ON THE NON-ABELIAN GROUP CODE CAPACITY OF MEMORYLESS CHANNELS

JORGE P. ARPAȘI

Avenida Tiaraju 810
Alegrete
RS, 97541-151, Brazil

Abstract. In this work is provided a definition of group encoding capacity $C_G$ of non-Abelian group codes transmitted through symmetric channels. It is shown that this $C_G$ is an upper bound of the set of rates of these non-Abelian group codes that allow reliable transmission. Also, is inferred that the $C_G$ is a lower bound of the channel capacity. After that, is computed the $C_G$ of the group code over the dihedral group transmitted through the 8PSK-AWGN channel then is shown that it equals the channel capacity. It remains an open problem whether there exist non-Abelian group codes of rate arbitrarily close to $C_G$ and arbitrarily small error probability.

1. Introduction

Group codes were introduced by Slepian in [19] as a generalization of binary linear codes. Group codes allow to use non-binary, highly spectral-efficient, geometrically uniform modulations, while inheriting many of the nice structural properties enjoyed by binary linear codes. An overview of the different research lines on group codes developed during these years can be seen at [4, 3, 5, 9, 11, 17, 14, 7, 13]. One line of research is about the channel-capacity achieved by group codes. Differently from linear and non-linear codes, to speak about ensembles of group codes achieving channel capacity $C$ demands the previous definition of group encoding capacity $C_G$, for each group $G$ over which is based the group code. This fact was studied first by Ahlswede in [1] and the literature cited there. It was shown that $C_G \leq C$ and $C_G$ satisfies the converse of the Shannon’s encoding theorem, that is, if a group code $C$ has a rate $R$ such that $R > C_G$ then its decoding error probability $P_e(C)$ is bounded away from zero. Thus, after [1], an ensemble of group codes over a group $G$ transmitted through a channel with capacity $C$ is said to achieve the channel capacity if $C_G = C$ and, for any $\epsilon > 0$ and any $R < C_G$, there is a code $C$ of the ensemble with rate $R$ such that $P_e(C) < \epsilon$. (The Shannon’s encoding Theorem for $C_G$).

H. A. Loeliger, in [12], conjectured whether group codes over cyclic groups transmitted trough MPSK-AWGN channels would achieve channel capacity. This conjecture was proved to be right in [4]. To prove this achievement, given a finite Abelian group $G$, it is defined a $G$-Symmetric channel in such a way that it is a generalization of MPSK-AWGN channels and the well known symmetric BSC and

2010 Mathematics Subject Classification: Primary: 94A05, 94A24; Secondary: 94B60.

Key words and phrases: Group codes, symmetric channels, group encoding capacity, non-Abelian group codes, converse of Shannon’s coding theorem, achievement of channel capacity.

The author is supported by Fundação Universidade Federal do Pampa - UNIPAMPA, Brazil.

* Corresponding author.
BEC channels. The formula that defines the group encoding capacity $C_G$ is a max-min choice among suitable weighted capacities of the sub-channels determined by the subgroups of $G$. Following the random coding exponent of [8] it is derived a formula of random coding exponent for group codes. The randomization is made from a single group code by using the technique proposed in [18]. Finally, the equality $C_G = C$ is obtained for $G = \mathbb{Z}_p$ transmitted through a $p^r$-PSK-AWGN channel and an example where $C_G < C$ is given. On the other hand, the paper [17] uses the asymptotic equipartition property (AEP) to deal with ensembles of group codes, over Abelian groups, with rates achieving the group encoding capacity $C_G$. It is not concerned with the equality $C_G = C$.

In this work we develop most of the above ideas about $C_G$ for a special class of non-Abelian groups and show that the group encoding capacity equals the channel capacity. The importance of this equality is clear since any ensemble of group codes with $C_G < C$ has not any possibility to achieve the channel capacity. The non-Abelian groups which we will deal are extensions of the form $G^{n-1}$. Following the random coding exponent of [8] it is derived a formula of random coding exponent for group codes. The randomization is made from a single group code by using the technique proposed in [18]. Finally, the equality $C_G = C$ is obtained for $G = \mathbb{Z}_p^r \sqsupset \mathbb{Z}_p$. We show that, also in this case, $C_G$ satisfies the converse of the Shannon’s encoding theorem, that is, $R < C_G$ is a necessary condition for reliable transmissions over $G$-Symmetric channels. After that, we will show analytically that if $G$ is the dihedral group with eight elements and the channel is 8PSK-AWGN then $C_G = C$. Computer aided proof of this result, for some values of the signal-to-noise ratio $\frac{E}{N_0}$ was presented at [2].

The paper is organized as follows:

- In Section 2 is reviewed extension of groups $H \sqsupset K$ and it is shown that the groups $(H \sqsupset K)^N$ and $H^N \sqsupset K^N$ are isomorphic [Proposition 1]. This property is fundamental to define group codes over non-Abelian groups.
- In Section 3 is reviewed $G$-Symmetric channels and the group codes for these channels in accordance to [4]. Then is provided a definition of group encoding capacity $C_G$ for non-Abelian groups $G = \mathbb{Z}_p^r \sqsupset \mathbb{Z}_p$ [Definition 2]. It is shown that this $C_G$ is an upper bound for any reliable rate transmission $R$ [Theorem 1]. Also is concluded that $R \leq C_G \leq C$, where $R$ is a reliable transmission rate and $C$ is the channel capacity. It is estimated the $C_G$ when $G$ is the dihedral group $D_4$ and the channel is 8PSK-AWGN.
- In Section 4 is shown that the $C_G$ for the dihedral group $D_4$ over the 8PSK-AWGN channel, denoted specifically by $C_{D_4}$, equals the channel capacity, that is, $C_{D_4} = C$ [Theorem 2]. The proof of this Theorem is divided in four Lemmas on the capacities of the sub-channels that determine the encoding capacity $C_{D_4}$.

2. Groups and extension of groups

2.1. Notation for groups and related. Cyclic groups of order $n$ will be represented by $\mathbb{Z}_n = \{id, a, a^2, \ldots, a^{n-1}\}$ with $a$ a generator. Sometimes it will be more convenient to write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. This last notation is useful to represent subgroups $m\mathbb{Z}_n = \{0, m, \ldots, m(n-1)\}$. The symbol $\oplus$ will represent the direct product of groups, that is, $H \oplus K$ will mean the direct product of the groups $H$ and $K$. Given a natural number $N$ and a group $G$, the notation $G^N$ will mean the multiple direct product $G^N = G \oplus G \oplus \cdots \oplus G$. For instance $\mathbb{Z}_{2^2}^3 = \mathbb{Z}_2^3 = \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$. 
A generalization of the direct product of groups is the extension of groups [16, 10]. The extension of groups $H$ by $K$ will be denoted by $H \times K$. If $G$ is an Abelian group and $H$, $K$ are subgroups of $G$ then the symbol $+$ will be used in the sense that $H + K = \{g \in G; g = h + k, h \in H, k \in K\}$. Notice that the group $H + K$ is very different from the group $H \times K$. The symbol $\otimes$ will be used for isomorphism of groups, that is $H \otimes K$ will mean $H$ is isomorphic with $K$. Finally the notation $H \subset G$ will mean “$H$ is a subgroup of $G$”.

