XXXI Simpósio Brasileiro de Telecomunicações

Canais Matriciais Multiplicativos sobre Anéis de Cadeia Finitos

Roberto W. Nóbrega[1], Chen Feng[2], Danilo Silva[1], Bartolomeu F. Uchôa-Filho[1]

[1]Departmento de Engenharia Elétrica, Universidade Federal de Santa Catarina, Brasil
[2]Department of Electrical and Computer Engineering, University of Toronto, Canada

rwnobrega@eel.ufsc.br, cfeng@eecg.utoronto.ca, danilo@eel.ufsc.br, uchoa@eel.ufsc.br

SBrT

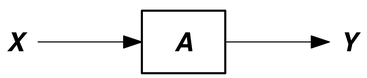
Sumário

► *O que são MMCs?*

Um ***canal matricial multiplicativo*** (***MMC***) sobre um anel R é um canal de comunicação no qual a entrada $\boldsymbol{X} \in R^{n\times\ell}$ e a saída $\boldsymbol{Y} \in R^{m\times\ell}$ são matrizes relacionadas pela expressão

$$\boldsymbol{Y} = \boldsymbol{A}\boldsymbol{X},$$

em que $\boldsymbol{A} \in R^{m\times n}$ é a ***matriz de transferência***.



► *Por que estudar MMCs?*

MMCs são modelos adequados para a comunicação fim-a-fim em redes de comunicação que empregam ***codificação de rede linear*** [1]. Nesse contexto,

- $\boldsymbol{X}$ é a matriz cujas linhas são os n pacotes transmitidos pelo nó fonte.
- $\boldsymbol{Y}$ é a matriz cujas linhas são os m pacotes recebidos pelo nó destino.
- $\boldsymbol{A}$ é uma matriz cujas entradas são determinadas pelos coeficientes (possivelmente aleatórios) das combinações lineares da codificação de rede.

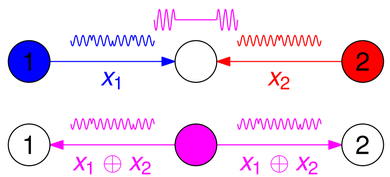
Tradicionalmente, R é um corpo finito e cada pacote é um elemento de R^ℓ.

Sumário [cont.]

► *Por que MMCs sobre anéis de cadeia?*

Em ***codificação de rede na camada física via reticulados aninhados***, mostra-se que [2]

- O anel R não é necessariamente um corpo finito, mas sim um ***anel de ideais principais*** (***PIR***) finito.
- Os pacotes são elementos de um ***R-módulo finito***, o qual não é necessariamente da forma R^ℓ.



Uma vez que todo PIR finito é um produto de ***anéis de cadeia finitos***, é natural considerar o estudo de *MMCs sobre anéis de cadeia finitos*.

► *Contribuições do trabalho*

Este trabalho adota um enfoque probabilístico, sob a ótica da teoria da informação. Como contribuições:

- Uma ***expressão fechada para a capacidade*** do canal é obtida.
- Um ***esquema prático de codificação*** que alcança a capacidade em complexidade de tempo polinomial é proposto.

Os resultados aqui apresentados estendem alguns daqueles em [3]. Um outro trabalho relacionado é [4].

Anéis de Cadeia Finitos

► *Definição*

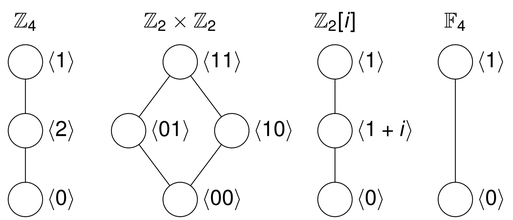
Um ***anel de cadeia*** é um anel no qual os ideias formam uma cadeia quando ordenados de acordo com inclusão de conjuntos ($\subseteq$).

Em particular, todo corpo é um anel de cadeia.

► *Notação*

R	um anel de cadeia finito
π	um gerador do ideal máximo de R
s	o número de ideais próprios de R
q	a ordem do corpo residual $R/\langle\pi\rangle$
Γ	um conjunto de representativos de $R/\langle\pi\rangle$

► *Exemplo: Anéis de ordem* 4



► *Expansão π-ádica*

Todo $x \in R$ pode ser escrito *unicamente* como

$$x = x^{(0)} + x^{(1)}\pi + x^{(2)}\pi^2 + \cdots + x^{(s-1)}\pi^{s-1},$$

em que $x^{(i)} \in \Gamma$, para $0 \le i < s$.

Álgebra Linear sobre Anéis de Cadeia

► *Definições*

Um ***s-shape*** é uma sequência

$$\mu = (\mu_0, \mu_1, \ldots, \mu_{s-1})$$

tal que $0 \le \mu_0 \le \mu_1 \le \cdots \le \mu_{s-1}$.

