^m, e_t x^n \rangle := d_{(s,m)} \delta_{\mu(s),t} \delta_{\nu(m),n}$$

so if $t \neq \mu(s)$ then $N_{t,0} \subseteq N_{s,0}^{\perp R}$ and hence $\bigoplus_{t \neq \mu(s)} N_{t,0} \subseteq N_{s,0}^{\perp R}$. Now, counting dimensions we get

$$\begin{aligned} \dim_{\mathbb{k}} \left(\bigoplus_{t \neq \mu(s)} N_{t,0} \right) &= \left(\sum_{t \neq \mu(s)} N \right) = N(|S| - 1) = N|S| - N \\ &= N|S| - \dim_{\mathbb{k}} N_{s,0} = \dim_{\mathbb{k}} N_{s,0}^{\perp R} \end{aligned}$$

which implies the equality whence $N_{s,0}^{\perp R} = \bigoplus_{t \neq \mu(s)} N_{t,0}$.

Assume $\nu(m) := N - 1 - m$ for all m (note that $\nu^2 = \text{Id}$). Since $N_{s,m} := e_s x^m R$ has basis $B = \{e_s x^t \mid m \leq t \leq N-1\}$, we get

$$\tau(B) = \left\{ e_{\mu^2(s)} x^{\nu^2(t)} \mid m \leq t \leq N-1 \right\} = \left\{ e_{\mu^2(s)} x^t \mid m \leq t \leq N-1 \right\}$$

and hence $N_{s,m}^{\perp R} = N_{\mu^2(s),m}^{\perp L}$.

We now compute $N_{s,m}^{\perp R}$.

If $t = \mu(s)$ then if $n \geq \nu(m) + 1 = N - m$ we get $\langle e_t x^n, e_s x^m \rangle = 0$, so $N_{\mu(s),N-m} \subseteq N_{s,m}^{\perp R}$. Since $N_{s,0}^{\perp R} = \bigoplus_{t \neq \mu(s)} N_{t,0}$ we have that $N_{s,0}^{\perp R} + N_{\mu(s),N-m} = N_{s,0}^{\perp R} \oplus N_{\mu(s),N-m}$ and hence

$$N_{s,0}^{\perp R} \oplus N_{\mu(s),N-m} \subseteq N_{s,m}^{\perp R}.$$

Now, counting dimensions we get

$$\begin{aligned} \dim_{\mathbb{k}} \left(N_{s,0}^{\perp R} \oplus N_{\mu(s),N-m} \right) &= (N|S| - N) + m = N|S| - N + m \\ &= N|S| - \dim_{\mathbb{k}} N_{s,m} = \dim_{\mathbb{k}} N_{s,m}^{\perp R} \end{aligned}$$

which implies the equality whence $N_{s,m}^{\perp R} = N_{s,0}^{\perp R} \oplus N_{\mu(s),N-m}$ as desired. \square

3. IDEALS AND THEIR ORTHOGONALS FOR HOPF ALGEBRAS

From now on, H will always be a finite-dimensional Hopf algebra with antipode S .

Consider H^* as a right Hopf module with action \leftarrow defined by $(f \leftarrow h)(l) := f(lS(h))$. Then, by [Sw, Corollary 5.1.6 and Theorem 5.1.3], we have that S is invertible, the space $\int_l(H^*)$ of left integrals in H^* is one-dimensional (recall that

$\lambda \in H^*$ belongs to $\int_l(H^*)$ if and only if $\sum h_1 \lambda(h_2) = 1_H \lambda(h)$ for all $h \in H$ and the map

$$\int_l(H^*) \otimes H \rightarrow H^* : f \otimes h \mapsto (f \leftarrow h)$$

is bijective. Since $\int_l(H^*)$ is one-dimensional, we can choose a non-zero integral $\lambda \in H^*$ and the map

$$\phi : H \rightarrow H^* : h \mapsto (\lambda \leftarrow h)$$

is invertible, see [DNR, page 306]. The map ϕ is right H -linear:

$$\phi(hh') = \lambda \leftarrow (hh') = (\lambda \leftarrow h) \leftarrow h' = \phi(h) \leftarrow h'.$$

Note that the structure of right H -module on H^* is not the canonical one \leftarrow given by $(f \leftarrow h)(l) = f(lh)$.

Through ϕ one has a bijective correspondence between right ideals in H and right H -submodules of H^* .

Remark 15. Set $t := \phi^{-1}(\varepsilon) \in H$. By [DNR, Section 7.4], we have that t is a right integral in H (i.e. $th = t\varepsilon(h)$ for every $h \in H$) and $\lambda(t) = 1$. Moreover

$$\phi^{-1}(f) = \sum t_1 f(t_2), \text{ for every } f \in H^*.$$

Note that given any right integral t' in H such that $\lambda(t') = 1$ then $S(t')$ is a left integral ([Ra, Exercise 10.5.1, page 305]) and $\lambda S(t') = \lambda(t')$ (by the left-right handed version of [Ra, Exercise 10.5.3, page 311]) so that $\phi(t')(y) = \lambda(yS(t')) = \lambda(\varepsilon(y)S(t')) = \varepsilon(y)\lambda(S(t')) = \varepsilon(y)\lambda(t') = \varepsilon(y)$ and hence $\phi(t') = \varepsilon$. As a consequence $t' = \phi^{-1}(\varepsilon) = t$.

We now are going to apply the results of Section 1 in the case V is a Hopf algebra H . In the setting of Section 3, for every $x, y \in H$, we set

$$(3.1) \quad \langle x, y \rangle := \phi(x)(y) = (\lambda \leftarrow x)(y) = \lambda[yS(x)].$$

Note that, since ϕ is an isomorphism and H is finite-dimensional, the bilinear form $\langle -, - \rangle$ is non-degenerate.

For $x, y, h \in H$, we have

$$(3.2) \quad \langle xh, y \rangle = \lambda[yS(xh)] = \lambda[yS(h)S(x)] = \langle x, yS(h) \rangle$$

and

$$(3.3) \quad \sum \langle x_1, y \rangle x_2 = \sum \lambda[yS(x_1)] x_2 \stackrel{(*)}{=} \sum y_1 \lambda[y_2 S(x)] = \sum y_1 \langle x, y_2 \rangle$$

where in $(*)$ we used [DNR, Lemma 5.1.4].

The Frobenius bilinear form $b : H \times H \rightarrow \mathbb{k}$ is defined by setting $b(x, y) := (\phi \circ S^{-1})(y)(x) = \lambda(xy)$ for every $x, y \in H$. This bilinear form is non-degenerate because $\phi \circ S^{-1}$ is invertible. Consider the associated Nakayama automorphism $\eta : H \rightarrow H$ (we know that it is an algebra map because H is an algebra and the form is associative). Note that η is uniquely determined by the equality $b(x, y) = b(y, \eta(x))$ i.e. $\lambda(xy) = \lambda(y\eta(x))$ for every $x, y \in H$.

Lemma 16. *In the setting of Proposition 10, take V the underlying algebra of H with left and right regular actions. Then, for every $h, x \in H$, we have*

$$\begin{aligned} h \triangleright x &= xS^{-1}(h) & \text{and} & & h \blacktriangleright x &= xS(h), \\ x \triangleleft h &= S^{-1}(\eta(h))x & \text{and} & & x \blacktriangleleft h &= \eta^{-1}(S(h))x. \end{aligned}$$

Moreover $\text{Ann}_{\bullet H}(h) = (\eta^{-1}(S(h)))^{\perp L}$ and $\text{Ann}_{H\bullet}(h) = (S(h))^{\perp L}$ for every $h \in H$.

