Um algoritmo de treliça para decodificação de códigos de grupo comutativo

Agnaldo J. Ferrari, Cristiano Torezzan, Grasiele C. Jorge e Sueli I. R. Costa.

***Resumo*— Códigos esféricos 2k-dimensionais gerados por grupos comutativos estão associados a reticulados k-dimensionais. Baseados neste fato, desenvolvemos um método para decodificação de códigos de grupo comutativo que utiliza o algoritmo de Viterbi num diagrama de treliça do reticulado associado ao código. No método aqui proposto, os cálculos são, essencialmente, feitos na metade da dimensão e não há a necessidade do armazenamento das palavras do código.**

***Palavras-Chave*— Decodificação, Códigos de grupo comutativo, Algoritmo de Viterbi, Reticulados, Treliça.**

***Abstract*— Spherical codes in $\mathbb{R}^{2k}$ generated by commutative groups are related to k-dimensional lattices. Based on this result, a method for decoding commutative group codes which uses the Viterbi algorithm for a lattice trellis diagram is developed here. This method does not require the storage of the codewords and the calculations are essencially done in the half of the code dimension.**

***Keywords*— Decoding, commutative group codes, Viterbi algorithm, lattices, trellis.**

I. Introdução

Códigos esféricos gerados por grupos comutativos formam uma classe especial dos denominados códigos geometricamente uniformes [9]. A forte estrutura geométrica desses códigos assegura que as regiões de decodificação por máxima verossimilhança das palavras do código são congruentes.

Neste artigo, com base nos resultados de [13], que associam códigos de grupo comutativo em $\mathbb{R}^{2k}$ a quociente de reticulados em $\mathbb{R}^k$, propomos um método para decodificação de tais códigos. O método aqui proposto utiliza um diagrama de treliça do reticulado associado e não requer o armazenamento das palavras do código.

Diagramas de treliça foram introduzidos por Forney [8] em 1967, onde o algoritmo de Viterbi, inicialmente apresentado em [1], foi utilizado para decodificação de códigos convolucionais. A estrutura de treliça associada a reticulados é abordada em [11], [12], [14] e também em [2], onde a complexidade destes diagramas é estudada para a decodificação eficiente de códigos baseados em reticulados.

Este trabalho está organizado da seguinte forma: na Seção II são apresentados pré-requisitos necessários sobre reticulados, códigos de grupo comutativo, diagramas de treliça e um breve resumo sobre o algoritmo de Viterbi. Na Seção III apresentamos uma abordagem do problema de encontrar a treliça mínima de um reticulado associado a código de grupo comutativo. O método proposto para decodificação de códigos de grupo comutativo é apresentado na Seção IV e alguns exemplos são incluídos.

Agnaldo J. Ferrari, Cristiano Torezzan, Grasiele C. Jorge e Sueli I. R. Costa, Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, São Paulo, Brasil, E-mails: [ferrari, cristiano, grajorge, sueli]@ime.unicamp.br. Este trabalho foi parcialmente financiado pela FAPESP (05/58102-7, 2007/56052-8) e pelo CNPq (312061/2006-4, 143269/2008-9)

II. Preliminares

A. Reticulados

Um reticulado Λ é o conjunto de todas as combinações lineares a coeficientes inteiros de um conjunto $\beta = \{b_1, b_2, \ldots, b_m\}$ de m vetores linearmente independentes do espaço vetorial $\mathbb{R}^n$, ou seja,

$$\Lambda = \left\{ x = \sum_{i=1}^{m} a_i b_i : a_i \in \mathbb{Z} \quad \forall \quad i \right\}.$$

O conjunto β é denominado uma *base* de Λ e a matriz B, cujas linhas são os vetores da base β, é chamada *matriz geradora* de Λ. Um reticulado pode admitir diferentes matrizes geradoras, ou seja, diferentes bases. Assim, a notação Λ_β ou Λ_B será utilizada quando for necessária uma referência específica a alguma base β ou matriz geradora B.

Um reticulado Λ é denominado *racional* se o produto interno entre dois vetores quaisquer da base é um número racional, i.e., a *matriz de Gram* $P = BB^t$ de Λ tem somente coeficientes racionais.

B. Códigos de grupo comutativo

Seja $\mathcal{O}_n$ o grupo multiplicativo de matrizes ortogonais de ordem $n \times n$ e $\mathcal{G}$ um subgrupo comutativo de ordem M de $\mathcal{O}_n$.

Um *código de grupo comutativo* $\mathcal{C}_\mathcal{G}(M, n)$, associado a $\mathcal{G}$, é um conjunto de M vetores unitários, não contidos em um hiperplano, que é a orbita de um vetor x_0 da esfera unitária $S^{n-1} \subset \mathbb{R}^n$ sob a ação de $\mathcal{G}$, isto é,

$$\mathcal{C}_\mathcal{G}(M, n) = \{G_1 x_0, G_2 x_0, ..., G_M x_0\}.$$

Como é usual, a *distancia mínima* em $\mathcal{C}_\mathcal{G}(M, n)$ é definida por

$$d = \min_{\substack{x, y \in \mathcal{C}_\mathcal{G} \\ x \neq y}} ||x - y||,$$

onde $||.||$ é a norma euclidiana usual de $\mathbb{R}^n$.

