Derived Subgroups and Controllability of Group Codes

Jorge Pedraza Arpasi, Blanca Rosa Maquera-Sosa

Abstract— **Convolutional codes over groups are defined by Loeliger and Mittelholzer in [6] as being controllable and observable group codes. This means the convolutional codes over groups deserve be studied from both algebraic and system theoretic point of view. We first give a fast review of algebraic facts which will be used to describe the encoder of a group code. Then, we use these facts together with system basics of group codes to show that the controllability of these codes depends on the existence of a class of normal series of subgroups from its state group.**

Keywords— **Group Codes, controllability, Derived Subgroups, Extension of Groups, Convolutional codes over Groups.**

I. Introduction

Group codes were first introduced by Slepian in [1] as the codes generated by a group of orthogonal matrices. Years later Forney, Trott and Loeliger, in [2], [3], [4], generalized the definition of these group codes. They noticed that the trellis section of the classical binary convolutional codes have several group structures interacting themselves according to rules which allow to define the convolutional encoder using the ISO (input/state/output) model of machines and, only, the additive operation of the mod 2 ring $\mathbb{Z}_2 = \{0, 1\}$. Thus, under the modern group codes point of view, a binary convolutional encoder (n, k, m) can be seen as a ISO machine $(\mathbb{Z}_2^k, \mathbb{Z}_2^m, \mathbb{Z}_2^n, \nu, \omega)$, where $\mathbb{Z}_2^k$, $\mathbb{Z}_2^m$, $\mathbb{Z}_2^n$ are the input(information) group, the state group and the output(encoded) group respectively. The mappings $\nu : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ and $\omega : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ are the encoding and the next state homomorphisms, respectively, with $x = (x_1, x_2, \ldots, x_k) \in \mathbb{Z}_2^k$ and $q = (q_1, q_2, \ldots, q_m) \in \mathbb{Z}_2^m$. This group description of binary convolutional codes allows its generalization over arbitrary groups, beyond the binary groups $\mathbb{Z}_2^n$. On the other hand, since a convolutional code is a class of infinite sequences flowing through states, at each instant of time, then under the dynamical point of view, it has some behavior properties such as controllability and observability. In [3], [4], by using, the dynamical systems paradigm proposed by Willems, in [5], is given this system theoretic treatment. Every known binary convolutional code is trivially controllable and observable but with many generalized codes based on arbitrary, especially non abelian, groups arises the lack of well behaviorness. Thus, towards to overcome this problem, in [6] a convolutional code over a group is defined as a group code which is controllable and observable.

The author is professor of the Instituto de Ciências Exatas e Geociências ICEG, University of Passo Fundo - UPF, Rio Grande do Sul, Brazil. Email: arpasi@upf.tche.br

The author is professor of the Faculdade de Engenharia e Arquitetura - FEAR, University of Passo Fundo - UPF, Rio Grande do Sul, Brazil. Email: blamaso@upf.tche.br

In this work we give necessary conditions for a group code be a controllable one and therefore, it be almost a convolutional code over a group. For this, in the Section 2 we present some algebraic facts collected from [7], [8] and [9]. In the Section 3 firstly we present some facts collected from [6] and some of the our basic results to show the main proposition of this work which is the Theorem 1. Finally, in the Section 4 some conclusions are given.

II. Algebraic prelude

Given a group G, a **normal series** of G is a sequence of subgroups $G_i \subset G$ such that $G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = e_G$, where e_G is the identity element of G and G_{i-1} is a normal subgroup of G_i, that is, $G_{i-1} \lhd G_i$ [7], [8], [9]. Also, in the literature just cited, the subgroup generated by elements of the form $ghg^{-1}h^{-1}$ is called either the **commutators** subgroup or **derived** subgroup of G and it is denoted by G'. Clearly, if G is abelian then G' is reduced to $\{e_G\}$. One important property of G', shown in [7], is its invariance under the action of the group of automorphisms of G, that is, $\phi(G') = G'$ for all $\phi \in Aut(G)$.

