Control in Trellis Codes produced by Finite State Machines with Information Group $\mathbb{Z}_p$

Jorge Pedraza Arpasi

***Abstract*— A trellis code is the image of a signal mapper from a time invariant group code produced by a Finite State Machine, FSM. Group codes can be described as dynamical systems and good group codes must be necessarily well behaved dynamical systems. For instance good group codes must be controllable and observable, among other properties of well-behaved systems. In this paper we work with trellis codes produced by Finite State Machines over non-abelian groups. The necessity of non-abelian groups on FSM is because there no exist any regular signal mapper between the outputs of a classical binary convolutional encoder and a $M-PSK$ signal set. Also, it has been shown that the capacity of an AWGN channel using abelian group codes is upper bounded by the capacity of the same channel using PSK modulation eventually with different energies per symbol. We will show that when the trellis section group is non-abelian and the input group of the FSM is a cyclic group $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$, p prime, then the trellis code produced by the FSM is non-controllable.**

***Index Terms*— Trellis codes, dynamical systems, controllability, p-groups.**

I. Introduction

Trellis Coded Modulation (TCM) is a method, introduced by Ungerboeck in [1], of reduction of power requirements of a communication system without increase in the requirements on bandwidth. The trellis encoder consists of two parts; the first is called Finite State Machine (FSM) that is also called Wide-Sense Homomorphic Encoder [2], [3], [4]; the second part is called *signal mapper*, [2], and essentially it is a memoryless application between the trellis section of the FSM and one constellation of signals. The FSM is a quintuple (U, S, Y, ν, ω) where U, S, and Y are finite groups, and ν and ω are group homomorphisms. Moreover, U is the group of inputs or group of uncoded information, S is the groups of the states, and Y is the group of outputs or group of encoded information; $\nu : U \boxtimes S \to S$ is any surjective homomorphism called the next state mapping, and $\omega : U \boxtimes S \to Y$ is a homomorphism such that the trellis mapping $\Psi : U \boxtimes S \to S \times Y \times S$ defined by

$$\Psi(u, s) = (s, \omega(u, s), \nu(u, s)) \quad (1)$$

is injective [4], [5], [6]. The group $U \boxtimes S$ is called the extension of U by S [7], [8]. The semi-direct product of groups and direct product of groups are examples of extension of groups. The systematic and binary convolutional encoder of the Figure 1 is an example of FSM.

We have that it has $\mathbb{Z}_2^2 = \{00, 10, 01, 11\}$ as its uncoded(input) group U, $\mathbb{Z}_2^3 =$

Centro de Tecnologia da Universidade Federal do Pampa, Alegrete CT-UNIPAMPA, RS. Email: jorgearpasi@unipampa.edu.br

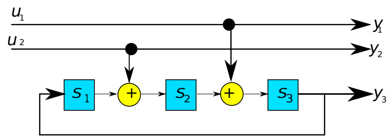

Fig. 1. Binary encoder $(\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^3, \nu, \omega)$

$\{000, 001, 010, 011, 100, 101, 110, 111\}$ as its sates group S, and again $\mathbb{Z}_2^3$ as its encoded(output) group Y. The next state homomorphism of this FSM is $\nu(u_1, u_2, s_1, s_2, s_3) = (s_3, u_2 + s_1, u_1 + s_2)$ and the encoder homomorphism is $\omega(u_1, u_2, s_1, s_2, s_3) = (u_1, u_2, s_3)$. For example, if the initial state is 000 for the sequence of inputs 00,10,01,11 the encoder responses with the states sequence 000, 001, 010, 011 and the output encoded sequence 000, 100, 010, 110. The 32 triplets $\{\Psi(u, s) = (s, \omega(u, s), \nu(u, s))\}_{u \in \mathbb{Z}_2^3, s \in \mathbb{Z}_2^3}$, form a subgroup of the direct product of groups $S \times Y \times S = \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \times \mathbb{Z}_2^3$ and are called transitions. The whole group of 32 transitions $\{\Psi(u, s)\}$ is called the trellis section group of the FSM.

