On Symmetric Channels and Codes Over the Quaternion Group

Jorge Pedraza Arpasi

***Abstract*—In this paper we study symmetric channels and group codes over the quaternion group Q_8. We show that, related to these channels, there is a number C_{Q8}, called group-capacity, which is less or equal than the capacity of the channel. Also we show that C_{Q8} is an upper bound for the rate of any reliable quaternion group code. Finally we show that the group-capacity equals the channel capacity.**

***Index Terms*—Groups codes, symmetric channels, group capacity, non-Abelian group codes, quaternion channels.**

I. Introduction

Group codes as generalization of binary linear codes were introduced in [1], which focused on the optimization of the minimal distance. When combined with symmetric channels, group codes have good properties such as the symmetry of the Voronoi regions which implies the uniform error property (UEP) when decoding them.

A crucial difference between linear codes and group codes is in the structure of the $(\mathcal{X}, \mathcal{Y}, p(y|x))$ channels through which they are transmitted. For a linear code $\mathcal{C} \subset F^N$, with F a field, the size of $\mathcal{X}$ must be a prime power, one-to-one related with F. As a field has only trivial sub-fields, for the alphabet $\mathcal{X}_s \subsetneq \mathcal{X}$ of any sub-channel, other than trivial, the respective subset $F_s \subsetneq F$ has no field structure. Then, there is no subspace $\mathcal{C}_s \subset \mathcal{C}$ such that $\mathcal{C}_s \subset F_s^N$. On the other hand, for a group code over a group G, the size of the channel alphabet is not restricted to being a prime power, and there may exist sub-channels with alphabet $\mathcal{X}_s \subsetneq \mathcal{X}$, $\mathcal{X}_s \neq \{0\}$, one-to-one related with a subgroup $G_s \subset G$, such that there is a subgroup $\mathcal{C}_s$ of the group code $\mathcal{C} \subset G^N$ satisfying $\mathcal{C}_s \subset G_s^N$. That is why, in this work, we can call these sub-channel codes as sub-codes.

For linear codes it is possible to prove Shannon's coding theorem. For group codes this may not be true as was shown in [2] and [3]. The sub-channels determine the existence of a number C_G, called the group-capacity of the channel which may be different from the channel's capacity C, more precisely, $C_G \leq C$. Moreover, any group code $\mathcal{C}$ with rate $R > C_G$ always will have error probability $P_e(\mathcal{C}) > A$, for some fixed $A > 0$. Therefore, in order to say that a group code achieves the channel capacity is necessary to check both $C_G = C$ and the Shannon's coding theorem for C_G, i.e., for any $R < C_G$ and for any $\epsilon > 0$ there is a group code $\mathcal{C}$ such that $P_e(\mathcal{C}) < \epsilon$.

This paper will deal with the group-capacity C_G for the case $G = Q_8$, the quaternion group which is non-Abelian. It is an extension of [3] where group-capacity was investigated for channels over Abelian groups. Also, it can be considered as a continuation of [4] where it was shown analytically that C_{D4}, the group-capacity for the dihedral group case, equals the channel capacity. The main difference between both the dihedral and quaternion cases comes from the dimension of the respective channels. For the dihedral case the 8-PSK channel has dimension 2, whereas for the quaternion case the respective channel has dimension 4. The analysis of the entropies, related to the capacities of the sub-channels, in the dihedral case, are reduced to one-dimensional integrals thanks to the polar coordinates of $\mathbb{R}^2$. For the quaternion case, the four dimensions of its channel do not allow such reduction.

This paper is organized as follows:
In Section II, we present Q_8 as ordered pairs of the Cartesian $\mathbb{Z}_4 \times \mathbb{Z}_2$, with a group structure called extension, and where $\mathbb{Z}_4$ and $\mathbb{Z}_2$ are the cyclic groups of orders four and two, respectively. Also, it is derived a formula that characterize its subgroups. This formula will be useful to analyze the codes of the sub-channels determined by the subgroups of Q_8
In Section III, following [3], the G-Symmetric channels are presented. A list of their properties, useful for this work, are mentioned. One special Q_8-Symmetric channel is introduced as an example.
In Section IV, group codes $\mathcal{C}$ are defined as subgroups of Q_8^N. It is shown that for each subgroup $Q_\imath \subset Q_8$ there is a subgroup of the code $\mathcal{C}_\imath \subset \mathcal{C}$ such that $\mathcal{C}_\imath$ is isomorphic to some subgroup of $Q_\imath^N$. Thus, $\mathcal{C}_\imath$ is a group code for the $Q_\imath$-Symmetric channels, [Proposition 1].
In Section V, it is defined the group-capacity C_{Q8} of the Q_8-Symmetric channel. It is shown that any group code transmitting with rate above C_{Q8} will have its decoding error probability bounded away from zero [Proposition 2]. Finally, it is presented a Montecarlo technique based proof, proving that C_{Q8} equals the channel capacity C. [Proposition 3].