A distância mínima no código $\mathcal{C}_\mathcal{G}(M, n)$ pode variar consideravelmente em função da escolha do vetor inicial x_0 e também da particular representação $\mathcal{G}$ escolhida em $\mathcal{O}_n$. O problema da procura pelo melhor código de grupo comutativo para um dado número de pontos M é apresentado em [4] e [5].

Um resultado conhecido sobre a representação irredutível de um grupo finito de matrizes ortogonais $\mathcal{G}$ é estabelecido no seguinte teorema:

Teorema 1 ([6]): Todo elemento G_i em grupo comutativo de matrizes ortogonais pode ser escrito, através de uma mesma matriz ortogonal Q, na seguinte forma pseudo diagonal:

$$Q^T G_i Q = diag[R_1(i), \ldots, R_k(i), \mu(i)_{2k+1}, \ldots, \mu(i)_n]_{n\times n}, \quad (1)$$

onde $R_j(i) = \begin{pmatrix} \cos(\frac{2\pi b_{ij}}{M}) & -\mathrm{sen}(\frac{2\pi b_{ij}}{M}) \\ \mathrm{sen}(\frac{2\pi b_{ij}}{M}) & \cos(\frac{2\pi b_{ij}}{M}) \end{pmatrix}$,
$b_{ij} \in Z$ e $\mu(i)_l = \pm 1$, $l = 2k+1, \ldots, n$.

Outro resultado importante nessa abordagem é a associação entre códigos de grupo comutativo e reticulados, como estudada em [13]. Em especial, a seguinte proposição:

Proposição 1 ([13], p. 5): Seja $\mathcal{C}_\mathcal{G}(M,n)$ um código de grupo comutativo de ordem M, em dimensão par, com vetor inicial $x_0 = (\delta_1, 0, \ldots, \delta_{n/2}, 0)$. Se $2k = n$ em (1), isto é, os elementos de $\mathcal{G}$ são livres de blocos 2×2 de reflexão, então a imagem inversa $\psi^{-1}(\mathcal{C}_\mathcal{G}(M,n))$ é um reticulado Λ gerado por k vetores da forma

$$b_i = \left(\frac{2\pi b_{i1}\delta_1}{M}, \frac{2\pi b_{i2}\delta_2}{M}, \cdots, \frac{2\pi b_{ik}\delta_k}{M}\right);\ 1 \le i \le k,$$

que contém um subreticulado ortogonal Λ' gerado por k vetores da forma

$$v_i = 2\pi\delta_i e_i,\ 1 \le i \le k,$$

onde e_i são os vetores canônicos do $\mathbb{R}^n$ e

$$\psi_{x_0}(y) = \left(\delta_1\left(\cos\frac{y_1}{\delta_1}, \mathrm{sen}\,\frac{y_1}{\delta_1}\right), \ldots, \delta_k\left(\cos\frac{y_k}{\delta_k}, \mathrm{sen}\,\frac{y_k}{\delta_k}\right)\right),$$

$\psi_{x_0}(y)$ é a parametrização canônica de um toro planar e $y = (y_1, \cdots, y_k)$. Os números δ_i são denominados raios do toro planar T_{x_0} e o definem precisamente.

Exemplo 1: O melhor código de grupo comutativo $\mathcal{C}_\mathcal{G}(200,6)$ com 200 pontos em $\mathbb{R}^6$, com máxima distância mínima, é órbita do vetor inicial

$$x_0 = (0.5551007, 0, 0.6194564, 0, 0.5551007, 0)^t$$

pela ação do grupo cíclico $\mathcal{G}$, de ordem 200, gerado pela matriz

$$G = \begin{pmatrix} R(\frac{2\pi 4}{200}) & 0 & 0 \\ 0 & R(\frac{2\pi 25}{200}) & 0 \\ 0 & 0 & R(\frac{2\pi 28}{200}) \end{pmatrix},$$

onde $R(\theta) = \begin{pmatrix} \cos(\theta) & -\mathrm{sen}(\theta) \\ \mathrm{sen}(\theta) & \cos(\theta) \end{pmatrix}$ é a matriz 2×2 de rotação no plano. Este código pertence ao toro planar de raios $\delta_1 = 0.5551007$, $\delta_2 = 0.6194564$ e $\delta_3 = 0.5551007$. O reticulado Λ associado é gerado pela matriz

$$B = \begin{pmatrix} \frac{2\pi\delta_1 4}{200} & \frac{2\pi\delta_2 25}{200} & \frac{2\pi\delta_3 28}{200} \\ 0 & \frac{2\pi\delta_2 50}{200} & 0 \\ 0 & 0 & \frac{2\pi\delta_3 200}{200} \end{pmatrix},$$

e um subreticulado ortogonal Λ' é gerado pela matriz

$$B' = \begin{pmatrix} 2\pi\delta_1 & 0 & 0 \\ 0 & 2\pi\delta_2 & 0 \\ 0 & 0 & 2\pi\delta_3 \end{pmatrix}.$$

A menos de uma deformação de $\frac{200}{2\pi\delta_1}, \frac{200}{2\pi\delta_2}, \frac{200}{2\pi\delta_3}$ em cada coordenada, respectivamente, podemos considerar o reticulado Λ gerado por

$$B_1 = \begin{pmatrix} 4 & 25 & 28 \\ 0 & 50 & 0 \\ 0 & 0 & 200 \end{pmatrix},$$

e o subreticulado Λ' gerado por

$$B_1' = \begin{pmatrix} 200 & 0 & 0 \\ 0 & 200 & 0 \\ 0 & 0 & 200 \end{pmatrix}.$$

É importante observar que esta deformação afeta a métrica do reticulado, mas não afeta sua treliça. Isso será levado em conta na decodificação.

