Reticulados e o Canal Gaussiano

Antonio Campello

22 de setembro de 2012

1 Introdução

O canal Gaussiano é um modelo de transmissão de informação de interesse bastante prático que pode ser utilizado para modelar diversos sistemas de comunicação. Podemos descrevê-lo informalmente da seguinte forma. Seja um valor X_i ao qual chamaremos de entrada do canal e que pretendemos transmitir a um destinatário. No processo de transmissão, um ruído distorcerá X_i somando a este valor uma variável aleatória Z_i com distribuição normal de média 0 e variância σ^2 (isto é, $Z_i \sim \mathcal{N}(0, \sigma^2)$). O valor $Y_i = X_i + Z_i$ será chamado de saída do canal. Um receptor observa várias amostras de Y_i ($\boldsymbol{Y} = (Y_1, \ldots, Y_n)$, digamos) e tenta, a partir daí, descobrir quanto vale $\boldsymbol{X} = (X_1, \ldots, X_n)$. O problema do canal Gaussiano pergunta pela melhor maneira de escolher os valores X_i enviados de modo que o receptor possa recuperá-los com confiabilidade. Daremos conceitos mais precisos sobre o canal Gaussiano na Seção 3.

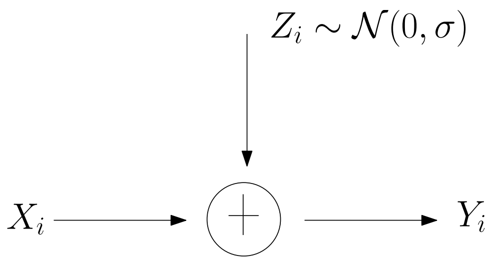

Figura 1: Representação do canal Gaussiano

De uma maneira geral, não é possível (por limitações físicas) transmitir qualquer vetor $\boldsymbol{X}$. Estaremos restritos aos vetores tais que

$$\|\boldsymbol{X}\| \leq nP$$

para algum $P > 0$, onde $\|.\|$ denota a norma euclidiana. Esta restrição é comumente chamada de restrição de potência média. Claude Shannon, em seu artigo seminal [5] demonstrou que ainda com esta restrição é possível desenvolver um esquema tal que o receptor adivinhará o vetor enviado com alta probabilidade, desde que o número de vetores escolhidos para serem enviados por dimensão não ultrapasse um certo número, o qual chamaremos de capacidade do canal. É interessante notar que sem a restrição de potência (ou com ruído nulo) a capacidade do canal Gaussiano é infinita.

2 Preliminares

Seja $\boldsymbol{x} \in \mathbb{R}^n$ e $R > 0$. Denotaremos por $B(\boldsymbol{x}, R)$ a bola euclidiana de raio R centrada em $\boldsymbol{x}$. O volume de $B(\boldsymbol{x}, R)$ será dado por

$$\operatorname{vol}(B(\boldsymbol{x}, R)) = \frac{R^n \pi^n}{(n/2)!},$$

onde $(n/2)!$ deverá ser entendido como a função gama se n for ímpar.

Teorema 1. *Seja Λ um reticulado e seja $S(R) = \Lambda \cap B(0, R)$ o conjunto dos pontos de Λ contidos em $B(0, R)$. Temos:*

$$\det \Lambda = \lim_{R \to \infty} \frac{\mathrm{vol}(B(0, R))}{\# S_n(R)}$$

Demonstração. Seja $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ uma base para Λ e

$$\mathcal{P} = \{\alpha_1 \boldsymbol{b_1} + \ldots + \alpha_n \boldsymbol{b_n} : 0 \leq \alpha_i < 1, i = 1, \ldots n\}$$

o paralelotopo fundamental associado a essa base. Definimos $L = \sup \{\|\boldsymbol{x}\| : \boldsymbol{x} \in \mathcal{P}\}$ e consideramos o conjunto $\bigcup_{\boldsymbol{x}} (\boldsymbol{x} + \mathcal{P})$, onde a união é tomada sobre todos os $\boldsymbol{x} \in S(R)$. Para $R > L$, temos:

$$B(0, R - L) \subset \bigcup_{\boldsymbol{x}} (\boldsymbol{x} + \mathcal{P}) \subset B(0, R + L).$$

