Some Necessary Conditions for Abelian Group Codes with prime Information Group

Jorge Pedraza Arpasi, Tiago Belmonte Nascimento

***Resumo*— Códigos de Grupo são uma generalização dos Códigos Convolucionais. Por isso, algumas vezes, os Códigos de Grupo também são chamados de Códigos Convolucionais Generalizados. Um codificador convolucional clássico com taxa $\frac{k}{n}$ e m registros de memória pode ser descrito como uma Máquina de Estados Finito em termos dos grupos binários $\mathbb{Z}_2^k$, $\mathbb{Z}_2^n$ e $\mathbb{Z}_2^m$ e homomorfismos adequadamente definidos sobre o produto direto $\mathbb{Z}_2^k \oplus \mathbb{Z}_2^m$. O código convolucional é a família de sequências bi-infinitas produzidas pelo codificador convolucional. Generalizando esta idéia um código de grupo é uma família de sequências produzidas por uma Máquina de Estados Finito definido sobre a extensão de dois grupos finitos $U \boxtimes S$. Considerado como um conjunto de sequências, um código de grupo é um Sistema Dinâmico e é fato conhecido que sistemas dinâmicos bem comportados devem necessariamente ser controláveis. Assim, um bom código de grupo deve ser controlável. Neste artigo trabalhamos com códigos de grupo definidos sobre grupos abelianos com grupo de informação $\mathbb{Z}_p$ e estabelecemos algumas condições necessárias sobre o controle destes códigos.**

***Palavras-Chave*— Códigos de grupo, sistemas dinâmicos, controle, p-grupos**

***Abstract*— Group Codes are a generalization of the well known Convolutional Codes. For this reason, sometimes, Group Codes are also called as Generalized Convolutional Codes. A classical convolutional encoder with rate $\frac{k}{n}$ and m memory registers can be described as a Finite State Machine in terms of the binary groups $\mathbb{Z}_2^k$, $\mathbb{Z}_2^n$ and $\mathbb{Z}_2^m$ and adequate homomorphisms over the direct product $\mathbb{Z}_2^k \oplus \mathbb{Z}_2^m$. The convolutional code is a family of bi-infinite sequences produced by the convolutional encoder. Generalizing the just above idea, a group code is a family of bi-infinite sequences produced by a Finite State Machine (FSM) homomorphic encoder defined on the extension of two finite groups $U \boxtimes S$. As a set of sequences, a group code is a Dynamical System and it is known that well behaved dynamical systems must be necessarily controllable. Thus, a good group code must be controllable. In this paper we work with group codes defined over abelian groups with information group $\mathbb{Z}_p$ and give necessary conditions on the control of these codes.**

***Keywords*— Group codes, dynamical systems, controllability, p-groups.**

I. INTRODUCTION

Let $\mathbb{Z}$ be the set of integers. Over a family of groups with integer indices, $\{G_k\}_{k\in\mathbb{Z}}$, we can construct the bi-infinite direct product $\mathcal{G} = \cdots \times G_{k-1} \times G_k \times G_{k+1} \times \ldots$. Each element of $\mathcal{G}$ is a sequence $\{g_k\}_{k\in\mathbb{Z}}$, $g_k \in G_k$, and with the group operations induced componentwise from each G_k, $\mathcal{G}$ is also a group. Then, a generalized *group code* $\mathcal{C}$, is a subgroup of $\mathcal{G}$. If each group G_k is equal to a fixed group G, then we have $\mathcal{G} = G^{\mathbb{Z}} = \cdots \times G \times G \times G \times \ldots$. In this last case, a subgroup $\mathcal{C}$ of $\mathcal{G}$ is called *time invariant group code* [1], [2], [3], [4]

Group codes are a subclass of Error Correcting Codes (ECC), which can detect and correct transmission errors originated from noisy communication channels. In communication engineering, noise is modeled as a random signal. The most known noise is the Gaussian noise, which is modeled as a random signal having a normal probabilistic distribution. The channels suffering Gaussian noise are called *additive white Gaussian noise* - AWGN channels [5], [6], [7], [8]. The essence of ECC is the addition of redundancy to the original message. More redundant information means more protected information. That fact reduces the transmission velocity of the channel. Then trade-off between velocity of transmission and protection of information must be done, and this depends on the channel class [9], [10]. Telephone channels need real time transmissions and they prioritize velocity over some little errors on the human voice. On the other hand bank transaction channels need strong protection on the transmitted data.

The purpose of this work is the study of group codes for the abelian case. In [11] it has been shown that there are not good group codes over non abelian groups with information group being $\mathbb{Z}_p$. A study on arbitrary abelian extensions $U \boxtimes S$ was did before in [12] where the main concern was a minimality of the states group. We will be concerned with control. For that this work is organized as follow:

In the Section II is defined the extension of a group U by the group S, this extension is denoted as $U \boxtimes S$. Then is defined the FSM encoder of a group code which also is called ISO (Input/State/Output) machine. The next state mapping $\nu : U \boxtimes S \to S$ and the encoder (output) mapping $\omega : U \boxtimes S \to Y$ are defined over the extension $U \boxtimes S$. Finally, is defined the group code $\mathcal{C}$, produced by the FSM encoder, as a family of bi-infinite sequences of outputs.

