The information group $\mathbb{Z}_p$ is bad for non abelian group codes

Jorge Pedraza Arpasi

Abstract— **We study non abelian time invariant group codes generated the extension of the additive group $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ by a finite group S, where p is a positive prime. When S is abelian the code has free distance limitations, and when S is non abelian we show that the code is non controllable. Therefore, the extension $\mathbb{Z}_p$ by S is bad for non abelian group codes.**

Keywords— **Extension of Groups, Homomorphic encoder, Group Codes, Controllability, Convolutional codes over Groups.**

I. Introduction

The construction of group codes over non abelian groups is interesting because in [1] it has been shown that the capacity of signal sets (with AWGN) matched to abelian groups are upper bounded by the capacity of a M-PSK signal set. Thus, non abelian and well behaved group codes could overcome such PSK limit. In such a direction in [2] is presented a multilevel method based on the semidirect product of two codes. The method which we are proposing differs from the just cited one in the fact that ours is indirect. We generalize the method given in [3] where was shown the badness of $\mathbb{Z}_2$ as information group. We will give criteria to find out non controllable group codes, then apply this to the family of non abelian extensions $\mathbb{Z}_p$ by S, where S is some finite group.

We will work with convolutional codes over groups defined in [4] which are observable, controllable, and time invariant group codes. These codes will be generated by the *wide-sense homomorphic encoder* [4]. This encoder is an automaton based device which, essentially, has two homomorphic mappings: the next state mapping and the output mapping both defined on an extension of the input(information) group U by the group of states S. When S is finite, the codes produced by this encoder are observable. Then we just need to be concerned about the controllability. For that the next state homomorphism has the key role. When the extension U by S is abelian of the type $\mathbb{Z}_2^n \times \mathbb{Z}_2^m$, as the standard binary convolutional codes are, there are a lot of ways to map the next state homomorphism, in such a way the resulting code is controllable. The reason for that easyness is the nature of the group elements, each one, but the identity, has order two. This fact explains why there are not considerations on control while the standard convolutional encoders are implemented. But in the case when U by S is non abelian, the next state homomorphism is mostly non controllable. That is the basis of the method presented in this work. We will give some properties for the controllable next state homomorphism, then we show that the majority of non abelian groups, when split as extensions, can not give any controllable next state homomorphism. We can refine this search taking only the codes without parallel transitions.

The author is with the Departamento de Matemática, Universidade Estadual do Rio Grande do Sul - UERGS, Rio Grande do Sul, Brazil. Email: jorge-arpasi@uergs.edu.br

In this article we will denote by e the *neutral* or *identity* element of an abstract group G, but in the case of the groups $\mathbb{Z}_p$ and D_8 where the neutral elements are denoted by 0 and 1 respectively. The notation $N \triangleleft G$ means N is a normal subgroup of G, while $H \cong K$ is the standard notation for an isomorphism between H and K. The notation $|G|$ is the order or cardinality of G. Finally $U \rtimes S$ and $U \boxtimes S$ are the semidirect product and the extension of U by G respectively. This paper is structured as follows.

In the section II we give a practical method to construct one explicit extension which we call a decomposition of a group. This means that given a group G which is the extension of U by S, by using this method, any g of G can be isomorphically decomposed as a unique ordered pair (u, s) of $U \times S$.

In the section III we follow [4], [1], and [5] to define and review trellis group codes generated by a wide-sense homomorphic encoders, and we find one criterion for controllability of these kind of codes. Such criterion is based on the existence of a especial normal series of subgroups of the states group S.

In the section IV we show some results about the group codes with non abelian trellis section isomorphic to the extension $\mathbb{Z}_p$ by S. We will show that when S is abelian then the code will have free distance limitations because it will have parallel transitions. This fact was noticed by Forney in [6] and also pointed out in [2]. Our main contribution is for the case when S is non abelian. In this case we show that a code with trellis section isomorphic to the extension $\mathbb{Z}_p$ by S is non controllable and therefore it can not be a convolutional code.

