Canais Matriciais Multiplicativos sobre Anéis de Cadeia Finitos

Roberto W. Nóbrega, Chen Feng, Danilo Silva, Bartolomeu F. Uchôa-Filho

***Resumo*— Motivado pela perspectiva de codificação de rede na camada física baseada em reticulados aninhados, este artigo considera comunicação em canais matriciais multiplicativos sobre anéis de cadeia finitos. Tais canais são descritos pela expressão $Y = AX$, em que X e Y são as matrizes de entrada e saída, respectivamente, e A é a matriz de transferência. É assumido que as instâncias da matriz de transferência são desconhecidas pelo transmissor, mas disponíveis ao receptor. Como contribuições, é obtida uma forma fechada para a capacidade do canal e é proposto um esquema de codificação que alcança a capacidade em complexidade de tempo polinomial. Os resultados aqui apresentados estendem os correspondentes para corpos finitos.**

***Palavras-Chave*— Anéis de cadeia finitos, canais matriciais multiplicativos, codificação de rede linear aleatória.**

***Abstract*— Motivated by nested-lattice-based physical-layer network coding, this paper considers communication in multiplicative matrix channels over finite chain rings. Such channels are defined by the law $Y = AX$, where X and Y are the input and output matrices, respectively, and A is called the transfer matrix. We assume that the instances of the transfer matrix are unknown to the transmitter, but available at the receiver. As contributions, we obtain a closed-form expression for the channel capacity, and we propose a coding scheme that can achieve this capacity with polynomial time complexity. Our results extend the corresponding ones for finite fields.**

***Keywords*— Finite chain rings, multiplicative matrix channels, random linear network coding.**

I. Introdução

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

$$\boldsymbol{Y} = \boldsymbol{A}\boldsymbol{X}, \tag{1}$$

em que $\boldsymbol{A} \in \mathbb{F}_q^{m\times n}$ é a *matriz de transferência*. Tais canais são modelos adequados para a comunicação fim-a-fim entre um nó fonte e um nó destino de uma rede de comunicação livre de erros (mas possivelmente sujeita a apagamentos de enlace), cujos nós intermediários efetuam codificação de rede linear aleatória [1]. Nesse contexto, $\boldsymbol{X}$ é a matriz cujas linhas são os n pacotes (de comprimento ℓ) transmitidos pelo nó fonte, $\boldsymbol{Y}$ é a matriz cujas linhas são os m pacotes recebidos pelo nó destino e $\boldsymbol{A}$ é uma matriz aleatória cujas entradas são determinadas por fatores tais como a topologia da rede e a escolha aleatória dos coeficientes de codificação de rede. Note que cada pacote pode ser visto como um elemento do espaço de mensagem $\Omega = \mathbb{F}_q^\ell$, um espaço vetorial finito.

R. W. Nóbrega, D. Silva, B. F. Uchôa-Filho: Departamento de Engenharia Elétrica, Universidade Federal de Santa Catarina, Brasil. E-mails: {rwnobrega, danilo, uchoa}@eel.ufsc.br. C. Feng: Department of Electrical and Computer Engineering, University of Toronto, Canada. Email: cfeng@eecg.utoronto.ca.
Este trabalho foi parcialmente financiado pelo CNPq.

O presente trabalho considera canais matriciais multiplicativos sobre *anéis de cadeia finitos* (dos quais corpos finitos são um caso particular). A motivação vem de *codificação de rede na camada física* [2] operando de acordo com a estratégia de comunicação cooperativa conhecida como *computa-e-encaminha* [3]. De fato, em [4] é mostrado que, em uma rede sem-fio empregando computa-e-encaminha sobre um reticulado aninhado qualquer, o canal de comunicação fim-a-fim entre um nó fonte e um nó destino ainda pode ser modelado pela mesma expressão (1). A diferença é que, nesse caso, o anel em questão não é um corpo finito, mas um *domínio de ideais principais* T (tipicamente os inteiros, $\mathbb{Z}$, os inteiros gaussianos, $\mathbb{Z}[i]$, ou os inteiros de Eisenstein, $\mathbb{Z}[\omega]$), sendo o espaço de mensagens Ω um *T-módulo finito*. Sendo assim, $\Omega \cong T/\langle d_1\rangle \times T/\langle d_2\rangle \times \cdots \times T/\langle d_\ell\rangle$, em que $d_1, d_2, \ldots, d_\ell \in T$ são elementos não-nulos e não-inversíveis satisfazendo $d_1 \mid d_2 \mid \cdots \mid d_\ell$. Uma situação particular comumente encontrada na prática é aquela na qual os d_is são todos potências de um dado primo de T. Nesse caso, o espaço de mensagens Ω também pode ser visto como um *R-módulo finito*, em que $R = T/\langle d_\ell\rangle$ é um *anel de cadeia finito*.