2.2. DIRECT PRODUCT OF EXTENSION OF GROUPS: $(H \times K)^N$. A group $G$ with normal subgroup $H \triangleleft G$ such that the quotient group $G/H$ is isomorphic with a group $K$ is said to be an extension of $H$ by $K$ [16]. Since each element $g \in G$ belongs to an unique coset $Hk \in G/H$, $g$ can be written as a “ordered pair” $g = hk$. The group operation $g_1g_2 = (h_1k_1)(h_2k_2) = h_1(k_1h_2k_2^{-1})k_1k_2$, with $k_1h_2k_2^{-1} = h_2^k \in H$, determines a group isomorphism between $G$ and the extension $H \times K$. The semi-direct product and direct product of groups are particular cases of extension of groups. It can be shown that when $h_2^k \neq h_2$, for some $h_2$ or else some $k_1$, then the extension $H \times K$ is a non-Abelian group. In this article, with the purpose of simplicity, the extension will be denoted by $H \times K$ whereas the direct product will be represented by $H \oplus K$ and, for any integer $N \geq 1$, $G^N$ will be the $N$-fold direct product of $G$.

**Proposition 1.** If $G = H \times K$ then: 

$$G^N = (H \times K)^N \cong H^N \times K^N.$$ 

**Proof.** For the case $N = 2$, define $\varphi : G^2 \to (G/H)^2$ as $\varphi(g_1, g_2) = (g_1H, g_2H)$. Then $\varphi((g_{11}, g_{12}) \ast (g_{21}, g_{22})) = \varphi(g_{11}g_{21}, g_{12}g_{22}) = (g_{11}g_{21}H, g_{12}g_{22}H)$. On the other hand

$$\varphi(g_{11}, g_{12}) \ast \varphi(g_{21}, g_{22}) = (g_{11}H, g_{12}H) \ast (g_{21}H, g_{22}H) = (g_{11}g_{21}H, g_{12}g_{22}H),$$

which shows that $\varphi$ is a group homomorphism. Clearly $\varphi$ is surjective with kernel $\ker(\varphi) = H^2$. Therefore, $H^2$ is a normal subgroup of $G^2 = (H \times K)^2$ and by the First Isomorphism Theorem for groups, $G^2/H^2 \cong (G/H)^2 \cong K^2$. For $N > 2$, suppose $(H \times K)^{N-1} \cong H^{N-1} \times K^{N-1}$. Then defining $\varphi : G^N \to (G/H)^N$ as $\varphi(g_1, g_2) = (g_1H^{N-1}, g_2H)$, where $g_1 \in G^{N-1}$ and $g_2 \in G$, we can show, analogously to the case $N = 2$, that $\varphi$ is a surjective group homomorphism with kernel $H^N$. Therefore $H^N$ is a normal subgroup of $G^N = (H \times K)^N$ and $G^N/H^N \cong (G/H)^N \cong K^N$. 

**Example.-** A normal subgroup of the dihedral group $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ is $H = \{e, a, a^2, a^3\} \cong \mathbb{Z}_4$, the respective quotient group is $D_4/H = \{H, Hb\} \cong \mathbb{Z}_2$. Then $D_4 = \mathbb{Z}_4 \times \mathbb{Z}_2$ and $D_4^N = \mathbb{Z}_4^N \times \mathbb{Z}_2^N$. Each element $g \in D_4$ has the form $g = a^ib^j$ with the group operation $(a^ib^j) \ast (a^ib^j) = a^{i_1+b_1j_1} = a^{i_1}b^{j_1}a^{i_2}b^{j_2} = a^{i_1+b_1j_1+b_1j_2}$, [16, 10].

3. G-SYMMETRIC CHANNELS, GROUP CODES AND GROUP ENCODING CAPACITY

In this Section we will provide the definition of group encoding capacity $C_G$ for a particular class of non-Abelian groups. We mention here that, in [4], $C_G$ is originally called $G$-Capacity. We will show that $C_G \in [R, C]$, where $R$ is a reliable transmission rate and $C$ is the channel capacity. Then, we will apply this estimation of $C_G$ for $G = D_4$, the dihedral group with eight elements, for transmission over the 8PSK-AWGN channel.
Definition 3.1. A channel \((\mathcal{X}, \mathcal{Y}, p(y|x))\), with \(\mathcal{X}\) finite is said to be \(G\)-Symmetric, if there is a group \(G\) such that:

- \(G\) acts simply and transitively over the input alphabet \(\mathcal{X}\),
- \(G\) acts isometrically over the output set \(\mathcal{Y}\) and
- \(p(gy|gx) = p(y|x)\) for all \(g \in G\), for all \(x \in \mathcal{X}\) and for all \(y \in \mathcal{Y}\).

\(\square\)

Some examples of \(G\)-Symmetric channels:

- The BSC channel, with \(\mathcal{X} = \{x_1, x_2\}, \mathcal{Y} = \{y_1 = x_1, y_2 = x_2\}\), \(G = S_2 = \{((), (12))\}\) is the permutation group of the list \(\{1, 2\}\). The conditional probabilities are \(p(y_1|x_2) = p(y_2|x_1) = \epsilon\) and \(p(y_1|x_1) = p(y_2|x_2) = 1 - \epsilon\).
- The BEC channel \(\mathcal{X} = \{x_1, x_2\}, \mathcal{Y} = \{y_1 = x_1, y_2 = \epsilon, y_2 = x_2\}, G = S_2\).
- The conditional probabilities are \(p(y_3|x_1) = p(y_3|x_2) = \epsilon\) and \(p(y_1|x_1) = p(y_2|x_2) = 1 - \epsilon\).
- The 8PSK-AWGN channel \(X_8(2) = \{x_k = e^{2\pi jk/8}, j = \sqrt{-1}; k = 0, 1, 2, \ldots, 7\}\), \(\mathcal{Y} = \mathbb{R}^2\), \(G = D_4\), and \(p(y|x_k) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{\|y-x_k\|^2}{2\sigma^2}\right)\). The group \(D_4\) has a representation in \(G(2, \mathbb{R})\), the set of orthogonal matrices of the plane \(\mathbb{R}^2\), via the mappings \(a \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\) and \(b \mapsto \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\). With this representation is a straightforward task to verify the three conditions about \(G\)-Symmetry on the above Definition 3.1.

Remark 1. We write here the simply transitive action of \(D_4\) over \(X_8\) which allows to represent the channel by the triple \((D_4, \mathbb{R}^2, p(y|x))\) instead of \((X_8, \mathbb{R}^2, p(y|x))\). The signals are: \(x_1 = b_2x_0, x_2 = ax_0, x_3 = abx_0, x_4 = a^2x_0, x_5 = a^2bx_0, x_6 = a^3x_0,\) and \(x_7 = a^3bx_0\).

