Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2011, Article ID 783516, 12 pages
doi:10.1155/2011/783516

Research Article

On the Uncontrollability of Nonabelian Group Codes with Uncoded Group $\mathbb{Z}_p$

Jorge Pedraza Arpasi

Technological Center of Alegrete, Federal University of Pampa (UNIPAMPA) 97546-550 Alegrete, RS, Brazil

Correspondence should be addressed to Jorge Pedraza Arpasi, arpasi@gmail.com

Received 5 November 2010; Revised 24 August 2011; Accepted 2 September 2011

Academic Editor: Gerhard-Wilhelm Weber

Error-correcting encoding is a mathematical manipulation of the information against transmission errors over noisy communications channels. One class of error-correcting codes is the so-called *group codes*. Presently, there are many good binary group codes which are abelian. 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. 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 nonabelian groups. This necessity on the encoder is because it has been shown that the capacity of an additive white Gaussian noise (AWGN) channel using abelian group codes is upper bounded by the capacity of the same channel using phase shift keying (PSK) modulation eventually with different energies per symbol. We will show that when the trellis section group is nonabelian and the input group of the encoder is a cyclic group with, p elements, p prime, then the group code produced by the encoder is noncontrollable.

1. Introduction

Data to be transmitted through a noisy channel may suffer impairments when it arrives to its destination. The most known channel 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 [1–4]. In the landmark paper [5], Shannon showed that there exist methods to encode data against channel noise. One key idea behind an error-correcting code—ECC—is the measure of the channel noise in terms of error probability $P(e)$. For binary data, $P(e)$ of a given physical channel can be obtained empirically. For instance, if after transmitting 10^{15} bits through the channel we observe that $10^{15} - 1$ bits were transmitted correctly and one bit was transmitted erroneously, then we can say that the upper bound of $P(e)$, of this channel, is 10^{-15} or $P(e) < 10^{-15}$. This error probability can be reduced by enhancing the hardware components of the channel or alternatively by using ECC. Mostly the use of ECC on the data to be transmitted is more economic than the enhancing of hardware components of the physical channel. That is why an ECC is important. Classically, the essence of an ECC is the splitting of the information data to be transmitted in packages with constant size, let us say m, then is the added k symbols which are functions of the previous m symbols. After that is transmitted, $n = m + k$ encoded symbols, instead of m. The introduction of the additional k symbols reduces the data rate through the channel. To maintain the original velocity of the data transmission, the physical channel demands either more power or more bandwidth.

In 1981, Ungerboeck in [6] introduced a way to encode data against transmission errors, without increasing the consumption of bandwidth by using a technique called *set partitioning* map. This technique matches the output symbols of a classical binary convolutional encoder and the signal constellation from a phase shift keying—PSK—modulation. Mathematically, the output symbols of a binary convolutional encoder with the modulo-2 addition constitute an abelian group, whereas the PSK constellation constitutes a discrete set of points from a bidimensional vector space isomorphic with the plane $\mathbb{R}^2$. Towards to generalize, Ungerboeck's technique proposed the matching of a generic group Υ that could represent the output set of an encoder with a discrete set of points from an Euclidean space $\mathbb{R}^n$ that could represent the signal constellation from ASK (amplitude shift keying), FSK (frequency shift keying), or PSK modulation, [2, 7–9]. In this direction in [7] is introduced the *wide sense homomorphic encoder* which is a finite state machine (FSM) defined over *extension of groups*. The bi-infinite outputs of this encoder are the codewords and constitute the *group code*. But, one important result that motivates our work was given in [8] where it was shown that any AWGN channel using group codes over abelian groups has its capacity upper bounded by some uncoded AWGN channel capacity using PSK modulation. Thus, nonabelian and *well-behaved* group codes could surmount this PSK limit. In the sense of control theory, a group code is well behaved when it is *controllable* and *observable*. Classical group codes over binary groups always are well behaved, that is why there is not any concern about control consideration of these kind of codes. This well behavior also is true for some especial cases of abelian group codes. In the current paper, we deal with nonabelian group codes but we do not construct any new code. Instead of it, we study the class of group codes produced by an FSM encoder with a group S, representing the states of the FSM, inputs group $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, cyclic group of order prime p. Then, our group codes are defined over nonabelian extensions of $\mathbb{Z}_p$ by S. For that, this paper is organized as follows.