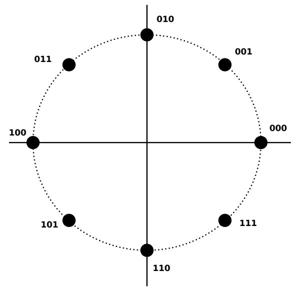

Fig. 2. 8-PSK Constelation

The signal mapping between the outputs of the FSM and a signal set is an issue that has not solved completely. But definitions and constraints working about signal mappers already were given. For example in [6] the matching map was defined as the following;

Definition 1: A group G with identity e is said to be matched to a signal set Sg if there is a signal mapping $\mu : G \to S$ such that $d(\mu(g_1), \mu(g_2)) = d(\mu(g_1^{-1} g_2), \mu(e))$, for any $g_1, g_2 \in G$. □

If we consider G as the group of outputs of the FSM of the Figure 1 and the signal set Sg as the $8-PSK$ constellation of the Figure 2, we will have that there is not any matching map μ satisfying the Definition 1. Thus more general definitions about signal mapper must be given. That is the case of the next Definition;

Definition 2: A matching map τ between a group G and a signal set Sg is said to be **quasi-regular** if the set of squared distances $D_{g_0} = \{d^2(\tau(g_0), \tau(g_0 g))\}_{g\in G}$ is independent of $g \in G$, for each $g_0 \in G$. □

Normally the set D_{g_0} has one or very few elements. The matching maps satisfying the Definition 1 are called *regular* signal mappers and a quasi-regular signal mapper of the Definition 2 is a generalization of regular signal mappers, [2]. The regular matchings have obvious advantages over the quasi-regular matchings such as the resulting codes always will be geometrically uniform. For the constellation $8-PSK$ of Figure 2 there exist the non-abelian group D_8=symmetries of the square, such that D_8 and $8-PSK$ are regularly matched accordingly the Definition 1. On the other hand, in [6] it has been shown that for a given AWGN channel using group codes over abelian groups, its capacity is upper bounded by some AWGN channel capacity using PSK constellations Thus, non-abelian and well-behaved group codes could surmount this PSK limit. In this work we will focused on the non-abelian case.

II. Finite State Machines and Time invariant group codes

A. Group extension

Definition 3: 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 $\frac{G}{N} \cong S$, [7]. □

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 [7], [8], specially in [8] 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,

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

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

$$\xi(s_1, s_2) = l(\psi(s_1, s_2))l(\psi(s_1))l(\psi(s_2)), \tag{3}$$

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

$$(u_1, s_1) * (u_2, s_2) = (u_1.\phi(s_1)(u_2).\xi(s_1, s_2)\,,\, s_1 s_2) \tag{4}$$

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 $(u', s_1 s_2 \ldots s_n)$, is the resulting pair of the multiple product $(u_1, s_1)\cdot(u_2, s_2)\cdot(u_3, s_3)\ldots(u_n, s_n)$, where u' is some element of U. Analogously, $(u, s)^n = (u', s^n)$ for some $u' \in U$.

B. Finite State machines FSM

Definition 4: A Finite State Machine (FSM) is a machine $M = (U, Y, S, \omega, \nu)$, where the input alphabet U, the output alphabet Y, and the state set S are groups, and the next state mapping $\nu : U \boxtimes S \to S$ is a surjective group homomorphism and the encoder-output $\omega : U \boxtimes S \to Y$ is a mapping such that Ψ defined by (1) is an injective homomorphism. □

Suppose that a given FSM (U, Y, S, ν, ω) has its initial state $s_0 \in S$, the neutral element of the group S, then given a finite sequence $\{u_i\}_{i=1}^n$ of uncoded elements of U, the FSM will respond with two sequences of states $\{s_i\}_{i=1}^n$ and of outputs $\{y_i\}_{i=1}^n$ in the following way;

