UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE COMUNICAÇÕES

CODIFICADORES HOMOMORFOS SOBRE GRUPOS

Jorge Pedraza Arpasi

Orientador: **Prof. Dr. Reginaldo Palazzo Jr.**

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação, FEEC - UNICAMP, como requisito parcial para obtenção do título de DOUTOR EM ENGENHARIA ELÉTRICA.

Junho - 1996
Campinas - SP

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

P342c

Pedraza Arpasi, Jorge
Codificadores homomorfos sobre grupos / Jorge Pedraza Arpasi.--Campinas, SP: [s.n.], 1996.

Orientador: Reginaldo Palazzo Jr.
Tese (doutorado) - Universidade Estadual de Campinas Faculdade de Engenharia Elétrica e de Computação.

1. Códigos de controle de erros (Teoria da informação) 2. Modulação digital. 3. Teoria da codificação. 4. Teoria da informação. 5. Sistemas de transmissão de dados. I. Palazzo Jr., Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

.... If a word were chosen to condense the substance of the Inca's civilization, that word would have to be order. The order may be used in connection with almost everything of Inca State, including the planting of crops, the behavior of the armies, the output of gold mines, a census results, the composition of work forces, the amount and kind of tributes, the contents of storehouses ..... At the time of the transfer of the power from one Inca Emperor to the next, **information stored on quipus** *was called upon to recount the accomplishments of the new leader's predecesors.*

Texto extraído de *THE CODE OF QUIPU*; por Marcia Ascher & Robert Ascher, Michigan Univ. Press, 1982. Figura extraída da página 360 de *NUEVA CRONICA Y BUEN GOBIERNO*; por Felipe Guaman Poma de Ayala, carta ao Rei Felipe III da Espanha, Ano 1615.

Resumo

Neste trabalho, usando conceitos de extensão de grupos, consideramos codificadores convolucionais homomorfos. Seguindo [2] denominamos tal extensão de grupos como Produto de Schreier. Assim, aos codificadores convolucionais homomorfos e aos códigos convolucionais associados a estes codificadores denominamos por codificadores de Schreier e códigos de Schreier, respectivamente. Os códigos de Schreier são invariantes no tempo e o seu grupo de estados possui cardinalidade finita. Portanto, são um caso particular dos *group codes* definidos em [1]. Entretanto, a classe dos códigos de Schreier contém a classe dos códigos lineares binários e invariantes no tempo. Por outro lado, a classe dos códigos Euclidianos casados com os códigos de Schreier contêm os códigos geometricamente uniformes [3] com cardinalidade finita de estados.

Estudando o produto de Schreier, reconhecemos quatro tipos diferentes de produtos de grupos, entre os quais um novo tipo, denominado de *produto cíclico* é apresentado. A sua importância está relacionada à decomposição dos grupos cíclicos da forma $\mathbb{Z}_{p^m}$. Usando o fato de que um grupo pode ser decomposto em um destes produtos, apresentamos uma classificação dos grupos e derivamos uma construção multinível de códigos do espaço de sinais via o produto de Schreier, como uma generalização da construção de códigos do espaço de sinais via o produto direto. Também, mostramos que os códigos de Schreier são completos e estabelecemos um teste para controlabilidade com menor complexidade do que a própria definição .

Finalmente, à guisa de aplicação destes resultados, propomos dois algoritmos para a construção de códigos de Schreier mínimos, completos e controláveis.

Abstract

In this work we consider homomorphic convolutional encoders over groups, with finite states, by using the concepts from extension of groups. Following [2] we call such a group extension Schreier product. In this way, we call the homomorphic convolutional encoders over groups Schreier encoders, and the convolutional codes produced by these machines as Schreier codes. The Schreier codes are time-invariant and they have a finite group of states. Therefore, they are a special subclass of the generalized group codes over groups. However, the class of Schreier codes is large enough to contain all known, linear and time-invariant codes. On the other hand, the class of Euclidean codes matched to Schreier codes contain the geometrically uniform codes [3], with finite cardinality of states.

By studying the Schreier product we recognize four different types of product of groups including a new product called *cyclic product.* Its importance is related to the decomposition of cyclic groups of the form $\mathbb{Z}_{p^m}$. Using the fact that a given group can be decomposed into one of these four distinct products, we derive a *multilevel* construction of signal space codes via the Schreier product as a generalization of the *multilevel* construction of signal space codes via the direct product. Also, we show that the Schreier codes are complete and we establish a controllability test, with low complexity, for the Schreier codes, which can not be applied to the group codes.

Finally, as an application of these results, we propose two algorithms for the construction of minimal, complete and controllable Schreier codes.

Agradecimentos

Um agradecimento sincero ao meu orientador, Professor Reginaldo Palazzo Jr., pela oportunidade de trabalhar junto com ele. Estendo este agradecimento aos Professores Weiler Finamore, Marcelo Martins, José Carmelo Interlando, Max Costa, Jaime Portugheis e Celso de Almeida membros da Banca examinadora.

Minha gratidão também vai para as autoridades da Universidade Nacional San Luis Gonzaga de Ica, Peru. De maneira especial aos colegas do Departamento de Matemática da Faculdade de Ciências.

Durante este período da minha permanência na UNICAMP, sinto que não soube responder a muitas pessoas que me ofereceram sua amizade. Poucos conseguiram compreender e, acima de tudo, me aguentar em todas as circunstâncias como fizeram meus bons amigos Rodrigo Lemos e Paulo Bueno. Tenho a certeza de que esta amizade perdurará mesmo que seja na distância.

Precisamente, a amizade na distância, é assunto de destaque nos dias atuais, por causa da popularização da Internet. Neste período do meu doutoramento, fui testemunha direta e participante desta explosão da Internet. Portanto, tenho que ficar grato a esta rede de redes. Por exemplo, via Internet, obtive em primeira mão as teses de Trott, de Loeliger e vários artigos de Willems que inspiraram este trabalho. Isto, sem falar nos tele-amigos dos diferentes *newsgroups* ou *mail-lists* dos quais participei. Sinto saudades dos românticos dias pré-WWW, com seus únicos navegadores *gopher* e *ftp*. Eram dias em que apenas existiam 715 hosts servidores nos EUA e 124 fora, eram dias de recriminação a quem tentasse vender alguma coisa usando a Internet, mesmo que fosse um par de tênis. Parece incrível que tudo isto tenha ocorrido a menos de 3 anos.

Agradeço também o apoio financeiro obtido através do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

Tabela de Notações

$\mathbb{Z}_n$	Grupo aditivo do anel *mod* n.
$H \times K$	Produto cartesiano dos conjuntos H e K.
$H_{\oplus}K$	Produto direto dos grupos H e K.
G^2	Produto direto $G_{\oplus}G$, se G é grupo. Nos casos em que G é considerado como conjunto G^2 é o produto cartesiano $G \times G$.
$H_{(\sigma)}K$	Produto semidireto dos grupos H e K, via o mapeamento σ.
$H_{(\mu)}K$	Produto cíclico dos grupos H e K, via o mapeamento μ.
$H_{(\sigma,\mu)}K$	Produto de Schreier dos grupos H e K, via os mapeamentos σ e μ.
$H^i{}_{[\sigma,\mu]}K$	Produto misturado dos grupos H^i e K, via os mapeamentos σ e μ.
$H \lhd K$	H é subgrupo normal de K.
$H \rhd K$	K é subgrupo normal de H.
$\frac{H}{K}$	Grupo das classes laterais do subgrupo K, no grupo H. Também chamado de grupo quociente.
$H \cong K$	Os grupos H e K são isomorfos.
$H \overset{\theta}{\cong} K$	O grupo H é isomorfo ao grupo K via o isomorfismo θ.
$Aut(G)$	Grupo dos automorfismos do grupo G.
$Ker(\varphi)$	Núcleo do homomorfismo φ.
$\|G\|$	Cardinalidade do grupo ou conjunto G
e_G	Elemento neutro do grupo G.
id	Elemento neutro do grupo $Aut(G)$.

Conteúdo

Resumo i

1 Introdução 1

2 O Produto de Schreier 7

2.1 Produtos de Grupos 9

2.1.1 Exemplos 13

2.2 Alguns Produtos de Schreier Especiais 15

2.2.1 Produto de Schreier de grupos cíclicos 16

2.2.2 Exemplo: $\mathbb{Z}_4$ e $\mathbb{Z}_2$ dão origem a 4 diferentes produtos de Schreier $\mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$. 17

2.2.3 Construção multinível de produtos de Schreier 20

2.2.4 Exemplos 23

2.3 Decomposição de Grupos 25

2.3.1 Decomposição máxima 26

2.3.2 Exemplos 27

3 Códigos de Schreier 31

3.1 Máquinas 33

3.2 Codificadores Convolucionais Elementares sobre Grupos 35

3.2.1 Redução dos estados 40

3.2.2 Exemplos 43

3.3 Codificadores Convolucionais Generalizados 46
3.3.1 Codificadores da classe $M1$ 50
3.3.2 Exemplos 51

4 Controlabilidade e Completitude dos Códigos de Schreier **57**
4.1 A Estrutura de Grupo de $X^i \times Q$ 58
4.2 Teorema da Controlabilidade 64
4.3 Teorema da Completitude 66
4.3.1 Espaços métricos 66
4.3.2 Códigos invariantes no tempo são completos 66

5 Aplicações : Casos e Exemplos **69**
5.1 Construção de Codificadores Isomorfos, Controláveis e Completos 70
5.2 Caso Abeliano 75
5.2.1 Subcaso binário : $Y \approx \mathbb{Z}_2^n \approx \mathbb{Z}_2^k \oplus \mathbb{Z}_2^{n-k}$ 75
5.2.2 Subcaso cíclico : $Y \approx \mathbb{Z}_{p^n} \approx \mathbb{Z}_{p^k}{}_{(\mu)}\mathbb{Z}_{p^{n-k}}$ 78
5.3 Caso Não Abeliano 79

6 Considerações Finais **87**
6.1 Conclusões 88
6.2 Propostas de Pesquisa Futura 90

A Demonstração do Teorema de Schreier **91**

B Outras Demonstrações **97**
B.1 Prova da Proposição 2.2 97
B.2 Prova do Teorema 2.4 99
B.3 Prova do Teorema 4.1 102

C Alguns Teoremas Fundamentais da Álgebra **107**

Lista de Figuras

1.1 Regiões de escolha de bons codificadores(códigos). 6

2.1 Classificação dos diferentes tipos de produtos de grupos 11

3.1 Máquina generalizada 34
3.2 Treliça para o CCE do Exemplo 3.1 44
3.3 Treliça para o CCE do Exemplo 3.2 45
3.4 Treliça para a máquina do Exemplo 3.3 46
3.5 Codificador convolucional generalizado 48
3.6 Treliça do codificador $M_{(\sigma',\mu')} = (\mathbb{Z}_4, \mathbb{Q}_{3\oplus}\mathbb{D}_4, \mathbb{Z}_{2\oplus}\mathbb{D}_4, \delta, \beta)$ 54
3.7 Treliça da máquina $M_{(\mu')} = (\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_2^2, \delta, \beta)$ (Codificador de Ungerboeck) . . 56

5.1 Codificador de Schreier $M_{\oplus} = (\mathbb{Z}_2^k, \mathbb{Z}_2^n, \mathbb{Z}_2^{n-k}, \delta, \beta)$. 79
5.2 Codificador de Schreier $M_{\overline{\sigma}} = (\mathbb{Z}_4, \mathbb{D}_4^2, \mathbb{Z}_{2\oplus}\mathbb{D}_4, \delta, \beta)$. 85

B.1 Sistema de coordenadas $N \times R$ para o grupo G 100

Lista de Tabelas

2.1 **Tabela de Cayley para** $\mathbb{Z}_{2(\sigma)}^2\mathbb{Z}_2$ 13

2.2 **Tabela de Cayley para** $\mathbb{Z}_{4(\sigma)}\mathbb{Z}_2$ 19

2.3 **Tabela de Cayley para** $\mathbb{D}_4$ 20

2.4 **Tabela de Cayley para** $\mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$ 21

2.5 **Tabela de Cayley para** $\mathbb{Q}_3$ 21

3.1 **O grupo das classes laterais** $\frac{\mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_2\oplus\mathbb{D}_4)}{H_1}$ 53

3.2 **O grupo das classes laterais** $\frac{\mathbb{Z}_{4(\mu')}\mathbb{Z}_2{}^2}{H_1}$ 55

3.3 **O grupo das classes laterais** $\frac{\mathbb{Z}_{4(\mu')}\mathbb{Z}_2{}^2}{H_2}$ 56

5.1 **O grupo das classes laterais** $\frac{\mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4}{H_1}$ 74

Capítulo 1

Introdução

Em seu célebre artigo [10], Ungerboeck apresenta e discute informalmente o conceito de *casamento entre os bits codificados de um código convolucional binário e os pontos de um conjunto de sinais*, através de um mapeamento que denominou *mapping by set partitioning.* Este método heurístico atingiu enorme popularidade na comunidade de Teoria da Informação. Estimamos que um grande número de publicações, artigos, livros e notas didáticas, reproduziram a célebre[1] Figura 4 de [10], relativa ao particionamento do conjunto de sinais 8-PSK.

Assim, enquanto uma boa parcela de pesquisa e esforços foram dedicados na determinação de bons códigos de treliça via métodos computacionais seguindo a receita intuitiva de Ungerboeck, uma outra parcela foi dedicada à procura de uma fundamentação teórica de caráter algébrico-geométrico para estes códigos. A beleza da partição de Ungerboeck, a simetria dos rótulos binários dados aos sinais 8-PSK pelo *mapping by set partitioning*, as simetrias das transições (e a simetria dos pesos das mesmas) nas treliças de 4, 8 e 16 estados foram a motivação dos pesquisadores que acreditavam que o método de Ungerboeck era um caso particular, um exemplo, de alguma teoria algébrico-geométrica.

[1] No Exemplo 2.6, efetuamos tal particionamento de uma maneira sistemática e mostramos que o *mapping by set partitioning*, na verdade, é um isomorfismo entre os grupos $\mathbb{Z}_8$ e $(\mathbb{Z}_{2(\mu_1)}\mathbb{Z}_2)_{(\mu)}\mathbb{Z}_2$, sendo este último grupo uma decomposição realizada através de um novo tipo de produto de grupos que introduzimos neste trabalho, o qual chamamos produto cíclico.

Entre os trabalhos desenvolvidos relacionados a esta linha de pesquisa, os mais notáveis foram os de Calderbank/Sloane [14], e o de Slepian [15]. A retomada de [15] motivada por [10], foi importante por duas razões: 1)aparecem os grupos como estruturas algébricas a serem usadas em códigos convolucionais[2]; 2)uma extensão do domínio do grupo das matrizes ortogonais para todo o espaço ambiente[3] permitiu dar a fundamentação e uma base teórica aos códigos de Ungerboeck. Mas em nossa opinião, o ponto mais importante desta linha de pesquisa, depois de [10] foi o artigo [3] de Forney, onde é apresentada uma classe ampla de códigos de treliça : a classe dos *códigos geometricamente uniformes.* Esta classe é uma generalização de quase todos os códigos de treliça conhecidos, incluídos os códigos de Ungerboeck e de Slepian.

Por outro lado os *códigos geometricamente uniformes* adquirem de fato a sua importância no trabalho de tese de doutorado de M. D. Trott [1]. Em sua tese, Trott define um *group code*[4] como sendo um subgrupo do produto direto infinito da família de grupos $\{G_k\}_{k\in\mathbb{Z}}$, isto é , $\sum_{k\in\mathbb{Z}} G_k = \ldots_{\oplus} G_{-i_{\oplus}} \ldots_{\oplus} G_{1_{\oplus}} G_{0_{\oplus}} G_{1_{\oplus}} \ldots_{\oplus} G_{i_{\oplus}} \ldots$, $i \in \mathbb{N}$, e mostra que para cada código geometricamente uniforme $\mathcal{G}$ de [3] existe um *group code* $\mathcal{C}$ tal que o respectivo código Euclidiano $\mathcal{G}_1$, é igual a $\mathcal{G}$. A "conversão " do *group code* $\mathcal{C}$ no código de treliça $\mathcal{G}_1$ corresponde ao casamento entre sinais e grupos definidos na tese de Loeliger [2]. Tal casamento é feito por componentes, isto ẽ, cada grupo G_k, $k \in \mathbb{Z}$, deve estar casado com algum conjunto de pontos do espaço Euclidiano. Em ambas as teses [1] e [2], desenvolvidas simultaneamente, é mostrado que o casamento entre um grupo G e um conjunto discreto S é a ação transitiva do grupo G sobre o conjunto S, definição esta que corresponde precisamente aos códigos geometricamente uniformes.

Os *group codes* propostos por Trott são uma generalização do modelo de sistemas dinâmicos propostos por Willems [6], os quais estão definidos sobre corpos algébricos. É oportuno ressaltar que no contexto da Matemática, da Física e da Engenharia existem várias

---

[2]Até então só foram usados na codificação por blocos.

[3]Inicialmente o domínio de uma matriz ortogonal é um conjunto discreto $S \subset \mathbb{R}^n$. Sob determinadas condições é possível estender este domínio a todo o espaço $\mathbb{R}^n$.

[4]Os group codes definidos por Trott são diferentes dos group codes definidos por Slepian.

maneiras de caracterizar os sistemas dinâmicos, mas o elo comum entre estas caracterizações é que um sistema dinâmico deve estar relacionado a algum processo ou fenômeno evolutivo. A discordância básica é pela consideração ou não do meio ambiente do processo evolutivo como parte do sistema. Como a classe completa dos sistemas dinâmicos é muito grande, critérios de escolha devem ser estabelecidos. Entre estes critérios, os mais conhecidos são *controlabilidade, observabilidade, minimalidade, e completitude.* Como é de se esperar, os bons *group codes* também deverão ser controláveis, minimais, observáveis e completos. Como a análise destas propriedades é realizada supondo que tais sistemas são variantes no tempo, muitos dos resultados obtidos em [1] e [2] valem para códigos de treliça *variantes no tempo.* Nestes códigos, dado $i \in \mathbb{Z}$, a seção da treliça em i, denotada por T_i pode ser diferente da seção da treliça em $i+1$, denotada por T_{i+1}. É claro que estes resultados também são válidos para treliças invariantes no tempo, as quais constituem casos particulares. Uma particularidade importante é que quando o código é invariante no tempo e a cardinalidade do conjunto dos estados do codificador é finita, então o código sempre será completo. Este resultado é interessante, pois a totalidade dos códigos conhecidos e utilizados até agora, satisfazem estas duas condições de completitude. Ao nosso ver, esta é uma razão do pouco conhecimento desta propriedade. No entanto, quando o código é variante no tempo ou a cardinalidade dos estados é infinita, a completitude é uma propriedade que requer outras condições para ser atingida. Algo similar acontece para a minimalidade, controlabilidade, etc., isto é , há uma enorme dificuldade em se obter resultados valendo para toda a classe dos *group codes.*

No presente trabalho, o objeto principal de estudo são os **códigos de Schreier**. Os códigos de Schreier são semi-infinitos, invariantes no tempo, e têm grupo de estados finito. Desse modo, os códigos de Schreier formam uma subclasse especial dos *group codes.* Estas condições fazem com que um volume muito maior de resultados importantes para os códigos de Schreier do que para os *group codes* possam ser obtidos. Por exemplo, um dos resultados centrais deste trabalho é o Teorema 4.2, que é uma condição necessária e suficiente de controlabilidade válida para os códigos de Schreier e que não é válida para um *group code* em geral.

Este trabalho consiste dos seguintes tópicos

No Capítulo 2, estudamos a extensão de um grupo H por um grupo K, onde denominamos esta extensão por produto de Schreier de H e K, como sugerida em [2]. Uma das justificativas do nome é que o produto de Schreier é uma generalização dos produtos direto e semidireto de grupos. Além disso, como uma terceira particularidade do produto de Schreier, exibimos um novo tipo de produto de grupos, que chamamos de produto cíclico. Este novo produto é uma excelente ferramenta para a decomposição de grupos cíclicos. Como uma amostra da utilidade deste produto, no Exemplo 3.6 construímos o codificador de 4 estados correspondente à Figura 4 de [10]. Como um outro exemplo, mostramos no Exemplo 2.6 que o mapeamento de rotulamentos de Ungerboeck é um isomorfismo. Como não existe um método geral de construção de produtos de Schreier quando os grupos H e K são arbitrários, apresentamos um método para o caso particular de H e K serem cíclicos. Também apresentamos uma outra técnica para construir produtos de Schreier a partir de outros produtos de Schreier conhecidos. Finalmente, consideramos o problema recíproco da extensão de grupos, isto é, a decomposição de grupos. Neste sentido, estabelecemos os critérios para a decomposição de grupos e concluímos que a decomposição de grupos é uma generalização dos seguintes teoremas clássicos da álgebra: o *teorema fundamental da aritmética*, o *teorema chinês do resto*, e o *teorema fundamental dos grupos abelianos finitamente gerados.* Estes fatos demonstram a importância do produto de Schreier. Todavia o escopo aplicativo deste produto é muito mais amplo.

No Capítulo 3, definimos codificadores como máquinas, no sentido da teoria de autômatas. Por abuso de linguagem, suporemos que uma propriedade do codificador também é propriedade do código associado a ele. Por exemplo, quando dizemos que o codificador é controlável, estamos dizendo também que o respectivo código é controlável, e vice-versa. Tomando como base os códigos convolucionais binários, definimos os codificadores convolucionais elementares (CCE) sobre grupos. Todos os códigos convolucionais binários conhecidos pertencem à classe dos CCE. Em seguida, estabelecemos as propriedades que os CCEs devem satisfazer. Estas propriedades servirão de guia para definir os codificadores homomorfos generalizados. Apre-

sentamos também uma técnica de redução de estados quando o codificador não é mínimo. Os codificadores convolucionais homomorfos generalizados são definidos usando o produto de Schreier. Assim, chamamos a estes codificadores de **máquinas de Schreier**. Um código de Schreier é precisamente um código associado a uma máquina de Schreier. Como é de se esperar, todos os CCEs estão contidos nesta classe de codificadores homomorfos generalizados. Estabelecemos o primeiro teste (o teste suave) de controlabilidade denominado teste $M1$. Mostramos que um codificador que não satisfaz o teste $M1$, não é controlável.

No Capítulo 4 estabelecemos a linearidade dos códigos de Schreier. Esta propriedade é obtida através da definição de uma operação adequada na classe de seqüências finitas de entrada $\{x_j\}_{j=1}^{i}$, da máquina de Schreier. Através desta operação mostramos que esta classe constitui um grupo. Portanto, dadas duas seqüências de entradas $\{x_j\}_{j=1}^{i}$ e $\{u_j\}_{j=1}^{i}$, as correspondentes respostas do codificador são $\{y_j\}_{j=1}^{i}$ e $\{v_j\}_{j=1}^{i}$. Então mostramos que a linearidade do codificador é no sentido que a resposta do produto das entradas $(\{x_j\}_{j=1}^{i})$ * $(\{u_j\}_{j=1}^{i})$ é igual ao produto das respostas $(\{y_j\}_{j=1}^{i})$ * $(\{v_j\}_{j=1}^{i})$. Usando deste fato, apresentamos uma condição necessária e suficiente para se atingir a controlabilidade (Teorema 4.2).

O Capítulo 5 é dedicado a considerações na construção de codificadores e à proposição de algoritmos para a determinação de bons códigos. Para isto, restringimos a procura de códigos (codificadores) de Schreier que sejam completos, mínimos, e controláveis. Como mencionado anteriormente, cada código invariante no tempo e com um número finito de estados é sempre completo. A minimalidade é atingida considerando os codificadores como sendo isomorfos. Por outro lado, a controlabilidade é atingida através da aplicação do teste $M1$ e do Teorema 4.2. Estas considerações são ilustradas na Fig. 1.1. Finalmente, no Capítulo 6 são apresentadas as conclusões e alguns tópicos de pesquisa futura decorrentes deste trabalho.

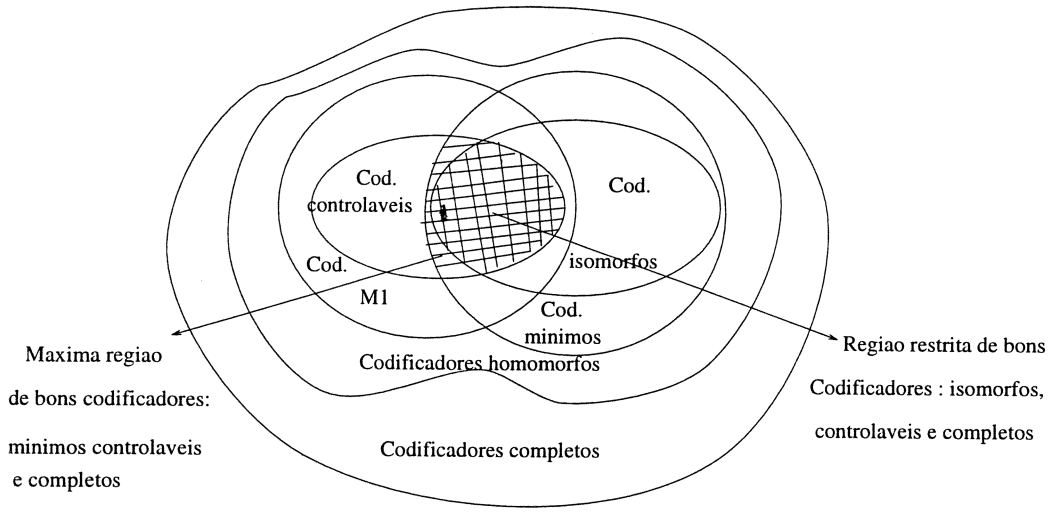

Figura 1.1: Regiões de escolha de bons codificadores(códigos).

Capítulo 2

O Produto de Schreier

Como resultado do esquema de modulação codificada, cujo alfabeto usado é constituído pelos sinais do canal, apareceram os códigos de treliça ou códigos Euclidianos(pois pode-se considerar os sinais como pontos de algum espaço Euclidiano). Trott e Forney em [1] e [18] e Loeliger em [2] e [19] mostram que os códigos Euclidianos podem ser casados com códigos convolucionais sobre grupos denominados *group codes*. Como um código Euclidiano e seu respectivo *group code* casado possuem treliças com a mesma dinâmica, é plausível esperar que muitas das propriedades requeridas, relativas ao desempenho de um código Euclidiano possam ser obtidas diretamente no correspondente *group code* associado. O estudo dos *group codes* está estreitamente relacionado ao conceito de decomposição de grupos. Dentro da álgebra pura este conceito tem tido um tratamento superficial, pois tal decomposição somente é feita em grupos abelianos.

No contexto da teoria da codificação, a necessidade desta decomposição de grupos surge pelo fato de que em [1] se prova que os estados de um *group code* formam um grupo e que este grupo dos estados induz uma operação sobre as transições da seção de treliça de modo que esta seção de treliça é também um grupo. Quando o grupo seção de treliça é abeliano não cíclico, então ele é isomorfo (algebricamente idêntico) ao produto direto do grupo dos estados e do grupo das entradas. Isto é , o grupo seção de treliça pode ser decomposto no

produto direto dos grupos das entradas e dos estados. Isto ocorre com a maioria dos *group codes* até então conhecidos, de maneira especial com os códigos convolucionais binários.

As dificuldades aparecem quando este grupo seção de treliça é não abeliano ou cíclico da forma $\mathbb{Z}_{p^n}$. Numa primeira tentativa, procura-se um isomorfismo com algum produto direto de dois grupos no qual um dos grupos componentes seja não abeliano; pois conforme veremos neste capítulo, um grupo não abeliano, não pode ser isomorfo a um produto direto de grupos abelianos. Quando não existir nenhum produto direto com estas condições, numa segunda tentativa, procura-se um isomorfismo com algum produto semidireto de dois grupos. Porém, existem grupos que não são decompostos como produto direto nem como produto semidireto, tal é o caso do grupo dos quatérnios $\mathbb{Q}_3$ ou dos grupos cíclicos da forma $\mathbb{Z}_{p^n}$. Assim sendo, é clara a necessidade de um produto generalizado de grupos que possa ser manipulável e sobretudo, que dado um grupo, sempre seja possível decompô-lo como o produto de dois grupos que seriam o das entradas e o dos estados. Este produto generalizado. que chamaremos produto de Schreier, é exatamente uma extensão de grupos.

Este capítulo é organizado da seguinte maneira. Na Seção 2.1 começamos lembrando o problema da extensão de grupos e o teorema de Schreier equivalente a este problema. Alguns autores denominam este teorema como a *solução de Schreier* para o problema da extensão de grupos. Usamos o teorema de equivalência de Schreier para dar a definição do produto de Schreier como uma estrutura que é equivalente a uma extensão de grupos. Mostramos que o produto de Schreier é a generalização dos produtos direto e semidireto de grupos, sendo esta a principal justificativa para a denominação *produto de Schreier de grupos* ao invés de *extensão de grupos.* Ao final da seção apresentamos alguns exemplos para ilustrar este produto. Na Seção 2.2 mediante a Proposição 2.2 deduzimos uma técnica para construir produtos de Schreier a partir de grupos cíclicos. Assim, podemos dizer que com esta proposição o problema da extensão de grupos para o caso de grupos cíclicos, é resolvido. O exemplo dos 4 grupos diferentes de ordem 8 obtidos aplicando esta técnica aos grupos cíclicos $\mathbb{Z}_4$ e $\mathbb{Z}_2$, é analisado em detalhe. Também, apresentamos uma técnica para construção multinível de novos produtos de Schreier a partir de produtos de Schreier conhecidos. Combinando

estas técnicas é realizada uma interpretação do código de Ungerboeck. Finalmente, na Seção 2.3 estudamos o problema inverso da extensão de grupos, que é o da decomposição de grupos. Baseados nas propriedades do produto de Schreier e no teorema de Jordan-Hölder estabelecemos o Teorema 2.5 sobre a existência e unicidade da decomposição máxima dos grupos.

2.1 Produtos de Grupos

Definição 2.1 *Dados os grupos H e K, uma* **extensão** *de H por K é um grupo G que possui um subgrupo normal $N \cong H$ e além disso $\frac{G}{N} \cong K$.*

$\diamond$

Desta definição decorre que dados H e K podem existir diferentes extensões de H por K. Isto é, podem existir G_1 e G_2, com $G_1 \ncong G_2$ tal que G_1 é uma extensão de H por K e G_2 é uma outra extensão de H por K.

O problema da extensão de grupos formulada por O. Hölder, consiste em determinar todas as extensões de um dado grupo H por um dado grupo K. Em 1926 O. Schreier colocou este problema da seguinte maneira:

Teorema 2.1 (O. Schreier) [11] *Dados os grupos H e K, se existirem aplicações $\sigma : K \to Aut(H)$, e $\mu : K \times K \to H$, tais que para todo $k_1, k_2, k_3 \in K$, e para todo $h \in H$ satisfazem as equações*

$$\sigma(k_1)(\mu(k_2, k_3)).\mu(k_1, k_2k_3) = \mu(k_1, k_2).\mu(k_1k_2, k_3) \tag{2.1}$$

$$\sigma(k_1)(\sigma(k_2)(h)) = \mu(k_1, k_2).\sigma(k_1k_2)(h).(\mu(k_1, k_2))^{-1}, \tag{2.2}$$

então existe uma extensão de H por K, cuja operação de grupo é dada por

$$(h, k) * (h', k') = (h.\sigma(k)(h').\mu(k, k'), kk'), \tag{2.3}$$

onde, $h \in H$ e $k \in K$.

As condições (2.1) e (2.2) são usadas essencialmente para garantir a propriedade associativa da operação explicitada em (2.3).

Schreier mostrou que existem tantas extensões quantos forem os pares de aplicações σ e μ satisfazendo (2.1) e (2.2). Muitos autores denominam este teorema de Schreier como sendo a *solução de Schreier* ao problema da extensão de grupos. Todavia, o problema continua existindo, pois as aplicações σ e μ sujeitas às condições (2.1) e (2.2) deverão ser determinadas. No contexto da Álgebra pura, a "solução de Schreier" foi interpretada em termos de cohomologias de segunda ordem(vide [11], [5] ou [8]). No contexto da teoria da codificação , interpretaremos a "solução de Schreier" como um produto de grupos.

Definição 2.2 *Sejam H e K grupos. Sejam $\sigma : K \to Aut(H)$ e $\mu : K \times K \to H$ aplicações satisfazendo* (2.1) *e* (2.2)*, portanto satisfazendo as condições do Teorema de Schreier. Então, definimos o* **produto de Schreier** *de H por K, denotado por $H_{(\sigma,\mu)}K$, como sendo a extensão de H por K para o homomorfismo σ e o mapeamento μ.*

◇

De acordo com a Definição 2.2, o Teorema de Schreier pode ser expresso da seguinte forma

Teorema 2.2 *O produto de Schreier $H_{(\sigma,\mu)}K$ é um grupo.*

Prova: Vide o Apêndice A ∎

A denominação *produto de Schreier*, e a notação $H_{(\sigma,\mu)}K$, em lugar de *extensão de grupos*, será justificada em seguida quando analisarmos os casos particulares de σ e μ.

Quando $\mu(k,k') = e_H \ ; \forall k,k' \in K$; onde e_H é o elemento neutro de H, então (2.1) e (2.2) são satisfeitas se e somente se $\sigma : K \to Aut(H)$ for um homomorfismo de grupos. Neste caso temos o **produto semidireto** de H e K, $H_{(\sigma)}K$, pois a operação (2.3) fica reduzida a

$$(h,k) * (h',k') = (h.\sigma(k)(h')\,,\ kk')\,. \tag{2.4}$$

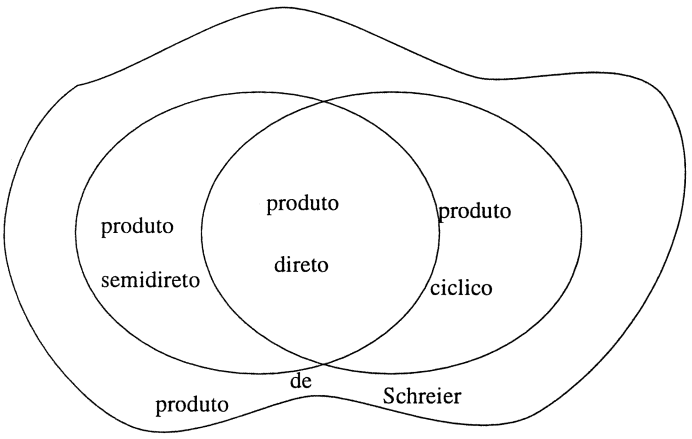

Figura 2.1: Classificação dos diferentes tipos de produtos de grupos

Quando $\sigma(k) = id \in Aut(H)$, $\forall\ k \in K$, então (2.2) é trivialmente satisfeita, mas (2.1) fica sendo dada por

$$\mu(k_2, k_3).\mu(k_1, k_2k_3) = \mu(k_1, k_2).\mu(k_1k_2, k_3). \tag{2.5}$$

Então, se $\mu : K \times K \rightarrow H$ satisfaz (2.5) definimos o **produto cíclico** de H e K, $H_{(\mu)}K$ como os pares ordenados (h, k), $h \in H$ e $k \in K$. Neste caso a operação (2.3) fica reduzida a

$$(h, k) * (h', k') = (h.h'.\mu(k, k'), kk')\,. \tag{2.6}$$

Finalmente, quando $\mu(k, k') = e_H\ , \forall k, k' \in K$ e $\sigma(k) = id \in Aut(H)$. $\forall\ k \in K$, então (2.1) e (2.2) são satisfeitas. Como resultado, temos o **produto direto** de H e K, $H_{\oplus}K$, pois a operação (2.3) fica reduzida a

$$(h, k) * (h', k') = (hh'\ ,\ kk')\,. \tag{2.7}$$

Desse modo, mostramos que o produto de Schreier é uma generalização dos conhecidos produto direto e semidireto de grupos. Esta é uma das razões pela qual denominamos esta estrutura de produto ao invés de extensão. Na Fig. 2.1 é mostrado o diagrama de Venn destes produtos. A interpretação que se deve fazer deste diagrama é no sentido de que a classe de grupos gerados a partir de produtos diretos está contida na classe de grupos gerados a partir do produto cíclico e assim sucessivamente.