II. The Quaternion group Q_8

After the Dihedral group D_4, the Quaternion group Q_8 is the best-known non-Abelian group with eight elements. One of the many ways to describe this classical group is by considering it as an extension of groups;

Definition 1: A group G is said to be an extension of the group H by the group K if there is a normal subgroup $N \subset G$ such that $N \approx H$ and $K \approx G/N$, where the symbol $\approx$ denotes isomorphism of groups and G/N is the group of the cosets determined by N, [5].
For practical reasons, in this work, a group extension G, of H by K, will be denoted by $G = H \boxtimes K$. One particular case

Jorge Pedraza Arpasi Centro Tecnologico de Alegrete, Universidade Federal do Pampa - UNIPAMPA Alegrete-RS Brasil, E-mail: jorgearpasi@unipampa.edu.br.
Digital Object Identifier: 10.14209/jcis.2022.15

of extension is the direct product of groups which is usually denoted by $H \oplus K$. The quaternion group is an extension $Q_8 = \mathbb{Z}_4 \boxtimes \mathbb{Z}_2$, where $\mathbb{Z}_4$ and $\mathbb{Z}_2$ are the cyclic groups of orders four and two respectively. This extension representation of Q_8 is fundamental for the analysis of the so called group-capacity of symmetric channels having group codes over Q_8. The following Table gives an explicit representation of the elements of Q_8, as ordered pairs of the extension $\mathbb{Z}_4 \boxtimes \mathbb{Z}_2$.

g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7
(0,0)	(1,0)	(0,1)	(1,1)	(2,0)	(3,0)	(2,1)	(3,1)

The group operation for the pairs $(a,b) \in \mathbb{Z}_4 \boxtimes \mathbb{Z}_2$ is given by the formula;

$$(a_1,b_1)*(a_2,b_2)=\begin{cases}(a_1+3^{b_1}a_2+2\,,b_1+b_2); & \text{if } b_1+b_2=2\\ (a_1+3^{b_1}a_2\,,b_1+b_2); & \text{if } b_1+b_2<2,\end{cases} \quad (1)$$

where the operations $a_1+3^{b_1}a_2+2$ and $a_1+3^{b_1}a_2+2$ are over the integers $\mod 4$ and b_1+b_2 are over the integers $\mod 2$. For instance $(2,1)*(0,1) = (2+3^1.0+2\,,\,1+1) = (0,0)$, also it can be verified that $(0,1)^2 = (2,0)$.

A. Characterizing the subgroups of Q_8

In order to determine how the group codes over Q_8 are and how they behave when transmitted through the quaternion channel, first we need to understand the structure of the subgroups of Q_8.

Lemma 1: Any subgroup of Q_8 can be written as $H \boxtimes K$, where H and K are such that $H \subset \mathbb{Z}_4$ and $K \subset \mathbb{Z}_2$ and $H = \{0\}$ implies $K = \{0\}$.

Proof.- The set $\{(0,0)\} \in \mathbb{Z}_4 \boxtimes \mathbb{Z}_2$ can be written as $\{0\} \boxtimes \{0\}$ and it is a trivial subgroup of Q_8, product of the trivial subgroups of $\mathbb{Z}_4$ and $\mathbb{Z}_2$. Also, for $2\mathbb{Z}_4 = \{0,2\}$, the set $2\mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = \{(0,0),(2,0),(0,1),(2,1)\}$ is a subgroup of Q_8. On the other hand, since $(0,1)^2 = (2,0)$, the set $\{0\} \boxtimes \mathbb{Z}_2 = \{(0,0),(0,1)\}$ is not a subgroup. These facts can be summarized by saying that whenever H subgroup of $\mathbb{Z}_4$, K subgroup of $\mathbb{Z}_2$ and $H = \{0\}$ implies $K = \{0\}$, the set $H \boxtimes K$ is a subgroup of Q_8.

But the converse, at first glance, seems to be incorrect: the subgroup $G_1 = \{(0,0),(1,1),(2,0),(3,1)\}$, apparently, has not a representation $H \boxtimes K$ where $H \subset \mathbb{Z}_4$ and $K \subset \mathbb{Z}_2$. To remedy this, let us remember that Q_8 has three normal subgroups of order four all of them isomorphic with $\mathbb{Z}_4$. One of them, certainly not G_1, was chosen to be represented by $\mathbb{Z}_4 \boxtimes \{0\}$. Then, changing this choice so that G_1 is represented by $\mathbb{Z}_4 \boxtimes \{0\}$ we will have $G_1 = H \boxtimes K$, H and K subgroups of $\mathbb{Z}_4$ and $\mathbb{Z}_2$ respectively. □