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

If we agree that the state s_0 is the present state, the state s_1 is the next state, the state at time 1, next state from s_1 is s_2, the state at time 2, and generally s_n is the next state from s_{n-1}. Then $\{s_i\}_{i=1}^n$ is a sequence of future states. On the other hand, since the mapping ν of the FSM is surjective, then there exists at least a pair (u_0, s_{-1}) such that $s_0 = \nu(u_0, s_{-1})$. The state s_{-1} is one past state from s_0, and we can agree that the negative index describes well such idea about past. Then, for the FSM, there exist 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;

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

Thus for any FSM and for any bi-infinite sequence $\{u_k\}_{k\in\mathbb{Z}}$, where $\mathbb{Z}$ is the integer set, there are two bi-infinite sequences; $\{s_k\}_{k\in\mathbb{Z}}$ of states and $\{y_k\}_{k\in\mathbb{Z}}$ of outputs; that are responses of the FSM to the input sequence $\{u_k\}_{k\in\mathbb{Z}}$. Each sequence of outputs of the FSM $\mathbf{y} = \{y_k\}_{k\in\mathbb{Z}}$ is called *codeword* and the family of codewords $\{\mathbf{y}\ ;\ \mathbf{y} \text{ is a codeword}\}$ is the time invariant group code $\mathcal{C}$ generated by the FSM, [3], [6], [5], [9]. Considering a group code $\mathcal{C}$ as a dynamical system, a FSM is one realization of $\mathcal{C}$, [5], [6], [10].

C. Control of time invariant group codes

Given two integers i, j, with $i \leq j$, we use the notations $[i,j]$, $[i,j)$, $(i,j]$, and (i,j) for integer intervals. For instance, $[i,j] = \{i, i+1, \ldots, j-1, j\}$, $[i,j) = \{i, i+1, \ldots, j-1\}$, and so on. This notation also works for non-finite and discrete sets such as $\{k \in \mathbb{Z} \; ; \; k \leq j\} = (-\infty, j]$. Then, a projection of a codeword $\{\mathbf{y}_k\}_{k\in\mathbb{Z}}$ over the set indices $[i,j]$ is denoted by $\{\mathbf{y}\}|_{[i,j]} = \{\mathbf{y}_i, \mathbf{y}_{i+1}, \ldots, \mathbf{y}_j\}$.

Given two codewords $\{\mathbf{y_1}_k\}_{k\in\mathbb{Z}}$, $\{\mathbf{y_2}_k\}_{k\in\mathbb{Z}} \in \mathcal{C}$, a *concatenation* of $\{\mathbf{y_1}_k\}_{k\in\mathbb{Z}}$ and $\{\mathbf{y_2}_k\}_{k\in\mathbb{Z}}$ in the instant j is a codeword $\{(\mathbf{y_1} \wedge_j \mathbf{y_2})_k\}_{k\in Z}$ defined as $(\mathbf{y_1} \wedge_j \mathbf{y_2})_k = \begin{cases} \mathbf{y_1}_k|_{(-\infty,j)}; & k < j \\ \mathbf{y_2}_k|_{[j,+\infty)}; & k \geq j. \end{cases}$.

If L is an integer greater than one, then a group code $\mathcal{C}$ is said L-controllable when for given words $\mathbf{y_1}$ and $\mathbf{y_2}$, there exists a third word $\mathbf{y_3}$ and one integer k such that the concatenation $\mathbf{y_1} \wedge_k \mathbf{y_3} \wedge_{k+L} \mathbf{y_2}$ is a word of the group code $\mathcal{C}$. [9], [3]. It is said that a natural number $l > 1$ is the index of controllability of a group code $\mathcal{C}$ when $l = min\{L \; ; \; \mathcal{C}$ is $L-$controllable $\}$. Any applicable group code in telecommunications needs to have an index of controllability.

