Invariant Subgroups and Controllability of Group Codes

by

Jorge Pedraza Arpasi

Universidade Estadual do Rio Grande do Sul - UERGS
Campus Erechim - RS
Rio Grande do Sul
Brazil
Introduction

Definition 1 (Loeliger, Mittelholzer 1996) A convolutional code over a group $G$ is a time-invariant, strongly controllable, and strongly observable group code over $G$. 
Introduction

Definition 1  (Loeliger, Mittelholzer 1996) A convolutional code over a group $G$ is a time-invariant, strongly controllable, and strongly observable group code over $G$.

The main examples of this definition are the binary convolutional codes with rate $\frac{k}{n}$ and memory $m$, which are controllable and observable group codes over the group $\mathbb{Z}_2^n$, with states group $\mathbb{Z}_2^m$ and uncoded group $\mathbb{Z}_2^k$. 
Introduction (cont...) 

➤ When $G$ is non abelian, there are not practical and general method to construct controllable group codes over a group $G$. 
Introduction (cont...)

➤ When $G$ is non abelian, there are not practical and general method to construct controllable group codes over a group $G$.

➤ In this work we study a subclass of group codes and we give a necessary condition to determine their controllability.
Given a group $G$, a **normal series** of $G$ is a sequence of subgroups $G_i \subset G$ such that $G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = \{id\}$, where $id$ is the identity element of $G$ and $G_{i-1}$ is a normal subgroup of $G_i$, that is, $G_{i-1} \triangleleft G_i$. 
Given a group $G$, a **normal series** of $G$ is a sequence of subgroups $G_i \subset G$ such that $G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = \{id\}$, where $id$ is the identity element of $G$ and $G_{i-1}$ is a normal subgroup of $G_i$, that is, $G_{i-1} \triangleleft G_i$.

The subgroup generated by elements of the form $ghg^{-1}h^{-1}$ is called either the **commutators** subgroup or **derived** subgroup of $G$ and it is denoted by $G'$. Clearly, if $G$ is abelian then $G'$ is reduced to $\{id\}$.
Algebraic facts

➤ Given a group $G$, a **normal series** of $G$ is a sequence of subgroups $G_i \subset G$ such that $G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = \{\text{id}\}$, where $\text{id}$ is the identity element of $G$ and $G_i \supset G_{i-1}$ is a normal subgroup of $G_i$, that is, $G_i \triangleleft G_i$.

➤ The subgroup generated by elements of the form $ghg^{-1}h^{-1}$ is called either the **commutators** subgroup or **derived** subgroup of $G$ and it is denoted by $G'$. Clearly, if $G$ is abelian then $G'$ is reduced to $\{\text{id}\}$.

➤ One important property of $G'$ is its **invariance** under the action of the group of automorphisms of $G$, that is, $\phi(G') = G'$ for all $\phi \in \text{Aut}(G)$. 
Algebraic facts (cont...)

Definition 2  If $X$ and $Q$ are groups, then an extension of $X$ by $Q$ is a group $G$ having a normal subgroup $N$, isomorphic to $X$, with the factor group $\frac{G}{N}$ isomorphic to $Q$. 
Definition 2  If $X$ and $Q$ are groups, then an extension of $X$ by $Q$ is a group $G$ having a normal subgroup $N$, isomorphic to $X$, with the factor group $\frac{G}{N}$ isomorphic to $Q$.

- An extension is a generalization of the direct and semidirect product of groups.

- If $G$ has a non-trivial normal subgroup then it has an decomposition $G \cong X \phi \varsigma Q$, with $X \cong N$ and $Q \cong G/N$. 
Construction of group codes from a given group $G$

Given a group $G$ with a non-trivial normal subgroup $N \triangleleft G$, we can construct a group code $C$, associated with $G$, as follows;

- Decompose $G$ as the extension $X_{\phi}Q$

- Define the next state homomorphism $\omega : X_{\phi}Q \rightarrow Q$. It must be surjective.