II. Extension of Groups

In this section we review some concepts and results about extension of groups. The proof of one of such extension theorems yields a useful method to construct an explicit extension or decomposition of a group. This construction will be used in order to decide if there exist controllable group codes with a trellis section isomorphic to a given group G. More precisely we will show that there are not controllable group codes with trellis section isomorphic to a non abelian extension of $\mathbb{Z}_p$ by S, with S non abelian and finite.

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

Theorem 1: Given the groups U and S; if there are mappings $\phi : S \to Aut(U)$ and $\varsigma : S \times S \to U$ such that, for all $s_1, s_2, s_3 \in S$,

$$\phi(s_1)(\varsigma(s_2, s_3)).\varsigma(s_1, s_2s_3) = \varsigma(s_1, s_2).\varsigma(s_1s_2, s_3), \quad (1)$$

and, for all $u \in U$ and for all $s_1, s_2 \in S$,

$$\phi(s_1)(\phi(s_2)(u)) = \varsigma(s_1, s_2).\phi(s_1s_2)(u).(\varsigma(s_1, s_2))^{-1}; \quad (2)$$

then $U \times S$ with the following operation

$$(u_1, s_2).(u_2, s_2) = (u_1.\phi(s_1)(u_2).\varsigma(s_1, s_2)\ ,\ s_1s_2) \quad (3)$$

is a group extension of U by S.

Proof: See [7], [8]. □

Theorem 2: Given a group G with a normal subgroup $N \triangleleft G$, let U, S be groups such that $U \cong N$ and $S \cong \frac{G}{N}$. Then:

1. There exist mappings on U and S satisfying (1) and (2),
2. $U \times S$, with the group operation (3) is isomorphic to G.

Proof:

1. Let

$$\upsilon : N \to U \quad (4)$$

and

$$\psi : S \to \frac{G}{N} \quad (5)$$

be the isomorphisms between N and U, and between S and $\frac{G}{N}$, respectively. For any $u \in U$ and $s \in S$ consider $\psi(s) \in \frac{G}{N}$ and $\upsilon^{-1}(u) \in N$. Also consider one lifting

$$l : \frac{G}{N} \to G \quad (6)$$

such that $l(N) = e$. Since N is normal, $l(\psi(s)).\upsilon^{-1}(u).(l(\psi(s)))^{-1} \in N$, thus we can define the mapping $\phi : S \to Aut(U)$ as being

$$\phi(s)(u) = \upsilon[l(\psi(s)).\upsilon^{-1}(u).(l(\psi(s)))^{-1}]. \quad (7)$$

On the other hand, consider $s, t \in S$ then $l(\psi(s)).l(\psi(t))$ and $l(\psi(st))$ belong to the coset $N * \psi(st)$. Hence $l(\psi(s)).l(\psi(t)).(l(\psi(st)))^{-1} \in N$. Thus we can define the mapping $\varsigma : S \times S \to U$ as being

$$\varsigma(s, t) = \upsilon[l(\psi(s)).l(\psi(t)).(l(\psi(st)))^{-1}]. \quad (8)$$

Now, we verify that these mappings (7) and (8) satisfy the above conditions (1) and (2);

$\phi(s_1)(\varsigma(s_2, s_3)).\varsigma(s_1, s_2s_3)$
$= \upsilon[l(\psi(s_1)).\upsilon^{-1}(\varsigma(s_2, s_3)).l(\psi(s_2s_3)).(l(\psi(s_1s_2s_3)))^{-1}]$
$= \upsilon[l(\psi(s_1)).l(\psi(s_2)).l(\psi(s_3)).(l(\psi(s_1s_2s_3)))^{-1}]$
$= \upsilon[l(\psi(s_1)).l(\psi(s_2)).(l(\psi(s_1s_2)))^{-1}].$
$\upsilon[(l(\psi(s_1s_2))).l(\psi(s_3)).(l(\psi(s_1s_2s_3)))^{-1}]$
$=\varsigma(s_1, s_2).\varsigma(s_1s_2, s_3).$