MMCs sobre corpos finitos foram estudados sob um enfoque probabilístico de acordo com diferentes suposições sobre a matriz de transferência [5]–[10]. Neste trabalho são considerados MMCs com conhecimento do estado do canal no receptor (CSIR), isto é, é assumido que as instâncias da matriz de transferência $\boldsymbol{A}$ são desconhecidas do transmissor, mas disponíveis ao receptor. Fora isso, não é imposta qualquer restrição às estatísticas de $\boldsymbol{A}$, exceto que essa deve ser independente de $\boldsymbol{X}$. Como contribuições, é obtida uma forma fechada para a capacidade do canal (§V-A) e é proposto um esquema de codificação capaz de alcançar essa capacidade em tempo polinomial (§V-B a §V-D). O esquema combina diversos códigos sobre um corpo finito para obter um código sobre o anel de cadeia finito e é baseado na *expansão π-ádica* de elementos do anel. Tais resultados podem ser adaptados para o cenário não-coerente, isto é, no caso em que as instâncias da matriz de transferência são desconhecidas tanto do transmissor quanto do receptor (§V-E). Os resultados aqui apresentados estendem alguns daqueles obtidos por Yang e colaboradores em [7], o qual lida com o caso de corpos finitos. As provas dos lemas e teoremas foram omitidas por falta de espaço, mas podem ser encontradas em [11].

II. Anéis de Cadeia Finitos

Apresentam-se aqui alguns conceitos sobre anéis de cadeia finitos e álgebra linear sobre tais anéis [12]–[15]. Subentende-se pelo termo *anel* um anel comutativo com identidade $1 \neq 0$.

A. Anéis de Cadeia Finitos

Um anel R é dito ser um *anel de cadeia* se, para quaisquer ideais I, J de R, tem-se $I \subseteq J$ ou $J \subseteq I$. É sabido que um anel finito R é um anel de cadeia se e somente se R for simultaneamente um *anel de ideais principais* (isto é, um anel no qual todos os ideais são gerados por um único elemento) e um *anel local* (isto é, um anel com um único ideal máximo). Seja $\pi \in R$ um gerador do ideal máximo de R e seja s o menor inteiro tal que $\pi^s = 0$. Pode-se então mostrar que R possui precisamente $s+1$ ideais, a saber,

$$R = \langle \pi^0 \rangle \supset \langle \pi^1 \rangle \supset \cdots \supset \langle \pi^{s-1} \rangle \supset \langle \pi^s \rangle = \{0\},$$

em que $\langle x \rangle$ denota o ideal gerado por $x \in R$. Neste trabalho, o parâmetro s é chamado de *profundidade* de R. Adicionalmente, sabe-se que o quociente $R/\langle \pi \rangle$ é um corpo, chamado de *corpo residual* de R. Se $q = |R/\langle \pi \rangle|$, então o tamanho de cada ideal de R é $|\langle \pi^i \rangle| = q^{s-i}$, $0 \leq i \leq s$; em particular, $|R| = q^s$. Note que $s = 1$ (de modo que $\pi = 0$) se e somente se R for um corpo finito.

Um exemplo de anel de cadeia é $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$, o anel dos inteiros modulo 8. Seus ideais são $\langle 1 \rangle = \mathbb{Z}_8$, $\langle 2 \rangle = \{0, 2, 4, 6\}$, $\langle 4 \rangle = \{0, 4\}$ e $\langle 0 \rangle = \{0\}$ (de modo que $s = 3$) e seu corpo residual é $\mathbb{Z}_8/\langle 2 \rangle \cong \mathbb{F}_2$ (de modo que $q = 2$).

Durante o restante deste artigo, R denota um anel de cadeia com profundidade s e corpo residual de ordem q. Além disso, $\pi \in R$ denota um gerador para o ideal principal de R e $\Gamma \subseteq R$ denota um conjunto fixo de representantes de classes laterais (*cosets*) do corpo residual de R. Sem perda de generalidade, assume-se que $0 \in \Gamma$.

Lema 1: Todo $x \in R$ pode ser escrito unicamente como

$$x = \sum_{i=0}^{s-1} x^{(i)} \pi^i,$$

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

A expressão acima é conhecida como *expansão π-ádica de x* (com relação a Γ). Por exemplo, a expansão 2-ádica de $6 \in \mathbb{Z}_8$ com relação a $\Gamma = \{0, 1\}$ é $6 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2$, isto é, a expansão binária usual de 6.

Note que a unicidade da expansão π-ádica (fixado Γ) permite que sejam definidos os mapeamentos $(\cdot)^{(i)} : R \to \Gamma$, para $0 \leq i < s$. Também define-se

$$x^{\underline{i}} = \sum_{j=0}^{i-1} x^{(j)} \pi^j,$$

para $0 \leq i \leq s$. Pode-se mostrar que $x^{\underline{i}} \equiv_{\pi^i} x$ para todo $x \in R$, em que $\equiv_a$ denota congruência módulo a (isto é, $x \equiv_a y$ se e somente se $x - y \in \langle a \rangle$). Em particular, $x^{(0)} = x^{\underline{1}} \equiv_\pi x$.