- Define the encoder homomorphism $\nu : X_{\phi}Q \rightarrow Y$, for some group $Y$. 
Consider an initial state \( q_0 \in Q \) and a sequence of information symbols, \( \{x_i\}_{i \in \mathbb{N}}, x_i \in X \). Then the response of \( \omega \) and \( \nu \) are the sequences \( \{q_i\}_{i \in \mathbb{N}} \) and \( \{y_i\}_{i \in \mathbb{N}} \) defined by;

\[
\begin{align*}
q_1 &= \omega(x_1, q_0) & y_1 &= \nu(x_1, q_0) \\
q_2 &= \omega(x_2, q_1) & y_2 &= \nu(x_2, q_1) \\
\vdots & \vdots & \vdots & \vdots \\
q_i &= \omega(x_i, q_{i-1}) & y_i &= \nu(x_i, q_{i-1}) \\
\vdots & \vdots & \vdots & \vdots
\end{align*}
\]
Construction of group codes from a given group $G$ (cont...)

➤ The group code $C$ associated is the collection of sequences $\{y_i\}_{i \in \mathbb{N}}$.

➤ The trellis section of this group code $T = \{(q, \nu(x, q), \omega(x, q)) ; x \in X, q \in Q\}$, is a group isomorphic to the given group $G$ and $X_{\phi \varsigma}Q$. That is,

$$T \cong G \cong X_{\phi \varsigma}Q.$$
Control

➤ A group code, constructed in such above way, is controllable if any pair of sequences of states have a not null intersection.

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

Consider the family \{Q_i\}, recursively defined by:

\[
Q_0 = \{id\}
\]
\[
Q_1 = \{\omega(x, q) ; x \in X, q \in Q_0\}
\]
\[
Q_2 = \{\omega(x, q) ; x \in X, q \in Q_1\}
\]
\[
\vdots \quad \vdots \quad \vdots
\]
\[
Q_i = \{\omega(x, q) ; x \in X, q \in Q_{i-1}\}
\]
\[
\vdots = \vdots
\]

Then \(Q_{i-1} \triangleleft Q_i\).
Main Results of this work

**Theorem 1**  *If* $Q_i$ *is invariant under* $\text{Aut}(Q)$ *then the group code is non controllable*

**Proof.-**
Main Results of this work

**Theorem 1**  If $Q_i$ is invariant under $\text{Aut}(Q)$ then the group code is non controllable.

**Proof.**- For the extension $G \cong X_{\phi \varsigma} Q$ we need to construct a next state homomorphism $\omega : G \rightarrow Q$. Let $\pi : G \rightarrow G/N$ be the fixed natural homomorphism and let $\psi : Q \rightarrow G/N$ be a fixed isomorphism. Then the choice of $\omega$ depends only on the choice of $\varphi \in \text{Aut}(Q)$. That is, $\omega = \varphi \psi^{-1} \pi$, as is shown in the following Figure. Therefore, $\omega(x, Q_i) = \varphi \psi^{-1} \pi(x, Q_i) = \varphi(Q_i) = Q_i$, for all $x \in X$. \hfill \blacksquare
The next state homomorphism $\omega$ depends on $\varphi \in \text{Aut}(Q)$.
Main Results of this work (cont...)

**Theorem 2** Let $X_{φs}Q$ be an extension. If there is a controllable associated group code $C$, then $Q$ must have a normal series $\{id\} = Q_0 \triangleleft Q_1 \triangleleft \cdots \triangleleft Q_{n-1} \triangleleft Q_n = Q$ such that

1. $Q_1 \triangleleft Q$ and $|Q_1|$ is a divisor of $|X|$,
2. $Q_i \not\subseteq Q'$, for all $i = 1, 2, \ldots$, where $Q'$ is the derived subgroup of $Q$. 
Main results of this work (cont...)

Proof.-
Main results of this work (cont...)

**Proof.**- On the contrary;

➢ If $Q$ has not a normal series with $|Q_1|$ dividing $|X|$, then for $X_0 = \{ x \in X ; \omega(x, id) = id \}$ we would have $\frac{X}{X_0}$ is not isomorphic to $Q_1$.

➢ If for each normal series of $Q$ there is some $Q_i$ such that $Q_i \subset Q'$ then $Q_i$ is invariant any automorphism of $Q$. Therefore $C$ is non controllable.
Example

Example 1  Consider the extension $\mathbb{Z}_{2\phi_5}D_8$

There are three normal series $D_8 = Q_n \triangleright Q_{n-1} \triangleright Q_{n-2} \triangleright \cdots \triangleright Q_1 \triangleright Q_0 = \{id\}$ with $|Q_1| = 2$. But all these series have $Q_1 = D_8'$, the commutators subgroups. Therefore there is not any controllable group code $C$ associated to the extension $\mathbb{Z}_{2\phi_5}D_8$. 