Definition 5: A group code $\mathcal{C}$ is called controllable when there is an integer $l > 1$ such that l is the index of controllability of $\mathcal{C}$. □

Considering the mapping Ψ from (1) the group $Im(\Psi(U \boxtimes U))$ is called the trellis section group, and its elements, which are the triplets $(s, \omega(u,s), \nu(u,s))$, have at least three names: transitions, edges and branches. Since we are working with trellises as graphical representations of dynamical system we choose to call such triplets as transitions. Given an initial state s_0 a finite path of transitions of the trellis section is a sequence $B_0, B_1, \ldots B_{n-1}$ such that $B_i = (s_i, \omega(u_i, s_i), \nu(u_i, s_i))$ with $s_{i+1} = \nu(s_i)$, for some finite sequence of inputs $\{u_i\}_{i=0}^{n-1}$. The beginning of the path is the state s_0 and the end is the state $s_{\{n-1\}}$.

Definition 6: It is said that the states s and r are connected when there exists a finite path of transitions $B_0, B_1, \ldots, B_n$ such that s and r are the beginning and the end of the path. With this definition of state connectedness we can show the next Theorem.

Theorem 1: If there are two states s and r such that they are not connected then the time invariant group code produced by the FSM is **non-controllable**.

III. TRELLIS CODES

Let τ a quasi-regular signal mapper, originally τ was defined on the output group $Y = \{\omega(u,s)\}_{(u,s)\in U\boxtimes S}$ of a FSM. But recently τ is defined on the whole trellis section group $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$, [2]. Notice that if $\omega = id$, then $\Psi(u,s) = (s, (u,s), \nu(u,s))$ is injective. Thus defining τ on the whole trellis section group instead of the outputs group give us more possibilities for the construction of trellis codes.

Definition 7: Given a finite Euclidean signal set Sg and a finite group $G = U \boxtimes S$ such that;

- Sg is the image of a quasi-regular signal mapping $\tau : G \rightarrow Sg$
- $G = U \boxtimes S$ is isomorphic to the trellis group of a FSM,

we define the **trellis code** as the set $\tau(\mathbf{c})$, were $\mathbf{c}$ is a codeword of a FSM □

Clearly the graphical dynamics of the trellis of a trellis code is the same of the group code. Then a trellis code is controllable if only if the associated group code is controllable.

Now we will see some properties of the group $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$.

Definition 8: Two different transitions $(s_1, \omega(u_1,s_1), \nu(u_1,s_1))$ and $(s_2, \omega(u_2,s_2), \nu(u_2,s_2))$ are parallels if $s_1 = s_2$ and $\nu(u_1,s_1) = \nu(u_2,s_2)$ and $\omega(u_1,s_1) \neq \omega(u_2,s_2)$ □

Lemma 1: Consider a FSM (U, S, Y, ν, ω). Let B^+ and B^- be subsets of the trellis section group $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$ such that $B^+ = \{(e, \omega(u,e), \nu(u,e) \; ; \; u \in U\}$, the transitions outcoming from the neutral state $\{e\}$, and $B^- = \{(s, \omega(u,s), \nu(u,s) \; ; \; \nu(u,s) = e\}$, the transitions incoming into the neutral state $\{e\}$. Also, let H^+ and H^- be subsets of $U \boxtimes S$ such that $H^+ = U \boxtimes \{e\} = \{(u,e) \; ; \; u \in U\}$ and $H^- = Ker(\nu) = \{(u,s) \; ; \; \nu(u,s) = e\}$, then;

1) $H^+ \cong B^+$ and $H^- \cong B^-$,
2) Both H^+ and H^- are normal subgroups of $U \boxtimes S$,
3) If $H^+ \cap H^- \neq \{(e,e)\}$ then $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$ has parallel transitions,
4) If $U \boxtimes S$ is non-abelian and the states group S is abelian then $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$ has parallel transitions

