Codes Closed under Arbitrary Abelian Group of Permutations

Bikash Kumar Dey and B. Sundar Rajan
Department of ECE, IISc, Bangalore 560012, India
e-mail: bikash@protocol.ece.iisc.ernet.in and bsrajan@ece.iisc.ernet.in

Abstract — **Algebraic structure of codes closed under arbitrary abelian group G of permutations is investigated resulting in insight into Dual of G-invariant codes and Self-dual G-invariant codes. For special types of the groups, these codes give cyclic, abelian, quasi-cyclic and quasi-abelian codes. Karlin's decoding algorithm for systematic one-generator quasi-cyclic codes is extended for systematic quasi-abelian codes with any number of generators.**

I. Summary

For any abelian group G with exponent ν relatively prime to $q = p^m$ (p is a prime), if r is the smallest positive integer such that F_{q^r} contains a primitive ν-th root of unity, then a map $\psi : G \times G \to F_{q^r}$ can be chosen (see [1]) such that (i) $\psi(x, yz) = \psi(x,y)\psi(x,z)$ (ii) $\psi(x,y) = \psi(y,x)$ (iii) $(\psi(x,y) = \psi(x',y), \forall y \in G) \Leftrightarrow x = x'$ and

$$(iv) \qquad \sum_{x\in G} \psi(x,y) = \begin{cases} |G|, & \text{if } y = 1 \\ 0, & \text{if } y \neq 1 \end{cases}$$

Using this map, the DFT of any element $\mathbf{a} = \sum_{x\in G} a_x x \in F_q G$ is defined as $\mathbf{A} \in F_{q^r} G$ with $A_y = \sum_{x\in G} \psi(x,y) a_x$.

Let a finite set I index the coordinate positions of a code over F_q and $G \subseteq Perm(I)$ be an abelian group with exponent ν relatively prime to q. Let $I_1, \cdots, I_t$ be the orbits of I under the action of G. If $G_k = \{g^{(k)} \triangleq g|_{I_k} \in Perm(I_k) | g \in G\}$ for $k = 1, \cdots, t$, then it is easy to check that $|G_k| = |I_k|$ ($|.|$ denotes the cardinality of the set inside). So, the coordinates of the code can be indexed by elements of $\mathcal{G} \triangleq \cup_{i=1}^t G_i$ instead of I such that $g(h^{(k)}) = g^{(k)} h^{(k)}$. The DFT of any $\mathbf{a} \in F_q^{\mathcal{G}}$ is defined as $\mathbf{A} \in F_{q^r}^{\mathcal{G}}$, where

$$A_y = \sum_{x \in G_k} \psi_k(y,x) a_x \qquad \forall y \in G_k, \ \forall k.$$

Here ψ_k is ψ (as discussed in the last paragraph) for G_k. This DFT satisfies the **conjugacy constraint:** $A_{x^q} = A_x^q$. If $\mathbf{b} = g(\mathbf{a})$, i.e. if $b_x = a_{g^{(k)-1}x}\ \forall x \in G_k, \forall k$, then $B_y = \psi_k(g^{(k)}, y) A_y\, \forall y \in G_k, \forall k$. We define the **cyclotomic coset, residue class and cyclotomic residue class** of $x \in \mathcal{G}$ as respectively $[x]^q \triangleq \{x, x^q, x^{q^2}, \cdots\}$, $\tilde{x} \triangleq \{x_1 \in \mathcal{G} | \langle g, x_1\rangle = \langle g, x\rangle$ for each $g \in G\}$ and $(x)^q \triangleq \{x_1 \in \mathcal{G}|$ for some non negative l, $\langle g, x_1\rangle^{q^l} = \langle g, x\rangle\ \forall g \in G\}$, where $\langle h, x\rangle \triangleq \psi_k(h^{(k)}, x)$ when $x \in G_k$. Suppose, $|\tilde{x}| = e_x$ and $|[x]^q| = r_x$. Then clearly, $|(x)^q| = e_x r_x$. For any subset $X = \{x_1, x_2, \cdots, x_k\} \subseteq \mathcal{G}$, A_X denotes the ordered tuple $(A_{x_1}, A_{x_2}, \cdots, A_{x_k})$ where an arbitrary fixed order in X is assumed.

