Consta-Dihedral Codes and their Transform Domain Characterization

V. Shashidhar and B. Sundar Rajan
Dept. of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012, INDIA
{shashidhar@protocol.,bsrajan@}ece.iisc.ernet.in

Abstract — **We identify a cocycle on the dihedral group D_n of $2n$ elements which results in a new class of codes called consta-dihedral codes. We define a new transform for these codes and then characterize all the consta-dihedral codes using this new transform.**

The dihedral group D_n is the set $D_n = \{1,\ r,\ r^2,\ \ldots,\ r^{n-1},\ s,\ rs,\ r^2s,\ \ldots,\ r^{n-1}s\}$ where $r^n = s^2 = 1$ and $rs = sr^{n-1}$. In this paper, we assume n is even. The results of this paper can be extended trivially to the case when n is odd. The following definition identifies a cocycle on dihedral group similar to the consta-cycle cocycle on cyclic group [1].

Definition 1 *Let β_r, β_s be two elements of the field F_q. We define ψ to be a map from $D_n \times D_n$ to F_q^* given by*

$$\psi(1,g) = \psi(g,1) = \psi(1,1) = 1,$$

$$\psi(r^i, r^j) = \psi(r^i, r^j s) = \beta_r^{\lfloor (i+j)/n \rfloor}, \quad for \quad i,j \neq 0$$

and $\psi(r^i s, r^j s^k) = \psi(r^i, r^{n-j})\beta_s^{\lfloor (k+1)/2 \rfloor}, \quad for \quad i,j \neq 0$. *The cocycle ψ is called a (β_r, β_s)-***constacyclic cocycle** *on D_n.*

Definition 2 *Let ψ be the (β_r, β_s)-constacyclic cocycle on D_n. Then, a right (left) (β_r, β_s)-consta-dihedral code is a subset of F_q^{2n} corresponding to a right (left) ideal in the cocyclic group ring $F_q^{\psi} D_n$. Clearly, when a code is both a right and left consta-dihedral code, it will correspond to a two-sided ideal in $F_q^{\psi} D_n$.*

With β_r and β_s equal to 1, we obtain the dihedral codes [2]. Let F_{q^m} be an extension of F_q such that β_r and β_s have n-th and square roots in F_{q^m} respectively. Let d be the order of β_r. Let λ_r be an n-th root of β_r and λ_s be a square root of β_s. We will assume that λ_s is in F_q. The transform matrix for a (β_r, β_s)-consta-dihedral code is defined as follows: The transform matrix has rows and columns indexed with conjugate classes and elements of D_n respectively. The $([g]), r^i s^j)$-th element of the transform matrix Φ is $\lambda_r^i \lambda_s^j \phi_{([g])}(r^i s^j)$, where $\phi_{([g])}$ is the irreducible representation of D_n corresponding to the conjugate class $\lceil g \rceil$.

Definition 3 (Consta-dihedral DFT (CD-DFT)) *Let $a = (a_1, a_r, \ldots, a_{r^{n-1}}, a_s, a_{rs}, \ldots, a_{r^{n-1}s}) \in F_q$ Then, the transform domain vector A of the time domain vector a is given as $A = \Phi a$.*

Lemma 1 (Conjugate Symmetry Property) *A vector $A = (A_1, A_{r^{n/2}}, A_s, A_{rs}, A_r, \ldots, A_{r^{n/2}-1}) \in F_{q^m}^4 \times M_2(F_q^m)^{n/2-1}$, is a transform domain vector of a vector $a = (a_1, a_r, a_{r^2}, \ldots, a_s, a_{rs}, \ldots, a_{r^{n-1}s})$ iff A satisfies the following properties:*

(1) $A_1^{q^j} = \begin{cases} A_{r^k}(1,1) + A_{r^k}(1,2) & \text{if } k = h(q^j - 1)/d \leq n/2 \\ A_{r^{n-k}}(2,2) + A_{r^{n-k}}(2,1) & \text{if } k = h(q^j - 1)/d > n/2 \end{cases}$

(2) $A_s^{q^j} = \begin{cases} A_{r^k}(1,1) - A_{r^k}(1,2) & \text{if } k = h(q^j - 1)/d \leq n/2 \\ A_{r^{n-k}}(2,2) - A_{r^{n-k}}(2,1) & \text{if } k = h(q^j - 1)/d > n/2 \end{cases}$

(3) $A_{r^{n/2}}^{q^j} = \begin{cases} A_{r^k}(1,1) + A_{r^k}(1,2) & \text{if } k = n/2 + h(q^j - 1)/d \leq n/2 \\ A_{r^{n-k}}(2,2) + A_{r^{n-k}}(2,1) & \text{if } k = n/2 + h(q^j - 1)/d > n/2 \end{cases}$

