On the Capacity of Some Symmetric Channels with Non-Abelian Group Codes

Jorge Pedraza Arpasi

***Abstract*—In this work we study group codes over non-Abelian groups which are extensions. Extension of groups is a generalization of semi-direct product and direct product of groups. For channels having as its input alphabet a signal set, one-to-one matched to a non-Abelian group which is an extension, is given a definition of encoding capacity adapted from an existent one that covers the Abelian group case. By using this adapted definition, formulas to compute the encoding capacity of the channel, are derived. Two important examples of application are given.**

Keywords*—*Symmetric channels, non-Abelian group codes, Encoding capacity.

I. Introduction

Group codes provide the possibility to use more spectrally efficient signal constellations while keeping many good qualities of binary-linear codes [1]. Also for channels with certain symmetric properties, like MPSK-AWGN channels, codes over algebraic structures with weaker algebraic structure than fields have better properties [2]. The concept of **group code** over a group G, that will be used in this work, is in the sense of [1], [2], [3], that is, a group code $\mathcal{C}$ is a subgroup of G^N, where $G^N = \overbrace{G \oplus G \oplus \cdots \oplus G}^{N}$ with $\oplus$ representing the direct product of groups. Equivalently the group code $\mathcal{C}$ is the image of an encoder mapping

$$\phi : \mathcal{U} \rightarrow G^N, \tag{1}$$

that must be an injective group homomorphism. Then the uncoded set $\mathcal{U}$ is also a group and isomorphic with $\mathcal{C}$.

In this paper we propose a constructive definition of **encoding capacity** of channels $(\mathcal{X}, \mathcal{Y}, p(y|x))$ having its input alphabet $\mathcal{X}$ bijectively matched with an extension group $G = \mathbb{Z}_{p_1^r}^{\eta} \boxtimes \mathbb{Z}_{p_2}$. Following [1], from which is adapted this definition, this encoding capacity is also called G-capacity and it is denoted by C_G. Roughly speaking the formula to calculate C_G is a minimal choice among weighted capacities, in the Shannon sense, of the sub-channels induced by the sub-groups of G. The channel capacity $C = \max\limits_{p_X(x)} H(Y) - H(Y|X)$, with weight one, is a candidate to be C_G. Then always $C_G \leq C$. When $C_G = C$ then it is said that the encoding capacity **achieves** the channel capacity.

To give examples of application we use two symmetric channels. The first is a three-dimensional channel with group code over the dihedral group of 8 elements. The input alphabet of this channel is a parameter dependent signal set. It is shown that for some values of the parameter the channel capacity is not achieved. The second example is a four-dimensional symmetric channel with group code over the quaternions group of 8 elements.

Federal University of Pampa - UNIPAMPA Alegrete-RS, Brazil, E-mail: jorgearpasi@unipampa.edu.br.

A. Contributions

We summarize the contributions of this paper as follows:

- It is shown that for a group extension $G = H \boxtimes K$ the direct product power can be distributed over the components of the extension, that is, $G^N \cong H^N \boxtimes K^N$ (Section II).
- It is constructed a definition of the encoding capacity, called G-capacity, for group codes over $G = \mathbb{Z}_{p_1^r}^{\eta} \boxtimes \mathbb{Z}_{p_2}$ for channels $(\mathcal{X}, \mathcal{Y}, p(y|x)$ where $\mathcal{X}$ is one-to-one matched with G. This definition is an adaptation from [1] which is for the Abelian group case (Section III).

II. Direct product power of extension of groups

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 [4]. Since each element $g \in G$ is in a unique lateral class $Hk \in G/H$ then g can be written as a "ordered pair" $g = hk$. This determines a group isomorphism between G and $H \times K$. The semi-direct product and direct product of groups are particular cases of extension of groups. In this article the extension H by K will be represented by the symbol "box-times": $H \boxtimes K$. The group operation on these pairs are performed with the rule $g_1 g_2 = (h_1 k_1)(h_2 k_2) = h_1(k_1 h_2 k_1^{-1}) k_1 k_2$, where $k_1 h_2 k_1^{-1}$, denoted in the literature about algebra as $h_2^{k_1}$, is in H and $k_1 k_2 \in K$. It can be shown that when $h_2^{k_1} \neq h_2$, for some h_2 or else some k_1, then $G \cong H \boxtimes K$ is a non-Abelian group.

Proposition 1: For an integer $N \geq 1$, if $G = H \boxtimes K$ then

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

Proof: For the case $N = 2$, define $\varphi : G^2 \rightarrow (G/H)^2$ as $\varphi(g_1, g_2) = (g_1 H, g_2 H)$. Then $\varphi((g_{11}, g_{12}) * (g_{21}, g_{22})) = \varphi(g_{11} g_{21}, g_{12} g_{22}) = (g_{11} g_{21} H, g_{12} g_{22} H)$. On the other side $\varphi(g_{11}, g_{12}) * \varphi(g_{21}, g_{22}) = (g_{11} H, g_{12} H) * (g_{21} H, g_{22} H) = (g_{11} g_{21} H, g_{12} g_{22} H)$, which shows that φ is a group homomorphism. Clearly φ is surjective with kernel $\ker(\varphi) = H^2$. Therefore, H^2 is a normal subgroup of $G^2 = (H \boxtimes K)^2$ and by the fundamental theorem of group homomorphisms, $G^2/H^2 \cong (G/H)^2 \cong K^2$. For $N > 2$, suppose $(H \boxtimes K)^{N-1} \cong H^{N-1} \boxtimes K^{N-1}$. Then defining $\varphi : G^N \rightarrow (G/H)^N$ as $\varphi(g_1, g_2) = (g_1 H^{N-1}, g_2 H)$, where $g_1 \in G^{N-1}$ and $g_2 \in G$, we can show, analogously to the case $N = 2$, that φ is a surjective group homomorphism with kernel H^N. Therefore H^N is a normal subgroup of $G^N = (H \boxtimes K)^N$ and $G^N/H^N \cong (G/H)^N \cong K^N$. ■