Seja $H_{(\sigma,\mu)}K$ o produto de Schreier dos grupos H e K, para um dado par (σ,μ). Seja Φ_K a classe de homomorfismos sobrejetores entre $H_{(\sigma,\mu)}K$ e K, isto é ,

$$\Phi_K = \{\phi : H_{(\sigma,\mu)}K \to K \ : \ \phi \text{ é sobrejetor}\}. \tag{2.8}$$

Seja $\mathcal{X}$ uma família de subconjuntos de $H_{(\sigma,\mu)}K$, definido por

$$\mathcal{X} = \{S \ : \ S = Ker(\phi),\ \phi \in \Phi_K\}. \tag{2.9}$$

Então, pelo teorema fundamental dos homomorfismos (vide Apêndice C), para cada $S \in \mathcal{X}$ temos que $S \lhd H_{(\sigma,\mu)}K$ e $\frac{H_{(\sigma,\mu)}K}{S} \cong K$.

Seja H_0 o subconjunto de $H_{(\sigma,\mu)}K$ definido por

$$H_0 = \{(h, e_K) \ : \ h \in H\}. \tag{2.10}$$

Então, $H_0 \in \mathcal{X}$ pois $H_0 = Ker(p_2)$, onde $p_2 : H_{(\sigma,\mu)}K \to K$ é a projeção dada por $p_2(h,k) = k$ consequentemente, $p_2 \in \Phi_K$ portanto, $\mathcal{X}$ é uma subclasse não vazia. Veremos que para efeitos de construção de bons códigos, os produtos de Schreier mais interessantes serão aqueles tais que $\mathcal{X}$ tenha mais do que um elemento.

Proposição 2.1 *Se existir $k_0 \in K$ tal que $\sigma(k_0) \neq id \in Aut(H)$ no produto de Schreier $H_{(\sigma,\mu)}K$, então $H_{(\sigma,\mu)}K$ é não abeliano.*

Prova: Considere o caso abeliano, isto é ,

$$(h,k)(h',k') = (h',k')(h,k) \ \ ;\forall\, h\,, h' \in H \text{ e } \forall\, k\,, k' \in K$$

Em particular para $k = k' = k_0$, e $h = e_H$ temos que

$$(e_H, k_0)(h', k_0) = (h', k_0)(e_H, k_0)\ ,\ \ \forall\, h' \in H$$
$$(e_H.\sigma(k_0)(h').\mu(k_0,k_0)\ ,\ k_0^2) = (h'.\sigma(k_0)(e_H).\mu(k_0,k_0)\ ,\ k_0^2)\ ,\ \ \forall\, h' \in H$$
$$\sigma(k_0)(h') = h'\ \ ,\ \ \forall\, h' \in H$$

Portanto $\sigma(k_0) = id$ ∎

Note que este resultado é independente de μ, consequentemente valendo para o produto semidireto $H_{(\sigma)}K$. Este resultado é um critério valioso para a construção de grupos não abelianos.

$\mathbb{Z}^2_{2(\sigma)}\mathbb{Z}_2$	(00,0)	(10,1)	(11,0)	(01,1)	(10,0)	(01,0)	(00,1)	(11,1)
(00,0)	(00,0)	(10,1)	(11,0)	(01,1)	(10,0)	(01,0)	(00,1)	(11,1)
(10,1)	(10,1)	(11,0)	(01,1)	(00,0)	(11,1)	(00,1)	(10,0)	(01,0)
(11,0)	(11,0)	(01,1)	(00,0)	(10,1)	(01,0)	(10,0)	(11,1)	(00,1)
(01,1)	(01,1)	(00,0)	(10,1)	(11,0)	(00,1)	(11,1)	(01,0)	(10,0)
(10,0)	(10,0)	(00,1)	(01,0)	(11,1)	(00,0)	(11,0)	(10,1)	(01,1)
(01,0)	(01,0)	(11,1)	(10,0)	(00,1)	(11,0)	(00,0)	(01,1)	(10,1)
(00,1)	(00,1)	(01,0)	(11,1)	(10,0)	(01,1)	(10,1)	(00,0)	(11,0)
(11,1)	(11,1)	(10,0)	(00,1)	(01,0)	(10,1)	(01,1)	(11,0)	(00,0)

Tabela 2.1: **Tabela de Cayley para** $\mathbb{Z}^2_{2(\sigma)}\mathbb{Z}_2$

2.1.1 Exemplos

Exemplo 2.1 *Construção do produto semidireto* $\mathbb{Z}^2_{2(\sigma)}\mathbb{Z}_2$ *que é isomorfo a* $\mathbb{D}_4$*, o grupo das simetrias do quadrado.*

Considere o homomorfismo $\sigma : \mathbb{Z}_2 \to Aut(\mathbb{Z}_2^2)$ definido por $\sigma(0) = id \in Aut(\mathbb{Z}_2^2)$ e $\sigma(1) \in Aut(\mathbb{Z}_2^2)$ o automorfismo definido por:

$$\sigma(1)(00) = 00$$
$$\sigma(1)(01) = 10$$
$$\sigma(1)(10) = 01$$
$$\sigma(1)(11) = 11.$$

Então, a operação de (h, k) por (h', k') é dada por $(h, k) * (h', k') = (h.\sigma(k)(h'), kk')$. Por exemplo, $h = 10$, $h' = 01$, $k = 1$, e $k' = 0$ produz

$$(10, 1)(01, 0) = (10 + \sigma(1)(01), 1 + 0) = (10 + 10, 1) = (00, 1).$$

A tabela de Cayley é mostrada na Tabela 2.1.

Comparando as Tabelas 2.1 e 2.3, pode ser visto que $\theta : \mathbb{Z}^2_{2(\sigma)}\mathbb{Z}_2 \to \mathbb{D}_4$ dado por

$$\begin{aligned} \theta(00,0) &= R_0 \quad & \theta(10,0) &= d_1 \\ \theta(10,1) &= R_1 \quad & \theta(01,0) &= d_2 \\ \theta(11,0) &= R_2 \quad & \theta(00,1) &= V \\ \theta(01,1) &= R_3 \quad & \theta(11,1) &= H \end{aligned}$$

é um isomorfismo e $\mathbb{D}_4 \overset{\theta}{\cong} \mathbb{Z}^2_{2(\sigma)}\mathbb{Z}_2$.

Exemplo 2.2 *Construção de um produto de Schreier não trivial para* $H = \mathbb{Z}_{4\oplus}\mathbb{Z}_2$ *e* $K = \mathbb{Z}_2$.

Note que, como H é abeliano, de acordo com a Proposição A.1(vide apêndice A), σ deve ser um homomorfismo. Portanto, a equação (2.2) é trivialmente satisfeita. Seja $\sigma : \mathbb{Z}_2 \to Aut(\mathbb{Z}_{4\oplus}\mathbb{Z}_2)$ definido por $\sigma(0) = id \in Aut(\mathbb{Z}_{4\oplus}\mathbb{Z}_2)$ e $\sigma(1) \in Aut(\mathbb{Z}_{4\oplus}\mathbb{Z}_2)$ tal que

$$\begin{aligned} \sigma(1)(00) &= 00 \quad & \sigma(1)(01) &= 01 \\ \sigma(1)(10) &= 30 \quad & \sigma(1)(11) &= 31 \\ \sigma(1)(20) &= 20 \quad & \sigma(1)(21) &= 21 \\ \sigma(1)(30) &= 10 \quad & \sigma(1)(31) &= 11. \end{aligned}$$

Agora, defina o mapeamento $\mu : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_{4\oplus}\mathbb{Z}_2$ como sendo

$$\mu(k_1,k_2) = \begin{cases} 00, & \text{se} \quad k_1 + k_2 < 2 \\ 01, & \text{se} \quad k_1 + k_2 = 2. \end{cases}$$

Para $H = \mathbb{Z}_{4\oplus}\mathbb{Z}_2$ e $K = \mathbb{Z}_2$, a equação (2.1) torna-se

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

Se $k_1 = 0$, então

$$\mu(k_2,k_3) = \mu(0,k_2) + \mu(k_2,k_3) + \mu(0,k_2+k_3).$$

Disto resulta que, $\mu(k_2,k_3) = \mu(k_2,k_3)$. Portanto, para $k_1 = 0$, a equação (2.1) é trivialmente satisfeita.

Se $k_1 = 1$, então para o par (k_2,k_3) temos as seguintes possibilidades $(k_2,k_3) = (0,0)$,

$(k_2, k_3) = (0,1)$, $(k_2, k_3) = (1,0)$, ou $(k_2, k_3) = (1,1)$. Sabendo que $\mu(x,y) = 0$ se $x + y < 2$, temos que para $k_1 = 1$ e $(k_2, k_3) = (0,0)$, $(k_2, k_3) = (0,1)$ ou $(k_2, k_3) = (1,0)$, a equação (2.1) é satisfeita. Finalmente, para o caso em que $k_1 = 1$ e $(k_2, k_3) = (1,1)$ temos $\sigma(1)(\mu(1,1)) = \mu(1,1) + \mu(1,1) + \mu(1,1)$. Logo $\sigma(1)(\mu(1,1)) = \mu(1,1)$ que é verdadeira pela definição de μ. Portanto, σ e μ satisfazem as condições (2.1) e (2.2). Logo, o produto de Schreier não trivial $\mathbb{Z}_{4\oplus}\mathbb{Z}_{2(\sigma,\mu)}\mathbb{Z}_2$ está bem definido.

Agora, dados (h,k), $(h',k') \in \mathbb{Z}_{4\oplus}\mathbb{Z}_{2(\sigma,\mu)}\mathbb{Z}_2$, a operação $(h,k) * (h',k')$ resulta em

$$
\begin{aligned}
(h,k) * (h',k') &= (h + \sigma(k)(h') + \mu(k,k')\,,\; k + k') \\
&= \begin{cases}
(h + h'\,,\, 0), & \text{se } k = 0 \text{ e } k' = 0 \\
(h + h'\,,\, 1), & \text{se } k = 0 \text{ e } k' = 1 \\
(h + \sigma(1)(h')\,,\, 1), & \text{se } k = 1 \text{ e } k' = 0 \\
(h + \sigma(1)(h') + 01\,,\, 1), & \text{se } k = 1 \text{ e } k' = 1.
\end{cases}
\end{aligned}
$$

Por exemplo, se $h = (2,1)$ e $h' = (3,0)$, onde h, $h' \in \mathbb{Z}_{4\oplus}\mathbb{Z}_2$, e $k = 0$ e $k' = 1$, onde k, $k' \in \mathbb{Z}_2$, temos que $(h,k) * (h',k') = (h + h', 1)$ =(21+30,1)= (11,1).

2.2 Alguns Produtos de Schreier Especiais

Como não existe uma técnica geral de construção de produtos de Schreier e consequentemente a pouca utilização do mesmo em problemas práticos, é que persiste o "problema da extensão de grupos". No sentido de enfatizar a importância deste produto é que apresentamos a seguir uma técnica de obtenção de produtos de Schreier para o caso particular em que os grupos H e K são grupos cíclicos. Também apresentamos uma outra técnica para a obtenção de produtos de Schreier a partir produtos de Schreier conhecidos. Estes procedimentos serão úteis na geração de uma parcela considerável de grupos não abelianos. Assim, o processo de geração de grupos não abelianos pode ser realizado através de um algoritmo, pois as respectivas operações reduzem-se às conhecidas operações $mod\, n$. A implementação computacional conduzirá, em um trabalho futuro, a obter novos códigos Euclidianos.

2.2.1 Produto de Schreier de grupos cíclicos

Proposição 2.2 *Sejam n, $m \in \mathbb{N}$, onde $n \geq 2$ e $m \geq 2$. Considere o sistema de equações*

$$\begin{aligned} x^m &= 1(mod\, n) \\ yx &= y(mod\, n). \end{aligned} \tag{2.11}$$

Então, para cada solução (x, y) deste sistema, existe um par de aplicações σ e μ satisfazendo (2.1) e (2.2) tal que podemos construir o produto de Schreier $\mathbb{Z}_{n(\sigma,\mu)}\mathbb{Z}_m$.

Prova: Vide Apêndice B ∎

Cada solução de (2.11) resulta em um produto de Schreier. Todavia a recíproca não é verdadeira. Para isto, considere os Exemplos 2.1 e 2.3 onde o grupo das simetrias do quadrado $\mathbb{D}_4$ é construído (portanto decomposto) de duas maneiras diferentes. Note que cada par $(1, j)$ do conjunto $\{(1,0),(1,2),\ldots,(1,n-1)\}$ é sempre uma solução de (2.11). Na demonstração da Proposição 2.2, σ foi estabelecido através da solução x, de modo que $x = 1$ implica em $\sigma(k) = id \in Aut(\mathbb{Z}_n)$, para todo $k \in \mathbb{Z}_m$. Nesta mesma demonstração, μ foi estabelecido através da solução y, de maneira que $y = 0$ implica em $\mu(k_1, k_2) = 0 \in \mathbb{Z}_n$, para todo k_1, $k_2 \in \mathbb{Z}_m$. Logo, a solução $(x, y) = (1, 0)$ conduz à construção do produto direto $\mathbb{Z}_{n\oplus}\mathbb{Z}_m$. Como conseqüência, temos que cada solução $(1, j)$ de (2.11), $j = 1, \ldots, n-1$, conduz necessariamente à construção de um grupo abeliano. (vide Proposição 2.1).

Uma regra prática para calcular $(i, j) * (s, t)$

Usando a notação da demonstração da Proposição 2.2, temos que o produto em $\mathbb{Z}_{n(\sigma,\mu)}\mathbb{Z}_m$ é dado por

$$\begin{aligned} (\gamma^i, \eta^j)(\gamma^s, \eta^t) &= (\gamma^i.\sigma(\eta^j)(\gamma^s).\mu(\eta^j, \eta^t) \;;\; \eta^j\eta^t) \\ &= (\gamma^i.\gamma^{s.x^j}.\mu(\eta^j, \eta^t) \;;\; \eta^{j+t}) \\ &= \begin{cases} (\gamma^{i+s.x^j}.\gamma^y \;;\; \eta^{j+t}) & \text{se} \quad j + t \geq m \\ (\gamma^{i+s.x^j} \;;\; \eta^{j+t}) & \text{se} \quad j + t < m. \end{cases} \end{aligned}$$

Portanto, se (x, y) é uma solução de (2.11) e usando do fato que $\mathbb{Z}_n$ e $\mathbb{Z}_m$ podem ser expressos por $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ e $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, temos que $\forall\ (i, j), (s, t) \in \mathbb{Z}_{n(\sigma,\mu)}\mathbb{Z}_m$ a

operação $(i,j)*(s,t)$ pode ser escrita como

$$(i,j)*(s,t)=\begin{cases}((i+s.x^j+y)mod\, n\ ,\ (j+t)mod\, m) & \text{se}\ \ j+t\geq m\\ ((i+s.x^j)mod\, n\ ,\ (j+t)mod\, m) & \text{se}\ \ j+t<m.\end{cases} \tag{2.12}$$

Para $x>1$ e $y=0$, a equação (2.12) resulta no produto semidireto $\mathbb{Z}_{n(\sigma)}\mathbb{Z}_m$ pois a operação $(i,j)*(s,t)$, é dada por

$$(i,j)*(s,t)=((i+s.x^j)mod\, n\ ,\ (j+t)mod\, m) \tag{2.13}$$

Por outro lado, quando $x=1$ e $y>0$, a equação (2.12) resulta no produto cíclico $\mathbb{Z}_{n(\mu)}\mathbb{Z}_m$ pois a operação $(i,j)*(s,t)$ é dada por

$$(i,j)*(s,t)=\begin{cases}((i+s+y)mod\, n\ ,\ (j+t)mod\, m) & \text{if}\ \ j+t\geq m\\ ((i+s)mod\, n\ ,\ (j+t)mod\, m) & \text{if}\ \ j+t<m.\end{cases} \tag{2.14}$$

Geradores

Os elementos $(1,0)$ e $(0,1)$ são chamados os geradores canônicos de $\mathbb{Z}_{n(\sigma,\mu)}\mathbb{Z}_m$, pois para todo $(h,k)\in\mathbb{Z}_{n(\sigma,\mu)}\mathbb{Z}_m$ temos

$$(h,k)=(1,0)^h.(0,1)^k. \tag{2.15}$$

2.2.2 Exemplo: $\mathbb{Z}_4$ e $\mathbb{Z}_2$ dão origem a 4 diferentes produtos de Schreier $\mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$.

Exemplo 2.3 *Considere os grupos cíclicos $\mathbb{Z}_4$ e $\mathbb{Z}_2$.*

O sistema

$$\begin{aligned}x^2 &= 1\,(mod\,4)\\ xy &= y\,(mod\,4)\end{aligned}$$

apresenta as seguintes soluções

$$(x,y)=\{(1,0),(1,1),(1,2),(1,3),(3,0),(3,2)\}$$

- A solução $(1,0)$ produz o produto direto $\mathbb{Z}_{4\oplus}\mathbb{Z}_2$.

- A solução $(1,2)$ produz o produto direto $\mathbb{Z}_{4\oplus}\mathbb{Z}_2$. Neste caso temos um produto cíclico $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$, e a respectiva operação $(i,j)*(s,t)$ é dada por

$$(i,j)*(s,t) = \begin{cases} ((i+s+2)mod 4\ ,\ 0) & \text{se}\quad j+t=2 \\ ((i+s)mod 4\ ,\ j+t) & \text{se}\quad j+t<2. \end{cases}$$

Dado $(i,j) \in \mathbb{Z}_{4(\mu)}\mathbb{Z}_2$, temos que $j=0$ ou $j=1$.

Se $j=0$, então $(i,0)^2=(i^2,0)$, $(i,0)^3=(i^3,0)$, e $(i,0)^4=(i^4,0)=(0,0)$. Assim a ordem de $(i,0)$ é menor ou igual a 4. Se $j=1$, então $(i,1)^2=(i^2+2,0)$, $(i,1)^3=(i^3+2,1)$, e $(i,1)^4=(i^4+2+2,0)=(0,0)$. Logo, a ordem de $(i,1)$ é também menor ou igual a 4. Portanto , $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$ não pode ser isomorfo a $\mathbb{Z}_8$. Por outro lado, considere $(1,0) \in Z_{4(\mu)}\mathbb{Z}_2$. Então $(1,0)^2=(2,0)$, $(1,0)^3=(3,0)$, e $(1,0)^4=(0,0)$. Portanto, $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$ não é isomorfo a $\mathbb{Z}_2^3$. Como $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$ é abeliano com cardinalidade 8, então deve ser isomorfo a $\mathbb{Z}_{4\oplus}\mathbb{Z}_2$.

- A solução $(1,1)$ conduz ao grupo cíclico $\mathbb{Z}_8$. Neste caso temos, um produto cíclico $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$, e a respectiva operação $(i,j)*(s,t)$ é dada por

$$(i,j)*(s,t) = \begin{cases} ((i+s+1)mod 4\ ,\ 0) & \text{se}\quad j+t=2 \\ ((i+s)mod 4\ ,\ j+t) & \text{se}\quad j+t<2. \end{cases}$$

Considere o elemento $(0,1) \in \mathbb{Z}_{4(\mu)}\mathbb{Z}_2$. Assim, $(0,1)^2=(1,0)$, $(0,1)^3=(1,1)$, $(0,1)^4=(2,0)$, $(0,1)^5=(2,1)$, $(0,1)^6=(3,0)$, $(0,1)^7=(3,1)$, $(0,1)^8=(4,0)=(0,0)$. Portanto, $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$ é isomorfo a $\mathbb{Z}_8$.

- A solução $(1,3)$ conduz ao grupo cíclico $\mathbb{Z}_8$. Neste caso temos, um produto cíclico $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$, e a respectiva operação $(i,j)*(s,t)$ é dada por

$$(i,j)*(s,t) = \begin{cases} ((i+s+3)mod 4\ ,\ 0) & \text{se}\quad j+t=2 \\ ((i+s)mod 4\ ,\ j+t) & \text{se}\quad j+t<2. \end{cases}$$

Considere o elemento $(0,1) \in \mathbb{Z}_{4(\mu)}\mathbb{Z}_2$. Temos, $(0,1)^2=(3,0)$, $(0,1)^3=(3,1)$, $(0,1)^4=(2,0)$, $(0,1)^5=(2,1)$, $(0,1)^6=(1,0)$, $(0,1)^7=(1,1)$, $(0,1)^8=(1+3,0)=(0,0)$.

$\mathbb{Z}_{4(\sigma)}\mathbb{Z}_2$	(0,0)	(1,0)	(2,0)	(3,0)	(1,1)	(3,1)	(0,1)	(2,1)
(0,0)	(0,0)	(1,0)	(2,0)	(3,0)	(1,1)	(3,1)	(0,1)	(2,1)
(1,0)	(1,0)	(2,0)	(3,0)	(0,0)	(2,1)	(0,1)	(1,1)	(3,1)
(2,0)	(2,0)	(3,0)	(0,0)	(1,0)	(3,1)	(1,1)	(2,1)	(0,1)
(3,0)	(3,0)	(0,0)	(1,0)	(2,0)	(0,1)	(2,1)	(3,1)	(1,1)
(1,1)	(1,1)	(0,1)	(3,1)	(2,1)	(0,0)	(2,0)	(1,0)	(3,0)
(3,1)	(3,1)	(2,1)	(1,1)	(0,1)	(2,0)	(0,0)	(3,0)	(1,0)
(0,1)	(0,1)	(3,1)	(2,1)	(1,1)	(3,0)	(1,0)	(0,0)	(2,0)
(2,1)	(2,1)	(1,1)	(0,1)	(3,1)	(1,0)	(3,0)	(2,0)	(0,0)

Tabela 2.2: **Tabela de Cayley para** $\mathbb{Z}_{4(\sigma)}\mathbb{Z}_2$

Portanto, $\mathbb{Z}_{4(\mu)}\mathbb{Z}_2$ é isomorfo a $\mathbb{Z}_8$.

- A solução (3,0) conduz ao grupo diedral $\mathbb{D}_4$ (as simetrias do quadrado). A operação $(i,j) * (r,s)$ é dada por

$$(i,j) * (r,s) = \Big((i + r.3^j) mod\, 4 \ , \ (j+s) mod\, 2\Big).$$

Por exemplo, se considerarmos os pares (1,1) e (2,0), então

$$(1,1) * (2,0) = \Big((1 + 2.3^1) mod\, 4 \ , \ (1+0) mod\, 2\Big) = (3,1).$$

A tabela de Cayley para $\mathbb{Z}_{4(\sigma)}\mathbb{Z}_2$ é mostrada na Tabela 2.2.

Comparando as Tabelas 2.2 e 2.3, podemos ver que $\theta : \mathbb{Z}_{4(\sigma)}\mathbb{Z}_2 \to \mathbb{D}_4$ dado por;

$$\begin{aligned} \theta(0,0) &= R_0 \qquad \theta(1,1) = d_1 \\ \theta(1,0) &= R_1 \qquad \theta(3,1) = d_2 \\ \theta(2,0) &= R_2 \qquad \theta(0,1) = V \\ \theta(3,0) &= R_3 \qquad \theta(2,1) = H, \end{aligned}$$

é um isomorfismo e $\mathbb{Z}_{4(\sigma)}\mathbb{Z}_2 \overset{\theta}{\cong} \mathbb{D}_4$.

$\mathbb{D}_4$	R_0	R_1	R_2	R_3	d_1	d_2	V	H
R_0	R_0	R_1	R_2	R_3	d_1	d_2	V	H
R_1	R_1	R_2	R_3	R_0	H	V	d_1	d_2
R_2	R_2	R_3	R_0	R_1	d_2	d_1	H	V
R_3	R_3	R_0	R_1	R_2	V	H	d_2	d_1
d_1	d_1	V	d_2	H	R_0	R_2	R_1	R_3
d_2	d_2	H	d_1	V	R_2	R_0	R_3	R_1
V	V	d_2	H	d_1	R_3	R_1	R_0	R_2
H	H	d_1	V	d_2	R_1	R_3	R_2	R_0

Tabela 2.3: **Tabela de Cayley para** $\mathbb{D}_4$

- A solução $(3,2)$ conduz ao grupo dos quatérnios $\mathbb{Q}_3$. A operação $(i,j)*(s,t)$ é dada por

$$(i,j)*(s,t) = \begin{cases} ((i+s.3^j+2)mod\,4 \ ; \ (j+t)mod\,2) & \text{se} \quad j+t \geq 2 \\ ((i+s.3^j)mod\,4 \ ; \ (j+t)mod\,2) & \text{se} \quad j+t < 2. \end{cases}$$

Por exemplo, $(2,1)*(1,1) = ((2+1.3^1+2)mod\,4, (1+1)mod\,2) = (3,0)$. A tabela de Cayley para $\mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$ é mostrada na Tabela 2.4. Portanto, da associação

$$\begin{array}{ll} (0,0) \mapsto \rho_0 & (1,1) \mapsto \lambda_1 \\ (1,0) \mapsto \rho_1 & (3,1) \mapsto \lambda_2 \\ (2,0) \mapsto \rho_2 & (0,1) \mapsto \xi_1 \\ (3,0) \mapsto \rho_3 & (2,1) \mapsto \xi_2, \end{array}$$

concluímos que $\mathbb{Q}_3 \cong \mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$.

2.2.3 Construção multinível de produtos de Schreier

Seja $S \subset \mathbb{R}^n$ um conjunto discreto de pontos de um espaço Euclidiano com distância mínima dada por $d_1 = min\{\|x_i - x_j\| \ : \ x_i \neq x_j, x_i, x_j \in S\}$. Considere $S^2 = S \times S$, a distância

$\mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$	(0,0)	(1,0)	(2,0)	(3,0)	(1,1)	(3,1)	(0,1)	(2,1)
(0,0)	(0,0)	(1,0)	(2,0)	(3,0)	(1,1)	(3,1)	(0,1)	(2,1)
(1,0)	(1,0)	(2,0)	(3,0)	(0,0)	(2,1)	(0,1)	(1,1)	(3,1)
(2,0)	(2,0)	(3,0)	(0,0)	(1,0)	(3,1)	(1,1)	(2,1)	(0,1)
(3,0)	(3,0)	(0,0)	(1,0)	(2,0)	(0,1)	(2,1)	(3,1)	(1,1)
(1,1)	(1,1)	(0,1)	(3,1)	(2,1)	(2,0)	(0,0)	(3,0)	(1,0)
(3,1)	(3,1)	(2,1)	(1,1)	(0,1)	(0,0)	(2,0)	(1,0)	(3,0)
(0,1)	(0,1)	(3,1)	(2,1)	(1,1)	(1,0)	(3,0)	(2,0)	(0,0)
(2,1)	(2,1)	(1,1)	(0,1)	(3,1)	(3,0)	(1,0)	(0,0)	(2,0)

Tabela 2.4: **Tabela de Cayley para** $\mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$

$\mathbb{Q}_3$	ρ_0	ρ_1	ρ_2	ρ_3	λ_1	λ_2	ξ_1	ξ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	λ_1	λ_2	ξ_1	ξ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	ξ_2	ξ_1	λ_1	λ_2
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	λ_2	λ_1	ξ_2	ξ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	ξ_1	ξ_2	λ_2	λ_1
λ_1	λ_1	ξ_1	λ_2	ξ_2	ρ_2	ρ_0	ρ_3	ρ_1
λ_2	λ_2	ξ_2	λ_1	ξ_1	ρ_0	ρ_2	ρ_1	ρ_3
ξ_1	ξ_1	λ_2	ξ_2	λ_1	ρ_1	ρ_3	ρ_2	ρ_0
ξ_2	ξ_2	λ_1	ξ_1	λ_2	ρ_3	ρ_1	ρ_0	ρ_2

Tabela 2.5: **Tabela de Cayley para** $\mathbb{Q}_3$

mínima de S^2 é dada por $d_2 = min\{\|y_i - y_j\| : y_i \neq y_j,\ y_i, y_j \in S^2\}$. Temos que $d_2 \geq d_1$.

Por outro lado, se $\Gamma(S)$ é o grupo de simetrias de S então $\Gamma(S)^2 = \Gamma(S)_{\oplus}\Gamma(S)$ será o grupo de simetrias de S^2. Em geral, dado $S \subset \mathbb{R}^n$ considere S^m como sendo m cópias de S, isto é , $S^m = \overbrace{S \times \ldots \times S}^{m}$ e a distância mínima de S^m dada por $d_m = min\{\|z_i - z_j\| : z_i \neq z_j,\ z_i, z_j \in S^m\}$, teremos que $d_1 \leq d_2 \leq \ldots \leq d_m$ e $\Gamma(S)^m$ é o grupo de simetrias de S^m.

Este é o principio da codificação multinível. Dado um código Euclidiano sobre S com distância livre de código d_{free_1} que é diretamente proporcional a d_1, obteremos um código Euclidiano sobre S^m com distância livre de código d_{free_m} que é diretamente proporcional a d_m. Portanto teremos que $d_{free_m} \geq d_{free_1}$.

Mas o processo de obtenção do código Euclidiano sobre S^m passa pela obtenção do grupo $\Gamma(S)^m$, que pode ser decomposto de várias maneiras. Isto significa que existem várias formas de construir o produto direto de m-cópias $\Gamma(S)^m$, incluindo o uso de produtos de Schreier. Isto é mostrado no seguinte teorema que tem uma semelhança com o Teorema 5 de [9].

Teorema 2.3 *Considere uma coleção finita de produtos de Schreier* $\left\{H_{i(\sigma_i,\mu_i)}K_i\right\}_{i=1}^{n}$. *Então, o produto cartesiano multinível* $(H_1 \times \ldots \times H_n) \times (K_1 \times \ldots \times K_n)$ *pode ser convertido em um produto de Schreier multinível* $(H_{1\oplus} \ldots_{\oplus} H_n)_{(\overline{\sigma},\overline{\mu})}(K_{1\oplus} \ldots_{\oplus} K_n)$, *se o mapeamento* $\overline{\sigma} : K_{1\oplus} \ldots_{\oplus} K_n \rightarrow Aut(H_{1\oplus} \ldots_{\oplus} H_n)$ *for definido por*

$$\overline{\sigma}(k_1, \ldots, k_n) = (\sigma_1(k_1), \ldots, \sigma_n(k_n)) : H_{1\oplus} \ldots_{\oplus} H_n \rightarrow H_{1\oplus} \ldots_{\oplus} H_n$$

de tal maneira que

$$(\sigma_1(k_1), \ldots, \sigma_n(k_n))(h_1, \ldots, h_n) = (\sigma_1(k_1)(h_1), \ldots, \sigma_n(k_n)(h_n)),$$

e se o mapeamento $\overline{\mu} : (K_{1\oplus} \ldots_{\oplus} K_n) \times (K_{1\oplus} \ldots_{\oplus} K_n) \rightarrow H_{1\oplus} \ldots_{\oplus} H_n$ *for definido por*

$$\overline{\mu}(k, l) = (\mu_1(k_1, l_1), \ldots, \mu_n(k_n, l_n)),$$

onde $k = (k_1, \ldots, k_n) \in (K_{1\oplus} \ldots_{\oplus} K_n)$, *e* $l = (l_1, \ldots, l_n) \in (K_{1\oplus} \ldots_{\oplus} K_n)$.

Prova : Para $(\mathbf{x};\mathbf{q}) = (x_1,\ldots,x_n \ ; \ q_1,\ldots,q_n)$ e $(\mathbf{y},\mathbf{r}) = (y_1,\ldots,y_n \ ; \ r_1,\ldots,r_n) \in (H_{1\oplus}\ldots_{\oplus} H_n) \times (K_{1\oplus}\ldots_{\oplus} K_n)$. Vamos definir $(\mathbf{x};\mathbf{q}) * (\mathbf{y};\mathbf{r})$ como

$$\begin{aligned}(\mathbf{x};\mathbf{q}) * (\mathbf{y};\mathbf{r}) &= (\mathbf{x}.\overline{\sigma}(\mathbf{q})(\mathbf{y}).\overline{\mu}(\mathbf{q},\mathbf{r}) \ ; \ \mathbf{q}.\mathbf{r}) \\ &= ((x_1,\ldots,x_n).(\sigma_1(q_1)(y_1),\ldots,\sigma_n(q_n)(y_n)).(\mu_1(q_1,r_1),\ldots,\mu_n(q_n,r_n) \ ; \ \mathbf{q}.\mathbf{r}) \\ &= (x_1.\sigma_1(q_1)(y_1).\mu_1(q_1,r_1),\ldots,x_n.\sigma_n(q_n)(y_n).\mu_n(q_n,r_n) \ ; \ q_1r_1,\ldots,q_nr_n)\end{aligned}$$

Com esta operação, $(H_{1\oplus}\ldots_{\oplus} H_n)_{(\overline{\sigma},\overline{\mu})}(K_{1\oplus}\ldots_{\oplus} K_n)$ é um grupo. ■

Corolário 2.3.1 *Dado um grupo G, se existir uma família de produtos de Schreier $\left\{H_{i(\sigma_i,\mu_i)}K_i\right\}_{i=}^{n}$ tal que $G \cong H_{i(\sigma_i,\mu_i)}K_i$ para $i = 1,\ldots,n$, então $G^n \cong (H_{1\oplus}\ldots_{\oplus} H_n)_{(\overline{\sigma},\overline{\mu})}(K_{1\oplus}\ldots_{\oplus} K_n)$, onde $G^n \cong G_{\oplus}\ldots_{\oplus} G$.*

Prova : Defina o mapeamento auxiliar $\phi : (H_{1\oplus}\ldots_{\oplus} H_n)_{(\overline{\sigma},\overline{\mu})}(K_{1\oplus}\ldots_{\oplus} K_n) \to G^n$ como

$$\phi(\mathbf{x};\mathbf{q}) = \phi(x_1,\ldots,x_n \ ; \ q_1,\ldots,q_n) = (g_1,\ldots,g_n),$$

onde $g_i = (x_i,q_i) \in H_{i(\sigma_i,\mu_i)}K_i$. Assim, como ϕ é bijetivo, concluímos que o mesmo é um isomorfismo. ■

2.2.4 Exemplos

Exemplo 2.4 *Iremos construir o produto direto $\mathbb{Z}_{8\oplus}\mathbb{Z}_2$ como um produto multinível*

$$\mathbb{Z}_{8\oplus}\mathbb{Z}_2 \cong \mathbb{Z}_{4(\mu')}\mathbb{Z}_2^2.$$

Para tal, considere o produto cíclico $\mathbb{Z}_8 = \mathbb{Z}_{4(\mu)}\mathbb{Z}_2$ correspondente à solução $(1,1)$ do Exemplo 2.3. Considere o produto direto trivial $\mathbb{Z}_2 = \{e\}_{\oplus}\mathbb{Z}_2$. Então, pelo Teorema 2.3, temos que

$$\mathbb{Z}_{8\oplus}\mathbb{Z}_2 \cong (\mathbb{Z}_{4\oplus}\{e\})_{(\overline{\mu})}(\mathbb{Z}_{2\oplus}\mathbb{Z}_2).$$

O mapeamento $\overline{\mu} : \mathbb{Z}_{2\oplus}\mathbb{Z}_2 \times \mathbb{Z}_{2\oplus}\mathbb{Z}_2 \to \mathbb{Z}_{4\oplus}\{e\}$ é dado por $\overline{\mu}(k_1,k_2;l_1,l_2) = (\mu(k_1,l_1),e)$. Portanto, temos que

$$\mathbb{Z}_{8\oplus}\mathbb{Z}_2 \cong \mathbb{Z}_{4(\mu')}\mathbb{Z}_2^2,$$

onde $\mu' : {\mathbb{Z}_2}^2 \times {\mathbb{Z}_2}^2 \to \mathbb{Z}_4$ é dado por $\mu'(k_1, k_2; l_1, l_2) = \mu(k_1, l_1)$. A operação $(h_1; k_1, k_2) * (h_2; l_1, l_2)$ em $\mathbb{Z}_{4(\mu')}{\mathbb{Z}_2}^2$ é dada por

$$(h_1; k_1, k_2) * (h_2; l_1, l_2) = (h_1.(h_2).\mu'(k_1, k_2; l_1, l_2); (k_1, k_2).(l_1, l_2))$$

$$= (h_1.(h_2).\mu(k_1, l_1); k_1.l_1, k_2.l_2)$$

$$= ((h_1 + h_2 + \mu(k_1, l_1))mod\,4\,,\ (k_1 + l_1)mod\,2, (k_2 + l_2)mod\,2).$$

Por exemplo, para (3;0,1) e (2;1,0) pertencentes a $\mathbb{Z}_{4(\mu')}{\mathbb{Z}_2}^2$, temos $(3; 1, 1) * (2; 1, 0) = ((3 + 2 + 1)mod\,4; (1 + 1)mod\,2, (1 + 0)mod\,2)$ = (2;0,1).