A segunda inclusão segue diretamente das definições dos conjuntos. Para a primeira inclusão, tome $\boldsymbol{y} \in B(0, R - L)$ e seja $\boldsymbol{z} \in \Lambda$ tal que $\boldsymbol{y} - \boldsymbol{z} \in \mathcal{P}$. Então:

$$\|\boldsymbol{z}\| \leq \|\boldsymbol{y}\| + \|\boldsymbol{z} - \boldsymbol{y}\| \leq (R - l) + L = R.$$

Temos portanto

$$\mathrm{vol}(B(0, R - L)) \leq \mathrm{vol}\left(\bigcup_{\boldsymbol{x}} (\boldsymbol{x} + \mathcal{P})\right) \leq \mathrm{vol}(B(0, R + L)) \Rightarrow$$
$$\mathrm{vol}(B(0, R - L)) \leq \# S(R) \det \Lambda \leq \mathrm{vol}(B(0, R + L)) \Rightarrow$$
$$\frac{\mathrm{vol}(B(0, R - L))}{\mathrm{vol}(B(0, R))} \leq \frac{\# S(R) \det \Lambda}{\mathrm{vol}(B(0, R))} \leq \frac{\mathrm{vol}(B(0, R + L))}{\mathrm{vol}(B(0, R))},$$

e tirando o limite para $R \to \infty$ temos o resultado. □

A proposição acima nos diz que a aproximação $\# S(R) \approx \mathrm{vol} B(0, R) / \det \Lambda$ é boa para R grande.

Do ponto de vista estatístico, necessitamos de algumas ferramentas para descrever o canal Gaussiano. A maioria dos argumentos de plausibilidade dos limitantes para este canal decorrem de um fato estatístico conhecido como a "Lei dos grandes números". Essencialmente, esta lei afirma que a média de amostras de uma variável aleatória converge (em probabilidade) para a média da distribuição, quando o número de amostras tende a infinito.

Teorema 2 (Lei (fraca) dos grandes números)**.** *Seja $X_1, X_2, \ldots$ uma sequência de variáveis aleatorias iid (independentes e identicamente distribuídas) com média μ e variância $\sigma^2 < \infty$. Seja $\overline{X}_n = (1/n)(X_1 + \ldots + X_n)$. Temos que, para qualquer $\varepsilon > 0$,*

$$P\left\{\left|\overline{X}_n - \mu\right| \geq \varepsilon\right\} \to 0 \textit{ quando } n \to \infty$$

Demonstração. Ver [4]. □

Em particular, o corolário abaixo segue diretamente da Lei dos grandes números e será necessário para alguns dos argumentos apresentados nas seções seguintes. Daqui para frente, denotaremos por $\mathcal{N}(\mu, \sigma^2)$ a distribuição normal com média μ e variância σ^2 i.e., a distribuição cuja função densidade de probabilidade é dada por

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/2\sigma^2}.$$

Corolário 1. *Seja* $X_1, X_2, \ldots,$ *uma sequência de variáveis aleatórias iid tal que* $X_i \sim \mathcal{N}(0, \sigma^2)$. *Então, para qualquer* $\varepsilon > 0$

$$P\left\{\left|\frac{X_1^2 + \ldots + X_n^2}{n} - \sigma^2\right| \geq \varepsilon\right\} \to 0 \text{ quando } n \to \infty.$$

Em particular, se $\boldsymbol{X} = (X_1, \ldots, X_n)$, *então*

$$P\left\{\boldsymbol{X} \in B\left(0, \sqrt{n(\sigma^2 + \varepsilon)}\right)\right\} \to 1 \text{ quando } n \to \infty.$$

3 A capacidade do canal

3.1 Descrição

O canal Gaussiano foi brevemente descrito na introdução. Daremos uma definição do que é um código para este canal, bem como uma definição precisa da capacidade. Primeiramente, precisamos de um conjunto de índices $\mathcal{I} = \{1, \ldots, M\}$ correspondente às possíveis mensagens a serem enviadas através do canal, que serão codificadas em pontos do $\mathbb{R}^n$.

