The semidirect product $\mathbb{Z}_2$ by a finite group S is bad for non abelian codes

Jorge Pedraza Arpasi

Abstract— **In this work we study the time invariant trellis group codes with non abelian trellis section group B which is the semidirect product of the additive group $\mathbb{Z}_2 = \{0, 1\}$ by a finite group S. We will show that when S is abelian then the code has free distance limitations, and on the other hand, when S is non abelian the code is non controllable. Therefore, there are not convolutional codes with non abelian trellis section isomorphic to the semidirect product $\mathbb{Z}_2$ by S.**

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

I. Introduction

It has been shown in [1] 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 construction of codes over non abelian groups are required as a possibility to overcome this PSK-limit. For that, in [2] it is presented a multilevel method based on the semidirect product of two codes. Since this just cited method does not allow an exhaustive search over small groups, in this work we give an indirect method to search exhaustively non abelian codes over small groups. We will work with convolutional codes over groups, defined in [3], which are observable, controllable, and time invariant group codes. The *wide-sense homomorphic 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 inputs 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 has order two but the identity. 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.

We will denote by e the *neutral* or *identity* element of an abstract group G, but in the case of the groups $\mathbb{Z}_2$ and Q_8, used in the Examples, 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. This paper is structured as follows.

In the section II we give a practical method to construct one explicit extension from a given group G. 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 [1], [3], and [4] to define and review group codes generated by a wide-sense homomorphic encoder, and we find one criterion for controllability of this 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 code with non abelian trellis section isomorphic to the semidirect product $\mathbb{Z}_2 \rtimes S$. We will show that when S is abelian then the code will have free distance limitations because it will have parallel transitions. When S is non abelian we show that a code with trellis section isomorphic to the semidirect product $\mathbb{Z}_2$ 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 of extension of groups and show a method to decompose a group.

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

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

for all $s_1, s_2, s_3 \in S$ and

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

for all $u \in U$ and for all $s_1, s_2 \in S$; then $U \times S$ with the following operation

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

is a group extension of U by S.

Proof: See [7], [6]. □

Theorem 2: Let G be a group with a normal subgroup $N \triangleleft G$, let U, S be groups such that $U \cong N$ and $S \cong \frac{G}{N}$. Then there exist the mappings satisfying (1) and (2) and $U \times S$, with the group operation (3) is isomorphic to G.

Proof: Let $\upsilon : N \to U$ and $\psi : S \to \frac{G}{N}$ 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 $\psi(s) \in \frac{G}{N}$

The author is with the Departamento de Engenharias e Ciência da Computação, Universidade Regional Integrada Frederico Westphalen - URI/FW, Rio Grande do Sul, Brazil. Email: arpasi@fw.uri.br

and $\upsilon^{-1}(u) \in N$. Then, consider one lifting $l : \frac{G}{N} \to G$ such that $l(N) = e$, where e is the neutral element of G. 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

$$\phi(s)(u) = \upsilon[l(\psi(s)).\upsilon^{-1}(u).(l(\psi(s)))^{-1}]. \quad (4)$$

On the other hand, consider $s, t \in S$ then $l(\psi(s)).l(\psi(t))$ and $l(\psi(st))$ belong to the coset $N * l(\psi(st))$. 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

$$\varsigma(s,t) = \upsilon[l(\psi(s)).l(\psi(t)).(l(\psi(st)))^{-1}]. \quad (5)$$

Now, we verify that these mappings (4) and (5) satisfy the 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 goup operation, (3) is a group.

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

$$\theta(g) = \theta(n.l(Ng)) = (\upsilon(n)\ ,\ \psi^{-1}(Ng)), \quad (6)$$

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. □

This group $U \times S$ with the operation (3) will be denotated by $U \boxtimes S$ and it will be called as one explicit extension or decomposition of G. It is clear that given a group G there are as many decompositions as many normal subgroups G has.

Notice that if the lifting $l : \frac{G}{N} \to G$ is a homomorphism then, ϕ of (4) becomes a group homomorphism and for ς of (5) we will have $\varsigma(q,r) = e$, for all $s, r \in S$. Therefore the group operation (3) will be reduced to

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

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

TABLE I
THE QUATERNIONS GROUP Q_8

which is the semidirect product operation $U \rtimes S$. From this, we conclude that the extension of groups is a generalization of the semidirect product.