Proof. By definition of \triangleright , \blacktriangleright and (3.2), we have

$$\langle h \triangleright x, y \rangle = \langle x, yh \rangle = \langle xS^{-1}(h), y \rangle \quad \text{and} \quad \langle y, h \blacktriangleright x \rangle = \langle yh, x \rangle = \langle y, xS(h) \rangle.$$

Since the form is non-degenerate, we get $h \triangleright x = xS^{-1}(h)$ and $h \blacktriangleright x = xS(h)$.

For every $x, y, h \in H$,

$$\begin{aligned} \langle x \triangleleft h, y \rangle &= \langle x, hy \rangle = \lambda(hyS(x)) = \lambda(yS(x)\eta(h)) = \langle S^{-1}(\eta(h))x, y \rangle \\ \langle y, x \blacktriangleleft h \rangle &= \langle hy, x \rangle = \lambda(xS(y)S(h)) = \lambda(\eta^{-1}(S(h))xS(y)) = \langle y, \eta^{-1}(S(h))x \rangle \end{aligned}$$

so that we obtain $x \triangleleft h = S^{-1}(\eta(h))x$ and $x \blacktriangleleft h = \eta^{-1}(S(h))x$.

By Proposition 10, we have

$$\begin{aligned} (\eta^{-1}(S(h)))^{\perp L} &= (H \blacktriangleleft h)^{\perp L} = \text{Ann}_{\bullet H}(h) \\ (S(h))^{\perp L} &= (h \blacktriangleright H)^{\perp L} = \text{Ann}_{H\bullet}(h). \end{aligned}$$

□

Lemma 17. *If I is a right ideal of H , then $I^{\perp R}$ and $I^{\perp L}$ are right ideals.*

Proof. Given $x \in I^{\perp L}$, $y \in I$ and $h \in H$, we get $\langle xh, y \rangle = \langle x, yS(h) \rangle = 0$, as $yS(h) \in I$, and hence $xh \in I^{\perp L}$, so $I^{\perp L}$ is a right ideal.

Let now $x \in I^{\perp R}$, $y \in I$ and $h \in H$. Since H is finite-dimensional, S is surjective so there exists an $h' \in H$ such that $h = S(h')$; we get $\langle y, xh \rangle = \langle y, xS(h') \rangle = \langle yh', x \rangle = 0$ since $yh' \in I$ and hence $xh \in I^{\perp R}$, so $I^{\perp R}$ is a right ideal. □

Remark 18. Let H be a Hopf algebra with basis $\mathcal{B} = \{v_1, \dots, v_n\}$. Let $\gamma : H \rightarrow H$ be a \mathbb{k} -linear isomorphism such that (1.1) holds true. Then $\lambda S(x) = \langle x, 1 \rangle = \langle 1, \gamma(x) \rangle = \lambda \gamma(x)$ so that

$$(3.4) \quad \lambda S = \lambda \gamma.$$

Lemma 19. *Let H be a Hopf algebra with basis $\mathcal{B} = \{v_1, \dots, v_n\}$.*

- (1) *Assume there is a right monomial transformation γ such that (1.1) holds true as in Remark 6. Then $\gamma = \gamma(1)S^2$.*
- (2) *Assume H is cosemisimple. If, for every $i \in \{1, \dots, n\}$, $S^2(v_i) = c_i v_i$, then for every $i, j \in \{1, \dots, n\}$, $\langle v_i, v_j \rangle = c_i \langle v_j, v_i \rangle$. Moreover the map $\gamma := T(\text{Id}, c_i)$ of Remark 6 is exactly S^2 .*

Proof. (1). We compute, for every $x, y \in H$

$$\langle y, \gamma(x) \rangle \stackrel{(1.1)}{=} \langle x, y \rangle \stackrel{(3.2)}{=} \langle 1, yS(x) \rangle \stackrel{(1.1)}{=} \langle yS(x), \gamma(1) \rangle \stackrel{(3.2)}{=} \langle y, \gamma(1)S^2(x) \rangle.$$

Since $\langle -, - \rangle$ is a non-degenerate we then get $\gamma(x) = \gamma(1)S^2(x)$ for every $x \in H$.

(2). Note that, in our setting, $\langle x, y \rangle = \lambda[yS(x)]$ for some non-zero integral λ . Since H is cosemisimple, it has a total integral Λ . Since $\int_l(H^*)$ is one-dimensional, there is $k \in \mathbb{k}$ such that $\lambda = k\Lambda$. Thus, from $\Lambda S = \Lambda$, we obtain $\lambda S = k\Lambda S = k\Lambda = \lambda$. Since S is invertible and $S^2(v_i) \in \mathbb{k}v_i$, there is a non-zero element $c_i \in \mathbb{k}$ such that $S^2(v_i) = c_i v_i$. Hence, for every $x, y \in H$, we have

$$c_i \langle v_j, v_i \rangle = c_i \lambda [v_i S(v_j)] = \lambda [S^2(v_i) S(v_j)]$$

$$= \lambda S[v_j S(v_i)] = \lambda[v_j S(v_i)] = \langle v_i, v_j \rangle.$$

By definition $\gamma(v_i) = c_i v_i = S^2(v_i)$. \square

As a consequence we recover the following well-known result.

Corollary 20. *Let H be a finite-dimensional Hopf algebra.*

- (1) *If $\langle -, - \rangle : H \otimes H \rightarrow \mathbb{k}$ is symmetric, then H is involutory (i.e. $S^2 = \text{Id}_H$).*
- (2) *Assume H is cosemisimple. If H is involutory, then $\langle -, - \rangle : H \otimes H \rightarrow \mathbb{k}$ is symmetric.*

Remark 21. Let H be a finite-dimensional involutory Hopf algebra (e.g. H is either commutative or cocommutative, see [DNR, Corollary 4.2.8]). Then H is semisimple and H cosemisimple if and only if $\text{char} \mathbb{k} \nmid \dim_{\mathbb{k}} H$, see [LR, Corollary 2.6].

Lemma 22. *Let H be a finite-dimensional Hopf algebra with basis $\mathcal{B} = \{v_1, \dots, v_n\}$ and let I be a right ideal of H . Then $S^{-1}(\text{Ann}_H(I)) \subseteq I^{\perp L}$, where S^{-1} denotes the composition inverse of the antipode.*

Assume there is a right monomial transformation γ such that (1.1) holds true. If $I^{\perp L}$ is a two-sided ideal, then equality holds.

Proof. Let $x \in \text{Ann}_H(I) := \{h \in H \mid yh = 0, \forall y \in I\}$. Then, for every $y \in I$, we have $\langle S^{-1}(x), y \rangle \stackrel{(3.2)}{=} \langle 1, yx \rangle = 0$ so that $S^{-1}(x) \in I^{\perp L}$.