C. Diagrama de treliça de um reticulado

Esta subseção faz um resumo dos conceitos básicos sobre diagramas de treliça de reticulados, baseado em [2], cuja notação será utilizada neste trabalho.

Sejam $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$ uma sequência de espaços vetoriais com $\dim(V_i) = i$, e W_i o complemento ortogonal de V_{i-1} em V_i para $1 \le i \le n$. Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado n-dimensional, P_{V_i} e P_{W_i} os operadores projeção de $\mathbb{R}^n$ sobre os espaços vetoriais V_i e W_i, respectivamente, $\Lambda_{V_i} = \Lambda \cap V_i$ e $\Lambda_{W_i} = \Lambda \cap W_i$.

Para a construção de um diagrama de treliça de um reticulado Λ, definimos os grupos quocientes:

$\sum_i(\Lambda) = \frac{P_{V_i}(\Lambda)}{\Lambda_{V_i}}$: *espaço de estado* no nível i, $0 \le i \le n$.
$G_i(\Lambda) = \frac{P_{W_i}(\Lambda)}{\Lambda_{W_i}}$: *grupo de rotulamento* na seção i, $1 \le i \le n$.

Definição 1: O diagrama de treliça T de um reticulado Λ é um grafo cujos nós em cada nível i, $0 \le i \le n$, são elementos de $\sum_i(\Lambda)$ e as arestas entre os níveis $i-1$ e i são rotuladas por elementos de $G_i(\Lambda)$.

No diagrama de treliça T de um reticulado Λ, cada $x \in \Lambda$ percorre um único caminho representado por uma sequência de nós $\sigma(x) = (\sigma_0(x), \cdots, \sigma_n(x))$, onde $\sigma_i(x) = \Lambda_{V_i} + P_{V_i}(x)$, que estão conectados por uma sequência de arestas $g(x) = (g_1(x), \cdots, g_n(x))$, onde $g_i(x) = \Lambda_{W_i} + P_{W_i}(x)$.

Na treliça do reticulado Λ_B tem-se que $\sigma(\Lambda)$ e $g(\Lambda)$ são isomorfos [10], e a cardinalidade de ambos, denotada por $N(\Lambda_B)$, é igual ao número de caminhos distintos na treliça.

Exemplo 2: Sejam $b_1 = (2,0)$ e $b_2 = (1,2)$ os vetores que geram um reticulado $\Lambda \subset \mathbb{R}^2$. Tomando a sequência de espaços vetoriais $\{0\} = V_0 \subset V_1 \subset V_2 = \mathbb{R}^2$, com $V_1 = ger((2,0))$, onde $ger(S)$ denota o espaço vetorial gerado por S. Temos $W_1 = V_1$ e $W_2 = ger((0,1)) = ger((0,4))$, logo

$$\sum_0(\Lambda) = \sum_2(\Lambda) = 0,\ \sum_1(\Lambda) = (1,0)\mathbb{Z}/(2,0)\mathbb{Z},$$
$$G_1(\Lambda) = (1,0)\mathbb{Z}/(2,0)\mathbb{Z},\ G_2(\Lambda) = (0,2)\mathbb{Z}/(0,4)\mathbb{Z},$$

onde $v\mathbb{Z}$ representa o grupo aditivo gerado por v (o conjunto de todos os múltiplos inteiros de v). E consequentemente,

$$\sigma(\Lambda) = \{(0,(2,0)\mathbb{Z},0), (0,(1,0)+(2,0)\mathbb{Z},0)\},$$
$$g(\Lambda) = \{((2,0)\mathbb{Z},(0,4)\mathbb{Z}), ((1,0)+(2,0)\mathbb{Z},(0,2)+(0,4)\mathbb{Z})\}.$$

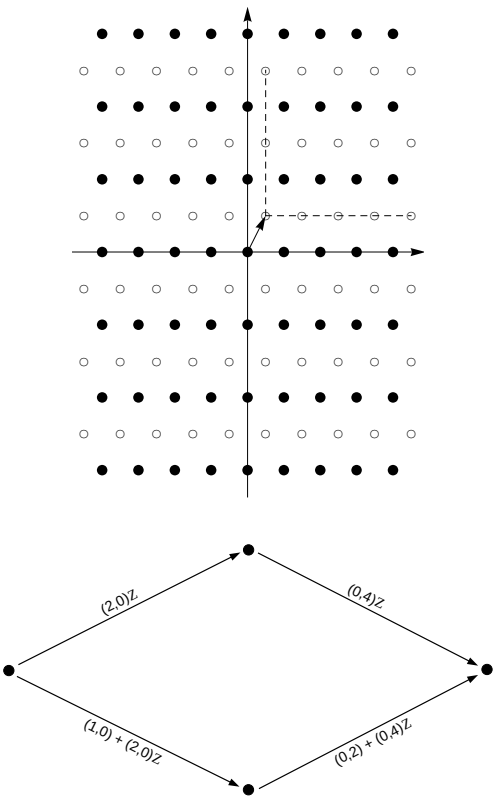

Fig. 1. O reticulado Λ e o diagrama de treliça correspondente.