Some important finite non-Abelian groups are extensions $H \boxtimes K$, where both H and K are Abelian or else cyclic. For example, the dihedral group D_n is an extension $D_n = \mathbb{Z}_n \boxtimes \mathbb{Z}_2$, where $\mathbb{Z}_n$ is the cyclic group $\{0, 1, \ldots, n-1\}$. The generalized quaternions Q_{2^n} is also an extension $Q = \mathbb{Z}_{2^{n-1}} \boxtimes \mathbb{Z}_2$. Also the alternant group A_4, which is non-abelian and has 12 elements is an extension $\mathbb{Z}_2^2 \boxtimes \mathbb{Z}_3$. These and other extensions have representations in the families of orthogonal matrices $\mathrm{O}(2,\mathbb{R})$, $\mathrm{O}(3,\mathbb{R})$, $\mathrm{O}(4,\mathbb{R}) \cong \mathrm{O}(2,\mathbb{C})$, where $\mathbb{R}$ is the real field and $\mathbb{C}$ is the complex field. So, this matrix representation possibility together with the distribution of the exponent $(H \boxtimes K)^N \cong H^N \boxtimes K^N$ makes that group extension may be very suitable for group codes over channels whose input alphabet is matched to G.

III. Encoding capacity of channels with group codes over extensions

In this section we study group codes over G and channels $(\mathcal{X}, \mathcal{Y}, p(y|x))$ such that: **1)** G and $\mathcal{X}$ are one-to-one matched and **2)** G is an extension $G = \mathbb{Z}_{p_1^r}^{\eta} \boxtimes \mathbb{Z}_{p_2}$, where p_1 and p_2 are prime numbers that do not need to be different.

If $G = \mathbb{Z}_{p_1^r}^{\eta} \boxtimes \mathbb{Z}_{p_2}$, by the Proposition 1, G^N must have the form:

$$G^N = \mathbb{Z}_{p_1^r}^{N\eta} \boxtimes \mathbb{Z}_{p_2}^N. \tag{2}$$

From here, the group code $\mathcal{C}$ or else the uncoded group $\mathcal{U}$ must have the structure:

$$\mathcal{U} = \left(\mathbb{Z}_{p_1}^{k_{11}} \oplus \mathbb{Z}_{p_1^2}^{k_{12}} \oplus \cdots \oplus \mathbb{Z}_{p_1^r}^{k_{1r}}\right) \boxtimes \mathbb{Z}_{p_2}^{k_{21}},$$

where $k_{11} + k_{12} + \cdots + k_{1r} \leq N\eta$ and $k_{21} \leq N$.

Then each subgroup $\mathcal{U}$ of G^N is determined by the array $\boldsymbol{k}$ = $\begin{pmatrix} k_{11}, k_{12}, \ldots, k_{1r} \\ k_{21} \end{pmatrix}$.

Let $(\mathcal{X}, \mathcal{Y}, p(y|x))$ be the channel with $\mathcal{X}$ one-to-one matched with G. Then, as it was said before, the channel can be represented by $(G, \mathcal{Y}, p(y|g))$. The subgroups of G will induce sub-channels that will have their respective subgroup codes of $\mathcal{U}$. To show how are these subgroup codes over these sub-channels it will be used arrays of integers $\boldsymbol{l}$= $\begin{pmatrix} l_{11}, l_{12}, \ldots, l_{1r} \\ l_{21} \end{pmatrix}$ such that $l_{ij} \leq j$ for all i, j. Then, let $\mathcal{U}(\boldsymbol{l})$ and $G(\boldsymbol{l})$ be groups defined by the Following formulas:

$$\mathcal{U}(\boldsymbol{l}) = \left[\bigoplus_{j=1}^{r} p_1^{j-l_{1j}} \mathbb{Z}_{p_1^j}^{k_{1j}}\right] \boxtimes p_2^{1-l_{21}} \mathbb{Z}_{p_2}^{k_{21}} \tag{3}$$

and

$$G(\boldsymbol{l}) = \left[\sum_{j=1}^{r} p_1^{j-l_{1j}} H_{(p_1^j)}\right] \boxtimes p_2^{1-l_{21}} \mathbb{Z}_{p_2}, \tag{4}$$

where $H = \mathbb{Z}_{p_1^r}^{\eta}$ and $H_{(p_1^j)}$ is the subgroup of elements of H with order p_1^j.