In general, the simply transitive action of the group \(G\) over the signal constellation \(\mathcal{X}\) allows to represent the channel as the triple \((G, \mathcal{Y}, p(y|x))\) instead of \((\mathcal{X}, \mathcal{Y}, p(y|x))\). The convenience of the group representation of a \(G\)-Symmetric channel comes when we choose a code against the noise of the channel. The natural choice is a group code which is a subgroup of \(G^N\). A group code \(C\) for a \(G\)-Symmetric channel is the image of an injective group homomorphism \(\phi : \mathcal{U} \rightarrow G^N\), with \(\mathcal{U}\) an uncoded channel source which must have a group structure such that \(\mathcal{U} \cong \phi(\mathcal{U}) := C \subset G^N\).

Now, let \(G\) be the extension group \(G = \mathbb{Z}_{p_1}^\eta \times \mathbb{Z}_{p_2}^r\) with \(p_1, p_2\) primes and \(\eta, r\) positive integers. By Proposition 4, \(G^N\) is isomorphic with \(\mathbb{Z}_{p_1}^{\eta N} \times \mathbb{Z}_{p_2}^{rN}\), which means that the encoding map is \(\phi : \mathcal{U} \rightarrow \mathbb{Z}_{p_1}^{\eta N} \times \mathbb{Z}_{p_2}^{rN}\). This implies that the group code \(C\) and the uncoded group \(\mathcal{U}\) must have the following structure:

\[
\mathcal{U} = \left( \mathbb{Z}_{p_1}^{k_{11}} \oplus \mathbb{Z}_{p_1}^{k_{12}} \oplus \cdots \oplus \mathbb{Z}_{p_1}^{k_{1r}} \right) \times \mathbb{Z}_{p_2}^{k_{21}} = \left( \bigoplus_{j=1}^{r} \mathbb{Z}_{p_1}^{k_{j1}} \right) \times \mathbb{Z}_{p_2}^{k_{21}},
\]

with the associated array of exponents \(k = \left( k_{11}, k_{12}, \ldots, k_{1r} \right)\) satisfying the conditions: \(k_{11} + k_{12} + \cdots + k_{1r} \leq N\eta\) and \(k_{21} \leq N\).

For each group code \(C\) with array of exponents \(k\) consider the arrays of integers \(l = \left( l_{i1}, l_{i2}, \ldots, l_{ir} \right)\) such that \(l_{ij} \leq j\) for all \(i, j\). Then, \(j - l_{ij} \geq 0\) and
with this we construct subgroups $\mathcal{U}(l) \subset \mathcal{U}$ as follows:

$$
\mathcal{U}(l) := \left[ \bigoplus_{j=1}^{r} p_{j}^{l_{ij}} Z_{p_{j}^{l_{ij}}} \right] \otimes p_{2}^{l_{21}} Z_{p_{2}^{l_{21}}} \cong \left[ \bigoplus_{j=1}^{r} Z_{p_{j}^{l_{ij}}} \right] \otimes Z_{p_{2}^{l_{21}}} \subset \mathcal{U}.
$$

In particular for $l$ with $l_{ij} = j$, $\mathcal{U}(l) = \mathcal{U}$.

On the other hand if the symbol $\sum$ represents the “addition” of subgroups $H + K = \{h + k; \ h \in H, k \in K\}$, then $\sum_{j=1}^{r} p_{j}^{r-l_{ij}} Z_{p_{j}^{r-l_{ij}}} \cong Z_{p_{j}^{l_{1m}}}^{r}$ with $l_{1m} = \max\{l_{11}, l_{12}, \ldots, l_{1r}\}$. From this, $G(l) := \left[ \sum_{j=1}^{r} p_{j}^{r-l_{ij}} Z_{p_{j}^{l_{1m}}}^{r} \right] \otimes p_{2}^{l_{21}} Z_{p_{2}^{l_{21}}} \cong Z_{p_{1}^{l_{1m}}}^{r} \otimes Z_{p_{2}^{l_{21}}}^{r}$ is isomorphic with $Z_{p_{1}^{l_{1m}}}^{r} \otimes Z_{p_{2}^{l_{21}}}^{r}$, which shows that $G(l)$ is a subgroup of $G$.

$$
\mathcal{U}(l) \subset G(l)^{N}
$$

which means $(G(l), Y, p(y|g))$ is a $G(l)$-Symmetric sub-channel with group code $C_{l} \cong \mathcal{U}(l)$.

Example. - $D_{4}^{N} = Z_{2}^{N} \otimes Z_{2}^{N} = Z_{2}^{2N} \otimes Z_{2}^{N}$, any group code $C$ is isomorphic with $\mathcal{U} = Z_{2}^{k_{11}} \oplus Z_{2}^{k_{12} \otimes Z_{2}^{k_{21}}}$ with $k_{11} + k_{12} \leq N$ and $k_{21} \leq N$. If we consider an array $l = \left[ \begin{array}{c}
11 \\
12
\end{array} \right]$ with $l_{ij} \leq j$, we have $U(l) = [2^{1-l_{11}} Z_{2}^{k_{11}} ] \oplus [2^{2-l_{12}} Z_{2}^{k_{12}} ] \oplus [2^{1-l_{21}} Z_{2}^{k_{21}} ] \cong \left[ Z_{2}^{k_{11}} \oplus Z_{2}^{k_{12}} \right] \otimes Z_{2}^{k_{21}} \subset \mathcal{U}$. On the other hand, $G(l) = [2^{2-l_{11}} Z_{4} \oplus 2^{2-l_{12}} Z_{4} ] \oplus [2^{1-l_{21}} Z_{2} ] \cong [ Z_{2}^{l_{11}} + Z_{2}^{l_{12}} ] \otimes Z_{2}^{l_{21}} \cong Z_{p_{1}^{l_{1m}}}^{r} \otimes Z_{p_{2}^{l_{21}}}^{r}$, with $l_{1m} = \max\{l_{11}, l_{12}\} \leq 2$. Thus $G(l) \subset D_{4}$ and $\mathcal{U}(l) \subset G(l)^{N}$.