B. Módulos sobre Anéis de Cadeia Finitos

Um *s-shape* é uma lista não-decrescente de s inteiros não-negativos. Seja $\mu = (\mu_0, \ldots, \mu_{s-1})$ um *s-shape*. Define-se

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

Sendo um produto cartesiano de ideais de R, sabe-se que R^μ é um R-módulo. Reciprocamente, todo R-módulo M é isomorfo a R^μ para um único *s-shape* μ. Diz-se então que μ é o *shape* de M, escrevendo-se $\mu = \operatorname{shape} M$. Tem-se $|R^\mu| = q^{|\mu|}$, em que $|\mu|$ é definido como $|\mu| = \mu_0 + \mu_1 + \cdots + \mu_{s-1}$.

Seja μ um *s-shape*. Define-se $\mu - n = (\mu_0 - n, \ldots, \mu_{s-1} - n)$, que também é um *$s$-shape*. Por conveniência, escreve-se o *s-shape* $(m, m, \ldots, m)$ simplesmente como m. De acordo com essa convenção, R^m representa o mesmo objeto, seja m interpretado como um inteiro ou como um *s-shape*.

C. Matrizes sobre Anéis de Cadeia Finitos

Para qualquer subconjunto $S \subseteq R$, denota-se por $S^{m \times n}$ o conjunto de todas as matrizes $m \times n$ com entradas em S. O conjunto de todas as matrizes $n \times n$ inversíveis sobre R é chamado de *grupo linear geral de grau n sobre R*, denotado por $\mathrm{GL}_n(R)$.

Seja $A \in R^{m \times n}$ e defina $r = \min\{n, m\}$. Uma matriz diagonal (não necessariamente quadrada)

$$D = \operatorname{diag}(d_1, d_2, \ldots, d_r) \in R^{m \times n}$$

é dita ser uma *forma normal de Smith* de A se existirem matrizes $P \in \mathrm{GL}_m(R)$ e $Q \in \mathrm{GL}_n(R)$ tais que $A = PDQ$ e $d_1 \mid d_2 \mid \cdots \mid d_r$. É sabido que matrizes sobre anéis de ideais principais (em particular, anéis de cadeia finitos) sempre possuem forma normal de Smith, a qual é única a menos de multiplicação das entradas da diagonal por elementos inversíveis do anel. Neste trabalho, será exigido que as entradas da diagonal sejam potências de $\pi \in R$; por conseguinte, a forma normal de Smith torna-se de fato única.

Seja $\operatorname{row} A$ e $\operatorname{col} A$ os espaços linha e coluna, respectivamente, de $A \in R^{m \times n}$. Utilizando a forma normal de Smith, pode-se mostrar que $\operatorname{row} A$ é isomorfo a $\operatorname{col} A$. Define-se o *shape* da matriz A como $\operatorname{shape} A = \operatorname{shape}(\operatorname{row} A) = \operatorname{shape}(\operatorname{col} A)$. Ademais, $\mu = \operatorname{shape} A$ se e somente se a forma normal de Smith de A for dada por

$$\operatorname{diag}(\underbrace{1, \ldots, 1}_{\mu_0}, \underbrace{\pi, \ldots, \pi}_{\mu_1 - \mu_0}, \ldots, \underbrace{\pi^{s-1}, \ldots, \pi^{s-1}}_{\mu_{s-1} - \mu_{s-2}}, \underbrace{0, \ldots, 0}_{r - \mu_{s-1}}),$$

em que $r = \min\{n, m\}$. Por exemplo, considere a matriz

$$A = \begin{bmatrix} 4 & 3 & 6 \\ 6 & 7 & 2 \end{bmatrix}$$

sobre $\mathbb{Z}_8$. Então, $A = PDQ$, em que

$$P = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} 4 & 3 & 6 \\ 1 & 2 & 6 \\ 5 & 6 & 3 \end{bmatrix},$$

de modo que $\operatorname{shape} A = (1, 2, 2)$.

Seja λ um *s-shape*. Denota-se por $R^{n \times \lambda}$ o subconjunto de matrizes em $R^{n \times \ell}$ cujas linhas são elementos de R^λ, em que $\ell = \lambda_{s-1}$. Tem-se $|R^{n \times \lambda}| = q^{n|\lambda|}$. Finalmente, estende-se os mapeamentos $(\cdot)^{(i)}$ de elementos de R para matrizes e vetores com entradas em R, entrada-a-entrada. Assim, $A \in R^{n \times \lambda}$ se e somente se $A^{(i)} = \begin{bmatrix} B_i & 0 \end{bmatrix} \in \Gamma^{n \times \ell}$, para algum $B_i \in \Gamma^{n \times \lambda_i}$, $0 \leq i < s$.