Since each $p_i^{j-l_{ij}} \mathbb{Z}_{p_i^j}^{k_{ij}} \cong \mathbb{Z}_{p_i^{l_{ij}}}^{k_{ij}}$, then $\mathcal{U}(\boldsymbol{l}) \cong \left[\bigoplus_{j=1}^{r} \mathbb{Z}_{p_1^{l_{1j}}}^{k_{1j}}\right] \boxtimes \mathbb{Z}_{p_2^{l_{21}}}^{k_{21}}$ which shows that $\mathcal{U}(\boldsymbol{l})$ is a subgroup of $\mathcal{U}$. Moreover if $l_{ij} = j$ for all i, j then $\mathcal{U}(\boldsymbol{l}) = \mathcal{U}$. On the other hand, for $G(\boldsymbol{l})$, we have that $H_{(p_1^j)} = p_1^{r-j} \mathbb{Z}_{p_1^r}^{\eta}$, then $p_1^{j-l_{1j}} H_{(p_1^j)} = p_1^{r-l_{1j}} \mathbb{Z}_{p_1^r}^{\eta} \cong \mathbb{Z}_{p_1^{l_{1j}}}^{\eta}$. Hence $\sum_{j=1}^{r} p_1^{j-l_{1j}} H_{(p_1^j)} \cong \mathbb{Z}_{p_1^{l_{1m}}}^{\eta}$, where $l_{1m} = \max\{l_{11}, l_{12}, \ldots, l_{1r}\}$. With this $G(\boldsymbol{l}) \cong \mathbb{Z}_{p_1^{l_{1m}}}^{\eta} \boxtimes \mathbb{Z}_{p_2^{l_{21}}}$ which shows that it is a subgroup of G. Therefore, $\mathcal{U}(\boldsymbol{l})$ is a subgroup code over the sub-channel $(G(\boldsymbol{l}), \mathcal{Y}, p(y|g))$, that is:

$$\mathcal{U}(\boldsymbol{l}) \subset G(\boldsymbol{l})^N. \tag{5}$$

The encoding rates of $\mathcal{U}(\boldsymbol{l})$ and $\mathcal{U}$ can be calculated by

$$R_{\boldsymbol{l}} = \frac{\log(|\mathcal{U}(\boldsymbol{l})|)}{N} = \frac{1}{N} \sum_{j=1}^{r_i} \sum_{i=1}^{2} l_{ij} k_{ij} \log(p_i) \tag{6}$$

and

$$R = \frac{1}{N} \sum_{j=1}^{r_i} \sum_{i=1}^{2} j k_{ij} \log(p_i), \tag{7}$$

where $r_1 = r$ and $r_2 = 1$.

If $\alpha_{ij} = \frac{j k_{ij} \log(p_i)}{\log(|\mathcal{U}|)}$ then $\sum_{i,j} \alpha_{ij} = 1$ and $k_{ij} = \frac{\alpha_{ij}}{j \log(p_i)} \log(|\mathcal{U}|)$. Thus,

$$R_{\boldsymbol{l}} = R \sum_{i,j} \frac{l_{ij}}{j} \alpha_{ij}.$$

Let $C_{\boldsymbol{l}}$ be the capacity of $(G(\boldsymbol{l}), \mathcal{Y}, p(y|g))$, then $R \sum_{i,j} \frac{l_{ij}}{j} \alpha_{ij} = R_{\boldsymbol{l}} \leq C_{\boldsymbol{l}}$. Therefore:

$$R \leq \min_{\boldsymbol{l}} \left\{ \frac{C_{\boldsymbol{l}}}{\sum_{i,j} \frac{l_{ij}}{j} \alpha_{ij}} \right\}. \tag{8}$$

Finally considering the family of probability arrays (α_{ij}) where $i = 1, 2$ and $j = 1, 2, \ldots, r_i$ such that $\sum_{i,j} \alpha_{ij} = 1$, we make the adaptation, for the extension group $\mathbb{Z}_{p_1^r}^{\eta} \boxtimes \mathbb{Z}_{p_2}$ case, of the Definition 20 of [1]:

Definition 1: For the extension $G = \mathbb{Z}_{p_1^r}^{\eta} \boxtimes \mathbb{Z}_{p_2}$, the G-encoding capacity of the G-symmetric channel $(G, \mathcal{Y}, p(y|x)$, $x \in G$, is:

$$C_G = \max_{(\alpha_{ij})} \min_{\boldsymbol{l}} \left\{ \frac{C_{\boldsymbol{l}}}{\sum_{i,j} \frac{l_{ij}}{j} \alpha_{ij}} \right\}. \tag{9}$$

□

Let C be the capacity of the channel, that is, C is the maximal mutual information $H(Y) - H(Y|X)$. For the maximal case of $\boldsymbol{l}$ where $l_{ij} = j$, for all i, j, we have $G_{\boldsymbol{l}} = G$ and the respective capacities are the same: $C_{\boldsymbol{l}} = C$. Hence $\min_{\boldsymbol{l}} \left\{ \frac{C_{\boldsymbol{l}}}{\sum_{i,j} \frac{l_{ij}}{j}\alpha_{ij}} \right\} \leq C$. Therefore;

$$C_G \leq C. \tag{10}$$

When $C_G = C$ then it is said that the G-encoding capacity of the G-symmetric channel **achieves** the capacity of the Channel [1].

Lemma 1: Let $\boldsymbol{l}^\rho$ be the array $\begin{pmatrix} 1, 2, \ldots, \rho-1, \rho, \rho, \ldots, \rho \\ l_{21} \end{pmatrix}$, for some $1 \leq \rho \leq r$. Then $\frac{C_{\boldsymbol{l}^\rho}}{\sum_{i,j} \frac{l^\rho_{ij}}{j}\alpha_{ij}} \leq \frac{C_{\boldsymbol{l}}}{\sum_{i,j} \frac{l_{ij}}{j}\alpha_{ij}}$ for each array $\boldsymbol{l} = (l_{ij})$ such that $\max\{l_{11}, l_{12}, \ldots, l_{1r}\} = \rho$.