Let us prove the last part of the statement. Let $x \in I^{\perp L}$. Then for every $z \in H$, we have

$$\langle yS(x), z \rangle \stackrel{(1.1)}{=} \langle \gamma^{-1}(z), yS(x) \rangle \stackrel{(3.2)}{=} \langle \gamma^{-1}(z)x, y \rangle \stackrel{\gamma^{-1}(z)x \in I^{\perp L}}{=} 0.$$

Since $\langle -, - \rangle$ is a non-degenerate, we get that $yS(x) = 0$ and hence $S(x) \in \text{Ann}_H(I)$. Thus $S(I^{\perp L}) \subseteq \text{Ann}_H(I)$. Applying S^{-1} on both sides we obtain $I^{\perp L} \subseteq S^{-1}(\text{Ann}_H(I))$. \square

4. Examples and applications

In the present section, for every $n \geq 2$ and $a, b \in \mathbb{Z}$, we use the notation

$$\delta_{a,b}^{\equiv n} := \begin{cases} 1, & \text{if } a \equiv_n b \\ 0, & \text{otherwise} \end{cases}$$

4.1. Cyclic group algebra . The aim of this section is to show how our treatment specializes to classical cyclic codes in case of the cyclic group algebra $H := \mathbb{k}[X]/(X^n - 1) = \mathbb{k}\langle x \mid x^n = 1 \rangle$ where $x := X + (X^n - 1)$.¹

Consider $\lambda \in H^*$ defined on generators by $\lambda(x^i) := \delta_{i,0}$ for $0 \leq i \leq n-1$, see [DNR, Example 5.2.9-2)]. Now $t = \sum_{i=0}^{n-1} x^i$ is both a left and right integral (see [Sw, Examples 1])), and $\lambda(t) = 1$ so that, by Remark 15,

$$\phi^{-1}(f) = \sum t_1 f(t_2) = \sum_{i=0}^{n-1} x^i f(x^i), \text{ for every } f \in H^*.$$

¹Note that here we use the notation x for the generator because it is standard in Code Theory. Later on, dealing with Taft algebras, we will use the notation g for the same element reminding it is a group-like element.

In this specific case we can express ϕ explicitly as follows:

$$\phi : H \rightarrow H^* : c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \mapsto \sum c_i \phi(x^i)$$

where $\phi(x^i) \in H^*$ is defined by $\phi(x^i)(x^j) = \lambda(x^{j-i}) = \delta_{i,j}, \forall j \in \{0, \dots, n-1\}$ so that $\phi(x^0), \dots, \phi(x^{n-1})$ is the dual basis of $1, \dots, x^{n-1}$.

Consider the isomorphism $\alpha : H^* \rightarrow \mathbb{k}^n : f \mapsto (f_0, f_1, \dots, f_{n-1})$ where $f_i := f(x^i)$. It permits to regard the elements of H^* as code words, although it strictly depends on the chosen basis for H . In view of [Ab, 2.2, page 70], α is an algebra map, where H^* carries the convolution product. The right H -module structure of H^* given by \leftarrow induces, via α , a right H -module structure on \mathbb{k}^n . We want to give this structure explicitly. To this aim, for every $f \in H^*$ and $0 \leq i \leq n-1$, let $f_i := f(x^i)$. In other words $\alpha(f) = (f_0, f_1, \dots, f_{n-1})$. We compute

$$(f \leftarrow x)_i = (f \leftarrow x)(x^i) = f(x^{i-1}) = \begin{cases} f_{n-1} & \text{if } i = 0, \\ f_{i-1} & \text{if } 1 \leq i \leq n-1 \end{cases}$$

so that $\alpha(f \leftarrow x) = (f_{n-1}, f_0, f_1, \dots, f_{n-2})$. Therefore the unique right H -module structure on \mathbb{k}^n which makes α a morphism of right H -modules is given by

$$(4.1) \quad (f_0, f_1, \dots, f_{n-1}) \leftarrow x := (f_{n-1}, f_0, f_1, \dots, f_{n-2}).$$

Thus we recover the right H -linear bijection (0.1) as

$$\alpha \circ \phi : \mathbb{k}\langle x \rangle \rightarrow \mathbb{k}^n : c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \mapsto (c_0, c_1, \dots, c_{n-1}).$$

This map gives a bijective correspondence between right ideals of H and right H -submodules of \mathbb{k}^n , with respect to the action \leftarrow . By formula (4.1), these submodules are exactly the cyclic codes of length n .

Note also that

$$(4.2) \quad \langle x^i, x^j \rangle = \lambda[x^j S(x^i)] = \lambda(x^{j-i}) = \delta_{i,j}$$

so that $\langle -, - \rangle : H \otimes H \rightarrow \mathbb{k}$ is symmetric, $\{1, x, x^2, \dots, x^{n-1}\}$ is an orthonormal basis and through (0.1), it corresponds to the scalar product on \mathbb{k}^n . Since the bilinear form is symmetric the left and the right orthogonal coincide.

Let $q \in \mathbb{k}$ be a primitive n -th root of unity.

Note that $\mathbb{k}\langle x \rangle$ identifies with the group algebra $\mathbb{k}G$ over the cyclic group $G := \langle x \rangle$ with x of order n , as above. The existence of a primitive n -th root of unity implies $\text{char}(\mathbb{k}) \nmid n$ so that, for every $t \in \mathbb{Z}$, we can consider

$$e_t := \frac{1}{n} \sum_{i=0}^{n-1} q^{ti} x^i.$$

It is well-known that the e_t 's form a complete set of orthogonal idempotents in $\mathbb{k}G$. This fact is the main tool used in [CGL].

As a consequence $\mathbb{k}\langle x \rangle$ can be regarded as the algebra $\mathbb{k}(\omega, N)$ where $\omega = \text{Id}$ and $N = 1$ with basis $\{e_t \mid 0 \leq t \leq n-1\}$.

For $0 \leq s, t \leq n-1$, we have

$$\langle e_s, e_t \rangle = \left\langle \frac{1}{n} \sum_{i=0}^{n-1} q^{si} x^i, \frac{1}{n} \sum_{j=0}^{n-1} q^{tj} x^j \right\rangle \stackrel{(4.2)}{=} \frac{1}{n^2} \sum_{i=0}^{n-1} q^{(s+t)i} = \frac{1}{n} \delta_{s+t, 0}^{\equiv n}.$$

In particular the form $\langle -, - \rangle$ is as in (2.2), where $\mu(t) := [-t]_n$, $\nu(0) := 0$ and $d_{(s,0)} := \frac{1}{n}$. Here $[t]_n$ denotes the remainder modulo n of t . As a consequence $\langle -, - \rangle$

is monomial with respect to $\mathcal{B} = \{e_s \mid 0 \leq s \leq n-1\}$. Since the form is symmetric, we get that the Nakayama isomorphism γ is the identity. Note also that, since $\mathbb{k}\langle x \rangle$ is commutative, also the Nakayama automorphism η is the identity.

Some direct consequences are then the following.

By Lemma 16 and since $S^{-1} = S$, we have $x \triangleleft h = S(h)x = x \blacktriangleleft h$.

By Theorem 12, we have $\mathcal{L}_{\text{in}}(A_A) = \{N_{s,0} = e_s \mathbb{k} \mid 0 \leq s \leq n-1\}$.

By Theorem 14, we have $N_{s,0}^\perp = \bigoplus_{t \neq \mu(s)} N_{t,0} = \bigoplus_{t \neq n-s} N_{t,0}$.