In Section 2 is defined the extension of a generic 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 and the encoder (output) mapping 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 Section 3, the group code $\mathcal{C}$ is presented as a dynamical system in the sense of [10]. 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 noncontrollability is made in Theorem 3.4. Also are presented the definition and conditions about parallel transitions that are used directly in our main result.

In Section 4, we present our original contributions about the noncontrollability of group codes produced by encoders defined on nonabelian extensions $\mathbb{Z}_p \boxtimes S$. The main result of this work, which is Theorem 4.7, states that (a) if $\mathbb{Z}_p \boxtimes S$ is nonabelian, with S abelian, then the resulting code will have parallel transitions and (b) if both $\mathbb{Z}_p \boxtimes S$ and S are nonabelian then the resulting code will be noncontrollable. Therefore, the extension $\mathbb{Z}_p \boxtimes S$ is bad for constructing group codes.

2. Group Extensions and Group Codes

2.1. Group Extensions

Definition 2.1. Given a group G with a normal subgroup N, consider the quotient group G/N. If there are two groups U and S such that U is isomorphic with N and S is isomorphic with G/N, then it is said that G is an *extension* of U by S [11].

We will denote the extension "U by S" by the symbol $U \boxtimes S$, also we will use the standard notations $U \cong N$ meaning "U is isomorphic with S" and $N \lhd G$ meaning "N normal subgroup of G." 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 semidirect product $U \rtimes S$ is a particular case of extension, but also it is known that the semidirect product is a generalization of the direct product $U \times S$. A canonical definition of extension of groups is given in [11, 12]; specially in [12] 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 $\upsilon : N \to U$, $\psi : S \to G/N$ and a lifting $l : G/N \to G$ such that $l(N) = e$, the neutral element of G. Then, defining $\phi : S \to \mathrm{Aut}(U)$ by

$$\phi(s)(u) = \upsilon\left[l(\psi(s)) \cdot \upsilon^{-1}(u) \cdot \left(l(\psi(s))\right)^{-1}\right], \tag{2.1}$$

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

$$\xi(s_1, s_2) = l(\psi(s_1, s_2)) l(\psi(s_1)) l(\psi(s_2)), \tag{2.2}$$

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

$$(u_1, s_1) * (u_2, s_2) = \left(u_1 \cdot \phi(s_1)(u_2) \cdot \xi(s_1, s_2), s_1 s_2\right) \tag{2.3}$$

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 (2.3), is $(u', s_1 s_2)$ for some $u' \in U$ and $s_1 s_2$ is the operation on S. This property allows 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 $(u', s_1 s_2 \cdots s_n)$ is the resulting pair of the multiple product $(u_1, s_1) * (u_2, s_2) * (u_3, s_3) * \cdots * (u_n, s_n)$, where u' is some element of U. Analogously, $(u, s)^n = (u', s^n)$ for some $u' \in U$.

Example 2.2. 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 of $(0, 0)$, 010 instead of $(0, 1, 0)$, and so forth, we have that the normal subgroup $N = \{000, 100\} \lhd \mathbb{Z}_2^3$ is isomorphic with $\mathbb{Z}_2$. The quotient group $\mathbb{Z}_2^3/N = \{\{000, 100\}, \{010, 110\}, \{001, 101\}, \{111, 011\}\}$ is isomorphic with $\mathbb{Z}_2^2$. Thus, in an expected way, we have shown that $\mathbb{Z}_2^3$ is an extension of $\mathbb{Z}_2 \boxtimes \mathbb{Z}_2^2$.

2.2. Finite State Machines and Group Codes

Finite state machines (FSM) are a subject of automata theory. Arbib in [13] 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, $\delta : I \times S \rightarrow S$ is the next-state mapping, and $\xi : I \times S \rightarrow O$ is the output mapping. Following [8, 9, 14] 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 2.3. Let U, S, and Y be finite groups. Let $\nu : U \boxtimes S \rightarrow S$ and $\omega : U \boxtimes S \rightarrow Y$ be group homomorphisms defined over an extension $U \boxtimes S$ such that the mapping $\Psi : U \boxtimes S \rightarrow S \times Y \times S$ defined by

$$\Psi(u, s) = (s, \omega(u, s), \nu(u, s)) \tag{2.4}$$

is injective with ν surjective.