Proof: Since each subgroup $p_1^{j-l_{1j}} H_{(p_1^j)}$ from (4) is equal to $p_1^{r-l_{1j}} \mathbb{Z}_{p_1^r}$ then $G(\boldsymbol{l}^\rho) = G(\boldsymbol{l})$. Thus the capacities of the sub-channels determined by these subgroups must be also equal, that is, $C_{\boldsymbol{l}^\rho}$ and $C_{\boldsymbol{l}}$.

On the other hand, $\sum_{i,j} \frac{l^\rho_{1j}}{j}\alpha_{ij} = \sum_{j=1}^{\rho} \alpha_{1j} + \rho \sum_{j=\rho+1}^{r} \frac{\alpha_{1j}}{j} + l_{21}\alpha_{21}$. Then, $\sum_{i,j} \frac{l^\rho_{ij}}{j}\alpha_{ij}$ - $\sum_{i,j} \frac{l_{ij}}{j}\alpha_{ij} = \sum_{j=1}^{\rho} \alpha_{1j}(1 - \frac{l_{1j}}{j}) + \rho \sum_{j=\rho+1}^{r} \alpha_{1j}(\frac{\rho - l_{1j}}{j}) \geq 0.$ ∎

The Lemma 1 allow us to simplify the formula (9) to:

$$C_G = \max_{(\alpha_{ij})} \min_{\rho=\{1,2,\ldots,r\}} \left\{ \frac{C_{\boldsymbol{l}^\rho}}{\sum_{i,j} \frac{l^\rho_{ij}}{j}\alpha_{ij}} \right\}. \tag{11}$$

IV. Two examples of non-Abelian group codes over symmetric channels

Given a group G and a set $\mathcal{X}$, it is said that G acts over $\mathcal{X}$ when **a)** $g_1(g_2x) = g_1g_2(x)$ for all $g_1, g_2 \in G$ and for all $x \in X$, **b)** $ex = x$, for all $x \in \mathcal{X}$, e is the identity element of G [5], [4]. The action is **transitive** when for all $x_1, x_2 \in \mathcal{X}$ there is $g \in G$ such that $x_2 = gx_1$. Forney in [3] calls a signal set $\mathcal{X}$ as *geometrically uniform set* when $\mathcal{X}$ enjoys the transitive action of a group G of isometric matrices. The action of G on $\mathcal{X}$ is said to be **simply transitive** if for all $x_1, x_2 \in \mathcal{X}$ there is an unique $g \in G$ such that $x_2 = gx_1$. Another type of action is the so called **isometric action**. For the case where $\mathcal{X}$ is a continuous subset of $\mathbb{R}^n$, it is said that G acts isometrically on $\mathcal{X}$ when it preserves Euclidean distances, that is, $\|x\| = \|gx\|$, for all $g \in G$ and for all $x \in \mathcal{X}$. For the case where $\mathcal{X}$ is a finite set, any group action is isometric action [1].

Definition 2: Let G be a group. Let $\mathcal{X}$ and $\mathcal{Y}$ be sets with joint probability distribution $p_{XY}(x, y)$ and conditional probability distribution $p_{Y|x}(y)$ denoted as $p(y|x)$. A memoryless channel $(\mathcal{X}, \mathcal{Y}, p(y|x))$ is said to be G-symmetric if

- G acts simply transitively on $\mathcal{X}$,
- G acts isometrically on $\mathcal{Y}$,
- $p(y|x) = p(gy|gx)$ for all $g \in G$, for all $x \in \mathcal{X}$, for all $y \in \mathcal{Y}$. [1]

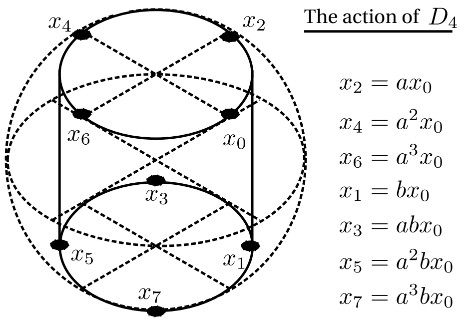

Fig. 1. The tri-dimensional constellation $\mathcal{X}_8^\beta$ and the action of the D_4 group

The simply transitive action of G over $\mathcal{X}$ implies that G and $\mathcal{X}$ are one-to-one matched, thus we can use the formulas (9) or else its simplified version (11) to compute the G-capacity of G-symmetric channels.

A. The dihedral case 3D

The group of symmetries of the square D_4 is a non-Abelian group that is an extension $\mathbb{Z}_4 \boxtimes \mathbb{Z}_2$ where $\mathbb{Z}_4 = \{a, a^2, a^3, e\}$ and $\mathbb{Z}_2 = \{b, e\}$. The generators a of $\mathbb{Z}_4$ and b of $\mathbb{Z}_2$ also generate D_4 with the group operation given by $(a^{h_1}b^{k_1}) * (a^{h_2}b^{k_2}) = a^{h_1+3^{k_1}h_2}b^{k_1k_2}$. For instance $(a^2b) * (ab) = a^{2+3^1.1}b^{1+1} = ae = a$. Thus, $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. This finite group has a representation in $\mathrm{O}(3, \mathbb{R})$, the set of orthogonal matrices of the space $\mathbb{R}^3$, via the mapping $a \mapsto \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $b \mapsto \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & -\sqrt{2} \end{pmatrix}$. With this representation is easy to verify that D_4 acts simply transitively on the tri-dimensional signal set $\mathcal{X}_8^\beta$ defined by:

$$\mathcal{X}_8^\beta = \left\{ x_k = \left(\sqrt{\tfrac{1}{1+\beta^2}} e^{jk\pi/4}, \sqrt{\tfrac{\beta^2}{1+\beta^2}} (-1)^k \right); \quad k = 0, 1, 2, \ldots, 7; \quad 0 \leq \beta < \infty; \quad j = \sqrt{-1} \right\}. \tag{12}$$