Definição 1. *Um código* (M, n) *para o canal Gaussiano consiste de:*

- *Um conjunto de índices* $\mathcal{I} = \{1, 2, \ldots, M\}$ *e uma função injetiva* $f : \mathcal{I} \to \mathbb{R}^n$ *tal que* $f(i) = \boldsymbol{x}(i) = (x_1(i), \ldots, x_n(i))$ *corresponde a uma palavra-código respeitando a restrição de potência* $\|\boldsymbol{x}(i)\| \leq nP$. $C = f(\mathcal{I})$ *é chamado de dicionário.*
- *Uma função* $g : \mathbb{R}^n \to \mathcal{I}$ *que leva cada possível do canal a uma possível mensagem. Como* f *é injetiva, a função* g *também relaciona cada possível saída do canal com uma palavra-código.*

Como uma palavra código está univocamente identificada com um elemento do conjunto de índices, de uma maneira geral não nos importamos com a maneira com que codificaremos a informação (isto é, com a função f), ou seja, trabalharemos apenas com o conjunto de palavras-código e regras de decodificação que levam a saída do canal em uma palavra código (em $\mathbb{R}^n$). De fato, g pode ser vista como a composição de $h : \mathbb{R}^n \to C$ com $f^{-1} : C \to \mathcal{I}$.

Definição 2. *A probabilidade de erro* λ_i *no envio de uma mensagem é definida como a probabilidade de que a regra de decodificação* g *devolva uma mensagem diferente de* i, *dado que* $\boldsymbol{x}(i)$ *foi enviado através do canal, isto é:*

$$\lambda_i = P(g(\boldsymbol{Y}) \neq i | \boldsymbol{X} = \boldsymbol{x}(i))$$

A probabilidade máxima de erro λ^n *de um código* (M, n) *é definida como*

$$\lambda^{(n)} = \max_{i \in \mathcal{I}} \lambda_i.$$

Definição 3. *A taxa (binária)* R *de um código* (M, n) *é definida como*

$$R = \frac{\log M}{n} \quad \text{bits/uso do canal.}$$

Uma taxa R *é dita atingível pelo canal Gaussiano se existir uma família de códigos com parâmetros* (M_n, n) *tal que* $\log M_n / n \to R$ *e* $\lambda^{(n)} \to 0$ *quando* $n \to \infty$.

Definição 4. *A capacidade do canal Gaussiano é o supremo de todas as taxas atingíveis, tomado sobre todas as possiveis escolhas de código.*

Shannon demonstrou que a capacidade do canal Gaussiano possui um valor bem determinado, dado pelo teorema a seguir, cuja demonstração pode ser encontrada em [1].

Teorema 3. *A capacidade C do canal Gaussiano com restrição de potência P e variância do ruído σ^2 é dada por*

$$C = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right) \text{ bits / uso do canal.} \tag{1}$$

Um fato interessante sobre a demonstração do teorema acima é o de que ele utiliza um argumento conhecido como codificação aleatória. Para o canal Gaussiano, as componentes das palavras-código são escolhidas *aleatoriamente* com distribuição normal com média 0 e variância $P - \varepsilon$. Isso nos diz que códigos aleatórios atingem a capacidade do canal Gaussiano, entretanto são completamente desestruturados e em geral não possuem uma regra de decodificação eficiente. A pergunta natural é, portanto, se códigos mais estruturados podem também atingir a capacidade no canal Gaussiano.

3.2 Plausibilidade

Apresentamos a seguir um argumento de empacotamento de esferas que nos dá uma intuição sobre a capacidade do canal Gaussiano. Seja um código C e $\boldsymbol{x} \in C$ uma palavra-código e seja $\boldsymbol{y}$ um vetor recebido. Escolhemos a regra decodificação h que assinala:

$$h(\boldsymbol{y}) = \boldsymbol{x}, \text{ se } \boldsymbol{y} \in B(\boldsymbol{x}, \sqrt{n(\sigma^2 + \varepsilon)})$$

e declara "erro" caso $\boldsymbol{y}$ não esteja contido em nenhuma das bolas centradas em palavras-código com este raio. Pela Lei dos Grandes números, dado um vetor enviado $\boldsymbol{x}$, o vetor recebido $\boldsymbol{y}$ está contido em uma esfera centrada em $\boldsymbol{x}$ de raio $\sqrt{n(\sigma^2 + \varepsilon)}$ com alta probabilidade e desta maneira, com alta probabilidade decodificaremos qualquer vetor recebido para a palavra-código correta.