Then, an encoder of a group code is the machine $M = (U, S, Y, \nu, \omega)$.

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:

$$\begin{array}{r|l} \nu(u_1, s_0) = s_1, & \omega(u_1, s_0) = y_1, \\ \nu(u_2, s_1) = s_2, & \omega(u_2, s_1) = y_2, \\ \nu(u_3, s_2) = s_3, & \omega(u_3, s_2) = y_3, \\ \vdots \qquad \vdots & \vdots \qquad \vdots \\ \nu(u_n, s_{n-1}) = s_n & \omega(u_n, s_{n-1}) = y_n. \end{array} \tag{2.5}$$

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, $\{s_i\}_{i=1}^n$, form 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} is one previous state from $s_{\{-i+1\}}$. Thus, for a given present state 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

$$\begin{array}{r|l} \nu(u_0, s_{-1}) = s_0, & \omega(u_0, s_{-1}) = y_0, \\ \nu(u_{-1}, s_{-2}) = s_{-1}, & \omega(u_{-1}, s_{-2}) = y_{-1}, \\ \nu(u_{-2}, s_{-3}) = s_{-2}, & \omega(u_{-2}, s_{-3}) = y_{-2}, \\ \vdots \quad\quad \vdots \;\; \vdots & \quad\quad\quad \vdots \\ \nu\big(u_{\{-n+1\}}, s_{-n}\big) = s_{\{-n+1\}} & \omega\big(u_{\{-n+1\}}, s_{-n}\big) = y_{\{-n+1\}}. \end{array} \tag{2.6}$$

Therefore, given bi-infinite sequence of inputs $\{u_i\}_{i\in\mathbb{Z}}$, $u_i \in U$, and one state $s_0 \in S$, 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 single sequences of inputs and the pair of sequences of outputs and states are 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 $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the natural numbers set.

Definition 2.4. 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* [7–9, 15].

Example 2.5. Consider the encoder $M = (\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_2^3, \nu, \omega)$ 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 $\omega(u, s_1, s_2) = (s_2, u, s_1)$.

Suppose that 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 $\{010, 011, 101, 101, 111, 110, 000, 010, 001, 110\}$.

3. Control and Group Codes

Each codeword of a group code satisfies the definition of a trajectory of a dynamical system in the sense of Polderman and Willems [10]. 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 $\mathcal{C}$ [8, 9, 16].

Given a codeword $\mathbf{y}$ and a set of consecutive indices $\{i, i+1, \ldots, j-1, j\} = [i, j]$, the projection of the codeword over these indices will be $\mathbf{y}|_{[i,j]} = \{y_i, y_{i+1}, \ldots, y_j\}$. Analogously, $\mathbf{y}|_{[i,j)} = \{y_i, y_{i+1}, \ldots, y_{j-1}\}$, $\mathbf{y}|_{[i,+\infty)} = \{y_i, y_{i+1}, \ldots\}$, 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

$$\begin{aligned} \mathbf{y_1} \wedge_j \mathbf{y_2}\big|_{(-\infty,j)} &= \mathbf{y_1}|_{(-\infty,j)}, \\ \mathbf{y_1} \wedge_j \mathbf{y_2}\big|_{[j,+\infty)} &= \mathbf{y_2}|_{[j,+\infty)}. \end{aligned} \tag{3.1}$$

Definition 3.1. If L is an integer greater than one, then a group code $\mathcal{C}$ is said L-controllable if, 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 $\mathcal{C}$ [7, 10, 15].

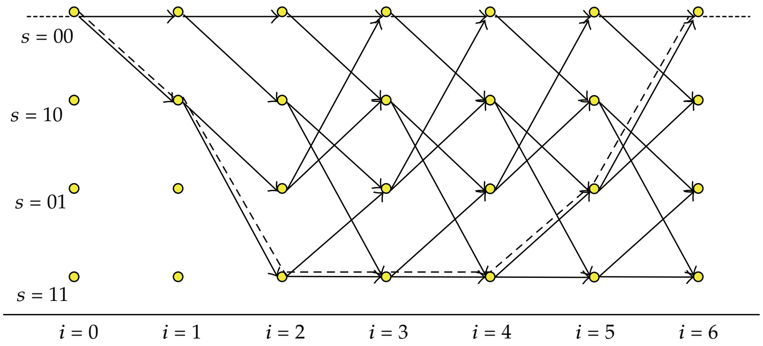


Figure 1: Trellis diagram of the encoder $M = (\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_2^3, \nu, \omega)$.