Example 1: Consider the group of symmetries of the square, denoted by $D8 = \{R_0, R_1, R_2, R_3, d_1, d_2, V, H\}$, whose generators are R_1 and d_1 via the relations;

$$\begin{cases} R_1^4 &= R_0 \\ d_1^2 &= R_0 \\ R_1 d_1 &= d_1 R_1^3. \end{cases}$$

By making $R_2 = R_1^2, R_3 = R_1^3, d_2 = R_1^2 d_1, H = R_1 d_1$, and $V = R_1^3 d_1$; the group operation of $D8$ is completely defined, for instance $R_1 d_2 = R_1 R_1^2 d_1 = R_1^3 d_1 = V$. The lattice diagram for the subgroups of $D8$ is shown at Figure 1. Some normal series of this group are;

$$\begin{array}{lllllll}
\{R_0\} & \lhd & \{R_0, R_2\} & \lhd & \{R_0, R_2, R_1, R_3\} & \lhd & D_8 \\
\{R_0\} & \lhd & \{R_0, R_2\} & \lhd & \{R_0, R_2, d_1, d_2\} & \lhd & D_8 \\
\{R_0\} & \lhd & \{R_0, R_2\} & \lhd & \{R_0, R_2, H, V\} & \lhd & D_8 \\
\{R_0\} & \lhd & \{R_0, H\} & \lhd & \{R_0, R_2, H, V\} & \lhd & D_8 \\
\{R_0\} & \lhd & \{R_0, R_2\} & \lhd & D_8 & & \\
\{R_0\} & \lhd & D_8, & & & &
\end{array}$$

whereas the derived subgroup $D_8' = \{ghg^{-1}h^{-1}\,;\, g, h \in G\}$ is $D8 = \{R_0, R_2\}$.

Definition 1: If X and Q are groups, then an **extension** of X by Q is a group G having a normal subgroup N, isomorphic to X, with the factor group $\frac{G}{N}$ isomorphic to Q. [7].

Let $\psi : Q \to \frac{G}{N}$ and $\upsilon : N \to X$ be the isomorphisms of the above Definition 1, that is, $Q \overset{\psi}{\cong} \frac{G}{N}$ and $N \overset{\upsilon}{\cong} X$. Then, the group operation for the ordered pairs (x, q) of $X \times Q$ is defined by (1)

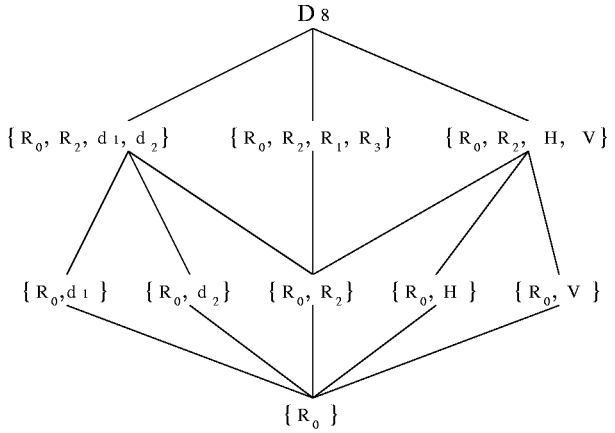

Fig. 1. Latice diagram of the group D_8

$$(x,q).(y,r) = (x.\phi(q)(y).\varsigma(q,r)\,,\, qr), \tag{1}$$

where $\phi : Q \to Aut(X)$ and $\varsigma : Q \times Q \to X$ are mappings defined by (2) and (3);

$$\phi(q)(x) = v[l(\psi(q)).v^{-1}(x).(l(\psi(q)))^{-1}], \tag{2}$$

$$\varsigma(q,r) = v[l(\psi(q)).l(\psi(r)).(l(\psi(qr)))^{-1}], \tag{3}$$

and where $l : \frac{G}{N} \to G$ is a lifting such that $l(N) = e_G$. In this way, by combining both (1) and (2) and (3) we have $\theta : G \to X \times Q$ defined by

$$\theta(g) = \theta(n.l(Ng)) = (v(n)\,,\, \psi^{-1}(Ng)), \tag{4}$$

is a group isomorphism. Therefore, given an abstract group G, the isomorphism θ can be used as a practical tool to decompose each $g \in G$ as an ordered pair (x,q) with $x \in X$ and $q \in Q$.