Entretanto, por restrições de potência, os vetores recebidos $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}$ estão contidos, com alta probabilidade, em $B(0, \sqrt{n(P + \sigma^2 + \varepsilon)})$. Assim, o número de palavras M do código tem que satisfazer

$$M \leq \frac{\operatorname{vol}(B(0, \sqrt{n(P + \sigma^2 + \varepsilon)}))}{\operatorname{vol}(B(0, \sqrt{n(\sigma^2 + \varepsilon)}))} \approx \left(\sqrt{\frac{P + \sigma^2}{\sigma^2}}\right)^n \text{ ou seja,}$$

$$R \leq \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right).$$

Este argumento nos diz que não podemos esperar codificar a uma taxa melhor do que C. O que o Teorema de Shannon afirma é que de fato podemos codificar arbitrariamente próximo desta taxa e, a qualquer taxa acima desta, a probabilidade de erro do código está necessariamente afastada de 0.

4 Códigos reticulados e probabilidade de erro

Seja Λ um reticulado e S um subconjunto limitado do $\mathbb{R}^n$. Um *código reticulado* $C_{\Lambda,S}$ é definido como a intersecção de Λ com S, ou seja $C_{\Lambda,S} = \Lambda \cap S$. O conjunto S é normalmente chamado de região de *shaping* do código. Regiões comumente utilizadas incluem esferas euclidianas, caixas, ou mesmo regiões de Voronoi de um sub-reticulado.

Com relação aos códigos reticulados, uma estratégia comum de decodificação que beneficia-se da estrutura de retiulados é conhecida como *lattice decoding*. Essencialmente, ela decodifica um vetor recebido $\boldsymbol{y}$ como o ponto de Λ mais próximo de $\boldsymbol{x}$, isto é:

$$h(\boldsymbol{y}) = \boldsymbol{x} \text{ se } \boldsymbol{y} \in \operatorname{Vor}(\boldsymbol{x}),$$

com empates resolvidos arbitrarmente. Utilizando esta estratégia, podemos estimar a probabilidade de erro na utilização de códigos reticulados para a transmissão de informação através de um canal Gaussiano. Seja $C_{\Lambda,S} = \{\boldsymbol{c_1}, \ldots, \boldsymbol{c_M}\}$ um código reticulado. Temos:

$$\lambda_i = P(\boldsymbol{c_i} + \boldsymbol{z} \notin \mathrm{Vor}(\boldsymbol{c_i}) \mid \boldsymbol{c_i} \text{ enviado}) = P(\boldsymbol{z} \notin \mathrm{Vor}(\boldsymbol{0}) \mid \boldsymbol{c_i} \text{ enviado}) = P(\boldsymbol{z} \notin \mathrm{Vor}(\boldsymbol{0})),$$

ou seja, a probabilidade não depende do ponto enviado. A última expressão pode ser desenvolvida como:

$$P(\boldsymbol{z} \notin \mathrm{Vor}(\boldsymbol{0})) = 1 - P(\boldsymbol{z} \in \mathrm{Vor}(\boldsymbol{0})) = 1 - \frac{1}{(\sqrt{2\pi\sigma^2})^n} \int_{\mathrm{Vor}(\boldsymbol{0})} e^{\frac{-\|\boldsymbol{x}\|^2}{2\sigma^2}} d\boldsymbol{x}$$

Podemos, além disso, podemos limitar λ_i da seguinte forma. Suponhamos que o vetor $\boldsymbol{c_i}$ tenha sido enviado e que os seus vizinhos mais próximos em Λ são $\boldsymbol{c_{i1}}, \ldots, \boldsymbol{c_{ir}}$ e definimos $\boldsymbol{v_{ik}} = \boldsymbol{c_i} - \boldsymbol{c_{ik}}$ e $\rho_k = 1/2 \, \|\boldsymbol{v_{ik}}\|$. Temos então que um erro de decodificação ocorre se a projeção do vetor-erro $\boldsymbol{z}$ em algum $\boldsymbol{v_{ik}}$ satisfaz

$$\frac{\langle \boldsymbol{z}, \boldsymbol{v_{ik}} \rangle}{\|\boldsymbol{v_{ik}}\|} > \rho_k.$$