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, 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 it is said that it is controllable [10]. Clearly, a code $\mathcal{C}$ to be L-controllable is a sufficient condition for $\mathcal{C}$ to be controllable.

3.1. *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 (2.4), can be represented graphically. In the context of graph theory [17], they are called *edges* whose vertexes set is S and the graph is called *state diagram* labeled by $\omega(u,s)$. In Figure 1, the full state diagram of the code generated by the FSM $M = (\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_2^3, \nu, \omega)$, from Example 2.5, is shown between the times 2 and 3; also it is repeated between the times 3 and 4 and so on until times 4 and 5. 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, the relation between the codewords $\mathbf{y}$ and paths $\mathbf{b}$ is bijective. Again from Example 2.5, consider the inputs sequence $\{u_i\}_{i\in\mathbb{Z}}$, such that $u_1 = 1$, $u_2 = 1$, $u_3 = 0$, $u_4 = 0$, $u_5 = 1$, $u_6 = 1$, and $u_i = 0$ for all $i \in \mathbb{Z} - \{1,2,3,4,5,6\}$. The response path $\mathbf{b} = \{b_i\}_{i\in\mathbb{Z}}$ is such that $b_0 = (00, 010, 10)$, $b_1 = (10, 011, 11)$, $b_2 = (11, 101, 11)$, $b_3 = (11, 101, 11)$, $b_4 = (11, 111, 01)$, $b_5 = (01, 110, 00)$, and $b_i = (00, 000, 00)$ for all $i \in \mathbb{Z} - \{0,1,2,3,4,5\}$. This response path is shown by a traced line in Figure 1.

Definition 3.2. Two states s and r are said to be *connected* when there are a path $\mathbf{b}$ and indices $i, j \in \mathbb{Z}$ such that $\mathbf{b}|_{[i,j]} = \{b_i, b_{i+1}, \ldots, b_j\}$ 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 3.3. *Let $\mathcal{C}$ be a group code produced by the encoder $M = (U, S, Y, \nu, \omega)$. If there are two states $s \in S$ and $r \in S$ for which there is no a finite path of transitions connecting them, then $\mathcal{C}$ is* noncontrollable.

Proof. On 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 $\mathbf{y_3}|_{[k+L,+\infty)} = \mathbf{y_2}|_{[k+L,+\infty)}$ and $\mathbf{b_3}|_{(k,k+L]}$, a finite path, connecting s and r, a 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

$$r = \nu(u_n, \nu(u_{n1}, \ldots \nu(u_2, \nu(u_1, s)) \cdots)). \tag{3.2}$$

Theorem 3.4. *Given an encoder (U, S, Y, ν, ω), consider the family of state subsets $\{S_i\}$, recursively defined by*

$$\begin{aligned} S_0 &= \{e\}, \\ \vdots \; &\vdots \; \vdots \\ S_i &= \{\nu(u, s);\; u \in U, s \in S_{i-1}\}, \quad i \geq 0 \\ \vdots \; &= \; \vdots \end{aligned} \tag{3.3}$$

then

(1) *each S_i is a subgroup of S,*

(2) *S_{i-1} is normal in S_i, for all $i \in \{1, 2, \ldots\}$,*

(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, $sr = \nu(u_1, s_1) * \nu(u_2, s_2) = \nu(u_3, s_1 s_2)$, $u_3 \in U$ and thus $sr \in S_i$.

(2) Clearly, $S_0 \lhd S_1$. For $i > 1$, suppose that $S_{j-1} \lhd S_j$, for all $j \leq i$. Given $s \in S_{i+1}$ and $r \in S_i$, consider $s \cdot r \cdot s^{-1} = \nu(u, s_1) * \nu(v, r_1) * \nu(u, s_1)^{-1}$, where $s_1 \in S_i$, $r_1 \in S_{i-1}$, $u, v \in U$. Hence, $s \cdot r \cdot s^{-1} = \nu(u_1, r_1 \cdot s_1 \cdot r_1^{-1}) \in S_i$, because $r_1 \cdot s_1 \cdot r_1^{-1} \in S_{i-1}$.