Alternatively, this constellation also can be described in terms of spherical coordinates as;

$$\mathcal{X}_8^\beta = \left\{ (\cos\varphi_k \cos\theta,\ \sin\varphi_k \cos\theta,\ (-1)^k \sin\theta) \quad \varphi_k = \tfrac{k\pi}{4}; \quad k = 0, 1, 2, \ldots, 7; \quad 0 \leq \theta < \tfrac{\pi}{2} \right\}, \tag{13}$$

where $\theta = \arctan(\beta)$. The Fig. 1 shows this constellation for the case $\beta = 1$ or else $\theta = \pi/4$. For the extreme case $\beta = 0$ the 3-D constellation $\mathcal{X}_8^\beta$ turns into the 8PSK constellation on the XY-plane. On the other side, when $\beta \to \infty$ the constellation $\mathcal{X}_8^\beta$ approaches to $\{(0, 0, 1), (0, 0, -1)\}$. If the signal set $\mathcal{X}_8^\beta$ is transmitted over an AWGN channel where the noise has probability density $p(y) = \frac{1}{(2\pi)^{3/2}\sigma^3} e^{-\frac{\|y\|^2}{2\sigma^2}}$, $y \in \mathbb{R}^3$, then the conditional probability transitions of the channel are

$$p(y|x_k) = \frac{1}{(2\pi)^{3/2}\sigma^3} \exp\left(-\frac{\|y - x_k\|^2}{2\sigma^2}\right)$$

Using again the matrix representation of D_4 it can be shown that $p(gy|gx_k) = p(y|x_k)$ for all $g \in D_4$, and $x_k \in \mathcal{X}_8^\beta$, $y \in \mathbb{R}^3$. Therefore this $\mathcal{X}_8^\beta$ is a D_4-symmetric channel.

By implementing the formula (4) for the generic array $\boldsymbol{l} = \begin{pmatrix} l_{11}, l_{12} \\ l_{21} \end{pmatrix}$ results the generic subgroup $G(\boldsymbol{l}) = (2^{2-l_{11}}\mathbb{Z}_2 + 2^{2-l_{12}}\mathbb{Z}_4) \boxtimes 2^{1-l_{21}}\mathbb{Z}_2$.

Particularly, the array $(l_{ij}) = \begin{pmatrix} 1 & 1 \\ 1 & \end{pmatrix}$ yields the subgroup $G(\boldsymbol{l}) = (2\mathbb{Z}_2 + 2\mathbb{Z}_4) \boxtimes \mathbb{Z}_2 = 2\mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = \{e, a^2\}\gamma\{e, b\} = \{e, b, a^2, a^2b\}$. The sub-constellation matched to this subgroup is $\{x_0, x_1, x_4, x_5\}$.

Analogously the array $\boldsymbol{l} = \begin{pmatrix} 1 & 1 \\ 0 & \end{pmatrix}$ yields the subgroup $(2\mathbb{Z}_2 + 2\mathbb{Z}_4) \boxtimes 2\mathbb{Z}_2 = 2\mathbb{Z}_4 \boxtimes \{e\} = \{e, a^2\} \boxtimes \{e\} = \{e, a^2\}$ matched to the sub-constellation $\{x_0, x_4\}$. Then, by the Lemma 1, to estimate the G-capacity with the formula (11) it will be sufficient to consider the arrays $\boldsymbol{l}_{110} = \begin{pmatrix} 1 & 1 \\ 0 & \end{pmatrix}$, $\boldsymbol{l}_{111} = \begin{pmatrix} 1 & 1 \\ 1 & \end{pmatrix}$, $\boldsymbol{l}_{120} = \begin{pmatrix} 1 & 2 \\ 0 & \end{pmatrix}$ and $\boldsymbol{l}_{121} = \begin{pmatrix} 1 & 2 \\ 1 & \end{pmatrix}$. These arrays with its matched subgroups $G(\boldsymbol{l}_{ijk})$, and its matched sub-constellations $\mathcal{X}(\boldsymbol{l}_{ijk})$ are organized in the Table I.

ρ	Array $\boldsymbol{l}_{ijk}$	Sub-group $G(\boldsymbol{l}_{ijk})$	Sub-Constellation $\mathcal{X}(\boldsymbol{l}_{ijk})$
1	$\begin{pmatrix} 1 & 1 \\ 0 & \end{pmatrix}$	$2\mathbb{Z}_4 \boxtimes \{0\} = \{e, a^2\}$	$\{x_0, x_4\}$
	$\begin{pmatrix} 1 & 1 \\ 1 & \end{pmatrix}$	$2\mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = \{e, b, a^2, a^2b\}$	$\{x_0, x_1, x_4, x_5\}$
2	$\begin{pmatrix} 1, 2 \\ 0 \end{pmatrix}$	$\mathbb{Z}_4 \boxtimes \{0\} = \{e, a, a^2, a^3\}$	$\{x_0, x_2, x_4, x_6\}$
	$\begin{pmatrix} 1 & 2 \\ 1 & \end{pmatrix}$	$\mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = D_4$	$\mathcal{X}$