Exemplo 2.5 *Construção multinível do grupo* $\mathbb{Q}_{3\oplus}\mathbb{D}_4$, *onde*

$$\mathbb{Q}_{3\oplus}\mathbb{D}_4 \cong \mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)$$

Sabemos do Exemplo 2.3 que $\mathbb{Q}_3 \cong \mathbb{Z}_{4(\sigma,\mu)}\mathbb{Z}_2$. Por outro lado, se $\{e\}$ é o grupo trivial unitário, então $\mathbb{D}_4 \cong \{e\}_{\oplus}\mathbb{D}_4$. Logo, pelo Teorema 2.3, temos que

$$\mathbb{Q}_{3\oplus}\mathbb{D}_4 \cong (\mathbb{Z}_{4\oplus}\{e\})_{(\overline{\sigma},\overline{\mu})}(\mathbb{Z}_{2\oplus}\mathbb{D}_4).$$

O mapeamento $\overline{\sigma} : \mathbb{Z}_{2\oplus}\mathbb{D}_4 \to Aut(\mathbb{Z}_{4\oplus}\{e\})$ é dado por $\overline{\sigma}(k_1, k_2)(h, e) = (\sigma(k_1)(h), e)$, $k_1 \in \mathbb{Z}_2$, $k_2 \in \mathbb{D}_4$, $h \in \mathbb{Z}_4$, $e \in \{e\}$. O mapeamento $\overline{\mu} : \mathbb{Z}_{2\oplus}\mathbb{D}_4 \times \mathbb{Z}_{2\oplus}\mathbb{D}_4 \to \mathbb{Z}_{4\oplus}\{e\}$ é dado por $\overline{\mu}(k_1, k_2; l_1, l_2) = (\mu(k_1, l_1), e)$. Portanto, podemos escrever

$$\mathbb{Q}_{3\oplus}\mathbb{D}_4 \cong \mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4),$$

onde $\sigma' : \mathbb{Z}_{2\oplus}\mathbb{D}_4 \to Aut(\mathbb{Z}_4)$ é dado por $\sigma'(k_1, k_2)(h) = \sigma(k_1)(h)$ e $\mu' : \mathbb{Z}_{2\oplus}\mathbb{D}_4 \times \mathbb{Z}_{2\oplus}\mathbb{D}_4 \to \mathbb{Z}_4$ é dado por $\mu'(k_1, k_2; l_1, l_2) = \mu(k_1, l_1)$. A operação $(h_1; k_1, k_2) * (h_2; l_1, l_2)$ em $\mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)$ pode ser escrita como

$$(h_1; k_1, k_2) * (h_2; l_1, l_2) = (h_1.\sigma'(k_1, k_2)(h_2).\mu'(k_1, k_2; l_1, l_2); (k_1, k_2).(l_1, l_2))$$

$$= (h_1.\sigma(k_1)(h_2).\mu(k_1, l_1); k_1.l_1, k_2.l_2)$$

$$= ((h_1 + \sigma(k_1)(h_2) + \mu(k_1, l_1))mod\,4\,,\ (k_1 + l_1)mod\,2, (k_2.l_2)mod\,\mathbb{D}_4),$$

onde $(k_2.l_2) mod \mathbb{D}_4$ significa que k_2, $l_2 \in \mathbb{D}_4$ e portanto a operação $k_2.l_2$ é realizada no grupo $\mathbb{D}_4$.

Por exemplo, para $(3, 1R_1)$ e $(1, 0d_1)$ pertencentes a $\mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)$, temos $(3, 1R_1) * (1, 0d_1) = (3 + \sigma(1)(1) + \mu(1, 1), 1 + 1, R_1 d_1)$ =$(3 + 1.3^1 + 2, 0, H)$ =$(0, 0H)$.

2.3 Decomposição de Grupos

Este é o problema inverso do problema de extensão de grupos. Sejam G e H grupos tais que H é um subgrupo normal de G, isto é, $H \lhd G$. Seja $\mathcal{N}_G$ a classe dos subgrupos normais de G, isto é ,

$$\mathcal{N}_G = \{H \ : \ H \lhd G\}. \tag{2.16}$$

Teorema 2.4 *Se $N \in \mathcal{N}_G$, então existem σ e μ como na Definição 2.2 tais que $G \cong N_{(\sigma,\mu)}\frac{G}{N}$.*

Prova: Vide Apêndice B. ∎

Sejam N_1 , N_2 $\in \mathcal{N}_G$, tais que $N_1 \ncong N_2$. Sejam K_1, K_2 e H_1, H_2 grupos tais que $N_i \cong H_i$ e $K_i \cong \frac{G}{N_i}$, $i = 1, 2$. Então, de acordo com a demonstração do Teorema 2.4, G pode ser decomposto em pelo menos dois diferentes produtos de Schreier $G \cong H_{1(\sigma_1,\mu_1)}K_1$ e $G \cong H_{2(\sigma_2,\mu_2)}K_2$ (Vide os Exemplos 2.1 e 2.3 onde $\mathbb{D}_4 \cong \mathbb{Z}^2_{2(\sigma_1)}\mathbb{Z}_2$ e $\mathbb{D}_4 \cong \mathbb{Z}_{4(\sigma)}\mathbb{Z}_2$). Para cada $g \in G$ existe um único par $(h_i, k_i) \in H_{i(\sigma_i,\mu_i)}K_i$, $i = 1, 2$, tal que $g = (h_i, k_i)$. Note que esta é uma generalização do **Teorema Chinês do Resto.**

Dado um grupo G com pelo menos um subgrupo normal N não trivial, isto é $N \neq e_G$ e $N \neq G$, considere a família $\{H_{i(\sigma_i,\mu_i)}K_i\}_{i=1}^{\infty}$ de todas as decomposições não triviais de G, isto é $|H_i| \neq 1$ e $|K_i| \neq 1$ para todo $i \in \mathbb{N}$.

Se para algum $j \in \mathbb{N}$, $\sigma_j(k_j) = id$, $\forall k_j \in K_j$ e $\mu_j(k_{j1}, k_{j2}) = e_{H_j}$, $\forall (k_{j1}, k_{j2}) \in K_j \times K_j$, então temos que G pode ser decomposto em um produto direto, pois $G \cong H_{j\oplus}K_j$. Neste caso, e com um certo abuso de linguagem, diremos que G pertence à *classe dos produtos diretos.*

No caso em que G não possa ser decomposto como um produto direto, então devemos procurar na família $\{H_{i(\sigma_i,\mu_i)}K_i\}_{i=1}^{\infty}$ uma possível decomposição como um produto cíclico. Se existir algum, diremos que G pertence à *classe dos produtos cíclicos* não triviais.

No caso em que G não possa ser decomposto nem como produto direto nem como produto cíclico, então devemos procurar na família $\{H_{i(\sigma_i,\mu_i)}K_i\}_{i=1}^{\infty}$ uma possível decomposição como um produto semidireto. Se existir um, diremos que G pertence à *classe dos produtos semidiretos* não triviais.

Finalmente, se G não puder ser decomposto como produto direto ou como produto cíclico ou como produto semidireto, então teremos que G pertence à *classe dos produtos de Schreier* não triviais.

Esta classificação dos grupos é ilustrada na Fig. 2.1. Por exemplo, o grupo dos quatérnios $\mathbb{Q}_3$ pertence à classe dos produtos de Schreier não triviais pois o mesmo não possui decomposição como produto semidireto, ou como produto cíclico, ou como produto direto. O grupo das simetrias do quadrado $\mathbb{D}_4$ pertence à classe dos produtos semidiretos não triviais. O grupo cíclico $\mathbb{Z}_{2^3}$ pertence à classe dos produtos cíclicos não triviais. Estes três grupos são analisados no Exemplo 2.3.

2.3.1 Decomposição máxima

Definição 2.3 *[11] Seja G um grupo. Uma* **série normal** *de G é uma família de subgrupos $\{G_i\}_{i=0}^{\infty}$ tal que $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n \rhd \ldots$*

$\diamond$

Quando a série normal é finita e tal que cada G_{i+1} é máxima em G_i ou $G_i = G_{i+1}$, então a série normal é denominada **série de composição** de G, [11].

Proposição 2.3 *Dado um grupo G, seja $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n \rhd \ldots$ uma série normal de G. Para cada i, seja Q_i o grupo $Q_i = \frac{G_i}{G_{i+1}}$. Então, existem famílias de aplicações $\{\sigma_i\}_{i=1}^{\infty}$, e $\{\mu_i\}_{i=1}^{\infty}$ tais que G tem a seguinte decomposição*

$$G \cong \left[\left[\left[\ldots\left[\left[\ldots Q_n\right]_{(\sigma_n,\mu_n)} Q_{n-1}\right]_{(\sigma_{n-1},\mu_{n-1})}\ldots\right]_{(\sigma_2,\mu_2)} Q_1\right]_{(\sigma_1,\mu_1)} Q_0\right].$$

Prova:

$G_1 \lhd G_0 = G$, então pelo Teorema 2.4 existem σ_1 e μ_1 tais que, $G \cong G_1(\sigma_1, \mu_1)Q_0$.

$G_2 \lhd G_1$, então pelo Teorema 2.4 existem σ_2 e μ_2 tais que, $G_1 \cong G_2(\sigma_2, \mu_2)Q_1$. Disto decorre que

$$G \cong \left[G_{2(\sigma_2,\mu_2)}Q_1\right]_{(\sigma_1,\mu_1)} Q_0. \tag{2.17}$$

Agora, $G_3 \lhd G_2$, então pelo Teorema 2.4 existem σ_3 e μ_3 tais que, $G_2 \cong G_3(\sigma_3, \mu_3)Q_2$. Substituindo em (2.17) e continuando este procedimento, a proposição fica demonstrada. ■

A decomposição de grupos estabelecida na Proposição 2.3 é dita **máxima** quando a correspondente série normal é uma série de composição $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e_G\}$. O Teorema de **Jordan-Hölder** (vide Apêndice C), estabelece que a série de composição de um grupo G, quando G possuir alguma, é essencialmente única. Disto podemos concluir que

Teorema 2.5 *Se um grupo G possui série de composição $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e_G\}$, então G possui uma única decomposição máxima dada por*

$$G \cong \left[\left[\left[\ldots\left[Q_{n(\sigma_n,\mu_n)}Q_{n-1}\right]_{(\sigma_{n-1},\mu_{n-1})}\ldots\right]_{(\sigma_2,\mu_2)} Q_1\right]_{(\sigma_1,\mu_1)} Q_0\right],$$

onde $Q_i \cong \frac{G_i}{G_{i+1}}$.

2.3.2 Exemplos

Exemplo 2.6 *Em [10], Ungerboeck, apresenta um esquema de modulação codificada usando os sinais 8-PSK e um codificador de 4 estados. A estratégia utilizada nesta associação de modulação codificada foi a de particionar o conjunto de sinais 8-PSK em sucessivos subconjuntos com distâncias Euclidianas crescentes via o esquema de particionamento de conjuntos. A conseqüência deste particionamento é o de rotular os sinais 8-PSK na forma binária. O objetivo deste exemplo é mostrar, via o produto de Schreier, a decomposição do grupo $\mathbb{Z}_8$ associado ao particionamento do 8-PSK, isto é , $\mathbb{Z}_8 \cong (\mathbb{Z}_{2(\mu_1)}\mathbb{Z}_2)_{(\mu)}\mathbb{Z}_2$.*

Considere o Exemplo 2.3, onde a solução $(1,1)$ da equação (2.11) implica o mapeamento $\mu : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ dado por $\mu(k_1,k_2) = 0 \in \mathbb{Z}_4$ se $k_1 + k_2 < 2$, e $\mu(1,1) = 1 \in \mathbb{Z}_4$ se $k_1 + k_2 = 2$. Assim, vimos que o grupo $\mathbb{Z}_8$ decompõe-se como $\mathbb{Z}_8 \overset{\theta}{\cong} \mathbb{Z}_{4(\mu)}\mathbb{Z}_2$, onde θ é o isomorfismo $\theta : \mathbb{Z}_8 \to \mathbb{Z}_{4(\mu)}\mathbb{Z}_2$ dado por

$$\begin{aligned} \theta(0) &= 00 \quad \theta(1) = 01 \\ \theta(2) &= 10 \quad \theta(3) = 11 \\ \theta(4) &= 20 \quad \theta(5) = 21 \\ \theta(6) &= 30 \quad \theta(7) = 31. \end{aligned}$$

Por outro lado, como $\{0,2\} \lhd \mathbb{Z}_4$, e $\{0,2\} \cong \mathbb{Z}_2$, pelo teorema da decomposição máxima, temos que existe $\mu_1 : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ tal que $\mathbb{Z}_4 \overset{\theta_1}{\cong} \mathbb{Z}_{2(\mu_1)}\mathbb{Z}_2$, para algum isomorfismo θ_1. Este μ_1 está definido por $\mu_1(l_1,l_2) = 0 \in \mathbb{Z}_2$ se $l_1 + l_2 < 2$, e $\mu_1(1,1) = 1 \in \mathbb{Z}_2$. A operação em $\mathbb{Z}_{2(\mu_1)}\mathbb{Z}_2$ é dada por

$$(i,j) * (s,t) = \begin{cases} ((i+s+1) mod 2 \ , \ 0) & \text{se} \quad j+t = 2 \\ ((i+s) mod 2 \ , \ j+t) & \text{se} \quad j+t < 2. \end{cases}$$

Assim, $(0,1)^2 = (1,0)$, $(0,1)^3 = (1,1)$, $(0,1)^4 = (0,0)$. Portanto, $\theta_1 : \mathbb{Z}_4 \to \mathbb{Z}_{2(\mu_1)}\mathbb{Z}_2$ é dado por

$$\begin{aligned} \theta_1(0) &= 00 \quad \theta_1(1) = 01 \\ \theta_1(2) &= 10 \quad \theta_1(3) = 11. \end{aligned}$$

Então, o isomorfismo $\theta_2 : \mathbb{Z}_{4(\mu)}\mathbb{Z}_2 \to (\mathbb{Z}_{2(\mu_1)}\mathbb{Z}_2)_{(\mu)}\mathbb{Z}_2$ está definido e o mesmo é dado por

$$\begin{aligned} \theta_2(00) &= \theta_1(0)0 = 000 \quad \theta_2(01) = \theta_1(0)1 = 001 \\ \theta_2(10) &= \theta_1(1)0 = 010 \quad \theta_2(11) = \theta_1(1)1 = 011 \\ \theta_2(20) &= \theta_1(2)0 = 100 \quad \theta_2(21) = \theta_1(2)1 = 101 \\ \theta_2(30) &= \theta_1(3)0 = 110 \quad \theta_2(31) = \theta_1(3)1 = 111. \end{aligned}$$

Finalmente, tomando o isomorfismo composição $\theta_3 = \theta_2 \circ \theta : \mathbb{Z}_8 \to (\mathbb{Z}_{2(\mu_1)}\mathbb{Z}_2)_{(\mu)}\mathbb{Z}_2$, dado por $\theta_3(x) = \theta_2(\theta(x))$, resulta no "mapeamento por partições " de Ungerboeck. Com isso acabamos de provar que o "mapeamento por partições " é um isomorfismo dado por

$$\theta_3(0) = 000 \quad \theta_3(1) = 001$$
$$\theta_3(2) = 010 \quad \theta_3(3) = 011$$
$$\theta_3(4) = 100 \quad \theta_3(5) = 101$$
$$\theta_3(6) = 110 \quad \theta_3(7) = 111.$$

Exemplo 2.7 *Neste exemplo, iremos considerar G como sendo um grupo abeliano finito, ao invés do caso $G = \mathbb{Z}_8$ do exemplo anterior.*

Pelo teorema fundamental dos grupos abelianos finitamente gerados, temos que G pode ser decomposto como

$$G \cong \mathbb{Z}_{{p_1}^{r_1}} \oplus \mathbb{Z}_{{p_2}^{r_2}} \oplus \ldots \mathbb{Z}_{{p_n}^{r_n}} \oplus \mathbb{Z}_{{p_{n+1}}^{r_{n+1}}}, \tag{2.18}$$

onde os p_i são primos, com $p_i \neq p_j$ se $i \neq j$. Sejam G_i subgrupos de G definidos por

$$\begin{aligned} G_n &\cong \{0\} \\ G_{n-1} &\cong \mathbb{Z}_{{p_1}^{r_1}} \\ G_{n-2} &\cong \mathbb{Z}_{{p_1}^{r_1}} \oplus \mathbb{Z}_{{p_2}^{r_2}} \\ &\vdots \\ G = G_0 &\cong \mathbb{Z}_{{p_1}^{r_1}} \oplus \mathbb{Z}_{{p_2}^{r_2}} \oplus \ldots \mathbb{Z}_{{p_n}^{r_n}} \oplus \mathbb{Z}_{{p_{n+1}}^{r_{n+1}}}. \end{aligned} \tag{2.19}$$

Temos que $\{e_G\} \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_1 \lhd G_0 = G$ é uma série normal de G, porém a mesma não é necessariamente a série de composição. Portanto, concluímos que a Proposição 2.3, é uma generalização do teorema fundamental dos grupos abelianos finitamente gerados(para grupos finitos). Note que a decomposição dada por (2.18) não é máxima, se algum r_i for tal que $r_i > 1$. Suponha que $r_i = r_1 > 1$, então o grupo cíclico $\mathbb{Z}_{{p_1}^{r_1}}$ tem a série de composição

$$\{0\} \lhd \mathbb{Z}_{p_1} \lhd \mathbb{Z}_{{p_1}^2} \ldots \lhd \mathbb{Z}_{{p_1}^{r_1}}.$$

Como $\frac{\mathbb{Z}_{{p_1}^{j+1}}}{\mathbb{Z}_{{p_1}^j}} \cong \mathbb{Z}_{p_1}$, para $j = 1, 2, \ldots, r_1$, então pela Proposição 2.3, temos

$$\mathbb{Z}_{{p_1}^{r_1}} \cong \left[\left[\ldots\left[\mathbb{Z}_{p_1(\mu_{r_1})}\mathbb{Z}_{p_1(\mu_{r_1-1})}\cdots\right]_{(\mu_2)}\mathbb{Z}_{p_1}\right]_{(\mu_1)}\mathbb{Z}_{p_1}\right]. \tag{2.20}$$

A decomposição (2.20) é realizada somente por produtos cíclicos, pois a Proposição 2.1 diz que se σ é não trivial, então o grupo é não abeliano, porém $\mathbb{Z}_{{p_1}^{r_1}}$ é um grupo abeliano. Realizando de maneira similar à decomposição de $\mathbb{Z}_{{p_1}^{r_1}}$ para cada $\mathbb{Z}_{{p_i}^{r_i}}$ e substituindo em (2.18), obteremos a decomposição máxima do grupo abeliano finito G.

Capítulo 3

Códigos de Schreier

Dado um conjunto discreto Euclidiano $S \subset \mathbb{R}^n$, considere o grupo das simetrias de S, denotado por $\Gamma(S)$, cujos elementos são mapeamentos $g : S \to \mathbb{R}^n$ tais que

- $\|g(s)\| = \|s\|$, $\forall\, s \in S$: Preservação da norma Euclidiana.
- $g(s) \in S$, $\forall\, s \in S$: Invariância de S.
- A operação de grupo de $\Gamma(S)$ é a composição de mapeamentos $g_1 {}_o g_2$.

Quando $\Gamma(S)$ é tal que para cada $s \in S$ existe $g \in \Gamma(S)$ tal que $s = g(s_0)$, para algum $s_0 \in S$, então dizemos que $\Gamma(S)$ atua transitivamente sobre S. O ponto $s_0 \in S$ é denominado como a *semente* ou *gerador* de S. Podem existir vários geradores de S.

Para se obter códigos Euclidianos de uma maneira prática e efetiva os *group codes* considerados devem ser constituídos por seqüências de simetrias, denominados de *códigos de simetrias*. Um código de simetria $\mathcal{G}$ é um subgrupo do produto direto infinito de grupos $\oplus_{k\in\mathbb{Z}} G_k = \ldots {}_{\oplus} G_{-i} {}_{\oplus} \ldots\ldots {}_{\oplus} G_{-1} {}_{\oplus} G_0 {}_{\oplus} \ldots G_1 {}_{\oplus} \ldots\ldots {}_{\oplus} G_i {}_{\oplus} \ldots$, $i \in \mathbb{N}$, onde para cada $k \in \mathbb{Z}$, $G_k = \Gamma(S_k)$ é o grupo de simetrias do conjunto discreto $S_k \subset \mathbb{R}^{n_k}$.

O código Euclidiano $\mathcal{C}$ casado a $\mathcal{G} \subset \oplus_{k\in\mathbb{Z}} G_k$ é obtido a partir de uma seqüência semente $\{x_k\}_{k\in\mathbb{Z}}$, $x_k \in \mathbb{R}^{n_k}$. Isto significa que cada palavra código $\{y_k\}_{k\in\mathbb{Z}} \in \mathcal{C}$ é tal que para cada $k \in \mathbb{Z}$, $y_k = g_k(x_k)$, $g_k \in G_k$. Estes códigos Euclidianos são denominados *códigos geometricamente uniformes*.

Note que cada $S_k \subset \mathbb{R}^{n_k}$ pode ter cardinalidade infinita, mesmo sendo discreto. Em tal caso a cardinalidade dos estados do código poderá ser também infinita. Uma outra observação é que quando os grupos de simetrias G_k são diferentes entre si, então o código será variante no tempo. A complexidade de um código que é variante no tempo e que possui cardinalidade de estados infinita é muito maior do que o de um código invariante no tempo e com número finito de estados, que é um código baseado num conjunto discreto Euclidiano $S \subset \mathbb{R}^n$ com cardinalidade $|S|$ finita, e tal que $S_k = S \subset \mathbb{R}^n$ para todo $k \in \mathbb{Z}$. Neste caso teremos que $G_k = G$, $\forall\, k \in \mathbb{Z}$ com $|G|$ finito. Agora, seja $G^{\mathbb{Z}} = \oplus_{k\in\mathbb{Z}} G_k$, $G_k = G$, $\forall k \in \mathbb{Z}$, considere um subgrupo $\mathcal{G} \subset G^{\mathbb{Z}}$, temos que $\mathcal{G}$ é um código de simetrias invariante no tempo e com número finito de estados. Esta classe de códigos de simetrias invariantes no tempo é o exemplo fundamental dos *códigos de Schreier* que apresentamos neste Capítulo.

Os códigos de Schreier são subgrupos de $G^{\mathbb{Z}}$, onde G é um grupo finito arbitrário, não necessariamente um grupo de simetrias de algum conjunto Euclidiano discreto $S \subset \mathbb{R}^n$. Esta generalidade somente facilita a aplicação do produto de Schreier, que como vimos no Capítulo 2 é sobre grupos arbitrários. Para "converter" os códigos de Schreier em códigos Euclidianos será necessário restringirmos os códigos de Schreier a serem códigos de simetrias ou ao menos de permutações.

Os códigos de Schreier admitem análise local, isto é , a análise da seção de treliça numa unidade do tempo é suficiente para determinar as propriedades tais como distância livre, controlabilidade, mínimoidade, etc. de todo o código. Esta análise local, também, permite determinar a relação equipotente entre a classe dos produtos de Schreier e a classe dos códigos de Schreier, via os codificadores isomorfos. Isto significa que para cada código de Schreier existe um único codificador isomorfo e para cada codificador isomorfo existe um único código de Schreier.

Este capítulo é organizado como segue. Na Seção 3.1 apresentamos uma rápida descrição de máquinas no sentido da teoria dos autômatas, pois todos os codificadores considerados neste trabalho usam este modelo. Na Seção 3.2 inspirados pela descrição matricial dos codificadores convolucionais binários, definimos os codificadores convolucionais elementares

sobre grupos (CCE). A classe dos codificadores convolucionais lineares binários está contida na classe dos CCEs. Estudamos algumas propriedades dos CCEs que servem como guia para definir os codificadores homomorfos generalizados. Também propomos um teste simples de exclusão de CCEs catastróficos. Uma outra proposta é a de reduzir os estados de um CCE, especialmente se este for catastrófico. Na Seção 3.3 estudamos os codificadores homomorfos generalizados ou codificadores de Schreier, pois a sua definição é baseada no produto de Schreier. Os códigos de Schreier são apresentados como aqueles associados aos codificadores homomorfos. Finalmente, é apresentada uma condição necessária mas não suficiente de controlabilidade denominado de teste $M1$. Este critério é prático quando o número de estados do código é pequeno.

3.1 Máquinas

A descrição de um sistema sob a excitação de alguma classe de entrada produzindo uma outra classe de saída tal que a sua estrutura interna possa também ser modificada, tem sido e será útil no modelamento de muitos dispositivos abstratos e fenômenos. Dentre as possíveis descrições, escolhemos aquela relativa à teoria dos autômatas, devido ao intenso uso do conceito de máquinas.

Definição 3.1 *Uma máquina é uma quíntupla* $M = (X, Y, Q, \delta, \beta)$*; onde*
X *é o conjunto finito das entradas*
Y *é o conjunto finito das saídas*
Q *é o conjunto dos estados (não necessariamente finito)*
$\delta : X \times Q \rightarrow Q$ *é o mapeamento do próximo estado*
$\beta : X \times Q \rightarrow Y$ *é o mapeamamento das saídas.*
$\diamond$

Esta definição é bastante ampla e geral no sentido de que máquinas podem caracterizar sistemas abstratos como por exemplo os sistemas de equações diferenciais, e até mesmo o caso de máquinas "reais" tal como máquina de lavar roupas etc., chegando até o processo

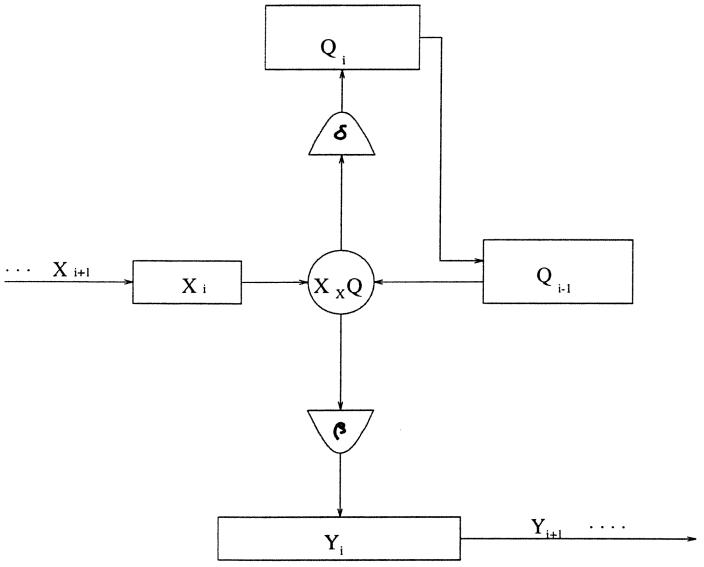

Figura 3.1: Máquina generalizada

evolutivo do comportamento de um ser humano. Willems em [6] usa de maneira precisa o termo *comportamento de um sistema* como sendo uma subclasse de seqüências bi-infinitas de algum produto cartesiano $\prod_{k\in\mathbb{Z}} S_k$, onde cada S_k é um corpo algébrico sendo este o alfabeto de saída da respectiva máquina M_k. A proposta de Trott [1] sobre o conceito de comportamento de um sistema é no sentido de que cada S_k seja um grupo algébrico. A noção de uma máquina generalizada tendo como ponto de partida a Definição 3.1 ocorre quando cada S_k é um conjunto arbitrário podendo apresentar ou não alguma estrutura algébrica.

Seja $\Psi : X \times Q \to Q \times Y \times Q$ a aplicação definida por

$$\Psi(x, q) = (q, \beta(x, q), \delta(x, q)). \tag{3.1}$$

Então, o conjunto $T \subset Q \times Y \times Q$, definido por

$$T = Im(\Psi) = \Psi(X \times Q), \tag{3.2}$$

é chamado **seção de treliça associada à máquina** M ou simplesmente a **treliça de** M. Cada elemento $t = (q, \beta(x, q), \delta(x, q)) \in T$ é chamado **transição** ou **ramo** da treliça.

Considere a classe de seqüências finitas do conjunto das entradas $X^* = \{x^* = \{x_i\}_{i=1}^n : x_i \in X\ n \in \mathbb{N}\}$. Dada uma seqüência finita $x^* = \{x_i\}_{i=1}^n$, denotamos o seu comprimento por

$|x^*|$, e assim $|x^*| = n$.

Definição 3.2 *Dizemos que a máquina* $M = (X, Y, Q, \delta, \beta)$ *é* **controlável** *se para todo* q *e* $q' \in Q$*; existir uma seqüência finita* x^**, com* $1 \leq |x^*| \leq n$ *tal que* $q' = \delta^*(x^*, q)$*, onde*

$$\delta^*(x^*, q) = \delta(x_n, \delta(x_{n-1}, \ldots, \delta(x_1, q)\ldots)$$

$\diamond$

Dado $j \in \mathbb{N}$, se para todo q, $q' \in Q$ existir um $x^* \in X^*$ com $1 \leq |x^*| \leq j$ tal que $q' = \delta^*(x^*, q)$ então , dizemos que a máquina é j-controlável. Dessa forma, fica fácil de precisar que se a máquina é j-controlável então, ela também será $(j+1)$-controlável.

O número $\nu = min\{j \ : \ M$ é j-controlável $\}$ é o **índice de controlabilidade** de M. Na verdade, controlabilidade é uma propriedade da classe de seqüências de saída $\mathcal{C}$ da máquina M, ou equivalentemente do comportamento do sistema. Mas como para uma máquina M existe uma única classe $\mathcal{C}$ de seqüências de saída associada com M, então é natural dizer que M é controlável para dizer que $\mathcal{C}$ é controlável. Assim, esta característica ocorrerá de maneira similar com as demais propriedades de $\mathcal{C}$. Isto é , quando M apresentar uma certa propriedade $\mathcal{P}$, então $\mathcal{C}$ apresentará a mesma propriedade $\mathcal{P}$.

3.2 Codificadores Convolucionais Elementares sobre Grupos

Sejam k e n números naturais. Seja L uma matriz $k \times n$ definida por $L = (l_{ij})$ onde $l_{ij} \in \mathbb{Z}$, $1 \leq i \leq k$, e $1 \leq j \leq n$. Seja G um grupo abeliano. Para qualquer $n \in \mathbb{N}$, considere G^n como sendo n cópias de G, com a G-operação sobre as respectivas coordenadas. Então , G^n é também um grupo abeliano. Dado $x \in G^k$ e L, defina o produto $x.L$ como sendo

$$x.L = \left(\sum_{i=1}^{k} x_i l_{i1}, \sum_{i=1}^{k} x_i l_{i2}, \cdots, \sum_{i=1}^{k} x_i l_{in} \right), \tag{3.3}$$

onde

$$x_i l_{ij} \doteq \begin{cases} \overbrace{x_i * x_i * ... * x_i}^{l_{ij}-vezes} & se\ l_{ij} > 0 \\ e_G & se\ l_{ij} = 0 \\ \overbrace{(x_i * x_i * ... * x_i)^{-1}}^{l_{ij}-vezes} & se\ l_{ij} < 0. \end{cases}$$

Devido a condição abeliana de G e G^n podemos usar o símbolo de adição $+$ em lugar do simbolo $*$, e também para o elemento identidade usar o símbolo 0 em lugar de e_G. Sob estas condições temos a seguinte definição para o codificador convolucional elementar.

Definição 3.3 *Sejam n, k e m números naturais tais que $n > k \geq 1$, e $m \geq 1$. Considere as matrizes $L_0, L_1, ..., L_m$, com $L_i = (l_{rs}^i)$, onde $l_i^{rs} \in \mathbb{Z}$, $1 \leq r \leq k$, $1 \leq s \leq n$, e $i = 0, 1, ..., m$. Um codificador convolutional elementar (CCE) com parâmetros (n, k, m) sobre G, onde n é o comprimento da palavra-código de transição, k é o número de dígitos de informação e m a memória total, é uma máquina $M \doteq (X, Y, Q, \delta, \beta)$ onde*

- $X \subset G^k$ *é o alfabeto das entradas;*
- $Y \subset G^n$ *é o alfabeto das saídas ;*
- $Q = \{q = (x_1, x_2, ..., x_m) \mid x_i \in X\} \subset \left(G^k\right)^m \cong G^{km}$, *é o conjunto (ou espaço) dos estados da máquina*
- $\delta : X \times Q \to Q$, *é uma aplicação definida por* $\delta(x_0; q) = (x_0; x_1, x_2, ..., x_{m-1}, x_m) = (x_0; x_1, x_2, ..., x_{m-1})$ *(aplicação do próximo estado)*;
- $\beta : X \times Q \to Y$, *é uma aplicação definida por* $\beta(x_0; q) = \beta(x_0; x_1, ..., x_m) = x_0 L_0 + x_1 L_1 + ... + x_m L_m$ *(aplicação das saídas).*

$\diamond$

Note que um CCE é um exemplo de máquina, isto é satisfaz a Definição 3.1. Assim, a classe dos CCEs está contida na classe das máquinas.

Da Definição 3.3, podemos extrair as seguintes propriedades dos codificadores convolucionais elementares.