III. Modelo do Canal

No decorrer deste artigo, símbolos em negrito são usados para representar variáveis aleatórias e símbolos regulares são usados para suas amostras.

Um *canal discreto sem memória* (*DMC*) [16] com entrada $\boldsymbol{x}$ e saída $\boldsymbol{y}$ é definido por uma tripla $(\mathcal{X}, p_{\boldsymbol{y}|\boldsymbol{x}}, \mathcal{Y})$, em que $\mathcal{X}$ e $\mathcal{Y}$ são chamados de *alfabeto de entrada e saída* do canal, respectivamente, e $p_{\boldsymbol{y}|\boldsymbol{x}}$, chamado de *probabilidade de transição* do canal, representa a probabilidade de $\boldsymbol{y} = y \in \mathcal{Y}$ ser recebido dado que $\boldsymbol{x} = x \in \mathcal{X}$ foi transmitido. O canal é sem memória no sentido de que o símbolo de saída em um dado instante depende apenas do símbolo de entrada nesse mesmo instante, sendo condicionalmente independente de símbolos de entrada e saída passados. A *capacidade* do canal é dada por

$$C = \max_{p_{\boldsymbol{x}}} \mathsf{I}(\boldsymbol{x}; \boldsymbol{y}),$$

em que $\mathsf{I}(\boldsymbol{x}; \boldsymbol{y})$ é a informação mútua entre $\boldsymbol{x}$ e $\boldsymbol{y}$, sendo a maximização efetuada sobre todas as possíveis distribuições de entrada $p_{\boldsymbol{x}}$.

Sejam R um anel de cadeia finito, n e m inteiros positivos, λ um s-*shape* e $p_{\boldsymbol{A}}$ uma distribuição de probabilidade sobre $R^{m\times n}$. Define-se o MMC com CSIR sobre R como um DMC com entrada $\boldsymbol{X} \in R^{n\times\lambda}$, saída $(\boldsymbol{Y}, \boldsymbol{A}) \in R^{m\times\lambda} \times R^{m\times n}$ e probabilidade de transição

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

Neste trabalho, denota-se o canal recém definido simplesmente por $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \lambda)$. Também faz-se uso da variável aleatória $\boldsymbol{\rho} = \operatorname{shape} \boldsymbol{A}$, distribuída de acordo com

$$p_{\boldsymbol{\rho}}(\rho) = \sum_{A:\, \operatorname{shape} A = \rho} p_{\boldsymbol{A}}(A).$$

Por fim, é definido $\ell = \lambda_{s-1}$ (comprimento do pacote).

Um *código (de bloco) matricial de comprimento* N destinado a $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \lambda)$ é definido por um par $(\mathcal{C}, \Phi)$, em que $\mathcal{C} \subseteq (R^{n\times\lambda})^N$ e $\Phi : (R^{m\times\lambda} \times R^{m\times n})^N \to \mathcal{C}$ é a *função de decodificação*. Muitas vezes, abusa-se da notação e escreve-se $\mathcal{C}$ no lugar de $(\mathcal{C}, \Phi)$. A *taxa* do código $\mathcal{C}$ é definida por $\mathrm{R}(\mathcal{C}) = (\log|\mathcal{C}|)/N$ e a *probabilidade de erro*, denotada por $\mathrm{P_e}(\mathcal{C})$, é definida de maneira usual [16]. Quando $N = 1$, diz-se que $\mathcal{C}$ é um código matricial *one-shot*; caso contrário, $\mathcal{C}$ é dito ser *multi-shot*.

IV. Revisão de MMCs sobre Corpos Finitos

Esta seção revisa alguns dos resultados existentes acerca de MMCs com CSIR sobre corpos finitos (isto é, $R = \mathbb{F}_q$). Note que, nesse caso, $s = 1$, $\lambda = \ell$ e $\boldsymbol{\rho} = \operatorname{rank} \boldsymbol{A} \triangleq \boldsymbol{r}$. O seguinte resultado é autoria de Yang e colaboradores [7], [8].

Teorema 2: [7, Prop. 1] A capacidade de $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \ell)$ é dada por

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

em dígitos q-ários por uso do canal, e é alcançada se a entrada for uniformemente distribuída sobre $\mathbb{F}_q^{n\times\ell}$. Em particular, a capacidade depende de $p_{\boldsymbol{A}}$ apenas através de $\mathsf{E}[\boldsymbol{r}]$.