TABLE I. $\boldsymbol{l}_{ijk}$ ARRAYS, $G(\boldsymbol{l}_{ijk})$ SUBGROUPS AND $\mathcal{X}(\boldsymbol{l}_{ijk})$ SUB-CONSTELLATIONS FOR THE D_4-SYMMETRIC CHANNEL

Then applying the formula (11), the G-capacity of this channel is;

$$C_{D_4} = \max_{(\alpha_{ij})} \min \left\{ \frac{C_{\boldsymbol{l}_{110}}}{\alpha_{11} + \frac{\alpha_{12}}{2}}, \frac{C_{\boldsymbol{l}_{111}}}{\alpha_{11} + \frac{\alpha_{12}}{2} + \alpha_{21}}, \frac{C_{\boldsymbol{l}_{120}}}{\alpha_{11} + \alpha_{12}}, C = C_{\boldsymbol{l}_{121}} \right\}; \quad (14)$$

where $C_{\boldsymbol{l}_{ijk}}$ is the capacity of the sub-channel which has $\mathcal{X}_{\boldsymbol{l}_{ijk}}$ as its input alphabet.

By choosing $\alpha_{11} = 0$, $\alpha_{12} = 2/3$, and for $\alpha_{21} = 1/3$ and combining the formulas (10) and (14) we obtain

$$C \geq C_{D_4} \geq \min\{3C_{\boldsymbol{l}_{110}}, \tfrac{3C_{\boldsymbol{l}_{111}}}{2}, \tfrac{3C_{\boldsymbol{l}_{120}}}{2}, C\}. \quad (15)$$

Since the channel is symmetric the capacities $C_{\boldsymbol{l}_{ijk}}$ can be computed with the formula $H(\lambda_{\boldsymbol{l}_{ijk}}) - H(p_0)$, where $H(\lambda_{\boldsymbol{l}_{ijk}})$ is the entropy of the random variable Y of the output of the sub-channel with probability density $\lambda_{\boldsymbol{l}_{ijk}}(y)$, $y \in \mathbb{R}^3$, and $H(p_0) = H(Y|X = x_0) = -\int_{\mathbb{R}^3} p(y|x_0)\log(p(y|x_0))dy = 3\log(\sqrt{2\pi e}\sigma)$, where $\log = \log 2$. Thus we can write

$$C_{\boldsymbol{l}_{ijk}} = H(\lambda_{\boldsymbol{l}_{ijk}}) - 3\log(\sqrt{2\pi e}\sigma). \quad (16)$$

All the probability density functions $\lambda_{\boldsymbol{l}}$ to compute the capacities of the sub-channels are showed in the Table II

$\boldsymbol{l}_{ijk}$	$\lambda_{\boldsymbol{l}_{ijk}}$
$\boldsymbol{l}_{110}$	$\lambda_{\boldsymbol{l}_{110}} = \frac{1}{2}(p_0 + p_4)$
$\boldsymbol{l}_{111}$	$\lambda_{\boldsymbol{l}_{111}} = \frac{1}{4}(p_0 + p_1 + p_4 + p_5)$
$\boldsymbol{l}_{120}$	$\lambda_{\boldsymbol{l}_{120}} = \frac{1}{4}(p_0 + p_2 + p_4 + p_6)$
$\boldsymbol{l}_{121}$	$\lambda_{\boldsymbol{l}_{121}} = \frac{1}{8}(p_0 + p_1 + \cdots + p_7) = \lambda$

TABLE II. OUTPUT PROBABILITY DENSITIES OF THE SUB-CHANNELS OF THE D_4-SYMMETRIC CHANNEL, WHERE $p_k := p(y|x_k)$

The implementation of the formula (16) with the **triplequad** command of the software Octave [6] to compute the capacities of (15), shows that the achievement of the channel capacity depends on β. For some β_0 such that $0.32 < \beta_0 < 0.72$, if $\beta < \beta_0$ then the channel capacity is achieved, on the contrary, if $\beta > \beta_0$ then the channel capacity is not achieved. Some results, for fixed noise level $\sigma = 0.5$, of these computations are shown in the Table III. For instance, for $\beta = 1$ the channel capacity is not achieved: $3H(\lambda_{\boldsymbol{l}_{120}}) - 2H(\lambda) = 2.6603 < H(p_0) = 3.1423$ that means $\frac{3C_{\boldsymbol{l}_{120}}}{2} < C$. It is interesting notice the behavior of the entropies as $\beta \to +\infty$. $H(\lambda_{\boldsymbol{l}_{110}}) \to H(\lambda_{\boldsymbol{l}_{120}})^- \to H(p_0)^+$ whereas $H(\lambda_{\boldsymbol{l}_{111}})^- \to H(\lambda)^-$. On the other hand for $\beta = 0$ the $\mathcal{X}_8^\beta$ signal set becomes the 8PSK constellation. In [7], by using the **dblquad** command of Octave, it was shown that the 8PSK-AWGN channel with group code over D_4 achieves the channel capacity.