Now, we will characterize the subgroups of Q_8 in terms of constrained arrays of integers $\boldsymbol{l} = (l_1,l_2,l_3)$. For that, it is necessary to remember that $\mathbb{Z}_{p^r}(p^j) = \{g \in \mathbb{Z}_{p^r}\ ;\ p^j g = 0\}$, the subgroup of $\mathbb{Z}_{p^r}$ whose elements have order p^j, can be written as $p^{r-j}\mathbb{Z}_{p^r}$, for any prime p. Then, by Lemma 1 a subgroup of Q_8 can be expressed by the formula

$$Q_8(\boldsymbol{l}) = [2^{1-l_1}\mathbb{Z}_4(2) + 2^{2-l_2}\mathbb{Z}_4(2^2)] \boxtimes 2^{1-l_3}\mathbb{Z}_2, \quad (2)$$

where the symbol $+$ is the group operation of $\mathbb{Z}_4$ and $\boldsymbol{l} = (l_1,l_2,l_3)$ is an array of integers satisfying $0 \le l_1, l_3 \le 1$ and $0 \le l_2 \le 2$, and $(l_1,l_2) = (0,0)$ implies $l_3 = 0$.

III. G-Symmetric Channels

Groups are sets with algebraic structure strongly related to symmetries since its conception by E. Galois in the nineteen century [5]. If $\mathcal{X}$ is a discrete subset of $\mathbb{R}^n$, related to it there is a group G called the group of symmetries of $\mathcal{X}$, such that G acts over $\mathcal{X}$. When the action of G over $\mathcal{X}$ is transitive, the set $\mathcal{X}$ is called Geometrically Uniform Constellation GUC [6]. Thus, a GUC $\mathcal{X}$ with a symmetry group G transmitted through a channel $p(y|x)$ such that $p(gx|gy) = p(y|x)$ for all x, y and for all $g \in G$ is called symmetric channel [3]. More precisely:

Definition 2: Let $(\mathcal{X}, \mathcal{Y}, p(y|x))$ be a memoryless channel. If there is a group G such that:

- G acts over $\mathcal{X}$ in such a way this action is transitive and one-to-one,
- G acts isometrically over $\mathcal{Y}$,
- $p(y|x) = p(gy|gx)$ for all $x \in \mathcal{X}$, for all $y \in \mathcal{Y}$ and for all $g \in G$;

then $(\mathcal{X}, \mathcal{Y}, p(y|x))$ is called G-Symmetric channel.

From the above definition, the symmetry of $(\mathcal{X}, \mathcal{Y}, p(y|x))$ depends on the existence of a group G satisfying the three conditions. That is the case of the BSC and BEC channels. They are G-Symmetric for the group of binary permutations $G = \{(), (12)\}$ [3]. On the other hand it may be the case that a channel to be symmetric for more than one group. For instance the 8PSK-AWGN channel is G-symmetric for both $G = \mathbb{Z}_8$ (cyclic) and $G = D_4$ (dihedral) [4], [3]. A final observation on Definition 2 is that the G-Symmetric channels preserve the two important properties of classical symmetric channels:

- The mutual Information $I(X;Y)$ equals the channel capacity C when $p(x)$, the probability distribution of the input set $\mathcal{X}$, is uniform. With this, the capacity of the channel C, can be computed with the formula
$$C = \int\limits_{\mathcal{Y}} p(y|x) \log\left(\frac{p(y|x)}{p(y)}\right) dy, \quad (3)$$
where x is an arbitrary but fixed element of $\mathcal{X}$, and $p(y) = \frac{1}{|\mathcal{X}|}\sum\limits_{x\in\mathcal{X}} p(y|x)$ is the probability density of $\mathcal{Y}$, page 94 of [7].
- All the codewords $\boldsymbol{c}$ of a group code $\mathcal{C}$, transmitted through a G-Symmetric channel, have the same probability of decoding error $p(\text{error}|\boldsymbol{c}) = P_e(\mathcal{C}|\boldsymbol{c})$. Therefore, $P_e(\mathcal{C}) = \sum\limits_{\boldsymbol{c}} p(\boldsymbol{c}) P_e(\mathcal{C}|\boldsymbol{c}) = P_e(\mathcal{C}|\boldsymbol{c})$. This property is known as the uniform error property (UEP).

An additional property of a G-Symmetric channel is that for each subgroup $H \subset G$, the sub-constellation $\mathcal{X}_H \subset \mathcal{X}$ over which H acts transitively, determines a sub-channel $(\mathcal{X}_H, \mathcal{Y}, p(y|x))$ such that it is H-Symmetric by itself.