Os caminhos na treliça correspondem às classes laterais do subreticulado ortogonal gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (0, 4)$. Estas classes são ilustradas pelos conjuntos de pontos pretos e brancos no reticulado Λ da Fig. 1.

Dizemos que Λ tem uma treliça finita se existe um diagrama de treliça para Λ com um número finito de nós (ou arestas). Um reticulado n-dimensional Λ possui treliça finita se, e somente se, ele possui um subreticulado ortogonal $n-$dimensional Λ' [2].

O sistema de subespaços $\{W_i\}_{i=1}^n$, correspondendo à cadeia $V_0, \cdots, V_n$, é chamado de *sistema de coordenadas-treliça* Λ para T. Assim, um reticulado Λ possui treliça finita se, e somente se, $\dim(\Lambda_{W_i}) = 1$, para todo i. Neste caso, o subreticulado ortogonal correspondente Λ' é $\Lambda_{W_1} \oplus \cdots \oplus \Lambda_{W_n}$.

Conforme visto no *Exemplo 1*, o diagrama de treliça de um reticulado Λ é uma maneira de representar Λ como a união de classes laterais de Λ' em Λ, onde cada classe lateral é representada por um caminho através da treliça. O número de classes laterais, que possui o mesmo valor do índice de Λ' em Λ, é igual a $N(\Lambda_B)$. Consequentemente, tem-se que

$$N(\Lambda_B) = \frac{det(\Lambda')}{det(\Lambda)}. \quad (2)$$

Escolhendo diferentes sistemas de coordenadas-treliça $\{W_i\}_{i=1}^n$, tem-se diferentes diagramas de treliça, logo o diagrama de treliça de um reticulado não é único.

Para melhorar a eficiência no processo de decodificação, é desejável encontrar uma treliça menos complexa para o reticulado. Usaremos $N(\Lambda_B)$ como medida de complexidade, isto é, dado um reticulado Λ associado a um código de grupo comutativo $\mathcal{C}_\mathcal{G}(M, n)$, queremos encontrar uma treliça para este reticulado tal que $N(\Lambda_B)$ seja o menor possível. As treliças mínimas de alguns importantes reticulados são conhecidas [2], mas de um modo geral, procurar pela treliça mínima de um reticulado qualquer é um problema difícil. Se Λ é um reticulado racional $n-$dimensional, então qualquer base $\{b_1, \cdots, b_n\}$ de Λ resulta em uma treliça finita para Λ (Lemma 3, [2]). Isto pode ser feito tomando $V_i = ger(b_1, \cdots, b_i)$, e $W_i = ger(\hat{b}_i)$, para $1 \leq i \leq n$, onde $\hat{b}_1, \cdots, \hat{b}_n \in \mathbb{R}^n$ é o conjunto dos vetores *Gram-Schmidt* de $b_1, \cdots, b_n \in \mathbb{R}^n$, isto é,

$$\hat{b}_i = b_i - \sum_{j=i}^{i-1} \frac{\langle b_i, \hat{b}_j \rangle}{\langle \hat{b}_j, \hat{b}_j \rangle} \hat{b}_j.$$

Observamos que existem múltiplos racionais de $\hat{b}_i$ formando uma base para um subreticulado ortogonal de Λ.

Exemplo 3: Sejam $b_1 = (-8, 0, -56)$, $b_2 = (-8, 0, -256)$ e $b_3 = (-4, -25, -425)$ os vetores que geram um reticulado Λ que é o mesmo apresentado no *Exemplo 1*. No sistema de coordenadas-treliça

$$W_1 = ger(\hat{b}_1) = ger(b_1),$$

$$W_2 = ger(\hat{b}_2) = ger((28, 0, -4)),$$

$$W_3 = ger(\hat{b}_3) = ger((0, -25, 0)),$$

Λ tem a treliça da Fig. 2. Os *grupos de rotulamento* são

$$G_1 = (-4, 0, -28)\mathbb{Z}/(-8, 0, -56)\mathbb{Z},$$

$$G_2 = (28, 0, -4)\mathbb{Z}/(56, 0, -8)\mathbb{Z} \text{ e}$$

$$G_3 = (0, -25, 0)\mathbb{Z}/(0, -50, 0)\mathbb{Z}.$$

Os quatro caminhos da treliça correspondem às classes laterais do subreticulado ortogonal gerado pelo vetores $v_1 = (-8, 0, -56)$, $v_2 = (56, 0, -8)$ e $v_3 = (0, -50, 0)$, em Λ.

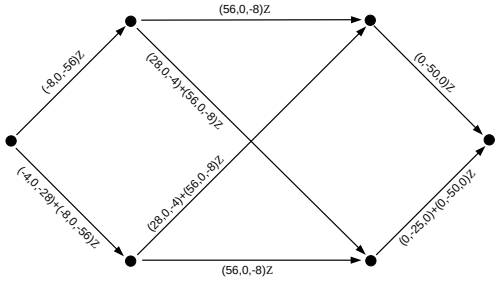

Fig. 2. Um diagrama treliça de Λ.