Define-se

$$R^\mu \triangleq \underbrace{\langle 1\rangle \times \cdots \times \langle 1\rangle}_{\mu_0} \times \underbrace{\langle \pi\rangle \times \cdots \times \langle \pi\rangle}_{\mu_1-\mu_0} \times \cdots \times \underbrace{\langle \pi^{s-1}\rangle \times \cdots \times \langle \pi^{s-1}\rangle}_{\mu_{s-1}-\mu_{s-2}},$$

o qual é um R-módulo.

► *Teorema de estrutura para R-módulos finitos*

Se M é um R-módulo finito, então

$$M \cong R^\mu$$

para algum s-shape μ *único*. Diz-se que μ é o ***shape*** de M e escreve-se $\mu = \text{shape}\, M$.

O shape de um R-módulo generaliza o conceito de dimensão de um espaço vetorial.

► *Shape de uma matriz*

O shape de uma matriz A é definido por

$$\text{shape}\, A = \text{shape}(\text{row}\, A) = \text{shape}(\text{col}\, A),$$

em que $\text{row}\, A$ e $\text{col}\, A$ são os espaços linha e coluna de A, respectivamente.

O shape de uma matriz generaliza o conceito de posto.

XXXI Simpósio Brasileiro de Telecomunicações

Canais Matriciais Multiplicativos sobre Anéis de Cadeia Finitos

Roberto W. Nóbrega[1], Chen Feng[2], Danilo Silva[1], Bartolomeu F. Uchôa-Filho[1]

[1]Departmento de Engenharia Elétrica, Universidade Federal de Santa Catarina, Brasil
[2]Department of Electrical and Computer Engineering, University of Toronto, Canada

rwnobrega@eel.ufsc.br, cfeng@eecg.utoronto.ca, danilo@eel.ufsc.br, uchoa@eel.ufsc.br

SBrT

Modelo do Canal

► ***Parâmetros do canal***

R	um anel de cadeia finito (parâmetros: s e q)
n	um inteiro (número de pacotes transmitidos)
m	um inteiro (número de pacotes recebidos)
$p_{\boldsymbol{A}}$	uma distribuição de probabilidade em $R^{m\times n}$
λ	um s-shape (shape do espaço de pacotes)

Observações:

- Se $R = \mathbb{F}_q$, então $\lambda = \ell$ é o comprimento do pacote.
- Cada pacote é um elemento de R^λ.
- O conjunto das matrizes com n linhas e cujas linhas pertencem a R^λ é denotado por $R^{n\times\lambda}$.

► ***Hipóteses***

- A cada uso do canal, $\boldsymbol{A}$ é ***i.i.d.*** de acordo com $p_{\boldsymbol{A}}$.
- As instâncias de $\boldsymbol{A}$ são desconhecidas do transmissor, mas disponíveis ao receptor, isto é, assume-se ***conhecimento do canal no receptor*** (***CSIR***).

► ***Definição do canal***

O MMC com CSIR é um ***canal discreto sem memória*** (***DMC***) com entrada $\boldsymbol{X}$ e saída $(\boldsymbol{Y}, \boldsymbol{A})$, de modo que

- Alfabeto de entrada: $\mathcal{X} = R^{n\times\lambda}$.
- Alfabeto de saída: $\mathcal{Y} = R^{m\times\lambda} \times R^{m\times n}$.
- Probabilidade de transição:

$$p_{\boldsymbol{Y},\boldsymbol{A}|\boldsymbol{X}}(Y, A|X) = \begin{cases} p_{\boldsymbol{A}}(A), & \text{se } Y = AX, \\ 0, & \text{caso contrário.} \end{cases}$$

Capacidade do Canal

► ***Resultado para corpos finitos***

Teorema [3]: A capacidade do MMC sobre um corpo finito $\mathbb{F}_q$, em símbolos q-ários por uso do canal, é

$$C = \mathrm{E}[\boldsymbol{r}]\ell,$$

em que $\boldsymbol{r} = \operatorname{rank} \boldsymbol{A}$ e ℓ é o comprimento do pacote. A capacidade é alcançada com entrada uniforme.

► ***Resultado para anéis de cadeia finitos***

Teorema: A capacidade do MMC sobre um anel de cadeia finito R, em símbolos q-ários por uso do canal, é

$$C = \sum_{i=0}^{s-1} \mathrm{E}[\boldsymbol{\rho}_{s-i-1}]\lambda_i,$$

em que $\boldsymbol{\rho} = \text{shape } \boldsymbol{A}$ e λ é o shape do espaço de pacotes. A capacidade é alcançada com entrada uniforme.