Theorem I.1 *Let G be an abelian group of permutations with order relatively prime to q. Then a code is G-invariant if and only if (i) for any $x \in \mathcal{G}$, $A_{\tilde{x}}$ takes values from a subspace of $F_{q^{r_x}}^{e_x}$ and (ii) if $(x_1)^q, \cdots, (x_k)^q$ are the distinct cyclotomic residue classes of $\mathcal{G}$, then $A_{\tilde{x}_1}, \cdots, A_{\tilde{x}_k}$ are unrelated.*

Corollary I.2 *If $\mathcal{C}_{(x_i)^q}$ denotes the subcode of $\mathcal{C}$ containing all the codewords with all the transform components outside $(x_i)^q$ zero, then $\mathcal{C} = \bigoplus_{i=1}^k \mathcal{C}_{(x_i)^q}$.*

Theorem I.3 *Let G be such that $|G_1| \equiv \ldots \equiv |G_t|$ mod p. For a G-invariant code $\mathcal{C}$, a vector $\mathbf{b} \in F_q^{\mathcal{G}}$ is orthogonal to $\mathcal{C}$ if and only if for all $\mathbf{a} \in \mathcal{C}$, $\sum_{y\in\tilde{x}} A_y B_{y^{-1}} = 0 \quad \forall$ cyclotomic residue classes $(x)^q$.*

We classify the cyclotomic residue classes into three categories: (i) $(x)^q$ with $x = x^{-1}$ (**Type A**): In this case, $r_x = 1$. (ii) $(x)^q$ with $x \neq x^{-1} \in (x)^q$ (**Type B**): In this case, r_x is even and $x^{-1} = x^{q^{\frac{r_x}{2}}}$ and (iii) $(x)^q$ with $x^{-1} \notin (x)^q$ (**Type C**).

Let $N(q,l)$, $N_E(q,l)$ and $N_H(q,l)$ denote respectively the number of subspaces of F_q^l, the number of self dual and Hermitian self dual codes of length l over F_q. Suppose, different types of cyclotomic cosets are: Type A: $(x_1)^q, \cdots, (x_{i_1})^q$, Type B: $(y_1)^q, \cdots, (y_{i_2})^q$, and Type C: $(z_1)^q, (z_1^{-1})^q \cdots, (z_{i_3})^q, (z_{i_3}^{-1})^q$.

Theorem I.4 *Let G be such that $|G_1| \equiv \ldots \equiv |G_t|$ mod p. Number of self dual G-invariant codes over F_q is $\prod_{i=1}^{i_1} N_E(q^{r_{x_i}}, e_{x_i}) \prod_{j=1}^{i_2} N_H(q^{r_{y_j}}, e_{y_j}) \prod_{k=1}^{i_3} N(q^{r_{z_k}}, e_{z_k})$, where the empty product is 1 by convention.*

Theorem I.5 *A G-invariant binary self-dual code $\mathcal{C}$ is Type II if and only if its binary component $\mathcal{C}_{\tilde{0}}$ is Type II.*

For $\frac{n}{l}$-quasi-cyclic codes of length n, the distinct cyclotomic residue classes corresponds to the distinct q-cyclotomic cosets in Z_l. With this correspondence, the theorems I.4 and I.5 give all the results of [2] regarding self-dual quasi-cyclic codes as special cases. The results can easily be extended to the general case (i.e. when $|G_1| \equiv \ldots \equiv |G_t|$ mod p does not necessarily hold true).

Quasi-abelian codes [3] on an abelian group G can be defined as submodules of $(F_q G)^l$ for some t. Karlin's decoding algorithm [4] for systematic one-generator quasi-cyclic codes is extended for systematic quasi-abelian codes with any number of generators. Moreover, for a G-invariant code, if the subspaces from which $A_{\tilde{x}}$ take values (see Theorem I.1) are known, then a set of parity check equations over F_{q^r} can be derived and used to get a lower bound on the minimum Hamming distance for the code using BCH-like argument [5]. Details is omitted due to lack of space.

References

[1] P. Delsarte, "Automorphisms of abelian codes," *Philips Research Reports*, vol. 25, pp. 389–402, 1970.

[2] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: Finite fields," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2751–2760, 2001.

[3] S. K. Wasan, "Quasi abelian codes," *Publ. de L'Institute Mathematique*, vol. 21, pp. 201–206, 1977.

[4] M. Karlin, "Decoding of circulant codes," *IEEE Trans. Inform. Theory*, vol. 16, pp. 797–802, 1970.

[5] R. M. Tanner, "A transform theory for a class of group-invariant codes," *IEEE Trans. Inform. Theory*, vol. 34, no. 4, pp. 752–775, 1988.