In the Section III the group code $\mathcal{C}$ is presented as a Dynamical System in the sense of [13]. Also a graphical description of a group code known as a trellis is presented. It is established that the trellis diagram is a set of paths of transitions between states. After given the control definition, a sufficient condition of non-controllability is made in the Theorem 2.

In the Section IV we present our original contributions about the controllability of group codes produced by encoders defined on abelian extensions $\mathbb{Z}_p \boxtimes S$. It is studied the group code of states S. The main result of this work, Theorem 5, refers to the sequence of subsets $\{S_i\}$ of S recursively defined

Jorge Pedraza Arpasi, Universidade Federal do Pampa - UNIPAMPA, Centro Tecnológico de Alegrete, E-mail: jorgearpasi@unipampa.edu.br, Tiago Belmonte Nascimento, Universidade Federal do Pampa - UNIPAMPA, Centro Tecnológico de Alegrete, E-mail: tiagonascimento@unipampa.edu.br

by

$$\begin{array}{lcl} S_0 & = & \{e\},\ e \text{ is the identity element of } S \\ S_1 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_0\} \\ S_2 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_1\} \\ \vdots & \vdots & \vdots \\ S_i & = & \{\nu(u,s)\ ;\ u \in U, s \in S_{i-1}\}, i \geq 0 \\ \vdots & = & \vdots \end{array} \quad (1)$$

Then, we will show that a necessary condition for an abelian group code with information group $\mathbb{Z}_p$ be controllable is: *If S_2 is cyclic then S_3 must be also cyclic*.

II. Group extensions and Group Codes

A. Group extensions

Definition 1: An **extension** of a group U by a group S is a group G with a normal subgroup N, such that $N \cong U$ and $\frac{G}{N} \cong S$, [14].

The extension "U by S"we will denote by the symbol $U \boxtimes S$. When G is an extension $U \boxtimes S$, each element $g \in G$ can be "factored" as an unique ordered pair (u, s), $u \in U$ and $s \in S$. The semi-direct product $U \rtimes S$ is a particular case of extension, but also it is known that the semi-direct product is a generalization of the direct product $U \times S$. Canonical definition of extension of groups is given in [14], [15], specially in [15] we find a "practical"way to decompose a given group G, with normal subgroup N, in an extension $U \boxtimes S$. That decomposition depends on the choice of isomorphisms $\upsilon : N \to U$, $\psi : S \to \frac{G}{N}$ and a lifting $l : \frac{G}{N} \to G$ such that $l(N) = e$, the neutral element of G. Then, defining $\phi : S \to Aut(U)$ by,

$$\phi(s)(u) = \upsilon[l(\psi(s)).\upsilon^{-1}(u).(l(\psi(s)))^{-1}], \quad (2)$$

and $\xi : S \times S \to U$

$$\xi(s_1, s_2) = l(\psi(s_1, s_2))l(\psi(s_1))l(\psi(s_2)), \quad (3)$$

the decomposition $U \boxtimes S$ with the group operation

$$(u_1, s_1) * (u_2, s_2) = (u_1.\phi(s_1)(u_2).\xi(s_1, s_2)\ ,\ s_1 s_2) \quad (4)$$

is isomorphic with G, that is, $g = (u, s)$.

Notice that the resulting pair of $(u_1, s_1).(u_2, s_2)$, of the above operation (4), is $(u', s_1 s_2)$ for some $u' \in U$, and $s_1 s_2$ is the operation on S. This property allow us to do not be concerned to obtain an explicit result when multiple factors are acting. For instance, in the proof of some Lemmas it will be enough to say that $(u', s_1 s_2 \dots s_n)$, is the resulting pair of the multiple product $(u_1, s_1) \cdot (u_2, s_2) \cdot (u_3, s_3) \dots (u_n, s_n)$, where u' is some element of U. Analogously, $(u, s)^n = (u', s^n)$ for some $u' \in U$.

Example 1: Consider the direct product group $\mathbb{Z}_2^3 = \{(x_1, x_2, x_3)\ ;\ x_i \in \mathbb{Z}_2\}$. This abelian group can be decomposed as an extension $\mathbb{Z}_2 \boxtimes \mathbb{Z}_2^2$.

By using the more convenient notation 00 instead $(0, 0)$, 010 instead $(0, 1, 0)$, etc., we have that the normal subgroup $N = \{000, 100\} \triangleleft \mathbb{Z}_2^3$ is isomorphic with $\mathbb{Z}_2$. The quotient group $\frac{\mathbb{Z}_2^3}{N} = \{\{000, 100\}, \{010, 110\}, \{001, 101\}, \{111, 011\}\}$ is isomorphic with $\mathbb{Z}_2^2$. Thus, in an expected way, we have shown that $\mathbb{Z}_2^3$ is an extension of $\mathbb{Z}_2 \boxtimes \mathbb{Z}_2^2$.