On the other hand $\phi(s_1)(\phi(s_2)(u))=$
$= \phi(s_1)\{\upsilon[l(\psi(s_2)).\upsilon^{-1}(u).(l(\psi(s_2)))^{-1}]\}$
$= \upsilon[l(\psi(s_1)).l(\psi(s_2)).\upsilon^{-1}(u).(l(\psi(s_2)))^{-1}.(l(\psi(s_1)))^{-1}]$
$= \upsilon[l(\psi(s_1)).l(\psi(s_2)).(l(\psi(s_1s_2)))^{-1}].$
$\upsilon[(l(\psi(s_1s_2))).\upsilon^{-1}(u).(l(\psi(s_1s_2)))^{-1}].$
$\upsilon[l(\psi(s_1s_2)).(l(\psi(s_2)))^{-1}.(l(\psi(s_1)))^{-1}]$
$= \varsigma(s_1, s_2).\phi(s_1s_2)(u).(\varsigma(s_1, s_2))^{-1}$

Therefore we have that $U \times S$, with the group operation, (3) is a group.

2. We construct the isomorphism between G and $U \times S$. For each $g \in G$ there is an unique $n \in N$ such that $g = n.l(Ng)$, then we define $\theta : G \to U \times S$ as being

$$\theta(g) = \theta(n.l(Ng)) = (\upsilon(n)\ ,\ \psi^{-1}(Ng)), \quad (9)$$

1	2	3	4	5	6	7	8
2	3	4	1	8	7	5	6
3	4	1	2	6	5	8	7
4	1	2	3	7	8	6	5
5	7	6	8	1	3	2	4
6	8	5	7	3	1	4	2
7	6	8	5	4	2	1	3
8	5	7	6	2	4	3	1

TABLE I

THE DIHEDRAL GROUP D_8

Only remains to prove that θ is a homomorphism. Let $g_1 = n_1.l(Ng_1)$ and $g_2 = n_2.l(Ng_2)$ be elements from G and suposse $\theta(g_1) = (\upsilon(n_1), \psi^{-1}(Ng_1)) = (u_1, s_1)$ and $\theta(g_2) = (\upsilon(n_2), \psi^{-1}(Ng_2)) = (u_2, s_2)$. Then $g_1g_2 = n_1.l(Ng_1).n_2.l(Ng_2) = n_1.l(Ng_1).n_2.(l(Ng_1))^{-1}.l(Ng_1).l(Ng_2).(l(Ng_1g_2))^{-1}.l(Ng_1g_2)$. Since N is normal, $n_3 = l(Ng_1).n_2.(l(Ng_1))^{-1}$ and $n_4 = l(Ng_1).l(Ng_2).(l(Ng_1g_2))^{-1}$ are in N. Hence, $\upsilon(n_1.n_2.n_3) = \upsilon(n_1).\upsilon(n_1).\upsilon(n_1)$ $=u_1.\phi(s_1)(u_2).\varsigma(s_1, s_2)$.

Thus, $\theta(g_1g_2) = \theta(\upsilon(n_1.n_2.n_3)\ ,\ \psi^{-1}(l(Ng_1g_2)))$
$=(u_1.\phi(s_1)(u_2).\varsigma(s_1, s_2), s_1s_2) =(u_1, s_1)\cdot(u_2, s_2) =\theta(g_1)\theta(g_2)$.
Therefore θ is an isomorphism.

□

For this group of ordered pairs $U \times S$ with the operation (3) we will henceforth use the notation $U \boxtimes S$ and we call it one explicit extension of G. It is clear that given a group G there are many extensions as many normal subgroups it has. This means that if $N_1 \triangleleft G$ and $N_2 \triangleleft G$ then $N_1 \times \frac{G}{N_1}$ and $N_1 \times \frac{G}{N_1}$ are two extensions of G.

Notice that if the lifting $l : \frac{G}{N} \to G$ of (6) is a homomorphism then, ϕ of (7) becomes a group homomorphism and for ς of (8) we will have $\varsigma(q, r) = e$, for all $s, r \in S$. Therefore the group operation (3) will be reduced to

$$(u, s).(v, t) = (u.\phi(s)(t)\ ,\ st), \quad (3')$$

which is the operation of the semidirect product of U by G and which is ordinarily denoted by $U \rtimes S$, [8]. From this, we conclude that the extension of U by S is a generalization of the semidirect product of U by S.