Proof.-

1) We have $B^+ = \Psi(H^+)$ and $B^+ = \Psi(H^+)$, where Ψ is defined in (1).
2) Immediate.
3) There exists $(u,e) \in H^+ \cap H^-$, with $u \neq e$ such that $\nu(u,e) = e$. Since Ψ of (1) is injective, $\omega(u,e) \neq e$. Therefore, the transitions $(e, \omega(e,e), \nu(e,e))$ and $(e, \omega(u,e), \nu(u,e))$ are parallels.
4) The states group S being abelian implies that $\frac{G}{H^+} \cong \frac{G}{H^-}$ are abelian factor groups. Then the commutators subgroup $(U \boxtimes S)'$ is a subgroup of $H^+ \cap H^-$. But $U \boxtimes S$ is non-abelian, then $(U \boxtimes S)' \neq \{(e,e)\}$. Therefore from the above item (3), $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$ has parallel transitions.

□

Given a FSM (U, S, Y, ν, ω) consider the family of state subsets $\{S_i\}$, recursively defined by;

$$\begin{array}{lcl} S_0 & = & \{e\} \\ S_1 & = & \{\nu(u,s) \; ; \; u \in U, s \in S_0\} \\ S_2 & = & \{\nu(u,s) \; ; \; u \in U, s \in S_1\} \\ \vdots & \vdots & \vdots \\ S_i & = & \{\nu(u,s) \; ; \; u \in U, s \in S_{i-1}\}, i \geq 0 \\ \vdots & = & \vdots \end{array} \quad (5)$$

Theorem 2: Some properties of the family $\{S_i\}$;

1) Each S_i is a subgroup of S
2) S_{i-1} is normal in S_i , for all $i = 1, 2, \ldots$.

3) If $S_{i-1} = S_i$ then $S_i = S_{i+1}$.
4) If the group code is controllable then $S = S_k$ for some k.

Proof.-

1) 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, $s.r.s^{-1} = \nu(u_1, r_1.s_1.r_1^{-1}) \in S_i$, because $r_1.s_1.r_1^{-1} \in S_{i-1}$.
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) If not, there are $s \in S_k$ and $s' \in S$ such that $s' \neq \nu(u_n, \nu(u_{n-1}, \nu(u_{n-2}, \ldots, \nu(u_2, \nu(u_1, s)) \ldots)))$, for any sequence $\{u_i\}_{i=1}^{n}$ of inputs.

□

IV. TRELLIS CODE PRODUCED BY A FSM $(\mathbb{Z}_p, S, Y, \nu, \omega)$ WITH p PRIME

In spite its apparent simplicity, there is not a general classification for p-groups. Only the p-groups of order at most p^6 have been completely classified, for $p \geq 3$, [11]. And for $p = 2$, the complete classification has been done only for groups with order $\leq 2^8$, [12], [13]. This classification of 2-groups has been implemented in softwares like the GAP, [13], which includes in its library all the 2-groups of order 256. The cyclic groups $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, where the group operation is given by $i + j$ module p, are the most simple instances of p-groups. The results that we will show here, about group codes with information group $\mathbb{Z}_p$, are valid for any p-group, independently of the existence of its classification.

Definition 9: Given a group G the group of commutators of G is the subgroup $G' = \{aba^{-1}b^{-1}\,;\, a, b \in G\}$

Lemma 2: Let $\mathbb{Z}_p \boxtimes S$ be an extension which is a p-group. If $\mathbb{Z}_p \boxtimes S_0 \subset (\mathbb{Z}_p \boxtimes S)'$, then $\mathbb{Z}_p \boxtimes S_i \subset (\mathbb{Z}_p \boxtimes S)'$, and $S_i \subset S'$, for each $i \geq 1$.