$H(\boldsymbol{l}_{ijk})$ \ β	0.32	0.72	1.00	1.3	3.07
$H(\lambda_{\boldsymbol{l}_{121}}) = H(\lambda)$	4.7709	4.8902	4.8323	4.6903	4.2731
$H(\lambda_{\boldsymbol{l}_{120}})$	4.5040	4.2875	4.1083	3.8831	3.3825
$H(\lambda_{\boldsymbol{l}_{111}})$	4.4523	4.6046	4.6113	4.5498	4.2545
$H(\lambda_{\boldsymbol{l}_{110}})$	4.0214	3.9424	3.8580	3.7305	3.3630

TABLE III. ENTROPIES OF THE OUTPUT RV OF THE SUB-CHANNELS OF THE D_4-CHANNEL WITH CONSTELLATION $\mathcal{X}_8^\beta$ AND FIXED NOISE LEVEL $\sigma = 0.5$

B. The quaternions case 4D

The group of quaternions Q_8 is also a non-Abelian group that can be expressed as an extension $\mathbb{Z}_4 \boxtimes \mathbb{Z}_2$. If a is the generator of $\mathbb{Z}_4$ and b is the generator of $\mathbb{Z}_2$, then the group operation of Q_8 is given by $(a^{h_1}b^{k_1}) * (a^{h_2}b^{k_2}) = a^{h_1+3^{k_1}h_2+\xi(k_1,k_2)}b^{k_1k_2}$, where $\xi(k_1, k_2) = \begin{cases} 0 \text{ if } k_1 + k_1 \leq 1 \\ 2 \text{ if } k_1 + k_2 = 2. \end{cases}$. For instance $(a^2b) * (ab) = a^{2+3^1.1+2}b^{1+1} = a^3e = a^3$. In this way, the complete list of elements is $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. This finite group has a representation in $\mathrm{O}(2, \mathbb{C}) \cong \mathrm{O}(4, \mathbb{R})$ via the mapping

$a \mapsto \begin{pmatrix} j & 0 \\ 0 & -j \end{pmatrix}$, where $j = \sqrt{-1} \in \mathbb{C}$, and $b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, where $1 \in \mathbb{R}$. Choosing the initial point $x_0 = (1,0) \in \mathbb{C}^2$ we have that $ax_0 = (j,0)$, $bx_0 = (0,1)$ and so on. The complete matching list determined by the simply transitive action of Q_8 over $\mathcal{X}$ is shown in the table IV.

Q_8	$\overset{gx_0}{\mapsto}$	$\mathcal{X}$	Q_8	$\overset{gx_0}{\mapsto}$	$\mathcal{X}$
e	$\mapsto$	$x_0 = (1,0)$	a	$\mapsto$	$x_1 = (j,0)$
a^2	$\mapsto$	$x_2 = (-1,0)$	a^3	$\mapsto$	$x_3 = (-j,0)$
b	$\mapsto$	$x_4 = (0,-1)$	ab	$\mapsto$	$x_5 = (0,j)$
a^2b	$\mapsto$	$x_6 = (0,1)$	a^3b	$\mapsto$	$x_7 = (0,-j)$

TABLE IV. THE ACTION OF Q_8 OVER THE SIGNAL SET $\mathcal{X} \subset \mathbb{C}^2$

If the signal set $\mathcal{X}$ is transmitted over an AWGN channel where the noise has the probability density $p(y) = \frac{1}{4\pi^2\sigma^4} e^{-\frac{\|y\|^2}{2\sigma^2}}$, $y \in \mathbb{C}^2 \cong \mathbb{R}^4$, then the conditional probability transitions of the channel are

$$p(y|x_k) = \frac{1}{4\pi^2\sigma^4} \exp\left(-\frac{\|y - x_k\|^2}{2\sigma^2}\right).$$

Clearly $p(y|x_k) = p(gy|gx_k)$. Therefore we have that this $\mathcal{X}$-AWGN channel is a Q_8-symmetric channel.

Applying the formula (4) for $\boldsymbol{l}_{111} = \begin{pmatrix} 1 & 1 \\ 1 & \end{pmatrix}$ we have $G(\boldsymbol{l}_{111}) = (2\mathbb{Z}_2 + 2\mathbb{Z}_4) \boxtimes \mathbb{Z}_2 = 2\mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = \{e, a^2\} \boxtimes \{e, b\} = \{e, b, a^2, a^2b\}$. The sub-constellation matched to this subgroup is $\{x_0, x_4, x_2, x_6\}$. As in for the D_4 case the subgroups and sub-constellations that allow the computation of the Q_8-capacity are organized in the Table V.

ρ	Array $\boldsymbol{l}_{ijk}$	Sub-group $Q_8(\boldsymbol{l}_{ijk})$	Sub-Constellation $\mathcal{X}(\boldsymbol{l}_{ijk})$
1	$\begin{pmatrix} 1,1 \\ 0 \end{pmatrix}$	$2\mathbb{Z}_4 \boxtimes \{0\} = \{e, a^2\}$	$\{x_0, x_2\}$
	$\begin{pmatrix} 1,1 \\ 1 \end{pmatrix}$	$2\mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = \{e, b, a^2, a^2b\}$	$\{x_0, x_4, x_2, x_6\}$
2	$\begin{pmatrix} 1,2 \\ 0 \end{pmatrix}$	$\mathbb{Z}_4 \boxtimes \{0\} = \{e, a, a^2, a^3\}$	$\{x_0, x_1, x_2, x_3\}$
	$\begin{pmatrix} 1,2 \\ 1 \end{pmatrix}$	$\mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = Q_8$	$\mathcal{X}$

TABLE V. $\boldsymbol{l}_{ijk}$ ARRAYS, $Q_8(\boldsymbol{l}_{ijk})$ SUBGROUPS AND $\mathcal{X}(\boldsymbol{l}_{ijk}) \subset \mathbb{C}^2$ SUB-CONSTELLATIONS FOR THE Q_8-SYMMETRIC CHANNEL

Then by same methodology applied in the D_4 case, it is obtained:

$$C \geq C_{Q_8} \geq \min\{3C_{\boldsymbol{l}_{110}}, \frac{3C_{\boldsymbol{l}_{111}}}{2}, \frac{3C_{\boldsymbol{l}_{120}}}{2}, C\}.$$

Now $H(p_0) = 2\log(2\pi e\sigma^2)$ and

$$C_{\boldsymbol{l}_{ijk}} = H(\lambda_{\boldsymbol{l}_{ijk}}) - 2\log(2\pi e\sigma^2).$$

where the formulas for the densities $\lambda_{\boldsymbol{l}_{ijk}}$ are organized in the Table VI.