Proposição 3.1 *Se X é um grupo, então*

i) *Q e $\beta(X_{\oplus}Q) \subset Y$ são grupos.*

ii) *O produto cartesiano $X \times Q$ converte-se em um produto direto de grupos e as funções δ e β são homomorfismos de grupos, com δ sendo sobretora.*

iii) *Os conjuntos $Y_0 = \{\beta(x, e_Q)\}_{x \in X}$ e $Y_1 = \{\beta(x,q) : \delta(x,q) = e_Q\}$ são subgrupos normais de $\beta(X,Q)$. Além disso, $\frac{\beta(X,Q)}{Y_0} \cong \frac{\beta(X,Q)}{Y_1} \cong Q$.*

iv) *O CCE é uma máquina controlável, com indice de controlabilidade $\nu \leq m$.*

Prova:

i) Dado $y = \sum_{i=0}^{m} x_i L_i \in Y$, e $y' = \sum_{i=0}^{m} x_i' L_i \in Y$, temos $y + y' = \sum_{i=0}^{m}(x_i L_i + x_i' L_i) = \sum_{i=0}^{m} x_i'' L_i \in Y$, pois X é um grupo. Analogamente, dado $q = (x_1, x_2, ..., x_m)$ e $q' = (x_1', x_2', ..., x_m')$, temos $q + q' = (x_1 + x_1', x_2 + x_2', ..., x_m + x_m') \in Q$, pois X é um grupo.

ii) Como X e Q são grupos, o produto direto $X_{\oplus}Q$ é um grupo. Assim, δ é um mapeamento entre dois grupos. Seja (x,q) e (x',q') dois elementos de $X \times Q$, com $q = (x_1, x_2, ..., x_m)$, e $q' = (x_1', x_2', ..., x_m')$. Então ,

$$\begin{aligned}\delta((x,q) + (x',q')) &= \delta(x + x', q + q') = (x + x', x_1 + x_1', x_2 + x_2', ..., x_{m-1} + x_{m-1}') \\ &= (x, x_1, x_2, ..., x_{m-1}) + (x', x_1', x_2', ..., x_{m-1}') = \delta(x,q) + \delta(x',q').\end{aligned}$$

Portanto , δ é um homomorfismo de grupos. Por outro lado, dado $q = (x_1, x_2, ..., x_m) \in Q$, assuma $q_0 = (x_2, x_3, ..., x_{m+1}) \in Q$ e $x_1 \in X$. Então, $\delta(x_1, q_0) = q$. Com isso, temos que δ é sobrejetora.

De maneira análoga, podemos mostrar que β é também um homomorfismo de grupos.

iii) Defina o mapeamento auxiliar $\psi : \beta(X_{\oplus}Q) \to Q$ por $\psi(\beta(x,q)) \doteq q$. Então,

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

Assim , ψ é um homomorfismo sobrejetor. Consequentemente, temos que

$$Ker(\psi) = \{\beta(x,q) : q = \psi(\beta(x,q)) = e_Q\} = Y_0.$$

Logo, pelo teorema fundamental dos homomorfismos (veja Apêndice C) concluímos que $\frac{\beta}{(}X_{\oplus}Q)Y_0 \cong Q$.

A prova para Y_1 é análoga. Neste caso definimos o mapeamento auxiliar $\psi : \beta(X_{\oplus}Q) \rightarrow Q$ como $\psi(\beta(x,q)) \doteq \delta(x,q)$.

iv) Dado os estados $q = (x_1, x_2, \ldots, x_m)$ e $q' = (x'_1, x'_2, \ldots, x'_m)$, considere a seqüência finita $x^* = x'_1 x'_2 \ldots x'_m \in X^*$; temos que;

$$q' = \delta^*(x^*, q).$$

Portanto, M é sempre m-controlável. ■

No que segue sempre consideraremos X como sendo um grupo. Portanto, todas as propriedades da Proposição 3.1 serão válidas.

Lema 3.1 *A seção de treliça do CCE, não possui transições paralelas. Portanto, o mapeamento Ψ dado em (3.1) é injetor.*

Prova : Lembremos que duas transições $t_1 = (q_1, \beta(x_1, q_1), \delta(x_1, q_1)) \in T$ e $t_2 = (q_2, \beta(x_2, q_2), \delta(x_2, q_2)) \in T$ são ditas *transições paralelas* se $q_1 = q_2$ e $\delta(x_1, q_1) = \delta(x_2, q_2)$. Agora, se a treliça do CCE tiver t_1 e t_2 como transições paralelas, então existe um $q \in Q$ tal que $t_1 = (q, \beta(x_1, q), \delta(x_1, q))$ e $t_2 = (q, \beta(x_2, q), \delta(x_2, q))$ com $\delta(x_1, q) = \delta(x_2, q)$. Disto, temos que $\delta(x_1 - x_2, 0) = 0 \in G^{km}$. Isto implica pela definição de δ, que $x_1 = x_2$. Logo, $t_1 = t_2$ ■

Seja $M = (X, Y, Q, \delta, \beta)$. Considere uma seqüência de entradas $\{x_i\}_{i=1}^{\infty}$, $x_i \in X$, e o estado inicial $q_0 \in Q$. Seja $\{q_i\}_{i=1}^{\infty}$, $q_i \in Q$, a seqüência de estados gerada por $\{x_i\}_{i=1}^{\infty}$ através

de M, definida por

$$\begin{aligned} q_1 &= \delta(x_1, q_0) \\ q_2 &= \delta(x_2, q_1) \\ &\vdots \\ q_i &= \delta(x_i, q_{i-1}) \\ &\vdots \end{aligned} \tag{3.4}$$

Seja $\{y_i\}_{i=1}^{\infty}$; $y_i \in Y$ a seqüência da saída gerada por $\{x_i\}_{i=1}^{\infty}$ através de M, definida por

$$\begin{aligned} y_1 &= \beta(x_1, q_0) \\ y_2 &= \beta(x_2, q_1) \\ &\vdots \\ y_i &= \delta(x_i, q_{i-1}) \\ &\vdots \end{aligned} \tag{3.5}$$

Definição 3.4 *Dado o $CCE = (X, Y, Q, \delta, \beta)$, o código convolucional $\mathcal{C}$ associado ao CCE é a família de seqüências $\{y_i\}_{i=1}^{\infty}$ definidas por (3.5)*

◇

Cada seqüência $\{y_i\}_{i=1}^{\infty}$ é chamada de *palavra-código.* Este código é **invariante** no tempo, pois é produzido por um único CCE.

Definição 3.5 *Seja $\mathcal{C}$ um código qualquer. Seja $\{C_i\}_{i\in\mathbb{N}}$ a família de codificadores associados com o código $\mathcal{C}$. Seja $\{s_i\}_{i\in\mathbb{N}}$ a familia de números naturais tal que, cada s_i é a cardinalidade dos estados de cada codificador C_i. Então, um codificador C_j é dito mínimo quando seu número de estados s_j é mínimo, isto é, $s_j \leq s_i$, para todo $i \in \mathbb{N}$.*

◇

Quando da determinação de codificadores dos códigos de treliça, é importante que sejam estabelecidas as condições de eliminação de códigos catastróficos pois os mesmos são tais que para um número finito de erros introduzidos pelo canal conduzem a um número infinito de

erros na decodificação . O Teorema 3.4 de [2] válido para **códigos completos**[1], veio resolver este problema. A versão deste teorema para os CCEs é :

Teorema 3.1 *Seja a máquina* $M = (X, Y, Q, \delta, \beta)$ *tal que* $X = G^k$, $Y = G^n$ *e* $Q = G^{km}$, *onde* G *é um grupo finito com caraterística* p *tal que* $mcm(p, (m+1)) = 1$. *Sejam* $L_0, \ldots, L_m$ *as matrizes que definem* β. *Então, o código* $\mathcal{C}$ *associado com* M *é não catastrófico se, e somente se,* $L = \sum_{i=0}^{m} L_i$ *é tal que* $x.L \neq 0 \in G^n$ *e* $m+1$ *não é um múltiplo da caraterística do grupo* G, *para todo* $x \in X$ *tal que* $x \neq 0$.

Prova : Seja $t \in T$ uma *transição horizontal* definida como sendo $t = (q, \beta(x,q), \delta(x,q))$, tal que $\delta(x,q) = q$. Se $q = (x_1, \ldots, x_m)$, temos que $\delta(x,q) = q$ se e somente se $x = x_1 = \ldots = x_m$.

O Teorema 3.4 de [2] garante que para o codificador ser mínimo uma condição necessária e suficiente é que a única transição horizontal rotulada com $0 \in Y$ deve ser a transição trivial $(0, \beta(0,0), \delta(0,0))$. Portanto, se $(x,q) \in X_{\oplus}Q$ é tal que $q = \delta(x,q)$ teremos que $\beta(x,q) = xL_0 + xL_1 + \ldots xL_m = (m+1)xL$. ∎

Dessa forma, o Teorema 3.1 é um critério de se evitar catastroficidade na construção do CCE. Por outro lado, o código catastrófico poderá ser transformado em um código não catastrófico através da determinação do correspondente codificador mínimo. Para isso necessitamos de técnicas que permitam a redução da cardinalidade dos estados.

3.2.1 Redução dos estados

Nesta subseção assumiremos que o mapeamento β é sobrejetor, isto é, $\beta(X_{\oplus}Q) = Y$

Proposição 3.2 *Seja* $Q' \subset Q$ *um subgrupo normal de* Q. *Se* Y' *é definido como* $Y' = \{\beta(x,q) \in Y \ : \ x \in X \ e \ q \ , \ \delta(x,q) \in Q'\}$. *Então,* Y' *é um subgrupo normal de* Y.

[1]Os códigos completos são definidos na Seção 4.3 do Capítulo 4. No Teorema 4.3, da mesma Seção, provamos que um código com cardinalidade finita de estados e invariante no tempo é completo. Em particular, um código associado a um CCE é completo.

Prova: Defina a aplicação auxiliar $\psi : Y \to \frac{Q}{Q'} \times \frac{Q}{Q'}$ como sendo

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

Então,

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

Por outro lado,

$$Ker(\psi) = \{\beta(x,q) \ : \ \psi(\beta(x,q)) = (Q',Q')\} = \{\beta(x,q) \in Y \ : \ q \in Q' \text{ e } \delta(x,q) \in Q'\} = Y'$$

Assim, Y' é normal em Y ■

Definição 3.6 *Dada uma máquina $M = (X,Y,Q,\delta,\beta)$, sejam $Y' \subset Y$ e $Q' \subset Q$, definidos como na Proposição 3.2, e tal que $\delta(0,q) \in Q'$, para todo $q \in Q'$. Então, definimos a máquina $M' = (X, \frac{\beta}{(}X_{\oplus}Q)Y', \frac{Q}{Q'}, \delta', \beta')$ onde*

- *$\delta' : X \times \frac{Q}{Q'} \to \frac{Q}{Q'}$ é dado por $\delta'(x, q+Q') = \delta(x,q)+Q'$;*
- *$\beta' : X \times \frac{Q}{Q'} \to \frac{Y}{Y'}$ é dado por $\beta'(x,q+Y') = \beta(x,q)+Y'$ (classe das transições paralelas).*

◇

Geralmente, uma máquina M' não é um CCE, pois se Y' é um subgrupo não trivial, M' possui transições paralelas. O Exemplo 3.3 ilustra esta afirmação .

Proposição 3.3 *As aplicações δ' e β' têm as seguintes propriedades*

- *δ' e β' estão bem definidas, i.e., elas não dependem da escolha do representante da classe $q+Q'$.*
- *δ' e β' são homomorfismos de grupos com δ' sendo sobrejetora.*

- *β' é tal que os conjuntos*

$$Y_{Q'_0} = \{\beta'(x, Q') : x \in X\},$$

e

$$Y_{Q'_1} = \left\{\beta'(x, q+Q') : (x, q+Q') \in X \times \frac{Q}{Q'},\ \delta'(x, q+Q') = Q'\right\},$$

são subgrupos normais de $\frac{Y}{Y'}$. Além disso,

$$\frac{\frac{Y}{Y'}}{Y_{Q'_0}} \cong \frac{\frac{Y}{Y'}}{Y_{Q'_1}} \cong \frac{Q}{Q'}.$$

Prova:

- Se q, $q_1 \in q+Q'$, então $\delta'(x, q+Q') = \delta(x, q)+Q'$ e $\delta'(x, q_1+Q') = \delta(x, q_1)+Q'$. Logo, $\delta'(x, q+Q') - \delta'(x, q_1+Q')$=$\delta(0, q-q_1)+Q'$. Como $\delta(0, q) \in Q'$ para todo $q \in Q'$, temos que $\delta'(x, q+Q') - \delta'(x, q_1+Q') = Q'$.

  A prova para β' é similar pois por definição de Y', $\beta(0, q) \in Y'$ para todo $q \in Q'$.

- $\delta'(x, q+Q') + \delta'(x_1, q_1+Q')$= $\delta(x, q) + \delta(x_1, q_1) + Q'$= $\delta(x+x_1, q+q_1) + Q'$= $\delta'(x+x_1, q+q_1+Q')$.

  A prova para β' é similar.

- Considere o mapeamento auxiliar $\phi : \frac{Y}{Y'} \to \frac{Q}{Q'}$ definido por $\phi(\beta'(x, q+Q')) = \delta'(x, q+Q')$. Como β' e δ' são homomorfismos de grupos, então ϕ é um homomorfismo. A sobrejetividade de ϕ decorre da sobrejetividade de δ'. Agora, $Ker(\phi) = \{\phi(\beta'(x, q+Q')) : \delta'(x, q+Q') = Q'\} = Y_{Q'_1}$. Portanto,

$$\frac{\frac{Y}{Y'}}{Y_{Q'_1}} \cong \frac{Q}{Q'}.$$

  Para $Y_{Q'_0}$ a prova é similar usando o mapeamento auxiliar $\phi : \frac{Y}{Y'} \to \frac{Q}{Q'}$ definido como a projeção $\phi(\beta'(x, q+Q')) = q+Q'$. ∎

3.2.2 Exemplos

Exemplo 3.1 *Dados* $G = \mathbb{Z}_2$, $n = 3$, $k = 2$, $m = 2$, *e* $L_0 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$; $L_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$; $L_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. *Considere a máquina* M *dada por*

$$X = \mathbb{Z}_2^2 = \{00, 01, 10, 11\}$$

$$Q = X^2 = \mathbb{Z}_2^4 = \left\{ \begin{array}{cccccccc} 0000 & 0100 & 1000 & 1100 & 0001 & 0101 & 1001 & 1101 \\ 0010 & 0110 & 1010 & 1110 & 0011 & 0111 & 1011 & 1111 \end{array} \right\}$$

$$Y = \mathbb{Z}_2^3 = \{000, 001, 010, 100, 011, 110, 101, 111\}$$

$$\delta(x_0, q) = \delta(x_0, (x_1, x_2)) = (x_0, x_1), \text{ com } x_i \in \mathbb{Z}_2^2$$

$$\beta(x_0, q) = \beta(x_0, (x_1, x_2)) = x_0 L_0 + x_1 L_1 + x_2 L_2$$

A seção da treliça da máquina $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^4, \delta, \beta)$ é mostrada na Fig. 3.2. O código associado é um código convolucional binário com distância $d_{free} = 5$, taxa $R_C = 2/3$ e memória 2, onde d_{free} é a menor distância de Hamming entre todas as palavras do código.

Exemplo 3.2 *Considere os grupos* $X = \mathbb{Z}_2^2$, $Y = \mathbb{Z}_2^3$, $Q = \mathbb{Z}_2^2$ *e as matrizes* $L_0 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ *e* $L_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

O mapeamento $\delta : X_{\oplus} Q \rightarrow Q$ é dado por $\delta(x, q) = x$. O mapeamento $\beta : X_{\oplus} Q \rightarrow Y$ é dado por $\beta(x, q) = xL_0 + qL_1$. A seção da treliça desta máquina $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^2, \delta, \beta)$ é mostrado na Figura 3.3. O código associado possui $d_{free} = 3$, $R_C = \frac{2}{3}$ e memória 2. Este código é catastrófico, pois para o estado inicial 01 a seqüência ....0101010101 é codificada na palavra código 00000000.....

Exemplo 3.3 *Dado o CCE do Exemplo 3.2, considere o subgrupo normal de* $Q' \lhd Q$ *especificado por* $Q' = \{00, 10\}$. *Então* $Y' \lhd Y$ *é dado por* $Y' = \{000, 110\}$.

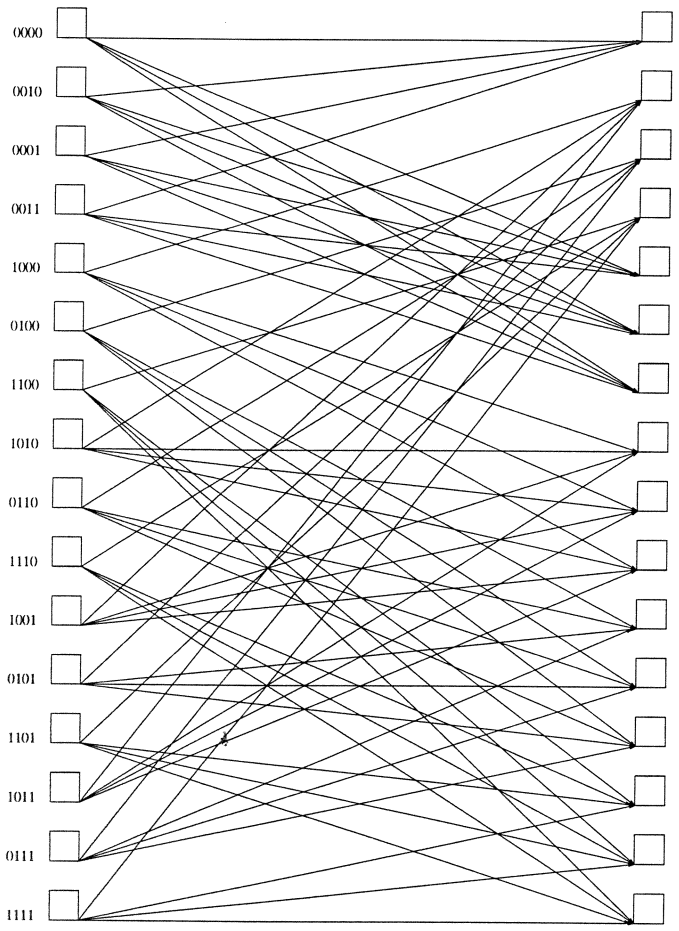

Figura 3.2: Treliça para o CCE do Exemplo 3.1

Com isso, as classes determinadas por Q' são

$$\begin{aligned} Q' &= \{00, 10\} \\ 01 + Q' &= \{01, 11\}. \end{aligned}$$

As classes determinadas por Y' são :

$$\begin{aligned} Y' &= \{000, 110\} \\ 100 + Y' &= \{100, 010\} \\ 001 + Y' &= \{001, 111\} \\ 011 + Y' &= \{011, 101\} \end{aligned}$$

Então a nova máquina $(X, \frac{Y}{Y'}, \frac{Q}{Q'}, \delta', \beta')$ é especificada pelo mapeamento $\delta' : X_{\oplus}\frac{Q}{Q'} \rightarrow \frac{Q}{Q'}$ definido por $\delta'(x, q + Q') = \delta(x, q) + Q'$ e pelo mapeamento $\beta' : X_{\oplus}\frac{Q}{Q'} \rightarrow \frac{Y}{Y'}$ definido por

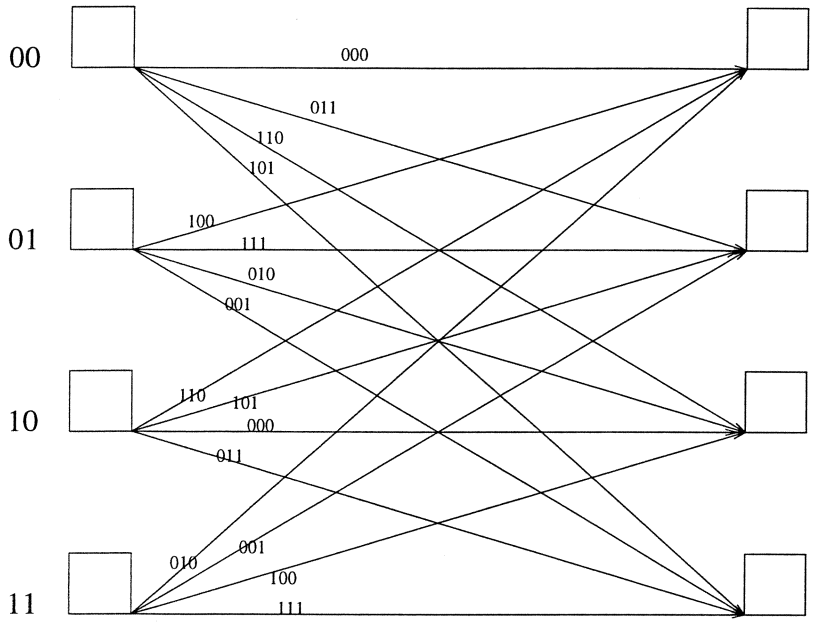

Figura 3.3: Treliça para o CCE do Exemplo 3.2

$\beta'(x, q + Q') = \beta(x, q) + Y'$, onde δ e β estão definidos no Exemplo 3.2

Uma representação da seção da treliça desta máquina é mostrada no lado esquerdo da Fig. 3.4.

No lado direito da mesma figura, é mostrado a representação completa, isto é, os elementos das classes de Y'. Nenhuma destas treliças corresponde à de um CCE. Considerando que $\{Q', 01 + Q'\} \cong \mathbb{Z}_2$, a treliça do lado direito é produzida pela máquina $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2, \delta, \beta)$ onde $\delta : \mathbb{Z}_2^2 \oplus \mathbb{Z}_2 \to \mathbb{Z}_2$ é definido por $\delta(x_1, x_2; q) = x_2$, e $\beta : \mathbb{Z}_2^2 \oplus \mathbb{Z}_2 \to \mathbb{Z}_2^3$ é definido por $\beta(x_1, x_2; q) = (x_1 + q, x_1 + x_2, x_2)$. Esta máquina produz o mesmo código que o CCE do Exemplo 3.2. Note que esta máquina **não satisfaz** todas as propriedades do CCE (por exemplo a cardinalidade dos estados é menor do que a cardinalidade do grupo de entradas). Por isso uma definição mais geral é necessária.

Definição 3.7 *Um codificador abeliano é uma máquina $M = (X, Y, Q, \delta, \beta)$, onde X, Y, Q são grupos abelianos finitos, e $\delta : X_{\oplus}Q \to Q$ e $\beta : X_{\oplus}Q \to Y$ são tais que*

- *δ é homomorfismo sobrejetor;*
- *β é um homomorfismo tal que a aplicação Ψ dada em (3.1) é injetora.*

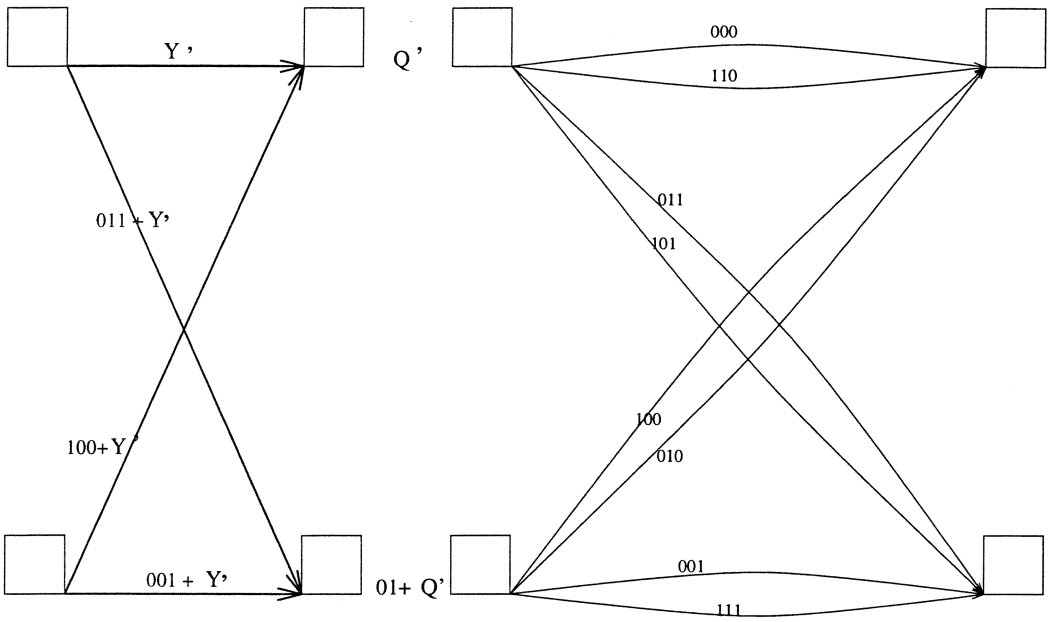

Figura 3.4: Treliça para a máquina do Exemplo 3.3

◇

Assim o CCE é um caso particular do codificador abeliano. Porém, um codificador abeliano não está definido para grupos não abelianos. Antes de fazer uma análise para estes codificadores abelianos, iremos definir e analisar os codificadores generalizados. Estes codificadores são gerais e incluem os CCEs, codificadores abelianos, e codificadores sobre grupos não abelianos.

3.3 Codificadores Convolucionais Generalizados

Nesta seção iremos definir o codificador convolucional generalizado. Para isso, consideraremos X como sendo o grupo finito das entradas, Q o grupo dos estados, e Y o grupo das saídas; juntamente com as aplicações $\sigma : Q \to Aut(X)$ e $\mu : Q \times Q \to X$, satisfazendo (2.1) e (2.2). Com isso o produto de Schreier está estabelecido. Desse modo, o codificador generalizado é definido como

Definição 3.8 *Um codificador convolucional generalizado é uma máquina* $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ *tal que*

- $\delta : X_{(\sigma,\mu)}Q \to Q$ *é um homomorfismo sobrejetor;*
- $\beta : X_{(\sigma,\mu)}Q \to Y$ *é um homomorfismo tal que* Ψ*, definida em (3.1), é injetora.*

$\diamond$

A melhor notação do codificador generalizado deveria ser $M = (X, Y, Q, \delta, \beta, \sigma, \mu)$, pois M depende também dos mapeamentos σ e μ, os quais determinam o produto de Schreier. Porém, o codificador é um caso particular de máquinas, onde tradicionalmente a notação é de uma quíntupla. Dessa forma, iremos denotar o codificador generalizado por $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$. Sob estas condições denominaremos o codificador generalizado como codificador de Schreier.

Note que no caso particular de σ e μ serem identidade, então o produto de Schreier resulta no produto direto $X_{\oplus}Q$ e o codificador de Schreier $M_{(\sigma,\mu)}$ torna-se $M_{(\sigma,\mu)} = M$. Observe que esta é a mesma notação utilizada para os codificadores abelianos da Seção 3.6. Com isso, fica claro que os CCEs são casos particulares do codificador de Schreier.

A partir de agora, usaremos equivalentemente os termos codificador de Schreier ou simplesmente codificador para denotar o dispositivo $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$. Como δ e β são homomorfismos estes codificadores também serão denominados de **codificadores homomorfos**. No caso particular de β ser um isomorfismo, denominaremos o codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ de **codificador isomorfo**.

Note que a seção de treliça T definida por (3.2) é um grupo tal que

$$T \cong X_{(\sigma,\mu)}Q, \tag{3.6}$$

pois Ψ é um isomorfismo e $T = Im(\Psi)$.

Considere a classe $\mathcal{H}$ definida por (2.9). Defina $H_1 \in \mathcal{H}$ como sendo

$$H_1 = Ker(\delta). \tag{3.7}$$

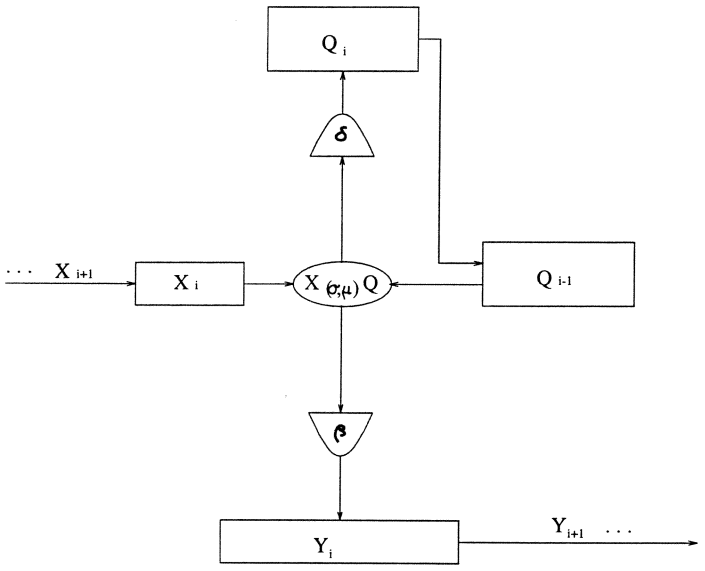

Figura 3.5: Codificador convolucional generalizado

Os subgrupos H_0 e H_1, onde H_0 é definido em (2.10), são fundamentais na construção de codificadores, como veremos a seguir. Dado o codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$, considere uma seqüência de entradas $\{x_i\}_{i=1}^{\infty}$, $x_i \in X$, e q_0 o estado inicial tal que $q_0 \in Q$. Seja $\{q_i\}_{i=1}^{\infty}$, $q_i \in Q$, a seqüência de estados gerada por $\{x_i\}_{i=1}^{\infty}$ através do codificador de Schreier, definida por

$$\begin{aligned} q_1 &= \delta(x_1, q_0) \\ q_2 &= \delta(x_2, q_1) \\ &\vdots \\ q_i &= \delta(x_i, q_{i-1}) \\ &\vdots \end{aligned} \tag{3.8}$$

Note que esta seqüência de estados é completamente similar à da equação (3.4). Seja $\{y_i\}_{i=1}^{\infty}$, $y_i \in Y$, a seqüência da saída gerada por $\{x_i\}_{i=1}^{\infty}$ através do codificador de Schreier,

definida por

$$\begin{aligned} y_1 &= \beta(x_1, q_0) \\ y_2 &= \beta(x_2, q_1) \\ &\vdots \\ y_i &= \delta(x_i, q_{i-1}) \\ &\vdots \end{aligned} \tag{3.9}$$

Note que esta seqüência de saídas é completamente similar à da equação (3.5). Portanto, a versão generalizada do código convolucional sobre grupos é similar àquela da Definição 3.4.

Definição 3.9 *Dado o codificador de Schreier* $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$, *o* **código de Schreier** $\mathcal{C}$ *associado a* $M_{(\sigma,\mu)}$, *é a família de seqüências* $\{y_i\}_{i=1}^{\infty}$ *definidas em (3.9)*

$\diamond$

Em outras palavras, o código de Schreier é o código convolucional $\mathcal{C}$ associado ao codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$. A classe dos códigos de Schreier é invariante no tempo, semi-infinito[2] e com grupo de estados finito. Então, os códigos de Schreier podem ser mergulhados na classe dos *group codes*.

Se um *group code* $\mathcal{G}$ é bom (em qualquer sentido: boa distância livre d_{free}, complexidade pequena, etc.) então $\mathcal{G}$ deve ser necessariamente controlável, completo e mínimo [1]. Portanto, por serem uma subclasse dos *group codes*, os bons códigos de Schreier deverão também ser controláveis, completos e minimais. No Teorema 4.3 mostramos que os códigos de Schreier sempre são completos. Quanto à mínimoidade, temos que um código de Schreier é mínimo se o correspondente codificador é um codificador isomorfo. Com relação à controlabilidade dos códigos de Schreier dois critérios são apresentados. O primeiro critério denominado teste $M1$, é uma condição necessária mas não suficiente de controlabilidade. O segundo critério é o teste definitivo pois o mesmo é uma condição necessária e suficiente para se atingir controlabilidade. Este resultado será apresentado no Capítulo 4, Teorema

[2]Cada código de Schreier pode ser mergulhado na classe das seqüências bi-infinitas adicionando a cada código uma seqüência semi-infinita de e_Ys, onde e_Y é o elemento neutro do grupo Y.

4.2. O Exemplo 3.5 é uma prova da existência de códigos que são do tipo $M1$ mas não são controláveis.

3.3.1 Codificadores da classe $M1$

Proposição 3.4 *Dado o codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$, sejam H_0 e H_1 definidos respectivamente por (2.10) e (3.7). Se $H_0 = H_1$ então $M_{(\sigma,\mu)}$ é não-controlável.*

Prova: Sejam U_0, $U_1 \subset T$ as transições associadas a H_0 e H_1 dados, respectivamente, por (2.10) e (3.7), isto é, $U_0 = \Psi(H_0)$ e $U_1 = \Psi(H_1)$. Logo, $H_0 = H_1$ implica $U_0 = U_1$. Para qualquer seqüência de entrada $\{x_i\}_{i=1}^n$, teremos

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

pois $U_0 = U_1 = \{(e_Q, \beta(x, e_Q), e_Q) \mid x \in X\}$. Portanto, quando $q \neq e_Q$ não existe uma seqüência $\{x_i\}_{i=1}^n$ tal que,

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

■

Com isso, temos a seguinte

Proposição 3.5 *Se a classe $\mathcal{T}$ definida em (2.9), não tem mais do que um elemento, então o codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é não-controlável.*

Como $U_0 \cong H_0$ e $U_1 \cong H_1$, então U_0 e U_1 são normais em T e $\frac{T}{U_0} \cong \frac{T}{U_1} \cong Q$. Daí $|U_1| = |U_0|$. Logo, dado um estado $q \in Q$, o número de transições *saindo* de q é $|U_1| = |U_0|$, isto é , $|\{\Psi(x, q) : x \in X\}| = |U_1| = |U_0|$. Também, teremos que, para qualquer estado $q \in Q$ o número de transições *chegando* a q é $|U_1| = |U_0|$, isto é , $|\{\Psi(x, q') = (q', \beta(x, q'), \delta(x, q')) : \delta(x, q') = q\}| = |U_1| = |U_0|$.

No Exemplo 3.5 temos que $H_0 \neq H_1$, mas este codificador não é controlável. Isto prova que as Proposições 3.4 e 3.5 não têm recíprocas. No entanto, para efeito de construção de codificadores este é um critério básico e prático.

Definição 3.10 *Um codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é dito de classe $M1$ se $H_0 \neq H_1$*

$\diamond$

Denotando $M0 = \{$Todos os codificadores convolucionais$\}$, temos que $M0 \supset M1$. Isto é, existem codificadores que não estão em $M1$.

