Introdução

Carina Alves
Antonio Aparecido de Andrade

ALVES, C., and ANDRADE, AA. Introdução. In: *Reticulados via corpos ciclotômicos* [online]. São Paulo: Editora UNESP, 2014, pp. 17-21. ISBN 978-85-68334-39-3. Available from SciELO Books <http://books.scielo.org>.

Introdução

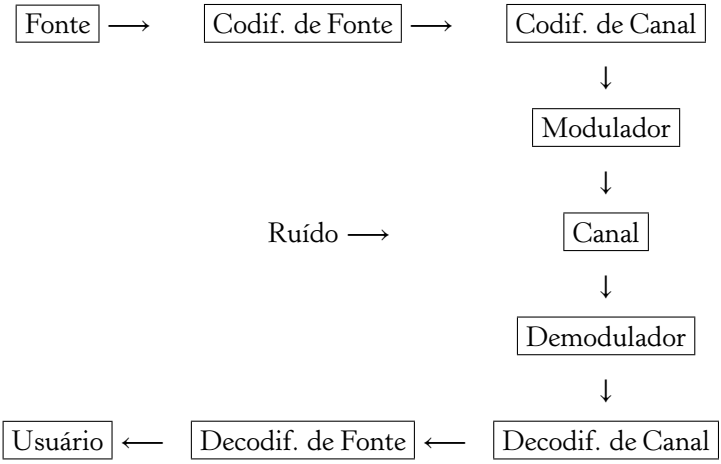
Em um sistema de comunicação digital, o objetivo é transmitir dados de uma fonte até um usuário. O meio usado para esta transmissão é chamado de canal e pode ser um cabo coaxial, fibra óptica, a atmosfera (no caso de ondas de rádio) etc.

Em um sistema tradicional, os dados gerados pela fonte são símbolos de um alfabeto A. Como cada símbolo tem sua probabilidade de ocorrência, estes dados são processados pelo codificador de fonte, com o objetivo de eliminar redundância, ou seja, tornar os símbolos equiprováveis e desta forma compactar a informação.

As sequências geradas pelo codificador de fonte são então processadas pelo codificador de canal, que introduz redundância, gerando sequências de símbolos de A que são chamadas de palavras código. Para a transmissão, o modulador associa a cada palavra código x um símbolo analógico, que é então enviado pelo canal.

A imperfeição do canal gera distorções e o sinal recebido nem

sempre coincide com o enviado. O demodulador faz então a melhor estimativa, fornecendo uma sequência r de símbolos de A. Devido ao ruído, é possível que r não seja uma palavra código. Então o decodificador de canal associará uma palavra código, que é a melhor estimativa. Finalmente, o decodificador de fonte associará a esta palavra código a suposta sequência original de símbolos enviada. O diagrama abaixo ilustra o processo.



Cada uma destas etapas gerou grandes áreas de pesquisa, que se desenvolveram, de certa forma, independentemente.

A teoria dos códigos corretores de erros nasceu em 1948, com o famoso trabalho de Shannon (1948), no qual foi demonstrado o Teorema da Capacidade de Canal. Em linhas gerais, este resultado diz que para transmissão de dados abaixo de uma taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco (AWGN), limitado em faixa consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano n-dimensional, para n suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Para cada n, Minkowski provou a existência de reticulados no espaço euclidiano n-dimensional com densidade de empacotamento esférico δ satisfazendo

$$\delta \geq \frac{\zeta(n)}{2^{n-1}},$$

onde ζ é a função zeta de Riemann. Como consequência, obtém-se

$$\frac{1}{n} log_2 \delta \geq -1. \tag{1}$$

Depois disto, Leech mostrou como usar códigos corretores de erros para construir empacotamentos esféricos densos no $\mathbb{R}^n$, Conway e Sloane (199) provaram que reticulados satisfazendo a cota de Minkowski, dada pela Equação (1) são equivalentes a códigos atingindo a capacidade do canal.

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço Euclidiano n-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Isto pode ser visto como a versão euclidiana do 18º Problema de Hilbert, proposto em 1900.

Dentre os métodos de geração de reticulados, o homomorfismo de Minkowski apresenta características interessantes. Usando teoria algébrica dos números, Craig (1978) reproduziu o reticulado de Leech Λ_{24} através da representação geométrica de um ideal no anel de inteiros de $\mathbb{Q}(\zeta_{39})$. Com o mesmo método, ainda obteve a família A_n^m em dimensões $n = p - 1$, através de $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Embora os resultados apresentados aqui não sejam traduções fiéis dos originais, eles são equivalentes ou consequências dos mesmos. Des-
sa forma, o restante do livro está delineado na sequência que segue.

O Capítulo 1, visa atender aos leitores com menos conhecimentos em teoria algébrica dos números. Sendo assim, introduzimos os conceitos de módulo, inteiro algébrico, norma e traço de um elemento, discriminante, base integral, anel de Dedekind e outros conceitos indispensáveis ao desenvolvimento dos demais capítulos. Além disso, estudamos formas quadráticas, cuja aplicação se faz quando tentamos determinar o raio de empacotamento da realização geométrica de um ideal em questão. No Capítulo 2, apresentamos um estudo sobre corpos de números, dando ênfase ao estudo dos anéis dos inteiros e discriminantes de corpos quadráticos e ciclotômicos. Também apresentamos a decomposição de um ideal primo em uma extensão fazendo uso do Teorema de Kummer.

No Capítulo 3, apresentamos as definições de reticulado, empacotamento esférico, volume e densidade de centro. Além disso,

apresentamos o método de Minkowski para obtenção de reticulados via a representação geométrica de ideais dos anéis de inteiros algébricos.

O estudo desses capítulos proporcionou-nos ferramentas necessárias para o estudo do Capítulo 4, no qual apresentamos o tema central desse livro. Este capítulo traz um método para o cálculo da densidade de centro de reticulados gerados através de ideais dos anéis de inteiros de $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$, onde p e q são números primos distintos e r é um inteiro maior ou igual a 1.

No Capítulo 5, no qual finalizamos nosso trabalho, apresentamos através do trabalho de Boutros; Viterbo; Rastello; Belfiori (1996), constelações de reticulados que são eficientes para ambos os canais Gaussianos e Rayleigh com desvanecimento, enfocando as construções das versões rotacionadas dos reticulados já conhecidos na literatura, tais como, $\boldsymbol{D}_4$, $\boldsymbol{K}_{12}$ e Λ_{16}, através da matriz mudança de base de um ideal contido no anel dos inteiros de um corpo de números.