Theorem 1: If the mapping $\phi : S \to Aut(U)$ is not trivial then the extension $U \boxtimes S$ is non-abelian

Proof.- Since ϕ is not trivial, there are $u \in U$ and $s \in S$ such that $\phi(s)(u) \neq u$. Now, consider the pairs $(e, s), (u, e) \in U \boxtimes S$, where e is the neutral element of the respective group. Then $(e, s)(u, e) = (e.\phi(s)(u).\xi(s, e), s) = (\phi(s)(u), s)$. On the other hand $(u, e)(e, s) = (u.\phi(e)(e).\xi(e, s), s) = (u, s)$. Therefore $(e, s)(u, e) \neq (u, e)(e, s)$.

B. Finite State Machines and Group Codes

Finite State Machines (FSM) are a subject of Automata Theory. M. Arbib in [16] describes a FSM as a quintuple $M = (I, S, O, \delta, \xi)$, where I is the inputs alphabet, S is the alphabet of states of the machine, O is the outputs alphabet, $\delta : I \times S \to S$ is the next state mapping, and $\xi : I \times S \to O$ is the output mapping. Following [17], [3], [2] and by making modifications on the FSM notation, suitable for our context of group codes, it is given the definition of an encoder as follows.

Definition 2: Let U, S, and Y be finite groups. Let $\nu : U \boxtimes S \to S$ and $\omega : U \boxtimes S \to Y$ be group homomorphisms defined over an extension $U \boxtimes S$ such that the mapping $\Psi : U \boxtimes S \to S \times Y \times S$ defined by

$$\Psi(u, s) = (s, \omega(u, s), \nu(u, s)) \quad (5)$$

is injective with ν surjective. Then, an encoder of a group code is the Machine $M = (U, S, Y, \omega, \nu)$.

The group U is called the uncoded information group and Y is called the encoded information group. To begin working, the encoder needs an initial state $s_0 \in S$ and a sequence of inputs $\{u_i\}_{i=1}^n$, $u_i \in U$. Then the encoder will respond with two sequences $\{s_i\}_{i=1}^n$, $s_i \in S$, and $\{y_i\}_{i=1}^n$, $y_i \in Y$ in the following way;

$$\begin{array}{rcl|rcl} \nu(u_1, s_0) & = s_1 & & \omega(u_1, s_0) & = y_1 \\ \nu(u_2, s_1) & = s_2 & & \omega(u_2, s_1) & = y_2 \\ \nu(u_3, s_2) & = s_3 & & \omega(u_3, s_2) & = y_3 \\ \vdots & \vdots & & \vdots & \vdots \\ \nu(u_n, s_{n-1}) & = s_n & & \omega(u_n, s_{n-1}) & = y_n \end{array}$$

If we agree that the present time is 0 (zero) and the state s_0 represents the present state, then the next integer time is 1 (one) and s_1 represents the next state from now. Analogously, the next state from s_1 will be s_2 and generally s_i will be the next state from s_{i-1}. In this way, states with positive indices, $\{s_i\}_{i=1}^n$, forms a sequence of future states.

On the other hand, since ν is surjective, then must exist at least one pair (u_0, s_{-1}) such that $s_0 = \nu(u_0, s_{-1})$. The state s_{-1} can represent the previous state from the present state s_0. Analogously for s_{-1} there must exist a pair (u_{-1}, s_{-2}) such that $\nu(u_{-1}, s_{-2}) = s_{-1}$ with s_{-2} representing a previous state from s_{-1} and so on $s_{\{-i+1\}}$ is one previous state from s_{-i}. Thus, for a given present sate s_0, there are sequences of past states $\{s_i\}_{i=-n}^{-1}$, past outputs $\{y_i\}_{i=-n}^{-1}$, and past inputs

$\{u_i\}_{i=-n+1}^{0}$ such that;

$$\begin{array}{cc|cc} \nu(u_0,s_{-1}) & =s_0 & \omega(u_0,s_{-1}) & =y_0 \\ \nu(u_{-1},s_{-2}) & =s_{-1} & \omega(u_{-1},s_{-2}) & =y_{-1} \\ \nu(u_{-2},s_{-3}) & =s_{-2} & \omega(u_{-2},s_{-3}) & =y_{-2} \\ \vdots & \vdots & \vdots & \vdots \\ \nu(u_{\{-n+1\}},s_{-n}) & =s_{\{-n+1\}} & \omega(u_{\{-n+1\}},s_{-n}) & =y_{\{-n+1\}} \end{array}$$

Therefore, given bi-infinite sequence of inputs $\{u_i\}_{i\in\mathbb{Z}}$, $u_i \in U$ and one state $s_0 \in S$, make sense to say that, the encoder $M=(U,S,Y,\nu,\omega)$ will response with the sequence $\{y_i\}_{i\in\mathbb{Z}}$, $y_i \in Y$, of outputs while its internal states will have the sequence $\{s_i\}_{i\in\mathbb{Z}}$, $s_i \in S$. Notice that once made the choice of one initial state s_0, the future relations between the inputs and outputs-states sequences is bijective, that is,
$\{\{u_k\}_{i\in\mathbb{N}}\} \overset{1-1}{\rightleftarrows} \{\{y_i\}_{i\in\mathbb{N}},\{s_i\}_{i\in\mathbb{N}}\}$, where $\mathbb{N}=\{1,2,3,\dots\}$ is the natural numbers set.

