Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Quantização de canal via códigos reticulados provenientes de corpos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$

Edson Donizete de Carvalho[1]

Departamento de Matemática, Unesp, Ilha Solteira, SP

Azucena M. Duarte Zelaya[2]

Programa de Pós-Graduação em Engenharia Elétrica, PUC-Rio, Rio de Janeiro, RJ

Jozué Vieira Filho[3]

Curso de Engenharia de Telecomunicações, Unesp, S.J.da Boa Vista, SP

Resumo. Por meio da teoria algébrica dos números propomos um eficiente método baseado na estratégica compute-and-forward para quantização de coeficientes de um canal associado a problemas de codificação em redes. O desenvolvimento desta técnica é realizado via partição de cadeias de códigos reticulados definidos sobre o anel de inteiros Eisentein-Jacobi, obtidos a partir de corpos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$ com $s \geq 2$, onde $\zeta_{9.2^s}$ denota raiz 9.2^s-ésima da unidade.

Palavras-chave. Anéis de Inteiros, Códigos Reticulados, Corpos de Números, Quantização de Canal, Técnica Compute and Forward.

1 Introdução

Um típico problema de transmissão de informação em uma rede sem fio é de que qualquer receptor não somente captura o sinal a partir de seu transmissor designado, mas também a partir de todos os outros transmissores próximos tal comportamento é conhecido por interferência. A interferência sempre foi vista como um obstáculo na comunicação em redes sem fio, diversos algorítmos e protocolos foram desenvolvidos para contornar problemas desta natureza.

Recentemente foi proposta uma nova técnica denominada de *compute-and-forward* [5] que tira proveito da interferência para obter altas taxas entre os transmissores de uma rede.

Cada relé, indexado por $m = 1, 2, \ldots, M$, observa as combinações ruídosas dos sinais transmitidos através do canal dadas por:

[1]edson@mat.feis.unesp.br
[2]azucenaduarte23@gmail.com
[3]jozue@sjbv.unesp.br

$$y_m = \sum_{l=1}^{L} h_{ml} x_l + z_m, \tag{1}$$

onde y_m denota o sinal recebido, x_m denota o sinal trasmitido, h_{ml} denota o canal e z_m o ruído no canal.

Esta técnica permite que os relés decodifiquem equações lineares das mensagens transmitidas por meio de combinações lineares ruídosas que são fornecidas pelo canal. Após os relés decodificam estas equações lineares, eles enviam estas mesmas aos destinos, os quais para um dado número suficiente de equações lineares é capaz de recuperar as mensagens transmitidas através da quantização dos coeficientes do canal.

2 Descrição Matemática do Problema

Tunali [5] provou a existência de cadeias de partições infinitas de códigos reticulados aninhados que são simultâneamente bons para problemas de codificação de canal e de quantização. Códigos reticulados aninhados são obtidos via a a *Construção A*, uma técnica que permite obter reticulados através do mergulho de um código linear definido sobre um corpo finito $\mathbb{F}_p$ em $\mathbb{R}^N$ ou em $\mathbb{C}^N$.

Em [5], os autores mostraram a existência de uma cadeia infinita de códigos reticulados aninhados sobre $\mathbb{Z}[\omega]$ (o anel de inteiros de Eisentein-Jacobi), garantindo que a técnica compute and forward possa ser aplicada.

O que permite que a analise possa ser realizada via um canal equivalente ao anterior induzido pela transformação módulo Λ. Neste novo modelo de canal "virtual"cada relé analise os pontos reticulados dados por combinações sobre $\mathbb{Z}[\omega]$ como sendo $\sum a_{ml} t_l$ sob a ação de um ruído efetivo $z_{eq,m}$, isto é,

$$y_m = \sum_{l=1}^{L} a_{ml} t_l + z_{eq,m}. \tag{2}$$

Supomos que ao aplicarmos a transformação unitária U recebemos o vetor (2). Assim, teremos

$$\bar{y}_m = U y_m = \sum_{l=1}^{L} a_{ml} U t_l + U z_{eq,m}, \tag{3}$$

onde $z_{eq,m}$ é um ruído Gaussiano que é circular complexo dado por (3). Agora, analisaremos os vetores da forma $a_{ml} U t_l$. Por simplicidade de notação, escreveremos da forma

$$\bar{x} = h \cdot U \cdot x, \tag{4}$$

DOI: 10.5540/03.2016.004.01.0105

onde $x = t_l$ é o ponto reticulado transmitido pelo considerado usuário e $h = a_{ml}$ é o coeficiente do canal. Podemos reescrever da maneira

$$\begin{pmatrix} h & 0 & \cdots & 0 \\ 0 & h & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h \end{pmatrix} \cdot U \cdot x = H \cdot U \cdot x. \tag{5}$$

