Codes as Ideals Over Some Pointed Hopf Algebras

J. Cuadra, J.M. García-Rubira and J.A. López-Ramos

***Abstract*— We give a Decomposition Theorem for a family of Hopf algebras containing the well-know family of Taft Hopf algebras. Therefore, those indecomposable codes over this family of algebras (cf. [4]) is an indecomposable code over the studied case. We use properties of Hopf algebras to show that dual (in the module sense) of an ideal code is again an ideal code.**

I. INTRODUCTION

Cyclic and Reed-Muller codes can be seen as ideals in the group ring $\mathbb{K}G$, where $\mathbb{K}$ is a finite field and G is a finite cyclic group, (cf. [1]). Since its mathematical foundations in Hamming's and McWilliams' works (see [3] and [5]), main results are the Extension Theorem and the so called McWilliams' Identities, both of them for vector spaces over finite fields. When trying to extend the theory of linear codes over finite rings, it is necessary to take into account that Wood ([8]) remarked the suitability of Frobenius rings. He gave an Extension Theorem and a version of MacWilliams' Identities for the case of finite Frobenius rings. In fact the importance of Frobenius rings has been completely remarked also by Wood in [9] where he states that a finite Frobenius ring is characterized by the fact of allowing the Extension Theorem for linear codes. Other authors ([2]) have studied linear codes over finite quasi-Frobenius modules.

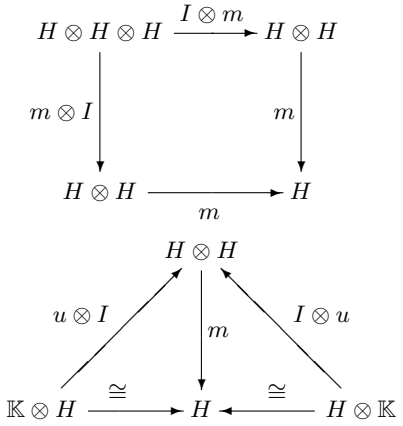
Finite-dimensional Hopf algebras are a generalization of group algebras and an example of Frobenius rings, those stated by Wood as a natural setting to study a theory of linear codes. This is set in [4] where the authors characterizes all indecomposable codes for a family of non-semisimple Hopf algebras: Taft Hopf algebras. Our aim in this work is to extend this characterization to a larger family of such Hopf algebras: Radford Hopf algebras. We will show a Decomposition Theorem for this new family of Hopf algebras where the family studied in [4] appears as one of the factors. Then we will only have to study codes over the factors different from those previously studied. We will show that duals (in the module theory sense) of ideal codes are again ideal codes, extending results given in [4]. We will calculate their main parameters and show that they are nothing but concatenation of cyclic codes. We will also remark that classical operations over some cyclic codes will allow us to get an ideal code over some Hopf algebras.

This work was partially supported by projects MTM2008-03339 from MICINN, P07-FQM03128 from Junta de Andalucía and TEC2009-13763-C02-02

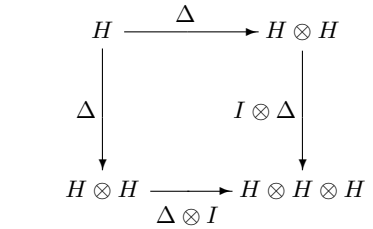
All authors are with the Department of Algebra and Mathematical Analysis, University of Almeria, E04120, Almería, Spain. Emails: jcdiaz@ual.es, jgr836@ual.es, jlopez@ual.es

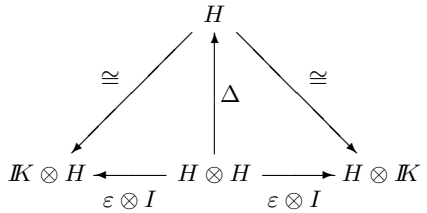
A. Hopf algebras

For prerequisites on Hopf algebras we refer the reader to [6]. However, let us introduce the concept of Hopf algebra. Let H be a $\mathbb{K}$-vector space together with maps $m : H \otimes H \to H$ and $u : \mathbb{K} \to H$, the multiplication and unit maps respectively. Here $\otimes$ denotes the tensor product over $\mathbb{K}$. Then the associativity and the identity element property of a $\mathbb{K}$-algebra H can be described in terms of commutativity of the following two diagrams:



Here I is the identity map on H. If we dualize these diagrams we get the definition of coalgebra structure. So let $\Delta : H \to H \otimes H$ and $\varepsilon : H \to \mathbb{K}$ be two maps called comultiplication and counit respectively. H is a *coalgebra* if the following two diagrams commute:





It is said that both structures on H are compatible if Δ and ε are algebra maps. In this case, H is called a *bialgebra*. Now we are in a position to recall the definition of a Hopf algebra. Using Sweedler's notation we express $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} \in H \otimes H$ for any $h \in H$. The convolution product of two linear maps $f, g : H \to H$ is defined by $(f * g)(h) = \sum_{(h)} f(h_{(1)})g(h_{(2)})$. A *Hopf algebra* is a bialgebra together with a $\mathbb{K}$-linear map $S : H \to H$ such that

ISBN 978-963-311-370-7

it is the inverse of the identity map $I : H \to H$ for the convolution product. The easiest example of Hopf algebra is the group algebra $\mathbb{K}G$ for a group G. The comultiplication, counit and antipode are given by:

$$\Delta(g) = g \otimes g, \quad \varepsilon(g) = 1, \quad S(g) = g^{-1},$$

for all $g \in G$. From a representation theoretic's point of view, the counit allows to consider $\mathbb{K}$ as a representation of H, the comultiplication permits to form the tensor product of two representations and the antipode allows to take dual representations.