On the other hand, since the operation on the extension group $X \times Q$ depends on ϕ and ς we will denotate this group as $X_{\phi\varsigma}Q$, that is, $G \overset{\theta}{\cong} X_{\phi\varsigma}Q$. Notice that if the lifting $l : \frac{G}{N} \to G$ is a homomorphism then, the mapping defined in (3) becomes $\varsigma(q,r) = e_X$, the identity element of the group X, for all $q, r \in Q$. Also, if l is homomorphism, ϕ of (2) is a group homomorphism and the operation defined by (1) is reduced to

$$(x,q).(y,r) = (x.\phi(q)(y)\,,\, qr), \tag{1'}$$

which is the semidirect product operation $X_{\phi\rtimes}Q$. From this, we can say the extension of groups is a generalization of the semidirect product

Example 2: Consider the abstract group $G = \{e, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma, \delta, \alpha\delta, \beta\delta, \alpha\beta\delta, \gamma\delta, \alpha\gamma\delta, \beta\gamma\delta, \alpha\beta\gamma\delta\}$, generated by four elements satisfying the following relations

$$\begin{cases} \alpha^2 = e \\ \beta^2 = e, \quad \beta\alpha = \alpha\beta, \\ \gamma^2 = e, \quad \gamma\alpha = \alpha\gamma, \quad \gamma\beta = \beta\gamma \\ \delta^2 = e, \quad \delta\alpha = \alpha\delta\gamma, \quad \delta\beta = \beta\delta, \quad \delta\gamma = \delta\gamma \end{cases}$$

We have $N = \{e, \beta\gamma\}$ is a normal subgroup of G. N is isomorphic to the additive mod 2 group $\mathbb{Z}_2 = \{0,1\}$, via the isomorphism $v(e) = 0$ and $v(\beta\gamma) = 1$. On the other hand the quotient group $\frac{G}{N}$ is isomorphic to $\cong D_8$, (Example 1), via the mapping $\psi : D_8 \to G/N$ defined by

$$\begin{array}{llll} R_0 \mapsto N & R_1 \mapsto N.\alpha\delta & R_2 \mapsto N.\beta & R_3 \mapsto N.\alpha\beta\delta \\ d_1 \mapsto N.\alpha & d_2 \mapsto N.\alpha\beta & H \mapsto N.\beta\delta & V \mapsto N.\delta \end{array}$$

Consider the lifting $l : G/N \to G$ defined by $l(N) = e$, $l(N.\alpha\delta) = \alpha\delta$, $l(N.\beta) = \beta$, $l(N.\alpha\beta\delta) = \alpha\beta\delta$, $l(N.\alpha) = \alpha$, $l(N.\alpha\beta) = \alpha\beta$, $l(N.\beta\delta) = \beta\delta$ and $l(N.\delta) = \delta$.