Example 1: Let the elements $g_0, g_1, \ldots, g_7$ of Q_8 represented as in the Table of Section II. If $\mathbb{C}$ is the complex number set, let $\mathcal{X} = \{x_0, x_1, \ldots, x_7\} \subset \mathbb{C}^2$ be the constellation defined in the following Table where $i = \sqrt{-1}$

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
$\binom{1}{0}$	$\binom{i}{0}$	$\binom{0}{1}$	$\binom{1}{i}$	$-\binom{1}{0}$	$-\binom{i}{0}$	$-\binom{0}{1}$	$-\binom{1}{i}$.

Consider the conditional Gaussian densities;

$$p(y|x_k) = \frac{1}{4\pi^2\sigma^4} e^{-\frac{\|y-x_k\|^2}{2\sigma^2}}, \tag{4}$$

where $y \in \mathcal{Y}$, $x_k \in \mathcal{X}$ and $\sigma > 0$.

Using a matrix representation $\mathrm{O}(\mathbb{C}, 2) \approx \mathrm{O}(\mathbb{R}, 4)$ of Q_8 we will have;

- $\|g_k y\| = \|y\|$, for all $g_k \in Q_8$ and for all $y \in \mathbb{C}^2$,
- $x_k = g_k x_0$, for all $k = 0, 1, \ldots, 7$,

which shows that $(\mathcal{X}, \mathcal{Y}, p(y|x_k))$ is a Q_8-Symmetric channel.

IV. Group codes and symmetric channels over Q_8

For a given group G and a positive integer N, it is customary to write the group of N-tuples of G as $G^N = G \oplus G \oplus \cdots \oplus G$, where $\oplus$ denotes the direct product of groups. Then, *a group code $\mathcal{C}$ over G is a subgroup of G^N* and it must be the image of some encoding mapping $\phi : \mathcal{U} \to G^N$, where ϕ is a injective group homomorphism and $\mathcal{U}$ is a group, the uncoded group of real information. From this, $\mathcal{U} \approx \mathcal{C}$.

For the specific case of the quaternion group, a group code must be a subgroup of $(\mathbb{Z}_4 \boxtimes \mathbb{Z}_2)^N$. A useful formula, shown in [4], is $(\mathbb{Z}_4 \boxtimes \mathbb{Z}_2)^N \approx \mathbb{Z}_4^N \boxtimes \mathbb{Z}_2^N$, which means there is a normal subgroup $N_0 \approx \mathbb{Z}_4^N$ with $(\mathbb{Z}_4^N \boxtimes \mathbb{Z}_2^N)/N_0 \approx \mathbb{Z}_2^N$. Hence, the structure of these N-fold subgroups must obey the structure of the single subgroups of $\mathbb{Z}_4 \boxtimes \mathbb{Z}_2$, based on Lemma 1. This means that a subgroup of $\mathbb{Z}_4^N \boxtimes \mathbb{Z}_2^N$ has to be a set $H \boxtimes K$, where H and K are such that $H \subset \mathbb{Z}_4^N$ and $K \subset \mathbb{Z}_2^N$ and $H = \{\mathbf{0}\}$ implies $K = \{\mathbf{0}\}$.

Therefore, a quaternary code $\mathcal{C} \subset (\mathbb{Z}_4 \boxtimes \mathbb{Z}_2)^N$ has the following structure;

$$\mathcal{C} \approx \mathcal{U} \approx (\mathbb{Z}_2^{k_1} \oplus \mathbb{Z}_4^{k_2}) \boxtimes \mathbb{Z}_2^{k_3} = (\mathbb{Z}_2^{k_1} \oplus \mathbb{Z}_{2^2}^{k_2}) \boxtimes \mathbb{Z}_2^{k_3}, \tag{5}$$

where the elements of the array of exponents $\boldsymbol{k} = (k_1, k_2, k_3)$ satisfy the conditions $k_1 + k_2 \leq N$, $k_3 \leq N$, and if $(k_1, k_2) = (0, 0)$ then $k_3 = 0$.

Proposition 1: Let $Q_8(\boldsymbol{l})$ be, as in equation (2), a subgroup of Q_8. Then, there is a subgroup $\mathcal{C}(\boldsymbol{l})$ of the code $\mathcal{C} \subset Q_8^N$ such that $\mathcal{C}(\boldsymbol{l}) \subset (Q_8(\boldsymbol{l}))^N$.

