PRO MATHEMATICA: *Vol. X, Nos. 19-20, 1996*

ALGEBRAIC STRUCTURE OF CONVOLUTIONAL ENCODERS

Jorge ***Pedraza-Arpasi***

Abstract

Traditionally the convolutional encoders were regarded as machines from automata theory without any algebraic structure. In this work we give a group structure on such encoders and get some elemental results.

Introduction. In direction to give an algebraic fundamentals of convolutional encoders, in a first step we observe that all known convolutional encoders, found in the respective literature, are over algebraic fields, i.e. its input alphabet, output alphabet, and state space are in a cartesian product of a field. After some manipulations we can see that this encoder uses only the first operation of the field, namely, the "sum". Because this fact, our convolutional encoders will be over groups.

We define the *encoders* as *machines* in the sense of [6]. So, when we say the terms *encoder* or *machine*; we will be talking about the same thing. In the first section we take the inputs, outputs, and the states of the machine, strictly, over an abelian group, and we name this machine as Elementary Convolutional Encoder (ECE). The whole class of know encoders it is included in this family of ECEs. We point out ECE's properties that will be a guide for the definition of generalized machines.
Like a collateral result, we give a technique to obtain a new machines from a given "old" machine. The characteristics of the new machine is that it have less states, the same inputs, and outputs than the old. We think by using the Axiom of the States, in the sense of [5]; this could be a practical way to find minimal encoders. A practical example is given.

In the second section, in order to define convolutional encoder machines over any group, abelian or not, we define the Schreier Product of groups. By using this product we define a General Convolutional Encoder (GCE). Of course, as is expected a ECE is a particular case of a GCE. Moreover, this class of GCEs is so wide that some restrictions are necessaries. For instance, we introduce the controllability restriction. So, only, will it be considered controlable machines. Finally we give criterions to build non-trivial convolutional encoders and some examples.

1 Elementary Convolutional Encoder (ECE) and Reduction of States

Given $k,n \in N$, consider a matrix $T = (t_{ij})$; $1 \leq i \leq k$; $1 \leq j \leq n$; $t_{ij} \in Z$ = Integers Set.

Let G be an abelian group. For any $n \in N$, consider G^n the cartesian product of G. With the G-operation over the coordinates; G^n is, also abelian group.

Given $x \in G^k$ and T as above, consider the product

$$x.T = \left(\sum_{i=1}^{k} x_i t_{i1}, \sum_{i=1}^{k} x_i t_{i2}, \ldots, \sum_{i=1}^{k} x_i t_{in}\right);$$

where

$$
x_i\, t_{ij} = \begin{cases} \overbrace{x_i * x_i \dots * x_i}^{t_{ij}\text{ - times}} & \text{if } t_{ij} > 0 \\ e_G & \text{if } t_{ij} = 0 \\ \underbrace{(x_i * x_i \dots * x_i)^{-1}}_{\mid t_{ij} \mid \text{ - times}} & \text{if } t_{ij} < 0 \end{cases}
$$

Because the abelian condition of G and G^n we can to write the plus simbol (+) instead the star (*), and to denote 0 instead e_G . So, we are ready for ECE's definition.

Def 1 *Let n,k,m be natural numbers such that $n>k\geq 1$; $m\geq 1$. Consider the matrices $T^0, T^1, \dots, T^m$; with $T^i = (t^i_{rs})$; $t^i_{rs} \in Z$; $1\leq r\leq k$; $1\leq s\leq n$; $i=0,1\dots,m$.*

We define an Elementary Convolutional Encoder (ECE); with parameters n,k,m; over G; as a machine $M = (X,Y,Q,\delta,\beta)$; where:

$X \subset G^k$; is the, finite, set of imput alphabets,

$Y \subset G^n$; is the set of output alphabets,

$Q = \{q = (x^1, x^2,\dots,x^m) \,/\, x^i \in X\} \subset (G^k)^m \approx G^{km}$;
is the set (or space) of the machine states,

δ: $X \times Q \to Q$; is defined by,
$\delta(x^0,q) = \delta(x^0,x^1,x^2,\dots,x^m) = (x^0,x^1,x^2,\dots,x^{m-1})$

β: $X \times Q \to Y$ is a surjective map, defined by
$\beta(x^0,q) = \beta(x^0,x^1,x^2,\dots,x^m) = x^0\,T^0 + x^1\,T^1 + x^2\,T^2 + \dots + x^m\,T^m$.

1.1 Some Properties of the ECE

pp 1 *If X group, then Y and Q are groups.*

pp 2 *If X is group, then δ and β are homomorphisms of groups, with δ being suryective.*

pp 3 *Assume that X is a group. Let* $Y_0 = \{\beta(x,e_Q)\}_{x\in X}$ *be the outputs "from" the neutral state* e_Q.