3.1. The Group Code Capacity, $C_{G}$, when $G = Z_{p_{1}^{r}}^{r} \otimes Z_{p_{2}^{r}}$. The encoding rate of the group code $C$ is $R = \frac{\log(|\mathcal{U}|)}{N} = \frac{1}{N} \sum_{j=1}^{r} \sum_{i=1}^{2} jk_{ij} \log(p_{i})$, with $k_{2j} = 0$ for $j > 1$, whereas the encoding rate of the group code $C_{l}$ is $R_{l} = \frac{\log(|\mathcal{U}(l)|)}{N} = \frac{1}{N} \sum_{j=1}^{r} \sum_{i=1}^{2} l_{ij} jk_{ij} \log(p_{i})$, with $k_{2j} = 0$ for $j > 1$. By making

$$
\alpha_{ij} := \frac{jk_{ij} \log(p_{i})}{\log(|\mathcal{U}|)}
$$

we see that $\alpha_{ij} > 0$ and $\sum_{i,j} \alpha_{ij} = 1$ that allow to consider $\alpha_{ij}$ as a distribution of probabilities on the array $k$ of $\mathcal{U}$. Moreover, $\alpha_{ij}$ is independent of any array $l$, it depends only on $N$. Thus the encoding rate $R$ is related to any sub-code rate $R_{l}$ by the equation;

$$
R = \frac{R_{l}}{\sum_{i,j} l_{ij} \alpha_{ij}}, \text{ for any array } l.
$$

Definition 3.2. Let $\mathcal{P}(k)$ be the set of probability distributions over the array $k$ of $\mathcal{U}$, that is, $\alpha \in \mathcal{P}(k)$ if $\alpha = \left( \frac{\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r}}{\alpha_{21}} \right)$, $\alpha_{ij} \geq 0$ and $\sum_{i,j} \alpha_{ij} = 1$. For the group extension $G = Z_{p_{1}^{r}}^{r} \otimes Z_{p_{2}^{r}}$, we define the Group Encoding capacity $C_{G}$ of
the $G$-symmetric channel $(G, Y, p(y|g))$ by:

$$C_G := \max_{\alpha \in P(k)} \left\{ \min_l \left\{ \frac{C_l}{\sum\limits_{i,j} \beta_{ij}} \right\} \right\},$$

with $C_l$ the capacity of the $G(l)$-sub-channel.

**Theorem 3.3.** Let $G$ and $C_G$ be as in Definition 3.2. Let $C$ be a group code with transmission rate $R$. If $R > C_G$ then the error probability of the code is bounded away from zero, that is, there is $A > 0$ such that $P_e(C) > A$.

**Proof.** Let $C$ be a group code with rate $R$ such that $R > C_G$. There is a fixed $\beta_{ij} := \frac{\lambda k_{ij} \log(p_{ij})}{\log(|G|)}$ such that $R = \frac{R_l}{\sum\limits_{i,j} \beta_{ij}}$ for any array $l$. On the other hand

$$C_G = \max_{\alpha \in P(k)} \left\{ \min_l \left\{ \frac{C_l}{\sum\limits_{i,j} \beta_{ij}} \right\} \right\} \geq \min_l \left\{ \frac{C_l}{\sum\limits_{i,j} \beta_{ij}} \right\} = \frac{C_l^*}{\sum\limits_{i,j} \beta_{ij}}$$

for some array $l^*$. Since $R = \frac{R_l}{\sum\limits_{i,j} \beta_{ij}}$ for any array $l$ then $R = \frac{R_{l^*}}{\sum\limits_{i,j} \beta_{ij}}$. Therefore:

$$R_{l^*} > C_l^*.$$  

By the converse of the Shannon’s Coding Theorem, the error probability $p_e(C_{l^*})$ is bounded away from zero, i.e., there is $A > 0$ such that $p_e(C_{l^*}) > A$. By the uniform error property (UEP), $p_e(C) = p_e(C(0))$ and $p_e(C_{l^*}) = p_e(C_{l^*}(0))$, with $0 \in C$ the $N$-tuple $(id, id, \ldots, id)$, with $id$ the identity element of $G$. Therefore

$$p_e(C) = p_e(C|0) \geq p_e(C_{l^*}|0) = p_e(C_{l^*}) > A.$$  

\[\square\]

When the array $l$ is such that $l_{ij} = j$ we have $C_l = C$, which is the capacity of the channel. Then, from Definition 3.2, $C_G \leq C$. Thus, for reliable group codes, $C_G$ can be considered a number in the interval

$$R \leq C_G \leq C.$$  

**Proposition 2.** Let $l^\rho$ be the array \( \left( \frac{1}{l_{21}}, \frac{2}{l_{21}}, \ldots, \frac{\rho - 1}{l_{21}}, \frac{\rho}{l_{21}}, \ldots, \rho \right) \), for some $1 \leq \rho \leq r$. Then

$$\sum\limits_{i,j} \frac{l^\rho_{ij}}{\alpha_{ij}} \leq \frac{C_l}{\sum\limits_{i,j} \frac{\beta_{ij}}{\alpha_{ij}}}$$

for each array $l = (l_{ij})$ such that

$$\max\{l_{11}, l_{12}, \ldots, l_{1r}\} = \rho.$$

**Proof.** Since $G(l^\rho) = G(l)$, also $C_{l^\rho} = C_l$. On the other hand, $\sum\limits_{i,j} l_{ij}^\rho \alpha_{ij} = \sum\limits_{j=1}^{\rho} \alpha_{1j} + \rho \sum\limits_{j=\rho+1}^{r} \frac{\alpha_{1j}}{j} + l_{21} \alpha_{21}$. Then

$$\sum\limits_{i,j} l_{ij}^\rho \alpha_{ij} - \sum\limits_{i,j} l_{ij} \alpha_{ij} = \sum\limits_{j=1}^{\rho} \alpha_{1j} - \sum\limits_{j=\rho+1}^{r} \frac{\alpha_{1j}}{j} + \rho \sum\limits_{j=\rho+1}^{r} \frac{\alpha_{1j}}{j}(\frac{\rho-l_{ij}}{j}) \geq 0.$$  

\[\square\]

The Proposition 2 allows us to simplify the formula of $C_G$ to:

$$C_G = \max_{\rho=1,\ldots,r} \left\{ \frac{C_{l^\rho}}{\sum\limits_{i,j} \frac{l_{ij}^\rho}{\alpha_{ij}}} \right\}.$$
3.2. The $C_G$ for $G = D_4$ and the SPSK-AWGN channel. Let us recall $G(l)$ for the dihedral case is $G(l) = (2Z_2 + 2Z_2, Z_2)$. For instance, for the array $l = (1, 1)$ we have the subgroup $G(l) = (2Z_2 + 2Z_2, Z_2)$. For instance, for the array $l = (1, 1)$ we have the subgroup $G(l) = (2Z_2 + 2Z_2, Z_2)$.

The densities and capacities of the four sub-channels are shown in the Table 2.

These arrays, their matched subgroups $G(l_{ijk})$, and their matched sub-constellations $X(l_{ijk})$, which determine the sub-channels $(G(l_{ijk}), R^2, p(y|x))$, are organized in the Table 1.

| $\rho$ | Array | Sub-group $G(l_{ijk})$ | Sub-Constellation $X(l_{ijk})$ |
|--------|-------|-----------------------|-------------------------------|
| 1      | $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $2Z_4 \otimes \{0\} = \{e, a^2\}$ | $\{x_0, x_1\}$ |
| 2      | $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $2Z_4 \otimes Z_2 = \{e, b, a^2, b^2\}$ | $\{x_0, x_1, x_4, x_5\}$ |
| 1      | $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ | $Z_4 \otimes \{0\} = \{e, a, a^2\}$ | $\{x_0, x_2, x_4, x_6\}$ |
| 1      | $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ | $Z_4 \otimes Z_2 = D_4$ | $\mathcal{X}_8$ |

Table 1. $G(l)$-Symmetric sub-channels the $D_4$-symmetric channel SPSK-AWGN.