Proof.- The equation (2) can be reduced by doing the following operations: $2^{1-l_1}\mathbb{Z}_4(2) + 2^{2-l_2}\mathbb{Z}_4(2^2) = 2^{1-l_1}2^{2-1}\mathbb{Z}_4 + 2^{2-l_2}2^{2-2}\mathbb{Z}_4 == 2^{2-l_1}\mathbb{Z}_4 + 2^{2-l_2}\mathbb{Z}_4 = 2^{2-l^*}\mathbb{Z}_4$, where $l^* = \max\{l_1, l_2\}$. Thus, the group structure of $Q_8(\boldsymbol{l})$ is;

$$Q_8(\boldsymbol{l}) = 2^{2-l^*}\mathbb{Z}_4 \boxtimes 2^{1-l_3}\mathbb{Z}_2 \approx \mathbb{Z}_{2^{l^*}} \boxtimes \mathbb{Z}_{2^{l_3}}. \tag{6}$$

On the other hand, for the same $\boldsymbol{l}$, the subset of $\mathcal{U}$ defined by; $\mathcal{U}(\boldsymbol{l}) = (2^{1-l_1}\mathbb{Z}_2^{k_1} \oplus 2^{2-l_2}\mathbb{Z}_{2^2}^{k_2}) \boxtimes 2^{1-l_3}\mathbb{Z}_2^{k_3}$, is a subgroup of $\mathcal{U}$. By the isomorphism $p^n\mathbb{Z}_{p^m} \approx \mathbb{Z}_{p^{m-n}}$, the structure of this subgroup is $\mathcal{U}(\boldsymbol{l}) \approx (\mathbb{Z}_{2^{l_1}}^{k_1} \oplus \mathbb{Z}_{2^{l_2}}^{k_2}) \boxtimes \mathbb{Z}_{2^{l_3}}^{k_3}$. Therefore, if $\mathcal{C}(\boldsymbol{l}) = \phi(\mathcal{U}(\boldsymbol{l}))$, then

$$\mathcal{C}(\boldsymbol{l}) \approx (\mathbb{Z}_{2^{l_1}}^{k_1} \oplus \mathbb{Z}_{2^{l_2}}^{k_2}) \boxtimes \mathbb{Z}_{2^{l_3}}^{k_3}. \tag{7}$$

Comparing equations (7) and (6) we have $\mathcal{C}(\boldsymbol{l}) \subset (Q_8(\boldsymbol{l}))^N$.
□

The above Proposition 1 is telling us that each $Q_8(\boldsymbol{l})$-Symmetric sub-channel has its own group code, namely $\mathcal{C}(\boldsymbol{l})$. That is why, sometimes, $\mathcal{C}(\boldsymbol{l}) \subset \mathcal{C}$ is called a sub-code.

Also, observe that for the trivial array $\boldsymbol{l} = (0, 0, 0)$, the subgroup $Q_8(\boldsymbol{l} = 000)$ in equation (6) is $Q_8(\boldsymbol{l} = 000) = 4\mathbb{Z}_4 \boxtimes 2\mathbb{Z}_2 = \{(0, 0\}$, the neutral element of Q_8. Thus, from equation (7), this array $\boldsymbol{l} = 000$ yields the trivial code $\mathcal{C}(\boldsymbol{l} = 000) = \{(\mathbf{0}, \mathbf{0})\}$ whose both rate and capacity are zero.

On the other hand, computing the formula (6) for the array $\boldsymbol{l} = (1, 2, 1)$ we have that $l^* = \max\{l_1, l_2\} = 2$ and $Q_8(\boldsymbol{l} = 121) = 2^{2-2}\mathbb{Z}_4 \boxtimes 2^{1-1}\mathbb{Z}_2 = \mathbb{Z}_4 \boxtimes \mathbb{Z}_2 = Q_8$.

Then, from (7), the respective code $\mathcal{C}(\boldsymbol{l} = 121)$ is

$$\mathcal{C}(\boldsymbol{l} = 121) = (\mathbb{Z}_2^{k_1} \oplus \mathbb{Z}_4^{k_2}) \boxtimes \mathbb{Z}_2^{k_3}, \tag{8}$$

which is exactly the full quaternion code $\mathcal{C}$ of (5). Therefore

$$\mathcal{C}(\boldsymbol{l} = 121) = \mathcal{C}. \tag{9}$$

V. The group-capacity of the quaternion channel

Let $\mathcal{C} = \phi(\mathcal{U})$ be an arbitrary quaternion code, as in (5), generated by $\boldsymbol{k} = (k_1, k_2, k_3)$ with $(k_1, k_2) \neq (0, 0)$. The rate of the sub-code $\mathcal{C}(\boldsymbol{l}) = \phi(\mathcal{U}(\boldsymbol{l}))$ through the sub-channel $(\mathcal{X}(\boldsymbol{l}), \mathcal{Y}, p(y|x))$ is: $R(\boldsymbol{l}) = \frac{\log|\mathcal{U}(\boldsymbol{l})|}{N} = \frac{\log(2^{\sum_{i=1}^3 l_i k_i})}{N} = \frac{\log(2)\sum_{i=1}^3 l_i k_i}{N}$. For the maximal array $\boldsymbol{l^*} = (l_1^*, l_2^*, l_3^*) = (1, 2, 1)$ of (9) we have: $R(\boldsymbol{l} = 121) = \frac{\log(2)\sum_{i=1}^3 l_i^* k_i}{N} = \frac{\log(2)(k_1 + 2k_2 + k_4)}{N} = \frac{\log|\mathcal{U}|}{N} = R$, where R is the rate of the code $\mathcal{C}$.