Definition 3: A time invariant group code $\mathcal{C}$ is the family of bi-infinite sequences $\mathbf{y}=\{y_i\}_{i\in\mathbb{Z}}$ produced by the encoder $M=(U,S,Y,\nu,\omega)$, with $y_i=\omega(u_i,s_{i-1})$. Each sequence $\mathbf{y}=\{y_i\}_{i\in\mathbb{Z}}$ is called a *codeword*, [1], [2], [3], [4].

Example 2: Consider the encoder $M=(\mathbb{Z}_2,\mathbb{Z}_2^2,\mathbb{Z}_2^3,\omega,\nu)$ where $\nu:\mathbb{Z}_2\boxtimes\mathbb{Z}_2^2\to\mathbb{Z}_2^2$ defined by $\nu(u,s_1,s_2)=(u+s_2,s_1)$ and $\omega:\mathbb{Z}_2\boxtimes\mathbb{Z}_2^2\to\mathbb{Z}_2^3$ is defined by $\omega(u,s_1,s_2)=(s_2,u,s_1)$

Suposse the encoder is initialized at state $s_0=00$ then for the inputs sequence $\{1,1,0,0,1,1,0,1,0,1\}$ the encoder states will be $\{10,11,11,11,01,00,00,10,01,00\}$ and the sequence of encoded outputs will be $\{010,011,101,101,111,110,000,010,001,110\}$.

III. Controll and Group Codes

Each codeword of a group code satisfies the definition of a trajectory of a Dynamical System in the sense of Willems [13]. From this each group code $\mathcal{C}$ is a dynamical system. In this context, the encoder $M=(U,S,Y,\nu,\omega)$ is a *realization* of $\mathcal{C}$, [3], [2], [12].

Given a codeword $\mathbf{y}$ and a set of consecutive indices $\{i,i+1,\dots,j-1,j\}=[i,j]$, the projection of the codeword over these indices will be $\mathbf{y}|_{[i,j]}=\{y_i,y_{i+1},\dots,y_j\}$. Analogously $\mathbf{y}|_{[i,j)}=\{y_i,y_{i+1},\dots,y_{j-1}\}$, $\mathbf{y}|_{[i,+\infty)}=\{y_i,y_{i+1},\dots\}$ and so on. With this notation the *concatenation* of two codewords $\mathbf{y_1},\mathbf{y_2}\in\mathcal{C}$ in the instant j is a sequence $\mathbf{y_1}\wedge_j\mathbf{y_2}$ defined by
$\begin{cases}(\mathbf{y_1}\wedge_j\mathbf{y_2})|_{(-\infty,j)}=\mathbf{y_1}|_{(-\infty,j)};\\ (\mathbf{y_1}\wedge_j\mathbf{y_2})|_{[j,+\infty)}=\mathbf{y_2}|_{[j,+\infty)}.\end{cases}$

Definition 4: If L is an integer greater than one, then a group code $\mathcal{C}$ is said L-controllable when for any pair of codewords $\mathbf{y_1}$ and $\mathbf{y_2}$, there are a codeword $\mathbf{y_3}$ and one integer k such that the concatenation $\mathbf{y_1}\wedge_k\mathbf{y_3}\wedge_{k+L}\mathbf{y_2}$ is a codeword of the group code $\mathcal{C}$. [4], [1], [13].

It is said that a natural number $l>1$ is the index of controllability of a group code $\mathcal{C}$ when $l=min\{L\ ;\ \mathcal{C}\text{ is }L-\text{controllable }\}$. Any applicable group code, for correction of errors of transmission and storage of information, needs to have an index of controllability. Shortly, when a code has an index of controllability then is said that it is controllable [13]. Clearly, a code $\mathcal{C}$ to be L-controllable is a sufficient condition for $\mathcal{C}$ to be controllable.

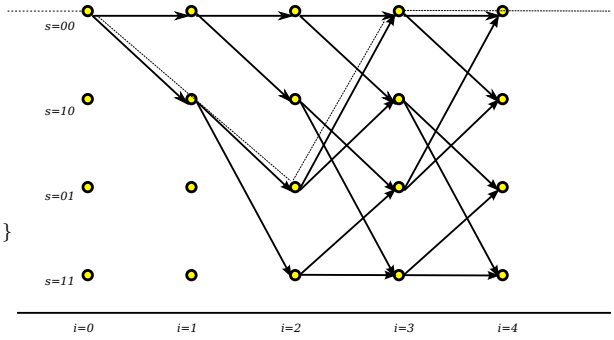

Fig. 1. Trellis diagram of the encoder $M=(\mathbb{Z}_2,\mathbb{Z}_2^2,\mathbb{Z}_2^3,\omega,\nu)$