Proof.- Since ν is a group homomorphism, the image $\nu(\mathbb{Z}_p \boxtimes S_0) = S_1$ is in the commutators subgroup S' of S. If $S_1 = S_0$ the Lemma holds trivially, (Figure 3 (a)). If $S_1 \neq S_0$, by the long commutators theorem from [14], there are $s \in (S_1 - S_0)$ and $a_1, a_2, \ldots, a_t \in S$ such that $s = a_1 a_2 \ldots a_t a_1^{-1} a_2^{-1} \ldots a_t^{-1}$. Now consider $u \in \mathbb{Z}_p$ and $\{u_1, u_2, \ldots, u_t\} \subset \mathbb{Z}_p$ such that $(u, s) = (u_1, a_1)(u_2, a_2) \ldots (u_t, a_t)(u_1, a_1)^{-1}(u_2, a_2)^{-1} \ldots (u_t, a_t)^{-1}$. We have $(u, s) \in (\mathbb{Z}_p \boxtimes S)'$ and $(u, s) \notin \mathbb{Z}_p \boxtimes S_0$. Therefore $\mathbb{Z}_p \boxtimes S_1 \subset (\mathbb{Z}_p \boxtimes S)'$ (Figure 3 (b)).
Again, since ν is a group homomorphism, $\nu(\mathbb{Z}_p \boxtimes S_1) = S_2$ is in the commutators subgroup S' of S. Then with very similar arguments we can proof that if $S_2 \neq S_1$, then $(\mathbb{Z}_p \boxtimes S_2) \subset (\mathbb{Z}_p \boxtimes S)'$ and $\nu(\mathbb{Z}_p \boxtimes S_2) = S_3 \subset S'$. Continuing in the same way we conclude that $(\mathbb{Z}_p \boxtimes S)'$ and $S_i \subset S'$, for any $i \geq 1$. □

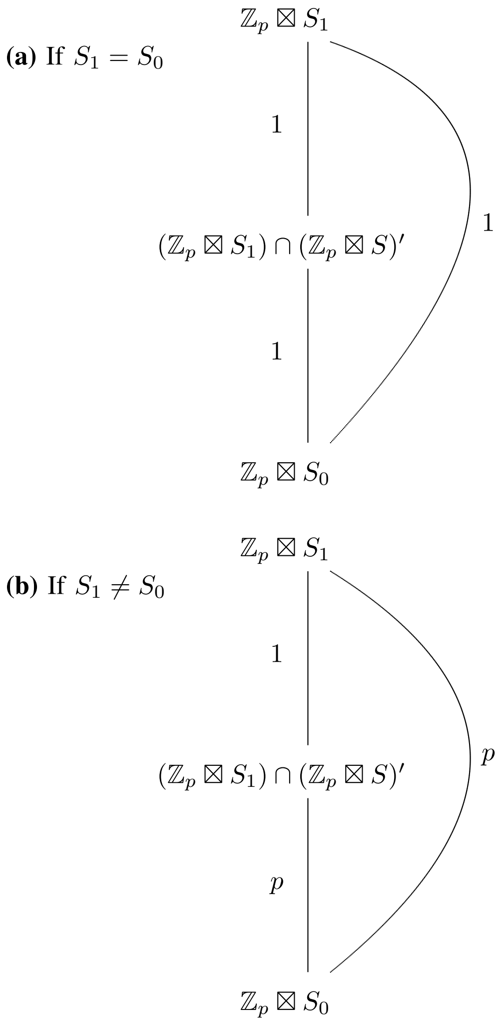

Fig. 3. The intersection $(\mathbb{Z}_p \boxtimes S_1) \cap (\mathbb{Z}_p \boxtimes S)'$ when $\mathbb{Z}_p \boxtimes S_0 \subset (\mathbb{Z}_p \boxtimes S)'$

Lemma 3: Let $\mathbb{Z}_p \boxtimes S$ be an extension which is a p-group. Consider the subgroups $\{S_i\}$ defined in equation (5). Then, for each i, either each S_i is abelian or $S_i \subset S'$.