Uma questão relevante é se esta é a treliça mínima para Λ. Ainda não se conhece um método geral para encontrar uma treliça mínima de um reticulado qualquer. Na Seção III apresentamos uma discussão que permite abordar este problema no caso de reticulados associados a códigos de grupo comutativo.

D. Algoritmo de Viterbi

Nesta subseção descrevemos o algoritmo de Viterbi, utilizado na decodificação de reticulados associados a uma treliça com um número finito de caminhos.

Seja T uma treliça finita de um reticulado Λ n-dimensional, com relação ao sistema de coordenadas-treliça $\{W_i\}_{i=1}^n$. Dado $x \in \mathbb{R}^n$, o objetivo é encontrar $y \in \Lambda$ tal que

$$||y - x|| \leq ||u - x||, \ \forall u \in \Lambda.$$

Seja v_i o vetor de menor comprimento em Λ_{W_i}, para $i = 1, 2, \cdots, n$, ou seja, $\Lambda_{W_i} = v_i\mathbb{Z}$. Como os vetores $v_1, v_2, \cdots, v_n$ são ortogonais, podemos escrever

$$x = \sum_{i=1}^{n} \beta_i v_i, \text{ onde } \beta_i = \frac{\langle x, v_i \rangle}{\langle v_i, v_i \rangle}.$$

Vamos atribuir a distância d_{ij} a cada uma das arestas da treliça T, que representam os elementos de

$$G_i(\Lambda) = \{a_{ij}v_i + v_i\mathbb{Z};\ a_{ij}v_i \in P_{W_i}(\Lambda)\},$$

para $i = 1, \cdots, n$ e $j = 1, \cdots, |G_i(\Lambda)|$.

Seja $z_{ik} = c_{ik}v_i$ o elemento da k-ésima classe de $G_i(\Lambda)$ mais próximo de $\beta_i v_i$, ou seja,

$$||z_{ik} - \beta_i v_i|| \leq ||\zeta_{ik} - \beta_i v_i||, \ \forall \zeta_{ik} \in \{a_{ik}v_i + v_i\mathbb{Z};\ a_{ik}v_i \in P_{W_i}(\Lambda)\},$$

onde $c_{ik} = a_{ik} + \lceil \beta_i - a_{ik} \rfloor$ e $\lceil t \rfloor$ denota o inteiro mais próximo do número t.

Assim,

$$d_{ij} = ||c_{ij}v_i - \beta_i v_i||^2 = ((\beta_i - a_{ij}) - \lceil \beta_i - a_{ij} \rfloor)^2 \, ||v_i||^2.$$

Algoritmo de Viterbi:

1º Passo: Calcule d_{ij} para todo $i = 1, \cdots, n$ e $j = 1, \cdots, |G_i(\Lambda)|$ e associe esta distância à aresta da treliça rotulada por $a_{ij}v_i + v_i\mathbb{Z}$. Faça $k = 2$.

2º Passo: Para todo $t = 1, \cdots, |\sum_k(\Lambda)|$, considere o elemento $S_{kt} \in \sum_k(\Lambda)$ e selecione todos os caminhos sobreviventes que saem de $\sum_0(\Lambda)$ e chegam em S_{kt}. Para cada um destes caminhos some as distâncias associadas e encontre o mínimo entre essas somas. Considere como caminho sobrevivente aquele cuja soma for mínima e descarte os demais caminhos.

3º Passo: Faça $k = k + 1$. Se $k \leq n$, repita o passo 2, caso contrário, com um único caminho sobrevivente partindo de $\sum_0(\Lambda)$ e chegando em $\sum_n(\Lambda)$, decodifique x como $y = c_{1k_1}v_1 + \cdots + c_{nk_n}v_n$, onde $c_{ik_i}v_i + v_i\mathbb{Z}$, para $i = 1, 2, \cdots, n$, é a classe associada a cada parte do caminho sobrevivente.

III. Treliça mínima de reticulados associados a código de grupo comutativo

Para os reticulados estudados neste trabalho uma treliça mínima foi encontrada através da implementação de um algoritmo computacional que procura um subreticulado ortogonal com o menor determinante, restrito à um conjunto finito de casos. Esta abordagem é baseada na seguinte idéia.

Seja Λ um reticulado n-dimensional com matriz de Gram racional. Vimos na Seção II que para cada escolha de subespaços $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$ existe um subreticulado ortogonal $\Lambda' = \Lambda_{W_1} \oplus \cdots \oplus \Lambda_{W_n}$ de Λ. Da mesma forma, dado um subreticulado ortogonal Λ' de Λ com base $\{v_1, \cdots, v_n\}$ e tomando $V_i = ger(v_1, \cdots, v_i)$ para todo $i = 1, \cdots, n$, temos que $\Lambda' = \Lambda_{W_1} \oplus \cdots \oplus \Lambda_{W_n}$. Assim, pela Equação (2), vemos que a procura por uma treliça minimal em um reticulado Λ é equivalente a procura por um subreticulado ortogonal Λ' de Λ com o menor determinante possível.

Pela *Proposição 1* a menos de uma deformação, o reticulado Λ possui um subreticulado ortogonal Λ' gerado pela matriz MI_n. Assim, é possível obter uma treliça com M caminhos para tal reticulado, pois $N(\Lambda) = \frac{det(\Lambda')}{det(\Lambda)} = \frac{M^n}{M^{n-1}} = M$. Para reduzir a complexidade na decodificação do código de grupo comutativo associado a Λ devemos encontrar uma treliça com o menor número de caminhos para esse reticulado, considerando o limitante superior M.