A. The Trellis of a Group Code

The triplets $(s,\omega(u,s),\nu(u,s))$ of the set $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$, where Ψ is defined by (5), can be represented graphically. In the context of Graph Theory, [18], they are called *edges* whose vertices set is S and the graph is called *state diagram* labeled by $\omega(u,s)$. In the Figure 1 the full state diagram of the code generated by the FSM $M=(\mathbb{Z}_2,\mathbb{Z}_2^2,\mathbb{Z}_2^3,\omega,\nu)$ is shown between the times 2 and 3 also it is repeated between the times 3 and 4. In the context of Coding Theory the elements of $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$ are called *transitions* or *branches*. The expansion in time of the state diagram is called *trellis diagram*. This is made by concatenating at each time unit separate state diagram. For two consecutive time units i and $i+1$, the transitions $b_i=(s_i,\omega(u_{i+1},s_i),\nu(u_{i+1},s_i))$ and $b_{i+1}=(s_{i+1},\omega(u_{i+2},s_{i+1}),\nu(u_{i+2},s_{i+1}))$ are said concatenated when $s_{i+1}=\nu(u_{i+1},s_i)$. Hence a bi-infinite *trellis path* of transitions is a sequence $\mathbf{b}=\{b_i\}_{i\in\mathbb{Z}}$ such that b_i and b_{i+1} are concatenated for each $i\in\mathbb{Z}$. The set of trellis paths form the trellis diagram. Since each codeword $\mathbf{y}$ passes only by one state s at each unit of time, then the relation between the codewords $\mathbf{y}$ and paths $\mathbf{b}$ is bijective. A path $\mathbf{b}=\{b_i\}_{i\in\mathbb{Z}}$ with $b_0=(00,010,10)$, $b_1=(10,001,01)$ $b_2=(01,110,00)$ and $b_i=(00,000,00)$ for all $i\in\mathbb{Z}-\{0,1,2\}$ it is shown by a traced line in Figure 1.

Definition 5: Two states s and r are said *connected* when there are a path $\mathbf{b}$ and indices $i,j\in\mathbb{Z}$ such that $\mathbf{b}|_{[i,j]}=\{b_i,b_{i+1},\dots,b_j\}$ with $b_i=(s_i,\omega(u_{i+1},s_i),\nu(u_{i+1},s_i))$ and $b_j=(s_j,\omega(u_{j+1},s_j),\nu(u_{j+1},s_j))$ such that $s=s_i$ and $r=\nu(u_{j+1},s_j)$.

Theorem 2: Let $\mathcal{C}$ be a group code produced by the encoder $M=(U,S,Y,\omega,\nu)$. If there are two states $s\in S$ and $r\in S$ for which there is not a finite path of transitions connecting them then $\mathcal{C}$ is **non-controllable**.

Proof: On the contrary there is $l>1$ such that l is the controllability index of $\mathcal{C}$. Let $\mathbf{y_1}$ be one codeword passing by the state s at time k, let $\mathbf{y_2}$ be a codeword passing by the state r at time $k+L$, $L\geq l$. There must exist $\mathbf{y_3}\in\mathcal{C}$ with its respective path $\mathbf{b_3}$ such that $\mathbf{y_3}|_{(-\infty,k)}=\mathbf{y_1}|_{(-\infty,k)}$ and $\mathbf{y_3}|_{[k+L,+\infty)}=\mathbf{y_1}|_{[k+L,+\infty)}$ and $\mathbf{b_3}|_{(k,k+L]}$, a finite path, connecting s and r. Contradiction. ■

Equivalently, we can say that two states s and r are connected when there is a finite sequence of inputs $\{u_i\}_{i=1}^{n}$ such that

$$r = \nu(u_n, \nu(u_{n1}, \dots \nu(u_2, \nu(u_1, s)) \dots)) \tag{6}$$

Theorem 3: Given a encoder (U, S, Y, ν, ω) consider the family of state subsets $\{S_i\}$, recursively defined in the equation (1) then;

1) Each S_i is a subgroup of S
2) S_{i-1} is normal in S_i , for all $i = 1, 2, \dots$.
3) If $S_{i-1} = S_i$ then $S_i = S_{i+1}$.
4) If S_i is cyclic then S_k is cyclic for all $k \leq i$.
5) If the group code is controllable then $S = S_k$ for some k.

Proof:

1) By induction. Consider $r, s \in S_i$, Since ν is surjective, there exist (u_1, s_1) and (u_2, s_2) with $s_1, s_2 \in S_{i-1}$ and $u_1, u_2 \in U$ such that $r = \nu(u_1, s_1)$ and $s = \nu(u_2, s_2)$. Hence, $sr = \nu(u_3, s_1 s_2)$, $u_3 \in U$ and thus $sr \in S_i$.
2) Clearly $S_0 \triangleleft S_1$. For $i > 1$, suppose $S_{j-1} \triangleleft S_j$, for all $j \leq i$. Given $s \in S_{i+1}$ and $r \in S_i$, consider $s.r.s^{-1} = \nu(u, s_1).\nu(v, r_1).\nu(u, s_1)^{-1}$, where $s_1 \in S_i$, $r_1 \in S_{i-1}$, $u, v \in U$. Hence, $s.r.s^{-1} = \nu(u_1, s_1.r_1.s_1^{-1}) \in S_i$, because $s_1.r_1.s_1^{-1} \in S_{i-1}$.
3) Given $s \in S_{i+1}$ there are $r \in S_i$ and $u \in U$ such that $\nu(u, r) = s$. Since $S_i = S_{i-1}$, $r \in S_{i-1}$. Hence $\nu(u, r) = s \in S_i$.
4) S_i means all its subgroups are cyclic.
5) If not, there is $s \in S$ such that $s \notin S_k$ for any $k \in \mathbb{N}$. Then, the neutral state $e \in S_k \subset S$ and s are not connected by any finite trellis path. Therefore the group code is non-controllable.