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

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

Consider the normal subgroup $N = \{e, \beta\}$. Then N is isomorphic to the additive group of $\mathbb{Z}_2 = \{0, 1\}$ and $\frac{G}{N}$ is isomorphic to the group of symmetries of the square, $Q8$, whose Cayley table is shown in Table I. We decompose G as $\mathbb{Z}_2 \rtimes Q_8$ following the proof of the Theorem 2;

1. We have that $\upsilon : N \to \mathbb{Z}_2$ is given by $\upsilon(e) = 0$ and $\upsilon(\beta) = 1$. Whereas the isomorphism $\psi : Q_8 \to G/N$ is given by

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

Considering the lifting $l : G/N \to G$ defined by $l(N) = e$, $l(N.\delta) = \delta$, $l(N.\gamma) = \gamma$, $l(N.\alpha) = \alpha$, $l(N.\alpha\gamma\delta) = \alpha\gamma\delta$, $l(N.\alpha\delta) = \alpha\delta$, $l(N.\alpha\gamma) = \alpha\gamma$ and $l(N.\gamma\delta) = \gamma\delta$, the mappings ϕ and ς of (4) and (5), respectively, are defined. In this case we have $\varphi(s_1, s_2) = 0$, for all $s_1, s_2 \in Q_8$
For instance,
$\phi(7)(1) = \upsilon[l(\psi(7)).\upsilon^{-1}(1).(l(\psi(7)))^{-1}]$
$= \upsilon[l(N.\alpha\gamma).\beta.(l(N.\alpha\gamma))^{-1}]$
$= \upsilon[\alpha\gamma.\beta.(\alpha\gamma)^{-1}]$
$= \upsilon[\beta] = 1,$
and
$\varsigma(4,2) = \upsilon[l(\psi(4)).l(\psi(2)).(l(\psi(42)))^{-1}]$
$= \upsilon[l(\psi(4)).l(\psi(2)).(l(\psi(6)))^{-1}]$
$= \upsilon[l(N.\alpha).l(N.\delta).(l(N.\alpha\delta))^{-1}]$
$= \upsilon[\alpha.\delta.(\alpha\delta)^{-1}]$
$= \upsilon[e] = 0.$

2. Since the lifting l is a group homomorphism, and in this case we have the semidirect product $\mathbb{Z}_2 \rtimes Q_8$, whose

group operation is defined by (3$\prime$). The group operation for $\mathbb{Z}_2 \rtimes Q_8$ is defined. For instance $(0,7)\cdot(1,3) = (0+\phi(7)(1)\ ,\ 7.3) = (0+1\ ,\ 1) = (0,1)$. Therefore the group G is decomposed as the semidirect product $\mathbb{Z}_2 \rtimes Q_8$ via the isomorphism θ of (6);

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

For instance, $\theta(\alpha\beta\delta) = (1,2)$ and $\theta(\alpha\beta\gamma\delta) = (1,8)$, then $\theta(\alpha\beta\delta).\theta(\alpha\beta\gamma\delta)) = (1,2).(1,8) = (0,3)$. On the other hand $\theta((\alpha\beta\delta).(\alpha\beta\gamma\delta)) = \theta(\gamma) = (0,3)$. □

III. Group Codes generated by Wide sense encoders

In this section we review some definitions and concepts from [3], [1], [4]. Given a group G, condider 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 map ω are homomorphisms onto and into respectively defined on an extension $U \boxtimes S$ by the following equations

$$\omega : U \boxtimes S \to Y \tag{7}$$

$$\nu : U \boxtimes S \to S \tag{8}$$

As pointed out in [3] 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

$$\Psi(u,s) = (s, \omega(u,s), \nu(u,s)). \tag{9}$$

Therefore we have

$$G \cong U \boxtimes S \cong B.$$

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 $s_{-k} = \nu(u_{-k}, s_{-k-1})$, $k \in \mathbb{N}$, 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 $\{u_i'\}_{i\in\mathbb{N}}$, the encoder (8)-(7)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 subsequences $\{s_i\}_{i\in\mathbb{N}}$ and $\{y_i\}_{i\in\mathbb{N}}$ are uniquely determined while the subsequences $\{s_i\}_{-\infty}^{i=-1}$ and $\{y_i\}_{-\infty}^{i=0}$ are dependent on the choice of the past of s_0. 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 $Y^{\mathbb{Z}} = \ldots Y \times Y \times Y \times \ldots$ therefore is a group code $\mathcal{C}$ over the group Y.

If S is finite this group code $\mathcal{C}$ produced by (8) and (7) 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 $s = \nu(u_n, \nu(u_n, \nu(u_{n-1}, \ldots, \nu(u_2, \nu(u_1, s')) \ldots)$, [1], [4].