B. Two related families of Hopf algebras

Let $n > 1$ be an integer and let $\mathbb{K}$ be a field containing a primitive n-th root of unity ω ($char(\mathbb{K}) \nmid n$). The free algebra $\mathcal{H} = \mathbb{K}\langle g, x\rangle$ over the non-commutative indeterminates g and x is a bialgebra with comultiplication and counit given by $\Delta(g) = g \otimes g$, $\Delta(x) = x \otimes g + 1 \otimes x$ and $\varepsilon(g) = 1$, $\varepsilon(x) = 0$ respectively. Let us consider the ideal Γ of $\mathcal{H}$ generated by $g^n - 1$, $xg - \omega gx$ and x^n. The quotient algebra, that we will denote by T_n, is a Hopf algebra (known as Taft Hopf algebra) with antipode given by $S(g) = g^{-1}$ and $S(x) = -xg^{-1}$. Observe that $\{g^i x^j : \ 0 \leq i, j, < n\}$ is a basis for T_n and so $dim(T_n) = n^2$. Indecomposable ideal codes over T_n where studied in [4].

Now let $p > 1$ be a prime number and assume $char(\mathbb{K}) \neq p$. Let Γ' be the ideal of $\mathcal{H}$ generated by $g^{pn} - 1$, $xg - \omega gx$, and $x^n - (g^n - 1)$ and let $A_p = \mathcal{H}/\Gamma'$. A_p is also a Hopf algebra with antipode given by $S(g) = g^{-1}$, $S(x) = -xg^{-1}$ (as above, now g and x denote the corresponding projections of the original elements g and x in $\mathcal{H}$). We easily see that the set $B = \{g^i x^j : 0 \leq i < pn, \ 0 \leq j < n\}$ is a basis for A_p and thus $dim(A_p) = pn^2$.

This family of Hopf algebras was introduced by Radford in [7] as an example of Hopf algebra H whose Jacobson radical $J(H)$ is not a Hopf ideal, i.e., the semisimple quotient algebra $H/J(H)$ does not admit a Hopf algebra structure making the canonical projection into a Hopf algebra map. We will refer to A_p as Radford Hopf algebra.

II. A Decomposition Theorem

We claim that $b = \sum_{k=0}^{p-1} g^{kn}$ is a central element in A_p. To show this we only have to prove the commutativity with the elements of the basis B.

$$\begin{aligned}(g^i x^j)b &= \textstyle\sum_{k=0}^{p-1} g^i x^j g^{kn} = \sum_{k=0}^{p-1} g^i \omega^{knj} g^{kn} x^j = \sum_{k=0}^{p-1} g^{kn} g^i x^k \\ &= b(g^i x^k)\end{aligned}$$

since ω is a n-th root of unit. Consider $e = \frac{1}{p} b$. By the above, e is a central element in A_p. The following calculation shows that e is idempotent:

$$e^2 = \frac{1}{p^2}\left(\sum_{i,j=0}^{p-1} (g^n)^{i+j}\right) = \frac{1}{p^2}\left(\sum_{r=0}^{p-1} p(g^n)^r\right) = e$$

Therefore we get that $A_p = A_p e \oplus A_p(1 - e)$ as algebras.

Lemma 2.1: $A_p e \cong T_n$ as algebras.

Proof. Consider the set $\{g^i x^j e : 0 \leq i < pn, \ 0 \leq j < n\} \subset A_p$. Then, for any $0 \leq j < n$ we have:

$$(g^n x^j)e = (\omega^{-nj} x^j g^n)e = x^j \frac{1}{p}\left(\sum_{i=0}^{p-1} g^{n(i+1)}\right) = x^j e.$$

Hence, for $0 \leq i < n$ it is $(g^{n+i} x^j)e = (g^i x^j)e$. This yields that $\{g^i x^j e : 0 \leq i, j < n\}$ is a generating set of $A_p e$. It is easy to see that it is also linearly independent and thus a basis of $A_p e$. Therefore $dim(A_p e) = n^2$. Putting $g' = ge$ and $x' = xe$ we get that $g'^n = (ge)^n = g^n e = e, x'^n = (xe)^n = x^n e = (g^n - 1)e = 0$ and, finally, $x'g' = (xe)(ge) = xge^2 = \omega(gx)e^2 = \omega(ge)(xe) = \omega g' x'$. Hence $A_p e$ is isomorphic to T_n as an algebra.

Theorem 2.2: Assume that K contains a primitive p-th root of unity θ and an n-th root of θ. Then

$$A_p \cong T_n \oplus M_n(\mathbb{K}) \oplus \overset{(p-1)}{\cdots} \oplus M_n(\mathbb{K})$$

as algebras.