Then, we have Y_0 *is a normal subgroup of Y and* $\frac{Y}{Y_0} \approx Q$

pp 4 *Assume X is a group. Let* $Y_1 = \{\beta(x,q)\ /\ \delta(x,q) = e_Q\}$ *be the outputs "to" neutral state.*

Then, we have Y_1 *is a normal subgroup of Y and* $\frac{Y}{Y_1} \approx Q$.

Proof 1

Given $y = \sum_{i=0}^{m} x^i\ T^i \in Y$ and $y' = \sum_{i=0}^{m} x'^i\ T^i \in Y$, we have $y+y' = \sum_{i=0}^{m} (x^i + x'^i)\ T^i \in Y$; because X is a group.

Analogously, given $q = (x^1, x^2, \dots, x^m)$ and $q' = (x'^1, x'^2, \dots, x'^m)$, we have $q+q' = (x^1 + x'^1, x^2 + x'^2, \dots, x^m + x'^m) \in Q$, because X is a group

Proof 2

Now X and Q are groups, hence $X \times Q$ is a group. Thus δ is a map between two groups. Let (x,q) and (x',q') be two elements of $X \times Q$, with $q = (x^1, x^2, \dots, x^m)$ and $q' = (x'^1, x'^2, \dots, x'^m)$; then

$$\begin{aligned}\delta((x,q) + (x',q')) &= \delta(x + x',\ q + q') = (x + x', x^1 + x'^1 + x'^{m-1}) \\ &= (x, x^1, \dots, x^{m-1}) + (x', x'^1, \dots, x'^{m-1}) = \delta(x,q) + \delta(x',q');\end{aligned}$$

therefore, δ is a homomorphism of groups.

By other side, given $q = (x^1, x^2, \dots, x^m) \in Q$, take the state $q_0 = (x^2, x^3, \dots, x^{m+1}) \in Q$ and $x^1 \in X$; then $\delta(x^1, q_0) = q$. So, δ is suryective.

Analogously is straightforward to show that β is a homomorphism.

Proof 3

Define the map $\psi: Y \to Q$, puting

$$\psi(\beta(x,q)) = q.$$

Then,

$$\psi(\beta(x,q) + \beta(x',q')) = \psi(\beta(x+x', q+q')) = q+q' = \psi(\beta(x,q)) + \psi(\beta(x',q')).$$

Thus ψ is a suryective homomorphism.
$Ker\,(\psi) = \{\beta(x,q)) \,/\, q = \psi(\beta(x,q)) = 0\} = Y_0$.
By the fundamental theorem of the homomorphisms:

$$\frac{Y}{Y_0} \approx Q$$

Proof 4

In analogous way to **Proof 3,** by defining the map $\psi\colon Y \to Q$ as $\psi(\beta(x,q)) = \delta(x,q)$

1.2 Reduction of States

pp 5 *Let $Q' \subset Q$ be a normal subgroup of Q. We write*

$$Y' = \{\beta\,(x,q) \in Y \,/\, q \in Q' \text{ and } \delta(x,q) \in Q'\};$$

then Y' is normal subgroup of Y.

Proof

Define the map $f\colon Y \to \frac{Q}{Q'} \times \frac{Q}{Q'}$ as being:

$$\psi\,(\beta\,(x,q)) = (q+Q'), \delta(x,q) + Q')$$

then

$$\begin{aligned}\psi(\beta(x,q) + \beta(x',q)) &= \psi(\beta(x+x', q+q')) \\ &= ((q+q') + Q', \delta(x+x', q+q') + Q) \\ &= (q+Q'), \delta(x,q) + Q') + (q'+ Q'), \delta(x',q') + Q') \\ &= \psi(\beta(x,q)) + \psi(\beta(x',q'))\end{aligned}$$

$Ker(\psi) = \{\beta(x,q) \,/\, \psi(\beta(x,q)) = (Q',Q')\} = \{\beta(x,q) \in Y \,/\, q \in Q';\ \delta(x,q) \in Q'\}$ $= Y'$. Thus Y' is normal in Y.

Note that, the above map ψ can be not suryective.