Thus, the mappings ς e ϕ de (3) and (2) respectively, are defined. Therefore the extension group $\mathbb{Z}_{2\phi\varsigma}D_8$ is isomorphic to G via the following mapping θ;

$$\begin{array}{rcl|rcl} e & \mapsto & (0,R_0) & \alpha & \mapsto & (0,d_1) \\ \beta & \mapsto & (0,R_2) & \gamma & \mapsto & (1,R_2) \\ \delta & \mapsto & (0,V) & \alpha\beta & \mapsto & (0,d_2) \\ \alpha\gamma & \mapsto & (1,d_2) & \alpha\delta & \mapsto & (0,R_1) \\ \beta\gamma & \mapsto & (1,R_0) & \beta\delta & \mapsto & (0,H) \\ \gamma\delta & \mapsto & (1,H) & \alpha\beta\gamma & \mapsto & (1,d_1) \\ \alpha\beta\delta & \mapsto & (0,R_3) & \alpha\gamma\delta & \mapsto & (1,R_3) \\ \beta\gamma\delta & \mapsto & (1,V) & \alpha\beta\gamma\delta & \mapsto & (1,R_1). \end{array}$$

III. CONTROLLABLE GROUP CODES

Given a group G, consider the bi-infinite Cartesian $G^{\mathbb{Z}} = \cdots \times G \times G \times G \times \ldots$, which with the componentwise operation induced from G is also a group. Then a **group code** $\mathcal{C}$ is a subgroup of $G^{\mathbb{Z}}$, [3], [2] [6]. For a **codeword** $c \in \mathcal{C}$ and $I \subset \mathbb{Z}$, let $c|_I$ be defined by $c|_I = \{c_k\ ;\ k \in I\}$, for instance if $I = [k,\infty) = \{k, k+1, \ldots \infty\}$ we will have $y|_{[k,\infty)} = \{c_k, y_{k+1}, \ldots\}$. Now, consider the codeword subsets $\mathcal{C}_I = \{c \in \mathcal{C}\,;\, c_k = e_G,\ \text{if}\, k \notin I\}$. These subsets are normal subgroups of $\mathcal{C}$. In particular consider $\mathcal{C}_{(-\infty,0)}$ and $\mathcal{C}_{[0,\infty)}$, since they are normal subgroups then the product $\mathcal{C}_{(-\infty,0)} * \mathcal{C}_{[0,\infty)}$ is also a normal one. Hence the quotient group $Q = \frac{\mathcal{C}}{\mathcal{C}_{(-\infty,0)} * \mathcal{C}_{[0,\infty)}}$ is well defined and it is called the **state group** of $\mathcal{C}$. Given a $[i,j] \subset \mathbb{Z}$ the $[i,j]$-projection map of a codeword is $proj_{[i,j]}(c) = \{c_i, c_{i+1}, \ldots, c_j\}$. Then, the **input group** X of the group code $\mathcal{C}$ is defined as the projection $proj_{[0,0]}(\mathcal{C}_{(-\infty,0)})$.

Definition 2: A group code $\mathcal{C}$ is said controllable when there is an integer $l > 0$ such that for any $j \in \mathbb{Z}$ and for

each pair of codewords y, $y\prime$ there is a codeword $y\prime\prime$ such that $y\prime\prime|_{(-\infty,j)} = y|_{(-\infty,j)}$ and $y\prime\prime|_{[j+l,\infty)} = y\prime|_{[j+l,\infty)}$.

Definition 3: Consider a group code $\mathcal{C} \subset Y^{\mathbb{Z}}$, with state group Q and input group X. Consider the extension $X_{\phi_\varsigma}Q$. An encoder of $\mathcal{C}$ is a machine $M = (X, Y, Q, \nu, \omega)$, where $\nu : X_{\phi_\varsigma}Q \to Y$ and $\omega : X_{\phi_\varsigma}Q \to Q$ are group homomorphisms, with ω being a surjective one.