■

In the Figure 1 $S_0 = \{00\}$, $S_1 = \{00, 10\}$, $S_2 = \{00, 10, 01, 11\} = S$, therefore the code is controllable.

Lemma 1: Let S^- be the full one-time past of the neutral state $s_0 = e \in S$, precisely defined by

$$S^- = \{s \in S \; ; \; \nu(u, s) = e \, , \text{for some} \, u \in U\}. \tag{7}$$

Then S^- is a normal subgroup of S and $|S^-| = |S_1|$

Proof: Consider the kernels of the second projection $\pi_2(u, s) = s$ and the next state mapping ν. Both are surjective homomorphisms, then by the fundamental Theorem of homomorphisms $\frac{U \boxtimes S}{ker(\nu)} \cong S$ and $\frac{U \boxtimes S}{ker(\pi_2)} \cong S$. Hence $|ker(\nu)| = |ker(\pi_2)|$. The statement of the Lemma is satisfied noticing that $S^- = ker(\nu)$ and $S_1 = ker(\pi_2)$. ■

IV. The encoder $(\mathbb{Z}_p, S, Y, \nu, \omega)$ with p prime

Lemma 2: The abelian extension $\mathbb{Z}_p \boxtimes \mathbb{Z}_m$ either is isomorphic to the direct product $\mathbb{Z}_p \oplus \mathbb{Z}_m$ or it is isomorphic to the cyclic group $\mathbb{Z}_{pm}$.

Proof: Consider the element $(1, 0) \in \mathbb{Z}_p \boxtimes \mathbb{Z}_m$. By the Theorem 1, about the equation (2), $(1, 0)^2 = (1 + 1 + \xi(0, 0), 0)$. Now, by the equation (3), $\xi(0, 0) = 0$. Thus, $(1, 0)^2 = (2, 0)$ and in general $(1, 0)^n = (n, 0)$, for any $n \in \{1, 2, \dots, p-1\}$. Therefore $H = \{(1, 0), (2, 0), \dots, (p-1, 0), (0, 0)\}$ is a cyclic subgroup isomorphic with $\mathbb{Z}_p$. On the other hand consider the element $(0, 1) \in \mathbb{Z}_p \boxtimes \mathbb{Z}_m$. If $(0, 1)^m = (0, 0)$, then the subgroup $K = \{(0, 1), (0, 2), \dots, (0, m-1), (0, 0)\}$ is isomorphic with $\mathbb{Z}_m$ and $H \cap K = \{(0, 0)\}$. In this case, in accordance with the Theorem 2.29, pg 40 of [14] $\mathbb{Z}_p \boxtimes \mathbb{Z}_m$ must be isomorphic with the direct product $\mathbb{Z}_p \oplus \mathbb{Z}_m$. In the case of $(0, 1)^m = (u, 0)$, with $u \neq 0$ we have that u is a generator of $\mathbb{Z}_p$, then $((0, 1)^m)^p = (u, 0)^p = (0, 0)$ with $((0, 1)^m)^i \neq (0, 0)$ for $0 < i < p$. Therefore, $(0, 1)^m = (u, 0)$ implies that $\mathbb{Z}_p \boxtimes \mathbb{Z}_m$ is isomorphic with the cyclic group $\mathbb{Z}_{pm}$. ■

Lemma 3: Consider the encoder $M = (\mathbb{Z}_p, S, Y, \omega, \nu)$, with p prime. Also consider the subgroup S^- of the Equation (7) and the sequence of subgroups S_i of the equation (1), then;

1) If there are $s \neq e$ and $s \in S^- \cap S_i$ then $S^- \subset S_i$, for $i \geq 0$;
2) If $S^- \subset S_i$ then $\nu(\mathbb{Z}_p, S^-) \subset S_i$, for $i \geq 0$.

Proof:

1) Since $s \in S^- \cap S_i$, then $\{s, s^2, \dots, s^{p-1}, s^p = e\} \subset S^- \cap S_i$.
2) Given $r \neq e$ such that $r \in S_i \cap S^-$ suppose there is some $u \in \mathbb{Z}_p$ such that $\nu(u, r) = s \notin S_i$. For the subgroup $S_1 = \{s_0, s_1 = \nu(u_1, e), s_2 = \nu(u_2, e), \dots, s_{p-1} = \nu(u_{p-1}, e)\}$, we have that sS_1 is a coset where each element is $\nu(u, r)\nu(u_i, e) = \nu(u', r)$, for some $u' \in \mathbb{Z}_p$. Hence $sS_1 = \{\nu(\mathbb{Z}_p, r)\}$ with $sS_1 \cap S_i = \emptyset$. But, since $r \in S^-$ there is at least one $u_0 \in \mathbb{Z}_p$ such that $\nu(u_0, r) = e$, in contradiction with $sS_1 \cap S_i = \emptyset$.