Def 2 *Given a machine* $M = (X,Y,Q,\delta,\beta)$; *let* $Y' \subset Y$ *and* $Q' \subset Q$ *be like above; such that;* $\delta(0,q) \in Q'$, $\forall q \in Q'$.
Then, we define a new machine $M' = (X, \frac{Y}{Y'}, \frac{Q}{Q'}, \delta', \beta')$, *where:*

$$\delta' : X \times \frac{Q}{Q'} \to \frac{Q}{Q'} \quad \textit{is given by}$$

$$\delta'((x,q) + Q') = \delta(x,q) + Q'$$

$$\beta' : X \times \frac{Q}{Q'} \to \frac{Y}{Y'} \quad \textit{is given by}$$

$$\beta'((x,q) + Y') = \beta(x,q) + Y' \quad \textit{(parallel transition class)}$$

The maps δ' and β', are well defined; i.e.; they are independent of the representant of the class $q+Q'$. Thus the new machine M' is a well defined ECE. Therefore it have the properties 1.1. So, δ' an β' are suryective homomorphisms; the sets

$Y_{Q'0} = \{\beta'(x,Q');\ x \in X\}$;
$Y_{Q'1} = \{\beta'(x,q+Q');\ (x,q+Q') \in X \times \frac{Q}{Q'}$ and $\delta'(x,q+Q') = Q'\}$;

are normal subgroups of $\frac{Y}{Y'}$ and

$$\frac{\frac{Y}{Y'}}{Y_{Q'0}} \approx \frac{\frac{Y}{Y'}}{Y_{Q'1}} \approx \frac{Q}{Q'}\ .$$

1.3 A family of Reduced Machines

Given a Machine $M = (X,Y,Q,\delta,\beta)$ with T^0 as the **Def 1**, we consider the family of subsets of Q defined by

$$Q^i = \{q = (x^1,x^2,\dots,x^m)\in Q \text{ such that } x^1,x^2,\dots,x^i \in Ker(T^0)\};$$
$i=1,2,\dots,m$

pp 6 *Q^i is a normal subgroup of Q*; $\forall i=1,\dots,m$

Proof

Given $q\in Q^i$, we write $q = (x,y)$, with $x = (x^1,x^2,\dots,x^i)$ and $y = (x^{i+1},\dots,x^m)$. Also, we write

$$x*T^0 = x^1\, T^0 + x^2\, T^0 + \dots + x^i\, T^0\,;$$

we have, always, $x*T^0 = 0$.
Let (x,q) and (x',q') be elements of Q^i. Then

$$(x,q) + (x',y') = (x+x',\, y+y'),$$

and $(x+x')*T^0 = 0$. This jointly to the abelian condition of Q shows the normality of Q^i.

A characteristic of the family $\{Q^i\}^m_{i=1}$, is that

$$Q^m \subseteq Q^{m-1} \subseteq \dots \subseteq Q^1 \subseteq Q.$$

Hence, we will have

$$|Q| \geq |.\frac{Q}{Q^m}.| \geq \dots \geq |.\frac{Q}{Q^1}.|\,.$$

Now, let Y^i be a subset of Y defined by

$$Y^i = \{\beta(x,q)\in Y\,/\, q\in Q^i \text{ and } \delta(x,q)\in Q^i\};$$

by **pp 5**, Y^i is normal in Y; $\forall i = 1,2,\dots,m$

pp 7 $\forall q\in Q^i$, *we have*, $\delta(0,q)\in Q^i$

Proof

Let $q = (x^1,x^2,\ldots,x^i,x^{i+1},\ldots,x^m)$ be a element of Q^i

We have

$$\delta(0,q) = \delta(0,(x^1,x^2,\ldots,x^i,x^{i+1},\ldots,x^m))$$
$$= (0,x^1,x^2,\ldots,x^{i-1},x^i,x^{i+1},\ldots,x^{m-1})$$

Making $x' = (0,x^1,x^2,\ldots,x^{i-1})$ we have $x'*T^0 = 0$.

Therefore $\delta(0,q)\in Q^i$

In this way, we can define a family $\{M^i\}_{i=1}^{m}$, of machines, putting for each machine:

$$M^i = (X,\frac{Y}{Y^i},\frac{Q}{Q^i}, \delta_i , \beta_i);$$

with

$$\delta_i\ (x,q+Q^i) = \delta(x,q)+Q^i$$
$$\beta_i\ (x,q+Q^i) = \beta(x,q)+Y^i$$

1.4 Example

Given $G = Z_2$, $n = 3$, $k = 2$, $m = 2$; $T^0 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ $T^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ $T^2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$; we have:

$$X = Z_2^2 = \{00, 01, 10, 11\}$$

$$Q = X^2 = Z_2^4 = \begin{Bmatrix} 0000 & 0100 & 1000 & 1100 & 0001 & 0101 & 1001 \\ 0010 & 0110 & 1010 & 1110 & 0011 & 0111 & 1111 \end{Bmatrix}$$

$$Y = Z_2^3 = \{000, 001, 010, 100, 011, 110, 101, 111\}$$

$$\delta(x^0,q) = \delta(x^0, (x^1, x^2)) = (x^0,x^1), x^i\in Z_2^2$$

$$\beta(x^0,q) = \beta(x^0, (x^1, x^2)) = x^0T^0 + x^1\ T^1 + x^2T^2.$$

The trellis representation of M, is showed in the Figure 1.