Proof.- Since S_1 is cyclic and S_2 has almost order p^2, we have both S_1 and S_2 are abelian. Then, let $i \geq 2$ be such that $S_1, S_2, \ldots, S_i$ are all abelian with S_{i+1} non abelian. Then there are $s_1, s_2 \in S_{i+1}$ such that $s_1 s_2 \neq s_2 s_1$. Also there must be $u_1, u_2 \in \mathbb{Z}_p$ and $r_1, r_2 \in S_i$, with $r_1 r_2 = r_2 r_1$, such that $s_1 = \nu(u_1, r_1)$ and $s_2 = \nu(u_2, r_2)$. Then;
$s_1 s_2 \neq s_2 s_1$,
$\nu(u_1, r_1).\nu(u_2, r_2) \neq \nu(u_2, r_2).\nu(u_1, r_1)$,
$\nu((u_1, r_1).(u_2, r_2).(u_1, r_1)^{-1}.(u_2, r_2)^{-1}) \neq e$
$\nu(u', r_1 r_2 r_1^{-1} r_2^{-1}) \neq e$, for some $u' \in \mathbb{Z}_p$
$\nu(u', e) \neq e$
From this, $u' \neq e$ and $(u', e) \in (\mathbb{Z}_p \boxtimes S)' \cap (\mathbb{Z}_p \boxtimes S_0)$. Since the order of $\mathbb{Z}_p \boxtimes S_0$ is p, we have that $\mathbb{Z}_p \boxtimes S_0 \subset (\mathbb{Z}_p \boxtimes S)'$. By the Lemma 2, $(\mathbb{Z}_p \boxtimes S_i) \subset (\mathbb{Z}_p \boxtimes S)'$ and $S_i \subset S'$, for each i. Therefore either S_i is abelian or $S_i \subset S'$. □

Suppose now that we have not the information about the order of $\mathbb{Z}_p \boxtimes S$, that is, we can not use the hypothesis $\mathbb{Z}_p \boxtimes S$ to be a p-group. In this case we need to consider S as a generic and finite group. By looking back, again, the family $\{S_i\}$ defined by equation (5) we will show that when $U = \mathbb{Z}_p$, each S_i must be a p-group. In that direction we begin by showing a result about one important normal subgroup of the states group is the second projection of the kernel of ν

$$S_d = \{s \in S \; ; \; \nu(u, s) = e \,\text{for some}\, u \in \mathbb{Z}_p\} \qquad (6)$$

Notice that this is a normal subgroup of S isomorphic to $\mathbb{Z}_p$ and;

Lemma 4: Consider the FSM $(\mathbb{Z}_p, S, Y, \nu, \omega)$ and the subgroup S_d defined in equation (6), then;

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

Proof.-

1) Since $p \in S_d \cap S_i$, then $\{s, s^2, \ldots, s^{p-1}, s^p = e\} \subset S_d \cap S_i$.
2) Given $r \neq e$ such that $r \in S_i \cap S_d$ suppose there is some $u \in \mathbb{Z}_p$ such that $\nu(u, r) = s \notin S_i$. For the subgroup $S_1 = \{s_0, s_1 = \nu(u_1, e), s_2 = \nu(u_2, e), \ldots, s_{p-1} = \nu(u_{p-1}, e)\}$, 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 $r \in S_d$ 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 3: Consider the FSM $(\mathbb{Z}_p, S, Y, \nu, \omega)$, where p is prime. Then each S_i of (5) 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 that 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 have order p^i, $i \leq k$. If $p > [S_{k+1} : S_k] > 1$ then $[S_{k+1} : S_k] = m = q_1^{r_1} q_2^{r_2} \ldots q_t^{r_t}$, where each q_i is a prime and $q_i < p$. Hence, 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 $\nu(u_1, r^{q_1}) = e$. Thus $r^{q_1} \in S_d \cap S_k$.

If $r \neq e$ then $r^{q_1} \neq e$, because $q_1 < p$. By Lemma 4, $S_d \subset S_k$ and $\nu(u, r) = s \in S_k$, contradiction.