■

Theorem 4: Consider the encoder $M = (\mathbb{Z}_p, S, Y, \omega, \nu)$, then each S_i of (1) must be a p-group.

Proof: By induction over i, for $i = 1$ we have $[S_1 : S_0] = p$ or $[S_1 : S_0] = 1$. Now suppose there is a natural number $k > 1$ such that $[S_i : S_{i-1}] = p$, for all $i \leq k$. We have that the subgroup S_k has p^k elements and each of its elements has order p^i, $i \leq k$. If $p > [S_{k+1} : S_k] > 1$ then $[S_{k+1} : S_k] = m = q_1^{r_1} q_2^{r_2} \dots q_t^{r_t}$, where each q_i is a prime and $q_i < p$. There must be an element $s \in (S_{k+1} - S_k)$ such that $s^{q_1} = e$.

Let $u \in \mathbb{Z}_p$ and $r \in S_k$ be such that $\nu(u, r) = s$, then $\nu(u_1, r^{q_1}) = e$. Hence $r^{q_1} \in S^- \cap S_k$.

If $r \neq e$ then $r^{q_1} \neq e$, because $q_1 < p$. By Lemma 3, $S^- \subset S_k$ and $\nu(u, r) = s \in S_k$, a contradiction.

If $r = e$ then $\nu(u, r) = s \in S_1 \subset S_k$, a contradiction. ■

Corollary 1: If $[S_k : S_{k-1}] = p$ then $\nu(u, s) \in S_k - S_{k-1}$ for all $s \neq e$

Corollary 2: If the code is controllable then $|S_i| = p^i$

Lemma 4: If $S^- \cap S_i \neq \{e\}$ for some $S_i \neq S$, then the code produced by the encoder $M = (\mathbb{Z}_p, S, Y, \omega, \nu)$ is non-controllable.

Proof: In accordance with item 1 of the above Lemma 3, S^- is a subset of S_i. By Theorem 4, S_i is a p-group which have S_1 and S^- as subgroups of order p. Since any p-group has only one subgroup with order p, then $S_1 = S^-$. Again, by the item 2 of the above Lemma 3 $\nu(\mathbb{Z}_p, S_1) \subset S_1$. Therefore, considering any $s \in S$ such that $s \notin S_1$ we have that there is not any finite path connecting the neutral element $e \in S_1 \subset S$ and s. By the Theorem 2 the code is non-controllable ■

Theorem 5: Consider the encoder $M = (\mathbb{Z}_p, S, Y, \omega, \nu)$ and

the subgroups S_i of the equation (1). If the code is controllable then S_2 cyclic implies that S_3 is cyclic

Proof: We have that $S_1 = \nu(\mathbb{Z}_p \boxtimes \{e\})$ is cyclic. If $S_2 = \nu(\mathbb{Z}_p \boxtimes S_1)$ is cyclic then $S_2 \cong \mathbb{Z}_p$ or $S_2 \cong \mathbb{Z}_{p^2}$. But if $S_2 \cong \mathbb{Z}_p$ then all $S_i \cong \mathbb{Z}_p$, Theorem 3. and the encoder $M = (U, S, Y, \omega, \nu)$ would be useless. Thus S_2 must be isomorphic to $\mathbb{Z}_{p^2}$. By contradiction, suppose $S_3 = \nu(\mathbb{Z}_p \boxtimes S_2)$ is not cyclic, then by Lemma 2, $S_3 \cong \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$. For the sake of clarity let S_3 be such that $S_3 = \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$. Then each state of S_3 is a pair (i, j) with $i \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ and $j \in \mathbb{Z}_{p^2} = \{0, 1, \ldots, p, \ldots, 2p, \ldots, p^2 - 1\}$.

Any subgroup of order p^2 of $\mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$ is cyclic and generated by a pair (i, j) where j must have order p^2. Hence $S_2 =< (i, j) >$ has the following elements;

$$\begin{array}{ccccc} (i,j) & (2i,2j) & (3i,3j) & \ldots & (0,pj) \\ (i,(p+1)j) & (2i,(p+2)j) & (3i,(p+3)j) & \ldots & (0,2pj) \\ (i,(2p+1)j) & (2i,(2p+2)j) & (3i,(2p+3)j) & \ldots & (0,3pj) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ (i,((p-1)p+1)j) & (2i,((p-1)p+2)j) & (3i,((p-1)p+3)j) & \ldots & (0,0) \end{array}$$

Consider the pair $(0, p) \in S_3$. The order of $(0, p)$ is p, therefore S_1 is generated by $(0, p)$. Now, chose any $(i, j) \in S_2 - S_1$ and let (x, y) be defined by $(x, y) = \nu(0, (i, j)) \in S_3$. On one side we have that $(x, y)^p = (0, pj) \in S_1$. On the other side $(x, y)^p = (\nu(0, (i, j)))^p = \nu((0, (i, j))^p) = \nu(u, (0, jp))$, for some $u \in U$. But by the Theorem 4, $\nu(u, (0, jp))$ must be in $S_2 - S_1$, a contradiction.