Consider an initial state $q_0 \in Q$ and a sequence of inputs, i.e. information symbols, $\{x_i\}_{i=1}^{\infty}$, $x_i \in X$, for each $i \in \mathbb{N}$. Then, the encoder M responds with two sequences, $\{q_i\}_{i=1}^{\infty}$ and $\{y_i\}_{i=1}^{\infty}$ as follows;

$$\begin{array}{llll} q_1 = & \omega(x_1, q_0) & y_1 = & \nu(x_1, q_0) \\ q_2 = & \omega(x_2, q_1) & y_2 = & \nu(x_2, q_1) \\ \vdots & \vdots & \vdots & \vdots \\ q_i = & \omega(x_i, q_{i-1}) & y_i = & \nu(x_i, q_{i-1}) \\ \vdots & \vdots & \vdots & \vdots \end{array}$$

Each element of the sequence $\{q_i\}_{i=1}^{\infty}$ is in the state group of $\mathcal{C}$ and each y_i is Y.

Proposition 1: Let Q be a finite sate group with identity element e_Q. If there is an state $q \in Q$ such that $q \neq \omega(x_n, \omega(x_n, \omega(x_{n-1}, \ldots, \omega(x_2, \omega(x_1, e_Q))\ldots)$, for all sequence $\{x_i\}_{i=1}^{n}$ of inputs; then the group code $\mathcal{C}$ is non controllable

Proof.- Since ω is surjective, then there is an ordered pair (x_1, q_1) such that $\omega(x_1, q_1) = q$. For q_1 there is (x_2, q_2) such that $\omega(x_2, q_2) = q_1$ In this iterative way we can construct a sequence $\{(x_m, q_m)\}_m$ with $\omega(x_m, q_m) = q_{m-1}$. Since Q is finite exists a subset $Q_q \subset Q$ such that $q_m \in Q_q$ for all m. Notice that Q_q must be a proper subset of Q because the condition of the Proposition. Then; for any code y, with $y_1 = \nu(x_1, e_Q)$, and the *all zeroes* code $y\prime$ given by $y_n = e_Y$ for all $n \in \mathbb{N}$; there is not any code $y\prime\prime$ satisfying the conditions of the Definition (2) ■

Given an encoder $M = (X, Y, Q, \nu, \omega)$ consider the family$\{Q_i\}$, recursively defined by;

$$\begin{array}{lcl} Q_0 & = & \{e_Q\} \\ Q_1 & = & \{\omega(x,q)\ ;\ x \in X, q \in Q_0\} \\ Q_2 & = & \{\omega(x,q)\ ;\ x \in X, q \in Q_1\} \\ \vdots & \vdots & \vdots \\ Q_i & = & \{\omega(x,q)\ ;\ x \in X, q \in Q_{i-1}\} \\ \vdots & = & \vdots \end{array} \tag{5}$$

Proposition 2: Some properties of the family $\{Q_i\}$;
1. $Q_1 \triangleleft Q$
2. $Q_{i-1} \triangleleft Q_i$, for all $i = 1, 2, \ldots$.
3. $Q_{i-1} = Q_i$ implies $Q_i = Q_{i+1}$
4. If the family $\{Q_i\}_i$ is not a normal series then the group code is non controllable