Remark 23. Consider a cyclic code I and its dual I^\perp . We want to show that I^\perp is, indeed, the classical orthogonal code. Consider the generator polynomial $g(X) = g_0 + g_1X + \cdots + g_{s-1}X^{s-1} + X^s$ for the code I so that $I = \langle g(x) \rangle$. Note that $d := \dim I = n - s$ as a \mathbb{k} -basis for I is given by $x^i g(x)$, $0 \leq i \leq n - s - 1$. Let

$$h(X) := h_0 + h_1X + \cdots + h_{d-1}X^{d-1} + X^d$$

be the unique monic polynomial such that $g(X)h(X) = X^n - 1$, i.e. the parity-check polynomial. Remark that $h(0) = h_0 \neq 0$ and $g(x)h(x) = 0$. By Lemma 16 we have

$$(S(h(x)))^{\perp_L} = \text{Ann}_{H_\bullet}(h(x)) = \langle g(x) \rangle = I.$$

Since $\perp_L = \perp_R$ we get $I^\perp = (S(h(x)))^{\perp\perp} = (S(h(x)))$. Now define

$$g^\perp(X) = h_0^{-1}X^d h(X^{-1}) \in \mathbb{k}[X].$$

We have $\deg g^\perp(X) = d = \deg h(X)$ and $g^\perp(x) = h_0^{-1}x^d S(h(x)) \in I^\perp$ thus $\langle g^\perp(x) \rangle \subseteq I^\perp$. Since $\dim \langle g^\perp(x) \rangle = n - \deg g^\perp(X) = n - d = s = \dim(I^\perp)$, we can conclude

$$I^\perp = \langle S(h(x)) \rangle = \langle g^\perp(x) \rangle$$

so I^\perp is the classical dual code.

4.2. Taft algebra . Let us consider the main example investigated in [CGL]. Let $N \geq 2$ be an integer and let $q \in \mathbb{k}$ be a primitive N -th root of unity. Consider the Taft algebra

$$A = \mathbb{k}\langle g, x \mid g^N = 1, x^N = 0, gx = qxg \rangle.$$

It is a Hopf algebra in a unique way such that

$$\Delta(g) = g \otimes g \quad \text{and} \quad \Delta(x) = g \otimes x + x \otimes 1.$$

Note that A has basis $\{x^n g^a \mid 0 \leq n, a \leq N-1\}$. From the structure above it follows that $S(g) = g^{-1}$ and $S(x) = -g^{-1}x = -q^{-1}xg^{-1}$.

Let $R = \mathbb{k}[x \mid x^N = 0]$ be the subalgebra of A generated by x .

Set $G := \langle g \rangle$ the group of group-like elements in A and set $H := \mathbb{k}G$. For the reader's sake we include in the following lemmas the proofs of main facts that will be used later on.

Lemma 24. *The following equalities hold for every $m \in \mathbb{N}$, $t, a \in \mathbb{Z}$,*

$$(4.3) \quad e_t x^m = x^m e_{t+m}, \quad g^a e_t = e_t g^a = q^{-ta} e_t$$

$$(4.4) \quad S(e_t) = e_{-t}, \quad S(x^m) = (-1)^m q^{-\frac{m(m+1)}{2}} x^m g^{-m}, \quad S^2(x^m) = q^{-m} x^m.$$

A basis of A is given by $\{x^m e_s \mid 0 \leq s, m \leq N-1\}$.

As a consequence $A = \mathbb{k}(\omega, N)$ as in Section 2 where the permutation ω of the indexes of the e_s 's is defined by $\omega(s) := s + 1$ modulo N .

Proof. We compute, for every $m \in \mathbb{N}, t, a \in \mathbb{Z}$,

$$\begin{aligned} e_t x^m &= \frac{1}{N} \sum_{i=0}^{N-1} q^{ti} g^i x^m = \frac{1}{N} \sum_{i=0}^{N-1} q^{(t+m)i} x^m g^i = x^m e_{t+m}, \\ e_t g^a &= \frac{1}{N} \sum_{i=0}^{N-1} q^{ti} g^{i+a} = \frac{1}{N} \sum_{i=0}^{N-1} q^{-ta} q^{t(i+a)} g^{i+a} = q^{-ta} e_t, \\ S(e_t) &= \frac{1}{N} \sum_{a=0}^{N-1} q^{ta} g^{-a} = \frac{1}{N} \sum_{a=0}^{N-1} q^{(-t)(-a)} g^{-a} = e_{-t}, \\ S(x^m) &= S(x)^m = (-g^{-1}x)^m = (-1)^m q^{\frac{-m(m+1)}{2}} x^m g^{-m}, \\ S^2(x^m) &= (S(-g^{-1}x))^m = (-S(x)S(g^{-1}))^m = (g^{-1}xg)^m = q^{-m} x^m. \end{aligned}$$

Since $e_t g^a = g^a e_t$, we get the thesis. These equations guarantee that the set $\{x^m e_s \mid 0 \leq s, m \leq N-1\}$ is a basis of A . \square

Lemma 25. *We have $\int_l(A^*) = \mathbb{k}\lambda$ where*

$$(4.5) \quad \begin{aligned} \lambda(x^m g^a) &= \delta_{m, N-1} \delta_{a, 1}^{\equiv N} \text{ for all } m \in \mathbb{N}, a \in \mathbb{Z}, \\ \lambda(x^m e_s) &= \frac{1}{N} q^s \delta_{m, N-1} \text{ for all } m \in \mathbb{N}, s \in \mathbb{Z}. \end{aligned}$$

Proof. One checks that $\int_l(H^*) = \mathbb{k}\lambda$ where $\lambda(x^m g^a) = \delta_{m, N-1} \delta_{a, 1}$ for $0 \leq m, a \leq N-1$. From this expression for λ one easily deduces the general one for $m \in \mathbb{N}, a \in \mathbb{Z}$. From it we get

$$\begin{aligned} \lambda(x^m e_s) &= \lambda\left(x^m \frac{1}{N} \sum_{i=0}^{N-1} q^{si} g^i\right) = \frac{1}{N} \sum_{i=0}^{N-1} q^{si} \lambda(x^m g^i) \\ &= \frac{1}{N} \sum_{i=0}^{N-1} q^{si} \delta_{m, N-1} \delta_{i, 1} = \frac{1}{N} q^s \delta_{m, N-1}. \end{aligned}$$

\square

We now compute explicitly our bilinear form in two slightly different basis, the first one needed in the proof of Theorem 29.

Lemma 26. *We have*

$$\begin{aligned} \langle e_t x^n, e_s x^m \rangle &= \frac{1}{N} (-1)^n q^{\frac{-(n+2t)(n+1)}{2}} \delta_{s+t, 1}^{\equiv N} \delta_{m+n, N-1}; \\ \langle x^v e_b, x^u e_a \rangle &= \frac{1}{N} (-1)^v q^{\frac{(v-2b)(v+1)}{2}} \delta_{a+b, 0}^{\equiv N} \delta_{u+v, N-1}. \end{aligned}$$

In particular the form $\langle -, - \rangle$ is as in (2.2), where $\mu(t) := [1-t]_N$, $\nu(n) := N-1-n$ and $d_{(s,m)} := \frac{1}{N} (-1)^m q^{\frac{-(m+2s)(m+1)}{2}}$. Here $[t]_N$ denotes the remainder modulo N of t . As a consequence $\langle -, - \rangle$ is monomial with respect to $\mathcal{B} = \{e_s x^m \mid 0 \leq s, m \leq N-1\}$. Moreover the Nakayama isomorphism γ is given by $\gamma(h) = hg$, for every $h \in A$.