Proof. Setting $e' = 1 - e$, we have that $A_p = A_p e \oplus A_p e'$ as algebras. By the previous lemma, $A_p e \cong T_n$. It is sufficient to show that

$$A_p e' \cong M_n(\mathbb{K}) \oplus \overset{(p-1)}{\cdots} \oplus M_n(\mathbb{K}).$$

Observe that $dim(A_p e') = dim(A_p) - dim(A_p e) = pn^2 - n^2 = (p-1)n^2$.

For $i = 1, ..., p-1$ consider

$$f_i = \frac{1}{p}\left(\sum_{j=0}^{p-1} \theta^{ij} g^{nj}\right) e'.$$

Let us show that $\{f_i\}_{i=1}^{p-1}$ is a complete set of orthogonal central idempotents in $A_p e'$. We first prove that they are orthogonal idempotents and that $\sum_{i=1}^{p-1} f_i = e'$.

$$\begin{aligned} f_i f_j &= \tfrac{1}{p^2}\left(\textstyle\sum_{u,v=0}^{p-1} \theta^{iu}\theta^{jv} g^{n(u+v)}\right) e' \\ &= \tfrac{1}{p^2}\left(\textstyle\sum_{r=0}^{p-1}\left(\sum_{u=0}^{p-1} \theta^{iu}\theta^{j(p-u+r)}\right) g^{n(u+p-u+r)}\right) e' \\ &= \tfrac{1}{p^2}\left(\textstyle\sum_{r=0}^{p-1} \theta^{jr}\left(\sum_{u=0}^{p-1} \theta^{(i-j)u}\right) g^{nr}\right) e' \end{aligned}$$

If $j = i$, then $\theta^{i-j} = 1$ and hence

$$f_i f_i = \frac{1}{p^2}\left(p\sum_{r=0}^{p-1} \theta^{ir} g^{nr}\right) e' = f_i$$

If $j \neq i$, then $\sum_{u=0}^{p-1} \theta^{(i-j)u} = 0$ and so $f_i f_j = f_j f_i = 0$.

Moreover, we have that

$$\begin{aligned} \textstyle\sum_{i=1}^{p-1} f_i &= \tfrac{1}{p}\left(\textstyle\sum_{i=1}^{p-1}\sum_{j=0}^{p-1} \theta^{ij} g^{nj}\right) e' \\ &= \tfrac{1}{p}\left(\textstyle\sum_{j=0}^{p-1}\left(\sum_{i=1}^{p-1} \theta^{ij}\right) g^{nj}\right) e' \\ &= \tfrac{1}{p}\left((p-1) - \textstyle\sum_{j=1}^{p-1} g^{nj}\right) e' \\ &= \tfrac{1}{p}(p - e)\, e' \\ &= e' \end{aligned}$$

where we have used that $\sum_{i=0}^{p-1} \theta^{ij} = p\delta_{j,0}$ (being $\delta_{j,0}$ the Kronecker's symbol) and $ee' = 0$.

To check that each f_i is central in $A_p e'$ notice that $x^l g^{nj} = \omega^{nlj} g^{nj} x^l = g^{nj} x^l$. Then, for $k \in \{0, ..., pn-1\}$ and $l \in \{0, .., n-1\}$ we have:

$$\begin{aligned} (g^k x^l e')f_i &= (g^k x^l)f_i = \tfrac{1}{p}\left(\textstyle\sum_{j=0}^{p-1} \theta^{ij} g^k x^l g^{nj}\right) e' \\ &= \tfrac{1}{p}\left(\textstyle\sum_{j=0}^{p-1} \theta^{ij} g^{nj}\right) e' e' g^k x^l \\ &= f_i e' g^k x^l \\ &= f_i(g^k x^j e') \end{aligned}$$

Consider the Pierce decomposition in $A_p e'$ corresponding to the set $\{f_i : i = 1, ..., p-1\}$, that is,

$$A_p e' = \oplus_{i=1}^{p-1}(A_p e')f_i = \oplus_{i=1}^{p-1} A_p f_i.$$

We will show now that $A_pf_i \cong M_n(\mathbb{K})$ as algebras for every $i = 1, ..., p-1$. Note that

$$\begin{aligned} g^n f_i &= \tfrac{1}{p}\left(\sum_{j=0}^{p-1}\theta^{ij}g^{n(j+1)}\right)e' = \tfrac{1}{p}\left(\sum_{k=0}^{p-1}\theta^{i(k-1)}g^{nk}\right)e' \\ &= \theta^{p-i}f_i \end{aligned}$$

and so, we get that

$$g^n x^j f_i = \omega^{nj} x^j g^n f_i = \theta^{p-i} x^j f_i.$$

From here it follows that $B_i = \{g^k x^j f_i : 0 \le j, k < n\}$ is a generating set for A_pf_i. Then $B = \cup_{i=1}^{p-1} B_i$ is a generating set for $A_pe' = \oplus_{i=1}^{p-1} A_pf_i$. Since $|B| = dim(A_pe') = (p-1)n^2$, we get that B is linearly independent and a basis of A_pe'. As a consequence, B_i is a basis of A_pf_i and $dim(A_pf_i) = n^2$. Moreover, writing $\alpha_i = \theta^{p-i}$ and $\beta_i = \theta^{p-i} - 1$ we get:

$$\begin{aligned} &(gf_i)^n = g^n f_i = \theta^{p-i} f_i = \alpha_i f_i \\ &(xf_i)^n = x^n f_i = (g^n - 1) f_i = (\theta^{p-i} - 1) f_i = \beta_i f_i \\ &(xf_i)(gf_i) = (xg) f_i f_i = (\omega gx) f_i f_i = \omega (gf_i)(xf_i) \end{aligned}$$