Em [7], [8] também são propostos dois esquemas de codificação *multi-shot* para MMCs sobre corpos finitos, capazes de alcançar a capacidade dada pelo Teorema 2. O primeiro faz uso de códigos de métrica de posto [17] e requer $\ell \geq n$; o segundo é baseado em codificação aleatória e não impõe nenhuma restrição sobre ℓ. Ambos têm complexidade de tempo polinomial. Ressalta-se que ambos os esquemas de codificação são "universais" no sentido de que apenas o valor esperado $\mathsf{E}[\boldsymbol{r}]$ é levado em conta na construção do código (não é necessário o conhecimento completo de $p_{\boldsymbol{A}}$, nem mesmo de $p_{\boldsymbol{r}}$).

V. MMCs sobre Anéis de Cadeia Finitos

Considere novamente o caso de um anel de cadeia finito genérico R.

A. Capacidade do Canal

O seguinte resultado generaliza o Teorema 2. A prova faz uso do fato de que se $\mathbf{X}$ for uniforme sobre $R^{n\times\lambda}$, então $A\mathbf{X}$ será uniforme sobre seu suporte, o qual tem cardinalidade dada por $q^{\rho_{s-1}\lambda_0+\rho_{s-2}\lambda_1+\cdots+\rho_0\lambda_{s-1}}$, em que $\rho = \operatorname{shape} A$.

Teorema 3: A capacidade de $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \lambda)$ é dada por

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

em símbolos q-ários por uso do canal, e é alcançada se a entrada for uniformemente distribuída sobre $R^{n\times\lambda}$. Em particular, a capacidade depende de $p_{\boldsymbol{A}}$ apenas através de $\mathsf{E}[\boldsymbol{\rho}]$.

B. Resultados Auxiliares

Antes de descrever o esquema de codificação proposto, são apresentados dois lemas que tratam da solução de sistemas de equações lineares sobre um anel de cadeia finito. O primeiro deles converte um sistema de equações lineares sobre um anel de cadeia finito em múltiplos sistemas sobre o corpo residual.

Lema 4: Seja $y \in R^n$ e $A \in \mathrm{GL}_n(R)$. Seja $x \in R^n$ a única solução de $Ax = y$. Então, a expansão π-ádica de x pode ser obtida recursivamente através de

$$A^{(0)}x^{(i)} \equiv_\pi y^{(i)} - \left(Ax^{\underline{i}}\right)^{(i)},$$

para $0 \leq i < s$. [Lembre-se de que $A \in \mathrm{GL}_n(R)$ se e somente se $A^{(0)} \in \mathrm{GL}_n(R/\langle\pi\rangle)$.]

O segundo problema trata da solução de sistemas diagonais de equações lineares. No que segue, $M_{j:j'}$ denota a submatriz de M contendo a linha j até (mas não incluindo) a linha j', em que as entradas das matrizes são indexadas começando de 0.

Lema 5: Seja $Y \in R^{m\times\lambda}$ e $D \in R^{m\times n}$, em que D está na forma normal de Smith e tem *shape* ρ. Se $Y = DX$, então

$$X^{(i)}_{0:\rho_{s-i-1}} = \begin{bmatrix} Y^{(i)}_{0:\rho_0} \\ Y^{(i+1)}_{\rho_0:\rho_1} \\ \vdots \\ Y^{(i+s-1)}_{\rho_{s-i-2}:\rho_{s-i-1}} \end{bmatrix},$$

para $0 \leq i < s$.

Exemplo: Seja $R = \mathbb{Z}_8$, com $\pi = 2$ e $\Gamma = \{0, 1\}$. Seja $n = 5$, $m = 4$ e $\lambda = (3, 4, 6)$. Suponha que $\rho = (1, 3, 4)$, de modo que $D = \operatorname{diag}(1, 2, 2, 4) \in \mathbb{Z}_8^{4\times 5}$. Além disso, suponha que

$$Y = \begin{bmatrix} 6 & 7 & 1 & 2 & 0 & 4 \\ 6 & 4 & 2 & 0 & 0 & 0 \\ 0 & 2 & 6 & 4 & 0 & 0 \\ 4 & 0 & 4 & 0 & 0 & 0 \end{bmatrix}.$$

Daí, pode-se concluir que

$$X^{(0)} = \begin{bmatrix} 0 & 1 & 1 & & & \\ 1 & 0 & 1 & & & \\ 0 & 1 & 1 & & & \\ 1 & 0 & 1 & & & \\ * & * & * & & & \end{bmatrix},$$

$$X^{(1)} = \begin{bmatrix} 1 & 1 & 0 & 1 & & \\ 1 & 1 & 0 & 0 & & \\ 0 & 0 & 1 & 0 & & \\ * & * & * & * & & \\ * & * & * & * & & \end{bmatrix},$$

$$X^{(2)} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{bmatrix},$$

em que $*$ denota entrada desconhecida e espaço em branco denota entrada igual a zero. Note que as entradas desconhecidas são devido a $\rho = \operatorname{shape} D$, enquanto que as entradas em branco são devido a λ (veja §II-C).