Uma treliça mínima para Λ pode ser encontrada através da inspeção de um conjunto finito de subreticulados ortogonais. Sem perda de generalidade, podemos considerar que os vetores v_i geradores de Λ', são tais que $||v_1|| \leq ||v_2|| \leq \cdots \leq ||v_n||$. Como estamos interessados em $det(\Lambda') \leq M^n$, segue que $||v_n|| \leq \frac{M^n}{\lambda^{n-1}}$, onde λ é a norma mínima do reticulado Λ.

Exemplo 4: Considere o reticulado Λ com matriz geradora

$$B = \begin{pmatrix} 4 & 25 & 28 \\ 0 & 50 & 0 \\ 0 & 0 & 200 \end{pmatrix}.$$

Temos que $det(\Lambda) = 200^2$. Como $200I_3$ é subreticulado ortogonal de Λ, existe uma treliça com 200 caminhos associada a Λ. O *Exemplo 3* mostra uma treliça com 4 caminhos de Λ, associada ao subreticulado ortogonal gerado pelos vetores $(-8, 0, -56), (56, 0, -8)$ e $(0, -50, 0)$. Considerando o subreticulado ortogonal Λ^* gerado pelos vetores $v_1^* = (-32, 0, -24), v_2^* = (-24, 0, 32)$ e $v_3^* = (0, 50, 0)$, obtemos uma treliça com dois caminhos, como pode ser visto na Fig 3. Como o reticulado Λ não é ortogonal, podemos concluir que essa treliça é mínima para Λ.

Uma implementação cuidadosa pode permitir a redução iterativa no conjunto de casos a ser analisados. A cada subreticulado Λ' encontrado, com $\det(\Lambda') = D < M^n$, a norma dos vetores que interessam passa a satisfazer

$$||v_n|| \leq \frac{D}{\lambda^{n-1}}.$$

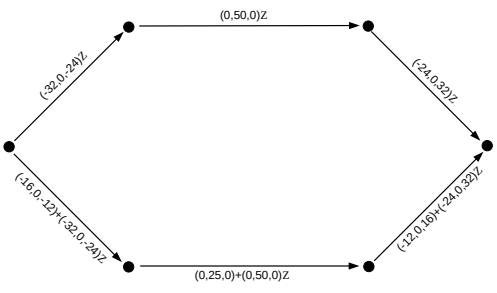

Fig. 3. Uma treliça mínima para Λ.

IV. DECODIFICAÇÃO EM CÓDIGOS DE GRUPO COMUTATIVO

Seja $x \in \mathbb{R}^{2k}$ um ponto qualquer, $\mathcal{C}_\mathcal{G}(M,2k)$ um código de grupo comutativo com vetor inicial $x_0 = (\delta_1, 0, \ldots, \delta_k, 0)$ e B uma matriz geradora do reticulado $k-$dimensional Λ associado a $\mathcal{C}_\mathcal{G}(M,2k)$.

Nesta seção desenvolvemos um método para decodificação de x em $\mathcal{C}_\mathcal{G}(M,2k)$. O método é baseado em máxima verossimilhança, ou decodificação por mínima distância, i.e., busca-se

$$y = \arg\min_{y_i \in \mathcal{C}} ||x - y_i||.$$

A proposição a seguir mostra que o primeiro passo para decodificar x é normalizá-lo.

Proposição 2: Para qualquer $x \in \mathbb{R}^n$ e qualquer código esférico $\mathcal{C}$, tem-se que

$$\arg\min_{y\in\mathcal{C}} \left\| \frac{x}{||x||} - y \right\| = \arg\min_{y\in\mathcal{C}} \|x - y\|.$$

Demonstração:
Se $y \in \mathcal{C}$ é tal que,

$$\left\| \frac{x}{||x||} - y \right\| \leq \left\| \frac{x}{||x||} - z \right\|, \quad \forall \quad z \in \mathcal{C},$$

tem-se que

$$2 - 2\left\langle \frac{x}{||x||}, y \right\rangle \leq 2 - 2\left\langle \frac{x}{||x||}, z \right\rangle \Rightarrow \langle x, y\rangle \geq \langle x, z\rangle.$$

Assim,

$$\|x - y\| = ||x||^2 + 1 - 2\langle x, y\rangle \leq ||x||^2 + 1 - 2\langle x, z\rangle = \|x - z\|.$$

Portanto,

$$\arg\min_{y\in\mathcal{C}} \left\| \frac{x}{||x||} - y \right\| = \arg\min_{y\in\mathcal{C}} \|x - y\|. \quad \blacksquare$$