Nossa meta é a de quantizar a matrix diagonal H por uma outra matriz diagonal. Faremos a abordagem matricial deste problema via códigos reticulados e as matrizes diagonais que usaremos na quantização será obtido como conseguência do procedimento algébrico que na qual mostraremos que cada matriz geradora M_k associado a cada código reticulado da cadeia infinita de partição de códigos reticulados é expressa na forma $M_k = B^k M$, onde M é uma matriz geradora de um reticulado da partição e cada B^k é matriz diagonal.

3 Formulação e Solução Matemática do Problema

A formulação e resolução do problema em questão será baseado na teoria algébrica dos números.

Neste sentido, consideremos uma cadeias de corpos ciclotômicos dados por $\mathbb{Q} \subset L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_s$, satisfazendo a condição de que $L_0 = \mathbb{Q}(\omega), L_1 = L_0(\zeta_{9.2})$ e para todo $s \geq 2$ temos $L_s = \mathbb{Q}(\zeta_{9.2^s})$, onde $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ denotam as raízes terceira 9.2^s-ésima da unidade, respectivamente.

A cadeia acima também pode ser denotada por $L_s/L_{s-1}/\cdots/L_2/L_1$. Cada corpo L_s pode ser visto como um espaço vetorial sobre $\mathbb{Q}$ ou sobre corpo ciclotômico L_{s-1}.

Diremos que L_s/L_{s-1} é uma extensão finita de corpos se L_s visto como espaço vetorial sobre L_s tem dimensão finita. Associado a cada extensão finita de corpos L_s/L_{s-1}, temos como consequência do fato de que $\zeta^2_{9.2^s} = \zeta_{9.2^{s-1}}$ e $L_s = L_{s-1}(\zeta_{9.2^s})$ as sequintes relações:

1. $\{1, \zeta_{9.2^s}\}$ é uma base de L_s sobre L_{s-1} tendo $\zeta_{9.2^s}$ como raiz do polinômio minimal $p_s(x) = (x - \zeta_{9.2^s})(x + \zeta_{9.2^s})$ e com o grupo de Galois associado a extensão dado por $Gal(L_s/L_{s-1}) = \{id, \sigma_s\}$ onde σ_s denota as permutações das raízes do polinômio minimal p_s.

2. $\{1, \zeta_{9.2^s}, \ldots, \zeta^{N-1}_{9.2^s}\}$ é uma base de L_s sobre K tendo $\zeta_{9.2^s}$ como raiz do polinômio minimal $\mu_{\zeta_{9.2^s}}(x) = \prod_{k=0}^{N-1}(x - \zeta^k_{9.2^s})$. As raízes de $\mu_{\zeta_{9.2^s}}(x)$ e com o grupo de Galois associado a extensão de corpos L/K é dado por $Gal(\mathbb{L}/F) = \{\sigma_j : \sigma_j(\zeta_{9.2^s}) = \zeta^j_{9.2^s}, \forall j = 0, 1, \ldots, N-1\}$, onde $N = 3.2^{s-1}$ se $K = \mathbb{Q}$ e $N = 3.2^{s-2}$ se $K = \mathbb{Q}(\omega)$.

3. O conjunto dos elementos de L obtido como um módulo sobre $\mathbb{Z}$ gerado pela base $\{1, \zeta_{9.2^s}, \zeta^2_{9.2^s}, \cdots, \zeta^{2^{s-1}}_{9.2^s}\}$ é chamado de anel de inteiros de L denotado por $\mathcal{O}_L$ ou $\mathbb{Z}[\zeta_{9.2^s}]$. Convém, desde que $\mathcal{O}_L$ também pode ser visto como um módulo sobre $\mathbb{Z}[\omega]$ gerado pela base $\{1, \zeta_{9.2^s}, \zeta^2_{9.2^s}, \cdots, \zeta^{2^{s-2}}_{9.2^s}\}$.