Let $\lambda \in \mathbb{K}$ be the n-th root of θ given by hypothesis. We claim that A_pf_i is isomorphic to $M_n(\mathbb{K})$ through the map given by:

$$gf_i \longrightarrow M = \lambda^{p-i} diag(1, \omega, \ldots, \omega^{n-1})$$

$$xf_i \longrightarrow N = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \beta_i & 0 & 0 & \cdots & 0 \end{pmatrix}$$

By direct computations one may check that $M^n = \alpha_i I_n, N^n = \beta_i I_n$ and $NM = \omega MN$, showing so that the above map is an algebra isomorphism. This finishes the proof.

III. Duals of the indecomposable Radford codes

By Theorem 2.2 we have an algebra isomorphism

$$A_p \cong T_n \oplus M_n(\mathbb{K}) \oplus \overset{(p-1)}{\cdots} \oplus M_n(\mathbb{K}).$$

Now if we want to determine all indecomposable codes in A_p we have to consider, on one hand, those in T_n, and on the other, those corresponding to the matrix blocks. Indecomposable codes in T_n are discussed in [4]. We include them here for completeness.

A. Indecomposable codes in T_n

Recall that $T_n = \mathbb{K}\langle g, x : g^n = 1,\ x^n = 0,\ xg = \omega gx\rangle$, $dim(T_n) = n^2$ and a basis for T_n is $B = \{g^i x^j : 0 \le i, j, < n\}$. The Jacobson radical $J(T_n)$ of T_n coincides with the ideal generated by x. Then the semisimple quotient algebra $\overline{T}_n = T_n/J(T_n)$ is isomorphic to the group algebra $\mathbb{K}\mathbb{Z}_n$ via the map sending $g \mapsto g$ and $x \mapsto 0$. The primitive idempotents of $\mathbb{K}\mathbb{Z}_n$,

$$e_l = \frac{1}{n}\left(\sum_{i=0}^{n-1}\omega^{li}g^i\right), \qquad 0 \le l < n,$$

will give us the complete set $\{S_l : 0 \le l < n\}$ of isomorphism classes of simple T_n-modules. Writing $u_l = e_l$ and $S_l = \overline{T}_n e_l = \mathbb{K}u_l$ we get that $g \cdot u_l = \omega^{-l} u_l$ and $x \cdot u_l = 0$. By lifting this set of orthogonal primitive idempotents to one of T_n we will obtain the set of isomorphism classes of projective indecomposable modules. Each of them is represented by the projective cover P_l of S_l. Observe that e_l, viewed as an element in T_n, provides a desired lifted idempotent of e_l. Therefore the above set is indeed a complete set of primitive orthogonal idempotents in T_n. Then $P_l = He_l$ is the projective cover of the simple $\overline{T}_n e_l$. Setting $v_i = x^i e_l$ for $i = 0, .., n-1$, the set $\{v_0, ..., v_{n-1}\}$ is a basis of P_l. The action of T_n on these elements is given by:

$$\begin{aligned} g \cdot v_i &= \omega^{-(l+i)} v_i \\ x \cdot v_i &= v_{i+1}, \qquad i = 0, \cdots, n-2, \\ x \cdot v_{n-1} &= 0 \end{aligned} \tag{1}$$

The antipode S of T_n allows us to equip the dual space P_l^* of P_l with a module structure in the following way: for $\varphi \in P_l^*, v \in P_l$ and $h \in T_n$, the action is $\langle h \cdot \varphi, v\rangle = \langle \varphi, S(h) \cdot v\rangle$. Here $\langle -, -\rangle : P_l^* \times P_l \to k$ is the evaluation map. Since T_n is a Frobenius algebra, P_l^* must be isomorphic to P_i for certain $i \in \{0, ..., n-1\}$. The next result tells us to which one:

Theorem 3.1: P_l^* is isomorphic to $P_{-(l-1)}$ as a module.

Proof. Let $\{v_0^*, \cdots, v_{n-1}^*\} \subset P_l$ be the dual basis of the basis of P_l given before. That is, $v_i^*(v_j) = \delta_{ij}$ for $i, j = 0, ..., n-1$. To compute the action of g and x on the elements of this dual basis, we need the following facts:

$$\begin{aligned} g^{-1} \cdot v_j &= g^{n-1} \cdot v_j \\ &= \omega^{-(n-1)(j+l)} v_j \\ &= \omega^{j+l} v_j, \qquad j = 0, ..., n-1; \end{aligned}$$

$$\begin{aligned} (-xg^{-1}) \cdot v_j &= -x \cdot (\omega^{j+l} v_j) \\ &= -\omega^{j+l} x \cdot v_j \\ &= -\omega^{j+l} v_{j+1}, \quad j = 0, ..., n-2; \end{aligned}$$

$$\begin{aligned} (-xg^{-1}) \cdot v_{n-1} &= -x \cdot (\omega^{n-1+l} v_{n-1}) \\ &= -\omega^{n-1+l} x \cdot v_{n-1} \\ &= 0 \end{aligned}$$