Proof.-
1. Let $\omega(x, e_Q)$ and q be arbitrary elements of Q_1 and Q, respectively. Since ω is surjective, there is $p \in Q$ such that $\omega(x_1, p) = q$, for some $x_1 \in X$. Hence, by using the fact that ω is a group homomorphism and the operation (1) of the extension group $X_{\phi_\varsigma}Q$; $q.\omega(x, e_Q).q^{-1} = \omega(x_1, p).\omega(x, e_Q).\omega(x_1, p)^{-1} = \omega((x_1, p).(x, e_Q).(x_1, p)^{-1}) = \omega(x_2, pe_Qp^{-1}) = \omega(x_2, e_Q) \in Q_1$. Therefore $Q_1 \triangleleft Q$.
2. In the first place we show that $Q_{i-1} \subset Q_i$, for any i. Clearly $Q_0 \subset Q_1$. Now, for $i > 1$, suposse $Q_{j-1} \subset Q_j$, for all $j \leq i$. Given $q \in Q_i$ There are $p \in Q_{i-1}$ and $x \in X$ such that $\omega(x, p) = q$. On the other hand, $p \in Q_{i-1} \subset Q_i$ implies that $\omega(x, p) = q \in Q_{i+1}$.
On the other hand, clearly $Q_0 \triangleleft Q_1$. For $i > 1$, suposse $Q_{j-1} \subset Q_j$, for all $j \leq i$. Given $q \in Q_{i+1}$ e $p \in Q_i$, consider $q.p.q^{-1} = \omega(x, p_1).\omega(u, q_1).\omega(x, p_1)^{-1}$, where $p_1 \in Q_i$, $q_1 \in Q_{i-1}$, $x, u \in X$. Hence, $q.p.q^{-1} = \omega(x_1, p_1.q_1.p_1^{-1}) \in Q_i$, because $p_1.q_1.p_1^{-1} \in Q_{i-1}$.
3. Given $q \in Q_{i+1}$ there are $p \in Q_i$ e $x \in X$ such that $\omega(x, p) = q$. Since $Q_i = Q_{i-1}$, $p \in Q_{i-1}$. Hence $\omega(x, p) = q \in Q_i$.
4. Let Q_S be such that $Q_S = \cup_i Q_i$. Then, $Q_i \subset Q_S$ for all i. If $Q_S = Q$ then $\{Q_i\}_i$ is a normal series. If $Q_S \neq Q$, there is $q \in Q$ such that $q \notin Q_S$. This q is an isolated state from respect the neutral e_Q state, as in the Proposition 1, thus the group code is a non controllable one.■

Proposition 3: If $Q_i \subsetneq Q$ is invariant under the group $Aut(Q)$ then the group code is non controllable.

Proof.- Let G be such that $G \overset{\theta}{\cong} X_{\phi_\varsigma}Q$. Let $\omega : G \to Q$ be a surjective homomorphism from the definition of the encoder. If $\pi : G \to G/N$ is the fixed natural homomorphism and $\psi : Q \to G/N$ is the fixed homomorphism used in (1), then the choice of ω depends only on the choice of $\varphi \in Aut(Q)$. That is, $\omega = \varphi_o\psi_o^{-1}\pi$, as is shown in the Figure 2. Therefore, $\omega(x, Q_i) = \varphi_o\psi_o^{-1}\pi(x, Q_i) = \varphi(Q_i) = Q_i$, for all $x \in X$. ■

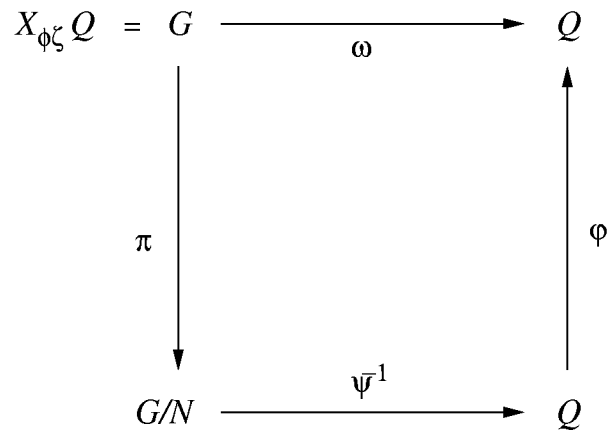

Fig. 2. The states homomorphism ω

In particular if some Q_i is contained in the derived subgroup Q', which is invariant under $Aut(Q)$, then the code will be non controllable.

On the other hand, given the extension $X_{\phi_\varsigma}Q$, the number of transitions flowing from the neutral state e_Q is $|X| = |X_0|.|Q_1|$, where X_0 is a normal subgroup of X given by $X_0 = \{x \in X\ ;\ \omega(x, e_Q) = e_Q\}$, [3]. Thus, $|Q_1|$ must be a divisor of $|X|$. In the particular case of the trellis be-

ing without parallel transitions, that is $|X_0| = 1$, we have $|Q_1| = |X|$.