Since, in this quaternion coding, $(k_1, k_2) \neq (0, 0)$, for any array $\boldsymbol{l} \neq (0, 0, 0)$, the $\sum_{i=1}^3 l_i k_i \neq 0$. Therefore, for $\boldsymbol{l} \neq (0, 0, 0)$, the rate $R(\boldsymbol{l})$ is positive and is legitimate to setup the relation $\frac{R(\boldsymbol{l})}{R} = \frac{\sum_{i=1}^3 l_i k_i}{\sum_{i=1}^3 l_i^* k_i}$ from which is obtained;

$$R = \frac{R(\boldsymbol{l})\sum_{i=1}^3 l_i^* k_i}{\sum_{i=1}^3 l_i k_i}; \quad \forall \boldsymbol{l} \neq (0, 0, 0). \tag{10}$$

Definition 3: Let $C(\boldsymbol{l})$ be the capacity of the sub-channel determined by $\boldsymbol{l}$. The group-capacity of a Q_8-Symmetric channel is defined by: $C_{Q8} = \max\limits_{\boldsymbol{k} \neq (0,0,0)} \left\{ \min\limits_{\boldsymbol{l} \neq (0,0,0)} \left\{ \frac{C(\boldsymbol{l})\sum_{i=1}^3 l_i^* k_i}{\sum_{i=1}^3 l_i k_i} \right\} \right\}$. Notice that for any $\boldsymbol{k} = (k_1, k_2, k_3) \neq (0, 0, 0)$, the number $\min\limits_{\boldsymbol{l} \neq (0,0,0)} \left\{ \frac{C(\boldsymbol{l})\sum_{i=1}^3 l_i^* k_i}{\sum_{i=1}^3 l_i k_i} \right\}$ is upper bounded by $C(\boldsymbol{l}^*) = C$, the capacity of the channel. Hence

$$C_{Q8} \leq C. \tag{11}$$

Proposition 2: If a code $\mathcal{C}$ over the quaternion group has a rate $R > C_{Q8}$ then its probability of error is bounded away from zero, i.e., $P_e(\mathcal{C}) > A$, for some $A > 0$.

Proof.- Let $\boldsymbol{l}^m = (l_1^m, l_2^m, l_3^m)$ and $\boldsymbol{k}^M = (k_1^M, k_2^M, k_3^M)$ be the arrays such that $C_{Q8} = \frac{C(\boldsymbol{l}^m)\sum_{i=1}^3 l_i^* k_i^M}{\sum_{i=1}^3 l_i^m k_i^M}$ and suppose there is a code $\mathcal{C}$ generated by an array $\boldsymbol{k} = (k_1, k_2, k_3)$ with rate $R > C_{Q8}$, then, by (10), $R = \frac{R(\boldsymbol{l}^m)\sum_{i=1}^3 l_i^* k_i}{\sum_{i=1}^3 l_i^m k_i} > \frac{C(\boldsymbol{l}^m)\sum_{i=1}^3 l_i^* k_i^M}{\sum_{i=1}^3 l_i^m k_i^M}$. On the other hand, since $\frac{\sum_{i=1}^3 l_i^* k_i}{\sum_{i=1}^3 l_i^m k_i} \leq \frac{\sum_{i=1}^3 l_i^* k_i^M}{\sum_{i=1}^3 l_i^m k_i^M}$, then $R(\boldsymbol{l}^m) > C(\boldsymbol{l}^m)$.

However, if $R(\boldsymbol{l}^m) > C(\boldsymbol{l}^m)$, by the converse of Shannon's Coding Theorem, the probability of error of the sub-code $\mathcal{C}(\boldsymbol{l}^m)$ is bounded away from zero, which means $P_e(\mathcal{C}(\boldsymbol{l}^m)) \geq A$, where A is some positive number. Combining this with the UEP of symmetric channels it can be seen that: $P_e(\mathcal{C}) = P_e(\mathcal{C}|\mathbf{0}) \geq P_e(\mathcal{C}(\boldsymbol{l}^m)|\mathbf{0}) = P_e(\mathcal{C}(\boldsymbol{l}^m)) \geq A$. □