■

Example 3: Consider the prime $p = 3$, and the subgroups S_0, $S_1 \cong \mathbb{Z}_3$. Suppose $S_2 \cong \mathbb{Z}_9$, Figure 2.
We have that for $S_3 = \mathbb{Z}_3 \oplus \mathbb{Z}_9$ the subgroups of order 9 are $\{01, 02, 03, 04, 05, 06, 07, 08, 00\}$, $\{11, 22, 03, 14, 25, 06, 17, 28, 00\}$ and $\{12, 24, 06, 18, 21, 03, 15, 27, 00\}$, and the subgroups of order 3 are $\{03, 06, 00\}$, $\{10, 20, 00\}$, $\{13, 26, 00\}$, $\{23, 16, 00\}$. Since $S_1 \subset S_2$, we must choice $S_1 = \{03, 06, 00\}$. In this example we choose $S_2 = \{01, 02, 03, 04, 05, 06, 07, 08, 00\}$. Suppose $\nu(0, 01) = 11$ then $\nu(u, 03) = 03 \in S_2$. In general $\nu(0, 01) = ij$ implies $\nu(u, 03) = 0r$ where $r \in \{0, 3, 6\}$. Therefore S_3 must be cyclic.

V. Conclusions

We had shown that for an encoder $(\mathbb{Z}_p, S, Y, \omega, \nu)$ the intersection $S^- \cap S_i$, for $i \geq 1$, must have only one element $\{e\}$. In other case the code will be non controllable. Also we had shown that if S_2 is cyclic then S_3 must be cyclic. In this direction the next work can be to show a general statement about the cyclic condition of S_i and S_{i+1} for any $i \geq 1$.

References

[1] H. A. Loeliger and T. Mittelholzer, "Convolutional codes over groups," *IEEE Trans. Inform. Theory*, vol. IT 42, pp. 1659–1687, 1996.

[2] H. A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol. IT 37, pp. 1675–1682, November 1991.

[3] D. G. 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), pp. 1491–1513, 1993.

[4] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*. New York: Cambridge University Press, 1995.

[5] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, 1st ed. New Jersey: Wiley-InterScience, 2005.

[6] C. Schlegel and L. Perez, *Trellis and Turbo Coding*. Piscataway NJ: Wiley Interscience, 2004.

[7] D. J. C. Mackay, *Information Theory, Inference, and Learning Algorithms*. United Kingdom: Cambridge University Press, 2005.

[8] S. Haykin, *Comunication Systems*, 4th ed. Wiley and Sons, 2001.

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

[10] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 9th ed. Amsterdam: North-Holland, 1996.

[11] J. P. Arpasi, "Control in trellis codes produced by finite state machines with information group $\mathbb{Z}_p$," in *Proceedings of the 2006 International Telecommunications Symposium*. Manaus, AM: IEEE, September 2010.

[12] F. Fagnani and S. Zampieri, "Minimal syndrome formers for group codes," *IEEE Trans. Inform. Theory*, vol. IT 45, no. 01, pp. 3–31, 1999.

[13] J. W. Polderman and J. C. Willems, *Introduction to Mathematical Systems Theory: A Behavioral Approach*. Springer-Verlag, 1998.

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

[15] M. Hall, *The Theory of Groups*. New York: Mac Millan, 1959.

[16] M. A. Arbib, *Brains, Machines and Mathematics*, 2nd ed. New York: Springer Verlag, 1986.

[17] J. P. Arpasi, "The semidirect product $\mathbb{Z}_2$ by a finite group s is bad for non abelian codes," in *Anais do XX Simpósio Brasileiro de Telecomunicações*. Rio de Janeiro,RJ: SBrT, Outubro 2003.

[18] R. Diestel, *Graph Theory*, 3rd ed. New York: Springer Verlag, 2005.

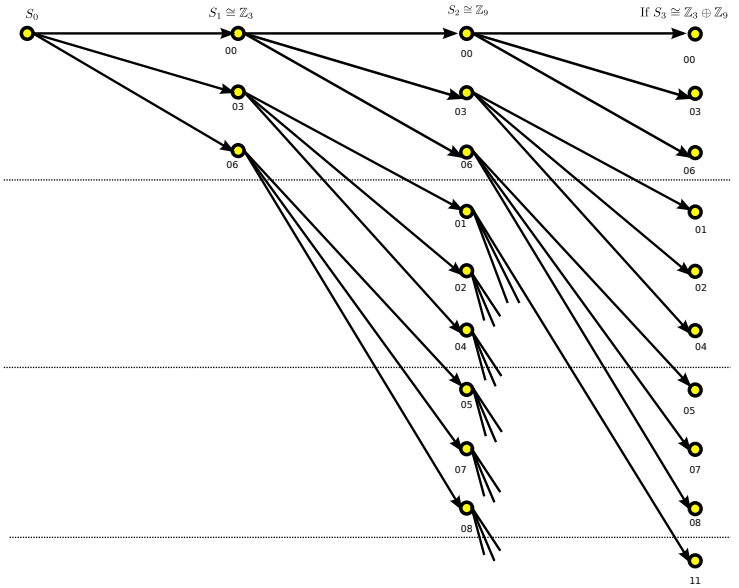

Fig. 2. Trellis of $\mathbb{Z}_3 \boxtimes S$