Proof. We compute

$$\begin{aligned} e_s x^m S(e_t x^n) &= e_s x^m S(x^n) S(e_t) \\ &= e_s x^m (-1)^n q^{\frac{-n(n+1)}{2}} x^n g^{-n} e_{-t} \end{aligned}$$

$$\begin{aligned}
&= (-1)^n q^{\frac{-n(n+1)}{2}} e_s x^{m+n} g^{-n} e_{-t} \\
&= (-1)^n q^{\frac{-n(n+1)}{2} - tn} e_s x^{m+n} e_{-t} \\
&= (-1)^n q^{\frac{-n(n+1)}{2} - tn} x^{m+n} e_{s+m+n} e_{-t} \\
&= (-1)^n q^{\frac{-n(n+1)}{2} - tn} \delta_{s+t+m+n,0}^{\equiv N} x^{m+n} e_{-t}.
\end{aligned}$$

Thus we have

$$\begin{aligned}
\langle e_t x^n, e_s x^m \rangle &= \lambda [e_s x^m S(e_t x^n)] \\
&= (-1)^n q^{\frac{-n(n+1)}{2} - tn} \delta_{s+t+m+n,0}^{\equiv N} \lambda (x^{m+n} e_{-t}) \\
&= (-1)^n q^{\frac{-n(n+1)}{2} - tn} \frac{1}{N} q^{-t} \delta_{s+t+m+n,0}^{\equiv N} \delta_{m+n,N-1} \\
&= \frac{1}{N} (-1)^n q^{\frac{-(n+2t)(n+1)}{2}} \delta_{s+t+N-1,0}^{\equiv N} \delta_{m+n,N-1} \\
&= \frac{1}{N} (-1)^n q^{\frac{-(n+2t)(n+1)}{2}} \delta_{s+t,1}^{\equiv N} \delta_{m+n,N-1}.
\end{aligned}$$

Moreover

$$\begin{aligned}
\langle x^v e_b, x^u e_a \rangle &= \langle e_{b-v} x^v, e_{a-u} x^u \rangle = \frac{1}{N} (-1)^v q^{\frac{-(v+2b-2v)(v+1)}{2}} \delta_{a-u+b-v,1}^{\equiv N} \delta_{u+v,N-1} \\
&= \frac{1}{N} (-1)^v q^{\frac{(v-2b)(v+1)}{2}} \delta_{a+b,0}^{\equiv N} \delta_{u+v,N-1}.
\end{aligned}$$

By the foregoing, it is clear that $\langle -, - \rangle$ is as in 2.2, where $\mu(t) := [1-t]_N$ and $\nu(n) := N-1-n$.

Thus, by Lemma 13 the form $\langle -, - \rangle$ is monomial with respect to the basis $\mathcal{B} = \{e_s x^m \mid 0 \leq s, m \leq N-1\}$. Moreover, γ is given by

$$\gamma(e_s x^m) = \frac{d_{(s,m)}}{d_{(\mu(s),\nu(m))}} e_{\mu^2(s)} x^{\nu^2(m)} \quad \forall s, m.$$

Since $\mu^2 = \text{Id} = \nu^2$ we obtain $\gamma(e_s x^m) = \frac{d_{(s,m)}}{d_{(\mu(s),\nu(m))}} e_s x^m$. We compute

$$\begin{aligned}
\frac{d_{(s,m)}}{d_{(\mu(s),\nu(m))}} &= \frac{\frac{1}{N} (-1)^m q^{\frac{-(m+2s)(m+1)}{2}}}{\frac{1}{N} (-1)^{N-1-m} q^{\frac{-(N-1-m+2-2s)(N-1-m+1)}{2}}} \\
&= (-1)^{N-1} q^{\frac{-(m+2s)(m+1) + (N-m+1-2s)(N-m)}{2}} \\
&= (-1)^{N-1} q^{\frac{N-2m-2s-2Nm-2Ns+N^2}{2}} = (-1)^{N-1} q^{-\frac{N(N+1)}{2} - (m+s)} \\
&= (-1)^{N-1} (-1)^{N-1} q^{-(m+s)} = q^{-(m+s)}.
\end{aligned}$$

where we note that $x^N - 1 = \prod_{i=0}^{N-1} (x - q^i)$ implies $-1 = (-1)^N q^{\frac{N(N-1)}{2}}$ and hence $q^{-\frac{N(N+1)}{2}} = (-1)^{N-1}$. Thus $\gamma(e_s x^m) = q^{-(m+s)} e_s x^m = q^{-m} e_s g x^m = e_s x^m g$ and hence $\gamma(h) = hg$ for every $h \in H$. \square

Lemma 27. *In the setting of Proposition 10, take V the Taft algebra A with left regular action. Then $\triangleleft = \blacktriangleleft$ and, for every $x \in H, r \in R$, we have $x \triangleleft r = S(r)x$.*

Proof. By Lemma 26, we have that the Nakayama isomorphism γ is given by $\gamma(h) = hg$, for every $h \in A$. Thus γ is left A -linear. By Proposition 10, we have that $\triangleleft = \blacktriangleleft$.

By (3.4), we have that

$$\lambda S(x^n e_t) = \lambda \gamma(x^n e_t) = \lambda(x^n e_t g) \stackrel{(4.3)}{=} q^{-t} \lambda(x^n e_t) \stackrel{(4.5)}{=} \frac{1}{N} \delta_{n, N-1}.$$

We compute

$$\begin{aligned} \lambda(x^u e_s x^m) &= \lambda(e_{s-u} x^u x^m) \\ &= \lambda(e_{s-u} x^{m+u}) \\ &= \frac{1}{N} q^{s+m} \delta_{m+u, N-1} \\ &= q^{-u} \frac{1}{N} q^{s+m+u} \delta_{m+u, N-1} \\ &= q^{-u} \lambda(e_s x^{m+u}) \\ &= \lambda(e_s x^m q^{-u} x^u) \\ &\stackrel{(4.4)}{=} \lambda(e_s x^m S^2(x^u)) \end{aligned}$$

which implies $\lambda(rh) = \lambda(hS^2(r))$ for every $r \in R, h \in A$. As a consequence, if η is the Nakayama automorphism, we get $\eta(r) = S^2(r)$ for every $r \in R$. By Lemma 16 we have $x \triangleleft r = S^{-1}(\eta(r))x = S(r)x$. \square

We are now ready to compute the indecomposable ideals and their orthogonal.

Denote by $\mathcal{L}(M_R)$ the set of right R -submodules of a given right R -module M_R . Let $\mathcal{L}_{\text{in}}(M_R)$ denote the set of right R -submodules which are indecomposable.

Theorem 28. *Consider the Taft Hopf algebra*

$$A = \mathbb{k} \langle g, x \mid g^N = 1, x^N = 0, gx = qxg \rangle$$

and let R be the subalgebra of A generated by x . As in [CGL], for $s, t = 0, \dots, N-1$ set $N_{s,t} := e_s J^t = e_s x^t R$. Then the $N_{s,t}$'s form an irredundant set of representatives of $\mathcal{L}_{\text{in}}(A_A)$ and

$$\mathcal{L}_{\text{in}}(A_A) = \{(1 + rx) N_{s,t} \mid r \in R, 0 \leq s, t \leq N-1\}.$$

Proof. By Lemma 24 A is of the form $\mathbb{k}(\omega, N)$ as in Section 2. Thus the statement follows by Theorem 12. \square

Theorem 29. *Let $a = a(x) \in R$ be an invertible element (we can assume $a(0) = 1$), s, m integers such that $0 \leq s, m \leq N-1$; then we have*

$$\begin{aligned} N_{s,0}^\perp &= \bigoplus_{t \neq N-1-s} N_{t,0}, & N_{s,m}^\perp &= N_{s,0}^\perp \oplus N_{1-s, N-m} \quad \text{and} \\ (aN_{s,m})^\perp &= S(a^{-1}) N_{s,m}^\perp. \end{aligned}$$