(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, then 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 noncontrollable. □

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

Definition 3.5. 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 Hamming distance $d_H(\mathbf{y_1}, \mathbf{y_2})$ between two codewords $\mathbf{y_1} = \{y_i^1\}_{i\in\mathbb{Z}}$ and $\mathbf{y_2} = \{y_i^2\}_{i\in\mathbb{Z}}$ is defined as the number of components which are different. The minimal distance of a group code is

$$d_{\min} = \min\{d_H(\mathbf{y_1}, \mathbf{y_2});\ \mathbf{y_1}, \mathbf{y_2} \text{ are different codewords}\}. \tag{3.4}$$

One desirable property of a group code is a high $d_{\min}$; the greater $d_{\min}$, the better the capability to correction of errors. Clearly, when the trellis of a group code has parallel transitions, then $d_{\min} = 1$ and therefore a group code with parallel transitions will not be a good group code.

Lemma 3.6. *Consider an encoder (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 $H^- = \mathrm{Ker}(\nu) = \{(u,s);\ \nu(u,s) = e\}$, 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 nonabelian 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 (2.4).

(2) Immediate.

(3) There exists $(u,e) \in H^+ \cap H^-$, with $u \neq e$ such that $\nu(u,e) = e$. Since Ψ of (2.4) 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.

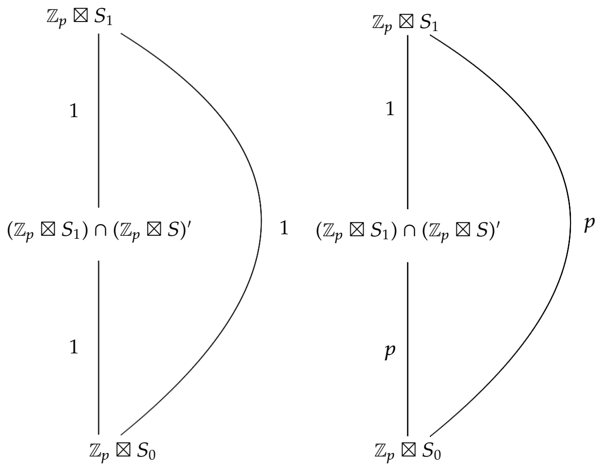
(4) The states group S being abelian implies that $G/H^+ \cong G/H^-$ are abelian factor groups. Then, the commutators subgroup $(U \boxtimes S)'$ is a subgroup of $H^+ \cap H^-$. But $U \boxtimes S$ is nonabelian, then $(U \boxtimes S)' \neq \{(e,e)\}$. Therefore, from the above item (2.3), $\{\Psi(u,s)\}_{(u,s)\in U\boxtimes S}$ has parallel transitions. □

4. Nonabelian Group Codes with $\mathbb{Z}_p$ as information Group Are Not Good

By using group extension of groups, subgroup of commutators, Theorem 3.4, and other group theory ideas, we show here that we must search for good nonabelian group codes outside the extension $\mathbb{Z}_p \boxtimes S$.

Definition 4.1. Given a finite group G and a subgroup $H \subset G$, the index of H in G, denoted by $[G : H]$, is the number of different cosets of H in G.

If $|G|, |H|$ denote the orders of G and H, respectively, then $[G : H] = |G|/|H|$. It is possible to represent graphically this index such as in Figure 2 where is represented the index $[\mathbb{Z}_p \boxtimes S_1\colon \mathbb{Z}_p \boxtimes S_0]$. We see that if $S_1 = S_0$, then $[\mathbb{Z}_p \boxtimes S_1\colon \mathbb{Z}_p \boxtimes S_0] = 1$, and if $S_1 \neq S_0$ then $[\mathbb{Z}_p \boxtimes S_1\colon \mathbb{Z}_p \boxtimes S_0] = p$.