Since the sub-channel $(G(l_{ijk}), R^2, p(y|x))$ is $G(l_{ijk})$-Symmetric, its capacity is achieved when the probability distribution over $X(l_{ijk})$ is uniform. With this the probability density of the output is

$$
\lambda_{l_{ijk}}(y) = \frac{1}{|X(l_{ijk})|} \sum_{x \in X(l_{ijk})} p(y|x).
$$

For instance, $\lambda_{l_{111}}(y) = \frac{1}{4}(p(y|x_0) + p(y|x_1) + p(y|x_4) + p(y|x_5))$ and the capacity for the respective sub-channel is $C_{l_{111}} = H(\lambda_{l_{111}}) - H(p_0)$, with

$$
H(\lambda_{l_{111}}) = -\int_{R^2} \lambda_{l_{111}}(y) \log(\lambda_{l_{111}}(y)) dy \quad \text{and} \quad H(p_0) = -\int_{R^2} p(y|x_0) \log(p(y|x_0)) dy.
$$

The densities and capacities of the four sub-channels are shown in the Table 2. Then, the encoding capacity $C_{D_4}$ of the channel is

$$
C_{D_4} = \max_{\alpha} \left\{ \min \left\{ \frac{C_{l_{110}}}{\alpha_{11} + \alpha_{12}}, \frac{C_{l_{111}}}{\alpha_{11} + \frac{\alpha_{12}}{2} + \alpha_{21}}, \frac{C_{l_{120}}}{\alpha_{11} + \alpha_{12}}, C = C_{l_{121}} \right\} \right\}.
$$

By choosing $\alpha_{11} = 0$, $\alpha_{12} = 2/3$, $\alpha_{21} = 1/3$ and combining the formulas (2) and (4) we have

$$
C \geq C_{D_4} \geq \min \left\{ 3C_{l_{110}}, \frac{3C_{l_{111}}}{2}, \frac{3C_{l_{120}}}{2}, C \right\}.
$$
With this shortened notations, the inequation (6) becomes:

\[
3H(\lambda_{l_{11}}) \geq H(p_0) + 2H(\lambda_{l_{121}}).
\]

On the Table 1 it can be seen that the array \(l_{121}\) generates the whole 8PSK-AWGN channel, the \(D_4\)-symmetric channel, hence the density \(\lambda_{l_{121}}\) can be denoted simply as \(\lambda := \lambda_{l_{121}}\). Also, on the same Table 1 it can be seen that the sub-constellation \(\{e, b, a^2, a^2b\} \cong \mathbb{Z}_2^2\) is the input of the sub-channel generated by the array \(\lambda_{l_{111}}\). Since the group \(\mathbb{Z}_2^2\), called the “Klein 4-group”, is denoted by \(V\) in many places of algebraic literature, we denote \(\lambda_V := \lambda_{l_{111}} = \frac{1}{4}(p_0 + p_1 + p_4 + p_5)\). With this shortened notations, the inequation (6) becomes:

\[
3H(\lambda_V) \geq H(p_0) + 2H(\lambda).
\]

4.1. Auxiliar probability vectors \(\nu, \omega_V\) and its entropies. Now we will transform (7) to the following formula (10). For that, consider the probability density \(\lambda_{V_C} := \frac{1}{4}(p_2 + p_3 + p_6 + p_7)\). Since \(\lambda_V + \lambda_{V_C} = 2\lambda\), a binary probability vector \(\nu\) can be defined by

\[
\nu = (\nu_1, \nu_2) := \left(\frac{\lambda_V}{2\lambda}, \frac{\lambda_{V_C}}{2\lambda}\right),
\]
whose entropy is \(H(\nu) = -\nu_1 \log(\nu_1) - \nu_2 \log(\nu_2)\).

On the other hand, the equalities \(p_0 + p_1 + p_4 + p_5 = 4\lambda_V\) and \(p_2 + p_3 + p_6 + p_7 = 4\lambda_{V_C}\) allow us to define two 4-dimensional probability vectors as being

\[
\omega_V := \frac{1}{4\lambda_V}(p_0, p_1, p_4, p_5), \quad \omega_{V_C} := \frac{1}{4\lambda_{V_C}}(p_2, p_3, p_6, p_7),
\]
whose entropies are

\[ H(\omega_V) = -\sum_{k=0,1,4,5} \frac{p_k}{4V_N} \log \left( \frac{p_k}{4V_N} \right) \]

and

\[ H(\omega_{V_{c}}) = -\sum_{k=2,3,6,7} \frac{p_k}{4V_{c}} \log \left( \frac{p_k}{4V_{c}} \right), \]

respectively.

**Lemma 4.1.** The entropies \( H(p_0) \) and \( H(\lambda_V) \) can be expressed as follows

\[
H(p_0) = H(\lambda_V) - 2 + \int_{\mathbb{R}^2} \nu_V H(\omega_V)
\]

and

\[
H(\lambda_V) = H(\lambda) - 1 + \int_{\mathbb{R}^2} \nu H(\nu).
\]

**Proof.** Considering \( H(p_0) = \frac{1}{3} \sum_{k=0,1,4,5} H(p_k) \) and \( H(\lambda_V) = \frac{1}{2} H(\lambda_V) + \frac{1}{2} H(\lambda_{V_c}) \) the proof is the same as of the Lemma 11, page 2045 of [4]. \( \square \)

After Lemma 4.1, the inequality (7) becomes

\[
(10) \quad 2 \int_{\mathbb{R}^2} \lambda(y)H(\nu(y))dy \geq \int_{\mathbb{R}^2} \nu(y)H(\omega_V(y))dy.
\]

4.2. INTEGRATING IN POLAR COORDINATES. In polar coordinates \( y = \rho e^{i\theta} \), (10) is equivalent to:

\[
(11) \quad 2 \int_{0}^{2\pi} \int_{0}^{\pi} \lambda(\rho e^{i\theta})H(\nu(\rho e^{i\theta}))d\theta d\rho \geq \int_{0}^{2\pi} \int_{0}^{\pi} \lambda_V(\rho e^{i\theta})H(\omega_V(\rho e^{i\theta}))d\theta d\rho.
\]

Assuming a finite noise level \( \sigma^2 = N_0/2 \), the entropy \( H(p_0) = \log(2\pi e\sigma^2) \) is finite as well as the other entropies \( H(\lambda) \) and \( H(\lambda_V) \) from (6). Therefore, the integrals of both inequalities (10) and (11) are convergent. Hence, in order to show that \( C_{D_4} \) equals the channel capacity \( C \) it will be sufficient to show, for a fixed \( \rho > 0 \), the inequality

\[
(12) \quad 2 \int_{0}^{2\pi} \lambda(\theta)H(\nu(\theta))d\theta \geq \int_{0}^{2\pi} \nu(\theta)H(\omega_V(\theta))d\theta.
\]

This last inequality (12) is what will be shown in the following Theorem 4.3 which is the main contribution of this paper.