C. Esquema de Codificação

Aqui propõe-se um esquema de codificação para o canal, o qual é baseado na expansão π-ádica discutida em §II-A e nas ideias da subseção anterior. Por simplicidade de exposição, inicia-se descrevendo o esquema para o caso particular de códigos *one-shot*. O caso geral será discutido em seguida. De agora em diante, seja $\mathbb{F}_q = R/\langle\pi\rangle$.

Sejam $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ (chamados de *códigos componentes*) códigos matriciais *one-shot* sobre o corpo residual $\mathbb{F}_q$, em que cada $\mathcal{C}_i$, para $0 \le i < s$, é um código para $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}_i, \lambda_i)$, para alguma matriz de transferência $\boldsymbol{A}_i \in \mathbb{F}_q^{m\times n}$. Os códigos componentes serão combinados para se obter um código matricial $\mathcal{C}$ *one-shot* sobre o anel de cadeia R, projetado para $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \lambda)$. O código $\mathcal{C}$ é chamado de *código composto*.

1) Construção do código: Denota-se por $\varphi : R \to \mathbb{F}_q$ a projeção natural de R sobre $\mathbb{F}_q$, e por $\bar{\varphi} : \mathbb{F}_q \to \Gamma$ o mapeamento seletor do representante da classe lateral, que possui a propriedade de que $\varphi(\bar{\varphi}(x)) = x$ para todo $x \in \mathbb{F}_q$. O código $\mathcal{C} \subseteq R^{n\times\lambda}$ é definido por

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

em que

$$X^{(i)} = \begin{bmatrix} \bar{\varphi}(X_i) & 0 \end{bmatrix} \in \Gamma^{n\times\ell}. \tag{2}$$

Verifica-se que $\mathcal{C}$ de fato satisfaz as restrições de $R^{n\times\lambda}$.

2) Decodificação: O procedimento de decodificação é descrito a seguir, sendo baseado nas ideias em §V-B. Intuitivamente, o decodificador decompõe um único MMC sobre o anel de cadeia em múltiplos MMCs sobre o corpo residual. No que segue, $M_{j\times k}$ denota a submatriz $j \times k$ superior-esquerda de M.

Passo 1. O decodificador, que conhece a matriz de transferência A, inicia computando $D \in R^{m\times n}$, a forma normal de Smith de A. O decodificador também calcula $P \in \mathrm{GL}_m(R)$ e $Q \in \mathrm{GL}_n(R)$ tais que $A = PDQ$.

Passo 2. Sejam as matrizes $\tilde{X} \triangleq QX \in R^{n\times\lambda}$ (desconhecida pelo decodificador) e $\tilde{Y} \triangleq P^{-1}Y \in R^{m\times\lambda}$ (calculada pelo decodificador), de modo que a equação $Y = AX$ passa a ser equivalente a $\tilde{Y} = D\tilde{X}$. Dessa última equação, o decodificador obtém informação parcial sobre $\tilde{X}$. Mais precisamente, o decodificador computa $\tilde{X}^{(i)}_{\rho_{s-i-1}\times\lambda_i}$, para $0 \le i < s$, de acordo com o Lema 5.

Passo 3. De posse de $\tilde{X}^{(i)}_{\rho_{s-i-1}\times\lambda_i}$, para $0 \le i < s$, o decodificador tentará então decodificar X baseado na equação

$$\tilde{X} = QX,$$

em um estilo similar à decodificação *multi-estágio*. De fato, analogamente ao Lema 4, tem-se, para $0 \le i < s$,

$$\tilde{X}^{(i)} - \left(QX^{\underline{i}}\right)^{(i)} \equiv_\pi Q^{(0)}X^{(i)}.$$

Considerando apenas as ρ_{s-i-1} linhas superiores (pois as linhas restantes são desconhecidas) e mantendo apenas as λ_i colunas da esquerda (pois sabe-se de antemão que as colunas restantes são nulas), obtém-se

$$\tilde{X}^{(i)}_{\rho_{s-i-1}\times\lambda_i} - \left(Q_{\rho_{s-i-1}\times n}X^{\underline{i}}_{n\times\lambda_i}\right)^{(i)} \equiv_\pi Q^{(0)}_{\rho_{s-i-1}\times n}X^{(i)}_{n\times\lambda_i}.$$

Projetando em $\mathbb{F}_q$ (ou seja, aplicando φ em ambos os lados da equação) e acrescentando um número suficiente de linhas nulas (de modo a se obter um sistema $m \times n$), chega-se finalmente a

$$Y_i = A_iX_i, \tag{3}$$

em que $Y_i \in \mathbb{F}_q^{m\times\lambda_i}$ e $A_i \in \mathbb{F}_q^{m\times n}$ são definidas por

$$Y_i = \begin{bmatrix} \varphi\left(\tilde{X}^{(i)}_{\rho_{s-i-1}\times\lambda_i}\right) - \varphi\left(\left(Q_{\rho_{s-i-1}\times n}X^{\underline{i}}_{n\times\lambda_i}\right)^{(i)}\right) \\ 0 \end{bmatrix}, \tag{4}$$

$$A_i = \begin{bmatrix} \varphi\left(Q_{\rho_{s-i-1}\times n}\right) \\ 0 \end{bmatrix}. \tag{5}$$

Note que a matriz Y_i só pode ser calculada depois de se conhecer $X_0, X_1, \ldots, X_{i-1}$. Portanto, neste passo, o decodificador obtém, sucessivamente, estimativas de $X_0, X_1, \ldots, X_{s-1}$ de acordo com (3). Após isso, o decodificador calcula uma estimativa de X utilizando (2) e a expansão π-ádica.