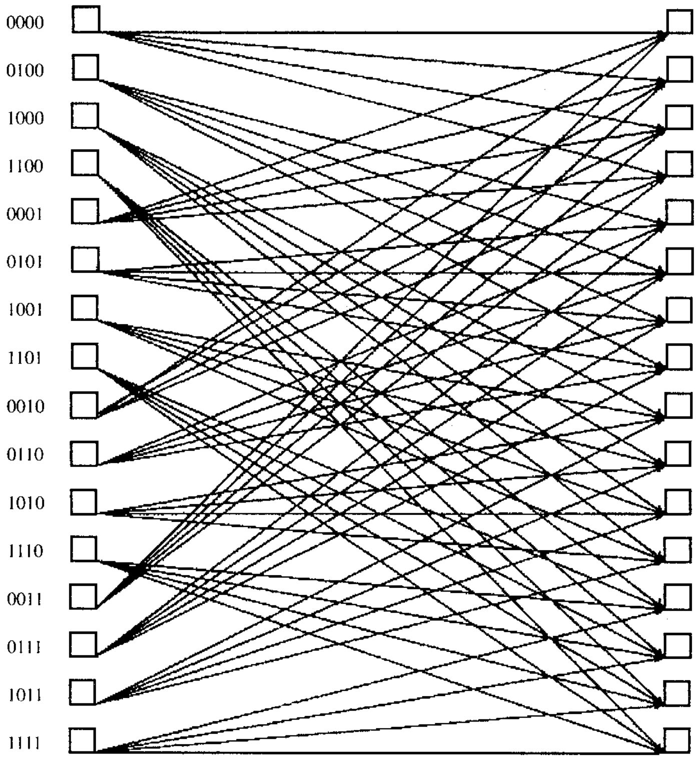


Figure 1: *Trellis diagram for the machine M*

1.4.1 Reduced Machine M^2

$$Q^2 = \{0000, 0011, 1100, 1111\} \overset{classes}{\Rightarrow} \begin{cases} 1000 + Q^2 = \{1000, 1011, 0100, 0111\} \\ 1001 + Q^2 = \{1001, 1010, 0101, 0110\} \\ 1101 + Q^2 = \{1101, 1110, 0001, 0010\} \end{cases}$$

$$Y^2 = \{000, 110\} \overset{classes}{\Rightarrow} \begin{cases} 100 + Y^2 = \{100, 010\} \\ 001 + Y^2 = \{001, 111\} \\ 011 + Y^2 = \{011, 101\} \end{cases}$$

$$\frac{Q}{Q^2} = \{Q^2, 1000 + Q^2, 0001 + Q^2\}$$

$$\frac{Y}{Y^2} = \{Y^2, 100 + Y^2, 001 + Y^2, 011 + Y^2\}$$

$$\delta_2(x, Q^2) = \begin{cases} Q^2, & \text{if } x \in \{00,11\} \\ 1000 + Q^2, & \text{if } x \in \{00,11\} \end{cases}$$

$$\delta_2(x, 1000+Q^2) = \begin{cases} 1001 + Q^2, & \text{if } x \in \{00,11\} \\ 1000 + Q^2, & \text{if } x \in \{01,10\} \end{cases}$$

$$\delta_2(x, 1001+Q^2) = \begin{cases} 1101 + Q^2, & \text{if } x \in \{00,11\} \\ 1001 + Q^2, & \text{if } x \in \{01,10\} \end{cases}$$

$$\delta_2(x, 1011+Q^2) = \begin{cases} Q^2, & \text{if } x \in \{00,11\} \\ 1000 + Q^2, & \text{if } x \in \{01,10\} \end{cases}$$

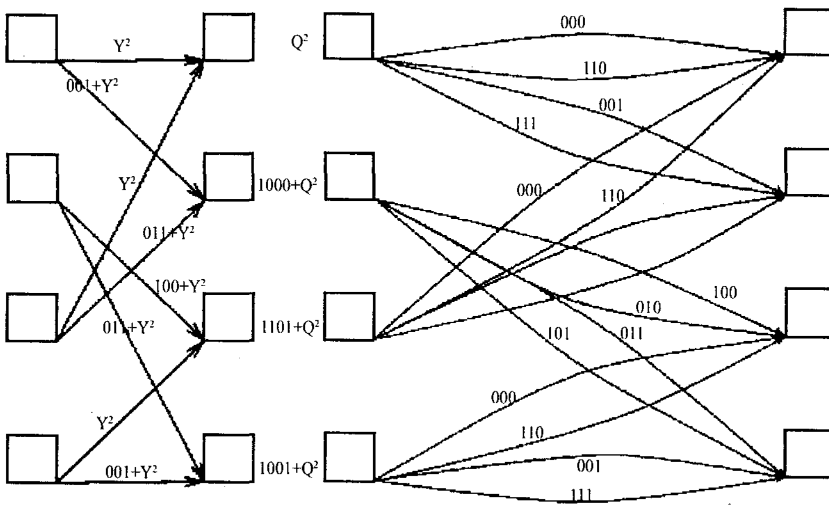
$$\beta_2(x, Q^2) = \begin{cases} Y^2, & \text{if } x \in \{00,11\} \\ 011 + Y^2, & \text{if } x \in \{01,10\} \end{cases}$$