$\mathbb{Z}_p \boxtimes S_1$
1
$(\mathbb{Z}_p \boxtimes S_1) \cap (\mathbb{Z}_p \boxtimes S)'$
1
1
$\mathbb{Z}_p \boxtimes S_0$
$\mathbb{Z}_p \boxtimes S_1$
1
$(\mathbb{Z}_p \boxtimes S_1) \cap (\mathbb{Z}_p \boxtimes S)'$
p
p
$\mathbb{Z}_p \boxtimes S_0$

(a) If $S_1 = S_0$

(b) If $S_1 \neq S_0$

Figure 2: The intersection $(\mathbb{Z}_p \boxtimes S_1) \cap (\mathbb{Z}_p \boxtimes S)'$ when $\mathbb{Z}_p \boxtimes S_0 \subset (\mathbb{Z}_p \boxtimes S)'$.

Definition 4.2. Given a group G, the group of commutators of G is the subgroup $G' = \{aba^{-1}b^{-1};\ a, b \in G\}$.

Lemma 4.3. *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 $S_1 = S_0$, then the lemma holds trivially (Figure 2(a)). If $S_1 \neq S_0$, then by the long commutators theorem from [18], there are $s \in (S_1 - S_0)$ and $a_1, a_2, \ldots, a_t \in S$ such that $s = a_1 a_2 \cdots a_t a_1^{-1} a_2^{-1} \cdots a_t^{-1}$. Now, consider $u \in \mathbb{Z}_p$ and $\{u_1, u_2, \ldots, u_t\} \subset \mathbb{Z}_p$ such that $(u, s) = (u_1, a_1) * (u_2, a_2) * \cdots * (u_t, a_t) * (u_1, a_1)^{-1} * (u_2, a_2)^{-1} * \cdots * (u_t, a_t)^{-1}$. 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 2(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 $i \geq 1$. □

Lemma 4.4. *Let $\mathbb{Z}_p \boxtimes S$ be an extension which is a p-group. Consider the subgroups $\{S_i\}$ defined in* (3.3)*. 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 at most order p^2, we have that 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} nonabelian. 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,

$$\begin{gathered}
s_1 s_2 \neq s_2 s_1, \\
\nu(u_1, r_1) * \nu(u_2, r_2) \neq \nu(u_2, r_2) * \nu(u_1, r_1), \\
\nu\Big((u_1, r_1) * (u_2, r_2) * (u_1, r_1)^{-1} * (u_2, r_2)^{-1}\Big) \neq e,
\end{gathered}$$

$$\begin{gathered}\nu\left(u', r_1r_2r_1^{-1}r_2^{-1}\right) \neq e, \text{ for some } u' \in \mathbb{Z}_p, \\ \nu(u', e) \neq e.\end{gathered} \tag{4.1}$$

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 Lemma 4.3, $(\mathbb{Z}_p \boxtimes S_i) \subset (\mathbb{Z}_p \boxtimes S)'$ and $S_i \subset S'$, for each i. Therefore, either S_i is abelian or $S_i \subset S'$. □

Suppose now that we do not have the information about the order of $\mathbb{Z}_p \boxtimes S$; that is, we cannot use the hypothesis that $\mathbb{Z}_p \boxtimes S$ is 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 (3.3), we will show that when $U = \mathbb{Z}_p$, each S_i must be a p-group. In that direction, we need to consider the subgroup H^- of Lemma 3.6 and from this the second projection of the kernel of ν:

$$S_d = \left\{s \in S;\ \nu(u, s) = e \text{ for some } u \in \mathbb{Z}_p\right\}. \tag{4.2}$$

Clearly, S_d is a normal subgroup of S and it is isomorphic to $\mathbb{Z}_p$ and we have the following lemma.

Lemma 4.5. *Consider the encoder $M = (\mathbb{Z}_p, S, Y, \nu, \omega)$. Also, consider the subgroup S_d defined in* (4.2)*, then*

(1) *if there are $s \neq e$ 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 4.6. *Consider the encoder $M = (\mathbb{Z}_p, S, Y, \nu, \omega)$, where p is prime. Then, each S_i of* (3.3) *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 has order p^i, $i \leq k$. If $p > [S_{k+1} : S_k] > 1$, then $[S_{k+1} : S_k] = m = q_1^{r_1} q_2^{r_2} \cdots q_t^{r_t}$, 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, $r^{q_1} \in S_d \cap S_k$.