Example 1: Consider the non abelian 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 $\{\alpha, \beta, \gamma, \delta\}$ satisfying the following relations

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

$N = \{e, \beta\gamma\}$ is a normal subgroup and N is isomorphic to the additive group of $\mathbb{Z}_2 = \{0, 1\}$. Then $\frac{G}{N}$ is isomorphic to the dihedral group $D8$, whose Cayley table is shown in the Table I. We construct an explicit extension $\mathbb{Z}_2 \boxtimes S$ for G by following the proof of the Theorem 2;

1. We have that $\upsilon : N \to \mathbb{Z}_2$ is given by $\upsilon(e) = 0$ and $\upsilon(\beta\gamma) = 1$. Whereas the isomorphism $\psi : D_8 \to G/N$ is given by

$$\begin{array}{llll} \psi(1) = N & \psi(2) = N.\alpha\delta & \psi(3) = N.\beta & \psi(4) = N.\alpha\beta\delta \\ \psi(5) = N.\alpha & \psi(6) = N.\alpha\beta & \psi(7) = N.\delta & \psi(8) = N.\beta\delta \end{array}$$

Considering 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 $l(N.\delta) = \delta$, the mappings ϕ and ς of (7) and (8), respectively, are defined. For instance,
$\phi(4)(1) = \upsilon[l(\psi(4)).\upsilon^{-1}(1).(l(\psi(4)))^{-1}]$
$= \upsilon[l(N.\alpha\beta\delta).\beta\gamma.(l(N.\alpha\beta\delta))^{-1}]$
$= \upsilon[\alpha\beta\delta.\beta\gamma.(\alpha\beta\delta)^{-1}]$
$= \upsilon[\beta\gamma] = 1,$
and
$\varsigma(4,2) = \upsilon[l(\psi(4)).l(\psi(2)).(l(\psi(42)))^{-1}]$
$= \upsilon[l(\psi(4)).l(\psi(2)).(l(\psi(1)))^{-1}]$
$= \upsilon[l(N.\alpha\beta\delta).l(N.\alpha\delta).(l(N))^{-1}]$
$= \upsilon[\alpha\beta\delta.\alpha\delta.(e)^{-1}]$
$= \upsilon[\beta\gamma] = 1.$
2. With the above ϕ and ς, the group operation for $\mathbb{Z}_2 \boxtimes D_8$ is defined. For instance $(0,4) \cdot (1,2) = (0 + \phi(4)(1) + \varsigma(4,2)\ ,\ 4.2) = (0 + 1 + 1\ ,\ 1) = (0,1)$. Therefore, $\mathbb{Z}_2 \boxtimes S$ is an explicit extension of G. The isomorphism θ is given by;

$$\begin{array}{lcl|lcl} \theta(e) & = & (0,1) & \theta(\alpha) & = & (0,5) \\ \theta(\beta) & = & (0,3) & \theta(\gamma) & = & (1,3) \\ \theta(\delta) & = & (0,7) & \theta(\alpha\beta) & = & (0,6) \\ \theta(\alpha\gamma) & = & (1,6) & \theta(\alpha\delta) & = & (0,2) \\ \theta(\beta\gamma) & = & (1,1) & \theta(\beta\delta) & = & (0,8) \\ \theta(\gamma\delta) & = & (1,8) & \theta(\alpha\beta\gamma) & = & (1,5) \\ \theta(\alpha\beta\delta) & = & (0,4) & \theta(\alpha\gamma\delta) & = & (1,4) \\ \theta(\beta\gamma\delta) & = & (1,7) & \theta(\alpha\beta\gamma\delta) & = & (1,2). \end{array}$$

We can test the linearity of θ for the elements $\alpha\beta\delta$ and $\alpha\beta\gamma\delta$; $\theta(\alpha\beta\delta) = (0,4)$ and $\theta(\alpha\beta\gamma\delta) = (1,2)$, then $\theta(\alpha\beta\delta).\theta(\alpha\beta\gamma\delta)) = (0,4).(1,2) = (0,1)$. On the other hand $\theta((\alpha\beta\delta).(\alpha\beta\gamma\delta)) = \theta(e) = (0,1)$.