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

Theorem 4: Consider the FSM $(\mathbb{Z}_p, S, Y, \nu, \omega)$, where $\mathbb{Z}_p \boxtimes S$ is non-abelian and p is a positive prime, then

1) If S is abelian then the code have parallel transitions,
2) If S is non-abelian then the code is non controllable

Proof.-

1) By the Lemma 1
2) If S is not a p-group then by Theorem 3 the resulting code is non-controllable. If S is a p-group, then $\mathbb{Z}_p \boxtimes S$ is also a p-group, then by Lemma 3 S is abelian, contradiction.

V. Examples and Conclusions

Controllable trellis section group $G = \mathbb{Z}_p \boxtimes S$ with $|G| \leq 32$ must be such that $p \in \{2, 3\}$. On the other hand, by the Theorem 3, $|S| = p^n$, for some n. Hence $|G| \in \{2^2, 2^3, 2^4, 2^5, 3^2, 3^3\}$. Also, a controllable trellis section $G = \mathbb{Z}_p \boxtimes S$ must have two normal subgroups $N_1 \cong U$ and $N_2 \cong U$ such that $\frac{G}{N_1} \cong \frac{G}{N_2} \cong S$ and $N_1 \cap N_2 = \{0\}$. That is because H^+, H^-, from Lemma 1, must have only $\{(0,0)\}$ in its intersection $H^+ \cap H^-$. Thus, for $|\mathbb{Z}_2 \boxtimes S| = 2^3$ we have 03 abelian groups and 02 non-abelian groups; D_8=symmetries of square and Q_8=quaternions. Both D_8 and Q_8 have only one normal subgroup of order 2. For $|\mathbb{Z}_2 \boxtimes S| = 2^4$ we have 06 abelian groups and 09 non-abelian groups. Each one of these last do not have two different normal subgroups satisfying Lemma 1.

In this way combining the Lemma 1 and Theorem 3 we can verify the statement of our main result Theorem 4 for any anon-abelian and finite group $G = \mathbb{Z}_p \boxtimes S$.

In [15] was proposed a non-abelian controllable trellis group with order 32, but the decomposition $G = U \boxtimes S$ is such that $U = \mathbb{Z}_2^2$ and $S = D_8$. With the help of software GAP [13] we found that there are more two different and controllable non-abelian groups with order 32 with $U = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ and $S = Q_8$, [16]. That lead us to focus our next research on decompositions $U \boxtimes S = \mathbb{Z}_p^n \boxtimes S$ and $\mathbb{Z}_{p^n} \boxtimes S$.

References

[1] G. Ungerboeck, "Channel coding with multilevel-phase signals," *IEEE Transactions on Information Theory*, vol. 28, pp. 55–67, 1982.

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

[3] H. A. Loeliger and T. Mittelholzer, "Convolutional codes over groups," *IEEE Transactions on Information Theory*, vol. 42, pp. 1659–1687, 1996.

[4] 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.

[5] G. Forney and M. 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.

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

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

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

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

[10] F. Fagnani and S. Zampieri, "Minimal syndrome formers for group codes," *IEEE Transactions on Information Theory*, vol. 45, no. 01, pp. 3–31, 1999.

[11] R. James, "The groups of order p^6 (p an odd order prime)," *Math. Comput.*, vol. 34, pp. 613–637, 1980.

[12] E. A. O'Brien, "The groups of order 256," *Journal of Algebra*, vol. 143, pp. 219–235, 1991.

[13] *GAP – Groups, Algorithms, and Programming, Version 4.4*, The GAP Group, 2005, (http://www.gap-system.org).

[14] Y. P., "On k-conjugacy in a group," *Proc. Edimburg Math. Soc.*, vol. 2, pp. 14:1–4, 1964/65.

[15] L. F. Wei, "Rotationally invariant convolutional channel coding with expanded signal space - part ii: nonlinear codes," *IEEE Journal on Selected Areas in Communications*, vol. SAC-2, no. 5, pp. 672–686, 1984.

[16] J. P. Arpasi and E. D. Carvalho, "Finite extensions of binary groups are bad for non-abelian group codes," *Advances and Applications in Discrete Mathematics*, vol. 2, no. 2, pp. 117–132, 2008.