Assim, temos

$$\begin{aligned} \lambda_i = P\left(\bigcup \left\{ \frac{\langle \boldsymbol{z}, \boldsymbol{v_{ik}} \rangle}{\|\boldsymbol{v_{ik}}\|} > \rho_k \right\}\right) &\leq \sum_{k=1}^{r} \frac{1}{\sqrt{2\pi\sigma^2}} \int_{\rho_k}^{+\infty} e^{-x^2/2\sigma^2} dx \\ &\leq r \frac{1}{\sqrt{2\pi\sigma^2}} \int_{\overline{\rho_i}}^{+\infty} e^{-x^2/2\sigma^2} dx, \end{aligned} \tag{2}$$

onde $\overline{\rho}_i = \min_k \rho_{ik}$. Deste modo, dada uma potência P, se quisermos operar a uma taxa R no canal Gaussiano e transmitir os pontos de um reticulado Λ sujeitos a esta restrição, necessitamos que o número de palavras código M satisfaça $M \approx 2^{nR}$. Entretanto, pelo Teorema 2 temos:

$$2^{nR} \approx \#S(\sqrt{nP}) \approx \frac{\mathrm{vol}(B(0, \sqrt{nP}))}{\det \Lambda} \implies \det \Lambda \approx \mathrm{vol}(B(0,1)) \frac{(\sqrt{nP})^n}{2^{nR}},$$

ou seja, ou volume de Λ está fixado. Por outro lado, para minimizar a Equação (2), temos que maximizar ρ_i (ou maximizar o raio de empacotamento do reticulado). Assim, fixado um volume para Λ, queremos maximizar o seu raio de empacotamento e portanto, maximizar a sua densidade, mostrando que o problema de transmissão de códigos reticulados através do canal Gaussiano está relacionado com o problema de encontrar o empacotamento mais denso. É importante notar que as aproximações feitas acima (e por conseguinte a relação com o problema de empacotamento) tornam-se fieis quando aumentamos o número de pontos $M \to \infty$ ou a relação sinal-ruído $SNR = P/\sigma^2 \to \infty$.

5 Referências complementares

Em 1997, Loeliger [3] demonstrou que é possível atingir taxas de $1/2 \log(P/\sigma^2)$ utilizando códigos reticulados (sem utilizar, entretanto, a estratégia de *lattice decoding*) através de argumentos similares ao limitante de Minkowski-Hlawka. Em 1998, Urbanke e Rimoldi [6] mostraram diretamente que taxas de $1/2 \log(1 + P/\sigma^2)$ são atingíveis utilizando códigos reticulados. Novamente, o decodificador utilizado não se beneficiava da estrutura de reticulados. O problema de quais taxas são atingíveis com a estratégia de *lattice decoding* foi resolvido por Erez e Zamir em [2], que mostraram que de fato é possível atingir $1/2 \log(1 + P/\sigma^2)$ utilizando *lattice decoding*. A questao de obtenção de códigos reticulados mais estruturados (ou explícitos) que atinjam uma fração da capacidade encontra-se ainda em aberto.

Referências

[1] T. Cover and J. Thomas. *Elements of Information Theory.* Wiley Series in Telecommunications and Signal Processing, 2nd edition, 2006.

[2] U. Erez and R. Zamir. Achieving 1/2 log (1+SNR) on the AWGN channel with lattice encoding and decoding. *IEEE Transactions on Information Theory*, 50(10):2293 – 2314, 2004.

[3] H.-A. Loeliger. Averaging bounds for lattices and linear codes. *IEEE Transactions on Information Theory,*, 43(6):1767 –1773, 1997.

[4] S. Ross. *A first course in probability.* Pearson, 8th edition, 2009.

[5] C. E. Shannon. A Mathematical Theory of Communication. *The Bell system technical journal*, 27:379–423, 1948.

[6] R. Urbanke and B. Rimoldi. Lattice codes can achieve capacity on the AWGN channel. *IEEE Transactions on Information Theory*, 44(1):273 –278, 1998.