Teorema 3.2 (Construção de codificadores da classe $M1$ a partir das entradas e dos estados) *Dado um produto de Schreier $X_{(\sigma,\mu)}Q$, considere a classe $\mathcal{H}$ relativa a $X_{(\sigma,\mu)}Q$, onde $\mathcal{H}$ é definido por (2.9). Seja $H_0 \in \mathcal{H}$ como em (2.10). Se existirem $H_1 \in \mathcal{H}$, tal que $H_1 \neq H_0$ e $H_2 \lhd X_{(\sigma,\mu)}Q$, tais que $H_2 \cap (H_1 \cap H_0) = \{elemento\, neutro\, de\, X_{(\sigma,\mu)}Q\}$ então, escolhendo $Y \cong \frac{X_{(\sigma,\mu)}Q}{H_2}$, podemos construir um codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ da classe $M1$, onde $\delta : X_{(\sigma,\mu)}Q \to Q$ é um homomorfismo tal que $Ker(\delta) = H_1$ e $\beta : X_{(\sigma,\mu)}Q \to Y$ é um homomorfismo tal que $Ker(\beta) = H_2$.*

Prova: Como a quíntupla (X, Y, Q, δ, β) está estabelecida, basta provar que Ψ, definido em (3.1), é injetor. Dados (x', q'), $(x, q) \in X_{(\sigma,\mu)}Q$, temos que se $\Psi(x', q') = \Psi(x, q)$ então,

$$\begin{aligned}
&\Psi\left((x', q')(x, q)^{-1}\right) = (e_Q, e_Y, e_Q) \\
&\Psi(x'', e_Q) = (e_Q, e_Y, e_Q) \\
&(e_Q, \beta(x'', e_Q), \delta(x'', e_Q)) = (e_Q, e_Y, e_Q).
\end{aligned}$$

Agora, $\beta(x'', e_Q) = e_Y$ implica que $(x'', e_Q) \in Ker(\beta) = H_2$, e $\delta(x'', e_Q) = e_Q$ implica que $(x'', e_Q) \in Ker(\delta) = H_1$. Pela definição de H_0, $(x'', e_Q) \in H_0$. Logo, $(x'', e_Q) \in H_2 \cap (H_1 \cap H_0) = \{elemento\, neutro\, de\, X_{(\sigma,\mu)}Q\}$. Portanto $(x'', e_Q) = \{elemento\, neutro\, de\, X_{(\sigma,\mu)}Q\} = ((\mu(e_Q, e_Q))^{-1}, e_Q)$. ■

Observe que os codificadores resultantes do Teorema 3.2 são , em geral, homomorfos. Para se obter codificadores isomorfos basta fazer $H_2 = \{elemento\, neutro\, de\, X_{(\sigma,\mu)}Q\} = ((\mu(e_Q, e_Q))^{-1}, e_Q)$.

3.3.2 Exemplos

Exemplo 3.4 *Considere $X = \mathbb{Z}_2^2$; $Q = \mathbb{Z}_2^4$ e $Y = \mathbb{Z}_2^3$.*

O produto direto $X_{\oplus}Q$ é isomorfo a $\mathbb{Z}_2^6$. Assim, definindo $\delta : \mathbb{Z}_2^6 \to \mathbb{Z}_2^4$ como sendo $\delta(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1, x_2, x_3, x_4)$ e $\beta : \mathbb{Z}_2^6 \to \mathbb{Z}_2^3$ como sendo $\beta(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1 + x_2 + x_5, x_2 + x_3 + x_4 + x_6, x_1 + x_4 + x_5 + x_6)$, obtemos o codificador $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^4, \delta, \beta)$. Note que este codificador é o mesmo CCE do Exemplo 3.1.

Exemplo 3.5 *Considere o Exemplo 2.5. Iremos construir um codificador isomorfo e pertencente à classe M1. Todavia, este codificador não é controlável. Consideraremos que o grupo das entradas é* $\mathbb{Z}_4$ *e o grupo dos estados é* $\mathbb{Z}_{2\oplus}\mathbb{D}_4$.

Considere os subgrupos $H_0 = \{(0, 0R_0), (1, 0R_0), (2, 0R_0)(3, 0R_0)\}$, $H_1 = \{(1, 1R_2), (2, 0R_0), (3, 1R_2), (0, 0R_0)\}$, e $H_2 = \{(0, 0R_0)\}$. É claro que H_0 e H_2 satisfazem as condições do Teorema 3.2. Para H_1, considerando o arranjo da Tabela 3.1, temos que $\frac{\mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)}{H_1} \cong \mathbb{Z}_{2\oplus}\mathbb{D}_4$. Logo H_1 também satisfaz as condições do Teorema 3.2. Portanto, defina $\delta : \mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4) \to \mathbb{Z}_{2\oplus}\mathbb{D}_4$ como sendo

$$\begin{aligned}
\delta(H_1) &= 0R_0 \quad & \delta((0, 0R_2)H_1) &= 0R_2 \\
\delta((0, 0R_1)H_1) &= 0R_3 \quad & \delta((0, 0R_3)H_1) &= 0R_1 \\
\delta((0, 1R_1)H_1) &= 1R_1 \quad & \delta((0, 1R_3)H_1) &= 1R_3 \\
\delta((0, 1R_0)H_1) &= 1R_2 \quad & \delta((0, 1R_2)H_1) &= 1R_0 \\
\delta((0, 0V)H_1) &= 0H \quad & \delta((0, 0H)H_1) &= 0V \\
\delta((0, 1V)H_1) &= 1H \quad & \delta((0, 1H)H_1) &= 1V \\
\delta((0, 0d_1)H_1) &= 0d_1 \quad & \delta((0, 0d_2)H_1) &= 0d_2 \\
\delta((0, 1d_1)H_1) &= 1d_1 \quad & \delta((0, 1d_2)H_1) &= 1d_2.
\end{aligned}$$

Por outro lado, como $\frac{\mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)}{H_2} \cong \mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)$, definimos $\beta : \mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4) \to \mathbb{Q}_{3\oplus}\mathbb{D}_4$ como o isomorfismo apresentado no Exemplo 2.5. Decorrente das definições de δ e β através de H_0 e H_1, o codificador resultante pertence à classe $M1$. Todavia, este codificador é não controlável, conforme veremos no Capítulo 5. A seção da treliça correspondente a este codificador é mostrada na Figura 3.6.

Exemplo 3.6 (Ungerboeck) *Considere o Exemplo 2.4. Neste exemplo, iremos construir um codificador onde o grupo das entradas é* $\mathbb{Z}_4$ *e o grupo dos estados é* $\mathbb{Z}_2^2$.

classe lateral		conteúdo da classe lateral	ordem da classe lateral
H_1	=	$\{(1,1R_2),(2,0R_0),(3,1R_2),(0,0R_0)\}$	(1)
$(0,0R_1)H_1$	=	$\{(1,1R_3),(2,0R_1),(3,1R_3),(0,0R_1)\}$	(3)
$(0,0R_2)H_1$	=	$\{(1,1R_0),(2,0R_2),(3,1R_0),(0,0R_2)\}$	(2)
$(0,0R_3)H_1$	=	$\{(1,1R_1),(2,0R_3),(3,1R_1),(0,0R_3)\}$	(3)
$(0,1R_1)H_1$	=	$\{(1,0R_3),(2,1R_1),(3,0R_3),(0,1R_1)\}$	(3)
$(0,1R_3)H_1$	=	$\{(3,0R_1),(0,1R_3),(1,0R_1),(2,1R_3)\}$	(3)
$(0,0V)H_1$	=	$\{(1,1H),(2,0V),(3,1H),(0,0V)\}$	(2)
$(0,0H)H_1$	=	$\{(1,1V),(2,0H),(3,1V),(0,0H)\}$	(2)
$(0,0d_1)H_1$	=	$\{(1,1d_2),(2,0d_1),(3,1d_2),(0,0d_1)\}$	(2)
$(0,0d_2)H_1$	=	$\{(1,1d_1),(2,0d_2),(3,1d_1),(0,0d_2)\}$	(2)
$(0,1R_0)H_1$	=	$\{(1,0R_2),(2,1R_0),(3,0R_2),(0,1R_0)\}$	(2)
$(0,1R_2)H_1$	=	$\{(1,0R_0),(2,1R_2),(3,0R_0),(0,1R_2)\}$	(2)
$(0,1d_2)H_1$	=	$\{(1,0d_1),(2,1d_2),(3,0d_1),(0,1d_2)\}$	(2)
$(0,1d_1)H_1$	=	$\{(1,0d_2),(2,1d_1),(3,0d_2),(0,1d_1)\}$	(2)
$(0,1V)H_1$	=	$\{(1,0H),(2,1V),(3,0H),(0,1V)\}$	(2)
$(0,1H)H_1$	=	$\{(1,0V),(2,1H),(3,0V),(0,1H)\}$	(2)

Tabela 3.1: **O grupo das classes laterais** $\frac{\mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)}{H_1}$

Considere os subgrupos $H_0 = \{(0,00),(1,00),(2,00),(3,00)\}$, $H_1 = \{(0,00),(1,01),(2,00),(3,01)\}$ e $H_2 = \{(0,00),(2,01)\}$. É claro que H_0 satisfaz as condições do Teorema 3.2. Para H_1, considerando o arranjo da Tabela 3.2, temos que $\frac{\mathbb{Z}_{4(\mu')}\mathbb{Z}_2{}^2}{H_1} \cong \mathbb{Z}_2^2$. Para H_2, considerando o arranjo da Tabela 3.3, temos que $\frac{\mathbb{Z}_{4(\mu')}\mathbb{Z}_2{}^2}{H_2} \cong \mathbb{Z}_{8\oplus}0 \lhd \mathbb{Z}_{8\oplus}\mathbb{Z}_2$. Finalmente, como $H_0 \cap H_1 \cap H_2 = \{(0,00)\}$ temos que H_1 e H_2 também satisfazem as condições do Teorema 3.2. Portanto,

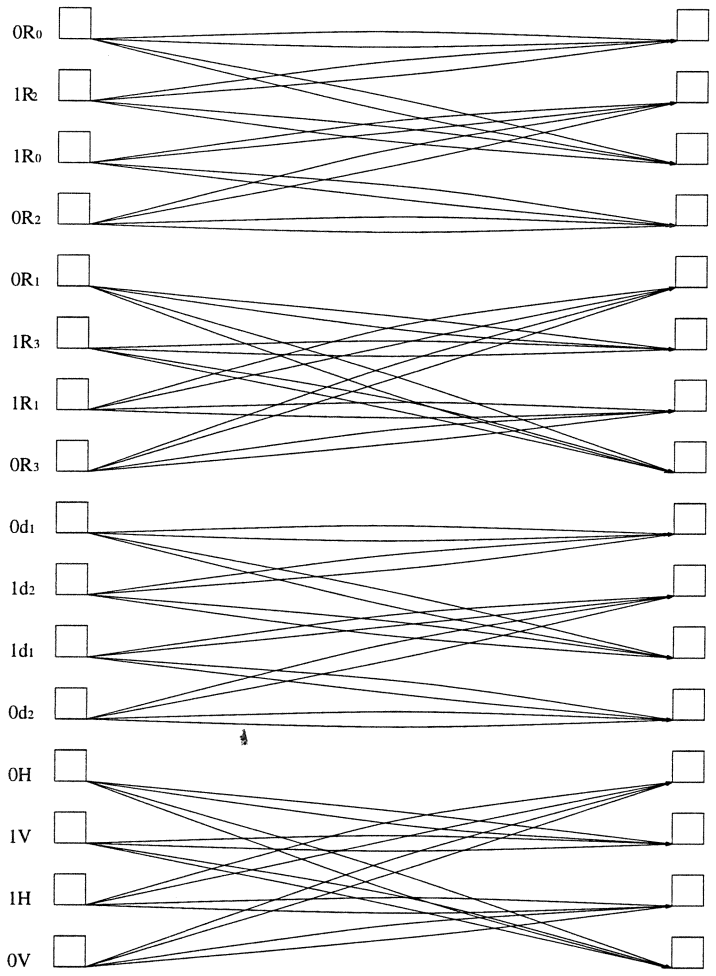

Figura 3.6: Treliça do codificador $M_{(\sigma',\mu')} = (\mathbb{Z}_4, \mathbb{Q}_{3\oplus}\mathbb{D}_4, \mathbb{Z}_{2\oplus}\mathbb{D}_4, \delta, \beta)$

através da Tabela 3.2, defina $\delta : \mathbb{Z}_{4(\sigma',\mu')}(\mathbb{Z}_{2\oplus}D_4) \rightarrow \mathbb{Z}_{2\oplus}D_4$ como sendo

$$\delta(H_1) = 00$$
$$\delta((2,11)H_1) = 01$$
$$\delta((3,00)H_1) = 10$$
$$\delta((0,10)H_1) = 11$$

Note que bastava definir δ sobre os geradores isto é

$$\delta(1,00) = 10$$
$$\delta(0,10) = 11$$
$$\delta(0,01) = 10$$

classe lateral		conteúdo da classe lateral	ordem da classe lateral
H_1	=	$\{(0,00),(1,01),(2,00),(3,01)\}$	(1)
$(2,11)H_1$	=	$\{(2,11),(3,10),(0,11),(1,10)\}$	(2)
$(3,00)H_1$	=	$\{(3,00),(0,01),(1,00),(2,01)\}$	(2)
$(0,10)H_1$	=	$\{(0,10),(1,11),(2,10),(3,11)\}$	(2)

Tabela 3.2: **O grupo das classes laterais** $\frac{\mathbb{Z}_{4(\mu')}\mathbb{Z}_2{}^2}{H_1}$

Para definir β, consideramos que $\mathbb{Z}_{8\oplus}0 \lhd \mathbb{Z}_{8\oplus}\mathbb{Z}_2 \cong \mathbb{Z}_8$ e fazemos uso da Tabela 3.3. Assim,

$$\begin{aligned} \beta(H_2) &= 0 \quad \beta((1,10)H_2) = 1 \\ \beta((1,00)H_2) &= 2 \quad \beta((0,10)H_2) = 3 \\ \beta((2,00)H_2) &= 4 \quad \beta((3,10)H_2) = 5 \\ \beta((3,00)H_2) &= 6 \quad \beta((2,10)H_2) = 7. \end{aligned}$$

Note que bastava definir β sobre os geradores, isto é,

$$\begin{aligned} \beta(1,00) &= 2 \\ \beta(0,10) &= 3 \\ \beta(0,01) &= 4 \end{aligned}$$

Com estas definições de δ e β o codificador de Ungerboeck $M_{(\mu')} = (\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_2^2, \delta, \beta)$ fica caracterizado. Este é um exemplo de un codificador mínimo que náo é isomorfo. A seção da treliça correspondente a este codificador é mostrada na Fig. 3.7.

classe lateral		conteúdo da classe lateral	ordem da classe lateral
H_2	=	$\{(0,00),(2,01)\}$	(1)
$(1,00)H_2$	=	$\{(1,00),(3,01)\}$	(4)
$(2,00)H_2$	=	$\{(2,00),(0,01)\}$	(2)
$(3,00)H_2$	=	$\{(3,00),(1,01)\}$	(4)
$(0,10)H_2$	=	$\{(0,10),(2,11)\}$	(8)
$(1,10)H_2$	=	$\{(1,10),(3,11)\}$	(8)
$(2,10)H_2$	=	$\{(2,10),(0,11)\}$	(8)
$(3,10)H_2$	=	$\{(3,10),(1,11)\}$	(8)

Tabela 3.3: **O grupo das classes laterais** $\frac{\mathbb{Z}_4(\mu')\mathbb{Z}_2{}^2}{H_2}$

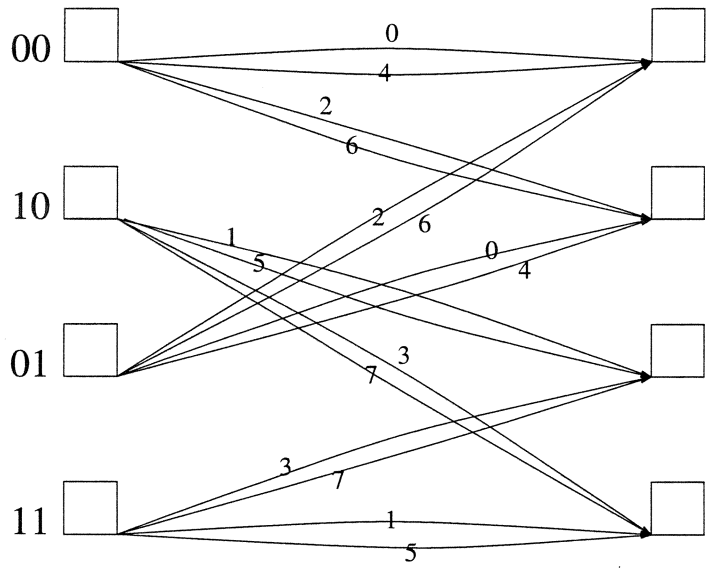

Figura 3.7: Treliça da máquina $M_{(\mu')} = (\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_2^2, \delta, \beta)$ (Codificador de Ungerboeck)

Capítulo 4

Controlabilidade e Completitude dos Códigos de Schreier

Como os *group codes* estão definidos sobre grupos algébricos, os mesmos podem ser considerados como uma generalização dos sistemas dinâmicos lineares definidos sobre corpos algébricos. Assim, propriedades importantes dos sistemas dinâmicos lineares tais como controlabilidade, observabilidade, minimalidade e completitude podem ser estendidas e definidas sobre os *group codes*.

Portanto, os bons códigos de simetrias, que são a subclasse dos *group codes* úteis para modulação codificada, terão que ser necessariamente controláveis, observáveis, minimais e completos [18]. Neste capítulo estaremos voltados principalmente sobre as propriedades de completitude e controlabilidade. Nesta direção, podemos colocar o seguinte problema: como determinar se um dado código de simetrias é controlável?. A resposta natural seria a de aplicarmos a definição de controlabilidade. Todavia, o problema relacionado a esta aplicação é a complexidade de implementação desta definição. Portanto, há a necessidade de se procurar por outros testes de menor complexidade. Um primeiro critério denominado de teste $M1$, apresentado no Capítulo 3, embora sendo uma condição necessária, e muito prático quando o número de estados é pequeno, o mesmo não é condição suficiente para atingir controlabilidade. Para obtermos um critério de suficiência com menor complexidade

do que a apresentada pela definição de controlabilidade, precisamos estabelecer a condição de linearidade dos códigos de Schreier, isto é feito na Seção 4.1. Esta é uma das particularidades importantes destes códigos, pois até o momento não conhecemos uma prova da linearidade dos *group codes* ou dos códigos de simetrias em geral. Na Seção 4.2, apresentamos o Teorema 4.2, sobre controlabilidade, que é um dos resultados centrais deste trabalho. Na Seção 4.3, apresentamos o Teorema 4.3 que mostra que todos os códigos de Schreier são completos.

4.1 A Estrutura de Grupo de $X^i \times Q$

Dados o codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ e $i \in \mathbb{N}$, considere o produto cartesiano

$$X^i \times Q = \overbrace{X \times X \times \ldots \times X}^{i-vezes} \times Q.$$

As seqüências de X^i de comprimento i serão representadas por $(x_i, x_{i-1}, \ldots, x_1) = \{x_{i-j+1}\}_{j=1}^{i}$. Denotamos a i-upla por

$$(x_i, x_{i-1}, \ldots, x_1) \doteq \overset{(i)}{x} \tag{4.1}$$

Esta notação é útil pois, além de sua simplicidade notacional, ela nos permite considerar seqüências parciais, por exemplo, se $(x_i, x_{i-1}, \ldots, x_1) = \overset{(i)}{x}$, então para todo $i \geq j \geq 1$ teremos

$$\overset{(i)}{x} = (x_i, \ldots, x_{j+1}, x_j, x_{j-1}, \ldots, x_1) = (x_i, \ldots, x_{j+1}, \overset{(j)}{x}). \tag{4.2}$$

Por outro lado, para a seqüência dos estados $\{q_j\}_{j=1}^{i} = (q_1, \ldots, q_i)$ e para a seqüência das saídas $\{y_j\}_{j=1}^{i} = (y_1, \ldots, y_i)$ usaremos a ordem crescente dos seus índices. Desse modo, dado $(\overset{(i)}{x}, q) \in X^i \times Q$, definimos as aplicações $\delta_i : X^i \times Q \to Q$ e $\beta_i : X^i \times Q \to Y$ como sendo

$$\begin{aligned} &\delta_1(x_1, q) = \delta(x_1, q), \ x_1 \in X \\ &\delta_j(\overset{(j)}{x}, q) = \delta(x_j, \delta_{j-1}(\overset{(j-1)}{x}, q)), \ \overset{(j)}{x} \in X^j \ , \ i \geq j \geq 2, \end{aligned} \tag{4.3}$$

analogamente para β_i, temos

$$\begin{aligned} &\beta_1(x_1, q) = \beta(x_1, q), \ x_1 \in X \\ &\beta_j(\overset{(j)}{x}, q) = \beta(x_j, \delta_{j-1}(\overset{(j-1)}{x}, q)), \ \overset{(j)}{x} \in X^j \ , \ i \geq j \geq 2. \end{aligned} \tag{4.4}$$

Agora, dados uma seqüência finita de entradas $\overset{(i)}{x}$ e qualquer estado inicial q, considere o par $(\overset{(i)}{x}, q) \in X^i \times Q$. As aplicações δ_i e β_i definem duas seqüências: a seqüência dos estados $\{q_j\}_{j=1}^i$, e a seqüência das saídas $\{y_j\}_{j=1}^i$, onde os elementos de cada seqüência são dados por

$$q_j = \delta_j(\overset{(j)}{x}, q), \tag{4.5}$$

e

$$y_j = \beta_j(\overset{(j)}{x}, q). \tag{4.6}$$

Mais precisamente, definimos as aplicações $\psi_i : X^i \times Q \to Q^i$ e $\lambda_i : X^i \times Q \to Y^i$ como sendo

$$\psi_i(\overset{(i)}{x}, q) = \{q_j\}_{j=1}^i, \tag{4.7}$$

e

$$\lambda_i(\overset{(i)}{x}, q) = \{y_j\}_{j=1}^i. \tag{4.8}$$

Usando a estrutura de grupo do produto de Schreier $X_{(\sigma,\mu)}Q$, definimos uma estrutura de grupo sobre $X^i \times Q$, para qualquer $i \in \mathbb{N}$.

Definição 4.1 *Dados um codificador de Schreier $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ e $i \in \mathbb{N}$, definimos o* **produto misturado** *$X^i{}_{[\sigma,\mu]}Q$ como sendo os pares ordenados $(\overset{(i)}{x}, q)$ dos elementos pertencentes aos seus respectivos grupos satisfazendo a seguinte operação*

$$(\overset{(i)}{x}, q) * (\overset{(i)}{y}, r) = (x_i, x_{i-1}, \ldots, x_1, q) * (y_i, y_{i-1}, \ldots, y_1, r) = (z_i, z_{i-1}, \ldots, z_1, qr)$$

onde

$$\begin{aligned}
z_1 &= x_1.\sigma(q)(y_1).\mu(q, r) \\
z_2 &= x_2.\sigma(\delta(x_1, q))(y_2).\mu\left(\delta(x_1, q), \delta(y_1, r)\right) \\
&\vdots \\
z_j &= x_j.\sigma(\delta_{j-1}(\overset{(j-1)}{x}, q))(y_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q), \delta_{j-1}(\overset{(j-1)}{y}, r)\right) \quad , \quad i \geq j \geq 2.
\end{aligned}$$

$\diamond$

Note a distinção entre as notações para o produto misturado, $X^i{}_{[\sigma,\mu]}Q$, e para o produto de Schreier, $X^i{}_{(\sigma,\mu)}Q$.

Lema 4.1 *Para todo $i \in \mathbb{N}$, as aplicações δ_i e β_i são lineares, isto é, para todo $\left(\overset{(i)}{x}, q\right)$, $\left(\overset{(i)}{y}, r\right) \in X^i{}_{[\sigma,\mu]}Q$ temos que,*

$$\delta_i\left(\overset{(i)}{x}, q\right).\delta_i\left(\overset{(i)}{y}, r\right) = \delta_i\left((\overset{(i)}{x}, q).(\overset{(i)}{y}, r)\right) \quad e \quad \beta_i\left(\overset{(i)}{x}, q\right).\beta_i\left(\overset{(i)}{y}, r\right) = \beta_i\left((\overset{(i)}{x}, q).(\overset{(i)}{y}, r)\right).$$

Prova: Seja $\left(\overset{(i)}{x}, q\right).\left(\overset{(i)}{y}, r\right) = \left(\overset{(i)}{z}, qr\right)$ tal que

$$\begin{aligned} z_1 &= x_1.\sigma(q)(y_1).\mu(q,r) \\ z_j &= x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(y_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\,,\, \delta_{j-1}(\overset{(j-1)}{y}, r)\right) \quad , \; j \geq 2. \end{aligned}$$

Fica claro que, para $j = 1$ o lema é verdadeiro. Suponha que para $j = 1, 2, \ldots, i$ o lema seja verdadeiro. Então, para $i+1$ temos,

$$\begin{aligned} &\delta_{i+1}\left(\overset{(i+1)}{x}, q\right).\delta_{i+1}\left(\overset{(i+1)}{y}, r\right) \\ &= \delta\left(x_{i+1}, \delta_i(\overset{(i)}{x}, q)\right).\delta\left(y_{i+1}, \delta_i(\overset{(i)}{y}, r)\right) = \delta\left((x_{i+1}, \delta_i(\overset{(i)}{x}, q)).(y_{i+1}, \delta_i(\overset{(i)}{y}, r))\right) \\ &= \delta\left(x_{i+1}.\sigma\left(\delta_i(\overset{(i)}{x}, q)\right)(y_{i+1}).\mu\left(\delta_i(\overset{(i)}{x}, q), \delta_i(\overset{(i)}{y}, r)\right) \;,\; \delta_i(\overset{(i)}{x}, q).\delta_i(\overset{(i)}{y}, r)\right) \\ &= \delta\left(z_{i+1}, \delta_i(\overset{(i)}{z}, qr)\right) = \delta_{i+1}\left(\overset{(i+1)}{z}, qr\right) \\ &= \delta_{i+1}\left(\left(\overset{(i+1)}{x}, q\right).\left(\overset{(i+1)}{y}, r\right)\right). \end{aligned}$$

A prova para β_i é análoga. ∎

Lema 4.2 *Seja $\left(\overset{(i)}{x}, e_Q\right)$ o elemento de $X^i{}_{[\sigma,\mu]}Q$ definido por*

$$\begin{aligned} x_1 &= (\mu(e_Q, e_Q))^{-1} \\ x_2 &= [\mu\left(\delta(x_1, e_Q)\,,\, \delta(x_1, e_Q)\right)]^{-1} \\ &\vdots \\ x_j &= \left[\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, e_Q)\,,\, \delta_{j-1}(\overset{(j-1)}{x}, e_Q)\right)\right]^{-1} \quad ; i \geq j \geq 2. \end{aligned} \tag{4.9}$$

Para todo $\left(\overset{(i)}{y}, r\right)$ *pertencente a* $X^i{}_{[\sigma,\mu]}Q$, *as seguintes identidades são verdadeiras*

$$
\begin{aligned}
&i) \quad \sigma\left(\delta_i(\overset{(i)}{x}, e_Q)\right)\left(\mu\left(\delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\right)\right) = \mu\left(\delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\right)\\
&ii) \quad \sigma\left(\delta_i(\overset{(i)}{x}, e_Q)\right)\left(\mu\left(\delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{y}, r)\right)\right) = \mu\left(\delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\right)\\
&iii) \quad \sigma\left(\delta_i(\overset{(i)}{y}, r)\right)\left(\mu\left(\delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\right)\right) = \mu\left(\delta_i(\overset{(i)}{y}, r)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\right).
\end{aligned}
$$

Prova:

i) Na equação (2.1) substitua (k_1, k_2, k_3) por $\left(\delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\right)$.

ii) Na equação (2.1) substitua (k_1, k_2, k_3) por $\left(\delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{y}, r)\right)$.

iii) Na equação (2.1) substitua (k_1, k_2, k_3) por $\left(\delta_i(\overset{(i)}{y}, r)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\,,\, \delta_i(\overset{(i)}{x}, e_Q)\right)$ ∎

Teorema 4.1 *Para todo* $i \in \mathbb{N}$, *o produto misturado* $X^i{}_{[\sigma,\mu]}Q$ *é um grupo.*

Prova: Vide Apêndice B ∎

Como conseqüência de que $X^i{}_{[\sigma,\mu]}Q$ é um grupo, temos

Corolário 4.1.1 *As aplicações*

$$
\begin{aligned}
&\delta_i : X^i{}_{[\sigma,\mu]}Q \to Q \quad \textit{definida por} \quad (4.3),\\
&\beta_i : X^i{}_{[\sigma,\mu]}Q \to Y \quad \textit{definida por} \quad (4.4),\\
&\psi_i : X^i{}_{[\sigma,\mu]}Q \to Q^i \quad \textit{definida por} \quad (4.7),\\
&\lambda_i : X^i{}_{[\sigma,\mu]}Q \to Y^i \quad \textit{definida por} \quad (4.8)
\end{aligned}
$$

são homomorfismos de grupos.

Dentre os homomorfismos do Corolário 4.1.1, os homomorfismos ψ_i e λ_i conduzem ao estabelecimento da linearidade dos códigos de Schreier. Esta linearidade é no sentido de que

as seqüências $(\overset{(i)}{x}, q)$ do grupo $X^i{}_{[\sigma,\mu]}Q$ são mapeadas homomorficamente, por ψ_i e λ_i, nas seqüências $\{q_j\}_{j=1}^i$ do grupo Q^i e $\{y_j\}_{j=1}^i$ do grupo Y^i, respectivamente. Isto é ilustrado no Exemplo 4.1.

Exemplo 4.1 . *Considere o codificador de Schreier* $M_{(\sigma)} = (\mathbb{Z}_2^2, Y, \mathbb{D}_4, \delta, \beta)$ *do Exemplo 5.1. Para* $i = 5$, *o produto misturado é* $(\mathbb{Z}_2^2)^5{}_{[\sigma]}\mathbb{Z}_2^3$. *Então, tomando* $(\overset{(5)}{x}, q)$, $(\overset{(5)}{u}, r) \in (\mathbb{Z}_2^2)^5{}_{[\sigma]}\mathbb{Z}_2^3$, *tal que* $(\overset{(5)}{x}, q) = (x_5, x_4, x_3, x_2, x_1; q) = (a, b, c, e, b; R_1)$ *e* $(\overset{(5)}{u}, r) = (u_5, u_4, u_3, u_2, u_1; r) = (b, a, a, c, e; H)$, *obtemos*

Seqüência de estados gerados por $(\overset{(5)}{x}, q) = (a, b, c, e, b; R_1)$

$$\begin{aligned}
q_1 &= \delta(x_1, q) = \delta(b, R_1) = V \\
q_2 &= \delta_2(\overset{(2)}{x}, q) = \delta(e, V) = d_2 \\
q_3 &= \delta_3(\overset{(3)}{x}, q) = \delta(c, d_2) = R_1 \\
q_4 &= \delta_4(\overset{(4)}{x}, q) = \delta(b, R_1) = V \\
q_5 &= \delta_5(\overset{(5)}{x}, q) = \delta(a, V) = d_1.
\end{aligned}$$

Seqüência de saídas geradas por $(\overset{(5)}{x}, q) = (a, b, c, e, b; R_1)$

$$\begin{aligned}
y_1 &= \beta(x_1, q) = \beta(b, R_1) = R_1 V \\
y_2 &= \beta_2(\overset{(2)}{x}, q) = \beta(e, V) = V d_2 \\
y_3 &= \beta_3(\overset{(3)}{x}, q) = \beta(c, d_2) = d_2 R_1 \\
y_4 &= \beta_4(\overset{(4)}{x}, q) = \beta(b, R_1) = R_1 V \\
y_5 &= \beta_5(\overset{(5)}{x}, q) = \beta(a, V) = V d_1.
\end{aligned}$$

Seqüência de estados gerados por $(\overset{(5)}{u}, r) = (b, a, a, c, e; H)$

$$\begin{aligned}
r_1 &= \delta(u_1, r) = \delta(e, H) = d_1 \\
r_2 &= \delta_2(\overset{(2)}{u}, r) = \delta(c, d_1) = R_3 \\
r_3 &= \delta_3(\overset{(3)}{u}, r) = \delta(a, R_3) = R_1 \\
r_4 &= \delta_4(\overset{(4)}{u}, r) = \delta(a, R_1) = R_3 \\
r_5 &= \delta_5(\overset{(5)}{u}, r) = \delta(b, R_3) = H.
\end{aligned}$$

Seqüência de saídas geradas por $(\overset{(5)}{u}, r) = (b, a, a, c, e; H)$

$$\begin{aligned}
v_1 &= \beta(u_1, r) = \beta(e, H) = Hd_1 \\
v_2 &= \beta_2(\overset{(2)}{u}, r) = \beta(c, d_1) = d_1R_3 \\
v_3 &= \beta_3(\overset{(3)}{u}, r) = \beta(a, R_3) = R_3R_1 \\
v_4 &= \beta_4(\overset{(4)}{u}, r) = \beta(a, R_1) = R_1R_3 \\
v_5 &= \beta_5(\overset{(5)}{u}, r) = \beta(b, R_3) = R_3H.
\end{aligned}$$

O produto $(\overset{(5)}{x}; R_1) * (\overset{(5)}{u}, H) = (\overset{(5)}{z}; d_2)$

$$\begin{aligned}
z_1 &= x_1.\sigma(q)(u_1) = b.\sigma(R_1)(e) = b \\
z_2 &= x_2.\sigma(q_1)(u_2) = e.\sigma(V)(c) = c \\
z_3 &= x_3.\sigma(q_2)(u_3) = c.\sigma(d_2)(a) = b \\
z_4 &= x_4.\sigma(q_3)(u_4) = b.\sigma(R_1)(a) = c \\
z_5 &= x_5.\sigma(q_4)(u_5) = a.\sigma(V)(b) = c.
\end{aligned}$$

Seqüência de estados gerados por $(\overset{(5)}{z}, s) = (c, c, b, c, b; d_2)$

$$\begin{aligned}
s_1 &= \delta(z_1, s) = \delta(b, d_2) = R_3 \\
s_2 &= \delta_2(\overset{(2)}{z}, s) = \delta(c, R_3) = V \\
s_3 &= \delta_3(\overset{(3)}{z}, s) = \delta(b, V) = R_2 \\
s_4 &= \delta_4(\overset{(4)}{z}, s) = \delta(c, R_2) = d_1 \\
s_5 &= \delta_5(\overset{(5)}{z}, s) = \delta(c, d_1) = R_3.
\end{aligned}$$

Seqüência de saídas geradas por $(\overset{(5)}{z}, s) = (c, c, b, c, b; d_2)$

$$\begin{aligned}
w_1 &= \beta(z_1, s) = \beta(b, d_2) = d_2R_3 \\
w_2 &= \beta_2(\overset{(2)}{z}, s) = \beta(c, R_3) = R_3V \\
w_3 &= \beta_3(\overset{(3)}{z}, s) = \beta(b, V) = VR_2 \\
w_4 &= \beta_4(\overset{(4)}{z}, s) = \beta(c, R_2) = R_2d_1 \\
w_5 &= \beta_5(\overset{(5)}{z}, s) = \beta(c, d_1) = d_1R_3.
\end{aligned}$$

Linearidade da aplicação ψ_5

Note que

$$\psi_5((\overset{(5)}{x}, q).(\overset{(5)}{u}, r)) = \psi_5(\overset{(5)}{z}, s) = (R_3, d_1, R_2, V, R_3; d_2).$$

Por outro lado,

$$\psi_5(\overset{(5)}{x}, q).\psi_5(\overset{(5)}{u}, r) = (d_1, V, R_1, d_2, V; R_1).(H, R_3, R_1, R_3, d_1; H)$$
$$= (R_3, d_1, R_2, V, R_3; d_2).$$

Portanto,

$$\psi_5((\overset{(5)}{x}, q).(\overset{(5)}{u}, r)) = \psi_5(\overset{(5)}{x}, q).\psi_5(\overset{(5)}{u}, r).$$

Linearidade da aplicação λ_5

Note que

$$\lambda_5((\overset{(5)}{x}, q).(\overset{(5)}{u}, r)) = \lambda_5(\overset{(5)}{z}, s) = (d_1R_3, R_2d_1, VR_2, R_3V, d_2R_3; d_2).$$

Por outro lado,

$$\lambda_5(\overset{(5)}{x}, q).\lambda_5(\overset{(5)}{u}, r) = (Vd_1, R_1V, d_2R_1, Vd_2, R_1V; R_1).(R_3H, R_1R_3, R_3R_1, d_1R_3, Hd_1; H)$$

$$= (d_1R_3, R_2d_1, VR_2, R_3V, d_2R_3; d_2).$$

Portanto,

$$\lambda_5((\overset{(5)}{x}, q).(\overset{(5)}{u}, r)) = \lambda_5(\overset{(5)}{x}, q).\lambda_5(\overset{(5)}{u}, r).$$

4.2 Teorema da Controlabilidade

Lema 4.3 *Seja* $Q_{0i} \subset Q$ *definido por* $Q_{0i} = \left\{q \in Q : \delta_i\left(\overset{(i)}{x}, e_Q\right) = q\right\}$. *Então* $Q_{0i} \lhd Q$.