$$\beta_2(x, 1000+Q^2) = \begin{cases} 100 + Y^2, & \text{if } x \in \{00,11\} \\ 011 + Y^2, & \text{if } x \in \{01,10\} \end{cases}$$

$$\beta_2(x, 1001+Q^2) = \begin{cases} Y^2, & \text{if } x \in \{00,11\} \\ 001 + Y^2, & \text{if } x \in \{01,10\} \end{cases}$$

$$\beta_2(x, 1101+Q^2) = \begin{cases} Y^2, & \text{if } x \in \{00,11\} \\ 011 + Y^2, & \text{if } x \in \{01,10\}. \end{cases}$$

The Trellis representation of M^2 is given in the Figure 2.



a: Classes Outputs **b: Classes Contain Outputs**

***Figure 2:** Trellis diagram for the machine M^2*

1.4.2 The Reduced Machine M^1

Q^1 = {0000, 0011, 1100, 1111, 0001, 0010, 1101, 1110}

$1000+Q^1$ = {1000, 1010, 1001, 1011, 0100, 0101, 0110, 0111} (the other class)

Y^1 = {000, 100, 010, 110}

$001 + Y^1$ = {001, 101, 011, 111} (the other class)

$\frac{Q}{Q^1}$ = {Q^1, $1001 + Q^1$ }

$\frac{Y}{Q^1}$ = {Y^1, $001 + Y^2$}

$$\delta_1(x, Q^1) = \begin{cases} Q^1, & \text{if } x \in \{00,11\} \\ 1000+Q^1, & \text{if } x \in \{01,10\} \end{cases}$$

$$\delta_2(x, 1000+Q^1) = \begin{cases} Q^1, & \text{if } x \in \{00,11\} \\ 1000+Q^1, & \text{if } x \in \{01,10\} \end{cases}$$

$$\beta_1(x, Q^1) = \begin{cases} Y^1, & \text{if } x \in \{00,11\} \\ 001+Y^1, & \text{if } x \in \{01,10\} \end{cases}$$

$$\beta_2(x, 1000+Q^1) = \begin{cases} Y^1, & \text{if } x \in \{00,11\} \\ 001+Y^1, & \text{if } x \in \{01,10\} \end{cases}$$

The trellis representation of M^1 is showed in the Figure 3.

2 General Convolutional Encoder (GCE)

2.1 Schreier Product

Def 3 *Let H and K be, two finite groups. Let* $\sigma: K \to Aut(H)$ *and* $\mu: K{\times}K \to H$ *be; mappings such that* $\forall k_1, k_2, k_3 \in K$ *y* $\forall h \in H$, *satisfying the following two conditions:*

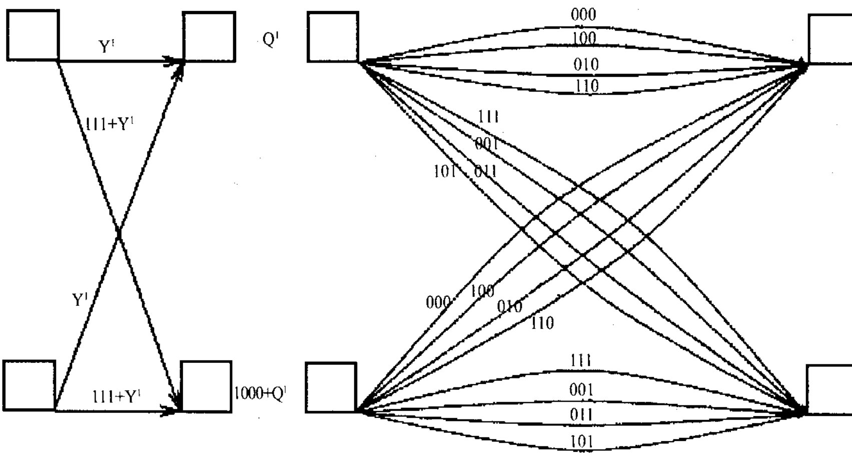
$$\sigma(k_1)(\mu(k_2,k_3)) \,.\, \mu(k_1,k_2,k_3) = (\mu(k_1,k_2)) \,.\, \mu(k_1,k_2,k_3) \qquad (1)$$

$$\sigma(k_1)(\sigma(k_2,h)) = \mu(k_1,k_2) \,.\, \sigma(k_1,k_2)(h) \,.\, \mu(k_1,k_2)^{-1} \qquad (2)$$