Then we have:

$$\begin{aligned} \langle g \cdot v_i^*, v_j\rangle &= \langle v_i^*, S(g) \cdot v_j\rangle \\ &= \langle v_i^*, g^{-1} \cdot v_j\rangle \\ &= \langle v_i^*, \omega^{j+l} v_j\rangle \\ &= \omega^{j+l}\langle v_i^*, v_j\rangle \\ &= \omega^{j+l}\delta_{ij}, \qquad j = 0, \cdots n-1, \end{aligned}$$

so $g \cdot v_i^* = \omega^{i+l} v_i^*$. On the other hand,

$$\begin{aligned} \langle x \cdot v_i^*, v_j\rangle &= \langle v_i^*, S(x) \cdot v_j\rangle \\ &= \langle v_i^*, (-xg^{-1}) \cdot v_j\rangle \\ &= -\langle v_i^*, \omega^{j+l} v_{j+1}\rangle \\ &= -\omega^{j+l}\langle v_i^*, v_{j+1}\rangle \\ &= -\omega^{j+l}\delta_{ij+1}, \qquad j = 0, \cdots n-2, \end{aligned}$$

and analogously, $\langle x \cdot v_i^*, v_{n-1}\rangle = 0$. Hence $x \cdot v_0^* = 0$ and $x \cdot v_i^* = -\omega^{i-1+l} v_{i-1}^*$ for $i = 1, \cdots, n-1$.

For $i = 0, ..., n-1$ set $u_i = x^i \cdot v_{n-1}^*$. Then,

$$\begin{aligned} g \cdot u_i &= g \cdot (x^i \cdot v_{n-1}^*) \\ &= \omega^{-i} x^i \cdot (g \cdot v_{n-1}^*) \\ &= x^i \cdot (\omega^{n-(i+1)+l} v_{n-1}^*) \\ &= \omega^{-i+l-1} x^i \cdot v_{n-1}^* \\ &= \omega^{-(i-(l-1))} u_i \end{aligned}$$

The set $\{u_0, ..., u_{n-1}\}$ is linearly independent because its elements are eigenvectors attached to different eigenvalues. Consequently, it is a basis of P_l^*. We next compute the action of x on each of these vectors:

$$\begin{aligned} x \cdot u_i &= x \cdot (x^i \cdot v_{n-1}^*) \\ &= x^{i+1} \cdot v_{n-1}^* \\ &= u_{i+1}, \qquad i = 0, \cdots, n-2, \\ x \cdot u_{n-1} &= x \cdot (x^{n-1} \cdot v_{n-1}^*) \\ &= x^n \cdot v_{n-1}^* \\ &= 0 \end{aligned}$$

Thus we get that $P_l^* \cong P_{-(l-1)}$ through the isomorphism $u_i \to v_i$ and we are done.

In the sequel we simply denote the Jacobson radical $J(T_n)$ by J. As T_n is a serial algebra, the only submodules of P_l are $N_{l,j} = J^j P_l$ for $j = 0, ..., n$. Taking into account (1), a basis for $N_{l,j}$ is $\{v_j, ..., v_{n-1}\}$ and so $dim(N_{l,j}) = n - j$. Then

$$\{0\} = N_{l,n} \subset N_{l,n-1} \subset \cdots \subset N_{l,2} \subset N_{l,1} \subset N_{l,0} = P_l$$

is a composition series of P_l and the composition factors are $N_{l,k}/N_{l,k+1} \cong S_{l+k}$ for $k = 0, ..., n-1$. We claim that the quotient module $P_l/N_{l,j}$ is isomorphic to $N_{l+j,n-j}$. For, denote by $[v]$ the class of $v \in P_l$. Then $\{[v_0], ..., [v_{j-1}]\}$ is a basis of $P_l/N_{l,j}$. The module structure is given by:

$$\begin{aligned} g \cdot [v_i] &= [g \cdot v_i] \\ &= [\omega^{-(i+l)} v_i] \\ &= \omega^{-(i+l)} [v_i], \qquad i = 0, ..., j-1, \\ x \cdot [v_i] &= [x \cdot v_i] \\ &= [v_{i+1}], \qquad i = 0, ..., j-2, \\ x \cdot [v_{j-1}] &= [x \cdot v_{j-1}] \\ &= [v_j] \\ &= [0] \end{aligned}$$

Hence the map $N_{l+j,n-j} \to P_l/N_{l,j}, v_{n-i} \mapsto [v_{j-i}]$ for $i = 1, ..., j$ is an isomorphism of modules.

We are now in a position to compute the dual of $N_{l,j}$:

Corollary 3.2: $N_{l,j}^* \cong N_{-(l+j-1),j}$ as modules.

Proof. Since $N_{l,j}$ is embedded into P_l, we have that that $N_{l,j}^*$ is a quotient of P_l^*. By the previous theorem, $P_l^* \cong P_{-(l-1)}$. So, $N_{l,j}^*$ is a quotient module of $P_{-(l-1)}$ of dimension $n - j$. By the preceding paragraph it must be $N_{l,j}^* \cong N_{-(l+j-1),j}$. This ends the proof.