3) Extensão para o caso multi-shot: Por fim, considera-se o caso *multi-shot*. Seja $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ uma sequência de códigos matriciais componentes de comprimento N, em que $\mathcal{C}_i \subseteq (\mathbb{F}_q^{n\times\lambda_i})^N$, para $0 \le i < s$. As palavras-código do código matricial composto $\mathcal{C}$ são então dadas por $(X(1), X(2), \ldots, X(N)) \in (R^{n\times\lambda})^N$, em que $X(j)$ é obtido da j-ésima coordenada das palavras-código dos códigos componentes, de maneira análoga ao caso *one-shot*.

Prosseguindo como nos Passos 1 e 2 acima, o decodificador obtém $\tilde{X}^{(0)}_{\rho_{s-1}\times\lambda_0}(j), \tilde{X}^{(1)}_{\rho_{s-2}\times\lambda_1}(j), \ldots, \tilde{X}^{(s-1)}_{\rho_0\times\lambda_{s-1}}(j)$ e $Q(j)$, para $j = 1, \ldots, N$. O Passo 3 também é análogo, com o detalhe importante de que, antes de prosseguir ao estágio $i+1$, a sequência $(X_i(1), X_i(2), \ldots, X_i(N)) \in \mathcal{C}_i$ é decodificada por completo, com base em $(Y_i(1), Y_i(2), \ldots, Y_i(N))$ e $(A_i(1), A_i(2), \ldots, A_i(N))$, utilizando o decodificador de $\mathcal{C}_i$.

D. Taxa, Probabilidade de Erro e Complexidade

Do esquema proposto, fica claro que o i-ésimo código componente deve ser projetado para $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}_i, \lambda_i)$, em que $\boldsymbol{A}_i \in \mathbb{F}_q^{m\times n}$ é definida em (5). Em princípio, poderia-se calcular a distribuição de probabilidade de $\boldsymbol{A}_i$ se a distribuição de $\boldsymbol{A}$ for conhecida. No entanto, se for utilizado um dos esquemas de codificação propostos em [7] (veja §IV), o conhecimento exato da distribuição de $\boldsymbol{A}_i$ torna-se desnecessário tão logo se saiba o valor esperado de seu posto. De (5), tem-se $\operatorname{rank} \boldsymbol{A}_i = \boldsymbol{\rho}_{s-i-1}$, de modo que, nesse caso, apenas é necessário o conhecimento do valor esperado $\mathsf{E}[\boldsymbol{\rho}]$.

Seja $\mathcal{C}$ o código composto obtido dos códigos componentes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$. Então, $\mathcal{C}$ tem taxa

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

em dígitos q-ários. Além disso, do limitante da união, a probabilidade de erro é limitada superiormente de acordo com

$$\mathrm{P_e}(\mathcal{C}) \leq \mathrm{P_e}(\mathcal{C}_0) + \mathrm{P_e}(\mathcal{C}_1) + \cdots + \mathrm{P_e}(\mathcal{C}_{s-1}).$$

Assim, se cada $\mathcal{C}_i$ alcança a capacidade em $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}_i, \lambda_i)$, tem-se $\mathrm{R}(\mathcal{C}_i)$ arbitrariamente próximo de $\mathsf{E}[\boldsymbol{\rho}_{s-i-1}]\lambda_i$ e $\mathrm{P_e}(\mathcal{C}_i)$ arbitrariamente próximo de zero, para $0 \leq i < s$. Por conseguinte, tem-se $\mathrm{R}(\mathcal{C})$ arbitrariamente próximo de $\sum_i \mathsf{E}[\boldsymbol{\rho}_{s-i-1}]\lambda_i$ (a capacidade do canal) e $\mathrm{P_e}(\mathcal{C})$ arbitrariamente próximo de zero.

A complexidade computacional associada à decodificação do código composto é simplesmente a soma das complexidades individuais das decodificações de cada código componente, acrescida do custo de calcular a forma normal de Smith de A (o que pode ser feito com $O(nm\min\{n,m\})$ operações em R), do custo de calcular $\tilde{Y}$ (o que requer $O(m^2(m+\ell))$ operações) e do custo de $s-1$ multiplicações e adições matriciais em (4) (o que exige $O(n^2\ell)$ operações cada).