For an arbitrary \( y = \rho e^{i\theta} \in \mathbb{R}^2 \) and a signal point \( x_i = e^{j\varphi_i} \) of the 8PSK constellation, the squared distance \( \|y-x_i\|^2 \) is \( \rho^2 + 1 - 2\rho \cos(\theta - \varphi_i) \), \( \varphi_i = \frac{\pi}{4}, i = 0, 1, \ldots, 7 \).

Thus, the conditional probability \( p_i(y) = p(y|x_i) = \frac{1}{2\pi\sigma^2} e^{-\|y-x_i\|^2/2\sigma^2} \) can be written as \( p_i(y) = K_0 e^{\kappa \cos(\theta - i\pi/4)} \), where \( K_0 = \frac{e^{-1/\sigma^2}}{2\pi\sigma^2} \) and \( \kappa = \frac{\rho^2}{\sigma^2} \).

To express the probability densities \( \lambda_V \), \( \lambda_{V_c} \), and \( \lambda \), from (7) and (8), with concise polar coordinates formulas, we define the periodical functions \( \gamma_{V}(\theta) := \sum_{i=0,1,4,5} e^{\kappa c_i(\theta)}, \gamma_{V_{c}}(\theta) := \sum_{i=2,3,6,7} e^{\kappa c_i(\theta)} \) and \( \gamma(\theta) := \sum_{i=0}^{7} e^{\kappa c_i(\theta)} \), with \( c_i(\theta) := \cos(\theta - i\pi/4) \). Then

\[
\lambda_V(\theta) = \frac{K_0}{4} \gamma_{V}(\theta),
\]

\[
\lambda_{V_c}(\theta) = \frac{K_0}{4} \gamma_{V_{c}}(\theta),
\]

\[
\lambda(\theta) = \frac{K_0}{4} \gamma(\theta).
\]
and
\[ \lambda(\theta) = \frac{K_o}{8} \gamma(\theta). \]

With this, the probability vectors \( \nu, \omega_V \) and \( \omega_{V_C} \), from (8) and (9), in polar coordinates are
\[
\nu(\theta) = \frac{1}{\gamma(\theta)} (\gamma V(\theta), \gamma V_C(\theta)),
\]
(13)
\[
\omega_V(\theta) = \frac{1}{\gamma V(\theta)} \left( e^{\kappa_{C_0}(\theta)}, e^{\kappa_{C_2}(\theta)}, e^{\kappa_{C_4}(\theta)}, e^{\kappa_{C_5}(\theta)} \right),
\]
\[
\omega_{V_C}(\theta) = \frac{1}{\gamma V_C(\theta)} \left( e^{\kappa_{C_2}(\theta)}, e^{\kappa_{C_3}(\theta)}, e^{\kappa_{C_5}(\theta)}, e^{\kappa_{C_7}(\theta)} \right).
\]

**Lemma 4.2.** Some periodical properties:

(i) \( \lambda, \lambda_V \) and \( \lambda_{V_C} \) are periodicals. The period of \( \lambda \) is \( \pi/4 \) and the period of both \( \lambda_V \) and \( \lambda_{V_C} \) is \( \pi \) and \( \lambda_{V_C}(\theta) = \lambda_V(\theta + \pi/2) \). Consequently, both \( \nu_1 \) and \( \nu_2 \) have period \( \pi \) and \( \nu_2(\theta) = \nu_1(\theta + \pi/2) \).

(ii) \( H(\nu(\theta)) \) has period \( \pi/2 \). Consequently, \( \lambda(\theta)H(\nu(\theta)) \) has period \( \pi/2 \).

(iii) Both \( H(\omega_V(\theta)) \) and \( H(\omega_{V_C}(\theta)) \) have period \( \pi \), and \( H(\omega_{V_C}(\theta)) = H(\omega_V(\theta + \pi/2)) \).

**Proof.** It can be verified with the recursive formula \( c_i = -c_{i+4} \), with \( c_i(\theta) = \cos(\theta - i\pi/4) \).

**4.3. The Group Encoding Capacity \( C_{D_4} \) Equals the Channel Capacity \( C \).**

**Lemma 4.3.** Consider the array
\[
\begin{array}{cc}
  a & b \\
  c & d \\
\end{array}
\]
with \( a, b, c, d \) real numbers such that either \( a > d \) and \( c > b \) or \( a < d \) and \( c < b \).

Let \( A \) be the normalized sum-of-rows vector \( A = \frac{1}{a+b+c+d} \) and \( B \), be the normalized sum-of-columns vector \( B = \frac{1}{a+b+c+d} \). Then, the entropy of \( A \) is greater or equal than the entropy of \( B \), that is,
\[ H(A) \geq H(B). \]

**Proof.** If \( t = \frac{a-d}{(a-d)+(c-b)} \) then \( 0 \leq t \leq 1 \) and
\[ (a + b, c + d) = t(a + c, b + d) + (1 - t)(b + d, a + d). \]

Let \( B_p \) be the permutation of the vector \( B \), that is, \( B_p := \frac{1}{a+b+c+d} (b + d, a + c) \).

Then, the vector \( A \) can be expressed as
\[ A = tB + (1 - t)B_p. \]

Since \( H \) is concave and \( H(B) = H(B_p) \) we have
\[ H(A) = H(tB + (1 - t)B_p) \geq tH(B) + (1 - t)H(B_p) = H(B). \]

**Lemma 4.4.** Let \( \nu, \omega_V, \omega_{V_C} \) be as in (13). If \( \theta \in \left[ 0, \frac{\pi}{2} \right] \) then
\[ 4\lambda(\theta)H(\nu(\theta + \pi/4)) \geq \lambda_V(\theta)H(\omega_V(\theta)) + \lambda_{V_C}(\theta)H(\omega_{V_C}(\theta)). \]
Proof. The components of the probability vector \( \nu = (\nu_1, \nu_2) \), for \( \theta + \pi/4 \), are

\[
\nu_1(\theta + \pi/4) = \frac{\gamma_V(\theta + \pi/4)}{\gamma(\theta + \pi/4)} = \frac{1}{\gamma(\theta)} \sum_{i=0,4,7} e^{\kappa_{c_i}(\theta)}
\]

and

\[
\nu_2(\theta + \pi/4) = \frac{\gamma_{\nu_c}(\theta + \pi/4)}{\gamma(\theta + \pi/4)} = \frac{1}{\gamma(\theta)} \sum_{i=1,5,2,6} e^{\kappa_{c_i}(\theta)}.
\]