Definition 2: A normal series of a group G is a sequence of subgroups $e = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$. [6], [7]

Given an encoder defined by (8) and (7) consider the family of state subsets $\{S_i\}$, recursively defined by;

$$\begin{array}{lcl} S_0 & = & \{e\} \\ S_1 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_0\} \\ S_2 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_1\} \\ \vdots & \vdots & \vdots \\ S_i & = & \{\nu(u,s)\ ;\ u \in U, s \in S_{i-1}\} \\ \vdots & = & \vdots \end{array} \tag{10}$$

Proposition 1: 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 $i = 1, 2, \ldots$.
3. If $S_{i-1} = S_i$ then $S_i = S_{i+1}$
4. If the family $\{S_i\}_i$ is not a normal series 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 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 $s = \nu(u_n, \nu(u_n, \nu(u_{n-1}, \ldots, \nu(u_2, \nu(u_1, e)) \ldots)$. □

□

IV. There are no controllable group codes without parallel transitions for semidirect product $\mathbb{Z}_2 \rtimes S$

In this section we define parallel transitions of a group code and show a result relating parallelism and the abelianness of the group of states S.Then we show that there is

not any controllable and non abelian group code with trellis section group isomorphic to $\mathbb{Z}_2 \rtimes S$.

Two 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 the encoder of (8), (7) 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 B has parallel transitions
3. If the states group S is abelian then B has parallel transitions

Proof:
1. Imediate.
2. There exists $(u, e) \in H^+ \cap H^-$, with $u \neq e$ such that $\nu(u, e) = e$ with, since Ψ of (9) 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. □

□

This result resembles the Theorem 4 of [5]

Lemma 2: Let G be a group with identity e and let S be any finite group, then;
1. If for each $g \in G$, $g^2 = 1e$ then G must be abelian.
2. Any semidirect product $\mathbb{Z}_2 \rtimes S$ becomes a direct product $\mathbb{Z}_2 \times S$
3. For $\mathbb{Z}_2 \rtimes S$, each subgroup of the family $\{S_i\}$ of (10) is abelian.

Proof:
1. $id = (ab)^2 = abab$ Then $a^{-1}b^{-1} = ba$. Hence $ab = ba$.
2. Since $Aut(\mathbb{Z}_2) = \{id\}$, then $\phi : S \to Aut(Z_2)$ of (4) is given by $\phi(s)(u) = u$ for all $s \in S$ and for any $u \in \{0, 1\} = \mathbb{Z}_2$. Therefore $(u_1, s_1).(u_2, s_2) = (u_1 + \phi(s_1)(u_2)\ ,\ s_1 s_2) = (u_1 + u_2, s_1 s_2)$ for all $u_1, u_2 \in \mathbb{Z}_2$ and for all $s_1, s_2 \in S$.
3. By induction. For $S_1 = \{0, s\}$ we have $s^2 = e$. Supose for $k > 1$, $s^2 = e$ for all $s \in S_k$. Now consider $r \in S_{k+1}$. There exist $s \in S_k$ and $u \in \mathbb{Z}_2$ such that $r = \omega(u, s)$. Then, by the above item 2, $r^2 = \omega((u, s)^2) = \omega(u+u, s^2) = \omega(0, e) = e$. Finally, by using the item 1 we conclude that each S_i must be abelian.

□

Thus by using the Proposition 1 and the Lemmas 1 and 2 we have the following Theorem.

Theorem 3: There is not any controllable group code without parallel transitions for the semidirect product $\mathbb{Z}_2 \rtimes S$.

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 $\mathbb{Z}_2 \rtimes Q_8$ of G there is not any controllable group code having trellis section B with inputs group $\mathbb{Z}_2$ and states group Q_8. The respective group code has non controllable trellis section. Searching over all the other $\mathbb{Z}_2 \rtimes S$ decompositions of G, we have not found any controllable group code.

V. Conclusions

We have shown that the semidirect product $\mathbb{Z}_2 \rtimes S$ is bad for the construction of non abelian codes. Consequently we need to search over other kind of extensions $U \boxtimes S$ in order to find good groups for non abelian codes. We implemented scripts by using the Theorem 3 and the Lemmas 1 and 2 in the system GAP [8] to search codes over non abelian groups such that their decomposition is different from $\mathbb{Z}_2 \rtimes S$.

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] H.A. Loeliger, Mittelholzer T.; "Convolutional Codes Over Groups", *IEEE Transactions on Information Theory* Vol IT 42, No 6, pp 1659-1687, November 1996.
[4] 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.
[5] 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.
[6] Rotman J. J.; *An Introduction to the Theory of the Groups*, Fourth Ed., Springer Verlag 1995.
[7] Hall M. Jr..; *The Theory of Groups*, MacMillan, New York, 1959.
[8] The GAP Group — Groups, Algorithms, and Programming, Version 4.2; Aachen, St Andrews, 1999. (http://www-gap.dcs.st-and.ac.uk/ gap)