III. Group Codes generated by wide sense homomorphic encoders

In this section we follow definitions and concepts from [4], [1], [5] and give a criterion of non controllability based on the the existence of a normal series of subgroups of the states group S.

Definition 2: Given a group G, consider the infinite direct product $G^{\mathbb{Z}} = \cdots \times G \times G \times G \ldots$. A **group code** over the group G is a subgroup of $G^{\mathbb{Z}}$

A wide-sense homomorphic encoder is a machine $M = (U, Y, S, \omega, \nu)$, where the input alphabet U, the output alphabet Y, and the the state set S are groups, and the next state map ν and the output(encoder) map ω are homomorphisms onto and into respectively defined on an extension $U \boxtimes S$ by the following mappings

$$\nu : U \boxtimes S \to S \tag{10}$$

$$\omega : U \boxtimes S \to Y \tag{11}$$

As pointed out in [4] these encoders give rise to time invariant trellis whose section elements are transitions or branches $(s, \omega(u,s), \nu(u,s)) \in S \times Y \times S$. The set of all branches $B = \{(s, \omega(u,s), \nu(u,s))\ ;\ (u,s) \in U \boxtimes S\}$ is the trellis section and it is isomorphic to $U \boxtimes S$ via the following mapping Ψ

$$\Psi(u,s) = (s, \omega(u,s), \nu(u,s)). \tag{12}$$

Therefore we have $B \cong U \boxtimes S$.

Since ν is surjective, for any $s_0 \in S$ there are $u_0 \in U$ and $s_{-1} \in S$ such that $s_0 = \nu(u_0, s_{-1})$. We can reconstruct one "past" of s_0 by putting $s_{-k} = \nu(u_{-k}, s_{-k-1})$, $k \in \mathbb{N}$, such that $s_0 = \nu(u_0, \nu(u_{-1}, \ldots \nu(u_{-k}, s_{-k-1}) \ldots))$. Therefore for a given $s_0 \in S$ and a sequence of inputs $\{u_i\}_{i\in\mathbb{Z}}$, the encoder (10)-(11)responds with two sequences $\{s_i\}_{i\in\mathbb{Z}}$ and $\{y_i\}_{i\in\mathbb{Z}}$ given by;

$$\begin{array}{lcl|lcl} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{-1} & = & \nu(u_{-1}, s_{-2}) & y_{-1} & = & \omega(u_{-1}, s_{-2}) \\ s_0 & = & \nu(u_0, s_{-1}) & y_0 & = & \omega(u_0, s_{-1}) \\ s_1 & = & \nu(u_1, s_0) & y_1 & = & \omega(u_1, s_0) \\ s_2 & = & \nu(u_2, s_1) & y_2 & = & \omega(u_2, s_1) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots, \end{array}$$

The family of sequences $\{s_i\}_{i\in\mathbb{Z}}$ is a subgroup of $S^{\mathbb{Z}} = \ldots S \times S \times S \times \ldots$ while the family of sequences $\{y_i\}_{i\in\mathbb{Z}}$ is a subgroup of $Y^{\mathbb{Z}} = \ldots Y \times Y \times Y \times \ldots$ defined as the group code $\mathcal{C}$ over the group Y generated by the encoder (11-10), [4], [5].

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 $\omega(u_1,s_1) \neq \omega(u_2,s_2)$

The following Lemma resembles the Theorem 4 of [6]

Lemma 1: Consider the encoder of (10)-(11) and suposse $U \boxtimes S$ non abelian. Let H^+ and H^- 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. Both H^+ and H^- are normal subgroups of $U \boxtimes S$,
2. If $H^+ \cap H^- \neq \{(e,e)\}$ then the trellis section B has parallel transitions
3. If the states group S is abelian then B has parallel transitions

Proof:
1. Immediate.
2. There exists $(u,e) \in H^+ \cap H^-$, with $u \neq e$ such that $\nu(u,e) = e$. Since Ψ of (12) is bijective, $\omega(u,e) \neq e$. Therefore, the transitions $(e, \omega(e,e), \nu(e,e))$ and $(e, \omega(u,e), \nu(u,e))$ are parallels.
3. The states group S being abelian implies that $\frac{G}{H^+} \cong \frac{G}{H^-} \cong S$ 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 2, B has parallel transitions.