(4) $A_{rs}^{q^j} = \begin{cases} A_{r^k}(1,1) - A_{r^k}(1,2) & \text{if } k = n/2 + h(q^j - 1)/d \leq n/2 \\ A_{r^{n-k}}(2,2) - A_{r^{n-k}}(2,1) & \text{if } k = n/2 + h(q^j - 1)/d > n/2 \end{cases}$

and

(5) $A_{r^k}^{q^j}(u,v) = \begin{cases} A_{r^l}(u,v) & \text{if } l = kq^j + \frac{h(q^j-1)}{d} \leq n/2 \\ A_{r^l}(3-u, 3-v) & \text{if } l = -kq^j - \frac{h(q^j-1)}{d} \leq n/2 \end{cases}$, *for* $u = 1$ *and* $v = 1, 2$

(6) $A_{r^k}^{q^j}(u,v) = \begin{cases} A_{r^l}(u,v) & \text{if } l = -kq^j + \frac{h(q^j-1)}{d} \leq n/2 \\ A_{r^l}(3-u, 3-v) & \text{if } l = +kq^j - \frac{h(q^j-1)}{d} \leq n/2 \end{cases}$ *for* $u = 2$ *and* $v = 1, 2$.

Let $I_k^{\psi}(i) = \Big\{ ((-1)^{(i-1)} kq^j + \frac{h(q^j-1)}{d})' \,\Big|\, ((-1)^{(i-1)} kq^j + \frac{h(q^j-1)}{d})$ is an nonzero integer $\Big\}$, for $i = 1, 2$, where $(x)'$ is equal to x if $x \leq n/2$ and $n - x$ otherwise. Then, from the conjugacy constraints of Φ_d, it is easy to see that the components $A_{r^k}(i,1)$ and $A_{r^k}(i,2)$ can take values only from the field $F_{q^{l_{k(i)}}}$, where $l_{k(i)}$ is the cardinality of the set $I_k^{\psi}(i)$ for $i = 1, 2$. Then, we have the following structure theorem for the cocyclic group ring $F_q^{\psi} G$.

Theorem 1 (Structure Theorem) *Let L be the set of elements one from each distinct q-cyclotomic coset $I_k^{\psi}(i)$. Then, the cocyclic group ring $F_q^{\psi} G$ is isomorphic to the algebra $\bigoplus_{k \in L} F_{q^{l_{k(i)}}}$ where $l_{k(i)}$ is the size of the set $I_i^{\psi}(i)$.*

For every $\lambda \in F_{q^m}^*$(nonzero elements of F_{q^m}), an F_q-subspace V of F_{q^m} is called λ-invariant if it is closed under multiplication by λ. A λ-invariant F_q-subspace of F_{q^m}, for brevity will be denoted as $[\lambda, q, m]$-subspace,

We now characterize all the right consta-dihedral codes in the transform domain we have defined. The characterizations of the left and two-sided consta-dihedral codes are similar to that of right codes.

Theorem 2 *Let $\mathcal{C}$ be a $2n$-length linear code over F_q, and let $A(\mathcal{C}) = \{\phi a | a \in \mathcal{C}\}$. Also let $A_{r^k}(\mathcal{C}) = \{A_{r^k} | A \in A(\mathcal{C})\}$ and $A_{r^k}(\mathcal{C})(u,v) = \{A_{r^k}(u,v) | A \in A(\mathcal{C})\}$ for $u, v = 1, 2$. Then, $\mathcal{C}$ is a right (β_r, β_s)-consta-dihedral code iff the following properties are satisfied:*
(1) $A(\mathcal{C})$ satisfies the conjugate symmetry property,
(2) $A_{r^k}(\mathcal{C})(1,1)$ is a $[\alpha^k \lambda_r, q, l_k]$-subspace; $A_{r^k}(\mathcal{C})(2,2)$ is a $[\alpha^{-k} \lambda_r, q, l_k]$-subspace; $A_{r^k}(\mathcal{C})(1,2)$ is an $[\alpha^k \lambda_r^{n-1}, q, l_k]$-subspace and $A_{r^k}(\mathcal{C})(2,1)$ is an $[\alpha^{-k} \lambda_r^{n-1}, q, l_k]$-subspace,
(3) The set $A_{r^k}(\mathcal{C})$ is a subspace of $M_2(F_{q^{l_k}})$ which is invariant under the right multiplication of $\begin{pmatrix} 0 & \lambda_s \\ \lambda_s & 0 \end{pmatrix}$.

[1]This work was partly funded by the IISc-DRDO Program on Advanced Research in Mathematical Engineering through a grant to B.S.Rajan.

References

[1] G. Hughes, "Constacyclic codes, cocycles and a $u+v|u-v$ construction," *IEEE Trans. Inform. Theory,* vol.46, no.2, pp.674-680, Mar 2000.

[2] MacWilliams, F. J., "Codes and ideals in group algebras," *Proc. Conf. Combinatorial Mathematics and its Applications,*, 1967, Chapel Hill, N.C., U. of N.C. Press, 1969.