A partir de uma extensão finita de corpos L/K de grau t, podemos definir o traço e a norma relativa de um elemento $\alpha \in \mathcal{O}_L$ como sendo os inteiros algébricos $Tr_{L/K}(\alpha) =$

$\sum_{i=0}^{t-1}\sigma_i(\alpha)$ and $N_{L/K}(\alpha)=\prod_{i=0}^{t-1}\sigma_i(\alpha)$, respectivamente. Observe que $Tr_{L/K}(\alpha)$ e $N_{L/K}(\alpha)$ pertence a $\mathcal{O}_K$. Caso $L/K/\mathbb{Q}$ seja uma cadeia de extensões finitas de corpos, então para cada elemento $\alpha\in L$ vale $N_{L/\mathbb{Q}}(\alpha)=N_{K/\mathbb{Q}}(N_{L/K}(\alpha))$.

Se $\alpha,\beta\in L$, então $N_{L/\mathbb{Q}}(\alpha\beta)=N_{L/\mathbb{Q}}(\alpha)N_{L/\mathbb{Q}}(\beta)$.

Exemplo 3.1. *1. Seja $\alpha=1-\omega\in\mathbb{Q}(\omega)$ então $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1-\omega)=id(1-\omega)\sigma(1-\omega)=1-\omega^2=3$, onde $\sigma^2=id$ e $Gal(\mathbb{Q}(\omega)/\mathbb{Q})=\langle\sigma\rangle=\{id,\sigma\}$.*

2. Seja $\alpha=1-\zeta_{9.2^s}\in\mathbb{Z}[\zeta_{9.2^s}]$, então, temos que $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1-\zeta_{9.2^s})=id(1-\zeta_{9.2^s})\sigma_r(1-\zeta_{9.2^s})=(1-\zeta_{9.2^s})(1+\zeta_{9.2^s})=1-\zeta_{9.2^s}^2=1-\zeta_{9.2^{s-1}}$.

Os trabalhos [3] e [4] mostraram maneiras de se obter reticulados algébricos Λ isomorfos a reticulados $\mathbb{Z}[\omega]^N$ via famílias de corpos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$.

A partir de um ideal $\Im\subseteq\mathcal{O}_L$, podemos obter um reticulado algébrico complexo Λ como consequência dos mergulhos complexos de L em $\mathbb{C}^N$ definido da seguinte maneira

$$\sigma: L\Rightarrow\mathbb{C}^N,\ \text{with}\ \sigma(x)=(\sigma_0(x),\cdots,\sigma_{N-1}(x)),\tag{6}$$

onde $\sigma_i\in Gal(L/\mathbb{Q}(\omega))$, $\forall i\in\{0,\ldots,N-1\}$.

Seja $\{w_0,\cdots,w_{N-1}\}$ a base integral de $\mathcal{O}_L$ sobre $\mathbb{Z}[\omega]$, isto é,

No caso particular em que o ideal $\Im=\mathcal{O}_L$, obtemos o reticulado complexo associado dado por

$$\Lambda=\{x=\lambda M|\lambda\in\mathbb{Z}[\omega]^N\},$$

onde M chamada de matriz geradora do reticulado algébrica Λ e é dada por:

$$M=\begin{pmatrix}\sigma_0(w_0) & \cdots & \sigma_{N-1}(w_0)\\ \vdots & \ddots & \vdots\\ \sigma_0(w_{N-1}) & \cdots & \sigma_{N-1}(w_{N-1})\end{pmatrix}.\tag{7}$$

Por outro lado, há uma outra matriz associado a um reticulado algébrico que chamamos de matriz Gram e dada por $G=M.\overline{M}^t$, onde $\overline{M}^t$ denota a matriz transposta conjugada da matriz M.

O próximo Proposição 3.1 estabelece a conexão entre reticulados algébricos obtidos a partir de um anel de inteiros $\mathbb{Z}[\zeta_{9.2^s}]$ e reticulados escalonados da forma $\mathbb{Z}[\omega]^N$.

Proposição 3.1. *[3] A matriz geradora $M_0=(\frac{1}{\sqrt{N}})M$ do reticulado algébrico associado a $\mathbb{Z}[\zeta_{9.2^s}]$ é unitária e a matriz Gram $G=M_0\overline{M_0}^t=Id$, onde $N=3.2^{s-2}$.*

3.1 Construção de cadeia de reticulados aninhados

Dizemos que uma cadeia de reticulados $\Lambda_{n-1},\cdots,\Lambda_1$ está aninhado no reticulado Λ se $\Lambda_{n-1}\subseteq\Lambda_{n-2}\subseteq\cdots\subseteq\Lambda_1\subset\Lambda$. Faremos uso da teoria algébrica dos números para construir explicitamente cadeias de reticulados aninhados.