Prova : Seja $H_i = \left\{\left(\overset{(i)}{x}, e_Q\right) : \overset{(i)}{x} \in X^i\right\}$, então considerando a projeção $p_2 : X^i{}_{[\sigma,\mu]}Q \to Q$ dada por $p_2\left(\overset{(i)}{x}, q\right) = q$, temos que p_2 é um homomorfismo sobrejetor com $Ker(p_2) = H_i$. Logo, $H_i \lhd X^i{}_{[\sigma,\mu]}Q$. Por outro lado, uma vez que δ é sobrejetora temos que δ_i também é sobrejetora. Logo, $\delta_i(H_i) \lhd Q$ (a imagem de um subgrupo normal por um homomorfismo sobrejetor é também normal). Consequentemente, $\delta_i(H_i) = \left\{\delta_i\left(\overset{(i)}{x}, e_Q\right) : \overset{(i)}{x} \in X^i\right\} = Q_{0i}$. ■

Lema 4.4 *Dado $q \in Q$, seja $Q_{qi} = \left\{\delta_i \left(\overset{(i)}{x}, q\right) : \overset{(i)}{x} \in X^i\right\}$. Então , Q_{qi} é uma classe lateral de Q_{0i}. Portanto, $|Q_{0i}| = |Q_{qi}|$.*

Prova : Considere a classe $(\overset{(i)}{u}, q).H_i$ de H_i. Então, $(\overset{(i)}{u}, q).H_i = (\overset{(i)}{u}, q).\left\{\left(\overset{(i)}{x}, e_Q\right) : \overset{(i)}{x} \in X^i\right\}$ $= \left\{\left(\overset{(i)}{x}, q\right) : \overset{(i)}{x} \in X^i\right\}$. Logo $\delta_i\left((\overset{(i)}{u}, q).H_i\right) = \left\{\delta_i \left(\overset{(i)}{x}, q\right) : \overset{(i)}{x} \in X^i\right\} = Q_{qi}$.
Por outro lado, $\delta_i\left((\overset{(i)}{u}, q).H_i\right) = \delta_i \left(\overset{(i)}{u}, q\right).\delta_i(H_i) = \delta_i \left(\overset{(i)}{u}, q\right).Q_{0i}$. Assim, $Q_{qi} = \delta_i \left(\overset{(i)}{u}, q\right).Q_{0i}$.
Isto mostra que Q_{qi} é uma classe lateral de Q_{0i} e que portanto $|Q_{0i}| = |Q_{qi}|$. ■

Teorema 4.2 *Seja $Q_{0i} \lhd Q$ o subgrupo normal de Q definido no Lema 4.3. Então, $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é controlável se e somente se $Q_{0i} = Q$, para algum $1 \leq i < |Q|$.*

Prova : Suponha $M_{(\sigma,\mu)}$ controlável. Então, se

$$i = max\left\{j \in \mathbb{N}, j < |Q| : \delta_j \left(\overset{(j)}{x}, e_Q\right) = q, \overset{(j)}{x} \in X^j, q \in Q\right\},$$

teremos[1] que para todo $q \in Q$ existe $\overset{(i)}{x} \in X^i$ tal que $\delta_i \left(\overset{(i)}{x}, e_Q\right) = q$, pois se $q = \delta_j \left(\overset{(j)}{u}, e_Q\right)$ para $j < i$, então tomando $\overset{(i)}{x} = x_i, \ldots, x_{1+i-j}, \overset{(i-j)}{x}$, onde $\overset{(i-j)}{x} = \{elemento\, neutro\, de\, X^{i-j}{}_{[\sigma,\mu]}Q\}$ (veja no apêndice B as equações dadas por (4.9)), e para $s > i - j$, tome x_s como sendo $x_s = u_{s-(i-j)}$; teremos que $q = \delta_i \left(\overset{(i)}{x}, e_Q\right)$. Portanto, para todo $q \in Q$ temos que $q \in Q_{0i}$.

Na outra direção do teorema, suponha que $Q = Q_{0i}$, para algum $i \geq 1$. Então, dados q e $r \in Q$, considere a classe $Q_{qi} = \left\{\delta_i \left(\overset{(i)}{x}, q\right) : \overset{(i)}{x} \in X^i\right\}$ definida no Lema 4.4. Como $|Q_{0i}| = |Q_{qi}| = |Q|$, então existe $\overset{(i)}{u} \in X^i$ tal que $\delta_i \left(\overset{(i)}{x}, q\right) = r$. ■

[1]Isto é o princípio da controlabilidade: j-controlabilidade implica $j+1$-controlabilidade.

4.3 Teorema da Completitude

4.3.1 Espaços métricos

Dado um conjunto X, se existir uma função $d : X \times X \to \mathbb{R}$ tal que

- $d(x, y) = 0$ se e somente se $x = y$.
- $d(x, y) = d(y, x)$ para todo x, $y \in X$.
- $d(x, y) \leq d(x, z) + d(z, y)$ para todo x, y, $z \in X$.

então dizemos que d é uma métrica em X e o par (X, d) é chamado de **espaço métrico**. Usualmente os elementos de um espaço métrico são denominados **pontos**.

Dada uma seqüência $\{x_n\}_{n\in\mathbb{N}}$ de pontos de X, dizemos que $\{x_n\}_{n\in\mathbb{N}}$ **converge** para $x \in X$, na métrica d, quando para cada número positivo real ϵ, existir um número natural n_0 tal que se $n > n_0$ então $d(x_n, x) < \epsilon$. Esta convergência é denotada por $x_n \xrightarrow{d} x$.

Um subconjunto $X' \subset X$ é dito **fechado** quando para cada seqüência $\{x_n\}_{n\in\mathbb{N}} \subset X'$ de pontos de X' convergindo a algum ponto $x \in X$ implica que $x \in X'$. Em símbolos,
$X' \subset X$ é fechado $\iff \forall \{x_n\}_{n\in\mathbb{N}} \subset X'$ tal que $x_n \xrightarrow{d} x \Rightarrow x \in X'$.

Um subconjunto $A \subset X$ é dito **aberto** quando o seu complementar é fechado.

4.3.2 Códigos invariantes no tempo são completos

Dado um conjunto finito Y, seja $Y^{\mathbb{N}} = \{\{y_i\}_{i=1}^{\infty} : y_i \in Y\}$. Em $Y^{\mathbb{N}}$, considere a função $d : Y^{\mathbb{N}} \times Y^{\mathbb{N}} \to \mathbb{R}$ definida por

$$d(\{y_i\}_{i=1}^{\infty}, \{u_i\}_{i=1}^{\infty}) = \frac{1}{2^t}, \tag{4.10}$$

onde $t = min\{j \in \mathbb{N} : y_j \neq u_j\} - 1$.

Por exemplo, se $\{y_i\}_{i=1}^{\infty} \cap \{u_i\}_{i=1}^{\infty} = \emptyset$ então $t = 0$, logo $d(\{y_i\}_{i=1}^{\infty}, \{u_i\}_{i=1}^{\infty}) = 1$. Se $y_1 = u_1$ com $y_i \neq u_i \, \forall i > 1$, então $t = 1$, logo $d(\{y_i\}_{i=1}^{\infty}, \{u_i\}_{i=1}^{\infty}) = \frac{1}{2}$. Assim, para todo

$\{y_i\}_{i=1}^{\infty}, \{u_i\}_{i=1}^{\infty} \in Y^{\mathbb{N}}$ temos que $0 \leq d(\{y_i\}_{i=1}^{\infty}, \{u_i\}_{i=1}^{\infty}) \leq 1$. Além disso, d é uma métrica em $Y^{\mathbb{N}}$.

Definição 4.2 *Considere o espaço métrico $(Y^{\mathbb{N}}, d)$ definido por (4.10). Um subconjunto $\mathcal{C} \subset Y^{\mathbb{N}}$ é dito* **completo** *quando $\mathcal{C}$ for fechado.*

Teorema 4.3 *Um código $\mathcal{C}$ associado a um codificador de Schreier $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é completo em $Y^{\mathbb{N}}$.*

Prova : Supondo o contrário. Então, existe uma seqüência de pontos de $\mathcal{C}$, $\{c_n\}_{n\in\mathbb{N}} \subset \mathcal{C}$ e um ponto $c \in Y^{\mathbb{N}} - \mathcal{C}$ no complemento de $\mathcal{C}$, tal que $c_n \xrightarrow{d} c$, com d definido em (4.10).

Como $c = \{c_i\}_{i=1}^{\infty} \notin \mathcal{C}$ e $\mathcal{C}$ possui um número finito de estados, então existe $k \in \mathbb{N}$ tal que $c_k \neq \beta_k(\overset{(k)}{x}, q)$ para todo $(\overset{(k)}{x}, q) \in X^i{}_{[\sigma,\mu]}Q$. Então, $d(\{y_i\}_{i=1}^{\infty}, c) \geq \frac{1}{2^k}$ para todo ponto $\{y_i\}_{i=1}^{\infty} \in \mathcal{C}$. Em particular, para os pontos $\{c_n\}_{n\in\mathbb{N}}$, temos $d(c_n, c) \geq \frac{1}{2^k}$, $\forall n \in \mathbb{N}$. Porém, $c_n \xrightarrow{d} c$, uma contradição. ■

Capítulo 5

Aplicações : Casos e Exemplos

Neste capítulo denominaremos ao grupo das saídas por *grupo dos rótulos* e ao grupo das entradas por *grupo das informações* . Os Teoremas 5.2, 4.2 e 4.3 são fundamentais no estabelecimento das condições necessárias e suficientes para que os codificadores sejam isomorfos, controláveis e completos. A controlabilidade é obtida considerando somente codificadores pertencentes à classe $M1$. Com isso, o Teorema 4.2,[1] poderá ser empregado.

Assumiremos que o grupo seção de treliça T definido em (3.2) é isomorfo ao grupo dos rótulos Y. Portanto, os codificadores serão isomorfos. A decomposição do grupo dos rótulos $Y \cong X_{(\sigma,\mu)}Q$ é feita de modo que $\mid X \mid < \mid Q \mid$. Para facilitar a análise, consideraremos os casos onde o grupo dos rótulos Y é abeliano e não abeliano.

Este capítulo é organizado como segue. Na Seção 5.1, propomos técnicas para construção de codificadores de Schreier isomorfos e controláveis independentemente do grupo da seção de treliça T ser abeliano ou não. Pelo Teorema 4.3 estes codificadores também são completos. Na Seção 5.2 propomos algoritmos de construção de codificadores isomorfos e controláveis para o caso abeliano distinguindo os subcasos binário e cíclico. Finalmente, na Seção 5.3 apresentamos a nossa versão da Proposição 4 de [4] sobre a limitação superior da distância livre do código quando o mesmo possui transições paralelas. Na nossa versão, esta

[1] O Teorema 4.2 pode ser empregado em qualquer codificador; o risco é desperdiçar esforços num codificador não controlável, que pode ser detectado pelo teste $M1$.

limitação está relacionada ao fato do grupo dos estados ser abeliano. Usando este resultado apresentamos uma construção de codificadores isomorfos e controláveis para o caso de T ser não abeliano.

5.1 Construção de Codificadores Isomorfos, Controláveis e Completos

Teorema 5.1 (Construção de codificadores controláveis isomorfos a partir das entradas e dos estados)

Dado um produto de Schreier $X_{(\sigma,\mu)}Q$, seja Y qualquer grupo isomorfo a $X_{(\sigma,\mu)}Q$ via β, isto é $Y \overset{\beta}{\cong} X_{(\sigma,\mu)}Q$. Seja $m \in \mathbb{N}$ definido por $m = \frac{|Q|}{2}$ se $|Q|$ é par e $m = \frac{|Q|+1}{2}$ se $|Q|$ é ímpar. Se H_0 e H_1, definidos respectivamente por (2.10) e (3.7), são tais que $H_0 \neq H_1$, e se existir um homomorfismo sobrejetor $\delta : X_{(\sigma,\mu)}Q \to Q$ tal que

$$\begin{aligned} &i) \quad Ker(\delta) = H_1 \\ &ii) \quad \left|\left\{\delta_m\left(\overset{(m)}{x}, e_Q\right) : \overset{(m)}{x} \in X^m\right\}\right| > m. \end{aligned}$$

Então, $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é um codificador isomorfo controlável.

Prova: Pelas hipóteses do teorema é obvio que $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é um codificador isomorfo. Só resta então provar a controlabilidade.

Seja Q_{0i} o subgrupo normal de Q definido no Lema 4.3. Pelo Teorema 4.2, temos que $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é não controlável se e somente se $|Q_{0i}| < |Q|$, para todo $i \in \mathbb{N}$. Mas, $|Q_{0i}| < |Q|$ implica que $|Q_{0i}| \leq \frac{|Q|}{2} \leq m$. Assim, $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é não controlável se e somente se $|Q_{0i}| \leq m$. Como $|Q_{0m}| > m$, então $Q_{0m} = Q$. Logo, $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é controlável. ■

Teorema 5.2 (Construção de codificadores isomorfos controláveis a partir das saídas)

Dado um grupo finito Y, suponha que $U_0 \lhd Y$ e $U_1 \lhd Y$ são subgrupos normais tais que:

$$\begin{aligned} &i) \quad |U_0| = |U_1| \\ &ii) \quad U_1 \neq U_0 \\ &iii) \quad \tfrac{Y}{U_1} \cong \tfrac{Y}{U_0}. \end{aligned}$$

Então,

- *Existe um produto de Schreier $X_{(\sigma,\mu)}Q$, para alguns X, Q e aplicações σ, μ satisfazendo (2.1) e (2.2) tais que $Y \overset{\xi}{\cong} X_{(\sigma,\mu)}Q$, para algum isomorfismo ξ.*

- *Se H_0 e H_1 são os subgrupos normais de $X_{(\sigma,\mu)}Q$ tais que $U_0 \overset{\xi}{\cong} H_0$ e $U_1 \overset{\xi}{\cong} H_1$, então H_0 satisfaz a equação (2.10); $H_1 \in \mathcal{X}$, onde $\mathcal{X}$ é definido por (2.9). Além disso $H_0 \neq H_1$.*

- *Se existir um homomorfismo sobrejetor $\delta : X_{(\sigma,\mu)}Q \to Q$ tal que*

$$\begin{aligned} &i) \quad Ker(\delta) = H_1 \\ &ii) \quad \left|\left\{\delta_m\left(\overset{(m)}{x}, e_Q\right) : \overset{(m)}{x} \in X^m\right\}\right| > m, \end{aligned}$$

  onde m é definido pelo Teorema 5.1 e $\beta = \xi^{-1}$. Então, $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é um codificador isomorfo controlável.

Prova:

- Pelo Teorema 2.4 e a sua prova, $Y \cong U_{0(\sigma_R,\mu_R)}\frac{Y}{U_0}$. Para $y \in Y$, seja $y_1 \in U_0$ e seja $y_2 \in R \subset Y$ o representante de $\frac{Y}{U_0}$, tal que $y = (y_1, y_2)$.

  Sejam X, Q grupos tais que $U_0 \overset{\theta_1}{\cong} X$ e $\frac{Y}{U_0} \overset{\theta_2}{\cong} Q$, para alguns isomorfismos θ_1 e θ_2. Então, $Y \cong U_{0(\sigma_R,\mu_R)}\frac{Y}{U_0} \overset{\xi}{\cong} X_{(\sigma,\mu)}Q$, onde $\xi = (\theta_1, \theta_2)$.

- Para $y = (y_1, y_2) \in Y \cong U_{0(\sigma_R,\mu_R)}\frac{Y}{U_0}$, temos que o representante de y em $X_{(\sigma,\mu)}Q$ é $(\theta_1(y_1), \theta_2(y_2))$. Em particular se $y \in U_0$, então $y = (y, e_Y)$, daí $\xi(y) = \xi(y, e_Y) = (\theta_1(y), \theta_2(e_Y)) = (\theta_1(y), e_Q) \in H_0 \subset X_{(\sigma,\mu)}Q$. Logo, H_0 satisfaz a equação (2.10).

Por outro lado, como $\frac{Y}{U_1} \cong \frac{Y}{U_0}$ e $\frac{Y}{U_0} \cong Q$ temos que $U_1 = Ker(\phi_1)$, onde ϕ_1 é algum homomorfismo sobrejetor $\phi_1 : Y \to Q$. Considere a composição de homomorfismos $\phi_1{}_o\xi^{-1} : X_{(\sigma,\mu)}Q \to Q$, então $\phi_1{}_o\xi^{-1}$ é sobrejetor e $Ker(\phi_1{}_o\xi^{-1})=\{(x,q) : \phi_1{}_o\xi^{-1}(x,q) = e_Q\} = \{(x,q) : \phi_1(\xi^{-1}(x,q)) = e_Q\} = \{(x,q) : \xi(y) = (x,q), \phi_1(y) = e_Q\} = H_1$. Finalmente, fica claro que $U_0 \neq U_1$ implica $H_0 \neq H_1$.

- Fazendo $\delta = \phi_1{}_o\xi^{-1}$, as condições do Teorema 5.1 são satisfeitas. ■

Corolário 5.2.1 (Construção de codificadores isomorfos controláveis a partir das entradas dos estados e das saídas)
Dados os grupos X, Q e Y, suponha que σ e μ são tais que seja possível construir o produto de Schreier $X_{(\sigma,\mu)}Q$ satisfazendo

- $X_{(\sigma,\mu)}Q \cong Y$
- $X_{(\sigma,\mu)}Q$ *cumpre as condições do Teorema 5.1*

Então, é possível obter um codificador isomorfo controlável $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$, onde β e δ estão definidos de acordo com o Teorema 5.1.

No exemplo a seguir, faremos uso do Teorema 5.2 ao código de Wei [20], com o objetivo de obter o correspondente codificador, ou equivalentemente, obter o grupo das entradas e o grupo dos estados.

Exemplo 5.1 *Considere o grupo de rótulos de permutações do código de Treliça CCITT V.32, encontrado por Trott na página 104 de [1]. Este grupo é isomorfo a um subgrupo de $\mathbb{D}_4 \oplus \mathbb{D}_4 = \mathbb{D}_4^2$.*

Mais precisamente,

$$Y = \left\{ \begin{array}{cccccccc} (R_0,R_0), & (R_0,R_2), & (R_0,d_1), & (R_0,d_2), & (R_2,R_0), & (R_2,R_2), & (R_2,d_1), & (R_2,d_2), \\ (R_1,V), & (R_1,H), & (R_1,R_1), & (R_1,R_3), & (R_3,V), & (R_3,H), & (R_3,R_1), & (R_3,R_3), \\ (d_1,V), & (d_1,H), & (d_1,R_1), & (d_1,R_3), & (d_2,V), & (d_2,H), & (d_2,R_1), & (d_2,R_3), \\ (V,R_0), & (V,R_2), & (V,d_1), & (V,d_2), & (H,R_0), & (H,R_2), & (H,d_1), & (H,d_2) \end{array} \right\}$$

Se $U_0 = \{(R_0,R_0),(R_0,R_2),(R_0,d_1),(R_0,d_2)\}$ e $U_1 = \{(R_0,R_0),(R_2,R_0),(V,R_0),(H,R_0)\}$ então $\frac{Y}{U_0} \cong \frac{Y}{U_1} \cong \mathbb{D}_4$. Assim, U_0, U_1 satisfazem às condições do Teorema 5.2. Sejam X, Q grupos tais que $X = \mathbb{Z}_2^2 \cong U_0$ e $Q = \mathbb{D}_4 \cong \frac{Y}{U_0}$. Seja $\sigma : \mathbb{D}_4 \to Aut(\mathbb{Z}_2^2)$ um homomorfismo tal que $\sigma(R_0) = \sigma(R_2) = \sigma(H) = \sigma(V) = id \in Aut(\mathbb{Z}_2^2)$ e

$$\sigma(R_1) = \sigma(R_3) = \sigma(d_1) = \sigma(d_2) : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$$

o mapeamento que associa os elementos de $\mathbb{Z}_2^2$ da seguinte maneira,

$$\begin{aligned} e &\mapsto e \\ a &\mapsto a \\ b &\mapsto c \\ c &\mapsto b. \end{aligned}$$

Dessa forma, obtemos o grupo $\mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4$. Seja $\xi : Y \to \mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4$ o mapeamento definido por

$$\begin{array}{cccc} (R_0,R_0) \mapsto (e,R_0) & (R_0,R_2) \mapsto (a,R_0) & (R_0,d_1) \mapsto (b,R_0) & (R_0,d_2) \mapsto (c,R_0) \\ (R_1,R_1) \mapsto (e,R_1) & (R_1,R_3) \mapsto (a,R_1) & (R_1,V) \mapsto (b,R_1) & (R_1,H) \mapsto (c,R_1) \\ (R_2,R_2) \mapsto (e,R_2) & (R_2,R_0) \mapsto (a,R_2) & (R_2,d_2) \mapsto (b,R_2) & (R_2,d_1) \mapsto (c,R_2) \\ (R_3,R_3) \mapsto (e,R_3) & (R_3,R_1) \mapsto (a,R_3) & (R_3,H) \mapsto (b,R_3) & (R_3,V) \mapsto (c,R_3) \\ (d_1,V) \mapsto (e,d_1) & (d_1,H) \mapsto (a,d_1) & (d_1,R_1) \mapsto (b,d_1) & (d_1,R_3) \mapsto (c,d_1) \\ (d_2,H) \mapsto (e,d_2) & (d_2,V) \mapsto (a,d_2) & (d_2,R_3) \mapsto (b,d_2) & (d_2,R_1) \mapsto (c,d_2) \\ (V,d_2) \mapsto (e,V) & (V,d_1) \mapsto (a,V) & (V,R_2) \mapsto (b,V) & (V,R_0) \mapsto (c,V) \\ (H,d_1) \mapsto (e,H) & (H,d_2) \mapsto (a,H) & (H,R_0) \mapsto (b,H) & (H,R_2) \mapsto (c,H) \end{array}$$

Então, ξ é um isomorfismo. Portanto, $\mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4 \cong Y$. Os subgrupos $H_0 \lhd \mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4$ e $H_1 \lhd \mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4$ tais que $H_0 \cong U_0$, $H_1 \cong U_1$ são,

$$H_0 = \{(e,R_0),(a,R_0),(b,R_0),(c,R_0)\} \text{ e } H_1 = \{(e,R_0),(a,R_2),(b,H),(c,V)\}.$$

classe lateral		conteúdo do classe lateral	ordem da classe lateral
H_1	=	$\{(e,R_0),(a,R_2),(b,H),(c,V)\}$	(2)
$H_1(a,R_0)$	=	$\{(a,R_0),(e,R_2),(c,H),(b,V)\}$	(2)
$H_1(b,R_0)$	=	$\{(b,R_0),(c,R_2),(e,H),(a,V)\}$	(2)
$H_1(c,R_0)$	=	$\{(c,R_0),(b,R_2),(a,H),(e,V)\}$	(2)
$H_1(b,R_1)$	=	$\{(b,R_1),(c,R_3),(e,d_1),(a,d_2)\}$	(2)
$H_1(a,R_1)$	=	$\{(a,R_1),(e,R_3),(c,d_1),(b,d_2)\}$	(4)
$H_1(e,R_1)$	=	$\{(e,R_1),(a,R_3),(b,d_1),(c,d_2)\}$	(4)
$H_1(c,R_1)$	=	$\{(c,R_1),(b,R_3),(a,d_1),(e,d_2)\}$	(2)

Tabela 5.1: **O grupo das classes laterais** $\frac{\mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4}{H_1}$

As classes laterais à direita são mostradas na Tabela 5.1.

Seja $H_2 = \{(e,000)\}$ o subgrupo trivial de $\mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4$. Então H_0, H_1 e H_2 satisfazem às condições do Teorema 3.2. Portanto, definimos o homomorfismo $\delta : \mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4 \to \mathbb{D}_4$ como sendo

$$\begin{aligned} \delta(H_1) = R_0 \quad & \delta(H_1(a,R_0)) = R_2 \\ \delta(H_1(e,R_1)) = R_1 \quad & \delta(H_1(a,R_1)) = R_3 \\ \delta(H_1(b,R_0)) = d_1 \quad & \delta(H_1(c,R_0)) = d_2 \\ \delta(H_1(b,R_1)) = V \quad & \delta(H_1(c,R_1)) = H. \end{aligned}$$

Claramente δ é sobrejetora.

Definindo $\beta : \mathbb{Z}_{2(\sigma)}^2\mathbb{D}_4 \to Y$ como sendo $\beta = \xi^{-1}$, obtemos o codificador $M_\sigma = (\mathbb{Z}_2^2, Y, \mathbb{D}_4, \delta, \beta)$ para código de treliça V32.

Observação :

No Exemplo 5.1, os grupos U_0, U_1 não são os únicos satisfazendo às condições do Teorema

5.2. Por exemplo, os subgrupos

$$U_0' = \{(R_0, R_0), (R_0, R_2), (R_2, R_0), (R_2, R_2), (d_1, V), (d_1, H), (d_2, V)(d_2, H)\}$$

e

$$U_1' = \{(R_0, R_0), (R_0, R_2), (R_2, R_0), (R_2, R_2), (V, R_0), (V, R_2), (H, R_0)(H, R_2)\};$$

são tais que $U_0' \neq U_1\prime$, $U_0' \cong \mathbb{Z}_2^3$, $\frac{T}{U_0'} \cong \frac{T}{U_1'} \cong \mathbb{Z}_4$. Portanto, considerando $X = \mathbb{Z}_2^3$ e $Q = \mathbb{Z}_4$, podemos encontrar σ e μ tais que $X_{(\sigma,\mu)}Q \cong Y$.

Assim, dado um grupo de rótulos Y, usando o Teorema 5.2 podemos obter mais de um código de Schreier com rótulos em Y. Portanto, critérios de escolha do melhor código de Schreier associado a Y são necessários. O propósito das próximas seções é o de fornecer tais critérios. Para maior clareza apresentaremos os casos em que o grupo dos rótulos Y é abeliano e não abeliano.

5.2 Caso Abeliano

Quando $G = X_{(\sigma,\mu)}Q$ é abeliano, pela Proposição 2.1, σ deve ser a identidade. Assim, G é o produto direto $X_{\oplus}Q$ ou o produto cíclico $X_{(\mu)}Q$ do grupo das informações e o grupo dos estados. Com base neste fato, consideramos dois subcasos especiais.

5.2.1 Subcaso binário : $Y \approx \mathbb{Z}_2^n \approx \mathbb{Z}_2^k \oplus \mathbb{Z}_2^{n-k}$

Tendo como base o Teorema 5.2, apresentamos um algoritmo para a construção da máquina $M = (\mathbb{Z}_2^k, \mathbb{Z}_2^n, \mathbb{Z}_2^{n-k}, \delta, \beta)$ associada a um código convolucional binário de taxa $r = k/n$ e memória $m = n - k$.

Algoritmo

Passo 1 - Encontrar $U_0 \lhd \mathbb{Z}_2^n$ e $U_1 \lhd \mathbb{Z}_2^n$ tal que,
1a $|U_0| = |U_1| = 2^k$.

1b $U_0 \neq U_1$.

1c Se $peso(U_0) = d_0$ e $peso(U_1) = d_1$, então $d_0 + d_1 = d$, deve ser tal que

$$d = max\{peso(V_0) + peso(V_1)\},$$

V_0 e V_1 estão sujeitos a V_0, $V_1 \lhd \mathbb{Z}_2^n$; $\mid V_0 \mid = \mid V_1 \mid = 2^k$ e $V_0 \neq V_1$.

1d De modo a evitar transições paralelas, então $U_0 \cap U_1 = 0 \in \mathbb{Z}_2^n$.

Passo 2 - Considere U_0 e U_1 como subespaços vetoriais de $\mathbb{Z}_2^n$, e considere as bases $\{u_1, \ldots, u_k\}$ de U_0, e $\{u_1, \ldots, u_t, v_1, \ldots, v_{k-s}\}$ de U_1. Note que $s = 0$ se e somente se $U_0 \cap U_1 = 0 \in \mathbb{Z}_2^n$.

Passo 3 - Seja $\{e_i\}_{i=1}^n$ a base canônica de $\mathbb{Z}_2^n$, onde e_i é definida por $e_i = (x_1, \ldots, x_i, \ldots, x_n)$ e seus componentes são tais que $x_j = 0$ if $j \neq i$ e $x_j = 1$ se $j = i$. Então, defina o *mapeamento de rotulamentos* como sendo o isomorfismo $\beta : \mathbb{Z}_{2\oplus}^k \mathbb{Z}_2^{n-k} \rightarrow \mathbb{Z}_2^n$ tal que

$$\beta^{-1}(u_i) = e_i,$$
$$\beta^{-1}(v_j) = e_{k+j};$$

com a finalidade de otimizar a distância livre, a definição de β para os restantes $n - (2k - s)$ vetores da base $\{e_i\}_{i=1}^n$ é deixada para o **Passo 7**.

Passo 4 - Calcular $H_0 = \beta^{-1}(U_0)$, $H_1 = \beta^{-1}(U_1)$, e $\Pi_2(H_1)$, onde $\Pi_2 : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{n-k}$ é a projeção definida por $\Pi_2(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) = (x_{k+1}, \ldots, x_n)$.

Passo 5 - Usando os elementos do grupo das classes laterais $\frac{\mathbb{Z}_2^n}{H_1}$, defina a *aplicação do próximo estado* como sendo o homomorfismo de grupos $\delta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{n-k}$ com as seguintes condições

5a $Ker(\delta) = H_1$, significando que

$$\delta(e_{k+j}) = 0 \text{ para } j = 1, \ldots, k - s.$$

5b Se $n - (2k - s) > 0$ então, $\delta(H_0) \cap \Pi_2(H_1) = 0 \in \mathbb{Z}_2^{n-k}$, significando que

$$\delta(e_i) \notin \Pi_2(H_1), \text{ para } i = 1, \ldots, k.$$

Passo 6 - A definição de δ para os remanescentes $n - (2k - s)$ vetores da base $\{e_i\}_{i=1}^n$ deve ser feito de modo que,

6a Satisfaça o teste de controlabilidade: $\left|\left\{\delta_{2^{n-k-1}}\binom{(2^{n-k-1})}{x}, 00\right) : {}^{(2^{n-k-1})}_{x} \in \mathbb{Z}_2^{k.2^{n-k-1}}\right\}\right| > 2^{n-k-1}$.

6b Tratando de que $\delta(x, \delta(H_0)) \notin \Pi_2(H_1)$ para todo $x \in X$.

6c Se $\delta(x, \delta(H_0)) \notin \Pi_2(H_1)$ para todo $x \in X$ então, fazer outra tentativa para que $\delta(x_2, \delta(x_1, \delta(H_0))) \notin \Pi_2(H_1)$, para todo x_2, $x_1 \in X$. Tentar outra vez para $x_3 \in X$, e assim por diante.

Usando a definição de δ com relação à base $\{e_i\}_{i=1}^n$, escrever a regra explícita de δ.

Passo 7 - Defina β para os remanescentes $n-(2k-s)$ vetores da base $\{e_i\}_{i=1}^n$ fazendo uma adequada distribuição dos pesos conforme a dinâmica da treliça obtida através de δ no **Passo 5** e **Passo 6**.

Usando a definição de β em relação à base $\{e_i\}_{i=1}^n$, escrever a regra explícita de β.

Este algoritmo gera a máquina $M = (\mathbb{Z}_2^k, \mathbb{Z}_2^n, \mathbb{Z}_2^{n-k}, \delta, \beta)$ associada a um código convolucional binário, não catastrófico com taxa $r = k/n$, memória $m = n-k$, e $d_{free} \geq d$.

Exemplo 5.2 *Construção de um código convolucional binário a partir da máquina* $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^4, \mathbb{Z}_2^2, \delta, \beta)$

Passo 1 - Determinação de U_0 e U_1,

$$U_0 = \{0000, 1001, 1110, 0111\} \quad U_1 = \{0000, 1100, 0011, 1111\}$$

Então, os pesos de U_0 e de U_1 são $peso(U_0) = peso(U_1) = 2$, respectivamente.

Passo 2 - Determinação das bases para U_0 e para U_1: $\{1001, 1110\}$ é uma base para U_0, e $\{1100, 0011\}$ é uma base para U_1.

Note que, como $U_0 \cap U_1 = 0000$, então $s = 0$.

Passo 3 -

$$\beta^{-1}(1001) = 1000 \qquad \beta^{-1}(0011) = 0010$$
$$\beta^{-1}(1110) = 0100 \qquad \beta^{-1}(1100) = 0001$$

Passo 4 -

$$H_0 = \{(00,00), (10,00), (01,00), (11,00) \quad H_1 = \{(00,00), (00,10), (00,01), (00,11)\}$$

$$\Pi_2(H_1) = \{00, 10, 01, 11\}$$

Passo 5 - Para que $Ker(\delta) = H_1$, devemos ter que

$$\delta(00, 10) = 00$$
$$\delta(00, 01) = 00$$

Como $n - (2k - s) = 4 - (4 - 0) = 0$ então , não é possível que $\delta(H_0) \cap \Pi_2(H_1) = 00$, logo

$$\delta(10, 00) = 11$$
$$\delta(01, 00) = 01$$

Passo 6 -Neste exemplo não existem $n - (2k - s)$ vetores remanescentes $\{e_i\}_{i=1}^4$, pois $n - (2k - s) = 4 - (4 - 0) = 0$. Portanto, δ é dado por

$$\begin{aligned}\delta(x_2, x_1; q_1, q_2) &= x_2\delta(e_1) + x_1\delta(e_2) + q_1\delta(e_3) + q_2\delta(e_4) \\ &= x_2.11 + x_1.01 + q_1.00 + q_2.00 \\ &= (x_2, x_2 + x_1)\end{aligned}$$

Passo 7 - Como não há vetores remanescentes, resta escrever a regra de correspondência de β, isto é,

$$\begin{aligned}\beta(x_2, x_1; q_1, q_2) &= x_2\beta(e_1) + x_1\beta(e_2) + q_1\beta(e_3) + q_2\beta(e_4) \\ &= x_2.1001 + x_1.1110 + q_1.0011 + q_2.1100 \\ &= (x_2 + x_1 + q_2, x_1 + q_2, x_1 + q_1, x_2 + q_1)\end{aligned}$$

O codificador resultante é mostrado na Fig. 5.1. O código correspondente têm taxa $R_c = \frac{1}{2}$, distância livre $d_{free} = 5$ e um ganho assintótico de 3.98 dB.