Proof. By Lemma 27 and (2.3),(2.4), we have that $(aN_{s,m})^{\perp L} = S(a^{-1}) N_{s,m}^{\perp L}$ and $(aN_{s,m})^{\perp R} = S(a^{-1}) N_{s,m}^{\perp R}$ for every s, m . Note that $\mu(s) = 1-s$ modulo N (so that $\mu^2 = \text{Id}$) and $\nu(m) = N-1-m$ in our case. Thus by Theorem 14, we get $N_{s,m}^{\perp R} = N_{s,m}^{\perp L}$ for every s, m (hence we can use the notation \perp) and the equalities in the present statement holds. \square

4.3. Another example. Consider the commutative Hopf algebra $H = \widehat{D}_n$ of [CDMM, Section 4] for $n = 6$, where D_n denotes the dihedral group of order $2n$ (note that in [CDMM] it is denoted by D_{2n}). Assume that \mathbb{k} contains ζ a primitive 6-th root of 1 and observe that in this case $H \cong (\mathbb{k}D_n)^* \cong \mathbb{k}^{D_n}$ so that H is both semisimple and cosemisimple. Recall that H is given by the generators a, b and relations $a^2 = 1 = b^6$ and $ab = ba$. The element a is group-like while

$$\Delta(b) = b \otimes e_0 b + b^{-1} \otimes e_1 b, \quad \varepsilon(b) = 1, \quad S(b) = e_0 b^{-1} + e_1 b,$$

where

$$e_0 = \frac{1}{2}(1 + a) \quad \text{and} \quad e_1 = \frac{1}{2}(1 - a).$$

We also set

$$f_j = \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} b^i \quad \text{and} \quad e_{i,j} := e_i f_j.$$

Since the subalgebra $\mathbb{k}\langle b \rangle$ of H generated by b is a group algebra (note it is not a subalgebra since is not group-like), as in Subsection (4.1), we get that the f_j 's form a complete set of orthogonal idempotents in $\mathbb{k}\langle b \rangle$. As a consequence, since H is commutative, the $e_{i,j}$'s form a complete set of orthogonal idempotents in H . It is clear that $\{e_{i,j} \mid 0 \leq i \leq 1, 0 \leq j \leq 5\}$ is a generating set whence a basis for H over \mathbb{k} .

In this section, consider as A the Hopf algebra $R\#H$ in [CDMM, Theorem 4.1], where $R := R_q(H, g, \chi)$ where $g := b^3$ (note that g is group-like) and $\chi : H \rightarrow \mathbb{k}$ is defined by $\chi(a) = 1$ and $\chi(b) = -1$. Note that $q = \chi(g) = \chi(b)^3 = -1$ so that $N = o(q) = 2$.

Following [CDMM, Section 2], we get that A is given by the generators x, a, b such that H is a Hopf subalgebra of A and with the further relations $x^2 = 0, hx = x \sum \chi(h_1) h_2$ for every $h \in H$. Taking $h = a, b$ we get $ax = xa$ and $bx = -xb$ respectively. Moreover

$$\Delta(x) = g \otimes x + x \otimes 1 = b^3 \otimes x + x \otimes 1, \quad \varepsilon(x) = 0, \quad S(x) = -gx = xg.$$

By the foregoing $\{x^m e_{i,j} \mid 0 \leq m, i \leq 1, 0 \leq j \leq 5\}$ is a basis for A over \mathbb{k} .

Lemma 30. *The following equality holds for every $m \in \mathbb{N}, i, j \in \mathbb{Z}$*

$$(4.6) \quad e_{i,j} x^m = x^m e_{i,j+3m}, \quad e_{i,j} g^m = g^m e_{i,j} = (-1)^{jm} e_{i,j},$$

$$(4.7) \quad e_{i,j} a^m = a^m e_{i,j} = (-1)^{im} e_{i,j}, \quad e_{i,j} b^m = b^m e_{i,j} = \zeta^{-jm} e_{i,j},$$

$$S(e_{i,j}) = (e_0 f_{-j} + e_1 f_j) e_i = e_{i,(-1)^{i+1}j},$$

$$S(x^m) = x^m g^m,$$

$$S^2(x^m) = (-1)^m x^m.$$

As a consequence $A = \mathbb{k}(\omega, N)$ as in Section 2 where the permutation ω of the indexes of the $e_{i,j}$'s is defined by $\omega((i, j)) := (i, [j + 3]_6)$ where $[t]_6$ denotes the remainder modulo 6 of t .

Proof. Since $e_{i,j} := e_i f_j$ the equalities involving a, b follows analogously to (4.3).

We compute

$$f_j x^m = \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} b^i x^m = x^m \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} (-1)^{im} b^i = x^m \frac{1}{6} \sum_{i=0}^5 \zeta^{(j+3m)i} b^i = x^m f_{j+3m}$$

and hence

$$e_{i,j}x^m = e_i f_j x^m = e_i x^m f_{j+3m} = x^m e_i f_{j+3m} = x^m e_{i,j+3m}.$$

Moreover

$$\begin{aligned} e_{i,j}g^m &= e_i f_j b^{3m} = e_i \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} b^{i+3m} \\ &= \zeta^{-3jm} e_i \frac{1}{6} \sum_{i=0}^5 \zeta^{j(i+3m)} b^{i+3m} = \zeta^{-3jm} e_{i,j} = (-1)^{jm} e_{i,j}. \end{aligned}$$

We have

$$\begin{aligned} S(f_j) &= \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} S(b)^i = \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} (e_0 b^{-i} + e_1 b^i) \\ &= e_0 \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} b^{-i} + e_1 \frac{1}{6} \sum_{i=0}^5 \zeta^{ji} b^i = e_0 f_{-j} + e_1 f_j. \end{aligned}$$

so that $S(e_{i,j}) = (e_0 f_{-j} + e_1 f_j) e_i = e_{i,(-1)^{i+1}j}$. Note that $gx = b^3x = -xb^3 = qgx$ so that the subalgebra of A generated by g and x is a Taft algebra. As a consequence $S(x^m)$ is as in (4.4) i.e.

$$\begin{aligned} S(x^m) &= (-1)^m q^{\frac{-m(m+1)}{2}} x^m g^{-m} = (-1)^m (-1)^{\frac{-m(m+1)}{2}} x^m g^m \\ &= (-1)^{\frac{m(m-1)}{2}} x^m g^m = x^m g^m \end{aligned}$$

as $0 \leq m \leq 1$. We also have

$$S^2(x^m) = S(x^m g^m) = S(g^m) S(x^m) = g^{-m} x^m g^m = (-1)^m x^m$$

where the last equality holds since $0 \leq m \leq 1$ again. \square

Lemma 31. *We have that $\int_l(A^*) = \mathbb{k}\lambda$ where*

$$\begin{aligned} \lambda(x^m a^i b^j) &= \delta_{m,1} \delta_{i,0} \delta_{j,3}^{\equiv 6} \text{ for all } m \in \mathbb{N}, i, j \in \mathbb{Z}, \\ \lambda(x^m e_{i,j}) &= \frac{(-1)^j}{12} \delta_{m,1} \text{ for all } m \in \mathbb{N}, i, j \in \mathbb{Z}. \end{aligned}$$