□

If S is finite the group code $\mathcal{C}$ produced by (10) and (11) is **controllable** if for any pair of states s and s' there exists a finite sequence of inputs $\{u_i\}_{i=1}^n$ such that $s = \nu(u_n, \nu(u_{n-1}, \nu(u_{n-2}, \dots, \nu(u_2, \nu(u_1, s'))\dots)))$, [1], [5].

Definition 3: A normal series of a group G is a sequence of subgroups $\{G_i\}_{i=0}^n$ such that $\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$. [8], [7] □

Lemma 2: The commutators subgroup S' is invariant for automorphisms, that is, $\varphi(S') \subset S'$, for all $\varphi \in Aut(S)$.

Proof: For $s \in S'$, $s = aba^{-1}b^{-1}$, for some $a, b \in S$. Then, for any $\varphi \in Aut(S)$, $\varphi(s) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} \in S'$. □

Given an encoder (10)-(11), consider the family of state subsets $\{S_i\}$, recursively defined by;

$$\begin{array}{lcl} S_0 & = & \{e\} \\ S_1 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_0\} \\ S_2 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_1\} \\ \vdots & \vdots & \vdots \\ S_i & = & \{\nu(u,s)\ ;\ u \in U, s \in S_{i-1}\}, i \geq 0 \\ \vdots & = & \vdots \end{array} \tag{13}$$

Theorem 3: Some properties of the family $\{S_i\}$;
1. S_1 is normal in 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. Let S' be the subgroup of commutators of S. Then, $S_i \subset S'$ implies $S_{i+1} \subset S'$.
5. If the family $\{S_i\}$ is not a normal series of S then the group code is non controllable.
6. Let $Aut(S)$ be the group of automorphisms of S. If for some $i \geq 1$, $\varphi(S_i) \subset S_i \subsetneq S$ for all $\varphi \in Aut(S)$ then the group code is non controllable.

Proof:
1. Since $U \times \{e\}$ is a normal subgroup of $U \boxtimes S$, then $S_1 = \nu(U \times \{e\})$ is normal in S.
2. In the first place we show that $S_{i-1} \subset S_i$, for any i. Clearly $S_0 \subset S_1$. Now, for $i > 1$, suposse $S_{j-1} \subset S_j$, for all $j \leq i$. Given $s \in S_i$, there are $r \in S_{i-1}$ and $u \in U$ such that $\nu(u, r) = s$. Since $r \in S_{i-1} \subset S_i$ then $\nu(u, r) = s \in S_{i+1}$.
On the other hand, clearly $S_0 \lhd S_1$. For $i > 1$, suposse $S_{j-1} \lhd S_j$, 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. Let $\pi_2 : U \boxtimes S \to S$ be the projection homomorphism given by $\pi_2(u, s) = s$. For any surjective homomorphism $\nu : U \boxtimes S \to S$ there is $\varphi \in Aut(S)$ such that $\nu = \varphi_o \pi_2$, Figure 1. If $s \in S'$ then $\nu(u, s) = \varphi(\pi_2(u, s)) = \varphi(s) \in S'$.
5. Let S_S be the union of the S_i's, that is, $S_S = \cup_i S_i$. Then, $S_i \subset S_S$ for all i. If $S_S = S$ then $\{S_i\}_i$ is a normal series. If $S_S \neq S$, there is $s \in S$ such that $s \notin S_S$. Then there is not any finite sequence $\{u_i\}_{i=1}^n$ such that $s = \nu(u_n, \nu(u_{n-1}, \nu(u_{n-2}, \dots, \nu(u_2, \nu(u_1, e))\dots)))$.