If $r \neq e$, then $r^{q_1} \neq e$, because $q_1 < p$. By Lemma 4.5, $S_d \subset S_k$ 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. □

Theorem 4.7. *Consider the encoder $M = (\mathbb{Z}_p, S, Y, \nu, \omega)$, where $\mathbb{Z}_p \boxtimes S$ is nonabelian and p is a positive prime, then*

(1) *if S is abelian, then the group code has bad minimal Hamming distance;*

(2) *if S is nonabelian, then the group code is noncontrollable.*

Proof. (1) By Lemma 3.6, the group code has parallel transitions and by (3.4) has $d_{\min} = 1$.

(2) If S is not a p-group, then by Theorem 4.6 the resulting code is noncontrollable. If S is a p-group, then $\mathbb{Z}_p \boxtimes S$ is also a p-group, then by Lemma 4.4 S is abelian, a contradiction. □

5. Conclusion

We have shown that there are no controllable group codes defined on the nonabelian extension $\mathbb{Z}_p \boxtimes S$, with p prime and for any finite nonabelian group S. When S is abelian, the group code will have parallel transitions and therefore distance limitations. In contrast, for the cases $\mathbb{Z}_{2^2} \boxtimes S$ and $(\mathbb{Z}_2)^2 \boxtimes S$, there are important examples of controllable and nonabelian group codes such as the Wei code [19] which has a trellis section isomorphic to the nonabelian 2-group $(\mathbb{Z}_2)^2 \rtimes D_8$, where D_8 is the symmetries of the square and the symbol $\rtimes$ denotes the semidirect product. This provides a strong clue about the controllability of some p-groups with information groups $\mathbb{Z}_{p^n}$ or $(\mathbb{Z}_p)^n$.

References

[1] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, Wiley-InterScience, Hoboken, NJ, USA, 1st edition, 2005.

[2] C. Schlegel and L. Perez, *Trellis and Turbo Coding*, Wiley-InterScience, Piscataway, NJ, USA, 2004.

[3] D. J. C. MacKay, *Information Theory, Inference and Learning Algorithms*, Cambridge University Press, London, UK, 2005.

[4] S. Haykin, *Comunication Systems*, John Wiley & Sons, New York, NY, USA, 4th edition, 2001.

[5] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 28, pp. 379–423, 1948.

[6] G. Ungerboeck, "Channel coding with multilevel-phase signals," *IEEE Transactions on Information Theory*, vol. 28, no. 1, pp. 55–67, 1982.

[7] H. A. Loeliger and T. Mittelholzer, "Convolutional codes over groups," *IEEE Transactions on Information Theory*, vol. 42, no. 6, part 1, pp. 1660–1686, 1996.

[8] H. A. Loeliger, "Signal sets matched to groups," *IEEE Transactions on Information Theory*, vol. 37, no. 6, pp. 1675–1682, 1991.

[9] D. G. Forney, and M. D. Trott, "The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders," *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1491–1513, 1993.

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

[11] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, New York, NY, USA, 4th edition, 1995.

[12] M. Hall, *The Theory of Groups*, Macmillan, New York, NY, USA, 1959.

[13] M. A. Arbib, *Brains, Machines, and Mathematics*, Springer-Verlag, New York, NY, USA, 2nd edition, 1987.

[14] 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*, SBrT, Rio de Janeiro, Brazil, 2003.

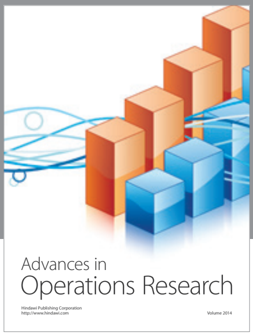
[15] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge University Press, Cambridge, UK, 1995.

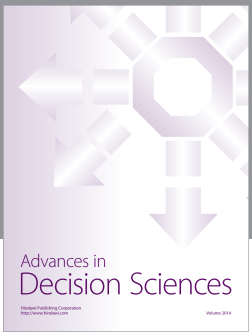
[16] F. Fagnani and S. Zampieri, "Minimal syndrome formers for group codes," *IEEE Transactions on Information Theory*, vol. 45, no. 1, pp. 3–31, 1999.

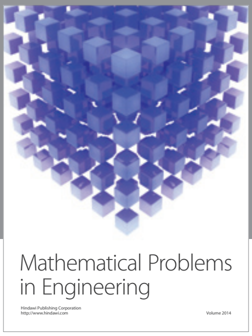
[17] R. Diestel, *Graph Theory*, Springer-Verlag, New York, NY, USA, 3rd edition, 2005.