Proof. We compute

$$\begin{aligned} \Delta(x^m a^i b^j) &= \Delta(x)^m \Delta(a)^i \Delta(b)^j \\ &= \left(\sum_{t=0}^m \binom{m}{t}_{-1} (x \otimes 1)^{m-t} (b^3 \otimes x)^t \right) (a^i \otimes a^i) (b^j \otimes e_0 b^j + b^{-j} \otimes e_1 b^j) \\ &= \sum_{t=0}^m \binom{m}{t}_{-1} (x^{m-t} a^i b^{3t+j} \otimes x^t a^i e_0 b^j) + \sum_{t=0}^m \binom{m}{t}_{-1} (x^{m-t} a^i b^{3t-j} \otimes x^t a^i e_1 b^j) \\ &= \sum_{t=0}^m \binom{m}{t}_{-1} (x^{m-t} a^i b^{3t+j} \otimes x^t e_0 b^j) + (-1)^i \sum_{t=0}^m \binom{m}{t}_{-1} (x^{m-t} a^i b^{3t-j} \otimes x^t e_1 b^j) \end{aligned}$$

Let us check that λ as in the statement is a left integral in A^* . For $0 \leq m, i \leq 1$ and $0 \leq j \leq 5$, we have

$$\begin{aligned}
\sum (x^m a^i b^j)_1 \lambda((x^m a^i b^j)_2) &= \sum_{t=0}^m \binom{m}{t}_{-1} x^{m-t} a^i b^{3t+j} \lambda(x^t e_0 b^j) \\
&\quad + (-1)^i \sum_{t=0}^m \binom{m}{t}_{-1} x^{m-t} a^i b^{3t-j} \lambda(x^t e_1 b^j) \\
&= \sum_{t=0}^m \binom{m}{t}_{-1} x^{m-t} a^i b^{3t+j} \frac{1}{2} \delta_{t,1} \delta_{j,3} \\
&\quad + (-1)^i \sum_{t=0}^m \binom{m}{t}_{-1} x^{m-t} a^i b^{3t-j} \frac{1}{2} \delta_{t,1} \delta_{j,3} \\
&= \frac{1}{2} \binom{m}{1}_{-1} x^{m-1} a^i \delta_{j,3} + \frac{1}{2} (-1)^i \binom{m}{1}_{-1} x^{m-1} a^i \delta_{j,3} \\
&= \frac{1+(-1)^i}{2} \binom{m}{1}_{-1} x^{m-1} a^i \delta_{j,3} \\
&= \frac{1+(-1)^i}{2} \frac{1-(-1)^m}{2} x^{m-1} a^i \delta_{j,3} \\
&\stackrel{i,m \leq 1}{=} \delta_{i,0} \delta_{m,1} x^{m-1} a^i \delta_{j,3} = \delta_{i,0} \delta_{m,1} \delta_{j,3} = \lambda(x^m a^i b^j).
\end{aligned}$$

Hence λ is a left integral in A^* . We have observed that $\int_l(A^*)$ is one-dimensional so that $\int_l(A^*) = \mathbb{k}\lambda$. We compute

$$\begin{aligned}
\lambda(x^m e_{i,j}) &= \lambda(x^m e_i f_j) = \sum_{s=0}^1 \sum_{t=0}^5 \frac{(-1)^s}{12} \zeta^{jt} \lambda(x^m a^s b^t) \\
&= \sum_{s=0}^1 \sum_{t=0}^5 \frac{(-1)^s}{12} \zeta^{jt} \delta_{m,1} \delta_{s,0} \delta_{t,3} = \frac{1}{12} \zeta^{3j} \delta_{m,1} = \frac{(-1)^j}{12} \delta_{m,1}.
\end{aligned}$$

□

Lemma 32. *We have*

$$\langle x^m e_{i,j}, x^n e_{u,v} \rangle = \frac{(-1)^{j(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} \delta_{m+n,1},$$

$$\langle e_{i,j} x^m, e_{u,v} x^n \rangle = \frac{(-1)^{j(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j-3}^{\equiv 6} \delta_{m+n,1}.$$

In particular the form $\langle -, - \rangle$ is as in 2.2, where

$$\mu((i,j)) := \left(i, \left[(-1)^{i+1} j - 3 \right]_6 \right), \quad \nu(m) := 1 - m \quad \text{and} \quad d_{(i,j),m} := \frac{(-1)^{j(m+1)}}{12}.$$

As a consequence the form $\langle -, - \rangle$ is monomial with respect to the basis $\mathcal{B} = \{e_{i,j} x^m \mid 0 \leq s, m \leq N-1\}$. Moreover the Nakayama isomorphism γ is given by $\gamma(h) = hg$, for every $h \in A$.

Proof. We compute

$$\begin{aligned}
x^n e_{u,v} S(x^m e_{i,j}) &= x^n e_{u,v} S(e_{i,j}) S(x^m) \\
&= x^n e_{u,v} e_{i,(-1)^{i+1}j} S(x^m)
\end{aligned}$$

$$\begin{aligned}
&= x^n e_{u,v} e_{i,(-1)^{i+1}j} x^m g^m \\
&= \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} x^n e_{u,v} x^m g^{-m} \\
&= \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} x^n x^m e_{u,v+3m} g^{-m} \\
&= (-1)^{(v+3m)m} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} x^{m+n} e_{u,v+3m}
\end{aligned}$$

Thus we have

$$\begin{aligned}
\langle x^m e_{i,j}, x^n e_{u,v} \rangle &= \lambda(x^n e_{u,v} S(x^m e_{i,j})) \\
&= (-1)^{(v+3m)m} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} \lambda(x^{m+n} e_{u,v+3m}) \\
&= \frac{(-1)^{v+3m}}{12} (-1)^{(v+3m)m} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} \delta_{m+n,1} \\
&= \frac{(-1)^{v(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} \delta_{m+n,1} \\
&= \frac{(-1)^{j(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j}^{\equiv 6} \delta_{m+n,1}.
\end{aligned}$$

We also have

$$\begin{aligned}
\langle e_{i,j} x^m, e_{u,v} x^n \rangle &= \langle x^m e_{i,j+3m}, x^n e_{u,v+3n} \rangle \\
&= \frac{(-1)^{(j+3m)(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v+3n,(-1)^{i+1}(j+3m)}^{\equiv 6} \delta_{m+n,1} \\
&= \frac{(-1)^{j(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v+3n,(-1)^{i+1}j+(-1)^{i+1}3m}^{\equiv 6} \delta_{m+n,1} \\
&= \frac{(-1)^{j(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v+3n,(-1)^{i+1}j-3m}^{\equiv 6} \delta_{m+n,1} \\
&= \frac{(-1)^{j(m+1)}}{12} \delta_{u,i}^{\equiv 2} \delta_{v,(-1)^{i+1}j-3}^{\equiv 6} \delta_{m+n,1}.
\end{aligned}$$

By the foregoing it is clear that as in 2.2, where $\mu((i,j)) := \left(i, \left[(-1)^{i+1}j - 3\right]_6\right)$, $\nu(m) := 1 - m$ and $d_{(i,j,m)} := \frac{(-1)^{j(m+1)}}{12}$.