A. The group-capacity equals the capacity

By the constraints about the arrays $\boldsymbol{l}$, $\boldsymbol{k}$ the conditions $\boldsymbol{l} \neq (0,0,0)$ and $\boldsymbol{k} \neq (0,0,0)$ are equivalent to $(l_1, l_2) \neq (0,0)$ and $(k_1, k_2) \neq (0,0)$ respectively. Defining the auxiliary function $f(\boldsymbol{l}) = f(l_1, l_2, l_3) = \sum_{i=1}^{3} l_i k_i$, it can be checked that $f(1,1,l_3) \geq f(1,0,l_3)$ and $f(1,1,l_3) \geq f(0,1,l_3)$ also $f(1,2,l_3) \geq f(0,2,l_3)$. Hence, denoting by $\boldsymbol{L} = \{(1,1,0),(1,1,1),(1,2,0),(1,2,1)\}$ the group-capacity becomes: $C_{Q8} = \max\limits_{\substack{\boldsymbol{k} \\ (k_1,k_2)\neq(0,0)}} \left\{ \min\limits_{\boldsymbol{l}\in\boldsymbol{L}} \left\{ \frac{C(\boldsymbol{l}) \sum_{i=1}^{3} l_i^* k_i}{\sum_{i=1}^{3} l_i k_i} \right\} \right\}$.

The group-capacity can be computed more efficiently if the arrays $\boldsymbol{k} = (k_1, k_2, k_3)$ are normalized. From $\log|\mathcal{U}| = \log(2) \sum_{i=1}^{3} l_i^* k_i$ it can be seen that $\alpha_i = \frac{\log(2) l_i^* k_i}{\log|\mathcal{U}|}$ is a probability vector, i.e, $\alpha_1 + \alpha_2 + \alpha_3 = 1$. Conversely, from each probability vector $\boldsymbol{\alpha}$, with $(\alpha_1, \alpha_2) \neq (0,0)$, a group code can be generated making $k_i = \frac{\alpha_i \log|\mathcal{U}|}{l_i^* \log(2)}$. Hence, the group-capacity of the quaternion channel can be computed with: $C_{Q8} = \max\limits_{\substack{\boldsymbol{\alpha} \\ (\alpha_1,\alpha_2)\neq(0,0)}} \left\{ \min\limits_{\boldsymbol{l}\in\boldsymbol{L}} \left\{ \frac{C(\boldsymbol{l})}{\sum_{i=1}^{3} \frac{l_i}{l_i^*} \alpha_i} \right\} \right\}$. For the sake of simplicity, for the array $\boldsymbol{l} = (l_1, l_2, l_3)$, let us denote by $C_{l_1 l_2 l_3}$ as the capacity of the sub-channel $(X(\boldsymbol{l}), \mathcal{Y}(\boldsymbol{l}), p(y|x))$. For instance, C_{121} is the capacity of the sub-channel whose input alphabet is $\mathcal{X}(\boldsymbol{l} = 121)$ which by (7) is the full input alphabet $\mathcal{X}$ of the channel. With this notation, if C is the capacity of the channel, we have that $C_{121} = C$.
From here:

$$C_{Q8} = \max_{\substack{\boldsymbol{\alpha} \\ (\alpha_1,\alpha_2)\neq(0,0)}} \left\{ \min \left\{ \frac{C_{110}}{\alpha_1 + \frac{\alpha_2}{2}}, \frac{C_{111}}{\alpha_1 + \frac{\alpha_2}{2} + \alpha_3}, \frac{C_{120}}{\alpha_1 + \alpha_2}, C \right\} \right\}$$
$$\geq \min \left\{ 3C_{110}, \frac{3C_{111}}{2}, \frac{3C_{110}}{2}, C \right\}. \quad (12)$$

For the array $\boldsymbol{l} = (l_1 l_2 l_3)$ the capacity $C_{l_1 l_2 l_3}$ can be computed with the formula (3). For instance, if $\boldsymbol{l} = (1,1,0)$, by formula (6), the subgroup is $Q_8(\boldsymbol{l} = 110) = 2^{2-1}\mathbb{Z}_4 \boxtimes 2^{2-0}\mathbb{Z}_2 = 2\mathbb{Z}_4 \boxtimes \{0\} = \{(0,0),(2,0)\} = \{g_0, g_4\}$ (Table of Section II). By the Table of Section III, the respective sub-constellation is $\{x_0, x_4\} = \{\binom{1}{0}, \binom{-1}{0}\} \subset \mathbb{C}^2$. Then the capacity integral (3) becomes:

$$C_{110} = \int\limits_{\mathbb{R}^4} p(y|x_0) \log\left(\frac{p(y|x_0)}{p_{110}(y)}\right) dy, \quad (13)$$

where $p_{110}(y) = \frac{1}{2}(p(y|x_0) + p(y|x_4))$ and $p(y|x_k)$ is the conditional density (4). Now, notice that the capacity integral (13) can be interpreted as the the expected value of the function $f_{110}(y) = \log\left(\frac{p(y|x_0)}{p_{110}(y)}\right)$, for the random variable Y whose density is $p(y|x_0)$. Then, by the law of large numbers, the capacity C_{110} is $C_{110} = \lim\limits_{n\to\infty} \left(\frac{\sum\limits_{k=1}^{n} f_{110}(y_k)}{n} \right)$, where the sequence $\{y_k\}_{k=1}^{n}$ is sampled in accordance to $p(y|x_0)$. The software Octave [8] has the command `normrnd` which makes this sampling job. In general, the capacity $C_{l_1 l_2 l_3}$ will be