5.2.2 Subcaso cíclico : $Y \approx \mathbb{Z}_{p^n} \approx \mathbb{Z}_{p^k(\mu)}\mathbb{Z}_{p^{n-k}}$

Proposição 5.1 *Se o grupo seção de treliça T é cíclico, então o codificador com o qual esta associaciado é não controlável.*

Prova : Se T é cíclico, então $T \cong \mathbb{Z}_{p^n}$, para algum primo p e para algum $n \in \mathbb{N}$. A única maneira de decompor $\mathbb{Z}_{p^n}$ é $\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^k(\mu)}\mathbb{Z}_{p^{n-k}}$. Mas, existe um único subgrupo $U_0 \lhd \mathbb{Z}_{p^n}$

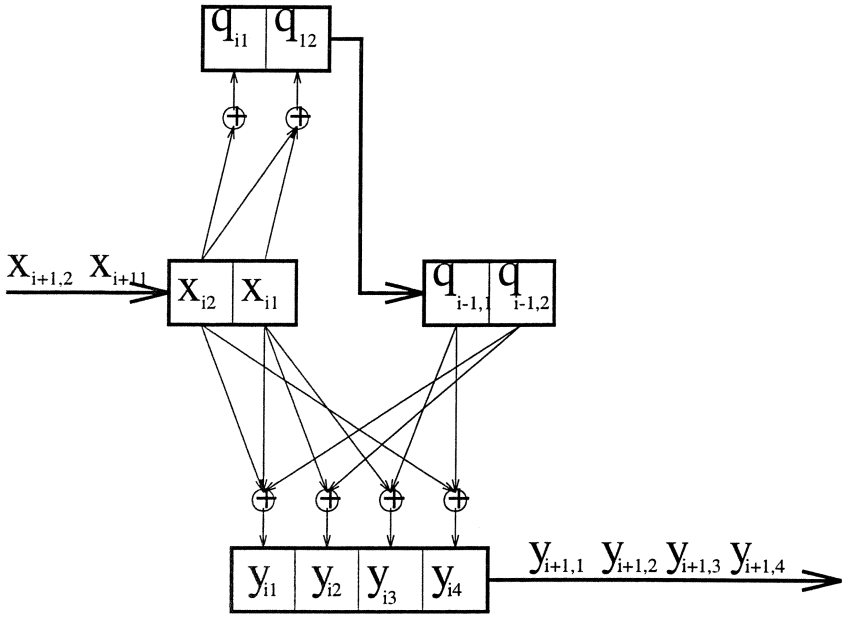

Figura 5.1: Codificador de Schreier $M_{\oplus} = (\mathbb{Z}_2^k, \mathbb{Z}_2^n, \mathbb{Z}_2^{n-k}, \delta, \beta)$.

tal que $|U_0| = |\mathbb{Z}_{p^k}| = p^k$. Assim, o subgrupo $H_0 \lhd \mathbb{Z}_{p^k}{}_{(\mu)}\mathbb{Z}_{p^{n-k}}$ definido em (3.7) é o único subgrupo normal com cardinalidade p^k de $\mathbb{Z}_{p^k}{}_{(\mu)}\mathbb{Z}_{p^{n-k}}$. Portanto, pela Proposição 3.4, o codificador é não controlável. ■

No caso em que $Y \cong T$, temos que o grupo dos rótulos Y não poderá ser cíclico. No entanto, é possível que Y seja cíclico quando $|Y| < |T|$, nesse caso é suficiente que $Ker(\beta) \neq \{elemento\, neutro\, de\, X_{(\sigma,\mu)}Q\}$ e que $\frac{X_{(\sigma,\mu)}Q}{Ker(\beta)}$ seja cíclico (veja o codificador de Ungerboeck no Exemplo 3.6).

5.3 Caso Não Abeliano

Se $Y \cong X_{(\sigma,\mu)}Q$ é não abeliano então a aplicação σ é diferente da identidade (Veja Proposição 2.1). Para analisar este caso apresentamos uma versão do Teorema 4 de [4].

Proposição 5.2 *Seja $G = X_{(\sigma,\mu)}Q$ um grupo não abeliano. Seja $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ um codificador controlável obtido de $X_{(\sigma,\mu)}Q$. Se o grupo dos estados Q é abeliano então, a seção de treliça tem transições paralelas.*

Prova: Como Q é abeliano, então $\frac{X_{(\sigma,\mu)}Q}{H_0} \cong \frac{X_{(\sigma,\mu)}Q}{H_1}$ são grupos de classes laterais abelianos, onde H_0 e H_1 são dados por (2.10) e (3.7). Então o subgrupo dos comutadores $G' \subset G$ é tal que $G' \subset H_0 \cap H_1$. Mas, G não abeliano implica que $G' \neq e_G$. Portanto , $H_0 \cap H_1 \neq e_G$. ■

É muito importante notar que a recíproca da Proposição 5.2 é falsa. O Exemplo 3.5 é um codificador com grupo seção de treliça não abeliano e grupo de estados não abeliano, no entanto possui transições paralelas.

Agora, quando Q é abeliano, então pela Proposição 5.2, teremos que a distância livre d_{free} do código resultante do codificador $M_{(\sigma,\mu)} = (X, Y, Q, \delta, \beta)$ é limitada superiormente pela distância entre as transições paralelas que são rotuladas por $Y' = \beta(H_0 \cap H_1)$. Assim, Y' é um subgrupo normal de Y. Note que, se cada elemento de Y é representado por um único símbolo de algum alfabeto, então a distância mínima de Hamming de Y' é 1.

Portanto, um alfabeto e uma distância adequadas devem ser usados. Se considerarmos a distância Euclidiana, então o grupo Y deve ser isomorfo a um grupo Γ que esteja atuando isometricamente sobre um subconjunto de pontos $S \subset \mathbb{R}^m$, onde $\mathbb{R}$ é o conjunto dos números reais. Quando a ação é transitiva, então diz-se que o código é *geometricamente uniforme,* e que S está casado com Y. O grupo das classes laterais $\frac{Y}{Y'}$ determina uma partição de S em *células* $S = \bigcup_{i=1}^{a} S_i$ onde a é a cardinalidade do grupo $\frac{Y}{Y'}$. Cada célula é invariante pela ação da correspondente classe determinada por Y'.

Como Γ atua transitivamente sobre S, então existe $s_0 \in S$ (o ponto inicial ou o centro de referência de S) tal que para todo $s \in S$ existe $\gamma \in \Gamma$ com $s = \gamma(s_0)$. Por outro lado, como $\Gamma \cong Y$ então, para cada $y \in Y$ existe um único $\gamma = \gamma_y \in \Gamma$ casado com y. Portanto, para todo $y \in Y$, é possível definir o número real $peso(y) \in \mathbb{R}$ com sendo

$$peso(y) = \|\gamma_y(s_0) - s_0\|, \tag{5.1}$$

onde o símbolo $\|.\|$ denota a norma Euclidiana $\|(x_1,\ldots,x_m)\| = \sqrt{x_1^2+\ldots+x_m^2}$. Note que $peso(e_Y) = \|\gamma_{e_Y}(s_0) - s_0\| = 0$. Se cada γ_y, que está atuando sobre S, pode ser estendido a todo o espaço ambiente $\mathbb{R}^m$ preservando sua propriedade isométrica[2], teremos $\gamma_y : \mathbb{R}^m \to \mathbb{R}^m$ é tal que $\|\gamma_y(x)\| = \|x\|$, para todo $x \in \mathbb{R}^m$ e para todo $y \in Y$. Em particular, se $y_1,\ y_2 \in Y$ para o ponto $(\gamma_{y_1}(s_0) - \gamma_{y_2}(s_0)) \in \mathbb{R}^m$ temos $\|\gamma_{y_2{}^{-1}}(\gamma_{y_1}(s_0) - \gamma_{y_2}(s_0))\| = \|\gamma_{y_1}(s_0) - \gamma_{y_2}(s_0)\|$. Porém, $\|\gamma_{y_2{}^{-1}}(\gamma_{y_1}(s_0) - \gamma_{y_2}(s_0))\| = \|\gamma_{y_1.y_2{}^{-1}}(s_0) - s_0\| = peso(y_1.y_2^{-1})$. Esta propriedade permite definir a *distância* de y_1 a y_2 ou reciprocamente de y_2 a y_1 como

$$d(y_1,y_2) = peso(y_1.y_2^{-1}). \tag{5.2}$$

Se $U \subset Y$ é um subconjunto de Y, então

$$peso(U) = min\{d(y_1,y_2) : y_1,y_2 \in U\,, y_1 \neq y_2\} = min\{peso(y_1.y_2^{-1}) : y_1,y_2 \in U\,, y_1 \neq y_2\}.$$

Porém, $y_3 = y_1.y_2^{-1} \in Y$ com $y_3 = e_Y$ se e somente se $y_1 = y_2$. Portanto, podemos definir $peso(U)$ como

$$peso(U) = min\{peso(y) : y \in U,\ y \neq e_Y\}.$$

Considerando o caso multinível, para $(y_1,\ldots,y_n) \in Y^n$, defina

$$peso(y_1,\ldots,y_n) = \sum_{i=1}^{n} peso(y_i).$$

Finalmente, se $V \subset Y^n$ é um subconjunto de Y^n então

$$peso(V) = min\{peso(y_1,\ldots,y_n) : (y_1,\ldots,y_n) \in V,\ (y_1,\ldots,y_n) \neq (e_Y,\ldots,e_Y)\}.$$

A seguir, apresentamos um algoritmo para a construção de codificadores em que o *grupo dos rótulos* é não abeliano. Este algoritmo é baseado no produto de Schreier multinível e na construção do produto de Schreier para grupos cíclicos (Teorema 2.3, Corolário 2.3.1, e Proposição 2.2), isto é ,

$$Y^n \cong (X_{1\oplus}\ldots_{\oplus} X_n)_{(\overline{\sigma},\overline{\mu})}(Q_{1\oplus}\ldots_{\oplus} Q_n),$$

onde $Y \cong X_{i(\sigma_i,\mu_i)}Q_i$ para $i = 1,\ldots,n$, é tal que X_i e Q_i são grupos cíclicos para algum j, isto é $X_j = \mathbb{Z}_s$ e $Q_j = \mathbb{Z}_t$. Portanto, $Y \cong \mathbb{Z}_{s(\sigma_j,\mu_j)}\mathbb{Z}_t$.

[2]Condições para tal extensão são apresentadas em [2]

Algoritmo

Passo 1 - Encontrar os subgrupos normais U_0 e U_1 em Y^n tais que,

1a) $U_0 \cong X_{1\oplus} \ldots_{\oplus} X_n$.

1b) $|U_1| = |U_0|$.

1c) $U_0 \neq U_1$.

1d) $\frac{Y^n}{U_0} \cong \frac{Y^n}{U_1} \cong Q_{1\oplus} \ldots_{\oplus} Q_n$.

1e) Se $peso(U_0) = d_0$ e se $peso(U_1) = d_1$, então $d_0 + d_1 = d$, onde

$$d = max\{peso(V_0) + peso(V_1)\}$$

V_0 and V_1 estão sujeitos a V_0, $V_1 \lhd \mathbb{Z}_2^n$; $\mid V_0 \mid = \mid V_1 \mid = 2^k$; $V_0 \neq V_1$ e $\frac{Y^n}{V_0} \cong \frac{Y^n}{V_1} \cong Q_{1\oplus} \ldots_{\oplus} Q_n$.

1f) Para evitar transições paralelas U_0 e U_1 devem satisfazer $U_0 \cap U_1 = \{elemento\, neutro\}$. Nesse caso, $Q_{1\oplus} \ldots_{\oplus} Q_n$ deve ser não abeliano.

Passo 2 - Usando os geradores canônicos de $\mathbb{Z}_{s(\sigma_j,\mu_j)}\mathbb{Z}_t$, dados em (2.15), considere a família $\{e_i\}_{i=1}^{2n}$ onde $e_i = (e_{i1}, \ldots, e_{i,2n})$ é uma base, isto é , um conjunto de geradores Y^n, com $e_{ij} \in \begin{cases} \mathbb{Z}_s & \text{se } j \text{ ímpar} \\ \mathbb{Z}_t & \text{se } j \text{ par} \end{cases}$ e $e_{ij} = \begin{cases} 0 & \text{se } j \neq i \\ 1 & \text{se } j = i \end{cases}$, para cada $i = 1, \ldots, 2n$.

Através desta base de geradores de Y^n determinar os geradores de U_0 e de U_1 e a correspondente família de geradores $\{g_i\}_{i=1}^{2n}$ de $(X_{1\oplus} \ldots_{\oplus} X_n)_{(\overline{\sigma},\overline{\mu})}(Q_{1\oplus} \ldots_{\oplus} Q_n)$ casado a $\{e_i\}_{i=1}^{2n}$.

Passo 3 - Considere $H_0 \lhd (X_{1\oplus} \ldots_{\oplus} X_n)_{(\overline{\sigma},\overline{\mu})}(Q_{1\oplus} \ldots_{\oplus} Q_n)$, como definida em (2.10). Use estes geradores para definir a aplicação dos rotulamentos $\beta : (X_{1\oplus} \ldots_{\oplus} X_n)_{(\overline{\sigma},\overline{\mu})}(Q_{1\oplus} \ldots_{\oplus} Q_n) \to Y^n$ tal que $H_0 = \beta^{-1}(U_0)$;

Passo 4 - Calcule $H_1 = \beta^{-1}(U_1)$ e $\Pi_2(H_1)$, onde $\Pi_2 : (X_{1\oplus} \ldots_{\oplus} X_n)_{(\overline{\sigma},\overline{\mu})}(Q_{1\oplus} \ldots_{\oplus} Q_n) \to Q_{1\oplus} \ldots_{\oplus} Q_n$ é a projeção $\Pi(x_1 \ldots, x_n; q_1, \ldots, q_n) = (q_1, \ldots, q_n)$.

Passo 5 - Defina $\delta : (X_{1\oplus} \ldots_{\oplus} X_n)_{(\overline{\sigma},\overline{\mu})}(Q_{1\oplus} \ldots_{\oplus} Q_n) \to Q_{1\oplus} \ldots_{\oplus} Q_n$ tal que $Ker(\delta) = H_1$. Note que δ deve satisfazer o teste de controlabilidade, isto é , se $m = \frac{|Q_1|.|Q_2|\ldots|Q_n|}{2}$, então $\left\{\delta_m \left(\overset{(m)}{x}, e_{Q_1 \ldots Q_n}\right) : \overset{(m)}{x} \in (X_{1\oplus} \ldots_{\oplus} X_n)^m\right\}$ deve ser tal que $\left|\left\{\delta_m \left(\overset{(m)}{x}, e_{Q_1 \ldots Q_n}\right) : \overset{(m)}{x} \in (X_{1\oplus} \ldots_{\oplus} X_n)^m\right\}\right| > m$.

Exemplo 5.3 *Considere o grupo $\mathbb{D}_4$, as simetrias do quadrado. Pelo Exemplo 2.3 sabemos que $\mathbb{D}_4 \cong \mathbb{Z}_{4(\sigma)}\mathbb{Z}_2$. Por outro lado, sabemos também que $\mathbb{D}_4 \cong \{e\}_{\oplus}\mathbb{D}_4$. Aplicando o Teorema 2.3 e o Corolário 2.3.1, temos que $\mathbb{D}_4^2 \cong (\mathbb{Z}_{4\oplus}\{e\})_{(\overline{\sigma})}(\mathbb{Z}_{2\oplus}\mathbb{D}_4) \cong \mathbb{Z}_{4(\overline{\sigma})}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)$. Isto significa que a treliça que esta sendo construída têm $\mathbb{Z}_4$ como o grupo de informações e $\mathbb{Z}_2 \oplus \mathbb{D}_4$ como o grupo de estados.*

Passo 1 - Considerando $U_0 = \{R_0R_0, R_1R_0, R_2R_0, R_3R_0\}$ e $U_1 = \{R_0R_0, R_0R_1, R_0R_2, R_0R_3\}$ temos que

a) $|U_0| = |U_1| = |\mathbb{Z}_4|$

b) $U_0 \neq U_1$

c) $\frac{\mathbb{D}_4^2}{U_0} \cong \frac{\mathbb{D}_4^2}{U_1} \cong \mathbb{Z}_{2\oplus}\mathbb{D}_4$.

Passo 2 - Usando a Tabela 2.2, os elementos de $\mathbb{D}_4^2$ podem ser escritos como

$$\mathbb{D}_4^2 = \{(x_1x_2, y_1y_2) \ : \ x_1, y_1 \in \mathbb{Z}_4 \text{ e } x_2, y_2 \in \mathbb{Z}_2\}.$$

Portanto, a base canônica de $\mathbb{D}_4^2$ é $\alpha = \{(10,00),(01,00),(00,10),(00,01)\}$. Desta maneira, o gerador de U_0 é $\{(10,00)\}$ e o gerador de U_1 é $\{(00,10)\}$. Por outro lado, uma base para $\mathbb{Z}_{4(\overline{\sigma})}(\mathbb{Z}_{2\oplus}\mathbb{D}_4)$ casada com α é $\alpha' = \{(1,000),(0,100),(0,010),(0,001)\}$.

Passo 3 - Defina o mapeamento dos rótulos como o isomorfismo $\beta : \mathbb{Z}_{4(\overline{\sigma})}(\mathbb{Z}_{2\oplus}\mathbb{D}_4) \rightarrow \mathbb{D}_4^2$ dado por

$$\begin{aligned}(1,000) &= \beta^{-1}(10,00)\\ (0,100) &= \beta^{-1}(01,00)\\ (0,010) &= \beta^{-1}(00,10)\\ (0,001) &= \beta^{-1}(00,01).\end{aligned}$$

Desse modo, β é dado por

$$\begin{aligned}\beta(x_1,q_1,q_2,q_3) &= \beta(1,000)^{x_1}.\beta(0,100)^{q_1}.\beta(0,010)^{q_2}.\beta(0,001)^{q_3}\\ &= (10,00)^{x_1}.(01,00)^{q_1}.(00,10)^{q_2}.(00,01)^{q_3}.\end{aligned}$$

Passo 4 - $H_0 = \{(0,000),(1,000),(2,000),(3,000)\}$, $H_1 = \{(0,000),(0,010),(0,020),(0,030$ e $\Pi_2(H_1) = \{000,010,020,030\}$.

Passo 5 - Defina $\delta : \mathbb{Z}_{4(\overline{\sigma})}(\mathbb{Z}_{2\oplus}\mathbb{D}_4) \rightarrow \mathbb{Z}_{2\oplus}\mathbb{D}_4)$ como sendo

$$\begin{aligned}
\delta(1,000) &= (1,10) \\
\delta(0,100) &= (1,11) \\
\delta(0,010) &= (0,00) \\
\delta(0,001) &= (1,01).
\end{aligned}$$

Note que não foi possível obter $\delta(H_0) \cap \Pi_2(H_1) = \{0,00\}$, devido ao fato de que se $\delta(1,000) = (u, v_1v_2)$, onde $u \in \mathbb{Z}_2$, $v_1 \in \mathbb{Z}_4$ e $v_2 \in \mathbb{Z}_2$, então para $(2,000) \in H_0$ teremos $\delta(2,000) = \delta((1,000)^2) = (u, v_1v_2)^2$. No entanto, para todo $u, v_1v_2 \in \mathbb{Z}_{2\oplus}\mathbb{D}_4$, $(u, v_1v_2)^2 = (0, z\,0)$ para algum $z \in \mathbb{Z}_4$. Portanto, δ é dado por

$$\begin{aligned}
\delta(x_1, q_1, q_2, q_3) &= \delta(1,000)^{x_1}.\delta(0,100)^{q_1}.\delta(0,010)^{q_2}.\delta(0,001)^{q_3} \\
&= (1,10)^{x_1}.(1,11)^{q_1}.(0,00)^{q_2}.(1,01)^{q_3} \\
&= (1,10)^{x_1}.(1,11)^{q_1}.(1,01)^{q_3}.
\end{aligned}$$

Sob esta condição, o código de Schreier resultante, associado ao codificador $M_{\overline{\sigma}} = (Z_4, \mathbb{D}_4^2, \mathbb{Z}_{2\oplus}\mathbb{D}_4, \delta$ está casado a um código Euclidiano cujos rótulos formam o conjunto de sinais 2×8-PSK. Este código Euclidiano alcança uma distância livre Euclidiana quadrática $d_{free} = 8$. O codificador $M_{\overline{\sigma}} = (Z_4, \mathbb{D}_4^2, \mathbb{Z}_{2\oplus}\mathbb{D}_4, \delta, \beta)$ é mostrado na Fig 5.2, onde as duplas caixas denotam elementos de $\mathbb{Z}_4$ e as caixas simples elementos de $\mathbb{Z}_2$, os círculos com chapéu denotam exponenciação e o círculo com um ponto operação de multiplicação .

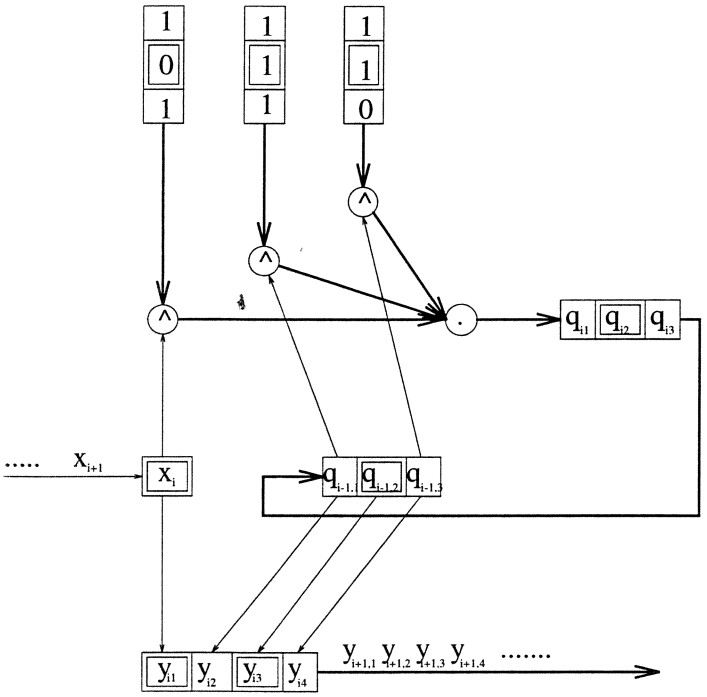

Figura 5.2: Codificador de Schreier $M_{\overline{\sigma}} = (\mathbb{Z}_4, \mathbb{D}_4^2, \mathbb{Z}_{2\oplus}\mathbb{D}_4, \delta, \beta)$.

Capítulo 6

Considerações Finais

O objetivo principal deste trabalho foi o de propor algoritmos de construção de bons códigos convolucionais sobre grupos. Os principais itens do programa que traçamos com este objetivo foram:

- Em [1, 18] é mostrado que o grupo dos estados Q_k é isomorfo ao grupo quociente $\frac{T_k}{X_k}$ do grupo seção de treliça T_k e do grupo das entradas X_k, em cada instante de tempo k. Em aritmética elementar é simples mostrar a equivalência das expresões $\frac{a}{b} = c$ e $a = bc$, se $b \neq 0$. Com a introdução do produto de Schreier, mostramos que este fato aritmético também vale para grupos, isto é, a expressão $Q_k \cong \frac{T_k}{X_k}$ é equivalente a $T_k \cong X_{k(\sigma,\mu)}Q_k$.

- Para facilitar a determinação de bons códigos, restringimos a busca sobre os códigos invariantes no tempo e com número de estados finito. Isto é, $Q_k = Q$, $T_k = T$, $X_k = X$, para todo $k \in \mathbb{Z}$ e $|Q| < \infty$. Estas restrições possibilitaram estabelecer critérios para se obter códigos controláveis e completos. Isto porque todo bom código é, necessariamente, controlável e completo.

- Um grupo T pode ter diferentes decomposições, isto é, pode existir uma família de produtos de Schreier $\{X_{i(\sigma_i,\mu_i)}Q_i\}_{i=1}^{n}$ tal que $T \cong X_{i(\sigma_i,\mu_i)}Q_i$ para cada $i = 1, \ldots, n$. A melhor decomposição será aquela cuja treliça tenha baixa complexidade e forneça uma

boa distância livre. Desse modo, algoritmos que se baseiam na escolha das melhores decomposições dos grupos de seção de treliça foram propostos.

6.1 Conclusões

Como resultado do estudo do produto de Schreier, apresentamos os códigos de Schreier. Estes códigos formam uma classe intermediária entre os tradicionais códigos convolucionais binários e os *group codes* apresentados em [1]. Os aportes deste trabalho foram:

No Capítulo 2

- Estabelecemos um novo produto de grupos, o *produto cíclico*, útil na decomposição dos grupos cíclicos da forma $\mathbb{Z}_{p^n}$, (Equação (2.6)).

- Propusemos uma técnica de construção de produtos de Schreier para grupos cíclicos (Proposição 2.2). Esta técnica permite operar uma boa parcela de grupos não abelianos finitos, em termos das operações de anéis $mod\, n$ já conhecidas.

- Propusemos uma técnica de construção multinível de produtos de Schreier (Teorema 2.3). Esta técnica foi utilizada na construção do código apresentado no Exemplo 5.3, que é o melhor até agora encontrado para o casamento entre o grupo $\mathbb{D}_4^2$ e a constelação $2 \times 8 - PSK$.

- Mostramos que cada grupo é decomponível em produtos de Schreier (Proposição 2.3). Segundo os tipos de produto de Schreier desta decomposição, estabelecemos uma classificação dos grupos. Uma outra conclusão é que esta decomposição, é uma generalização de três teoremas clássicos: *O teorema fundamental da aritmética, o teorema chinês do resto e o teorema fundamental dos grupos abelianos finitamente gerados.* Finalmente, provamos que quando um grupo possui *série de composição,* então o mesmo possui uma decomposição única (Teorema 2.5).

No Capítulo 3

- Na apresentação dos codificadores convolucionais elementares (CCE), foi introduzido um teste prático de minimalidade, portanto de não catastroficidade.(Teorema 3.1).

- Foram estabelecidos os códigos de Schreier como sendo aqueles produzidos pelos codificadores de Schreier (Definição 3.9).

- Estabelecemos um critério necessário, embora não sufuciente, para construir códigos de Schreier controláveis (Proposição 3.4). Entretanto, quando o número de estados é pequeno, este teste é suficiente para se determinar a controlabilidade do codificador, através de sua treliça.

No Capítulo 4

- Mostramos que os códigos de Schreier são lineares, independentemente de os grupos dos estados, informações, rótulos, ou o grupo seção de treliça serem abelianos ou não (Teorema 4.1).

- Usando a linearidade destes códigos, foi estabelecido um critério necessário e suficiente para a obtenção de códigos de Schreier controláveis (Teorema 4.2). Fica para uma pesquisa futura a otimização deste teste.

- Mostramos que os códigos de Schreier são completos (Teorema 4.3)

No Capítulo 5

Usando a teoria desenvolvida nos Capítulos 2, 3 e 4,

- Propusemos um algoritmo para obtenção de bons códigos binários não catastróficos.

- Mostramos que quando o grupo da treliça é cíclico, então o correspondente código de Schreier é não controlável (Proposição 5.1).

- Exibimos as limitações em distância dos códigos de Schreier quando o grupo dos estados é abeliano (Proposição 5.2). Esta é a nossa versão do Teorema 4 de [4].

- Propusemos um algoritmo para construir bons códigos de Schreier não abelianos usando o Teorema 2.3.

6.2 Propostas de Pesquisa Futura

- Na decomposição maximal única de um grupo G

$$G \cong \left[\left[\left[\ldots\left[Q_{n(\sigma_n,\mu_n)}Q_{n-1}\right]_{(\sigma_{n-1},\mu_{n-1})}\ldots\right]_{(\sigma_2,\mu_2)}Q_1\right]_{(\sigma_1,\mu_1)}Q_0\right],$$

apresentada no Teorema 2.5, será que cada grupo Q_i é cíclico?

- Mediante a implementação computacional da Proposição 2.2 podemos fazer uma procura exaustiva por bons códigos de Schreier que tenham como grupo seção de treliça T, tal que T é isomorfo a um produto de Schreier de dois grupos cíclicos. É plausível esperar que existam bons códigos de Schreier cujo grupo seção de treliça não é isomorfo a algum produto de Schreier de dois grupos cíclicos. Como usar o Teorema 2.5 na implementação de um algoritmo que permita uma busca destes códigos?. Em que medida ajudaria nesta implementação se cada Q_i do Teorema 2.5 for cíclico?.

- Os únicos códigos de Euclidianos casados com códigos de Schreier, sobre grupos não abelianos até então encontrados estão em [20] e [9]. Em [20] encontramos os códigos de Wei CCITT V.32 e V.64 usados em modems de 14.4 bps e que usam constelações QAM de 32 e 64 sinais respectivamente. O CCITT V.32, que possui 8 estados e uma distância livre $d_{free} = 8$, No Exemplo 5.1 é determinado que a seção de treliçdo CCITT V.32 está casada a um subgrupo de 32 elementos do grupo $\mathbb{D}_4^2$. Em [9] encontramos um código Euclidiano que utilisa a constelação $2 \times 8PSK$ e cuja seção de treliça está casada ao grupo não abeliano $\mathbb{D}_4$ atingindo uma distância livre $d_{free} = 1.61$. No Exemplo 5.3 é efetuado um casamento diferente entre os mesmos $2 \times 8PSK$ e $\mathbb{D}_4$ obtendo-se uma distância livre de $d_{free} = 8$. Será que existem outros grupos não abelianos nào relativos a $\mathbb{D}_4$ casados a constelações de sinais?.

Apêndice A

Demonstração do Teorema de Schreier

Substituindo elementos notáveis dos grupos H e K, tais como e_H, e_K, em (2.1) e (2.2), podemos fazer uma lista de propriedades elementares de $H_{(\sigma,\mu)}K$. Estas propriedades são úteis na demonstração de que $H_{(\sigma,\mu)}K$ é um grupo. Estas propriedades são explicitadas na Proposição A.1.

Proposição A.1 *Sejam e_K o elemento neutro de K e e_H o elemento neutro de H. Então,*

i) $\sigma(e_K)(\mu(e_K, e_K)) = \mu(e_K, e_K)$.

ii) $\sigma(e_K)(\mu(e_K, k)) = \mu(e_K, e_K)$; $\forall\, k \in K$.

iii) $\sigma(k)(\mu(e_K, e_K)) = \mu(k, e_K)$; $\forall\, k \in K$.

iv) $\sigma(k)[\mu(k^{-1}, k).\mu(k, e_K)] = \mu(k, k^{-1}).\mu(e_K, k)$; $\forall\, k \in K$.

v) $\sigma(e_K)(h) = \mu(e_K, e_K).h.(\mu(e_K, e_K))^{-1}$; $\forall\, h \in H$.

vi $\mu(e_K, e_K) = \mu(e_K, k)$; $\forall\, k \in K$.

vii) $\sigma(e_K)^{-1}(h) = (\mu(e_K, e_K))^{-1}.h.\mu(e_K, e_K);\ \forall h \in H.$

viii) *Se* $\mu(e_K, e_K) = e_H$, *então* $\mu(e_K, e_K) = \mu(e_K, k) = \mu(k, e_K);\ \forall k \in K$

ix) $\sigma(k)(h) = \mu(k, k^{-1}).\sigma(e_K)\left((\sigma(k^{-1}))^{-1}(h)\right).(\mu(k, k^{-1}))^{-1};\ \forall\, h \in H,\ \forall k \in K.$

x) *Se* H *é abeliano, então* $\sigma : K \to Aut(H)$ *é um homomorfismo.*

xi) *Se* $\sigma : K \to Aut(H)$ *é um homomorfismo, então* $h.\mu(k_1, k_2) = \mu(k_1 k_2).h;\ \forall\, k_1, k_2 \in K$ *e* $\forall\, h \in H;$

Prova : i) Substitua (k_1, k_2, k_3) de (2.1) por (e_K, e_K, e_K).

ii) Substitua (k_1, k_2, k_3) de (2.1) por (e_K, e_K, k).

iii) Substitua (k_1, k_2, k_3) de (2.1) por (k, e_K, e_K).

iv) Substitua (k_1, k_2, k_3) de (2.1) por (k, k^{-1}, k).

v) Fazendo $k_1 = k_2 = e_K$ e $h = h'$, na equação (2.2), temos

$$\sigma(e_K)(\sigma(e_K)(h')) = \mu(e_K, e_K).\sigma(e_K)(h').(\mu(e_K, e_K))^{-1}\ ;\forall h' \in H.$$

Como $\sigma(e_K) \in Aut(H)$, então $\sigma(e_K)$ é um-a-um. Daí, $\forall\, h \in H$, existe um único $h' \in H$ tal que $h = \sigma(e_K)(h')$.

Portanto,

$$\sigma(e_K)(h) = \mu(e_K, e_K).h.(\mu(e_K, e_K))^{-1};\ \forall h \in H.$$

vi) De **i)** e **ii)**, temos que $\sigma(e_K)(\mu(e_K, e_K)) = \sigma(e_K)(\mu(e_K, k))$. Logo, como $\sigma(e_K)$ é um-a-um então

$$\mu(e_K, e_K) = \mu(e_K, k).$$

vii) De **i)** temos que $\sigma(e_K)(\mu(e_K, e_K)) = \mu(e_K, e_K)$. Assim, $\sigma(e_K)^{-1}(\mu(e_K, e_K)) = \mu(e_K, e_K)$. Agora, de **v)** temos que

$$h = (\sigma(e_K))^{-1}[\mu(e_K, e_K).h.(\mu(e_K, e_K))^{-1}]$$

$$h = \mu(e_K, e_K).\sigma(e_K)^{-1}(h).(\mu(e_K, e_K))^{-1}$$

$$\sigma(e_K)^{-1}(h) = (\mu(e_K, e_K))^{-1}.h.\mu(e_K, e_K).$$

viii) De **iii)** temos que $\mu(k, e_K) = \sigma(k)(\mu(e_K, e_K))$. Por hipótese, $\sigma(k)(\mu(e_K, e_K)) = \sigma(k)(e_H) = e_H$.

ix) Substituindo $k_1 = k$, $k_2 = k^{-1}$ e $h = h'$ na equação (2.2), obtemos

$$\sigma(k)(\sigma(k^{-1})(h')) = \mu(k, k^{-1}).\sigma(e_K)(h').(\mu(k, k^{-1}))^{-1}.$$

Fazendo $h = \sigma(k^{-1})(h')$, obtemos $h' = (\sigma(k^{-1}))^{-1}(h)$ e cosequentemente que

$$\sigma(k)(h) = \mu(k, k^{-1})\sigma(e_K)(\sigma(k^{-1}))^{-1}(h).(\mu(k, k^{-1}))^{-1}.$$

x) Como H é abeliano, a equação (2.2), fica sendo

$$\sigma(k_1)\sigma(k_2)(h) = \sigma(k_1k_2)(h);\ \forall k_1, k_2 \in K;\ \forall h \in H$$

Portanto, $\sigma(k_1)\sigma(k_2) = \sigma(k_1k_2)\,;\ \forall\, k_1, k_2 \in K$.

xi) Como $\sigma(k_1)\sigma(k_2) = \sigma(k_1k_2)$, a equação (2.2), fica sendo

$$\sigma(k_1k_2)(h) = \mu(k_1, k_2).\sigma(k_1k_2)(h).(\mu(k_1, k_2))^{-1}$$
$$\sigma(k_1k_2)(h).\mu(k_1, k_2) = \mu(k_1, k_2).\sigma(k_1k_2)(h)$$
$$h'.\mu(k_1, k_2) = \mu(k_1, k_2).h',$$

para todo $\sigma(k_1k_2)(h) = h' \in H$.