DOI: 10.5540/03.2016.004.01.0105

Caso os reticulados desta cadeia de reticulados sejam códigos reticulados, então denominamos de cadeia de códigos reticulados aninhados. Uma importante classe de códigos reticulados podem serem obtidos a partir de $\mathbb{Z}[\omega]^N$. Para isto basta que consideremos o código $\mathcal{C}$ como sendo o conjunto de todos as N-uplas de $\mathbb{Z}[\omega]^N$ congruente modulo $\phi = 1 - \omega$. Neste caso caso, obtemos $\mathcal{C} \simeq \mathbb{Z}[\omega]^N/\phi\mathbb{Z}[\omega]^N$.

Note que a partir do reticulado complexo $\mathbb{Z}[\omega]^N$ podemos uma cadeia de partição infinita de subreticulados na forma $\mathbb{Z}[\omega]^N/\phi\mathbb{Z}[\omega]^N/\phi^2\mathbb{Z}[\omega]^N/\cdots$

Forney [2] mostrou que podemos expressar $\phi^k\mathbb{Z}[\omega]^N$ por meio de uma fórmula código complexa

$$\phi^k\mathbb{Z}[\omega]^N = \phi^{k-1}\mathbb{Z}[\omega]^N + \phi^{k-2}\mathcal{C}_{k-1} + \cdots \mathcal{C}_0, \tag{8}$$

e que estes reticulados complexos $\phi^k\mathbb{Z}[\omega]^N$ são identificados por códigos lineares sobre o corpo finito $\mathbb{F}_3$ e que podem serem vistos como um ideal primo no anel fatorial $\mathbb{F}_3[x]/(x^N - 1) \simeq \mathbb{F}_3^N$

O que garante que os códigos reticulados aninhados podem serem caracterizados na forma $\phi^k\mathbb{Z}[\omega]^N$.

Consideremos uma cadeia de ideais em $\mathbb{Z}[\zeta_{9.2^s}]$ rotulados por rotulados por $\Im^k = (\alpha)^k\mathbb{Z}[\zeta_{9.2^s}]$, onde $\alpha = (1 - \zeta_{9.2^s})$.

Desde que $\{w_0, \ldots, w_{N-1}\}$ é uma base integral do anel de inteiros $\mathbb{Z}[\zeta_{9.2^s}]$ sobre $\mathbb{Z}[\omega]$. Da teoria de reticulados algébricos, temos que $\{\alpha^k w_0, \ldots, \alpha^k w_{N-1}\}$ é uma base integral de ideal $\Im^k\mathbb{Z}[\zeta_{9.2^s}]$ visto como um módulo sobre $\mathbb{Z}[\omega]$, onde $w_i = \zeta_{9.2^s}^i \;\; i \in \{0, 1, \ldots, N-1\}$.

No caso particular em que $k = 0$, obtemos ideal trivial $\Im^0 = \mathbb{Z}[\zeta_{9.2^s}]$. Para este caso a matriz geradora M_0 do reticulado algébrico Λ_0 descrita pela Proposição 3.1. A próxima Observação 3.1 que é baseada nos resultados de [3] e [4] que estabelecem uma importante conexão entre reticulados algébricos Λ_k associados aos ideais $\Im^k$ e a matrizes geradoras de reticulados obtidos via a forma traço.

Observação 3.1. *A matriz Gram $G = M_k\overline{M_k}^t$ concide a matriz $T_{L/\mathbb{Q}(\omega)}(\alpha w_j\overline{\alpha w_j})_{j=0}^{N-1}$ para reticulados ideais, isto é reticulados obtidos a através de ideais gerados por α via forma fórmula traço a partir de famílias de corpos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$.*

Assim, matriz Gram do reticulado Λ_k é escrita na forma $G_k = M.B^k\overline{M}\overline{B^k}$, onde $B^k = diag(\alpha^k, \sigma(\alpha^k), \ldots, \sigma^{N-1}(\alpha^k))$.