E. Extensão para o Caso Não-Coerente

Até agora considerou-se apenas o caso no qual o estado do canal é conhecido pelo receptor. No entanto, como mencionado na Introdução, é possível reutilizar o esquema de codificação proposto em §V-C mesmo no cenário não-coerente, através do uso da técnica de *treinamento de canal*. Nessa técnica, as instâncias de $\boldsymbol{A}$ são fornecidas ao receptor através da introdução de cabeçalhos na matriz transmitida $\boldsymbol{X} \in R^{n\times\lambda}$, ou seja, fixando $\boldsymbol{X} = \begin{bmatrix} I & \boldsymbol{X'} \end{bmatrix}$, em que $I \in R^{n\times n}$ é a matriz identidade e $\boldsymbol{X'} \in R^{n\times(\lambda-n)}$ é uma matriz originária de um código matricial. Para que isso funcione, é necessário que $\lambda_0 \geq n$. Note que essa técnica introduz uma sobrecarga (*overhead*) de n^2 símbolos. Entretanto, tal sobrecarga torna-se desprezível se for permitido aumentar o tamanho do pacote arbitrariamente. Assim, o esquema proposto é capaz de alcançar a capacidade nesse cenário assintótico.

VI. Conclusão

Neste trabalho foram investigados canais matriciais multiplicativos sobre anéis de cadeia finitos, os quais têm aplicações práticas em codificação de rede na camada física baseada em reticulados aninhados. Como contribuições, a capacidade do canal foi determinada, generalizando o resultado correspondente para corpos finitos. Além disso, um esquema de codificação prático que alcança a capacidade foi proposto, combinando vários códigos sobre o corpo residual para obter um novo código sobre o anel de cadeia.

Vários pontos ainda estão em aberto. O cálculo da capacidade do MMC não-coerente, um problema abordado em [7], [9] para o caso de corpos finitos, ainda necessita ser generalizado para anéis de cadeia finitos. Adicionalmente, o projeto de esquemas de codificação para o MMC não-coerente com parâmetro λ pequeno é ainda um problema em aberto mesmo no caso de corpos finitos.

Referências

[1] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, pp. 3579–3591, Aug. 2008.

[2] S. C. Liew, S. Zhang, and L. Lu, "Physical-layer network coding: Tutorial, survey, and beyond," *Physical Communication*, vol. 6, pp. 4–42, May 2013.

[3] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, pp. 6463–6486, Oct. 2011.

[4] C. Feng, D. Silva, and F. R. Kschischang, "An algebraic approach to physical-layer network coding," *Computing Research Repository (CoRR)*, vol. abs/1108.1695, Oct. 2012. To appear in the IEEE Transactions on Information Theory.

[5] M. Jafari Siavoshani, S. Mohajer, C. Fragouli, and S. Diggavi, "On the capacity of non-coherent network coding," *IEEE Transactions on Information Theory*, vol. 57, pp. 1046–1066, Feb. 2011.

[6] D. Silva, F. R. Kschischang, and R. Koetter, "Communication over finite-field matrix channels," *IEEE Transactions on Information Theory*, vol. 56, pp. 1296–1305, Mar. 2010.

[7] 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.

[8] S. Yang, J. Meng, and E.-h. Yang, "Coding for linear operator channels over finite fields," in *Proceedings of the 2010 IEEE International Symposium on Information Theory (ISIT'10)*, (Austin, Texas), pp. 2413–2417, June 2010.

[9] R. W. Nóbrega, D. Silva, and B. F. Uchôa-Filho, "On the capacity of multiplicative finite-field matrix channels," *Computing Research Repository (CoRR)*, vol. abs/1105.6115, Apr. 2013. To appear in the IEEE Transactions on Information Theory.

[10] S. Yang, S.-W. Ho, J. Meng, and E.-h. Yang, "Capacity analysis of linear operator channels over finite fields," *Computing Research Repository (CoRR)*, vol. abs/1108.4257, Dec. 2012.

[11] R. W. Nóbrega, C. Feng, D. Silva, and B. F. Uchôa-Filho, "On multiplicative matrix channels over finite chain rings." To be presented in the 2013 IEEE International Symposium on Network Coding (NetCod'13).

[12] B. R. McDonald, *Finite Rings with Identity*, vol. 28 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., 1974.

[13] A. A. Nechaev, "Finite rings with applications," in *Handbook of Algebra* (M. Hazewinkel, ed.), vol. 5, pp. 213–320, North-Holland, 2008.

[14] T. Honold and I. Landjev, "Linear codes over finite chain rings," *The Electronic Journal of Combinatorics*, vol. 7, 2000.

[15] W. C. Brown, *Matrices over Commutative Rings*, vol. 169 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., 1992.

[16] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2nd ed., 2006.

[17] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, pp. 3951–3967, Sept. 2008.