B. Indecomposable codes in the matrix blocks

By Theorem 2.2,

$$A_p \cong T_n \oplus M_n(\mathbb{K}) \oplus \overset{(p-1)}{\cdots} \oplus M_n(\mathbb{K}).$$

By Wedderburn Structure Theorem, each block $M_n(\mathbb{K})$ has a unique isomorphism type of simple (left) module. The unique (up to isomorphism) simple module is $S = k^n$ where $M_n(\mathbb{K})$ acts on S by the usual matrix-vector multiplication. This simple module becomes a simple A_p-module when A_p acts on it through the canonical projection of A_p onto the block $M_n(\mathbb{K})$. This gives rise to $p-1$ non-isomorphic simple (left) A_p-modules S_j, $j = 1, ..., p-1$. As a vector space S_j is k^n. Let $\{v_0, ..., v_{n-1}\}$ be the basis of S_j where v_i is the vector with 1 in the position $n - i$ and zero elsewhere. Taking into account the isomorphism described in the proof of Theorem 2.2, the action of A_p on this basis is given as follows:

$$\begin{aligned} g \cdot v_i &= \lambda_j \omega^{-i} v_i, \qquad i = 0, ..., n-1, \\ x \cdot v_i &= v_{i+1}, \qquad i = 0, ..., n-2, \\ x \cdot v_{n-1} &= (\theta^{p-j} - 1) v_0 \end{aligned} \tag{2}$$

Recall that θ is a primitive p-th root of unity and λ_j is an n-root of θ^{p-j}. If λ is an n-th root of θ we may take $\lambda_j = \lambda^{p-j}$.

The next result identifies the dual of S_j:

Theorem 3.3: $S_j^* \cong S_{p-j}$ as A_p-modules.

Proof. We start by distinguishing two cases: $p = 2$ and $p \neq 2$. If $p = 2$, then $A_p \cong T_n \oplus M_n(\mathbb{K})$ and S_1 is the unique simple A_p-module of dimension n. The simple A_p-modules arising from T_n are 1-dimensional. Since S_1^* is simple and has dimension n it must be $S_1^* \cong S_1$. Suppose now that $p \neq 2$. Write $p - 1 = 2q$. Then we may take the λ_j's in (2) satisfying $\lambda_{p-l} = \lambda_l^{-1}$ for $l = 1, ..., q$. Indeed, as $\lambda_l^n = \theta^{p-l}$, we have $(\lambda_l^{-1})^n = \theta^l = \theta^{p-(p-l)} = \lambda_{p-l}^n$. This implies that $\lambda_j^{-1} = \lambda_{p-j}$ for every $j = 1, ..., p-1$.

Consider in S_j^* the dual basis $\{v_0^*, ..., v_{n-1}^*\}$. To establish the isomorphism between S_j^* and S_{p-j} some previous computations are needed.

$$\begin{aligned} g^{-1} \cdot v_i &= g^{pn-1} \cdot v_i \\ &= (\omega^{-i})^{pn-1} (\lambda_j)^{pn-1} v_i \\ &= \omega^i \lambda_{p-j} v_i, \qquad i = 0, \cdots, n-1. \end{aligned}$$

Thus we get:

$$\begin{aligned} \langle g \cdot v_k^*, v_i \rangle &= \langle v_k^*, S(g) \cdot v_i \rangle \\ &= \langle v_k^*, g^{-1} \cdot v_i \rangle \\ &= \langle v_k^*, \omega^i \lambda_{p-j} v_i \rangle \\ &= \omega^i \lambda_{p-j} \langle v_k^*, v_i \rangle \\ &= \omega^i \lambda_{p-j} \delta_{k,i}, \qquad i, k = 0, \cdots, n-1, \end{aligned}$$

and so $g \cdot v_k^* = \omega^k \lambda_{p-j} v_k^*$.

In order to set the desired isomorphism we define a new basis for S_j^* given by $u_0 = v_0^*$ and $u_k = x \cdot u_{k-1}$ for $k = 1, \cdots, n-1$. Taking into account that $gx = \omega^{-1} xg$ it is easy to prove by induction that $g \cdot u_k = \lambda_{p-j} \omega^{-k} u_k$. Hence $\{u_0, ..., u_{n-1}\}$ is a basis of S_j^* because it consists of eigenvectors attached to different eigenvalues. By definition, $x \cdot u_k = u_{k+1}$ for $k = 0, \cdots, n-2$ and

$$\begin{aligned} x \cdot u_{n-1} &= x^n \cdot u_0 \\ &= (g^n - 1) \cdot u_0 \\ &= g^n \cdot u_0 - u_0 \\ &= (\lambda_{p-j})^n u_0 - u_0 \\ &= \theta^j u_0 - u_0 \\ &= (\theta^j - 1) u_0 \end{aligned}$$

Finally, denoting by $\{w_0, ..., w_{n-1}\}$ the basis of S_{p-j} and bearing in mind the action of A_p on S_{p-j} (2), we have shown that the map from S_j^* to S_{p-j} mapping $u_k \to w_k$ for $k = 0, ..., n-1$ is an isomorphism of A_p-modules.