Thus, by Lemma 13, the form $\langle -, - \rangle$ is monomial with respect to the basis $\mathcal{B} = \{e_{i,j} x^m \mid 0 \leq s, m \leq N - 1\}$. Moreover the Nakayama isomorphism γ is given by $\gamma(e_{i,j} x^m) = \frac{d_{(i,j,m)}}{d_{(\mu((i,j)), \nu(m))}} e_{\mu^2(i,j)} x^{\nu^2(m)}$ for all i, j, m . Since $\mu^2 = \text{Id} = \nu^2$, we obtain $\gamma(e_{i,j} x^m) = \frac{d_{(i,j,m)}}{d_{(\mu((i,j)), \nu(m))}} e_{i,j} x^m$. We compute

$$\frac{d_{(i,j,m)}}{d_{(\mu((i,j)), \nu(m))}} = \frac{\frac{(-1)^{j(m+1)}}{12}}{\frac{(-1)^{((-1)^{i+1}j-3)(1-m+1)}}{12}} = \frac{(-1)^{j(m+1)+(-1)^{i+1}jm-3m}}{12} = (-1)^{j+m}$$

Thus

$$\gamma(e_{i,j} x^m) = \frac{d_{(i,j,m)}}{d_{(\mu((i,j)), \nu(m))}} e_{i,j} x^m = (-1)^{j+m} e_{i,j} x^m = (-1)^m e_{i,j} g x^m = e_{i,j} x^m g$$

and hence $\gamma(h) = hg$ for every $h \in H$. \square

Lemma 33. *In the setting of Proposition 10, take V the algebra A as above with left regular action. Then $\triangleleft = \blacktriangleleft$ and, for every $x \in H, r \in R$, we have $x \triangleleft r = S(r)x$.*

Proof. By Lemma 32, we have that the map γ is given by $\gamma(h) = hg$ for every $h \in H$. Thus γ is left A -linear. By Proposition 10, we have $\triangleleft = \blacktriangleleft$. \square

By (3.4) we have

$$\begin{aligned} \lambda S(x^m e_{s,t}) &= \lambda \gamma(x^m e_{s,t}) = \lambda(x^m e_{s,t} g) \\ &= (-1)^t \lambda(x^m e_{s,t}) = (-1)^t \frac{(-1)^t}{12} \delta_{m,1} = \frac{1}{12} \delta_{m,1}. \end{aligned}$$

We compute

$$\begin{aligned} \lambda(x^u x^m e_{s,t}) &= \lambda(x^{u+m} e_{s,t}) = \frac{(-1)^t}{12} \delta_{u+m,1} \\ &= (-1)^u \frac{(-1)^{t+3u}}{12} \delta_{u+m,1} = (-1)^u \lambda(x^{u+m} e_{s,t+3u}) \\ &= (-1)^u \lambda(x^m x^u e_{s,t+3u}) = \lambda(x^m e_{s,t} (-1)^u x^u) = \lambda(x^m e_{s,t} S^2(x^u)) \end{aligned}$$

which implies $\lambda(rh) = \lambda(hS^2(r))$ for every $r \in R, h \in A$. As a consequence, we get $x \triangleleft r = S(r)x$ as in the proof of Lemma 27.

We are now able to compute the indecomposable ideals and their orthogonals.

Theorem 34. *Consider the Hopf algebra*

$$A = \mathbb{k} \langle a, b, x \mid a^2 = 1 = b^6, x^2 = 0, ab = ba, ax = xa, bx = -xb \rangle$$

and let R be the subalgebra of A generated by x . For $0 \leq m, s \leq 1, 0 \leq t \leq 5$ set $N_{s,t,m} := e_{s,t} x^m R$. Then the $N_{s,t,m}$'s form an irredundant set of representatives of $\mathcal{L}(A_A)$ and

$$\mathcal{L}_{\text{in}}(A_A) = \{(1 + rx) N_{s,t,m} \mid r \in R, 0 \leq m, s \leq 1, 0 \leq t \leq 5\}.$$

Proof. By Lemma 24 A is of the form $\mathbb{k}(\omega, N)$ as in Section 2. Thus the statement follows by Theorem 12. \square

Theorem 35. *Let $a = a(x) \in R$ be an invertible element (we can assume $a(0) = 1$), s, t, m integers such that $0 \leq m, s \leq 1, 0 \leq t \leq 5$; then we have*

$$\begin{aligned} N_{s,t,0}^\perp &= \left(\bigoplus_j N_{1-s,j,0} \right) \oplus \left(\bigoplus_{j \not\equiv_6 (-1)^{s+1}t+3} N_{s,j,0} \right), \\ N_{s,t,m}^\perp &= N_{s,t,0}^\perp \oplus N_{s,(-1)^{s+1}t+3,2-m}, \\ (aN_{s,t,m})^\perp &= S(a^{-1}) N_{s,t,m}^\perp. \end{aligned}$$

Proof. By Lemma 33 and (2.3),(2.4), we have that $(aN_{s,t,m})^{\perp L} = S(a^{-1}) N_{s,t,m}^{\perp L}$ and $(aN_{s,t,m})^{\perp R} = S(a^{-1}) N_{s,t,m}^{\perp R}$ for every s, t, m . We know that $\mu((i, j)) := \left(i, \left[(-1)^{i+1} j - 3 \right]_6 \right) = \left(i, \left[(-1)^{i+1} j + 3 \right]_6 \right)$ (so that $\mu^2 = \text{Id}$) and $\nu(m) := 1 - m$ in our case. Thus by Theorem 14, we get $N_{s,t,m}^{\perp R} = N_{s,t,m}^{\perp L}$ for every s, t, m (hence we can use the notation \perp) and the equalities in the present statement holds as $(i, j) \neq \mu((s, t)) = \left(s, \left[(-1)^{s+1} t + 3 \right]_6 \right)$ means either $i = 1 - s$ or $j \not\equiv_6 (-1)^{s+1} t + 3$. \square

REFERENCES

- [Ab] E. Abe, *Hopf algebras*. Translated from the Japanese by Hisae Kinoshita and Hiroko Tanaka. Cambridge Tracts in Mathematics, **74**. Cambridge University Press, Cambridge-New York, 1980.
- [CDMM] C. Călinescu, S. Dăscălescu, A. Masuoka, C. Menini, *Quantum lines over non-cocommutative cosemisimple Hopf algebras*. J. Algebra **273** (2004), no. 2, 753–779.
- [CGL] J. Cuadra, J. M. García-Rubira, J. A. López-Ramos, *Determining all indecomposable codes over some Hopf algebras*. J. Comput. Appl. Math. **235** (2011), no. 7, 1833–1839.
- [CVZ] H. Chen, F. Van Oystaeyen, Y. Zhang, *The Green rings of Taft algebras*. Proc. Amer. Math. Soc. **142** (2014), no. 3, 765–775.
- [DNR] S. Dăscălescu, C. Năstăsescu, Ş. Raianu, *Hopf algebras. An introduction*. Monographs and Textbooks in Pure and Applied Mathematics, **235**. Marcel Dekker, Inc., New York, 2001.
- [Fa] A. Facchini, *Module theory. Endomorphism rings and direct sum decompositions in some classes of modules*. Progress in Mathematics, **167**. Birkhäuser Verlag, Basel, 1998.
- [Ja] N. Jacobson, *Basic algebra I*. 2nd ed., W. H. Freeman and Company, New York, 1985.
- [LR] R. G. Larson, D. E. Radford, *Finite-dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple*. J. Algebra **117** (1988), no. 2, 267–289.
- [Ra] D. E. Radford, *Hopf algebras*. Series on Knots and Everything, **49**. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.
- [Sw] M. E. Sweedler, *Hopf algebras*. Mathematics Lecture Note Series W. A. Benjamin, Inc., New York 1969.
- [Wo] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*. Amer. J. Math. **121** (1999), no. 3, 555–575.

UNIVERSITY OF TURIN, DEPARTMENT OF MATHEMATICS “G. PEANO”, VIA CARLO ALBERTO 10, I-10123 TORINO, ITALY.

E-mail address: alessandro.ardizzoni@unito.it

URL: sites.google.com/site/aleardizzonihome

UNIVERSITY OF FERRARA, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, VIA MACHIAVELLI 30, FERRARA, I-44121, ITALY.

E-mail address: f.stumbo@unife.it