Para qualquer vetor unitário $x = (x_1, x_2, \ldots, x_{2k-1}, x_{2k})$, podemos escrever

$$\begin{aligned} x &= \left(\sqrt{x_1^2 + x_2^2} \left(\frac{x_1}{\sqrt{x_1^2+x_2^2}}, \frac{x_2}{\sqrt{x_1^2+x_2^2}} \right), \ldots, \right), \\ x &= \left(\gamma_1 \left(\cos\frac{\theta_1}{\gamma_1}, \text{sen}\,\frac{\theta_1}{\gamma_1} \right), \ldots, \gamma_k \left(\cos\frac{\theta_k}{\gamma_k}, \text{sen}\,\frac{\theta_k}{\gamma_k} \right) \right), \end{aligned}$$

onde,

$$\begin{aligned} \gamma_i &= \sqrt{x_{2i-1}^2 + x_{2i}^2}, \quad 1 \leq i \leq k, \\ \theta_i &= \arccos\left(\frac{x_{2i-1}}{\gamma_i} \right) \gamma_i, \quad 1 \leq i \leq k. \end{aligned}$$

Isto significa que x pertence ao toro planar de raios $\gamma_i, \quad 1 \leq i \leq k$.
De acordo com a *Proposição* 1, sejam T_{x_0} o toro planar que contém o código $\mathcal{C}_\mathcal{G}(M,2k)$, e w o vetor em T_{x_0} mais próximo de x.
De acordo com [3],

$$w = \left(\delta_1 \left(\cos\frac{\theta_1}{\gamma_1}, \text{sen}\,\frac{\theta_1}{\gamma_1} \right), \ldots, \delta_k \left(\cos\frac{\theta_k}{\gamma_k}, \text{sen}\,\frac{\theta_k}{\gamma_k} \right) \right),$$

e a distância mínima entre T_{x_0} e x é dada por $d_* = \|x - w\|$. Portanto, o segundo passo para decodificação é projetar x em T_{x_0} obtendo w.
Como $w \in T_{x_0}$ podemos utilizar a imagem inversa $z = \psi_{x_0}^{-1}(w) \in \mathbb{R}^k$ ("planificar o toro") e obter $z \in \mathbb{R}^k$, ou seja,

$$z = \left(\frac{\delta_1\theta_1}{\gamma_1}, \frac{\delta_2\theta_2}{\gamma_2}, \cdots, \frac{\delta_k\theta_k}{\gamma_k} \right).$$

Finalmente a decodificação pode ser realizada procurando o ponto do reticulado Λ mais próximo de z, utilizando o algoritmo de Viterbi descrito na seção anterior.

A seguir apresentamos um resumo do método.

Algoritmo para decodificação em $C_\mathcal{G}(M,2k)$:
Dado um código de grupo comutativo $C_\mathcal{G}(M,2k)$, com vetor inicial $x_0 = (\delta_1, 0, \delta_2, 0, \cdots, \delta_k, 0)$, uma treliça T do reticulado Λ associado ao código e um ponto $x \in \mathbb{R}^{2k}$:

1º Passo: Faça

$$\frac{x}{||x||} = (x_1, x_2, \ldots, x_{2k-1}, x_{2k});$$

2º Passo: Obtenha o ponto $z \in \mathbb{R}^k$,

$$z = \left(\frac{\delta_1\theta_1}{\gamma_1}, \frac{\delta_2\theta_2}{\gamma_2}, \cdots, \frac{\delta_k\theta_k}{\gamma_k} \right),$$

e utilize o algoritmo de Viterbi para decodificar z no reticulado Λ através da treliça T, obtendo o ponto $u = (u_1, u_2, \cdots, u_k)$.

3º Passo: O resultado da decodificação de x em $C_\mathcal{G}(M,2k)$ é a imagem de u por ψ_{x_0}, ou seja,

$$y = \left(\delta_1 \cos\left(\frac{u_1}{\delta_1}\right), \delta_1 \sin\left(\frac{u_1}{\delta_1}\right), \ldots, \delta_k \cos\left(\frac{u_k}{\delta_k}\right), \delta_k \sin\left(\frac{u_k}{\delta_k}\right) \right).$$

A etapa mais cara do processo de decodificação apresentado acima é o **2º Passo**, que consiste numa decodificação em reticulado na metade da dimensão do código. Como já foi comentado, este custo está diretamente relacionado à complexidade da treliça do reticulado associado ao código. O número de operações C requeridas pelo Algoritmo de Viterbi para decodificar $\Lambda_T \subset \mathbb{R}^k$ satisfaz [2]

$$C \leq k(7N(\Lambda_T) - N(\Lambda_T)^{1/k} + 4k).$$

Na decodificação que estamos propondo, não se faz necessário gerar os pontos do código esférico $C_\mathcal{G}(M,2k)$, o que pode significar uma importante vantagem do ponto de vista de utilização de memória na decodificação. O número de candidatos que precisam ser efetivamente computados e armazenados na memória é menor ou igual ao número de caminhos na treliça utilizada.

Na Fig 4 apresentamos uma ilustração do método de decodificação aqui proposto. Os rótulos das linhas pontilhadas indicam a sequência de passos do método.