A notação $\overline{a}$ denota o conjugado transposta de um elemento $a = a_1 + a_2\omega \in \mathbb{Z}[\omega]$ dada por $\overline{a} = a_1 + a_2\omega^2$. No sentido de fornecermos uma caracterização algébrica explicita dos reticulados obtidos por meio da cadeia de ideais $\Im^k = (\alpha^k)\mathbb{Z}[\zeta_{9.2^s}]$ é que consideraremos a Proposição 3.2.

Proposição 3.2. *A norma relativa $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}$ aplicada sobre o elemento $1 - \zeta_{9.2^s}$ é dada por $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(1 - \zeta_{9.2^s}) = 1 - \omega, \forall s > 2$.*

Demonstração.

1. para $s = 0$, segue-se que $N_{\mathbb{Q}(\zeta_9)/\mathbb{Q}(\omega)}(1-\zeta_9) = id(1-\zeta_9)\sigma_3(1-\zeta_9) = (1-\zeta_9)(1+\zeta_9) = 1-\zeta_9^2 = 1-\omega$.

2. Assumiremos por indução sobre $s-1$ que $N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}(\omega)}(1 - \zeta_{9.2^{s-1}}) = 1 - \omega$.

Pelo item (2) do Exemplo 3.1, temos que $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1-\zeta_{9.2^s}) = 1-\zeta_{9.2^{s-1}}$.

Pela propriedade de norma relativa em uma extensão finita de corpos, temos que $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(1-\zeta_{9.2^s}) = N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}(\omega)}(N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1-\zeta_{9.2^s}))$.

Portanto,concluímos que $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(1-\zeta_{9.2^s}) = 1-\omega$.

□

Proposição 3.3. *Seja $\alpha = 1-\zeta_{9.2^s}$. Para cada reticulado ideal Λ_k in $\mathbb{C}^N$ associado a um ideal $\Im^k = (\alpha)^k\mathbb{Z}[\zeta_{9.2^s}]$ é isomorfo a um código reticulado $(1-\omega)^k\mathbb{Z}[\omega]^N$ para todo inteiro $k \geq 1$.*

Demonstração. Analisaremos primeiro a matriz Gram matrix $G = M_k\overline{M_k}^t$ associada ao reticulado ideal Λ_k. Temos que a matriz M_k pode ser escrita na forma

$M_k = \sigma_\alpha(\zeta_{9.2^s}^j)_{j=0}^{N-1}.diag(\alpha^k,\ldots,\sigma_k(\alpha^k))$ e $\overline{M_k}^t = \overline{\sigma(w_j))}_{j=0}^{N-1}.diag(\overline{\alpha^k},\ldots,\overline{\sigma_k(\alpha^k)})$

Usando de forma conveniente as propriedades da transposta conjugada do produto de matrizes, podemos expressar a matriz Gram por:

$$G = (\sigma_\alpha(\zeta_{9.2^s}^j)_{j=0}^{N-1}).(\overline{\sigma_\alpha(\zeta_{9.2^s}^j)})_{j=0}^{N-1})^t \prod_{i=0}^{N-1}\sigma_i(\alpha^k)\prod_{i=0}^{N-1}\overline{\sigma_i(\alpha^k)}.$$

No entanto, temos que $M_0 = (\sigma_\alpha(\zeta_{9.2^s}^j)_{j=0}^{N-1})$ e $\prod_{i=0}^{N-1}\sigma_i(\alpha) = N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(\alpha^k)$.

Pelo Exemplo 3.2, temos $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(\alpha) = 1-\omega$.

Assim, obtemos $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(\alpha)^k = (1-\omega)^k$.

O que nos permite reescrever G na forma

$$G = (1-\omega)^k M_0(\overline{(1-\omega)})^k M_0\overline{M_0}^t = M_0\overline{M_0}^t = (1-\omega)^k M_0\overline{(1-\omega)^k M_0} \tag{9}$$

Desde que M_0 é a matriz geradora do código reticulado $\mathbb{Z}[\omega]^N$, podemos concluir que $(1-\omega)^k M_0$ denota a matriz geradora do código reticulado $(1-\omega)^k\mathbb{Z}[\omega]^N$.