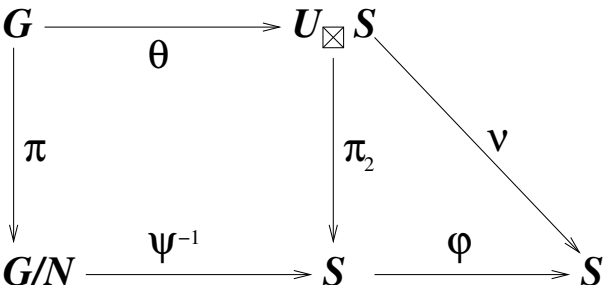

Fig. 1. The dynamic of the next state homomorphism $\nu : U \boxtimes S \to S$

6. $\nu(u, S_i) = \varphi((\pi_2(u, S_i)) = \varphi(S_i) \subset S_i \subsetneq S$. Therefore by the above item the code is non controllable.

□

IV. The extension $\mathbb{Z}_p \boxtimes S$

Let p be a prime and let S be a finite group, then the extension group $\mathbb{Z}_p \boxtimes S$ is defined as the Definition 1

Lemma 3: Let p be a prime and let B be a controllable trellis section isomorphic to $\mathbb{Z}_p \boxtimes S$, then
1. $Aut(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$
2. Let $\phi : G \to H$ be a group homomorphism. If $n = |G|$ and $m = |H|$ are relative primes, then ϕ is the trivial homomorphism, that is, $\phi(g) = e \in H$, for all $g \in G$.
3. $|\mathbb{Z}_p \boxtimes S| = p^n$, for some $n \in \mathbb{N}$.
4. The semidirect product $\mathbb{Z}_p \rtimes S$ becomes the direct product $\mathbb{Z}_p \times S$.

Proof:
1. See [8], page 157.
2. By the fundamental theorem of homomorphisms.
3. By item 2 snd 3 of the Theorem 3, $|S| = p^{n-1}$.
4. Since $p^n = (p-1)(p^{n-1} + p^{n-2} + \cdots + p + 1) + 1$, then $gcd(p^n, p-1) = 1$, for all $n \in \mathbb{N}$. Then by the above item 2 we conclude that the mapping $\phi : S \to Aut(\mathbb{Z}_p)$, defined by (7) is reduced to $\phi(s) = id$, for all $s \in S$. Therefore for any couple of pairs (u_1, s_1) and (u_2, s_2) we have $(u_1, s_1).(u_2, s_2) = (u_1 + u_2, s_1 s_2)$.

□

Lemma 4: If H and K are subgroups of G then the intersection $H \cap K$ is subgroup of G.

Lemma 5: For the extension $\mathbb{Z}_p \boxtimes S$ consider the subgroups $\{S_i\}$ defined in (13). Let S' be the commutators subgroup of S. Then, for $i = 1, 2, 3, \dots$, either S_i is abelian or $S_i \subset S'$.

Proof: Clearly S_1 and S_2 are abelians. Consider any $i \geq 2$ such that $S_1, S_2, \dots, S_i$ are abelians. Then for given $s_1, s_2 \in S_{i+1}$ we have $s_1 = \nu(u_1, r_1)$ and $s_2 = \nu(u_2, r_2)$, with $u_1, u_2 \in \mathbb{Z}_p$ and $r_1, r_2 \in S_i$ and $r_1 r_2 = r_2 r_1$. From this, $s_1.s_2 = \nu(u_1, r_1).\nu(u_2, r_2) = \nu(u_1 + u_2 + \varsigma(r_1, r_2), r_1 r_2)$ and $s_2.s_1 = \nu(u_1 + u_2 + \varsigma(r_2, r_1), r_1 r_2)$, where ς is as (8). Hence, $s_1.s_2 \neq s_2.s_1$ if only if $\varsigma(r_1, r_2) \neq \varsigma(r_2, r_1)$.