For any \( \theta \in [0, \pi/4] \), we have the chain of inequalities:

\[
(14) \quad e^{\kappa_{c_0}} \geq e^{\kappa_{c_1}} \geq e^{\kappa_{c_2}} \geq e^{\kappa_{c_3}} \geq e^{\kappa_{c_4}},
\]

and for any \( \theta \in [\pi/4, 7\pi/2] \) the chain is

\[
(15) \quad e^{\kappa_{c_1}} \geq e^{\kappa_{c_0}} \geq e^{\kappa_{c_2}} \geq e^{\kappa_{c_3}} \geq e^{\kappa_{c_4}} \geq e^{\kappa_{c_5}}.
\]

Both chains (14) and (15) are such that the array

\[
\begin{bmatrix}
    e^{\kappa_{c_0}} + e^{\kappa_{c_7}} & e^{\kappa_{c_3}} + e^{\kappa_{c_4}} \\
    e^{\kappa_{c_1}} + e^{\kappa_{c_2}} & e^{\kappa_{c_3}} + e^{\kappa_{c_5}}
\end{bmatrix}
\]

satisfies the conditions of the Lemma 4.3. The normalized sum-of-columns vector is

\[
\nu(\theta + \pi/4) = \frac{1}{\gamma(\theta)} \left( \sum_{i=0,4,7} e^{\kappa_{c_i}(\theta)}, \sum_{i=3,4,6,5} e^{\kappa_{c_i}(\theta)} \right)
\]

which can be decomposed as

\[
B = \frac{1}{\gamma(\theta)} \left( \sum_{i=0,1} e^{\kappa_{c_i}}, \sum_{i=4,5} e^{\kappa_{c_i}} \right) + \frac{1}{\gamma(\theta)} \left( \sum_{i=2,4} e^{\kappa_{c_i}}, \sum_{i=6,3} e^{\kappa_{c_i}} \right)
\]

\[
= \frac{\nu_1}{\gamma_V} \left( \sum_{i=0,1} e^{\kappa_{c_i}}, \sum_{i=4,5} e^{\kappa_{c_i}} \right) + \frac{\nu_2}{\gamma_{\nu_c}} \left( \sum_{i=2,7} e^{\kappa_{c_i}}, \sum_{i=6,3} e^{\kappa_{c_i}} \right)
\]

with 

\[
\omega^{(1)}_V := \frac{1}{\gamma_V} \left( \sum_{i=0,1} e^{\kappa_{c_i}}, \sum_{i=4,5} e^{\kappa_{c_i}} \right) \quad \text{and} \quad \omega^{(1)}_{\nu_c} := \frac{1}{\gamma_{\nu_c}} \left( \sum_{i=2,7} e^{\kappa_{c_i}}, \sum_{i=6,3} e^{\kappa_{c_i}} \right)
\]

are 2-dimensional probability vectors by themselves. Therefore, by the Lemma 4.3 and the concavity of the entropy we have

\[
(16) \quad H(\nu(\theta + \pi/4)) \geq H(\nu_1 \omega^{(1)}_V + \nu_2 \omega^{(1)}_{\nu_c}) \geq \nu_1 H(\omega^{(1)}_V) + \nu_2 H(\omega^{(1)}_{\nu_c}).
\]

The same chains (14) and (15) also allow the array

\[
\begin{bmatrix}
    e^{\kappa_{c_0}} + e^{\kappa_{c_7}} & e^{\kappa_{c_3}} + e^{\kappa_{c_4}} \\
    e^{\kappa_{c_1}} + e^{\kappa_{c_2}} & e^{\kappa_{c_3}} + e^{\kappa_{c_5}}
\end{bmatrix}
\]

to satisfy the condition of the Lemma 4.3. For this array the normalized sum-of-columns vector is

\[
\nu(\theta + \pi/4) = \frac{1}{\gamma(\theta)} \left( \sum_{i=0,5} e^{\kappa_{c_i}}, \sum_{i=4,1,2} e^{\kappa_{c_i}} \right)
\]

This time, after making

\[
\omega^{(2)}_V := \frac{1}{\gamma_V} \left( \sum_{i=0,5} e^{\kappa_{c_i}}, \sum_{i=4,1} e^{\kappa_{c_i}} \right) \quad \text{and} \quad \omega^{(2)}_{\nu_c} := \frac{1}{\gamma_{\nu_c}} \left( \sum_{i=6,7} e^{\kappa_{c_i}}, \sum_{i=6,3} e^{\kappa_{c_i}} \right)
\]

we obtain:

\[
B = \nu_1 \omega^{(2)}_V + \nu_2 \omega^{(2)}_{\nu_c}.
\]
Then, again, by Lemma 4.3 and the concavity of the entropy:

(17) \[ H(\nu(\theta + \pi/4)) \geq H(\nu_1 \omega_V^{(2)} + \nu_2 \omega_V^{(2)}) \geq \nu_1 H(\omega_V^{(2)}) + \nu_2 H(\omega_V^{(2)}). \]

Combining (16) and (17) we have:

(18) \[ 2H(\nu(\theta + \pi/4)) \geq \nu_1 [H(\omega_V^{(1)}) + H(\omega_V^{(1)})] + \nu_2 [H(\omega_V^{(1)}) + H(\omega_V^{(1)})]. \]

Now, by the chain rule of the entropy, see page 22 of [6]:

(19) \[ H(\omega_V) \leq H(\omega_V^{(1)}) + H(\omega_V^{(1)}) \quad \text{and} \quad H(\omega_V) \leq H(\omega_V^{(1)}) + H(\omega_V^{(1)}). \]

Then, after (18) and (19) we have

\[ 2H(\nu(\theta + \pi/4)) \geq \nu_1 (\theta) H(\omega_V(\theta)) + \nu_2 (\theta) H(\omega_V(\theta)), \quad \forall \theta \in \left[0, \frac{\pi}{4}\right]. \]

Finally, using the equation (8) we obtain

\[ 4\lambda(\theta) H(\nu(\theta + \pi/4)) \geq \lambda_V(\theta) H(\omega_V(\theta)) + \lambda_{VC}(\theta) H(\omega_{VC}(\theta)), \quad \forall \theta \in \left[0, \frac{\pi}{4}\right]. \]

On the other hand, for \( \theta \in \left[\frac{\pi}{4}, \frac{\pi}{2}\right] \) the analysis is similar. The chains to be considered are:

\[ e^{\kappa_1} \geq e^{\kappa_2} \geq e^{\kappa_3} \geq e^{\kappa_4} \geq e^{\kappa_5} \geq e^{\kappa_6}, \quad \pi/4 \leq \theta \leq 3\pi/8, \]

\[ e^{\kappa_1} \geq e^{\kappa_2} \geq e^{\kappa_3} \geq e^{\kappa_4} \geq e^{\kappa_5} \geq e^{\kappa_6}, \quad 3\pi/8 \leq \theta \leq \pi/2. \]