We define the SCHREIER PRODUCT $H_\alpha K$, of H and K as the ordered pair group (h,k), *having the operation:*

$$(h,k)*(h',k') = (h.\sigma(k)(h').\mu(k,k'), kk').$$

So, the Schreier Product depends of the mappings σ and μ .



a: Classes Outputs **b: Classes Contain Outputs**

Figure 3: *Trellis diagram for the machine* M^{t}

2.1.1 Some Properties

pp 8 *When* $\mu(k_1,k_2) = id$, $\forall k_1, k_2 \in K$; *and* σ *is a group homomorphism, we have the particular case of Semidirect Product.*
When $\mu(k_1,k_2) = id$, $\forall k_1, k_2 \in K$; *and* $\sigma(k) = \mathrm{id}$, $\forall k \in K$, *we have the particular case of Direct Product.*

pp 9 *The neutral element of this, new, group is* $(\mu(e_K, e_K)^{-1}, e_K)$. *And the inverse element of any* (x,q) *is*

$$(x,q)^{-1} = (\sigma(q)^{-1} [\mu(q, q^{-1}) \,.\, \mu(e_k, e_k) \,.\, x]^{-1} , q^{-1})$$

pp 10 *If* $H \propto K$ is a semidirect product, with $\sigma \neq id$, *then is not abelian.*

pp 11 *The mapping* $\varphi: H \rightarrow H \propto K$ *given by* $\varphi(h) = (\mu(e_K, e_K)^{-1} h, e_K)$ *and the proyection* $\pi_2 : H \propto K$ *given by* $\pi_2 (h,k) = k$ *are group homomorphisms.*

Conversily; if $H \times K$ *is a group such that the mappings* φ *y* π_2, *as above, are homomorphisms, then* $H \times K$ *is a Schreier Product.*

Because the **pp 8** is almost evident, and the **pp 9** and **pp 10** are indicate in [4], and the **pp 11** is implicitly showed in [2]; we omit the proof of these properties.

2.2 General Encoder Machine

Def 4 *Let X, Q and Y be groups, with X and Q finites. Let* $X_\alpha Q$ *be, a Schreier Product. Let* δ*:* $X_\alpha Q \to Q$ *and* β*:* $X_\alpha Q \to Y$ *be group homomorphisms, with* δ *suryective.*
We define the General Convolution Encoder (GCE) as a machine $M = (X,Y,Q,X_\alpha Q,\delta,\beta)$ *such that the map* $\Psi: X_\alpha Q \to Q\times Y\times Q$*, given by* $\Psi(x,q) = (q,\beta(x,q), \delta(x,q))$ *is inyective.*

2.2.1 Some Properties

pp 12 *The ECE is particular case of GCE*

pp 13 *Let* $T = Im(\Psi) = \Psi(X_\alpha Q) \subset Q\times Y\times Q$*. Then T is a group and* $X_\alpha Q \approx T$*; moreover*

$$T_0 = \{(e_Q, \beta(x,e_Q), \delta(x,e_Q))\in T \,/\, x\in X\},$$

and

$$T_1 = \{(q,\beta(x,q), \delta(x,q))\in T \,/\, (x,q)\in X\alpha Q,\ \delta(x,q) = e_Q\},$$

are normal subgroups of T and $\frac{T}{T_0} \approx \frac{T}{T_1} \approx Q$.

pp 14 *Given* $q\in Q$*, let*

$$T_{q0} = \{(q,\beta(x,q), \delta(x,q)) \,/\, x\in X\}$$

be the transitions "from" the q state; and let

$$T_{q1} = \{(q',\beta(x,q'), \delta(x,q')) \in X_\alpha Q;\ \delta(x,q') = q\}$$

be the transitions "to" the q state.

Then T_{q0} *is a lateral class for* T_0 *and* T_{q1} *is a lateral class for* T_1

Proof 12

On the ECE, making the direct product $X{\times}Q$ as a Schreier Product $X_\alpha Q$; we see that the mapping Ψ of the **Def 4** is inyective

Proof 13

Consider the group $T = Q{\times}\beta(X_\alpha Q) \times Q \subseteq Q{\times}Y{\times}Q$. The mapping Ψ is a homomorphism between $X_\alpha Q$ and T. by the inyectivity, $X_\alpha Q \approx T$.