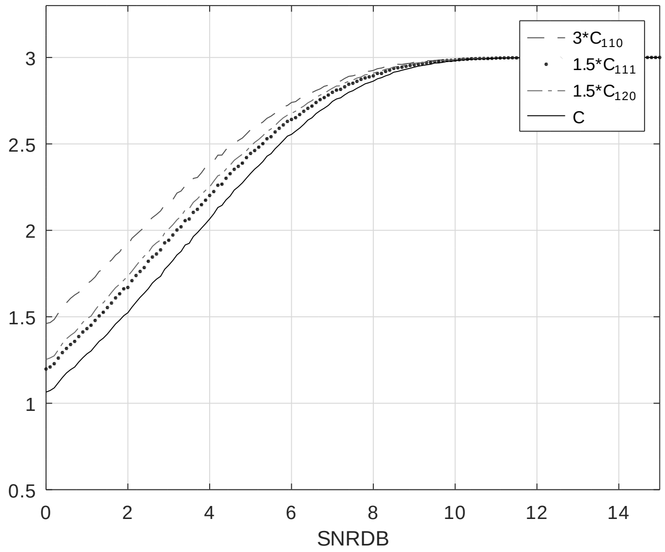

Fig. 1: C=min$\{3C_{110}, 1.5C_{111}, 1.5C_{120}, C\}$

$$C_{l_1 l_2 l_3} = \lim_{n\to\infty} \left(\frac{\sum\limits_{k=1}^{n} f_{l_1 l_2 l_3}(y_k)}{n} \right). \quad (14)$$

Proposition 3: The group-capacity C_{Q8}, of the channel of Example 1, equals the channel capacity C.

Proof .- Computing the capacities $C = C_{121}$, C_{110}, C_{111} and C_{120} with the Montecarlo method described in (14) it can be produced the data which allows Figure 1 showing that:

$$C \leq 3C_{110} \;\Big|\; C \leq \tfrac{3}{2} C_{120} \;\Big|\; C \leq \tfrac{3}{2} C_{111},$$

for all SNRDB in the interval [0,15]. Therefore

$$C = \min\{C, 3C_{110}, \tfrac{3}{2}C_{111}, \tfrac{3}{2}C_{120}\} \quad (15)$$

Comparing (15) and (12) we obtain

$$C_{Q8} \geq C \quad (16)$$

Finally, comparing (16) and (11) we conclude

$$C_{Q8} = C.$$

□

VI. Conclusion

We have shown that the group-capacity C_{Q8} is an upper bound for the transmission rate of any reliable group code over Q_8. Also, we have exhibited a Montecarlo technique based proof showing that $C_{Q8} = C$. A couple of tasks to be done, to give continuity to this work, would be:

- To find a totally analytical proof for the equality $C_{Q8} = C$.
- To prove Shannon's coding theorem with respect to C_{Q8}, that is, for any $R < C_{Q8}$ and for any $\epsilon > 0$ there is a group code $\mathcal{C}$ over Q_8, with rate R, such that $P_e(\mathcal{C}) < \epsilon$. With this, it would be complete the proof that quaternion group codes achieve the channel capacity.

REFERENCES

[1] D. Slepian, "Group codes for the gaussian channels," *Bell Systems Technical Journal*, vol. 47, pp. 575–602, 1968.

[2] R. Ahlswede, "Group codes do not achieve shannon's channel capacity for general discrete channels," *The Annals of Mathematical Statistics*, vol. 42, pp. 224–240, 1971.

[3] 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, doi: 10.1109/TIT.2009.2015992.

[4] J. P. Arpasi, "On the non-abelian group code capacity of memoryless channels," *Advances in Mathematics of Communications*, vol. 14, no. 03, pp. 423–436, 2020, doi:10.3934/amc.2020058.

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

[6] D. G. Forney, "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. IT 37, no. 5, pp. 1241–1260, 1991, doi: 10.1109/18.133243.

[7] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley and Sons, 1968.

[8] J. W. Eaton, D. Bateman, S. Hauberg, and R. Wehbring, *GNU Octave version 7.1.0 manual: a high-level interactive language for numerical computations*, 2022. [Online]. Available: octave.org/doc/v7.1.0/