Exemplo 5: Considerando o código de grupo comutativo $C_\mathcal{G}(200,6)$ apresentado no *Exemplo 1*, vamos decodificar o

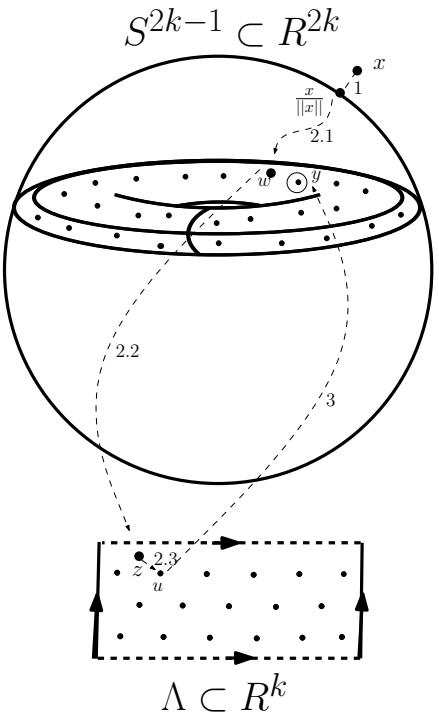

Fig. 4. Ilustração do método de decodificação.

ponto $x = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0\right)$, seguindo os passos do algoritmo proposto.

1º Passo:

$$\frac{x}{||x||} = \frac{1}{\sqrt{5}}\,(1, 1, 1, 1, 1, 0)\,;$$

2º Passo:

$$z = (0.435975, 0.48652, 0);$$

Como o reticulado Λ, associado ao código $C_{\mathcal{G}}(200, 6)$, possui uma treliça com apenas dois caminhos (*Exemplo 4*), temos apenas dois candidatos à decodificação, $u_1 = (0.558, 0.973, 0.418)$ e $u_2 = (0.488, 0.486, -0.0697)$. Estes pontos são obtidos da decodificação de z em cada uma das classes laterais de Λ, representadas pelos caminhos na treliça[1]. O cálculo de u_1 e u_2 envolve apenas operações elementares de soma e multiplicação, produto interno e arredondamento, não existe nenhum procedimento de busca envolvido.

Como $||u_2 - z|| < ||u_1 - z||$, concluímos que u_2 é a decodificação de z em Λ.

3º Passo:

$$y = (0.3538, 0.4277, 0.4380, 0.4380, 0.5507, -0.06957)$$

é o ponto de $C_{\mathcal{G}}(200, 6)$ mais próximo do ponto $x = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0\right)$.

[1]Conforme dito no *Exemplo 1*, para simplificar a notação, o diagrama de treliça foi construído considerando uma deformação em cada coordenada, para a decodificação esta deformação foi revertida. Geometricamente essa deformação equivale à uma dilatação ou contração na caixa que representa o toro planar associado ao código, ela não afeta a forma da treliça de Λ.

V. Conclusão

Neste trabalho, apresentamos um algoritmo para decodificação em códigos esféricos gerados por grupos comutativos. O método desenvolvido é baseado na associação entre um código de grupo comutativo em $\mathbb{R}^{2k}$ e o diagrama treliça de um reticulado $k-$dimensional. A complexidade do algoritmo está relacionada com o número de caminhos na treliça e, durante o processo de decodificação, não é necessário gerar os pontos do código, o que em termos práticos, significa uma importante economia de memória no decodificador.

Referências

[1] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," IEEE Trans. Inform. Theory, vol IT-13, pp. 260-269, Apr. 1967.

[2] A.H. Banihashemi and I.F. Blake, "Trellis complexity and minimal trellis of lattices," IEEE Trans. Inform. Theory, vol IT-44, n 5, pp. 1829-1847, Sep. 1998.

[3] C. Torezzan, S. I. R. Costa and V. Vaishampayan, "Spherical codes on Torus Layers," 2009 International Symposium on Information Theory. Seoul, Coréia, Jun - 2009.

[4] C. Torezzan, J. E. Strapasson, S. I. R. Costa and R. M. Siqueira, "Optimum commutative group codes," Submited, 2009.

[5] C. Torezzan, J. E. Strapasson, S. I. R. Costa e R. M. Siqueira, "Códigos de grupo comutativo para o canal gaussiano: Aproximando-se do limitante," XXVI Simpósio Brasileiro de Telecomunicações - SBrT08 - Rio de Janeiro-RJ, 2008.

[6] F. R. Gantmacher, "The theory of matrices," Chelsea, New York, 1959, vol 1.

[7] D. Slepian,"Group codes for the Gaussian Channel," The Bell System Technical Journal, vol 47, pp. 575-602, 1968.

[8] G. D. Forney Jr., "Final report on a coding system design for advanced solar missions," Contract NAS2-3637, NASA Ames Research Center. Moffet Field, CA, Dec 1967.

[9] G. D. Forney, "Geometrically uniform codes," IEEE Trans. Inform. Theory, vol 37, No. 6, pp. 1241-1259, September 1991.

[10] G. D. Forney Jr. and M. D. Trott, "The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders," IEEE Trans. Inform. Theory, vol IT-39, no 9, pp. 1491-1513, Sept. 1993.

[11] G. D. Forney Jr., "Coset codes-I: Introduction and geometrical classification," IEEE Transactions on Information Theory 34(5): 1123-1151 (1988).

[12] G. D. Forney Jr., "Coset codes-II: Binary lattices and related codes," IEEE Transactions on Information Theory 34(5): 1152-1187 (1988).

[13] R. M. Siqueira and S. I. R. Costa, "Flat Tori, Lattices and Bounds for Commutative Group Codes," Designs, Codes and Cryptography, vol 49, pp 307-312, Dez, 2008.

[14] V. Tarokh, A. Vardy and K. Zeger, "Universal Bound on the Performance of Lattice Codes," IEEE Transactions on Information Theory 45(2): 670-681 (1999).