By other side, considering the proyection $\pi_1 : T \to Q$, given by

$$\pi_1\ (q,\beta(x,q),\ \delta(x,q) = q;$$

we see that π_1 is a suryective homomorphism with $Ker(\pi_1) = T_0$. Thus

$$\frac{T}{T_0} \approx Q.$$

Analogously, for T_1

Proof 14

Given $t'_q = (q,\beta(x',q),\delta(x',q)$; $t_q = (q,\beta(x,q),\ \delta(x,q) \in T_{q0}$; is suffice to show that $t'_q\, t^{-1}_q \in T_0$.

Indeed,

$$\begin{aligned} t'_q\, t^{-1}_q &= (q,\beta(x',q),\delta(x',q));\ (q,\beta(x,q),\ \delta(x,q))^{-1} \\ &= (q,\beta(x',q),\delta(x',q));\ (q^{-1}, \beta((x,q)^{-1}),\ \delta((x,q)^{-1})). \end{aligned}$$

But

$$(x,q)^{-1} = (\sigma(q)^{-1}\,[\mu(q, q^{-1}) \,.\, \mu(e_k, e_k) \,.\, x]^{-1}, q^{-1})$$

Hence, we can take $(x,q)^{-1} = (x'', q^{-1})$. Therefore

$$\begin{aligned} t'_q\, t^{-1}_q &= (e_Q,\ \beta((x',q)(x'', q^{-1})),\ \delta(x',q)(x'', q^{-1}))) \\ &= (e_Q,\ \beta(x'.\sigma(q)(x'').\mu(q,q^{-1}),\ e_Q),\ \delta(x'.\sigma(q)(x'').\mu(q,q^{-1}),\ e_Q)) \in T_0 \end{aligned}$$

The proof for T_{q1} is similar

2.3 Some Criteria to Construct Encoders

Def 5 *Given a encoder* $M = (X,Y,Q,X_\alpha Q,\delta,\beta)$ *we say that M is* **controllable**, *when* $\forall q,q' \in Q$, *there is a finite sequence* $\{x_1,x_2,...,x_n\} \subset X$, *such that*

$$q' = \delta(x_n, \delta(x_{n-1}, \delta(x_{n-2},...,\delta(x_2,\delta(x_1,q))...).$$

Our definition of controlability of encoders is compatible with the controlability of Codes given in [2], the controlability of Group Codes given in [3] and [1], and the controlability of Dynamical Systems given in [5] and [1].

pp 15 *Assume that the group Q is not trivial. If* T_0 *and* T_1, *defined in* **pp 13**, *are equals; then the machine is non-controllable.*

Proof

Given any sequence $\{x_i\}_{i=1}^{n}$, we have

$$\delta(x_n, \delta(x_{n-1}, \delta(x_{n-2}, \delta(x_2,\delta(x_1,e_Q))...) = e_Q\ ;$$

because, $T_0 = T_1 = \{(e_Q, \beta(x,e_Q), e_Q) / x \in X\}$.

Therefore for $q \neq e_Q$, there is not $\{x_i\}_{i=1}^{n}$, such that

$$q = \delta(x_n, \delta(x_{n-1}, \delta(x_{n-2},...,\delta(x_2,\delta(x_1,e_Q))...)$$

By joining this result to fact $X_\alpha Q \approx T$; we conclude that to build controllable machines is suffice to check the normal subgroups of $X_\alpha Q$ such that they have the same cardinality than X. Therefore:

pp 16 *If the class:*

$$\mathcal{X} = \{H \subset X_\alpha Q \text{ such that } H \text{ is a normal subgroup with } |H| = |X|\}$$

has not more than one element; then, the machine is non-controllable.

2.3.1 Examples

Ex 1

Let $X = Z_4$ and $Q = Z_5$ be two ciclic groups. The direct product $Z_4 \times Z_5$ it have only one normal subgroup of cardinality four and only one of cardinality five. Therefore; there is not any controlable machine for this Schreier Product.

Ex 2

Let $X = Q$ be the ciclic group

$$Z_4 = \{e_X = q_Q = e, \eta, \eta^2, \eta^3\}.$$

Let $\sigma: Z_4 \to Aut(Z_4)$ be, the homomorphism defined by:

$$\sigma(\eta^i)(\eta^j) = \eta^{j.3^i}$$

Take the Schreier Product $X_\alpha Q$ as being the Semidirect Product $X_\sigma Q$ as being the Semidirect Product $X_\alpha Q$, with the operation

$$(x,q)\,(x',q') = (x.\sigma(q)(x'), qq')$$

Since $x = \eta^i$, $q = \eta^j$, $x' = \eta^r$, $q' = \eta^s$, we have

$$\begin{aligned}(x,q)\,(x',q') &= (\eta^i,\eta^j)(\eta^i.\sigma(\eta^j)(\eta^r), \eta^j.\eta^s) \\ &= (\eta^{r.3^j+i}, \eta^{j+s})\end{aligned}$$