IV. Practical results

The ideal code steaming from S_j is called a Radford code. Our aim in this section is to give the main parameters of these codes. We remark that everything concerning Taft codes, those arising from T_n, is shown in [4]. Our first step is to find the (left) ideal of A_p isomorphic to S_j. Taking into account the algebra isomorphism $A_p f_j \cong M_n(\mathbb{K})$ established in the proof of Theorem 2.2 such ideal corresponds to the left ideal in $M_n(\mathbb{K})$ generated by the idempotent matrix e_{11} which has 1 in the position $(1,1)$ and zero elsewhere. The idempotent in $A_p f_j$ corresponding to e_{11} is

$$\overline{e}_j = \frac{1}{n} \left(\sum_{i=0}^{n-1} \frac{1}{\lambda^{(p-j)i}} (g f_j)^i \right).$$

Then $A_p \overline{e}_j$ is the simple (left) ideal of A_p isomorphic to S_j.

Lemma 4.1: $\{\overline{e}_j, x\overline{e}_j, ..., x^{n-1}\overline{e}_j\}$ is a basis of $A_p \overline{e}_j$.

Proof. We compute:

$$\begin{aligned} (g f_j)\overline{e}_j &= \tfrac{1}{n} \left(\textstyle\sum_{i=0}^{n-1} \frac{1}{\lambda^{(p-j)i}} (g f_j)^{i+1} \right) \\ &= \tfrac{1}{n} \left(\theta^{p-j} \frac{1}{\lambda^{(p-j)(n-1)}} f_j + \sum_{i=0}^{n-2} \frac{1}{\lambda^{(p-j)i}} (g f_j)^{i+1} \right) \\ &= \tfrac{1}{n} \lambda^{p-j} \left(f_j + \textstyle\sum_{i=0}^{n-2} \frac{1}{\lambda^{(p-j)(i+1)}} (g f_j)^{i+1} \right) \\ &= \lambda^{p-j} \overline{e}_j, \end{aligned}$$

where we used that $(g f_j)^n = \theta^{p-j} f_j$ and $(\lambda^{p-j})^n = \theta^{p-j}$. Taking into account that $gx = \omega^{-1} xg$ it is easy to show by induction that $g x^k \overline{e}_j = \lambda^{p-j} \omega^{-k} x^k \overline{e}_j$ for $k = 0, ..., n-1$. Then the given set is a basis because it consists of eigenvectors attached to different eigenvalues.

Proposition 4.2: $d_{min}(A_p\overline{e}_j) = pn$ and the weight distribution is given by $W(jpn) = |\mathbb{K}^*|^j \binom{n}{i}$.

Proof. To compute these parameters we find the coordinates of the basis vectors of $A_p\overline{e}_j$ in the basis $\{x^r g^k : r = 0, ..., n-1; k = 0, ..., pn-1\}$ of A_p. For, first recall that $e = \frac{1}{p}\left(\sum_{l=0}^{p-1} g^{nl}\right)$ is a central idempotent in A_p, $e' = 1-e$, and $f_j = \frac{1}{p}\left(\sum_{i=0}^{p-1} \theta^{ij} g^{ni}\right) e'$ is a central idempotent in $A_p e'$. Observe that for any natural number r we have $(gf_j)^r = g^r f_j$. We now are ready to compute the coordinates:

$$\begin{aligned} x^m\overline{e}_j &= \tfrac{1}{n}\left(\sum_{i=0}^{n-1} \tfrac{1}{\lambda^{(p-j)i}} x^m (gf_j)^i\right) \\ &= \tfrac{1}{n}\left(\sum_{i=0}^{n-1} \tfrac{1}{\lambda^{(p-j)i}} x^m g^i f_j\right) \\ &= \tfrac{1}{n}\left(\sum_{i=0}^{n-1} \tfrac{1}{\lambda^{(p-j)i}} x^m g^i\right) f_j \\ &= \tfrac{1}{n}\left(\sum_{i=0}^{n-1} \tfrac{1}{\lambda^{(p-j)i}} x^m g^i\right) \tfrac{1}{p}\left(\sum_{l=0}^{p-1} \theta^{lj} g^{nl}\right) e' \\ &= \tfrac{1}{pn}\left(\sum_{i=0}^{n-1} \tfrac{1}{\lambda^{(p-j)i}} x^m g^i\right) \left(\sum_{l=0}^{p-1} \theta^{lj} g^{nl}\right)(1-e) \end{aligned}$$

We claim that $\left(\sum_{l=0}^{p-1} \theta^{lj} g^{nl}\right) e = 0$. Indeed,

$$\begin{aligned} \left(\sum_{l=0}^{p-1} \theta^{lj} g^{nl}\right) e &= \tfrac{1}{p}\left(\sum_{l=0}^{p-1} \theta^{lj} g^{nl}\right)\left(\sum_{k=0}^{p-1} g^{nk}\right) \\ &= \tfrac{1}{p}\left(\sum_{l,k=0}^{p-1} \theta^{lj} g^{n(l+k)}\right) \\ &= \tfrac{1}{p}\left(\sum_{r=0}^{p-1}(\sum_{s=0}^{p-1} \theta^{js}) g^{nr}\right) \\ &= 0 \end{aligned}$$