Esquema de Codificação

► ***Notação***

$F = R/\langle\pi\rangle$	corpo residual de R
$\varphi : R \to F$	projeção natural de R em F
$\bar{\varphi} : F \to \Gamma$	seletor de representativo

► ***Ideia básica do esquema***

O esquema adota uma ***abordagem em camadas***, combinando diversos códigos sobre o corpo residual (por exemplo, os de [3]) para obter um novo código sobre o anel de cadeia.

Esquema de Codificação [cont.]

► ***Construção do código***

Seja $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ uma sequência de códigos sobre o corpo residual, em que cada $\mathcal{C}_i \subseteq F^{n\times\lambda_i}$. Define-se

$$\mathcal{C} = \left\{ \sum_{i=0}^{s-1} X^{(i)}\pi^i : X_i \in \mathcal{C}_i, 0 \le i < s \right\},$$

em que $X^{(i)} = \begin{bmatrix} \bar{\varphi}(X_i) & 0 \end{bmatrix} \in \Gamma^{n\times\ell}$.

► ***Decodificação***

Via um ***algoritmo multi-estágio***:

Entrada: $(Y, A) \in R^{m\times\lambda} \times R^{m\times n}$, com shape $A \triangleq \rho$.

Saída: $X \in \mathcal{C}$ tal que $Y = AX$.

Passo 1: Calcule matrizes P, D, Q tais que $A = PDQ$, em que (i) D é a forma normal de Smith de A e (ii) P e Q são inversíveis.

Passo 2: Defina as matrizes $\tilde{X} \triangleq QX$ (desconhecida) e $\tilde{Y} \triangleq P^{-1}Y$ (conhecida), de modo que

$$Y = AX \iff \tilde{Y} = D\tilde{X}.$$

Daí, calcule $\tilde{X}^{(0)}_{\rho_{s-1}\times\lambda_0}, \tilde{X}^{(1)}_{\rho_{s-2}\times\lambda_1}, \ldots, \tilde{X}^{(s-1)}_{\rho_1\times\lambda_{s-1}}$.

Passo 3: Baseado em $\tilde{X} = QX$, pode-se mostrar que

$$Y_i = A_i X_i,$$

para $0 \le i < s$, em que $Y_i \in F^{m\times\lambda_i}$ e $A_i \in F^{m\times n}$ são calculadas em função de dados conhecidos (veja artigo). Daí, decodifique sucessivamente $X_0, X_1, \ldots, X_{s-1}$ e calcule X de acordo com a decomposição π-ádica.

Características do Código

► ***Taxa e probabilidade de erro***

A ***taxa*** do código é dada por

$$\mathrm{R}(\mathcal{C}) = \mathrm{R}(\mathcal{C}_0) + \mathrm{R}(\mathcal{C}_1) + \cdots + \mathrm{R}(\mathcal{C}_{s-1}),$$

e a ***probabilidade de erro*** é limitada por

$$\mathrm{P}_{\mathrm{err}}(\mathcal{C}) \le \mathrm{P}_{\mathrm{err}}(\mathcal{C}_0) + \mathrm{P}_{\mathrm{err}}(\mathcal{C}_1) + \cdots + \mathrm{P}_{\mathrm{err}}(\mathcal{C}_{s-1}).$$

Como consequência, se cada $\mathcal{C}_i$ alcançar a capacidade em $\mathrm{MMC}(F, n, m, p_{\boldsymbol{A}_i}, \lambda_i)$, então $\mathcal{C}$ alcançará a capacidade em $\mathrm{MMC}(R, n, m, p_{\boldsymbol{A}}, \lambda)$.

► ***Complexidade***

O esquema tem ***complexidade de tempo polinomial***.

► ***Universalidade***

Analogamente a [3], não é necessário o conhecimento completo da distribuição de probabilidade de $\boldsymbol{A}$, mas apenas o conhecimento de $\mathrm{E}[\text{shape } \rho]$.

Referências Bibliográficas

[1] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, pp. 782–795, Oct. 2003.

[2] C. Feng, D. Silva, and F. R. Kschischang, "Algebraic approach to physical-layer network coding," *To appear in the IEEE Transactions on Information Theory*, vol. abs/1108.1695, Oct. 2012.

[3] S. Yang, S.-W. Ho, J. Meng, E.-h. Yang, and R. W. Yeung, "Linear operator channels over finite fields," *Computing Research Repository (CoRR)*, vol. abs/1002.2293, Apr. 2010.

[4] C. Feng, R. W. Nóbrega, F. R. Kschischang, and D. Silva, "Communication over finite-ring matrix channels," in *Proceedings of the 2013 IEEE International Symposium on Information Theory (ISIT'13)*, (Istanbul, Turkey), July 2013.