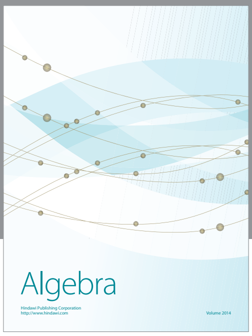
[18] P. Yff, "On k-conjugacy in a group," *Proceedings of the Edinburgh Mathematical Society*, vol. 14, pp. 1–4, 1964.

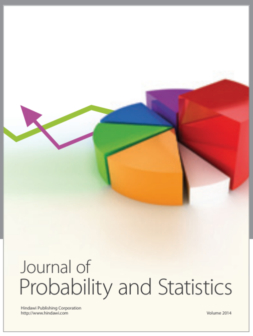
[19] L. F. Wei, "Rotationally invariant convolutional channel coding with expanded signal space—part II: nonlinear codes," *IEEE Journal on Selected Areas in Communications*, vol. 2, no. 5, pp. 672–686, 1984.


Advances in
Operations Research

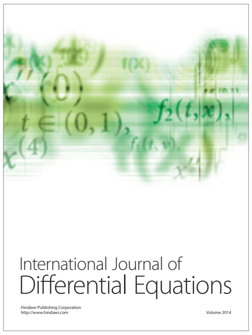

Advances in
Decision Sciences

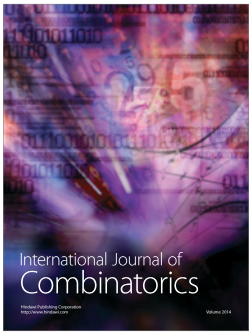

Mathematical Problems
in Engineering

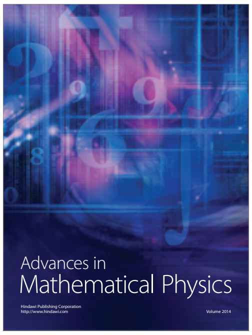

Algebra

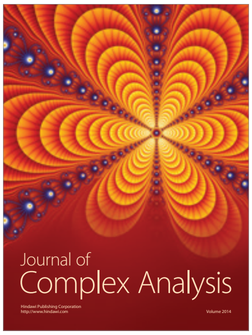

Journal of
Probability and Statistics

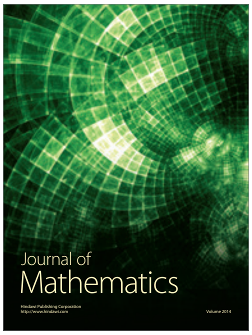
The Scientific
World Journal

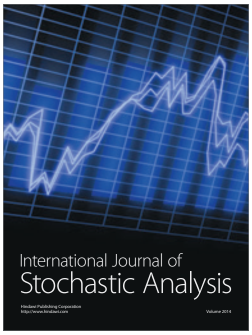

International Journal of
Differential Equations

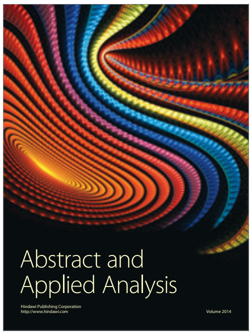

International Journal of
Combinatorics

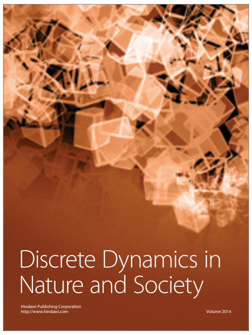

Advances in
Mathematical Physics

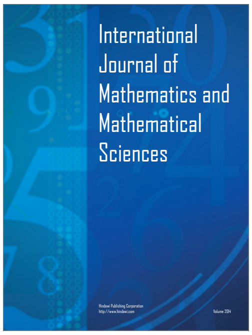

Journal of
Complex Analysis


Journal of
Mathematics


International Journal of
Stochastic Analysis

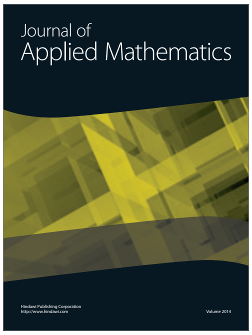

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


Journal of
Applied Mathematics

Journal of
Optimization