□

Um fato bem conhecido é que a partir da sequência de ideais $\Im^k\mathbb{Z}[\zeta_{9.2^s}]$ em $\mathbb{Z}[\zeta_{9.2^s}]$, podemos obter uma outra sequência de ideais $\Im^{-k}\mathbb{Z}[\zeta_{9.2^s}]$ inversos de $\Im^k\mathbb{Z}[\zeta_{9.2^s}]$ em $\mathbb{Z}[\zeta_{9.2^s}]$. Estes ideais são definidos por $\Im^{-k} = \{x \in \mathbb{Q}(\zeta_{9.2^s}) \mid x\Im^k \subseteq \mathbb{Z}[\zeta_{9.2^s}]\}$ e também satisfazem a relação de que $\mathcal{O}_L = \Im^k\Im^{-k}$.

logo, obtemos a próxima Proposição.

Proposition 3.1. *Seja $\alpha = 1-\zeta_{9.2^s}$. Então para cada reticulado ideal Λ_{-k} em $\mathbb{C}^N$ associado a um ideal $\Im^{-k} = (\alpha)^{-k}\mathbb{Z}[\zeta_{9.2^s}]$ é isomorfo a um código reticulado $\frac{1}{(1-\omega)^k}\mathbb{Z}[\omega]^N$ para todo inteiro negativo $k \leq 1$.*

Demonstração. A demonstração é análoga é realizada na Proposição 3.3. A única diferença é de que neste caso ao desenvolver a matriz Gramm do reticulado Λ_{-k}, obtemos

$$G = (\sigma_\alpha(\zeta_{9.2^s}^j)_{j=0}^{N-1}).(\overline{\sigma_\alpha(\zeta_{9.2^s}^j)})_{j=0}^{N-1})^t \prod_{i=0}^{N-1}\sigma_i(\alpha)^{-k}\prod_{i=0}^{N-1}\overline{\sigma_i(\alpha)^{-k}}.$$

DOI: 10.5540/03.2016.004.01.0105

Utilizando o fato de que $\prod_{i=0}^{N-1} \sigma_i(\alpha)^{-k} = (\prod_{i=0}^{N-1} \sigma_i(\alpha)^k)^{-1} = (N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(\alpha)^k)^{-1}$, obtem-se o desejado.

□

4 Resultados

A partir da cadeis de ideais $\Im^k = (\alpha^k)\mathbb{Z}[\zeta_{9.2^s}]$ para $\alpha = 1 - \zeta_{9.2^s}$ e k inteiro, obtemos uma cadeia infinita de reticulados complexas $\ldots/\Lambda_{-t}\ldots/\Lambda_{-1}\Lambda_0/\Lambda_1/\ldots,\Lambda_t\ldots$ que corresponde a uma cadeia infinita de códigos reticulados $\ldots/(1-\omega)^{-k}\mathbb{Z}[\omega]^N/\ldots/(1-\omega)^{-1}\mathbb{Z}[\omega]^N/\mathbb{Z}[\omega]^N/(1-\omega)\mathbb{Z}[\omega]^N/\ldots/(1-\omega)^k\mathbb{Z}[\omega]^N/\ldots$, onde cada reticulado complexo Λ_k é isomorfo a um código reticulado $(1-\omega)^k\mathbb{Z}[\omega]^N$.

5 Conclusões

Propomos uma novo método para aproximar os coeficientes de um canal a partir de cadeias de particões infinitas de códigos reticulados sobre $\mathbb{Z}[\omega]$.

Agradecimentos

Os autores agradecem a Fapesp pelo apoio financeiro, Processo Fapesp 2013/25977-7.

Referências

[1] J.H. Conway and N.J.A. Sloane; *Sphere packings, lattices and groups*, Springer-Verlag, New York, 1988.

[2] G. D. Forney; *Coset Codes - Part I: Introduction and geometrical classification*, IEEE Trans. Inform. Theory, 34, 1123-1151, 1988.

[3] X. Giraud; E. Boutilon and J. C. Belfiore, *Algebraic tools to built modulation schemes for fading channels*, IEEE Trans. Inform. Theory, **43**(3), (1997) 938-952.

[4] F. Oggier; *Algebraic methods for channel coding*, Phd dissertation École Polytechnique Fédérale de Lausanne, Lausanne, 2005.

[5] N. E. Tunali; K. R. Narayanan; J. J. Boutros and Y.C. Huang, *Lattices over Eisentein integer for compute-and-forward*, Fiftieth Annual Conference Allerton House, UIUC, Illinois, USA, October 1-5, 2012, pp. 33-40.