V. Conclusions

We gave a definition of G-capacity for some non-Abelian groups which are extensions $G = \mathbb{Z}_{p_1^r}^{\eta} \boxtimes \mathbb{Z}_{p_2}$. This definition

$\boldsymbol{l}_{ijk}$	$\lambda_{\boldsymbol{l}_{ijk}}$
$\boldsymbol{l}_{110}$	$\lambda_{\boldsymbol{l}_{110}} = \frac{1}{2}(p_0 + p_2)$
$\boldsymbol{l}_{111}$	$\lambda_{\boldsymbol{l}_{111}} = \frac{1}{4}(p_0 + p_4 + p_2 + p_6)$
$\boldsymbol{l}_{120}$	$\lambda_{\boldsymbol{l}_{120}} = \frac{1}{4}(p_0 + p_1 + p_2 + p_3)$
$\boldsymbol{l}_{121}$	$\lambda_{\boldsymbol{l}_{121}} = \frac{1}{8}(p_0 + p_1 + \cdots + p_7) = \lambda$

TABLE VI. OUTPUT PROBABILITY DENSITIES OF THE SUB-CHANNELS OF THE Q_8-SYMMETRIC CHANNEL, WHERE $p_k := p(y|x_k)$

is an adaptation from the G-capacity for Abelian groups $H = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{r_i} \mathbb{Z}_{p_i^j}^{\eta_{ij}}$ given in [1]. To make this adaptation, it has been shown that if $G = H \boxtimes K$ then $G^N \cong H^N \boxtimes K^N$. We did not make an adaptation for extensions like:

$$G = \left[\bigoplus_{i=1}^{s} \bigoplus_{j=1}^{r_i} \mathbb{Z}_{p_i^j}^{\eta_{ij}}\right] \boxtimes \mathbb{Z}_p,$$

which would be a truly generalization of the Abelian case, because the analyzed examples D_4 and Q_8 did not require such a general formula, also because we do not found, for this general case, a simple proof showing that $\mathcal{U}(\boldsymbol{l}) \subset G(\boldsymbol{l})^N$ which is a critical fact to fit in the sub-codes $\mathcal{U}(\boldsymbol{l})$ over the sub-channels $(G(\boldsymbol{l}), \mathcal{Y}, p(y|g))$, $g \in G(\boldsymbol{l})$.

In the dihedral 3D example it was numerically shown that the channel capacity is not achieved. The same $\mathcal{X}_8^{\beta}$-AWGN channel with group code over the cyclic group $\mathbb{Z}_8$ was exhibited in [1] as an example where the G-capacity does not achieve the channel capacity. A possible explanation for this common behavior of this channel could be in the internal group structure of $\mathbb{Z}_8$ and D_4. Both $\mathbb{Z}_8$ and D_4 have a unique subgroup isomorphic to $\mathbb{Z}_4$: $2\mathbb{Z}_8 \subset \mathbb{Z}_8$ and $G(\boldsymbol{l}_{120}) \subset D_4$. Whatever the sub-constellation matched to $2\mathbb{Z}_8$ it will be also matched to $G(\boldsymbol{l}_{120})$. Therefore, the capacities of the respective sub-channels will be the same.

For the four-dimensional channel with group code over Q_8, remains as an unsolved problem whether the channel capacity is achieved or not.

References

[1] G. Como and F. Fagnani, “The capacity of abelian group codes over symmetric channels,” *IEEE Trans. Inform. Theory*, vol. IT 45, no. 01, pp. 3–31, 2009.

[2] A. G. Sahebi and S. Pradhan, “Abelian group codes for channel coding and source coding,” *IEEE Trans. Inform. Theory*, vol. IT 61, no. 05, pp. 2399–2414, 2015.

[3] D. G. Forney, “Geometrically uniform codes,” *IEEE Trans. Inform. Theory*, vol. IT 37, no. 5, pp. 1241–1260, 1991.

[4] J. J. Rotman, *An Introduction to the Theory of the Groups*, 4th ed. New York: Springer-Verlag, 1995.

[5] I. N. Herstein, *Topics in Algebra*, 2nd ed. New York: Wiley and Sons, 1975.

[6] S. H. John W. Eaton, David Bateman and R. Wehbring, *GNU Octave version 3.8.1 manual: a high-level interactive language for numerical computations*. CreateSpace Independent Publishing Platform, 2014, ISBN 1441413006. [Online]. Available: http://www.gnu.org/software/octave/doc/interpreter

[7] J. P. Arpasi, “One example of a non-abelian group code over awgn channels,” in *Proceedings of the 14th Canadian Workshop on Information Theory - CWIT-2015*, St John’s, NL, Canada, pp. 115 – 119.