Thus we have shown the main result of this work;

Theorem 1: Let $X_{\phi_\varsigma}Q$ be an extension. If there is an controllable associated group code $\mathcal{C}$, then Q must have a normal series $e_Q = Q_0 \triangleleft Q_1 \triangleleft \cdots \triangleleft Q_{n-1} \triangleleft Q_n = Q$ such that
1. $Q_1 \triangleleft Q$ and $|Q_1|$ is a divisor of $|X|$,
2. $Q_i \not\subset Q'$, for all $i = 1, 2, \ldots$, where Q' is the derived subgroup of Q.

Example 3: Consider the extension $\mathbb{Z}_{2\phi_\varsigma}D_8$ from the Example 2.

Among all the normal series just the following ones satisfy the necessary first condition of the above Theorem
- $\{R_0\} \triangleleft \{R_0, R_2\} \triangleleft \{R_0, R_2, R_1, R_3\} \triangleleft D_8$,
- $\{R_0\} \triangleleft \{R_0, R_2\} \triangleleft \{R_0, R_2, d_1, d_2\} \triangleleft D_8$.
- $\{R_0\} \triangleleft \{R_0, R_2\} \triangleleft \{R_0, R_2, H, V\} \triangleleft D_8$.

But both the three series fault the second necessary condition beacuse $\{R_0, R_2\}$ is the derived subgroup of D_8. Therefore there is not any controllable group code $\mathcal{C}$ associated to the extension $\mathbb{Z}_{2\phi_\varsigma}D_8$.

IV. Conclusions

In this work we have shown the fundamentals of one necessary test of controllability of group codes. This test combines both the algebraic and system theoretic point of view. We hope that this can be the basis for an algorithm which may be implemented in GAP [10], for instance. We also expect this work may help to achieve more elaborated algebraic techniques to overcome the control problem of group codes.

References

[1] Slepian, D.; "Group Codes for the Gaussian Channels". *Bell* Systems Technical Journal, 47:575–602.

[2] G.D.Forney, "Geometrically uniform codes" *IEEE Trans. Inform. Theory*; vol. IT-37 No 5, pp. 1241-1260, 1991.

[3] G.D. Forney and M.D. Trott, "The dynamics of group codes: state spaces, trellis diagrams and canonical encoders", *IEEE Trans. Inform. Theory*, vol IT 39(5):1491-1513, September 1993.

[4] H.A. Loeliger; "Signal sets matched to groups", *IEEE Transactions on Information Theory* Vol 37, No 6, pp 1675-1682, November 1991.

[5] J.C.Willems, "Models for dynamics" em *Dynamics Technical Report* vol. 2, U.Kirchgraber e H.O.Walther, Eds. Wiley and Teubner, 1989.

[6] H.A. Loeliger, Mittelholzer T.; "Convolutional Codes Over Groups", *IEEE Transactions on Information Theory* Vol IT 42, No 6, pp 1659-1687, November 1996.

[7] Rotman J. J.; *An Introduction to the Theory of the Groups*, Fourth Ed., Springer Verlag 1995.

[8] Hall M. Jr..; *The Theory of Groups*, MacMillan, New York, 1959.

[9] A. Garcia, Y Lequain, *Álgebra, um Curso de Introdução;* Projeto Euclides 18, IMPA Rio de Janeiro, 1988.

[10] The GAP Group — Groups, Algorithms, and Programming, Version 4.2; Aachen, St Andrews, 1999.
(http://www-gap.dcs.st-and.ac.uk/ gap)

[11] G. Ungerboeck; "Channel coding with multilevel phase signal", *IEEE Transactions on Information Theory* Vol IT 25, pp 55-67, Jan 1982.

[12] J. Bali, Rajan, S; "Block-Coded modulation using two-level group-codes over dihedral groups", *IEEE Transactions on Information Theory* Vol IT 44, pp 1620-1631, July 1998.