Hence,

$$\begin{aligned} x^m\overline{e}_j &= \tfrac{1}{pn}\left(\sum_{i=0}^{n-1} \tfrac{1}{\lambda^{(p-j)i}} x^m g^i\right)\left(\sum_{l=0}^{p-1} \theta^{lj} g^{nl}\right) \\ &= \tfrac{1}{pn}\left(\sum_{l=0}^{p-1}\sum_{i=0}^{n-1} \theta^{lj} \tfrac{1}{\lambda^{(p-j)i}} x^m g^{nl+i}\right) \end{aligned}$$

We can rescale the vectors $x^m\overline{e}$ multiplying them by pn. The coordinates of each of these new vectors with respect to the basis $\{x^r g^k : r = 0, ..., n-1; k = 0, ..., pn-1\}$ of A_p is a list $(\overline{0}, ..., \overline{0}, B_m, \overline{0}, ..., \overline{0})$ of length pn^2, where $\overline{0}$ denotes a block of pn zeros and the block B_m, of length pn, is placed in position m. This block is given by $B_m = (B_{m\ 0}, ..., B_{m\ p-1})$ with each $B_{m\ l}$ being the block of length n given by $B_{m\ l} = \theta^{lj}(1, \lambda^{p-j}, \lambda^{2(p-j)}, ..., \lambda^{(n-1)(p-j)})$.

Thus, words of $A_p\overline{e}_j$ are linear combinations of vectors of the above basic vectors, that do not overlap and therefore, $d_{min}(A_p\overline{e}_j) = pn$ and it easily follows that the weight distribution is given by $W(jpn) = |\mathbb{K}^*|^j \binom{n}{i}$. This finishes the proof.

In [4] it is showed that indecomposable projective codes in the Taft Hopf algebra part can be considered as a concatenation of cyclic codes with the advantages that we get to encoding / decoding algorithms when we make them block by block and augmenting the capability of correcting errors under some circumstances (cf. [4]).

Now, from the above and taking into account that $\lambda^{(p-j)} = \theta^{-j}$ and that in this way $\lambda^{(p-j)}$ is a pn-th root of unit, block B_m for $m = 1, \cdots, n$ can be identified with a code equivalent to the cyclic code given by $\lambda^{(p-j)}$. Therefore, what we get is that these simple codes in the matrix part of the Radford's Hopf algebra consist in n blocks of repetitions of this cyclic code. This also have two interesting consequences. On one hand, we have block by block classical encoding / decoding good algorithms to be applied on these ideal codes. On the other hand, if we consider n copies of such a cyclic code and consider them into a bigger vector space, with the appropiate reordering of the basis, what we would get is an ideal simple code over such Radford's Hopf algebras.

V. CONCLUSIONS AND FUTURE WORKS

A. Conclusions

We have studied codes in a family of Hopf algebras that extend a well-known family of Hopf algebras known as Taft algebras. To do so we have given a structure theorem (Theorem 2.2) for this family. Then we have studied indecomposable ideal codes in the two given parts of these algebras. First part was studied in [4] and, for the second part we have determined the indecomposable ideal codes and showed that their corresponding duals (as modules) are again ideal codes that can easily be identified. We have also calculated their main parameters. Finally we have shown that these codes can be considered as a concatenation of cyclic codes and so, usual encoding / decoding algorithms for cyclic codes can be used in this case and that standard operations over certain cyclic code enable us to get ideal codes over a Hopf algebra.

B. Future Works

Given that results on these new ideal codes are similar to those in the Taft algebras studied in [4], our aim is to determine if tensor products of these new indecomposable ideal codes are again, as in [4], ideal codes can be easily calculated by a similar formula

VI. ACKNOWLEDGMENTS

The second named author was supported by a predoctoral fellowship of the project *Teoría de Anillos y Aplicaciones a la Geometría no Conmutativa* (MTM2008-03339) from Ministerio de Ciencia e Innovación.

REFERENCES

[1] J. Berman, On the Theory of Group Codes, *Kibernetika (Kiev)* vol. 1, 1967, pp. 31-39 (Russian): translated as *Cybernetics* vol. 1, 1969, pp. 25-39.

[2] M. Greferath, A. Nechaev and R. Wisbauer, Finite Quasi-Frobenius Modules and Linear Codes, *J. Algebra Appl.* vol. 3 (3), 2004, pp. 247-272.

[3] R.W. Hamming, Error detecting and error correcting codes, *Bell System Tech. J.* vol. 29, 1950, pp. 147-160.

[4] J. Cuadra, J.M. García-Rubira and J.A. López-Ramos, Determining all indecomposable codes over some Hopf algebras. Preprint, 2009.

[5] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New-York-Oxford; 1977.

[6] S. Montgomery, *Hopf Algebras and Their Actions on Rings,* CBMS 82 A.M.S., Chicago; 1982.

[7] D.E. Radford, On the coradical of a finite-dimensional Hopf algebra. Proc. Amer. Math. Soc. vol. 53 (1), 1975, 9-15.

[8] J.A. Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.* vol. 121 (3), 1999, pp. 555-575.

[9] J.A. Wood, Code equivalence characterizes finite Frobenius rings, *Proc. Amer. Math. Soc.* vol. 136 (2), 2008, pp. 699-706 (electronic).