Teorema A.1 *O produto $H_{(\sigma,\mu)}K$ é um grupo.*

Prova: Fica claro que

$$(h, k)(h', k') = (h.\sigma(k)(h').\mu(k, k')\,,\ kk') \in H_{\sigma,\mu}K\ ;\forall(h, k)\,,\ (h', k') \in H_{\sigma,\mu}K.$$

Associatividade

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

Usando a condição (2.1), na última igualdade, resulta em

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

Usando a condição (2.2) nesta última igualdade, temos

$$= (h.\sigma(k)(h').\mu(k,k').\sigma(kk')(h'').(\mu(k,k'))^{-1}.\mu(k,k').\mu(kk',k'')\ ,\ kk'k'')$$
$$= (h.\sigma(k)(h').\mu(k,k').\sigma(kk')(h'').\mu(kk',k'')\ ,\ kk'k'')$$
$$= (h.\sigma(k)(h').\mu(k,k')\,,\ kk')\,(h'',k'')$$
$$= (h,k)(h',k')](h'',k'').$$

O elemento neutro é $((\mu(e_K,e_K))^{-1}\ ,\ e_K)$

Verificação pela esquerda

Suponha que (h',k') é elemento neutro pela esquerda. Então, $\forall (h,k) \in H_{\sigma,\mu}K$, temos que

$$(h',k')(h,k) = (h,k).$$

Logo, $k' = e_K$. Além disso,

$$h'.\sigma(e_K)(h).\mu(e_K,k) = h$$
$$h'.\sigma(e_K)(h) = h.(\mu(e_K,e_K))^{-1}$$
$$\mu(e_K,e_K).h'.\sigma(e_K)(h) = \mu(e_K,e_K).h.(\mu(e_K,e_K))^{-1}.$$

Usando o ítem **v)** da Proposição A.1, pelo lado direito, temos que

$$\mu(e_K,e_K).h'.\sigma(e_K)(h) = \sigma(e_K)(h)$$
$$\mu(e_K,e_K).h' = e_H$$
$$h' = (\mu(e_K,e_K))^{-1}.$$

Verificação pela direita

Suponha que (h', k') é o elemento neutro pela direita. Então, $\forall (h,k) \in H_{\sigma,\mu}K$, temos que

$$(h,k)(h',kl) = (h,k).$$

Logo, $k' = e_K$ e $h.\sigma(k)(h').\mu(k, e_K) = h$. Do ítem **iii)** da Proposição A.1, temos que

$$\begin{aligned}
&\sigma(k)(h').\sigma(k)\left(\mu(e_K, e_K)\right) = e_H \\
&\sigma(k)[h'.\mu(e_K, e_K)] = e_H \\
&h'.\mu(e_K, e_K) = e_H \\
&h' = (\mu(e_K, e_K))^{-1}.
\end{aligned}$$

$\forall (h,k) \in H_{\sigma,\mu}K$, o inverso de (h,k) é $(h,k)^{-1} = ([\sigma(k^{-1})(h).\mu(k^{-1},k).\mu(e_K,e_K)]^{-1}\ , k^{-1})$

Verificação pela esquerda

Dado $(h,k) \in H_{\sigma,\mu}K$, suponha (h',k') é o inverso pela esquerda. Então,

$$(h',k')(h,k) = \left((\mu(e_K,e_K))^{-1}; e_K\right).$$

Logo, $k' = k^{-1}$ donde

$$\begin{aligned}
&h'.\sigma(k^{-1})(h).\mu(k^{-1},k) = (\mu(e_K,e_K))^{-1} \\
&h' = (\mu(e_K,e_K))^{-1}.\mu(k^{-1},k)^{-1}.\sigma(k^{-1})(h^{-1}) \\
&h' = [\sigma(k^{-1})(h).\mu(k^{-1},k).\mu(e_K,e_K)]^{-1}.
\end{aligned}$$

Verificação pela direita

Dado $(h,k) \in H_{\sigma,\mu}K$, suponha que (h',k') é o inverso pela direita de (h,k). Então,

$$(h,k)(h',k') = \left((\mu(e_K,e_K))^{-1}\ , e_K\right).$$

Logo, $k' = k^{-1}$. Além disso,

$$h.\sigma(k)(h').\mu(k,k^{-1}) = (\mu(e_K,e_K))^{-1}. \tag{A.1}$$

Usando o ítem **v)** da Proposição A.1 no fator $\sigma(k)(h')$ do lado esquerdo da equação A.1, temos que

$$h.\mu(k,k^{-1}).\sigma(e_K)(\sigma(k^{-1}))^{-1}(h').(\mu(k,k^{-1}))^{-1}.\mu(k,k^{-1}) = (\mu(e_K,e_K))^{-1}$$
$$\sigma(e_K)(\sigma(k^{-1}))^{-1}(h') = (\mu(k,k^{-1}))^{-1}.h^{-1}.(\mu(e_K,e_K))^{-1}$$
$$(\sigma(k^{-1}))^{-1}(h') = \sigma(e_K)^{-1}[(\mu(k,k^{-1}))^{-1}.h^{-1}.(\mu(e_K,e_K))^{-1}].$$

Agora, usando o ítem **vii)** da Proposição A.1, temos que

$$(\sigma(k^{-1}))^{-1}(h') = (\mu(e_K,e_K))^{-1}.[(\mu(k,k^{-1}))^{-1}.h^{-1}.(\mu(e_K,e_K))^{-1}].\mu(e_K,e_K)$$
$$(\sigma(k^{-1}))^{-1}(h') = (\mu(e_K,e_K))^{-1}.(\mu(k,k^{-1}))^{-1}.h^{-1}$$
$$h' = \sigma(k^{-1})[(\mu(e_K,e_K))^{-1}.(\mu(k,k^{-1}))^{-1}].\sigma(k^{-1})(h^{-1})$$
$$h' = [\sigma(k^{-1})[\mu(k,k^{-1}).\mu(e_K,e_K)]]^{-1}.\sigma(k^{-1})(h^{-1}).$$

Finalmente, usando o ítem **iv)** da Proposição A.1, obtemos

$$h' = [\mu(k^{-1},k).\mu(e_K,e_K)]^{-1}.\sigma(k^{-1})(h^{-1})$$
$$h' = [\sigma(k^{-1})(h).\mu(k^{-1},k).\mu(e_K,e_K)]^{-1}.$$

■

Apêndice B

Outras Demonstrações

B.1 Prova da Proposição 2.2

Construção de σ .

Sejam η e γ geradores de $\mathbb{Z}_m$ e $\mathbb{Z}_n$, respectivamente. Seja $\sigma : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_n$ definido por

$$\sigma(\eta^i, \gamma^j) = \sigma(\eta^i)(\gamma^j) = \gamma^{j.x^i} \; ; \quad 0 \leq i \leq m \; ; \; 0 \leq j \leq n.$$

Note que $\sigma(\eta^i)$ é um homomorfismo, pois

$$\sigma(\eta^i)(\gamma^r.\gamma^s) = \sigma(\eta^i)(\gamma^{r+s}) = \gamma^{(r+s)x^i} = \gamma^{rx^i}.\gamma^{sx^i} = \sigma(\eta^i)(\gamma^r).\sigma(\eta^i)(\gamma^s).$$

Por outro lado, uma vez que $x^m = 1(mod\, n)$ temos que γ^{x^i} é também um gerador de $\mathbb{Z}_n$, para todo $i = 0, \ldots, m-1$. Agora, a aplicação $\sigma(\eta^i)$ mapeia γ em γ^{x^i}. Desse modo, $\sigma(\eta^i)$ é bijetora. Portanto, $\sigma(\eta^i) \in Aut(\mathbb{Z}_n)$ e $\sigma : \mathbb{Z}_m \to Aut(\mathbb{Z}_n)$.

Finalmente, para todo $i, j = 0, 1, \ldots, m-1$ e para $r = 0, 1, \ldots, n-1$, temos que

$$\sigma(\eta^i.\eta^j)(\gamma^r) = \sigma(\eta^{i+j})(\gamma^r) = \gamma^{r.x^{j+i}} = \gamma^{(r.x^j).x^i} = \sigma(\eta^i)(\gamma^{r.x^j}) = \sigma(\eta^i)\sigma(\eta^j)(\gamma^r).$$

Portanto, $\sigma : \mathbb{Z}_m \to Aut(\mathbb{Z}_n)$ é um homomorfismo.

Definição de μ

Como $xy = y(mod\, n)$, então o elemento $\gamma^y \in \mathbb{Z}_n$ é um ponto fixo de $\sigma(\eta^i)$, para qualquer i,

pois

$$\sigma(\eta)(\gamma^y) = \gamma^{yx} = \gamma^y.$$

Seja $e_n = \gamma^n$ o elemento neutro de $\mathbb{Z}_n$. Definimos $\mu : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_n$ como sendo

$$\mu(\eta^i, \eta^j) = \begin{cases} e_n, & \text{if } i+j < m \\ \gamma^y, & \text{if } i+j \geq m. \end{cases} \tag{B.1}$$

Ambas as aplicações σ e μ satisfazem as condições (1) e (2)

A condição (2) é trivialmente satisfeita. Então, resta somente verificar a condição (1). Para as ternas (η^i, η^j, η^r), temos que considerar os seguintes casos: a) $i+j+r < m$, e b) $i+j+r \geq m$.

Caso a

Se $i+j+r < m$, então $i+j < m$, e $j+s < m$. Assim,

$$\mu(\eta^j, \eta^r) = \mu(\eta^i, \eta^{j+r}) = \mu(\eta^i, \eta^j) = \mu(\eta^{i+j}, \eta^r) = e_n.$$

Portanto,

$$\sigma(\eta^i)(\mu(\eta^j, \eta^r)).\mu(\eta^i, \eta^{j+r}) = \mu(\eta^i, \eta^j).\mu(\eta^{i+j}, \eta^r).$$

Caso b

Se $i+j+r \geq m$, então existem quatro possibilidades a serem consideradas. Elas são as seguintes:

b.1) $i+j \geq m$, e $j+r \geq m$;

b.2) $i+j < m$, e $j+r \geq m$;

b.3) $i+j \geq m$, e $j+r < m$;

b.4) $i+j < m$, e $j+r < m$.

Se b.1), então $\eta^{i+j} = \eta^s$, para algum $s < m$, e $\eta^{j+r} = \eta^t$, para algum $t < m$. Logo,

$$\mu(\eta^j, \eta^r) = e_n \ ; \ \mu(\eta^i, \eta^{j+r}) = e_n \ ; \ \mu(\eta^i, \eta^j) = e_n \ ; \ \mu(\eta^{i+j}, \eta^r) = e_n.$$

Portanto,

$$\sigma(\eta^i)(\mu(\eta^j, \eta^r)).\mu(\eta^i, \eta^{j+r}) = \mu(\eta^i, \eta^j).\mu(\eta^{i+j}, \eta^r).$$

Se b.2), então $\eta^{j+r} = \eta^t$, para algum $t < m$. Assim,

$$\mu(\eta^j, \eta^r) = \gamma^y \; ; \;\; \mu(\eta^i, \eta^{j+r}) = e_n \; ; \; \mu(\eta^i, \eta^j) = e_n \; ; \; \mu(\eta^{i+j}, \eta^r) = \gamma^y.$$

Portanto,

$$\sigma(\eta^i)(\mu(\eta^j, \eta^r)).\mu(\eta^i, \eta^{j+r}) = \mu(\eta^i, \eta^j).\mu(\eta^{i+j}, \eta^r).$$

Se b.3), então $\eta^{i+j} = \eta^t$, para algum $t < m$. Dessa forma,

$$\mu(\eta^j, \eta^r) = e_n \; ; \;\; \mu(\eta^i, \eta^{j+r}) = \gamma^y \; ; \; \mu(\eta^i, \eta^j) = \gamma^y \; ; \; \mu(\eta^{i+j}, \eta^r) = e_n.$$

Portanto,

$$\sigma(\eta^i)(\mu(\eta^j, \eta^r)).\mu(\eta^i, \eta^{j+r}) = \mu(\eta^i, \eta^j).\mu(\eta^{i+j}, \eta^r)$$

Se b.4), então temos que

$$\mu(\eta^j, \eta^r) = \gamma^y \; ; \;\; \mu(\eta^i, \eta^{j+r}) = \gamma^y \; ; \; \mu(\eta^i, \eta^j) = \gamma^y \; ; \; \mu(\eta^{i+j}, \eta^r) = \gamma^y.$$

Portanto,

$$\sigma(\eta^i)(\mu(\eta^j, \eta^r)).\mu(\eta^i, \eta^{j+r}) = \mu(\eta^i, \eta^j).\mu(\eta^{i+j}, \eta^r).$$

■

B.2 Prova do Teorema 2.4

Seja $\frac{G}{N}$ o grupo quociente relativo a N, cujos elementos denotaremos por u, v, w, etc. Seja $R \subset G$, um conjunto de **representantes** de $\frac{G}{N}$. Estes representantes são escolhidos com a única condição de que o representante da classe $N \in \frac{G}{N}$ deve ser o elemento neutro e_G do grupo G. Se $u \in \frac{G}{N}$, então o representante de u é denotado por $\bar{u} \in \mathbb{R}$. Também, se v , w pertencem a $\frac{G}{N}$, os representantes serão $\bar{v}$ para v e $\bar{w}$ para w e assim por diante.

Definição de μ_R

Dados os representantes $\bar{u}$ e $\bar{v}$ temos que $\bar{u} \in u$ e $\bar{v} \in v$. Temos também que $\bar{u}\bar{v} \in uv$, mas $\bar{u}\bar{v}$ não necessariamente é o representante $\overline{uv}$ de uv. Assim, é melhor dizer que existe $n \in N$ tal que $\bar{u}\bar{v} = n.\overline{uv}$. Isto é ilustrado na Fig. B.1.

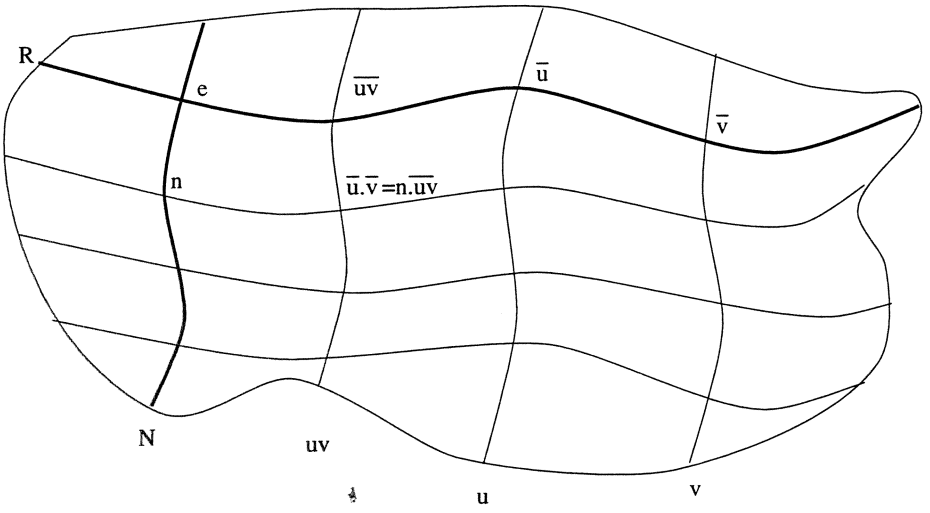

Figura B.1: Sistema de coordenadas $N \times R$ para o grupo G

Este $n \in N$ depende de $u \in \frac{G}{N}$, de $v \in \frac{G}{N}$ e da escolha de R. Logo, podemos escrever n como sendo $n = \mu_R(u, v)$. Portanto, $\mu_R : \frac{G}{N} \times \frac{G}{N} \to N$ fica definido por

$$\bar{u}\bar{v} = \mu_R(u, v).\overline{uv}, \tag{B.2}$$

ou, equivalentemente, por

$$\mu_R(u, v) = \bar{u}.\bar{v}.(\overline{uv})^{-1}. \tag{B.3}$$

Definição de σ_R

Como N é normal, então $\bar{u}.n.\bar{u}^{-1} \in N$. Portanto, $\sigma_R : \frac{G}{N} \to Aut(N)$ fica definido por

$$\sigma_R(u)(n) = \bar{u}.n.\bar{u}^{-1}. \tag{B.4}$$

Esquematicamente, temos

$$\begin{array}{rcl} \sigma_R : \frac{G}{N} & \to & Aut(N) \\ u & \mapsto & \sigma_R(u) : \quad N \to N \\ & & \qquad\quad n \mapsto \sigma_R(u)(n) = \bar{u}.n.\bar{u}^{-1}. \end{array}$$

O produto de Schreier $N_{(\sigma_R,\mu_R)}\frac{G}{N}$

Dados $u\,,v\,,w \in \frac{G}{N}$ temos

$$\begin{aligned}
\sigma_R(u)(\mu_R(v,w)).\mu_R(u,vw) &= \sigma_R(u)(\mu_R(v,w)).\bar{u}.\overline{vw}.(\overline{uvw})^{-1} \\
&= \sigma_R(u)(\mu_R(v,w)).\bar{u}.\overline{vw}.(\overline{uv}.\bar{w})^{-1}.\overline{uv}.\bar{w}.(\overline{uvw})^{-1} \\
&= \sigma_R(u)(\mu_R(v,w)).\bar{u}.\overline{vw}.(\overline{uv}.\bar{w})^{-1}.\mu_R(uv,w) \\
&= \bar{u}.\mu_R(v,w).\bar{u}^{-1}.\bar{u}.\overline{vw}.(\overline{uv}.\bar{w})^{-1}.\mu_R(uv,w) \\
&= \bar{u}.\bar{v}.\bar{w}.(\overline{vw})^{-1}.\overline{vw}.\bar{w}^{-1}.(\overline{uv})^{-1}.\mu_R(uv,w) \\
&= \bar{u}.\bar{v}.(\overline{uv})^{-1}.\mu_R(uv,w) \\
&= \mu_R(u,v).\mu_R(uv,w).
\end{aligned}$$

Por outro lado, dados $u\,,v\,,w \in \frac{G}{N}$ e $n \in N$ temos que

$$\begin{aligned}
\sigma_R(u)(\sigma_R(v)(n)) &= \sigma_R(u)(\bar{v}.n.\bar{v}^{-1}) = \bar{u}.\bar{v}.n.\bar{v}^{-1}.\bar{u}^{-1} \\
&= \bar{u}.\bar{v}.(\overline{uv})^{-1}.\overline{uv}.n.(\overline{uv})^{-1}.\overline{uv}.\bar{v}^{-1}.\bar{u}^{-1} \\
&= \mu_R(u,v).\sigma_R(uv)(n).(\bar{u}.\bar{v}.(\overline{uv})^{-1})^{-1} \\
&= \mu_R(u,v).\sigma_R(uv)(n).\mu_R(u,v)^{-1}
\end{aligned}$$

Desta maneira, σ_R e μ_R satisfazem as condições (2.1) e (2.2). Então, podemos definir o produto de Schreier $N_{(\sigma_R,\mu_R)}\frac{G}{N}$ com a operação

$$(n,u) * (n',v) = (n.\sigma_R(u)(n').\mu_R(u,v)\ ,\ uv)\,.$$

Seja $e_{G/N} \in \frac{G}{N}$ o elemento neutro deste grupo quociente. Seja $e_G \in G$ o elemento neutro de G e N. Então, o produto de Schreier $N_{(\sigma_R,\mu_R)}\frac{G}{N}$ é um grupo com elemento neutro $(e_G, e_{G/N})$ e inverso $(n,u)^{-1} = ((\sigma_R(u^{-1})(n).\mu_R(u^{-1},u))^{-1}\ ,\ u^{-1})$.

G é isomorfo ao produto de Schreier $N_{(\sigma_R,\mu_R)}\frac{G}{N}$

Dados $g,\ g' \in G$, necessariamente $g \in u$ e $g' \in v$, para algum par $u \in \frac{G}{N}$ e $v \in \frac{G}{N}$. Então, podemos escrever $g = n.\bar{u}$ e $g' = n'.\bar{v}$ onde $\bar{u} \in R$ e $\bar{v} \in R$ são os representantes de u e de v respectivamente e $n,\ n' \in N$. Logo,

$$gg' = (n.\bar{u}).(n'.\bar{v}) = n.\bar{u}.n'.\bar{u}^{-1}.\bar{u}.\bar{v} = n.\sigma_R(u)(n').\bar{u}.\bar{v} = n.\sigma_R(u)(n').\mu_R(u,v).\overline{uv}.$$

Desta maneira, podemos descrever G como sendo um grupo de pares ordenados $(n, \bar{u}) \in N \times R$, cuja operação é dada por

$$(n, \bar{u}) * (n', \bar{v}) = (n.\sigma_R(u)(n').\mu_R(u, v) \ , \ \overline{uv}) .$$

De maneira equivalente, podemos dizer que $G \cong N \times R$.

Finalmente, a aplicação $\varphi : N \times R \to N_{(\sigma_R,\mu_R)}\frac{G}{N}$ dada por $\varphi(n, \bar{u}) = (n, u)$ é um homomorfismo bijetivo de grupos pois:

$$\begin{aligned}
&\varphi\left((n, \bar{u})(n', \bar{v})\right) = \varphi\left(n.\sigma_R(u)(n').\mu_R(u, v) \ , \ \overline{uv}\right) \\
&= (n.\sigma_R(u)(n').\mu_R(u, v) \ , \ uv) \\
&= (n, u) * (n', v) = \varphi(n, \bar{u}).\varphi(n', \bar{v}).
\end{aligned}$$

Portanto,

$$G \cong N_{(\sigma_R,\mu_R)}\frac{G}{N}.$$

■

Na prova do Teorema 2.4, denotamos σ e μ por σ_R e μ_R respectivamente, com o propósito de ressaltar a dependência de σ_R e de μ_R, com respeito a escolha do conjunto R.

B.3 Prova do Teorema 4.1

Associatividade

Dados $\binom{(i)}{x}, q)$, $\binom{(i)}{y}, r)$, $\binom{(i)}{z}, s)$ $\in X^i{}_{[\sigma,\mu]}Q$ temos que

$$\left[\binom{(i)}{x}, q) . \binom{(i)}{y}, r)\right] . \binom{(i)}{z}, s) = \binom{(i)}{w}, qr) . \binom{(i)}{z}, s) ,$$

onde

$$\begin{aligned}
w_1 &= x_1.\sigma(q)(y_1).\mu(q, r) \\
w_j &= x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(y_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q) \, , \, \delta_{j-1}(\overset{(j-1)}{y}, r)\right) \quad ; \ i \geq j \geq 2.
\end{aligned}$$

Agora, $\left(\overset{(i)}{w}, qr\right).\left(\overset{(i)}{z}, s\right)=\left(\overset{(i)}{t}, qrs\right)$ onde

$$
\begin{aligned}
t_1 &= w_1.\sigma(qr)(z_1).\mu(qr,s)\\
t_j &= w_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{w}, qr)\right)(z_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{w}, qr),\, \delta_{j-1}(\overset{(j-1)}{z}, s)\right) \quad ; \quad i \geq j \geq 2.
\end{aligned}
$$

Por outro lado,

$$
\left(\overset{(i)}{x}, q\right).\left[\left(\overset{(i)}{y}, r\right).\left(\overset{(i)}{z}, s\right)\right] = \left(\overset{(i)}{x}, q\right).\left(\overset{(i)}{\zeta}, rs\right),
$$

onde

$$
\begin{aligned}
\zeta_1 &= y_1.\sigma(r)(z_1).\mu(r,s)\\
\zeta_j &= y_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{y}, r)\right)(z_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{y}, r),\, \delta_{j-1}(\overset{(j-1)}{z}, s)\right) \quad ; \quad i \geq j \geq 2.
\end{aligned}
\tag{B.5}
$$

Agora, $\left(\overset{(i)}{x}, q\right).\left(\overset{(i)}{\zeta}, rs\right)=\left(\overset{(i)}{\rho}, qrs\right)$ onde

$$
\begin{aligned}
\rho_1 &= x_1.\sigma(q)(\zeta_1).\mu(q,rs)\\
\rho_j &= x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(\zeta_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q),\, \delta_{j-1}(\overset{(j-1)}{\zeta}, rs)\right) \quad ; \quad i \geq j \geq 2.
\end{aligned}
\tag{B.6}
$$

Como a propriedade associativa vale para o produto de Schreier ordinário, temos que $\rho_1 = t_1$. Agora, para $j \geq 2$, a substituição ζ_j de (B.5), em (B.6) conduz a

$$
\begin{aligned}
\rho_j = x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)\left[y_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{y}, r)\right)(z_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{y}, r),\, \delta_{j-1}(\overset{(j-1)}{z}, s)\right)\right].\\
\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q),\, \delta_{j-1}(\overset{(j-1)}{\zeta}, rs)\right).
\end{aligned}
$$

Fazendo uso da linearidade de $\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)$, que está em $Aut(X)$, obtemos os seguintes cinco fatores de ρ_j

$$
\begin{aligned}
\rho_j = \overbrace{x_j}^{a}.\overbrace{\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(y_j)}^{b}.\overbrace{\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)\left(\sigma\left(\delta_{j-1}(\overset{(j-1)}{y}, r)\right)(z_j)\right)}^{c}.\\
\overbrace{\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)\left(\mu\left(\delta_{j-1}(\overset{(j-1)}{y}, r), \delta_{j-1}(\overset{(j-1)}{z}, s)\right)\right)}^{d}.\\
\overbrace{\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q), \delta_{j-1}(\overset{(j-1)}{\zeta}, rs)\right)}^{e}.
\end{aligned}
\tag{B.7}
$$

Pela linearidade de δ_{j-1}, temos que $\delta_{j-1}\left(\overset{(j-1)}{\zeta}, rs\right) = \delta_{j-1}\left(\overset{(j-1)}{y}, r\right).\delta_{j-1}\left(\overset{(j-1)}{z}, s\right)$ e $\delta_{j-1}\left(\overset{(j-1)}{w}, qr\right) = \delta_{j-1}\left(\overset{(j-1)}{x}, q\right).\delta_{j-1}\left(\overset{(j-1)}{y}, r\right)$.

Fazendo uso de (2.2), o fator **c** de ρ_j em (B.7) fica sendo

$$\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)\left(\sigma\left(\delta_{j-1}(\overset{(j-1)}{y}, r)\right)(z_j)\right) = \mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\ ,\ \delta_{j-1}(\overset{(j-1)}{y}, r)\right)$$
$$\sigma\left(\delta_{j-1}(\overset{(j-1)}{\zeta}, rs)\right)(z_j).\left[\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\ ,\ \delta_{j-1}(\overset{(j-1)}{y}, r)\right)\right]^{-1}.$$

Por outro lado, através de (2.1), o fator **d.e** de ρ_j em (B.7) fica sendo

$$\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)\left(\mu\left((\delta_{j-1}(\overset{(j-1)}{y}, r), (\delta_{j-1}(\overset{(j-1)}{z}, s)\right)\right).\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q), \delta_{j-1}(\overset{(j-1)}{\zeta}, rs)\right)$$
$$= \mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\ ,\ \delta_{j-1}(\overset{(j-1)}{y}, r)\right).\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q).\delta_{j-1}(\overset{(j-1)}{y}, r)\ ,\ \delta_{j-1}(\overset{(i)}{z}, s)\right)$$
$$= \mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\ ,\ \delta_{j-1}(\overset{(j-1)}{y}, r)\right).\mu\left(\delta_{j-1}(\overset{(j-1)}{w}, qr)\ ,\ \delta_{j-1}(\overset{(i)}{z}, s)\right).$$

Assim,

$$\rho_j = x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(y_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\ ,\ \delta_{j-1}(\overset{(j-1)}{y}, r)\right).$$
$$\sigma\left(\delta_{j-1}(\overset{(j-1)}{w}, qr)\right)(z_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{w}, qr)\ ,\ \delta_{j-1}(\overset{(j-1)}{z}, s)\right)\ ;\ i \geq j \geq 2.$$

Portanto,

$$\rho_j = w_j.\sigma(\delta_{j-1}(\overset{(j-1)}{w}, qr))(z_j).\mu\left((\delta_{j-1}(\overset{(j-1)}{w}, qr), (\delta_{j-1}(\overset{(j-1)}{z}, s)\right) = t_j\ ;\ i \geq j \geq 2$$

Elemento neutro

Considere a seqüência $\{y_j\}_{j=1}^{i}$ definida por 4.9.

Afirmamos que $\left(\overset{(i)}{y}, e_Q\right)$ é o elemento neutro de $X^i{}_{[\sigma,\mu]}Q$. Com efeito, se $\left(\overset{(i)}{x}, q\right).\left(\overset{(i)}{y}, e_Q\right) = \left(\overset{(i)}{z}, q\right)$, então

$$z_1 = x_1.\sigma(q)(y_1).\mu(q, e_Q)$$
$$z_j = x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(y_j).\overbrace{\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\ ,\ \delta_{j-1}(\overset{(j-1)}{y}, e_Q)\right)}^{f}\ ;\ i \geq j \geq 2. \tag{B.8}$$

Usando o produto de Schreier ordinário, temos que $z_1 = x_1$. Para $j \geq 2$ fazendo uso do Lema 4.2 no fator $\mathbf{f}$ de z_j em (B.8), temos

$$\begin{aligned} z_j &= x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(y_j).\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)\left(\mu\left(\delta_{j-1}(\overset{(j-1)}{y}, e_Q), \delta_{j-1}(\overset{(j-1)}{y}, e_Q)\right)\right) \\ &= x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)\left(y_j.\mu\left(\delta_{j-1}(\overset{(j-1)}{y}, e_Q), \delta_{j-1}(\overset{(j-1)}{y}, e_Q)\right)\right) \\ &= x_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q)\right)(e_X) \\ &= x_j. \end{aligned}$$

O elemento inverso

Dado $\left(\overset{(i)}{x}, q\right) \in X^i{}_{[\sigma,\mu]}Q$, considere o elemento $\left(\overset{(i)}{z}, q^{-1}\right) \in X^i{}_{[\sigma,\mu]}Q$ definido por

$$\begin{aligned} &z_1 = (\mu(e_Q, e_Q))^{-1}.(\mu(q^{-1}, q))^{-1}.[(\sigma(q^{-1})(x_1))]^{-1} \\ &z_j = \left[\mu\left(\delta_{j-1}(\overset{(j-1)}{y}, e_Q), \delta_{j-1}(\overset{(j-1)}{y}, e_Q)\right)\right]^{-1}.\left[\mu\left(\delta_{j-1}(\overset{(j-1)}{x}, q^{-1}), \delta_{j-1}(\overset{(j-1)}{x}, q)\right)\right]^{-1}. \\ &\left[\sigma\left(\delta_{j-1}(\overset{(j-1)}{x}, q^{-1})\right)(x_j)\right]^{-1} \quad ; \quad i \geq j \geq 2. \end{aligned} \tag{B.9}$$

Se $\left(\overset{(i)}{z}, q^{-1}\right).\left(\overset{(i)}{x}, q\right) = \left(\overset{(i)}{w}, e_Q\right)$, onde

$$\begin{aligned} w_1 &= z_1.\sigma(q^{-1})(x_1).\mu(q^{-1}, q) \\ w^j &= z_j.\sigma\left(\delta_{j-1}(\overset{(j-1)}{z}, q^{-1})\right)(x_j).\mu\left(\delta_{j-1}(\overset{(j-1)}{z}, q^{-1}), \delta_{j-1}(\overset{(j-1)}{x}, q)\right) \; ; i \geq j \geq 2, \end{aligned}$$

substituindo z_j dado em (B.9) para $j = 1, \ldots, i$, obtemos $w_j = y_j$ ■

Apêndice C

Alguns Teoremas Fundamentais da Álgebra

Apresentamos neste apêndice algumas definições e teoremas fundamentais da álgebra que são usados neste trabalho.

1.- Teorema Fundamental dos Homomorfismos

Teorema C.1 *Sejam G e G' dois grupos. Seja $\phi : G \to G'$ um homomorfismo de grupos com imagem $Im(\phi) = \{g' \in G' : g' = \phi(g)$, para algum $g \in G\}$ e com núcleo $Ker(\phi) = \{g \in G : \phi(g) = e_{G'}\}$. Então: $Ker(\phi)$ é um subgrupo normal de G e além disso $\frac{G}{Ker(\phi)} \cong Im(\phi)$.*

Quando ϕ for sobrejetora teremos que $Im(\phi) = G'$ então $\frac{G}{Ker(\phi)} \cong G'$.

2.- Teorema de Jordan-Hölder

Definição C.1 *Sejam G um grupo e $S_1 : G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e_G\}$ e $S_2 : G = G'_0 \rhd G'_1 \rhd \ldots \rhd G'_m = \{e_G\}$ duas séries normais finitas de G. Então, dizemos que as séries normais S_1 e S_2 são* **equivalentes** *se $n = m$ e $\frac{G_i}{G_{i+1}} \cong \frac{G'_i}{G'_{i+1}}$, para todo $i = 1, \ldots, n$.*

Teorema C.2 Jordan-Hölder *Qualquer par de séries de composição S_1 e S_2, de um grupo G, são equivalentes.*

Bibliografia

[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 Technology, Zurich, 1992.

[3] G.D.Forney, "Geometrically uniform codes" *IEEE Trans. Inform. Theory*, vol. IT-37 No 5, pp. 1241-1260, 1991.

[4] G.D.Forney, "On the Hamming distance properties of group codes" *IEEE Trans. Inform. Theory*, vol. IT-38 pp. 1797-1801, Nov. 1992.

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

[6] J.C.Willems, "Models for dynamics" em *Dynamics Technical Report* vol. 2, U.Kirchgraber e H.O.Walther, Eds. Wiley and Teubner, 1989.

[7] M.A. Arbib, "Automaton Decomposition e Semigroup Structure" em *Algebraic Structure de Machine Languages*, M.A. Arbib editor, 1968.

[8] M.Hall, *The Theory of the Groups*; Macmillan, New York, 1961.

[9] R. Garello, and S.Benedetto, "Multilevel construction of block and trellis group codes", *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 1257-1264, Sept. 1995.

[10] G. Ungerboeck, "Channel coding with multilevel/phase signals", *IEEE Trans. Inform. Theory*, vol 28, pp 55-67, Jan. 1982.

[11] J.J. Rotman, *An Introduction to the Theory of Groups*; Springer-Verlag, Fourth ed.; 1995.

[12] A. Garcia, Y. Lequain; *Álgebra : Um Curso de Introdução* ; Projeto Euclides, Num. 18, IMPA, Rio de Janeiro, 1988.

[13] S. Benedetto, E. Biglieri, V. Castellani; *Digital Transmission Theory*; Prentice-Hall International ed., 1987.

[14] A.R. Calderbank, and N.J.A. Sloane, "New trellis codes based on lattices and cosets", *IEEE Trans. Inform. Theory*, vol. 33, pp. 177-195, Jan. 1987.

[15] D. Slepian, "Group codes for the Gaussian channels", *Bell Syst. Tech. Journal*, vol. 47, pp. 575-602, April 1968.

[16] H.A. Loeliger, G.D. Forney, T. Mittelholzer, and M.D. Trott, "Minimality and observability of group systems", *Linear Algebra and its Applications*, vol 205-206, pp 937-963, July 1994.

[17] M.A. Arbib; *Brains, Machines, and Mathematics*; Springer-Verlag, Second ed.; 1986.

[18] 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.

[19] H.A. Loeliger, "Signal sets matched to groups", *IEEE Trans. Inform. Theory*, vol IT-37, no 6, pp 1675-1682, 1991.

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