Both chains yield the arrays

\[
\begin{align*}
&\begin{bmatrix} e^{\kappa_1} & e^{\kappa_2} & e^{\kappa_3} \\
e^{\kappa_1} & e^{\kappa_2} & e^{\kappa_3} \\
e^{\kappa_1} & e^{\kappa_2} & e^{\kappa_3} \end{bmatrix} & \begin{bmatrix} e^{\kappa_1} & e^{\kappa_2} & e^{\kappa_3} \\
e^{\kappa_1} & e^{\kappa_2} & e^{\kappa_3} \\
e^{\kappa_1} & e^{\kappa_2} & e^{\kappa_3} \end{bmatrix}
\end{align*}
\]

to satisfy the conditions of the Lemma 4.3. Thus

\[ 4\lambda(\theta) H(\nu(\theta + \pi/4)) \geq \lambda_V(\theta) H(\omega_V(\theta)) + \lambda_{VC}(\theta) H(\omega_{VC}(\theta)), \quad \forall \theta \in \left[\frac{\pi}{4}, \frac{\pi}{2}\right]. \]

\[ \square \]

**Main Theorem.** The group encoding capacity \( C_{D_4} \) of the 8PSK-AWGN channel equals the Shannon’s channel capacity.

**Proof.**

\[
\begin{align*}
\int_0^\pi \lambda H(\nu) & = 2 \int_0^{\pi/2} \lambda H(\nu) \\
& = 2 \int_0^{\pi/2} \lambda(\theta) H \left( \nu \left( \theta + \frac{\pi}{4} \right) \right) d\theta \\
& = \frac{1}{2} \int_0^{\pi/2} 4\lambda(\theta) H \left( \nu \left( \theta + \frac{\pi}{4} \right) \right) d\theta \\
& \geq \frac{1}{2} \left( \int_0^{\pi/2} \lambda_V H(\omega_V) + \int_0^{\pi/2} \lambda_{VC} H(\omega_{VC}) \right) \\
& = \frac{1}{2} \left( \int_0^{\pi} \lambda_V H(\omega_V) + \int_0^{\pi} \lambda_V H(\omega_V) \right) \\
& = \frac{1}{2} \int_0^{\pi} \lambda_V H(\omega_V)
\end{align*}
\]

Therefore

\[ 2 \int_0^{2\pi} \lambda(\theta) H(\nu(\theta)) d\theta \geq \int_0^{2\pi} \lambda_V(\theta) H(\omega_V(\theta)) d\theta. \]

\[ \square \]
5. Conclusion

We provided a definition of group encoding capacity $C_G$ for group codes over non-Abelian groups transmitted through symmetric channels and showed that $C_G$ satisfies the converse of the coding theorem of Shannon, that is, we proved that $R < C_G$ is a necessary condition for the Shannon’s coding theorem. After, for the particular case of $G = D_4$ the dihedral group of 8 elements and 8PSK-AWGN channel, we proved that $C_G$ achieves the channel capacity. Some still open problems closely related to this work are:

- It was shown in [4, 17] that the condition $R < C_G$, for Abelian $G$, is also a sufficient condition to prove the coding theorem of Shannon, that is, it was shown that for each $\epsilon > 0$ and each rate $R < C_G$ there is a group code $C$ such that $P_e(C) < \epsilon$. The natural question that arises here is whether $R < C_G$ would also be a sufficient condition for the coding theorem if $G$ is non-Abelian.
- The application of the theory for alternating groups and generalized quaternion groups. Both are non-Abelian and are extensions $G = H \rtimes K$, where $H$ and $K$ are related to cyclic groups. Also the quaternions and alternating groups have simply matrix representations in $O(\mathbb{R}, 2)$, $O(\mathbb{R}, 3)$ and $O(\mathbb{R}, 4)$ [16].
- The study of decoding methods for these class of non-Abelian group codes. Initial references and guides are [14, 15].

Acknowledgments

The author would like to thank the reviewers and editors for their detailed and constructive comments, which substantially improved the presentation of the paper.

References

[1] R. Ahlswede, Group codes do not achieve shannon’s channel capacity for general discrete channels, The Annals of Mathematical Statistics, 42 (1971), 224–240.
[2] J. P. Arpasi, One example of a non-Abelian group code over AWGN channels, Proceedings of the 14th Canadian Workshop on Information Theory, (2015), 115–119.
[3] G. Como, Group codes outperform binary-coset codes on non-binary memoryless channels, IEEE Trans. Inform. Theory, 56 (2010), 4321–4334.
[4] G. Como and F. Fagnani, The capacity of abelian group codes over symmetric channels, IEEE Trans. Inform. Theory, 45 (2009), 3–31.
[5] G. Como and F. Fagnani, Average spectra and minimum distance of low-density parity-check codes over abelian groups, SIAM J. Discrete Math., 23 (2008/09), 19–53.
[6] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd edition, Wiley InterScience, Piscataway, NJ, 2006.
[7] G. D. Forney, Geometrically uniform codes, IEEE Trans. Inform. Theory, 37 (1991), 1241–1260.
[8] R. Gallager, Information Theory and Reliable Communication, Wiley and Sons, 1970.
[9] F. Garin and F. Fagnani, Analysis of serial turbo codes over abelian groups for symmetric channels, SIAM J. Discrete Math., 22 (2008), 1488–1526.
[10] I. N. Herstein, Topics in Algebra, 2nd edition, Wiley and Sons, New York, 1975.
[11] H. J. Kim, J. B. Nation and A. V. Shepler, Group coding with complex isometries, IEEE Trans. Inform. Theory, 61 (2015), 33–50.
[12] H. A. Loeliger, Signal sets matched to groups, IEEE Trans. Inform. Theory, 37 (1991), 1675–1682.
[13] H. A. Loeliger and T. Mittelholzer, Convolutional codes over groups. Codes and complexity, IEEE Trans. Inform. Theory, 42 (1996), 1660–1686.
[14] T. Mittelholzer and J. Lahtonen, Group codes generated by finite reflection groups, IEEE Trans. Inform. Theory, 42 (1996), 519–528.
[15] W. W. Peterson, J. B. Nation and M. P. Fossorier, Reflection group codes and their decoding, *IEEE Trans. Inform. Theory*, 56 (2010), 6273–6293.

[16] J. J. Rotman, *An Introduction to the Theory of the Groups*, 4th edition, Graduate Texts in Mathematics, 148. Springer-Verlag, New York, 1995.

[17] A. G. Sahebi and P. S. Pradhan, Abelian group codes for channel coding and source coding, *IEEE Trans. Inform. Theory*, 61 (2015), 2399–2414.

[18] N. Shulman and M. Feder, Random coding techniques for non-random codes, *IEEE Trans. Inform. Theory*, 45 (1999), 2101–2104.

[19] D. Slepian, Group codes for the gaussian channels, *Bell Systems Technical Journal*, 47 (1968), 575–602.

Received November 2018; revised August 2019.

*E-mail address*: arpas@gmail.com