In this way we can write;

$$X_\alpha Q = \begin{Bmatrix}(0,0), (1,0), (2,0), (3,0), (0,1), (0,2), (0,3), (1,1), \\ (1,2), (1,3), (2,1), (3,1), (2,2), (3,2), (2,3), (3,3)\end{Bmatrix}$$

And the operation over $X_\sigma Q$ induced by σ, now is:

$$(i,j)(r,s) = (r3^j + i, j + s);\ (Mod4)$$

Also, we back to write

$$Z_4 = X = Q = \{0,1,2,3\}.$$

The normal subgroups of cardinality four are $U_0 = \{(0,0), (1,0), (2,0), (3,0)\}$ and $U_1 = \{(0,0), (1,2), (2,0), (3,2)\}$.

For the definition of δ in a way that it be a suryective homomorphism, we use the **pp 14.** We must take $T_0 \approx U_0$ and $T_1 \approx U_1$. Therefore, if $\delta: X_\sigma Q \rightarrow Q$ is defined, using the lateral classes of U_1, as being;

$$\delta(i,j) = \begin{cases} 0, & if \quad (i,j) \in \{(0,0),(1,2)(2,0),(3,2)\} \\ 1, & if \quad (i,j) \in \{(1,0) * (0,0),(1,2),(2,0),(3,2)\} \\ 2, & if \quad (i,j) \in \{(0,1) * (0,0),(1,2),(2,0),(3,2)\} \\ 3, & if \quad (i,j) \in \{(0,3) * (0,0),(1,2),(2,0),(3,2)\} \end{cases}$$

We have that δ is a suryective homomorphism.

Finally by making $Y = X_\sigma Q$, we can define $\beta = id.$ so, we have the machine $M = (X,Y,Q, X_\sigma Q,\delta,\beta)$ whose trellis graphic is showed in the Figure 4.

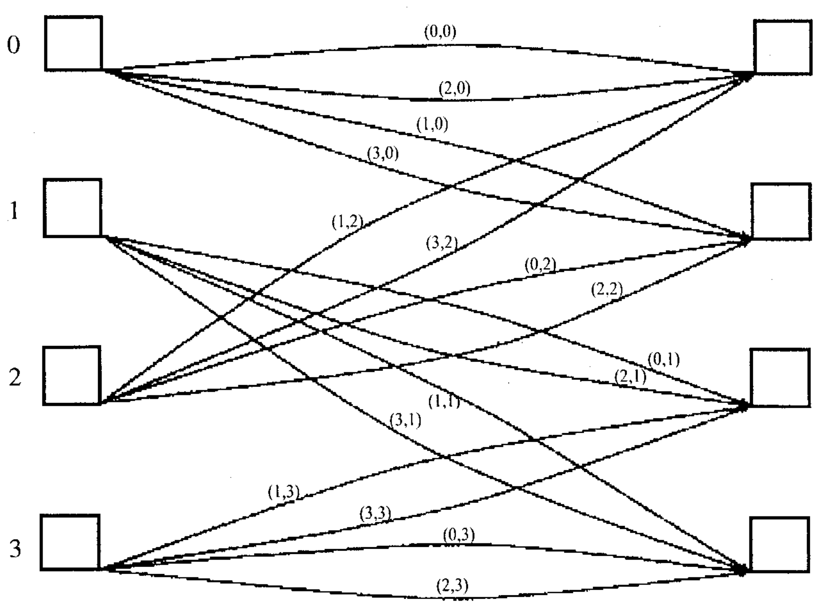


Figure 4: Trellis diagram for the machine $M = (X,Y,Q,X_\sigma Q,\delta,\beta)$

References:

[1] *M.D. Trott;* "The Algebraic Structure of Trellis Codes", Ph.D. dissertation, Dept. of Elect. Eng., Stanford University; Stanford CA, Aug. 1992.

[2] *H.A. Loeliger;* "On Euclidean-Space Group Codes", Ph.D. dissertation, Swiss Federal Institute of Tecnology, Zurich, 1992.

[3] *G.D. Forney, M.D. Trott;* "State Spaces, Trellis Diagrams and Minimal Encoders for Linear Codes over Groups"; IEEE Trans. Information Theory IT 39(5) 1491-1513; September 1993.

[4] *N. Jacobson;* "Basic Algebra II" 2nd ed., New York, Freeman, 1989.

[5] *J.C. Willems;* "Models for Dynamics" in Dynamics Reported Vol. 2, U. Kirchgraber and H.O. Walther, Eds. Wiley and Teubner, 1989.

[6] *M. Arbib;* "Automaton Decomposition and Semigroup Structure"; in "Algebraic Structure of Machines, Languages"; Michael A. Arbib ed. 1968.

arpasi@decom.fee.unicamp.br