We can supose that $\varsigma(r_1, r_2) = u \in \mathbb{Z}_p$ and $\varsigma(r_2, r_1) = v \in \mathbb{Z}_p$. Then, for the lifting l of (6), we have $l(\psi(r_1)).l(\psi(r_2)).(l(\psi(r_1 r_2)))^{-1} = n_1 \in N$ and $l(\psi(r_2)).l(\psi(r_1)).(l(\psi(r_1 r_2)))^{-1} = n_2 \in N$, where N is such that $\upsilon(N) = \mathbb{Z}_p$ with υ as (4). From this $n_2 n_1^{-1} = l(\psi(r_2)).l(\psi(r_1)).(l(\psi(r_1)))^{-1}.l(\psi(r_2)))^{-1} \in G'$. If $n_2 \neq n_1$

then $n_2 n_1^{-1} \neq e$ and $N \cap G\prime \neq \{e\}$. Since $|N| = p$, $N \subset G\prime$ and therefore $\mathbb{Z}_p \boxtimes \{e\} \subset (\mathbb{Z}_p \boxtimes S)'$ and $\nu(\mathbb{Z}_p \boxtimes \{e\}) = S_1 \subset S'$. Hence $S_i \subset S'$.

□

Theorem 4: Consider a group code $\mathcal{C}$ with information group $\mathbb{Z}_p$ and states group S, with S finite, then;

1. If S is abelian, then the free distance of the group code is bounded by the hamming distance of the output group Y.

2. If S is non abelian, then the group code is non controllable.

Proof:

1. By the item 3 of the Lemma 1 the code has parallel transitions.

2. By the Lemma 5, S_i of (13) is abelian or $S_i \subset S'$, for each i. Then this family is not a normal series of S. Therefore, by the Theorem 3, the group code is non controllable.

□

Example 2: Consider the non abelian group $G = \{e, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma, \delta, \alpha\delta, \beta\delta, \alpha\beta\delta, \gamma\delta, \alpha\gamma\delta, \beta\gamma\delta, \alpha\beta\gamma\delta\}$ of the Example 1

For the decomposition $\mathbb{Z}_2 \boxtimes D_8$ given in that Example 1 there is not any controllable group code having trellis section B with inputs group $\mathbb{Z}_2$ and states group D_8. The other 16 non abelian explicit extensions are $\mathbb{Z}_2 \boxtimes D_8$, $\mathbb{Z}_2 \boxtimes Q_8$, $\mathbb{Z}_4 \boxtimes Z_4$, etc. For no one of these extensions there exists a controllable code.

V. Conclusions

We have studied the case of non abelian group codes with information group $\mathbb{Z}_p$ and states group being any finite group S. The trellis section of these codes are isomorphic to the extension $\mathbb{Z}_p \boxtimes S$ and we have shown that for the case S abelian, the code has parallel transitions with distance limitations. For the case S non abelian the code is non controllable

Presently, by using the Theorem 4, and the criteria, on normal series of the group of states S, given by the Theorem 3 we implemented some scripts on the system GAP [9] for an exhaustive searching over all the 3349 non abelian groups with cardinality ≤ 128. We have found that there are only 77 non abelian groups G which yield group codes with trellis section $B \cong G \cong U \boxtimes S$ such that;

- The trellis section B has not parallel transitions
- The respective group code is controllable.

To simplify this exhaustive search we are now focusing our efforts on extensions such as the semidirect products $\mathbb{Z}_{pn} \rtimes S$, $\mathbb{Z}_{p^n} \rtimes S$ with p prime.

References

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

[2] S.Benedetto, "Multilevel construction of block and trellis group codes", *IEEE Trans. Inform. Theory*; vol. IT-41 No 5, pp. 1257-1264, September 1995.

[3] J. P. Arpasi "The semidirect product $\mathbb{Z}_2$ by a finite group S is bad for non abelian codes", *CD-ROM XX Simpósio Brasileiro de Telecomunicações*, Rio de Janeiro, 05-08 de Outubro de 2003.

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

[5] 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.

[6] G.D.Forney, "On the Hamming distance properties of group codes" *IEEE Trans. Inform. Theory*; vol. IT-38 No 6, pp. 1797-1801, November 1992.

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

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

[9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*; 2002, (`http://www.gap-system.org`).